NUREG/CR-4780
EPRI NP-5613
Vol. 2

Procedures for Treating Common Cause Failures in Safety and Reliability Studies

Analytical Background and Techniques

Pickard, Lowe, and Garrick, Inc.

Prepared for
U.S. Nuclear Regulatory Commission

Electric Power Research Institute

NUREG/CR--4780-Vol.2

TI89 006721

NUREG/CR-4780
EPRI NP-5613
PLG-0547
Vol. 2
RX

Procedures for Treating Common Cause Failures in Safety and Reliability Studies

Analytical Background and Techniques

Manuscript Completed: October 1988
Date Published: January 1989

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

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

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

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

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

ABSTRACT

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

The framework comprises four major stages:

1. System Logic Model Development. The basic system failure logic is modeled in terms of basic events that represent component status.

2. Identification of Common Cause Component Groups. The principal object is to identify, using quantitative and qualitative screening, the groups of components that are felt to have significant potential for common cause failures.

3. Common Cause Modeling and Data Analysis. Common cause basic events are defined for inclusion in the logic model, to represent the residual dependent failures and probability models are constructed for each new basic event. At this stage, the logic model is extended from a component state basis to a component group impact basis. Historical data on multiple failure events are analyzed and the parameters of the probability models for common cause basic events estimated.

4. System Quantification and Interpretation of Results. The results are integrated into the system and sequence analyses and the results are analyzed.

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

The present volume contains a series of appendices that provide additional background and methodological detail on several important topics discussed in Volume I.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

ILLUSTRATIONS

TABLES

ACRONYMS

Acronym	Definition
ADS	automatic depressurization system
AFW	auxiliary feedwater
AFWS	auxiliary feedwater system
BFR	binomial failure rate
BWR	boiling water reactor
CCF	common cause failure
CCF-RBE	Common Cause Failure Reliability Benchmark Exercise
CCS	containment cooling system
CST	condensate storage tank
ECS	emergency cooling system
ECWS	emergency cooling water system
EDG	emergency diesel generator
EOP	emergency operations procedure
EPRI	Electric Power Research Institute
ESAS	engineered safeguards actuation system
ESWS	emergency service water system
FMEA	failure mode and effects analysis
HPCI	high pressure coolant injection
HPIS	high pressure safety injection system
ISI	in-service inspection
KWU	Kraftwerk Union, Federal Republic of Germany
LER	Licensee Event Report
LOCA	loss of coolant accident
LOSP	loss of offsite power
MCS	minimal cutset
MGL	multiple Greek letter
MOV	motor-operated valve
NPE	Nuclear Power Experience
PRA	probabilistic risk assessment
PSNH	Public Service of New Hampshire
PWR	pressurized water reactors

ACRONYMS (continued)

Acronym	Definition
RBE-CCF	Reliability Benchmark Exercise in Common Cause Failures
RCIC	reactor core isolation cooling system
RHR	residual heat removal
UKAEA	United Kingdom Atomic Energy Authority
USNRC	U.S. Nuclear Regulatory Commission

GLOSSARY OF TERMS AND DEFINITIONS

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

1. Component. A component is an element of plant hardware designed to provide a particular function. Its boundaries depend on the level of detail chosen in the analysis. The hierarchy of the level of detail of modeling a plant in risk and reliability analysis flows from plant, to system, to subsystem, to component, then to cause (see definition below). For system modeling purposes, a component is at the lowest level of detail in the representation of plant hardware in the models. Events that represent causes of one or more component states in a system logic model (e.g., fault tree) are found at the level of detail below the component.

2. Component State. Component state defines the component status in regard to the function that it is intended to provide. In this context, the following two general categories of component states are defined (the same states apply to higher levels of plant hardware, such as system):

   a. Available. The component is available if it is capable of performing its function according to a specified success criterion. (Not to be confused with availability, which is defined below.)

   b. Unavailable. The component is unable to perform its intended function according to a stated success criterion. It is important to note that the success criterion defined by the analyst to enable him to distinguish between available and unavailable states is not unique. This is because there are cases of several functions and operating modes for a given component, each with a different success criterion. Also, a given event in one plant may be classified differently than a similar component in another plant with different success criteria. Therefore, the specification and documentation of the success criteria and the reconciliation of potential mismatches between the data base and systems models become important tasks of the systems analyst.

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

(1) Failure. The component is not capable of performing its specified operation according to a success criterion. In order to restore the component to a state in which it is capable of operation, some kind of repair or replacement action is necessary. Additionally, the event may also be considered a failure when a component performs its function when not required or performs its function as required, but does not stop operating once meeting its success criteria. The latter is equivalent to saying that stopping when required is part of the success criterion. Therefore, failure encompasses functioning when not required, as well as not functioning when required.

(2) Functionally unavailable. The component is capable of operation, but the function normally provided by the component is unavailable due to lack of proper input, lack of support function from a source outside the component (i.e., motive power, actuation signal), maintenance, testing, or the improper interference of a person.

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

c. Potentially Unavailable. The component is capable of performing its function according to a success criterion, but an incipient or degraded condition, as defined below, exists.

(1) Degraded. The component is in such a state that it exhibits reduced performance but insufficient degradation to declare the component unavailable according to the specified success criterion. Examples of degraded states are relief valves

opening prematurely outside the technical specification limits but within a safety margin and pumps producing less than 100% flow but within a stated performance margin.

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

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

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

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

3. Cause. A cause is simply an explanation for why a component became unavailable or is potentially unavailable. In complete, traditional system logic models, the cause level is the most detailed level of analysis and is almost always implicit in the quantification model, being located below the component level. With every cause, there exists a mechanism fully or partially responsible for the state of a component when an event includes a single component state; the cause of the component state is referred to loosely as a root cause. In more complex events involving two or more component states, a particular component state or set of component states can result from either a root cause or can be caused by the state of another component; i.e., component cause.

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

5. Independent Event. An independent event is an event in which a component state occurs, causally unrelated to any other component state. Two events, A and B, are independent if and only if $P(A \text{ and } B) = P(A) \cdot P(B)$.

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

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

7. Common Cause Event. It is not the purpose of this report to resolve, once and for all, the issues associated with attempts to provide a clear and unambiguous definition of the term "common cause event." The only way to treat these issues is to adopt a cause-effect event classification system, such as that described in detail in Reference 2-4 and summarized in Appendix A. Here, we define what common cause events mean to the systems analyst. In the context of system modeling, common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are a direct result of a shared cause. It is also implied that the shared cause is not another component state because such cascading of component states is normally due to a functional coupling mechanism. Such functional dependencies are normally modeled explicitly in systems models without the need for special common cause event models. The special models that have been developed to model common cause events, such as the beta factor, binomial failure rate, multiple Greek letter, basic parameter, common load, and other models, all apply to root-caused events branching into impact multiple components, but are generally not applied to component-caused events. A more focused definition of common cause events is presented in Section 2.

8. Root Cause. Ideally, the cause of an event can be traced to an event that occurred at some distinct but possibly unknown point in time. These causal events are known as "root cause." There are four general types of root causes.

   a. Hardware. Isolated random equipment failures due to causes inherent in the affected component.

   b. Human. Errors during plant operations (dynamic interaction with the plant), errors during equipment testing or maintenance, and errors during design, manufacturing, and construction.

   c. Environmental. Events that are external to the equipment but internal to the plant that result in environmental stresses being applied to the equipment.

d. External. Events that initiate external to the plant that result in abnormal environmental stresses being applied to the equipment.

9. Coupling Mechanism. A coupling mechanism is a way to explain how a root cause propagates to involve multiple equipment items; e.g., components. The three broad categories of coupling mechanisms are functional, spatial, and human.

   a. Functional Couplings

      (1) Connected equipment. Encompasses plant design involving shared equipment, common input, and loop dependencies plus situations in which the same equipment provides multiple functions.

      (2) Nonconnected equipment. Encompasses interrelated success criteria, such as the relationship between a standby system and the system it is supporting. More subtle forms of nonconnected equipment couplings are environmental conductors, such as heating, ventilation, and air conditioning systems.

   b. Spatial Couplings

      (1) Spatial proximity. Refers to equipment found within a common room, fire barriers, flood barriers, or missile barriers.

      (2) Linked equipment. Equipment in different locations that, although not functionally related, is similarly affected by an extreme environmental condition possibly due to the breach of a barrier.

   c. Human Couplings. Refers to activities, such as design, manufacturing, construction, installation, quality control, plant management, station operating procedures, emergency procedures, maintenance, testing and inspection procedures, and implementation, etc.

10. Unavailability. The probability (relative frequency) that a system or component occupies the unavailable state at a point in time. In applied risk and reliability evaluations, this point in time is when a randomly occurring initiating event or system or component challenge occurs. Availability is the complement of unavailability.

11. Unreliability. The probability (relative frequency) that a system or component fails (in regard to specified success criteria) during a specified time interval. This time interval is often referred to as the "mission time."

12. Shock. A concept used in some common cause models, such as the BFR model, to explain how component states other than intrinsic, random, independent failures occur. A shock is an event that occurs at a random point in time and acts on the system; i.e., all the components in the system simultaneously. There are two kinds of shocks distinguished by the potential impact of the shock event, as defined below.

    a. Lethal Shock. A lethal shock is a shock in which all the components in a system are failed, with certainty, any time the shock occurs.

    b. Nonlethal Shock. A nonlethal shock is a shock that has some independent chance that each component in the system fails as a result of the shock. The range of possible outcomes (each having a different probability of occurrence) of a nonlethal shock range from no component failures to all the components failed.

13. Common Cause Component Group. A group of usually similar components that are considered to have a high potential of failing due to the same cause.

14. Common Cause Basic Event. An event involving common cause failure of a specific subset of components within a common cause component group.

15. Impact Vector. An assessment of the impact an event would have on a common cause component group. The impact is usually measured as the number of failed components out of a set of similar components in the common cause component group.

16. Defensive Strategy. A set of operational, maintenance, and design measures taken to diminish the frequency and/or the consequences of common cause failures. Common cause design review, surveillance testing, and redundancy are, therefore, examples of tactics contributing to a defensive strategy.

ACKNOWLEDGMENTS

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

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

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

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

INTRODUCTION

This is the second volume of a two-volume report on Procedures for Treating Common Cause Failures in Safety and Reliability Studies developed under the joint sponsorship of the Electric Power Research Institute and the U. S. Nuclear Regulatory Commission.

The overall objectives of this work are to:

1. Provide a procedural framework for system-level common cause analysis for use in applied risk and reliability evaluations by and for the nuclear industry.

2. Provide a comprehensive and integrated systems analysis framework for common cause events 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 events analyst.

4. Account for advances that have been made in the state of the art in common causes and thereby serve to update previously published PRA procedures guides.

5. Identify important interfaces between the various tasks, including qualitative analysis, systems modeling, event classification, parameter estimation, and quantitative analysis tasks.

6. Provide the flexibility of choice among alternative systems modeling approaches and techniques for parameter estimation and data handling when alternatives exist and when the superior choice cannot be easily determined.

7. Solicit a sufficiently broad base of input to achieve a consensus on the principles of common cause failure analysis to the extent possible within the constraints of schedule and budget.

Volume I, entitled "Procedural Framework and Examples," presents a framework and a set of procedures for the analysis of system-level common cause failures in risk and reliability studies. This procedure involves four major stages, each of which contains a number of steps, as outlined in Figure 1 and explained in detail in Section 3 of Volume I.

The present volume contains a series of appendices that provide additional background and methodological detail on several important topics discussed in Volume I. Each appendix is self-contained and addresses one specific issue.

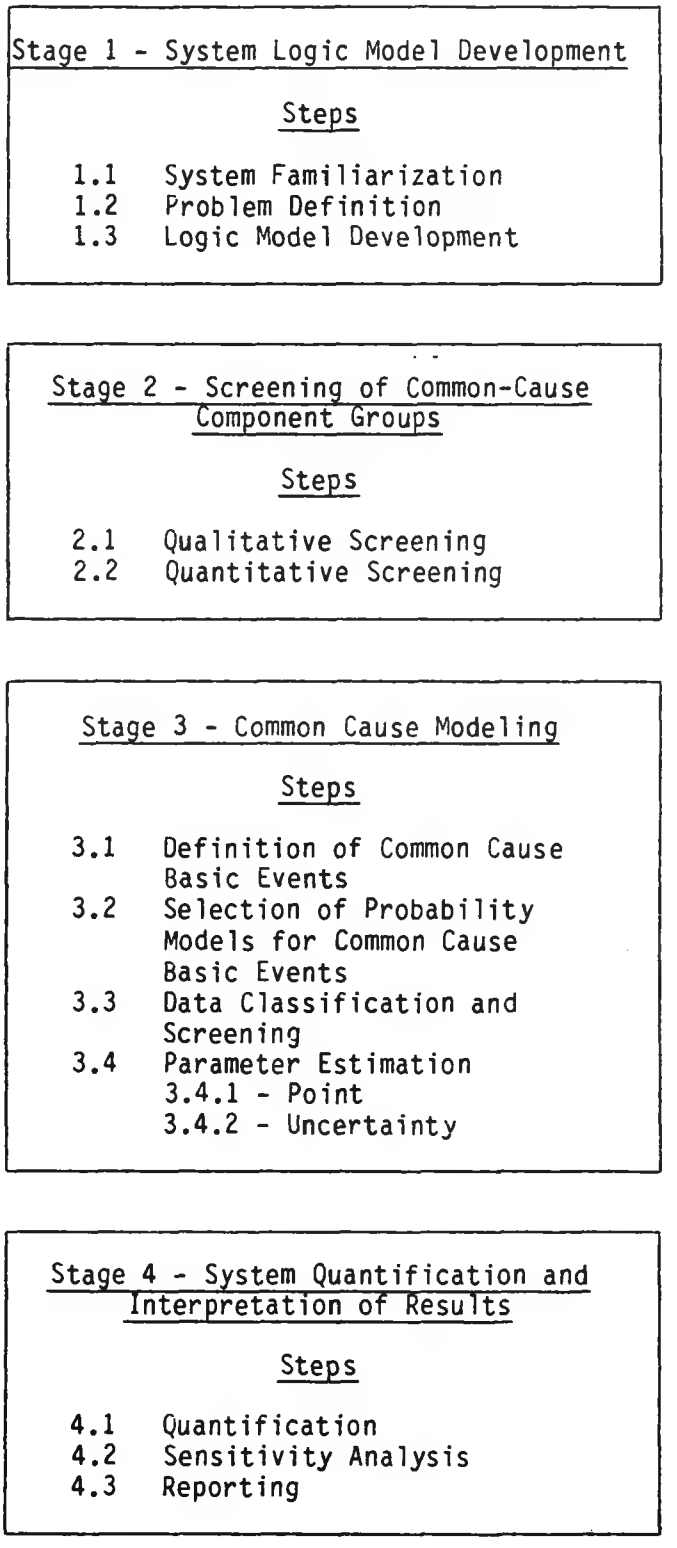


Figure 1. Stages and Steps of a Procedural Framework for Common Cause Analysis

Appendix A describes a classification system that has been used to classify and analyze failure reports and to extract information in support of step 3.3 (Data Classification and Screening) of the procedure. This scheme should be regarded as state-of-the-art development and some evolution and refinement is ongoing.

Appendix B is a more detailed presentation of the so-called Generic Cause Approach to the qualitative screening of common cause scenarios and determination of those components within the system that need to be considered for more detailed modeling from the point of view of common cause failures.

Appendix C describes the various parametric common cause failure models and the estimators for their parameters. It discusses key assumptions behind the models and the estimators and the implication of those assumptions. The material in this appendix supplements the presentation, in Volume I, of steps 3.2 (Selection of Probability Models), and 3.4 (Parameter Estimation - Point Estimate) of the procedure.

Appendix D establishes the relationships among data bases of systems of identical components having different levels of redundancy. It obtains the relationships among model parameters that stem from the data base relationships and provides guidance for interpretation of data from systems of different size and for the assignment of impact vectors; i.e., for mapping up and mapping down impact vectors. The material in this appendix supplements a summary presentation in Volume I, step 3.3 (Data Classification and Screening).

Appendix E presents statistical uncertainty distributions for the model parameters in support of step 3.4 (Parameter Estimation). It also derives mean value estimators for the various parameters.

Appendix F provides additional guidance on dealing with practical difficulties in implementing the fault tree expansion approach discussed in step 3.1 (Definition of Common Cause Basic Events).

Appendix G discusses consideration of recovery actions in common cause failure analysis in support of stages 2 and 4 of the procedure.

Finally, Appendix H discusses the pitfalls of using generic common cause failure probabilities for plant-specific analyses.

APPENDIX A

A DATA CLASSIFICATION SYSTEM

This appendix briefly describes a classification system that can be used to classify and categorize event reports to extract information for the study of dependent events and, in particular, for the context of this report, to identify candidate common cause events for further analysis. The classification system described below is essentially the system developed in a project sponsored by EPRI (Reference A-1) and applied to a large number of failure events in a companion project (Reference A-2). In the following presentation of the classification system, it is assumed that the reader is familiar with the basic concepts and definitions presented in Section 2 of this report. While this scheme has been, and will continue to be used as the current state-of-the-art, it is not necessarily definitive, and other more comprehensive schemes may be developed to more explicitly present information, particularly on root causes, coupling mechanisms, and failures of defenses.

A.1 COMPONENT STATES AND FAULT MODES

A.1.1 Component State Space

Various states that a component can occupy with regard to its intended function and according to a given success criterion are presented in Figure A-1. The first tier reflects the principle that all component states can be categorized based on whether the component was available to perform its function according to the specified success criterion. The second tier breakdown of the available category shows that even though a component may be capable of fulfilling its function, an incipient or degraded condition could exist in that component or in a component directly impacting it. The available states, therefore, are categorized as either "nominal" (i.e., "good") or "potentially unavailable."

The final breakdown in Figure A-1 is the distinction between "failed" and "functionally unavailable" states in the case of unavailable states, and "potentially failed" and "potentially functionally unavailable" in the case of potentially unavailable states. This figure also shows the symbols provided for each of the above component states. The application of event classification will be discussed later. Brief descriptions of the component states used are listed below:

- Functionally Unavailable State (⊠). The component is capable of operating, but the function normally provided by the component is unavailable for one of the following reasons:

  --Loss of Input. This refers to loss of motive power, command signal, water source, cooling water, air, etc.

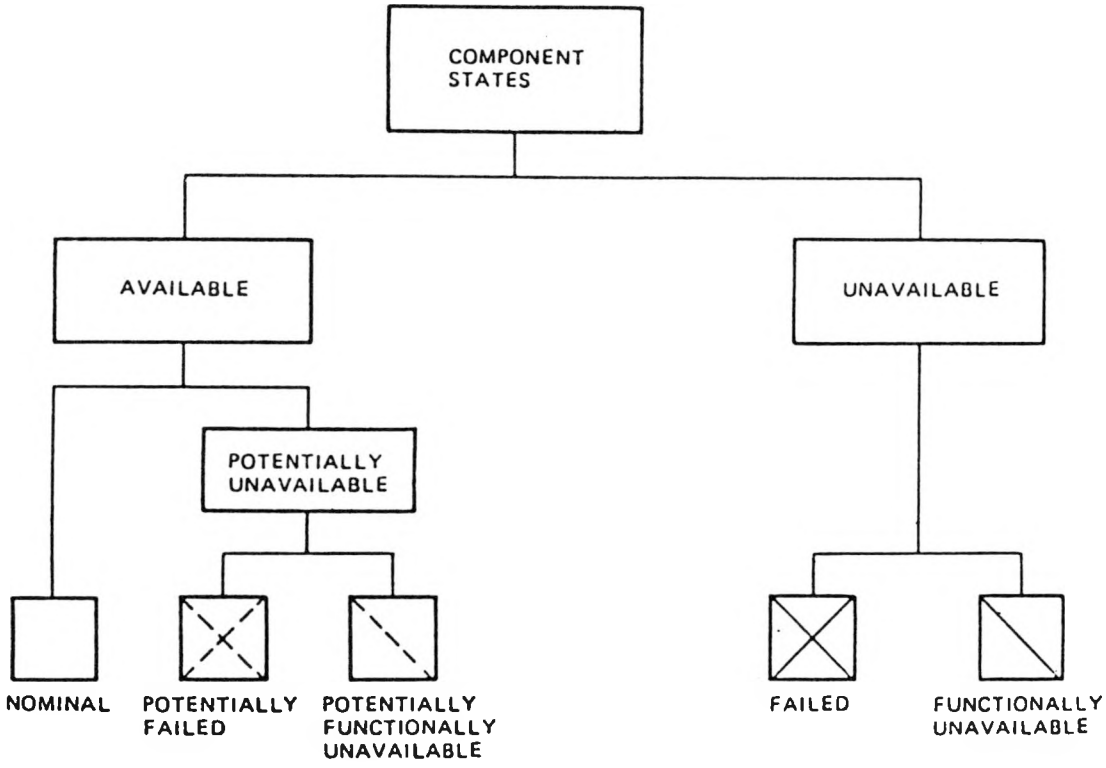


Figure A-1. Component States Used in Classification System

--Preventive Maintenance and Calibration. The component has been removed from service to perform a preventive maintenance activity (including modifications) or calibration check, thereby rendering the component incapable of performing its function.

--Testing. Some form of diagnostic test is being performed on the component that necessitates the component's isolation from the system, resulting in its inability to fulfill its function.

- Failed State (⊠). The component is not capable of performing its function, or it functions when not required. In order to restore the component to operability, some kind of repair or replacement action is necessary. In cases where a component becomes damaged and needs to be repaired and the cause of the damage is the failure of another component or system on which the damaged component is functionally dependent, the damaged component is classified as failed. An example of this case is overheating of a component due to HVAC system failure.

- Potentially Functionally Unavailable State (⧅). An incipient or degraded condition exists, generally for a component on which the component of interest is dependent so that, if left unremedied, it could result in failure of the first component. The component of interest would then become functionally unavailable.

- Potentially Failed State (⧅). A condition exists either in the component of interest or in a component impacting the component of interest that, if left unremedied, could render the component failed. This category of states includes:

  --Degraded. The component is in such a state that it exhibits reduced performance that, potentially, if left uncorrected, could result in failure.

  --Incipient. The component is in a condition (i.e., exhibiting a small oil leak, loose piece of equipment, or wear) for which performance has not been interfered with, yet if the condition is left unremedied, it could potentially render the component failed.

- Nominal State (□). The component is capable of performing its function according to a success criterion, and no incipient or degraded condition exists.

A.1.2 Fault Modes

The fault modes of a component are its characteristic symptoms of not being able to perform its function. They describe the manner in which component states occur. The term "fault" modes is used in favor of the more frequently used "failure" modes because such modes can be ascribed to component states other thar the "failed" state. In fact, all states except the nominal state can be ascribec fault modes. The assignment of an unavailable component state signifies that its success criteria were in some way violated. However, the fault mode describes the manner in which the success criteria were violated. The distinction between

fault modes can be important for equipment (e.g., valves) that can operate in more than one way (e.g., open/close), depending on system requirements. This distinction also enables users of classified data to extract only those portions of the unavailable state statistics that are applicable to the specific problem.

In general, fault modes vary from one component type to another. However, several generic modes can be defined that describe to a large extent the most frequently observed fault modes for a large number of components. A generic list of fault modes is provided in Tables A-1a and A-1b. For example, the mode "transfers open" (TO) applies to both reactor trip breakers and relief valves, and "fails to start" is applicable to diesel generators, as well as pumps.

Depending on the level of detail desired and the availability of information, one may choose to define more specific fault modes. For instance, a valve may fail to open automatically although it is still operational manually. In this case, the fault mode can be specified as "fails to open automatically (FOA)," instead of a more general mode of "fails to open (FO)." It is important to note that FO applies to the case in which the valve fails to open both automatically and manually as well as the case in which, due to lack of information, no distinction can be made. In a situation in which the component state is classified as potential, the corresponding fault mode is also labeled potential. The mode code for this situation is formed by using the letter "P" in conjunction with the code for the actual mode; e.g., PFO for "potentially fails to open."

A.2 CAUSE CATEGORIES

The discussion in this section is presented as an example. Additional work on a hierarchy of root causes is in progess.

The causes, which are the mechanism(s) directly responsible for the state of a component, fall into eight broad classes, as presented below. Each class has also been subdivided to provide a means of recording more detailed information on the cause(s) when such information is available.

- Other Component. The cause of the state of the component under consideration is the state of another component.

- Design, Manufacturing, and Construction Inadequacy. This category of causes encompasses actions and decisions during design or manufacturing or installation of components both before and after the plant is operational.

- Procedures Inadequacy (ambiguous, incomplete, or erroneous). This category refers to ambiguity, incompleteness, or error in procedures for operation and maintenance of equipment.

- Human Actions, Plant Staff Error. Represents causes related to errors of omission and commission on the part of plant staff, such as failure to follow a correct procedure.

- Maintenance and Test. The cause of component state is a scheduled or nonscheduled maintenance activity or a test and inspection.

Table A-1a

SOME GENERIC FAULT MODES - COMPONENT FAILS TO TRANSFER
FROM INITIAL STATE TO DESIRED STATE

Code	Fault Mode	Initial State	Desired State
FO	Fails To Open	Closed	Open
FC	Fails To Close	Open	Closed
FS	Fails To Start	Stopped	Operating
FT	Fails To Stop	Operating	Stopped

Table A-1b

SOME GENERIC FAULT MODES - COMPONENT TRANSFERS
FROM INITIAL STATE TO UNDESIRED STATE

Code	Fault Mode	Initial State	Undesired State
FR	Fails To Run	Operating	Stopped
TO	Transfers Open	Closed	Open
TC	Transfers Closed	Open	Closed
SS	Spuriously Starts	Stopped	Operating
ST	Spuriously Stops	Operating	Stopped
L	Leaking	Nonleaking	Leaking

- Abnormal Environmental Stress. This category includes all causes related to a harsh environment that is not within the component's specified design criteria.

- Internal. The component state is due to malfunctioning of something internal to the component as a result of normal wearout or other intrinsic failure. It includes the influence of the ambient environment of the component.

- Unknown. The cause of the component state cannot be identified.

Table A-2 provides a list of subcategories for the above cause categories along with the corresponding symbolic codes which will be used later in cause-effect logic diagrams. In the case for which the immediate cause of the state of a component is the state of another component, the cause codes are basically the component state codes (□). For noncomponent causes (root cause), the code is a circle (◯) with one or two letters representing the cause category or subcategory. The use of cause codes in the context of event classification will be explained later in this section. The following paragraphs provide additional guidelines for handling cases in which various cause categories may seem to overlap.

The key for distinction between "ambient environmental stress (IE)" and "abnormal environmental stress (E)" is the design limits for the normal operating environment and the expected variations of that environment. Any stress higher than such expected limits should be considered abnormal and should be classified as (E); otherwise, the stress should be classified as ambient. Examples are:

- Boron. Ambient stress for boron injection tank inlet/outlet valves.

- Salt-Induced Corrosion. Ambient stress for some service water system components at coastal sites.

- Extremely High or Low Room Temperatures. Abnormal stress for diesel generators.

- Water. Abnormal stress for compressed air system.

Any of the following environmental stresses could be considered ambient or abnormal depending on the component and the degree of stress compared to the design basis: vibration, moisture/humidity, boron, fatigue, sand/salt, or salt-induced corrosion.

The distinction between utilizing "unknown, (U)" and "wearout or other intrinsic failure, (IC)" is sometimes governed by the language of the report. As an example, if it is stated that a motor operator had loose screws, this could be attributed to (1) a human error due to insufficiently tightening the screws, (2) a severe environmental stress (e.g., vibration), (3) an ambient environmental stress (e.g., vibration), or (4) an intrinsic nature of the component to have its threads worn with time leading to loosening. Therefore, if it is not explicitly stated that an intrinsic condition caused the component state and a variety of causes could easily be hypothesized, the cause is designated as unknown, (U).

It is important to realize that most component states resulting from an ambient environmental condition are ultimately due to a human oversight; in particular,

Table A-2

CAUSE CODES

▭	State of a Component*
(D)	Design, Manufacturing, and Construction Inadequacy
(DR)	Plant Definition Requirements Inadequacy
(DE)	Design Error or Inadequacy
(DM)	Manufacturing Error or Inadequacy
(DC)	Construction Error or Inadequacy
(DX)	Other (explain)
(P)	Procedures Inadequacy (ambiguous, incomplete, or erroneous)
(PO)	Defective Operational Procedure
(PM)	Defective Maintenance Procedure
(PC)	Defective Calibration/Test Procedure
(PX)	Other (explain)
(H)	Human Actions, Plant Staff
(HP)	Failure To Follow Procedures
(HM)	Misdiagnosis (followed wrong procedure)
(HA)	Accidental Action
(HX)	Other (explain)
(M)	Maintenance
(MS)	Scheduled Preventive Maintenance (including surveillance tests and calibration)
(MF)	Forced Maintenance (repair of a known failure)

*Refer to Figure A-1 for component-caused symbols.

Table A-2 (continued)

- (E) Abnormal Environmental Stress
  - (EE) Electromagnetic Interference
  - (EM) Moisture (spray, flood, etc.)
  - (EF) Fire
  - (ET) Temperature (abnormally high or low)
  - (ER) Radioactive Radiation (irradiation)
  - (EC) Chemical Reactions
  - (EV) Vibration Loads
  - (EI) Impact Loads
  - (EH) Human-Caused External Event
  - (EN) Acts of Nature
- (I) Internal (internal to component, piece-part ambient environmental stress)
  - (IC) Internal to Component, Piece-Part
  - (IE) Ambient Environmental Stress
- (U) Unknown

in not applying or incorrectly applying defenses against the failure mechanisms. Examples are:

- Loose Screws Occurring due to Vibration. The use of a sealing compound, washers, or locking wire could prevent this.
- Moisture Shorting Motor Wires. A watertight design could prevent this.
- Boron Crystallization on Valve Stems. Proper maintenance and/or operating procedures could prevent this.
- Fatigue Failures and Salt-Induced Corrosion. Use of materials capable of withstanding the environment or operating conditions could prevent this.

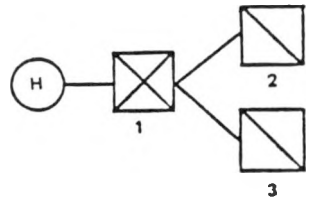
There are a few exceptions against which the ambient environment cannot really be defended, such as when breaker contacts become dirty due to the dust in the air. Short of continuously cleaning them (an impractical idea), the component can be made subject to routine preventive maintenance, which may or may not prevent dirt from interfering with contact operation.

In general, the ambient environmental designator (IE) is used when there is inadequate information provided to discern what root human cause allowed the ambient environment to impact the component, resulting in its state. This leaves some room for varied interpretations of these events, either as a human error or an internal failure.

Finally, the maintenance cause code for "repair of a known failure, (MF)," is used only when no information is provided regarding the cause of the component's failed state. Otherwise, the appropriate cause code from Table 2-2 is used.

A.3 CAUSE-EFFECT LOGIC DIAGRAM

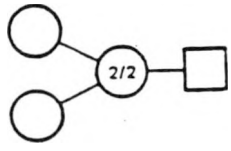
The symbols introduced earlier to represent the basic elements of an event (namely, causes and component states) can now be used to graphically represent event scenarios. This is achieved by showing the cause and effect relationship between various causes and component states involved in an event in a cause-effect logic diagram. The following is an example:



Translated into words, the above diagram means that a human error caused component 1 to fail, which in turn led to components 2 and 3 becoming functionally unavailable.

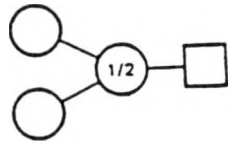
In general, the progression of an event is reconstructed from left to right and the cause-effect logic diagram always begins with one or more circles representing one or more root causes, and should always end with boxes representing the resulting component states. Links (i.e., solid lines connecting any two elements) represent the coupling mechanisms between those elements in such a way that the element to the left is the cause of the element to the right.

If a cause impacts several components, the situation is represented by multiple lines connecting the corresponding cause code with every resulting component state. On the other hand, there are situations where more than one cause can be identified as being involved in creating a given component state. For instance, there may be a case in which a given component state is the result of several causes acting together. Similarly, there are situations for which several causes can be identified based on the available information but a subgroup of those causes is sufficient to cause the event. In order to represent these situations, a logic operator is introduced that graphically shows what configuration of the identified causes has resulted in the state of the component being considered. This logic operator is called a "node" and is represented by a circle, which is placed between the cause and the effect symbols. An example is the following:



The cause node, 2/2 , with the inscribed 2/2 logic means that there are two causes and that both are required to cause the component state. This situation corresponds with the "AND" gate used in reliability logic diagrams.

As another example, consider the following:



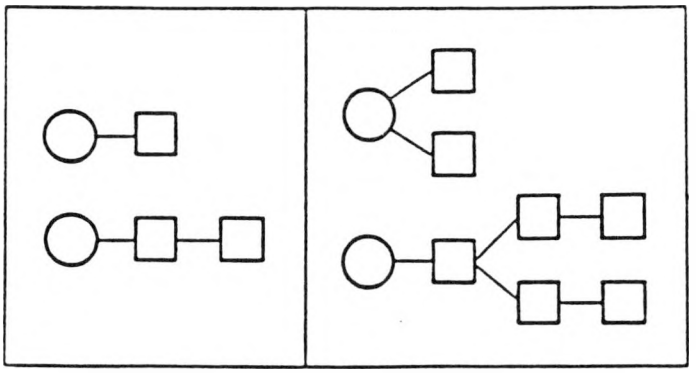
In this case, 1/2 indicates that two causes are present and either one of them is capable of causing the component state. This situation corresponds with the "OR" gate used in reliability logic diagrams.

A.4 EVENT CATEGORIES

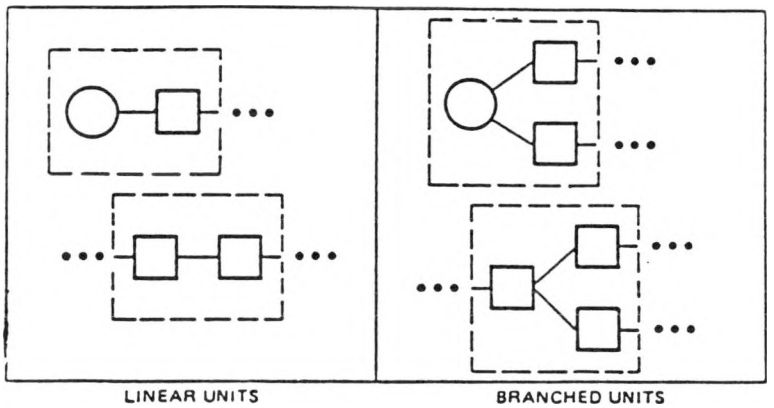
The event categories are based on the structure of the cause-effect logic diagram. Although the number of different cause-effect logic configurations that can be postulated is large, a reasonable number of event categories can be defined by keying on some general features of these logic configurations. Before discussing such event categories, it is helpful to define some general features of a cause-effect logic diagram useful to key on to establish event categories.

One feature of importance in event categorization is whether there is any branching in the structure of the cause-effect logic diagram. Branching occurs when two or more components states directly result from a cause, either a root cause or a component state that constitutes a cause. A branched event is any event with at least one such propagation of a cause to directly result in two or

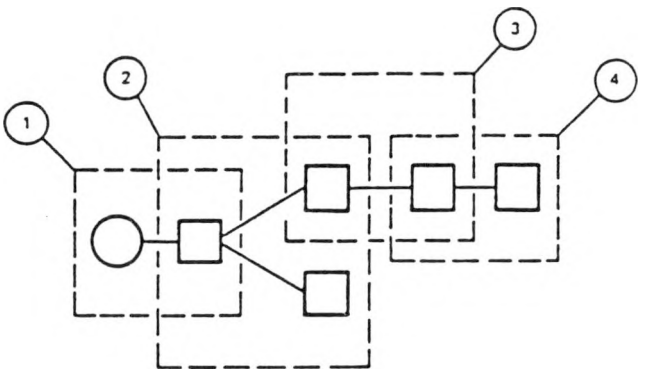
more component states. All other events are called linear events. The names of these categories reflect the structures of the corresponding cause-effect logic diagrams, as indicated in the examples illustrated below:



Another characteristic feature of the cause-effect logic diagram useful in event categorization is the event substructure known as the unit. A unit of a cause-effect logic diagram is any portion of the diagram consisting of a cause and all the component states that directly result from that cause. Just as events can be categorized as linear or branched, there are also linear and branched units, as indicated in the following.



As an example, consider an event having the following logic structure and consisting of the four indicated units.



The event is classified as a branched event because it includes a branched unit, Unit 2. This event also includes three linear units: Units 1, 3, and 4.

The above definitions provide a basis for describing the particular hierarchy used in this study to categorize the possible cause-effect logic configurations, which are illustrated in Figure A-2. Events are first categorized into linear events, which have only linear units, and branched events, which have at least one branched unit. The linear event category is further subdivided into single-unit (LS) and multiple-unit (LM) categories. Linear, multiple-unit events are sometimes described in the literature as "cascade events."

As indicated in Figure A-2, branched events are first broken down into separate categories based on whether there is a single-branched unit or multiple-branched units within the event logic structure. The single-branched unit category and the multiple-branched unit category can have, in addition to the branched units, any number of linear units. A final breakdown of the branched categories is afforded by distinguishing between two types of causes associated with the branched unit or units. There are root-caused (BSR) and component-caused (BSC) categories for single-branched units and component-caused (BMC) and mixed-caused (BMM) categories for multiple-branched unit events. It was not necessary to subdivide the linear categories in this manner because of the properties already built into the system. All single-unit linear events have a single root cause and a single component state. All multiple-unit linear events have one component state resulting from a root cause and all subsequent component states are component caused.

As a result of the above breakdown, six event categories are defined in terms of the general characteristics of the cause-effect logic diagrams. Although many additional categories can be defined (for example, by keying on the number of linear units combined with branched units), the set defined in Figure A-2 is the extent of breakdown provided in the statistical analysis of data in Section 3. No particular advantage to defining further categories could be identified.

The relationship between dependent events and the cause-effect logic structure categories defined above is depicted in Table A-3. As seen in this table, logic structure category, LS, corresponds and is synonymous with what have been described earlier as independent events. This is because events in category LS include and wholly contain all events having one and only one component state. All remaining logic structure categories (i.e., LM, BSR, BSC, BMC, and BMM) have at least two component states that are interdependent (i.e., "connected within the same cause-effect logic diagram") and are therefore dependent events.

Having defined dependent and independent events in terms of the six basic logic diagram event categories, it is convenient to identify the subset of these logic diagrams which represent the common cause failure events as defined in Section 2. The definition given there was that common cause events are that subset of the more general class of dependent events whose causes are not normally explicitly modeled as basic events in the system logic models. Component-caused events, whether they be linear or branched, should always be modeled explicitly in the system model if the model is to be an accurate representation of the system, but root-caused branched events may not be. Logic models are generally described down to the component state level but not the

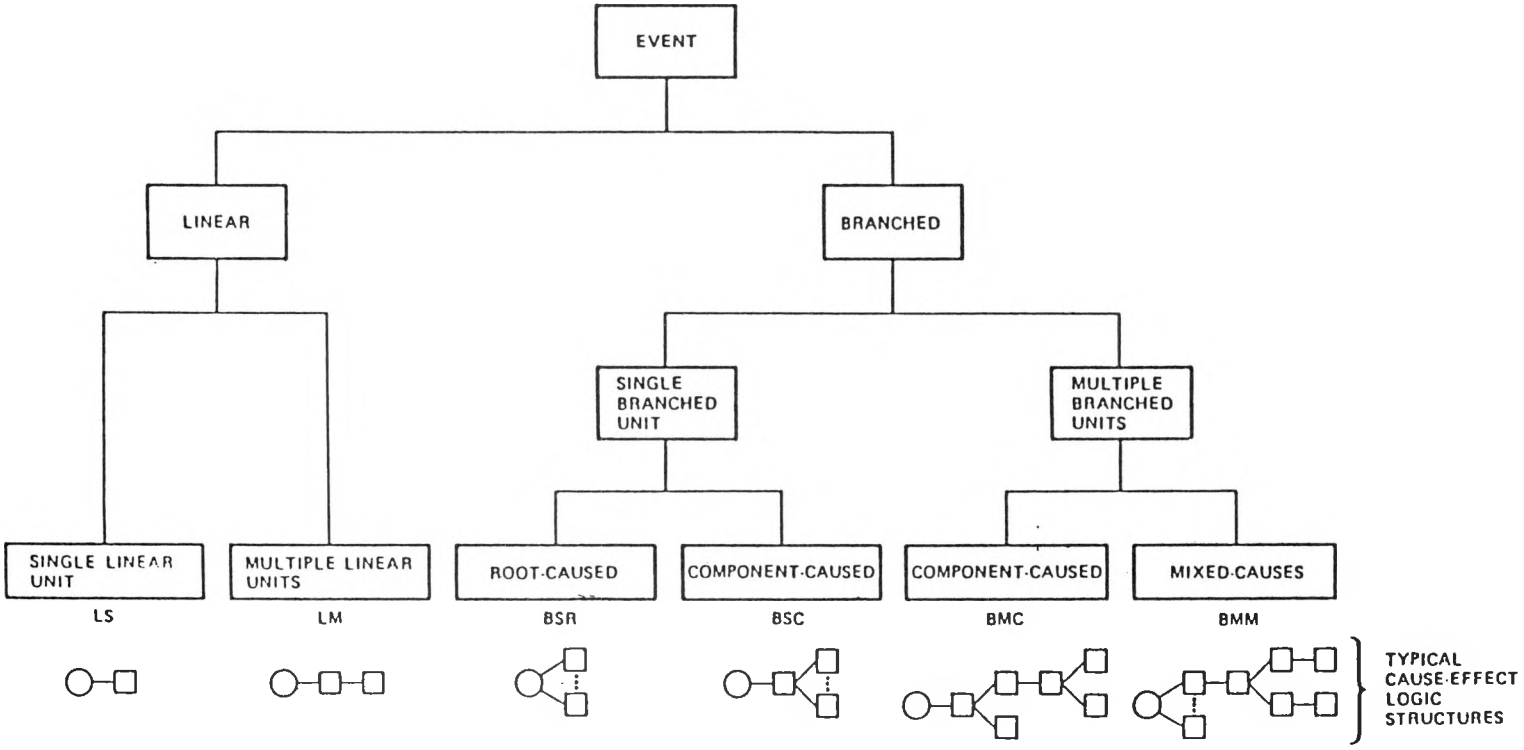
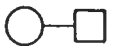
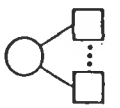
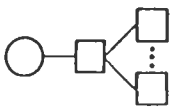
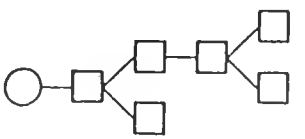
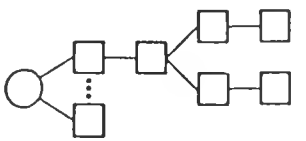


Figure A-2. Hierarchy of Event Categories

Table A-3

RELATIONSHIP BETWEEN DEPENDENT EVENTS AND LOGIC DIAGRAM EVENT CATEGORIES

Event Type	Characteristic	Event Classification System Categories				
		Name			Code	Typical Cause-Effect Logic
Independent	One Actual or Potential Component State	Linear	Single Unit		LS	
Dependent	Two or More Interdependent Actual or Potential Component States	Linear	Multiple Units		LM	
		Branched	Single Unit	Root-Caused	BSR	
				Component-Caused	BSC	
			Multiple Units	Component-Caused	BMC	
				Mixed Causes	BMM	

failure cause, except in the analysis of particular causes, such as fires and floods, where the causes of failure may also be dealt with explicitly. Thus, the common cause events that are to be used to obtain qualitative and quantitative information on common cause failures as defined in this report are to be found among the root-caused branched events only.

A.5 REFERENCES

A-1. Los Alamos Technical Associates, Inc., "A Study of Common-Cause Failures, Phase 2: A Comprehensive Classification System for Component Fault Analysis," EPRI NP-3837, June 1985.

A-2. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," Pickard, Lowe and Garrick, Inc., EPRI NP-3967, prepared for Electric Power Research Institute, June 1985.

APPENDIX B

THE GENERIC CAUSE APPROACH TO THE QUALITATIVE SCREENING

A detailed engineering analysis of CCFs must consider the root causes of component failures and the degree of dependence among component failures with regard to each root cause. A plant-specific CCF analysis should, in addition, evaluate the plant defense strategies designed to protect against equipment failures and human errors that lead to equipment unavailability. When a CCF analysis is performed on a nuclear power plant, it is not feasible, due to the complexity of the analysis problem, to analyze in detail every possible CCF scenario; i.e., every root cause event and the group of components that could all fail as a result of the occurrence of that event. However, there is an analysis method, the generic cause approach to common cause failure analysis, that allows the analyst to identify, through a series of six screening tasks, CCF scenarios that contribute most to system unavailability.

This method begins with the identification of a wide range of postulated causes of CCF events, events that each involve a particular group of components; e.g., a group of components that would all be affected by a common design error or a group of components that would all be susceptible to a fire in a certain location. The following tasks permit the analyst to separate potentially important cause/component group combinations from unimportant combinations based on qualitative arguments as early in the analysis as such judgments are possible. As the analysis progresses, more information is collected and the cause/component group combinations that survived the previous screening tasks are then analyzed in greater detail. The result of the screening is a list of CCF scenarios the analyst feels confident--due to the wide range of postulated causes of CCF events and the carefully selected screening arguments--represents the failures that contribute most to system unavailability.

Figure B-1 summarizes the six tasks involved in a system analysis using the generic cause approach. Specifically, the six screening tasks an analyst can use to identify the most important CCF scenarios of a plant are:

- Task 1. Identify important root causes of common failures and define the groups of components that are susceptible to each root cause of failure.

  Review the FMEA for the system of interest, the plant operating experience, the operating experience of similar plants, and previous CCF studies to identify important root causes of failures for the system being analyzed. All of the causes of failure underlying the reported events should be identified for the plant-specific CCF analysis. These failure causes usually fall into a few general categories, such as those defined by Edwards and Watson (Reference B-1).

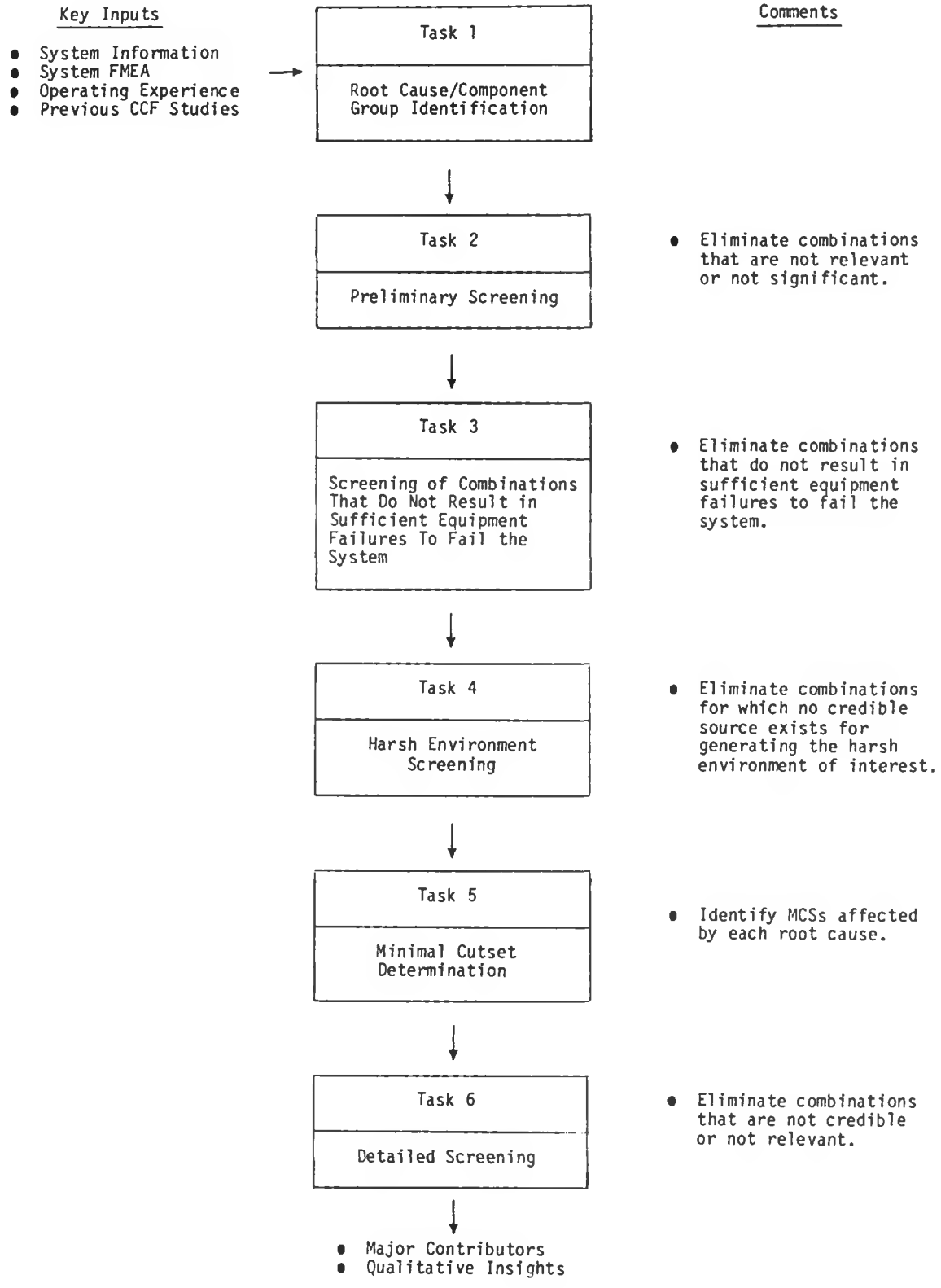


Figure B-1. Overview of the Generic Cause Approach

The identification of root causes of failure is based mostly, but not solely, on operational experience data. This raises the issue of completeness. The data may not reflect all the possible root causes of failure to which the system equipment could be vulnerable. In particular, low frequency events with potentially high consequences may not be reflected in the data. Furthermore, the quality of the data is an important consideration. Insufficient investigation and documentation of failure events make it difficult or impossible to determine some causes of failure.

The problems are particularly evident when the plant being analyzed is at the design stage. Nevertheless, the wealth of data from all sources, such as from failure reports or design studies, does allow a comprehensive, if not complete, list of root causes to be developed.

After important generic failure causes have been identified, determine groups of components that are susceptible to the causes of failure. There are at least three types of these root cause/component group combinations that must be identified for the CCF analysis: (1) root causes that primarily affect similar equipment, (2) root causes that affect equipment operated according to the same procedures, and (3) root causes that affect equipment in the same location.

- Type 1 - Root Causes that Affect Similar Equipment. Similar components are usually affected by the same installation, maintenance, and testing procedures and by common design and manufacturing processes. These commonalities allow for multiple failures due to systematically repeated human errors. Therefore, for these causes of CCFs, the component groups of interest are groups of similar components.

  To identify all similar equipment in the system, examine P&IDs, the FSAR, and other relevant system documentation and interview utility personnel. Each group of similar components will be considered a combination of potential interest.

- Type 2 - Root Causes that Affect Equipment Operated According to the Same Procedures. Components that are all affected by the same emergency or normal operating procedures should also be considered a component group of potential interest because these components could all fail due to a common operator error. Unlike the first type of component group just defined, the component groups defined by common emergency or normal operating procedures may involve dissimilar components.

  For the proper identification of the group of components operated according to the same procedures, first identify all plant emergency and normal operating procedures that affect each component in the system of interest. Then, identify those components that are all affected by a particular procedure and do this for every procedure being considered in

the analysis. Each group of components affected by a specific procedure will be considered a component group of potential interest.

Very often the analyst will find that these root causes are also more likely to affect similar equipment; thus, a portion of this type of root cause may be considered a subset of the first type--root causes that affect similar equipment. It is still convenient, however, to consider these procedure-related root causes as a separate type for analysis purposes.

The benefit of considering this type separately is that a detailed analysis of emergency and normal operating procedures permits a closer scrutiny of the utility's testing, maintenance, and operational activities. This in turn allows closer examination of the procedure-related root causes of failure.

- Type 3 - Root Causes that Affect Equipment in the Same Location. CCFs can also be attributable to harsh environments; i.e., adverse environmental conditions caused by fire, flood, moisture, etc. Most causes of harsh environments generate an adverse environment only within a limited area. The spread of the adverse conditions is mitigated or stopped by barriers, such as walls and fire doors, within the plant. Therefore, for environmental causes of CCFs, the component groups of interest are the components that are all susceptible to a specific harsh environment and in the same location with respect to the harsh environment; i.e., not separated from the source of the harsh environment by barriers.

  For the proper identification of the groups of components of interest for specific harsh environments, first locate the system components of interest identified in the PRA fault trees. [Exact locations are not necessary at this point in the analysis; it is only necessary to identify the room (or rooms) containing each component.] This part of this task can usually be accomplished without a plant visit. Then, identify barriers to each harsh environment. (This part of this task may require a plant visit since barriers to one environmental agent may not be barriers to another.) Safety analysis reports, since they describe fire barriers and flood zones within plants, can be used for a preliminary identification of barriers to some harsh environments; a more reliable identification can be accomplished through the plant visit to obtain detailed barrier descriptions for analyzing each environment of interest.

  Next, use component and barrier locations to develop domains (areas within a plant that are bounded by barriers to a particular harsh environment) for the harsh environments of interest. A group of components of interest for a specific

harsh environment will consist of the components that are susceptible to the harsh environment and in the domain of that harsh environment.

There are two categories of harsh environments: (1) harsh environments caused by energetic events (fires, floods, earthquakes, explosions, missiles, etc.) and (2) harsh environments caused by nonenergetic events or extremes of normal environmental conditions (contamination, vibration, moisture, corrosion, high temperature, etc.). An in-depth analysis of nonenergetic harsh environments has shown that these events almost invariably affect similar components (Reference B-2). This is due, in part, to the fact that most of these events are often caused by human errors in design, installation, and maintenance activities, etc. For example, most moisture-related CCF events involve a designer's failure to specify properly qualified equipment during the design stage or an operator's failure to properly seal the equipment following maintenance. Since an operational environment of high temperature and high relative humidity is common in several locations (e.g., pump rooms) of some plants, these design and maintenance errors frequently result in multiple component failures. These are human error-related failures that involve mostly similar equipment.

Although most nonenergetic harsh environments are caused by human errors, as just described, there are some instances when nonenergetic harsh environments can be caused by abnormal occurrences that affect equipment in the same location; e.g., equipment damage due to moisture and heat from a defective valve in close proximity to the equipment. Plant operational experience suggests that these nonenergetic events also result in the failure of similar equipment only. This observation is, however, based on sparse data. This lack of data indicates this type of event is less frequent than the other type of nonenergetic harsh environment, the type caused by human errors.

Analyzing CCFs caused by these two types of nonenergetic harsh environments as CCFs of similar equipment is more efficient than analyzing these failures of equipment in the same location. That is, the analysis of these events as failures that involve similar equipment will save the CCF analyst time because domains of susceptibility will not have to be established and analyzed for these nonenergetic events as is the case with the events caused by energetic harsh environments. Also, the CCF analyst will not have to search for all credible sources of nonenergetic harsh environments in a subsequent task of the analysis (Task 4). The search for credible sources of nonenergetic harsh environments and the analysis of their impacts on the system components (e.g., accounting for barriers to harsh environments) can be performed later in Task 6 when the MCSs have been determined and the analyst is dealing with a smaller number of potentially important component groups.

It is important to consider the susceptibility of the component piece-parts to the harsh environments of interest when analyzing component susceptibilities to those environments. Basic events in the system fault trees often represent the sum of the failures of the component piece-parts. For example, basic events representing pump and valve failures may also include cable faults, a circuit breaker failure, a circuit breaker control circuit failure, junction box faults, and other failures. Similar piece-parts belonging to dissimilar components could be susceptible to CCFs caused by harsh environments.

- Task 2. Screen the root cause and component group combinations initially defined for analysis and eliminate from the analysis those component groups that can be determined to be not relevant or not a significant contributor to system unavailability.

  The number of root cause and component group combinations postulated in Task 1 for the system of interest is necessarily large to ensure a comprehensive analysis. In this second task, some of these combinations can be eliminated from the analysis based on simple observations about the system and the nature of the root causes of failures. For example, suppose a CCF analysis was being conducted on a two-train emergency feedwater system with a common intake line from the condensate storage tank. In Task 1, three type A check valves (two valves in the system discharge lines and one valve in the common intake line) are identified as a group of similar components due to the fact that they are all identical valves maintained in the same way. In this second task, the CCF of the two type A check valves in the discharge lines of the pump would be considered relatively unimportant because the common intake line also contains a type A check valve, maintained in a similar way, whose single failure could cause system failure. Therefore, the CCF of the check valves in the discharge line can be screened as irrelevant to further analysis because any postulated cause of these valve failures could also be a cause of failure of the valve in the common intake line and this failure has already been considered a system failure in the system fault tree. (The CCF of the check valves in the discharge line would be relatively unimportant regardless of the failure probability of the check valves and the correlation among failures of type A check valves in redundant trains.) This type of screening is based on the logic of the system model.

  Other root cause and component group combinations for the system of interest could also be eliminated from the analysis at this time for other reasons, such as a very low probability of occurrence of the root cause event compared with the system failure probability from "normal" hardware and operator failures; e.g., an explosion in certain areas of the plant. This implies a screening on probability grounds. While it can be argued that this is quantitative screening, the implication here is that the

screening can be performed without a detailed probabilistic analysis, relying on the use of a relative assessment of probability instead.

- Task 3. Screen the root cause and component group combinations and eliminate from further analysis those combinations that do not result in sufficient equipment failures to fail the system.

  Several root cause and component group combinations do not result in sufficient equipment failures to fail the system (barring any additional failures). For example, consider a motor design deficiency that results in failure of two motor-driven pumps in an emergency feedwater system. This combination will not result (barring any additional failures) in EFW system unavailability if the system consists of two full capacity turbine-driven pumps in addition to the two motor-driven pumps. Similarly, a break in the steam supply line to one of the turbine-driven pumps has only a limited impact on system unavailability if the motor-driven pumps are in a different location from the steam supply line (and thus cannot fail due to the adverse high temperature environment generated from the line break).

  For some systems, the combinations that cannot by themselves cause system unavailability may not have to be analyzed in detail and can be screened in this task if it is clear, without having to perform a detailed quantitative assessment, that the additional failures necessary to cause system failure are sufficiently unlikely. Although this may be possible when analyzing a simple system, these combinations can be important in an accident sequence analysis because of their potential impact on other systems involved in the accident sequence. NUREG/CR-4837 (to be published soon) will describe the generic cause approach tailored to an accident sequence analysis. Screening as performed here does require an implicit assumption about relative probabilities of events and thus is not strictly qualitative. Quantitative screening as described in Section 3.2.2 may be of value here.

  In any case, the group of components that can by themselves cause system failure must be retained for further analysis. When no groups are identified that can cause system failure, the analyst should retain for further analysis other groups that, in combination with independent failures and/or other CCFs, can cause system failure.

  This task can be performed with the aid of a computer program designed to test system fault trees to see if the top event can occur as a result of the occurrence of a group of basic events.

  A number of computer programs [e.g., COMCAN III (Reference B-3), SETS (Reference B-4), and WAMCOM (Reference B-5)] can be used to test the system fault trees in this step. These programs will "turn on" the appropriate basic events to see if the top event can occur as a result of the occurrence of the group of basic events.

- Task 4. Screen each harsh environment-related combination to determine if there is a root cause event that can trigger the scenario.

  This task is only applicable to harsh environment-related root causes. Each harsh environment-related combination represents a harsh environment (e.g., high temperature) and a domain; e.g., the area within the plant that is bounded by barriers to the harsh environment. In addition, since each combination has survived the screening in Task 3, it is now known that the occurrence of the harsh environment within that domain can disable the system of interest; e.g., it is known that the system fails if a high temperature condition in that domain causes all susceptible system equipment to fail. Thus, a search for credible sources of the harsh environments of interest is warranted.

  This task requires a substantial amount of plant-specific information. A visit to the plant to accomplish this task is recommended. Use the information obtained from this visit and information from plant documents to identify possible sources of harsh environments for each domain associated with the scenarios identified in Task 3. For each harsh environment considered, determine if there are credible sources for generating the harsh environment identified for the respective domain. If there are no sources for the harsh environment/domain of interest, then eliminate the scenario from further analysis at this point. Involve specialists in the analysis of some causes of harsh environments (e.g., fires) to verify the adequacy of barriers to the harsh environment and to help determine if there are credible sources for generating the harsh environment identified for the respective domain.

- Task 5. Determine the component minimal cutsets that are involved in each root cause and component group combination retained for analysis.

  Each combination that survived the previous screening tasks represents a root cause of failure and the group of affected components. In addition, it is known that the occurrence of the root cause can disable all affected components and contribute significantly to system failure; e.g., high temperature in a certain domain can cause sufficient system equipment failures to result in loss of the high pressure injection system. In this task, determine the minimal cutsets associated with each combination; e.g., high temperature causes HPIS failure by failing the lube oil system in all HPIS pumps, or by failing all HPIS pump motors, and so on.

  The input required for this task are the system fault trees and the list of potential root cause and component group combinations that passed the previous screening tasks.

Several computer programs, such as COMCAN III (Reference B-3), SETS (Reference B-4), and WAMCOM (Reference B-5), are available for determining MCSs for CCF scenarios.

- Task 6. Screen the scenarios that have been retained for analysis and eliminate scenarios that are not credible or not relevant by considering details of the relationships between the root causes of failure and the component failures in the MCSs.

  This task identifies unimportant scenarios retained from Task 5 and eliminates them from further consideration by considering details of the relationships between the root causes of failure and the component failures in the MCSs. This screening task is effective for eliminating installation, maintenance, testing, and operator error scenarios and scenarios caused by harsh environments.

  The input required for performing this task are the lists of root causes of failures and MCSs identified in step 5; copies of the plant procedures that have an effect on these scenarios; information on testing, maintenance, and scheduling activities; and, for harsh environment scenarios, additional information from a plant visit.

  The following is a description of some criteria that can be used to screen scenarios involving errors in the installation, maintenance, testing, or operation of components and scenarios involving harsh environments. These criteria are only examples of how engineering insights can be applied to the screening of scenarios. For any given case, there may be other powerful screening criteria. In all analyses, the screening criteria must be carefully applied to ensure no important scenarios are eliminated from the analysis.

  In the screening of installation, maintenance, testing, and operating error scenarios, determine if there are any plausible errors in performing the task that could result in component unavailability. If there are none, the scenario may be discarded. For example, if a procedure does not call for removing a component from service, there is little chance that the component will be left in a disabled state at the end of the task.

  Look at the plant testing and maintenance schedules to determine if a specific testing or maintenance-related scenario is credible. For example, consider an MCS involving three pumps. A common preventive maintenance task is to be performed at 1-month intervals on each of the three pumps. The plant maintenance schedule calls for this maintenance to be staggered among the three pumps; that is, pump 2 is to be serviced 1 month after pump 1, and pump 3 is to be serviced 2 months after pump 1. A functional test of the pumps is also to be performed monthly, and it too is to be staggered among the three pumps. Each pump is to be tested 1 month after its preventive maintenance. Therefore, an error that occurs during the maintenance of pump 1 will probably

be discovered and corrected before the same error can fail pump 3 and possibly even pump 2. Thus, the MCS will likely never occur due to errors in this maintenance task, and the scenario may be eliminated from the analysis. In general, it is only necessary to consider MCSs whose basic events are all affected by the same procedure within one testing interval.

Also, screen out scenarios in which different personnel perform a task on multiple components in an MCS. The systematic repetition of task-related errors is highly dependent on the interpretation of the working procedure and on the effects of stress, fatigue, and personnel abilities. These factors can vary considerably among individuals.

Finally, for analyzing scenarios involving harsh environments, a plant visit is required for making a detailed survey to determine the spatial relationships of components, sources of harsh environments, and barriers to the harsh environments of interest. The plant visit may determine some scenarios incredible in light of these details.

For example, in Task 1, an analyst may discover several penetrations with unsealed conduits connecting equipment in different locations. Moisture in one location (e.g., at an upper floor) could propagate through the conduits and cause the components connected to these conduits in the other locations (e.g., at a lower floor) to fail. Since operating experience indicates several component failures due to moisture propagating through conduits, the analyst postulates in Task 1 that moisture could cause CCFs of components in these locations. In Task 6, the MCSs for this scenario are all known. A detailed analysis of the locations may reveal that the unsealed conduits do not connect equipment in the same MCS to a common source of moisture. Thus, the scenario can be screened out. Note that the analysis of locations in this task is more detailed than in previous tasks because the MCSs are now known, and the analyst can investigate the specific equipment of interest. In addition, the number of scenarios to be investigated in detail has been reduced to a smaller, more manageable number.

The result of performing the six screening tasks just described is a list of the CCF scenarios the analyst feels confident represents the failures that contribute most to system unavailability and plant risk. These CCF scenarios have been identified through a detailed engineering analysis and, therefore, are valuable intermediate results of a CCF analysis. In addition, they are valuable input to a quantitative analysis of CCF contributions to system unavailability and plant risk.

REFERENCES

B-1. Edwards, G. T., and I. A. Watson, "A Study of Common Mode Failures," SRD-R-146, United Kingdom Atomic Energy Authority, Safety and Reliability Directorate, July 1979.

B-2. Paula, H. M., and D. J. Campbell, "Analysis of Dependent Failure Events and Failure Events Caused by Harsh Environmental Conditions," JBFA-LR-111-85, JBF Associates, Inc., August 1985.

B-3. Rasmuson, D. M., et al., "Use of COMCAN III in System Design and Reliability Analysis," EG&G Idaho, Inc., EGG-2187, October 1982.

B-4. Stack, D. W., "A SETS Users Manual for Accident Sequence Analysis," NUREG/CR-3547, prepared for U.S. Nuclear Regulatory Commission by Sandia National Laboratories, January 1984.

B-5. Putney, B., "WAMCOM, Common-Cause Methodologies Using Large Fault Trees," Electric Power Research Institute, EPRI NP-1851, May 1981.

APPENDIX C

PARAMETRIC MODELS AND THEIR ESTIMATES

C.1 INTRODUCTION

This appendix provides a more detailed description of the various parametric models presented in Section 3 of Volume I, 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 E discusses the representation of the statistical uncertainty in the values of these estimates. The models presented in the following are described by showing how each model is used to calculate the probability of occurrence of the various "basic events." It is therefore helpful to review the definition of common cause basic events and other key concepts prior to the discussion of the models.

Definition of Common Cause Basic Events

In the context of the procedures of this report and as described in Section 3.3.1, Volume I, 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 3.3.1, 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}, 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 components 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

$$A_I = \sum_i A_I^{(i)} + \sum_j A_{C1}^{(j)} \qquad (C.1)$$

where $A_I^{(j)}$ is a truly independent failure of component A as a result of cause i, and $A_{C1}^{(j)}$ 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 a coupling mechanism.

Similarly, define

$$C_{AB} = \sum_i C_{AB\,(C2)}^{(i)} \tag{C.2}$$

where $C_{AB(C2)}^{(i)}$ is a failure of components A and B from the occurrence of a common cause, which resulted in the two failures only.

If the events C_{AB}, A_I, etc., are regarded as being independent, the following cutset expansions result:

$$A_I \cdot B_I = \sum_i A_I^{(i)} \cdot \sum_j B_I^{(j)} + \sum_i A_I^{(i)} \cdot \sum_j B_{C1}^{(j)} + \sum_i A_{C1}^{(i)} \cdot \sum_j B_I^{(j)} + \sum_i A_{C1}^{(i)} \cdot \sum_j B_{C1}^{(j)} \tag{C.3}$$

$$C_{AB} \cdot C_{BC} = \sum_i C_{AB(C2)}^{(i)} \cdot \sum_j C_{BC(C2)}^{(j)} \tag{C.4}$$

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

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

$$A_{C1}^{(k)} \cdot B_{C1}^{(k)}$$

$$C_{AB(C2)}^{(k)} \cdot C_{BC(C2)}^{(k)}$$

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 result from a common cause, cutsets such as $A_{C1}^{(k)} \cdot B_{C1}^{(k)}$ would be indistinguishable from $C_{AB(C2)}^{(k)}$, and should be classified as the latter. Similarly, $C_{AB(C2)}^{(k)} \cdot C_{BC(C2)}^{(k)}$ would be indistinguishable from $C_{ABC(C3)}^{(k)}$. Thus, when the common cause failures are introduced at the impact level, the basic events can now no longer be regarded as truly independent, and this may cause logical inconsistencies with the system model.

A convenient approach to properly model common cause failures events is to define the events A_I, C_{AB}, C_{AC}, and C_{ABC} to be mutually exclusive, since they partition the failure 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 the 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 component. 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 $A_{CI}^{(j)}$ in Equation (C.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.

Symmetry Assumption

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. For example, if A, B, and C are identical components, then

$$P(A_I) = P(B_I) = P(C_I) = Q_1$$

$$P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2$$

$$P(C_{ABC}) = Q_3 \qquad \text{(C.5)}$$

Note that, with the symmetry assumption, the probability of failure of any given 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.* Therefore, the general representation of the probabilities of basic events is the following

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

and, in general,

$$Q_k^{(m)} \neq Q_k^{(\ell)} \qquad \ell \neq m \qquad \text{(C.7)}$$

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

*See glossary in front of this volume for the definition of common cause component group.

C.2 PARAMETRIC MODELS

The objective of all the parametric models described in this report is to develop the probability of the basic events based on a set of parameters. Numerous parametric models have been proposed over the past decade, and some have been widely used in risk and reliability analyses. The models presented in this appendix and also in Section 3, Volume I, cover a wide range of such models. The main characteristics of these models are summarized in Table C-1.

Table C-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

The "shock models" recognize 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 system 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 mechanisms. 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 of multiple component failure rates or probabilities to total failure rates or probabilities from one source of data, and, independently a total failure rate or probability from another source. For example, plant-specific data may 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 (Reference C-1) may be used to estimate ratios of multiple to simple component failure events. It should be noted that parameter estimators for all these models estimators for the parameters are dependent on the assumptions made about success data.

Basic Parameter Model

The basic parameter model (Reference C-2) refers to the straightforward definition of the probabilities of the basic events as given by Equation (C.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 (C.6), the total failure probability, Q_t, of a component in a common cause group of m components is

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)} \qquad (C.8)$$

Table C-1

KEY CHARACTERISTICS OF THE PARAMETRIC MODELS

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

*REFER TO THE TEXT FOR DEFINITION OF VARIOUS PARAMETERS
**FORMULAS ARE PRESENTED FOR THE BASIC EVENTS IN A COMMON CAUSE COMPONENT GROUP OF SIZE m

where the binomial term

$$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(m-k)!\ (k-1)!} \tag{C.9}$$

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 (C.8) is still valid under the rare event approximation.

Beta Factor Model

The beta factor model (Reference C-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 applied risk and reliability analysis. This model assumes that a constant fraction (β) of the component failure rate 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 are assumed to fail. Therefore, for a group of m components, all Q_k's defined in Equation (C.6) are zero except Q_1 and Q_m. The last two quantities are written as (dropping the superscript m)

$$Q_1 = (1-\beta)\ Q_t$$

$$Q_m = \beta\ Q_t \tag{C.10}$$

This implies that

$$\beta = \frac{Q_m}{Q_1 + Q_m} \tag{C.11}$$

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

$$Q_t = Q_1 + Q_m \tag{C.12}$$

which is the special case of Equation (C.8) when $Q_2 = Q_3 = \cdots = Q_{m-1} = 0$.

Therefore, using the beta factor model, the frequencies of various basic events in a common cause group of m components are

$$Q_k = \begin{cases} (1-\beta)\ Q_t & k=1 \\ 0 & 2 \leq k < m \\ \beta Q_t & k=m \end{cases} \tag{C.13}$$

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 (Reference C-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 (Reference C-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 (Reference C-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 probabilty, 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 more 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:

$$Q_t = Q_1^{(3)} + 2\,Q_2^{(3)} + Q_3^{(3)} \tag{C.14}$$

$$\beta^{(3)} = \frac{2Q_2^{(3)} + Q_3^{(3)}}{Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)}}$$

$$\gamma^{(3)} = \frac{Q_3^{(3)}}{2Q_2^{(3)} + Q_3^{(3)}} \tag{C.15}$$

δ and higher order terms are identically zero.

For a group of four similar components, the MGL parameters are:

$$Q_t = Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)} \tag{C.16}$$

$$\beta^{(4)} = \frac{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}{Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}$$

$$\gamma^{(4)} = \frac{3Q_3^{(4)} + Q_4^{(4)}}{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}$$

$$\delta^{(4)} = \frac{Q_4^{(4)}}{3Q_3^{(4)} + Q_4^{(4)}} \tag{C.17}$$

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 multiparameter 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.

$$Q_1 = (1-\beta)\, Q_t$$

$$Q_2 = \frac{1}{2}\, \beta\, (1-\gamma)\, Q_t$$

$$Q_3 = \gamma\, \beta\, Q_t \qquad \text{(C.18)}$$

For a four-component group, the equations are:

$$Q_1 = (1-\beta)\, Q_t$$

$$Q_2 = \frac{1}{3}\, \beta\, (1-\gamma)\, Q_t$$

$$Q_3 = \frac{1}{3}\, \beta\gamma\, (1-\delta)\, Q_t$$

$$Q_4 = \beta\gamma\delta\, Q_t \qquad \text{(C.19)}$$

The generalization of this is given by

$$Q_k = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^{k} \rho_i \left(1-\rho_{k+1}\right) Q_t \qquad (k=1, \ldots, m) \qquad \text{(C.20)}$$

where

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

Alpha-Factor Model

As explained in Appendix E, 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 (Reference C-7). A rigorous approach to estimating beta factors is presented in Reference C-8 by introducing an intermediate event-based parameter, which is much easier to estimate from observed data. Reference C-9 uses the multiparameter generalizations of event-based parameters directly to estimate the common cause basic event probabilities. This multiparameter common cause model is called the alpha factor model.

Alpha factor parameters are estimated from system failure data. The MGL parameters are estimated from component failures. This difference and its implications are described more fully in Appendix E.

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 are defined as

$$\alpha_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}} \qquad (C.21)$$

where $\binom{k}{m} Q_k^{(m)}$ 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,

$\alpha_k^{(m)}$ = ratio of the probability of failure events involving any k components over the total probability of all failure events in a group of m components.

For example, for a group of three similar components we have

$$\alpha_1^{(3)} = \frac{3Q_1^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_2^{(3)} = \frac{3Q_2^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_3^{(3)} = \frac{Q_3^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}} \qquad (C.22)$$

and $\alpha_1^{(3)} + \alpha_2^{(3)} + \alpha_3^{(3)} = 1$ as expected.

Using Equations (C.21) and (C.8), we can see that the basic event probabilities can be written as a function of Q_t and the alpha factors as follows:

$$Q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_t} Q_t \qquad (C.23)$$

where

$$\alpha_t \equiv \sum_{k=1}^{m} k\,\alpha_k^{(m)} \tag{C.24}$$

To see how Equation (C.23) is obtainted from Equations (C.8) and (C.21), note that Equation (C.21) can also be written as

$$\frac{k}{m}\left\{\sum_{k=1}^{m}\binom{m}{k} Q_k^{(m)}\right\}\alpha_k^{(m)} = \binom{m-1}{k-1} Q_k^{(m)}$$

By summing both sides over k we get

$$\frac{1}{m}\left\{\sum_{k=1}^{m}\binom{m}{k} Q_k^{(m)}\right\}\sum_{k=1}^{m} k\,\alpha_k^{(m)} = \sum_{k=1}^{m}\binom{m-1}{k-1} Q_k^{(m)}$$

or

$$\sum_{k=1}^{m}\binom{m}{k} Q_k^{(m)} = \frac{m}{\alpha_t} Q_t$$

where we have used Equations (C.8) and (C.24). By using the above equation in Equation (C.21) and solving for $Q_k^{(m)}$ we get Equation (C.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

$$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$$

$$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3} \tag{C.25}$$

Similarly, the alpha factor model parameters for the same group are written as

$$\alpha_1 = 3(1-\beta)$$

$$\alpha_2 = \frac{3}{2}\beta(1-\gamma)$$

$$\alpha_3 = \beta\gamma \tag{C.26}$$

Binomial Failure Rate Model

The BFR model (Reference C-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. The name of this model arises from the fact that, for a group of components, the distribution of the number of failed components resulting from each nonlethal shock occurrence follows a binomial distribution. The BFR model is, therefore, more restrictive because of these assumptions than all other multiparameter models presented here. When originally presented and applied, the model only included this nonlethal shock. Because of its structure, the model tended to underestimate the probabilities of failure of higher order groups of components in a highly redundant system; therefore, the concept of lethal shock was included. This version of the model is the one recommended.

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

$Q_I \equiv$ independent failure frequency for each component.

$\mu \equiv$ frequency of occurrence of nonlethal shocks.

$p \equiv$ conditional probability of failure of each component, given a nonlethal shock.

$\omega \equiv$ frequency of occurrence of lethal shocks.

Thus, the frequency of basic events involving k specific components is given as

$$Q_k = \begin{cases} Q_I + \mu p(1-p)^{m-1} & k=1 \\ \mu(p)^k\,(1-p)^{m-k} & 2 \leq k < m \\ \mu p^m + \omega & k=m \end{cases} \qquad (C.27)$$

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.

C.3 ESTIMATORS FOR MODEL PARAMETERS

C.3.1 Incompleteness in Data, Modeling Assumptions, and Parameter Estimates

In order to estimate a parameter value, it is necessary to find an expression that relates to measurable quantitites that can be obtained from data. This expression is called an estimator. Before deriving a general set of estimators for the models discussed in Section C.2, it is important to recognize the relationship between adopting specific modeling assumptions and the derivation of parameter estimates. Two types of modeling assumptions will be discussed; the first is that associated with the choice of a reliability model for basic events. The second is associated with a response to the incompleteness in the data, with respect to success data.

In the approach to system modeling, certain basic events have been defined. Consider those basic events, either of independent failures or multiple (dependent) failures that represent the failure to start of a standby component. Two models are commonly used for such events (Reference C-11). The first assumes a constant failure probability on demand. In N demands, the probabilities of i failures, (i = 0, 1, ..., N), are binomially distributed and a maximum likelihood estimator of the probability of failure, given n failures were observed in N demands, is n/N. The second model assumes a constant failure rate, λ_S, while in standby. If it is assumed that the component is replaced when failed, a maximum likelihood estimator of λ_S is given by n/T where n is the number of failures observed in a total time T on standby. (Note this failure rate should not be confused with the failure rate of a standby component to run once it has started.) In this model, if it is assumed that the time between tests is T_T, then the probability of failure on a randomly occurring real demand is $\lambda_S T_T/2$, assuming $\lambda_S T$ is small, since on average the demand would occur halfway between tests.

Note that the time between tests does not however enter the expression for the estimator of λ_S. Therefore, the estimator is the same whatever the value of T_T. The reason can be seen in Figure C-1, which represents the pointwise probability of a basic event with two values of the time between tests, T_T and $T_T/2$. At the end of each test interval, the probability that a failure occurred in that interval is $\lambda_S T_T$ and $\lambda_S T_T/2$, respectively. The expected number of failures, n, in a total time T therefore is $\lambda_S T_T \times T/T_T$ and $\lambda_S T_T/2 \times 2T/T_T$, respectively. Since the failure rate is assumed constant, then in the rare event approximation the number of failures is directly proportional to the total time of observation. The expected numbers of failures are equal since, while in the second case, the probability of a failure having occurred before the test is halved, there are twice as many opportunities to reveal a failure. This is clear since, in this model, the test does not cause failures, but merely reveals if they have occurred. However, the unavailability on a real demand is given by $\lambda_S T_T/2$ and $\lambda_S T_T/4$, respectively, showing, in this model of failures, the advantage of reducing the time between tests. The significance of the distinction between the two basic event models, the failure on demand and the failure rate models, in the context of common cause modeling and the role of testing strategies will be further discussed below.

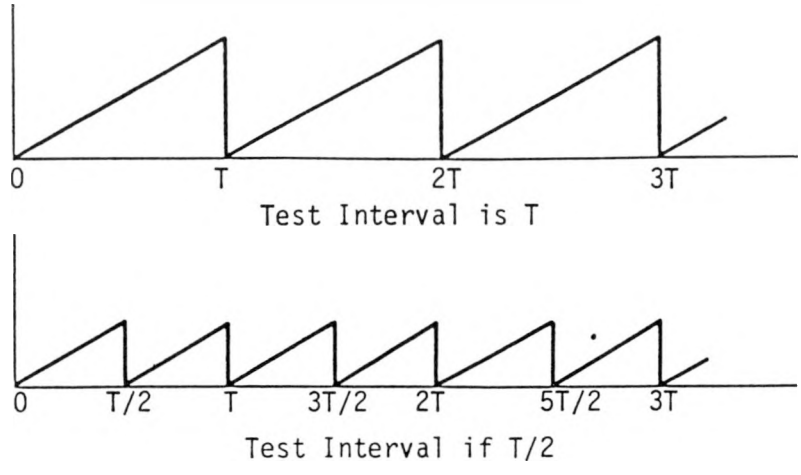


Figure C-1. Pointwise Unavailability as a Function of Time for Two Different Test Intervals

Having identified two models for common cause basic events, consider the estimation of the basic event probabilities in these two models. First, consider the probability of failure on demand model. The maximum likelihood estimators are of the form n_k/N_k, where n_k is the number of occurrences of the event, "k components fail," and N_k is the number of demands on k components, or the number of opportunities that the cause that resulted in k components failing had a chance of being revealed. For the beta factor, defined as in Equation (C.11), it is clear that to derive an estimator it is necessary to have at least a measure of the ratio of N_m to N_1. This can be seen to be true of the other models, such as the MGL and alpha factor models, where the ratios N_k to N_i are also needed. The importance of this observation can be seen by considering the data.

Suppose the data for the common cause failure estimation has been established by the procedure discussed in Section 3, an interpretation and reinterpretation of event data for plant-specific conditions. This data base consists of numbers of events with 1, 2, up to m failures. But it does not provide the success data; i.e., how many times was it possible for such failures to be revealed? This information is generally not recorded in compilations of event data. Nevertheless, there are good rules of thumb for estimating the numbers of demands on the component population, based on technical specifications related to surveillance testing. If it is assumed that the majority of demands are from surveillance tests, which is usually the case for the major standby component, such as pumps, valves, and diesel generators, then it is relatively straightforward to estimate the number of demands on single components, especially if the technical specifications specify that, for instance, each pump must be tested once a month. Of course, there are other demands on components from interfacing maintenance, real demands, etc., which must be accounted for. In common cause analysis however this evaluation may be circumvented to some extent, by fixing the number of demands to provide a single failure probability, which agrees with an estimate from another source, such as plant-specific data, as discussed in Section 3 of Volume 1.

Technical specifications do not, however, specify how to perform tests. Consequently, the exact number and method of component test in each test episode may not be known. Also, since success data are not normally recorded and reported in the generic sources of data, the particular way components are tested in each plant in the generic population is usually unknown to the data analyst although the plant procedures may be quite clear. We will now show how the assumption the data analyst has to make regarding testing schemes affect the estimators.

As an example, consider two testing strategies; nonstaggered testing where all trains are tested simultaneously, in each test episode, and staggered testing where different trains are tested at different test episodes. We will derive estimators for a beta factor for a two-train system assuming both testing strategies.

Estimate 1: Nonstaggered Testing

In this case, if the number of single component demands is N_1, the number of failures of one component n_1, and of 2, n_2, then the single component failure probability is

$$Q_1 = n_1/N_1 \qquad (C.28)$$

There are clearly N_2 = N 1/2 demands on the group of two components, which is the number of test episodes. Thus

$$Q_2 = n_2/N_2$$

$$= 2n_2/N_1 \qquad (C.29)$$

and

$$\beta = 2n_2/(n_1 + 2n_2) \qquad (C.30)$$

which is the result found in, for instance, NUREG/CR-2300 (Reference C-11).

Estimate 2: Staggered Testing

Suppose in this testing strategy it is known that there are, in a certain period, a number, N_D, of testing episodes. A testing episode is defined as follows. At each episode, one component is tested. If it succeeds, no more is done until the next scheduled testing episode that may be a week, 2 weeks or a month later. If however the component tested fails, the other is tested immediately. If the second fails, a multiple failure is revealed. If it does not fail, the failure is confirmed as a single component failure. In this strategy, therefore, the number of tests against the multiple failure is precisely N_D, the number of testing episodes. However, the number of tests performed on individual components, N_1, is slightly higher and given by

$$N_1 = N_D + n_1 + n_2 \qquad (C.31)$$

where n_1 is the number of independent component failures, and n_2 the number of multiple failure events. The additional $n_1 + n_2$ demands arise from the necessity to test the second component, given the first has failed. Without testing the second, it is not known how to partition the observed failures of the first component between n_1 and n_2. Thus, there are $n_1 + n_2$ failures of the first component leading to $n_1 + n_2$ extra tests on the second.

Therefore, in this regime

$$Q_1 = \frac{n_1}{N_D + n_1 + n_2} \qquad (C.32)$$

and

$$Q_2 = \frac{n_2}{N_D} \qquad (C.33)$$

The beta factor is approximately (since $N_D >> n_1 + n_2$)

$$\beta \simeq \frac{n_2}{n_1 + n_2} \qquad (C.34)$$

Note that when these two different, reasonable assumptions regarding the unknown testing strategies at the plants that form the basis for the common cause data base are made, the two estimates of the common cause failure probability differ

by a factor of approximately 2. This shows that making assumptions regarding the testing strategies adopted directly affects the estimates. Such assumptions are usually necessary because of incompleteness of the success data in the data base.

Now consider the standby failure rate model. We will again investigate the difference between the estimates of common cause failure probability and beta factors for different testing strategies. It was shown earlier that the test interval did not affect the estimator of the standby failure rate. Again, consider the two-train system. If the number of failures are n_1 and n_2 as before, the standby failure rate for event Q_1 is

$$\lambda_s^{(1)} = \frac{n_1}{2T} \tag{C.35}$$

where T is the calendar time on standby; that is, each component has been on standby for T.

For event Q_2, the time that both components have been on standby as a group is T, thus

$$\lambda_s^{(2)} = \frac{n_2}{T} \tag{C.36}$$

This is independent of the assumption of staggered versus nonstaggered testing at the plants in the data base, since, as discussed previously, increased testing against the common cause (as would be obtained by staggered testing) lowers the probability of failure by common cause per demand, but increases the number of opportunities to observe failure by the same fraction in a compensating way. However, the testing scheme at the plant being analyzed is of interest as seen below. The time between tests of each component is T_T.

Estimate 1: Nonstaggered Testing (at the plant being analyzed)

$$Q_1 = \lambda_s^{(1)} T_T/2 \qquad \text{or} \qquad n_1 T_T/4T \tag{C.37}$$

and

$$Q_2 = \lambda_s^{(2)} T_T/2 \qquad \text{or} \qquad n_2 T_T/2T \tag{C.38}$$

and

$$\beta = 2n_2/(n_1 + 2n_2) \tag{C.39}$$

as before in Equation (C.30).

Estimate 2: Staggered Testing (at the plant being analyzed)

$$Q_1 = \lambda_s^{(1)} T_T/2 \qquad \text{or} \qquad n_1 T_T/4T \tag{C.40}$$

but now

$$Q_2 = \lambda_s^{(2)} T_T/4 \qquad \text{or} \qquad n_2 T_T/4T \tag{C.41}$$

since the effective time between tests for a common cause failure is halved, as the successful test of the first component indicates the common cause failure has not occurred.

In this case

$$\beta \simeq \frac{n_2}{n_1 + n_2} \tag{C.42}$$

as in Equation (C.34).

It should be noticed that while both the standby failure rate and demand models above produce similar estimation of the beta factor for the cases of staggered and nonstaggered testing, respectively, the differences between the two testing regimes arise in different ways in the two models. In the probability on demand model, the testing assumption has to be made for the plants in the data base. In the failure rate model, no such assumption has to be made. However, the apparent advantage of not having to make this assumption in this case is bought at the expense of assuming the standby failure rate model applies.

In summary, adopting the probability of failure on demand model introduces into the estimation process the need to resolve an uncertainty with respect to how the data was collected at the group of plants that constitute the data base. Adopting the standy failure rate model introduces no such uncertainty; the impact of the testing scheme is at the level of the plant being analyzed. Thus, when performing a common cause analysis, it is important to be clear what assumptions are being made and what effects these assumptions have.

C.3.2 Some Estimators for Parameters of the Common Cause Models

There are several possible estimators that can be used even if no modeling uncertainties, as discussed before, exist. 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 statistical uncertainty distributions for the various parameters in Appendix E.

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_1. A consistent set of estimators, based on alternative strategies, has not yet been evaluated, but some discussion is given in Section C.4.

Estimators for Basic Parameters

The maximum likelihood estimator for Q_k is given as

$$\hat{Q}_k = \frac{n_k}{N_k} \tag{C.43}$$

where

$n_k \equiv$ number of events involving k components in a failed state

and

$N_k \equiv$ 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

$$N_k = \binom{m}{k} N_D \tag{C.44}$$

The binomial terms $\binom{m}{k}$ represents the number of groups of k components that can be formed from m components. We, therefore, have

$$\hat{Q}_k = \frac{n_k}{\binom{m}{k} N_D} \tag{C.45}$$

Thus, Equation (C.45) 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 (C.45). 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 (C.8) with the corresponding estimator yields the following estimator for the total failure frequency for a specific component

$$\hat{Q}_t = \frac{1}{m\ N_D} \sum_{k=1}^{m} k\ n_k \tag{C.46}$$

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).

$$\beta = \frac{1}{Q_t} \sum_{k=2}^{m} \frac{(m-1)!}{(m-k)!(k-1)!} Q_k \tag{C.47}$$

Using the estimator of Q_k, given by Equation (C.45), and Q_t, given by Equation (C.48), in the above equation results in the following estimator for β.

$$\hat{\beta} = \frac{\sum_{k=2}^{m} k n_k}{\sum_{k=1}^{m} k n_k} \tag{C.48}$$

For a two-unit system (m=2), the above estimator reduces to the familiar estimator of the β-factor,

$$\hat{\beta} = \frac{2n_2}{n_1 + 2n_2} \tag{C.49}$$

Note that the estimator for 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 (C.47). (See Appendix E.)

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,

$$\beta = \frac{1}{Q_t} \sum_{k=2}^{m} \frac{(m-1)!}{(m-k)!\ (k-1)} Q_k \tag{C.50}$$

$$\gamma = \frac{1}{\beta Q_t} \sum_{k=3}^{m} \frac{(m-1)!}{(m-k)!\ (k-1)} Q_k \tag{C.51}$$

$$\delta = \frac{1}{\beta\gamma Q_t} \sum_{k=4}^{m} \frac{(m-1)!}{(m-k)!\ (k-1)!} Q_k \tag{C.52}$$

Therefore, by using Equations (C.45) and (C.46) in the above, we obtain the following estimators.

$$\hat{\beta} = \frac{\sum_{k=2}^{m} k n_k}{\sum_{k=1}^{m} k n_k} \tag{C.53}$$

$$\hat{\gamma} = \frac{\sum_{k=3}^{m} k n_k}{\sum_{k=2}^{m} k n_k} \tag{C.54}$$

$$\hat{\delta} = \frac{\sum_{k=4}^{m} k n_k}{\sum_{k=3}^{m} k n_k} \tag{C.55}$$

For instance, for a three-unit system (m=3), we have

$$\hat{\beta} = \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} \tag{C.56}$$

Similarly,

$$\hat{\gamma} = \frac{3n_3}{2n_2 + 3n_3} \tag{C.57}$$

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 (C.54), 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 the estimates of the α-factor model, which are in terms of the ratio of events rather than component states. This is seen in the following.

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,

$$\hat{\alpha}_k = \frac{n_k}{\sum_{k=1}^{m} n_k} \tag{C.58}$$

It is shown in Appendix E 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 p. To develop estimators for these parameters, several other quantities are defined as

$\lambda_t \equiv$ rate of nonlethal shocks that cause at least one component failure.

$$n_t \equiv \sum_{k=1}^{m} n_k \tag{C.59}$$

where, as before, n_k is the number of basic events involving k components.

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 p, as presented in Appendix E, are

$$\hat{Q}_I = \frac{n_I}{mN_D} \tag{C.60}$$

$$\hat{\lambda}_t = \frac{n_t}{N_D} \tag{C.61}$$

$$\hat{\omega} = \frac{n_L}{N_D} \tag{C.62}$$

and $\hat{p}$ is the solution of the following equation:-

$$\hat{s} = \hat{p} \frac{m\, n_t}{1 - (1-p)^m} \tag{C.63}$$

where

$$\hat{s} = \sum_{k=1}^{m} k\, n_k \tag{C.64}$$

Based on the above estimators, an estimator for μ can be obtained from the following equation:

$$\lambda_t = \mu[1-(1-p)^m] \tag{C.65}$$

which is based on the definition of λ_t as the rate of nonlethal shocks that cause at least one component failure. Therefore,

$$\hat{\mu} = \frac{\hat{\lambda}_t}{1 - (1-\hat{p})^m} \tag{C.66}$$

Table 3-6, Volume I, summarizes the point estimators for the various model parameters.

C.4 THE EFFECT OF TESTING SCHEMES ON ESTIMATORS

As explained before, estimators presented here (and in Table 3-6, Volume I) assume that periodic tests or actual demands on systems challenge all components of the system. This assumption is explicit in some models (e.g., basic parameter) and implicit in others; e.g., MGL and alpha factor.

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:

$$N_k = \binom{m}{k} N_D \tag{C.67}$$

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:

$$N_D = N_{TS}$$

As shown earlier for the case of a two component group, the assumption of a staggered testing scheme results in different values of N_k. The value depends on the response to the failure observed. Suppose, for the sake of argument as was assumed previously, that, given a 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 episodes N_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 nonstaggered testing case. In fact, for the same technical specification 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 nonstaggered 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*. 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

$$N_k = \left(N_D' - \sum_{j=1}^{m} n_j\right)\binom{m-1}{k-1} + \left(\sum_{j=1}^{m} n_j\right)\binom{m-1}{k-1}$$

$$= N_D'\binom{m-1}{k-1} = mN_{TS}\binom{m-1}{k-1} \qquad (C.68)$$

The number of single component demands is given by

$$N_D' + \sum_{j=1}^{m} nj \cdot (m-1) \qquad (C.69)$$

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 nonstaggered testing scheme, using Equation (C.67),

$$Q_k^{NS} = \frac{n_k}{\binom{m}{k} N_{TS}} \qquad (C.70)$$

For staggered testing scheme, using Equation (C.68),

$$Q_k^{S} = \frac{n_k}{m\binom{m-1}{k-1} N_{TS}} \qquad (C.71)$$

Therefore $Q_k^S \leq Q_k^{NS}$ because

$$\frac{Q_k^S}{Q_k^{NS}} = \frac{1}{k} \qquad (C.72)$$

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

$$\beta = \frac{Q_2}{Q_1 + Q_2} \qquad (C.73)$$

*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 $Q_1 \cdot Q_k$ at each testing episode, this term would be $\binom{m}{k}$. However, since the n_j are collectively usually much smaller than N_D', this subtle distinction will make little difference.

Therefore

$$\beta^S = \frac{Q_2^S}{Q_1^S + Q_2^S} \tag{C.74}$$

and

$$\beta^{NS} = \frac{Q_2^{NS}}{Q_1^{NS} + Q_2^{NS}} \tag{C.75}$$

thus

$$\beta^{NS} = \frac{2Q_2^S}{Q_1^S + 2Q_2^S} \cong 2\,\frac{Q_2^S}{Q_1^S + Q_2^S} = 2\,\beta^S \tag{C.76}$$

where we assumed, as it is true in most cases, that $Q_2 << Q_1$.

The staggered-based estimator is approximately a factor of 2 smaller.

The estimator presented by Equation (C.74) is similar in form to the estimator of a single parameter model called the C-factor model (Reference C-4). In this respect, the C-factor is another estimator of the β-factor under the assumptions leading to Equation (C.74). 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 aspects 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).

C.5 REFERENCES

C-1. Nuclear Power Experience, S. M. Stoller Corporation, updated monthly.

C-2. Fleming, K. N., and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," Pickard, Lowe and Garrick, Inc., EPRI NP-3967, prepared for Electric Power Research Institute, June 1985.

C-3. Fleming, K. N., "A Reliability Model for Common Mode Failure in Redundant Safety Sytems," Proceedings of the Sixth Annual Pittsburgh Conference on

Modeling and Simulation, General Atomic Report GA-A13284, April 23-25, 1975.

C-4. Parry, G. W., "Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty," 1984 Annual Meeting of the Society for Risk Analysis.

C-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.

C-6. Poucet, A., A. Amendola, and P. C. Cacciabue, "Summary of the Common Cause Failure Reliability Benchmark Exercise," Joint Research Center Report, EUR-11054 EN, Ispra, Italy, 1987.

C-7. Mosleh, A., "Hidden Sources of Uncertainty: Judgment in Collection and Analysis of Data," Nuclear Engineering and Design, August 1985.

C-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.

C-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.

C-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.

C-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 D

ACCOUNTING FOR COMMON CAUSE GROUP SIZE DIFFERENCES IN COMMON CAUSE PARAMETER ESTIMATION; i.e., HOW TO MAP IMPACT VECTORS

D.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 data bases associated with groups having different numbers of components; i.e., different levels of redundancy. These relationships are intended to help combine the data bases 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 data bases of systems* 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.

D.2 DEFINITION OF BASIC EVENTS

As an example, consider a system* (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

*In this context, system can be thought of as meaning "common cause component group."

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 in Reference D-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 D-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 D-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

Table D-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	$Q_1^{(4)**}$	A	A	A
	B		B	B	None
	C		C	None	None
	D		None	None	None
Common Cause Impacting Two Components	AB	$Q_2^{(4)**}$	AB	AB	A
	AC		AC	A	A
	AD		A	A	A
	BC		BC	B	None
	BD		B	B	None
	CD		C	None	None

*Impact expressed in terms of the specific set of components failed by each basic event.
**Applies to each basic event within the braces.

Table D-1 (continued)

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)*
Common Cause Impacting Three Components	ABC	$Q_3^{(4)}$**	ABC	AB	A
	ABD		AB	AB	A
	ACD		AC	A	A
	BCD		BC	B	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.

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 failure 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 D-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 D-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.

These probabilities are the parameters of the basic parameter model that, for the four-train system, include:

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:

$$M_j^{(4)} = \binom{4}{j} Q_j^{(4)} N \qquad (D.1)$$

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 (D.1) for the parameters in a four-train model yields

$$M_1^{(4)} = 4Q_1^{(4)}N; \quad M_2^{(4)} = 6Q_2^{(4)}N; \quad M_3^{(4)} = 4Q_3^{(4)}N; \quad M_4^{(4)} = Q_4^{(4)}N \qquad (D.2)$$

The total data base generated by N demands on the four-train system is given by

$$\text{Event Data Vector} = \left\{M_1^{(4)}, M_2^{(4)}, M_3^{(4)}, M_4^{(4)}\right\} \qquad (D.3)$$

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

$$q_j^{(4)} = \frac{M_j^{(4)}}{N}, \quad j = 1, 2, 3, 4 \qquad (D.4)$$

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 data base that is normalized against the number of system demands.

Returning to Table D-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 D-1, the following relationships are easily established:

$$q_0^{(3)} = Q_1^{(4)} = \frac{1}{4} q_1^{(4)}$$

$$q_1^{(3)} = 3Q_1^{(4)} + 3Q_2^{(4)} = \frac{3}{4} q_1^{(4)} + \frac{1}{2} q_2^{(4)}$$

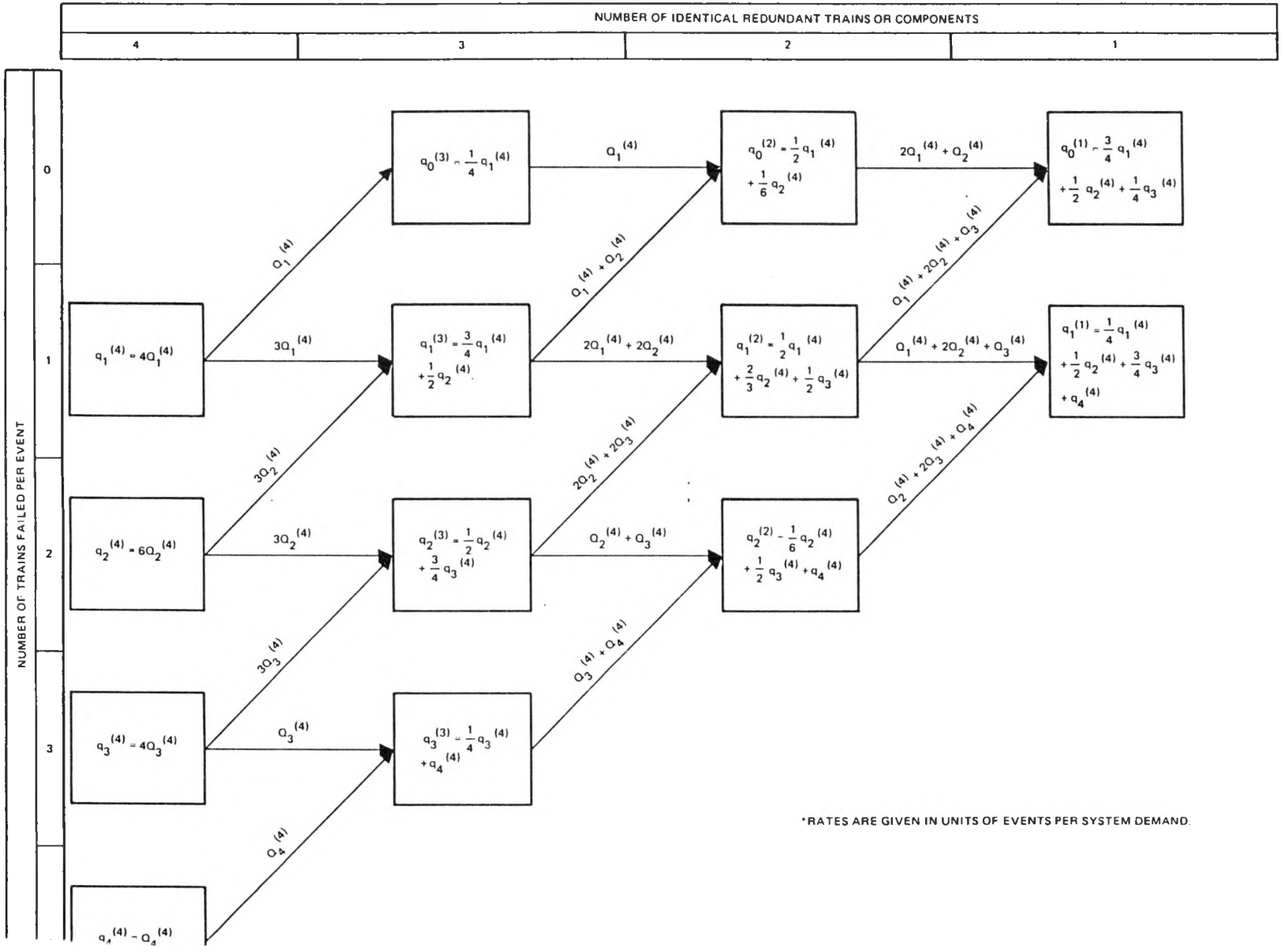
$$q_2^{(3)} = 3Q_2^{(4)} + 3Q_3^{(4)} = \frac{1}{2} q_2^{(4)} + \frac{3}{4} q_3^{(4)}$$

$$q_3^{(3)} = Q_3^{(4)} + Q_4^{(4)} = \frac{1}{4} q_3^{(4)} + q_4^{(4)} \qquad (D.5)$$

These and the remaining relationships among the data bases are summarized in Table D-2. Each column of Table D-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.

Table D-2

AVERAGE RATE OF OCCURRENCE* OF BASIC EVENTS IN SYSTEMS AS A FUNCTION OF SYSTEM SIZE AND THE NUMBER OF TRAINS FAILED PER EVENT



*RATES ARE GIVEN IN UNITS OF EVENTS PER SYSTEM DEMAND.

D.3 MAPPING DOWN IMPACT VECTORS

The relationships in Table D-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 data bases indicated in Table D-2. The key property is that, when moving from left to right to simulate downward mapping of 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 D-2

$$\text{Prob}\{1^{(4)} \rightarrow 1^{(3)}\} = \frac{3Q_1^{(4)}}{4Q_1^{(4)}} = .75 \qquad (D.6)$$

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 formulas for mapping down data from systems having four, three, or two components to any identical system having fewer components is presented in Table D-3. The application of these formulas to binary impact vectors (i.e., impact vectors whose entries are either zero or one) is illustrated in Table D-4 for mapping down data from four or three-train systems. This provides the basis for the formulas presented in Section 3 for downward mapping of impact vectors. Note that, because these formulas depend on Equation D.2, they are dependent on the assumption made about the sampling scheme that produced the data. (See Appendix C for a fuller discussion.)

The probability of impact of zero components is carried through these tables (D-2, D-3, and D-4) for bookkeeping purposes--to show how the event impact probability is conserved. Also, the accounting of the P_0 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 data base, a picture of what the data base 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 D-4, which covers the case of mapping single component failure events in four-train systems to systems having fewer components. Carrying through the P_0 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 data base 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 single component failures for use in parameter

Table D-3

FORMULAS FOR MAPPING DOWN EVENT IMPACT VECTORS

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

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

Table D-4

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

MAPPING OF EVENT 1

SYSTEM	IMPACT VECTOR* P_0	P_1	P_2	P_3	P_4
ORIGINAL FOUR-TRAIN SYSTEM	0	0	0	0	1.00
IDENTICAL THREE-TRAIN SYSTEM	0	0	0	1.00	—**
IDENTICAL TWO-TRAIN SYSTEM	0	0	1.00	—	—
IDENTICAL ONE-TRAIN SYSTEM	0	1.00	—	—	—

MAPPING OF EVENT 2

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

MAPPING OF EVENT 3

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

MAPPING OF EVENT 4

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

MAPPING OF EVENT 5

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

MAPPING OF EVENT 6

SYSTEM	IMPACT VECTOR P_0	P_1	P_2	P_3
ORIGINAL THREE-TRAIN SYSTEM	0	0	0	1.00
IDENTICAL TWO-TRAIN SYSTEM	0	0	1.00	—
IDENTICAL ONE-TRAIN SYSTEM	0	1.00	—	—

MAPPING OF EVENT 7

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

MAPPING OF EVENT 8

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

MAPPING OF EVENT 9

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

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

**(—) MEANS THE IMPACT CATEGORY IS INAPPLICABLE

estimation. However, if 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 D-4) as 40(.5) + 30(.67) + 20 = 60 occurrences of single component failure events. The sensitivity of this factor in an example systems analysis is explored in Section 4.1 of Volume I. The numerical importance of system size mapping in the estimation of common cause parameters was first explained by Peter Doerre of KWU, Federal Republic of Germany, as part of a contribution to the CCF Reliability Benchmark Exercise (References D-2 and D-3).

D.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 formulas are based are accepted. Mapping up, however, is a different story. To understand this point, let us return to Table D-2. Suppose an $n_i^{(3)}$ 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 D-2, the following statements can be made about the probability that this event would result in one or two component failures, respectively.

$$P\left\{1^{(3)} \rightarrow 1^{(4)}\right\} = \frac{3Q_1^{(4)}}{3Q_1^{(4)} + 3Q_2^{(4)}} \tag{D.7}$$

$$P\left\{1^{(3)} \rightarrow 2^{(4)}\right\} = \frac{3Q_2^{(4)}}{3Q_1^{(4)} + Q_2^{(4)}} \tag{D.8}$$

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, the underlying basic event probabilities. This is a transcendental problem because we need to assign the impact vectors in order to determine what the underlying basic event probabilities are!

There are some aspects of the downward mapping relationships presented in Tables D-2, D-3, and D-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 analyst to understand the nature of the cause. Independent failures (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.

D.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 data base of applicable events would look like if it all was generated by systems of the same size (i.e., the number of components in each common cause group) as the system being analyzed. In the case of independent events, the number of such events observed in the data base 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, $\underline{M}_I^{(j)}$, 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.

$$M_I^{(j)} = \frac{j}{k} M_I^{(k)} \tag{D.9}$$

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.

$$M_I^{(\ell)} = \sum_{k=1} \frac{\ell M_I^{(k)}}{k} \tag{D.10}$$

For the purpose of mapping impact vectors of each independent event, Equation (D.9) translates into

$$P_I^{(\ell)} = \frac{\ell P_I^{(k)}}{k} \tag{D.11}$$

Because this approach adds events that were not actually observed, it artificially strengthens the data base 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.

D.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 on the system is constant and independent of system size. This is a reasonable assumption. From it follows the following simple relationship.

$$P_\ell^{(\ell)} = P_j^{(j)}, \quad \text{for all } \ell \text{ and } j \tag{D.12}$$

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 components in an ℓ component system without modification.

D.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 components 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, that each component fails. The quantity 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,

$$n_0^{(2)} = \mu (1-\rho)^2$$

$$n_1^{(2)} = 2\mu (1-\rho) \rho$$

$$n_2^{(2)} = \mu\rho^2 \qquad \text{(D.13)}$$

   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 is to be applied. For mapping up from a system size i=2 to a system size j=4 for example, these equations are

$$n_0^{(4)} = \mu (1-\rho)^4$$

$$n_1^{(4)} = 4\mu (1-\rho)^3 \rho$$

$$n_2^{(4)} = 6\mu (1-\rho)^2 \rho^2$$

$$n_3^{(4)} = 4\mu\ (1-\rho)\ \rho^3$$

$$n_4^{(4)} = \mu\rho^4 \qquad \text{(D.14)}$$

These equations postulate (if the μ and ρ are used from step 1) that we would have observed the values of $n_1^{(4)}$, $n_2^{(4)}$, $n_3^{(4)}$, and $n_4^{(4)}$ from the same BFR process that generated the values of $n_1^{(2)}$ and $n_2^{(2)}$ 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,

$$n_1^{(4)} = 4\mu\ (1-\rho)^3\ \rho\ = [2\mu\ (1-\rho)\ \rho]\quad 2\ (1-\rho)^2$$

$$= 2\ (1-\rho)^2\ n_1^{(2)} \qquad \text{(D.15)}$$

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 D-1. Table D-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,

$$n_3^{(4)} = 4\mu\ (1-\rho)\ \rho^3 = 2\mu\ (1-\rho)\ \rho^3 + 2\mu\ (1-\rho)\ \rho^3$$

$$= \rho^2\ [2\mu\ (1-\rho)\ \rho] + 2\ (1-\rho)\ \rho\quad \mu\rho^2$$

$$= \rho^2\ n_1^{(2)} + 2\ (1-\rho)\ \rho\ n_2^{(2)} \qquad \text{(D.16)}$$

Table D-5 includes formulas 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 formulas in Table D-5 take care of all the bookkeeping problems of enumerating the possibilities and factoring in the system size effects.

While it is the analyst's responsibility to assess, document, and defend his assessment of the parameter 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 ($\rho < .5$).

Table D-5

FORMULAS FOR UPWARD MAPPING OF EVENTS CLASSIFIED AS NONLETHAL SHOCKS

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

- If a nonlethal shock fails a number of components intermediate to the number present, it is unreasonable to expect that ρ is either very small ($\rho \to 0$) or very large ($\rho \to 1$).

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

A final observation to be aware of is that, based on the example problem presented in Section 4.1, the final results of a common cause analysis are much more sensitive to uncertainties in the classification of lethal shocks than nonlethal shocks.

D.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 D-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 data base, as well as for the system being analyzed, and the use of the appropriate mapping formulas derived in this appendix. Examples of impact vector mapping are presented in Tables D-4 and D-6 for downward and upward mapping, respectively. It should be stressed that the particular formulas 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.

D.6 REFERENCES

D-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.

D-2. Poucet, A., A. Amendola, and P. C. Cacciabue, "Summary of the Common Cause Failure Reliability Benchmark Exercise," Joint Research Center Report, PER 1133/86, Ispra, Italy, April 1986.

D-3. Doerre, P., "Possible Pitfalls in the Process of CCF Event Data Evaluation," Proceedings of PSA 87 International Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30-September 4, 1987.

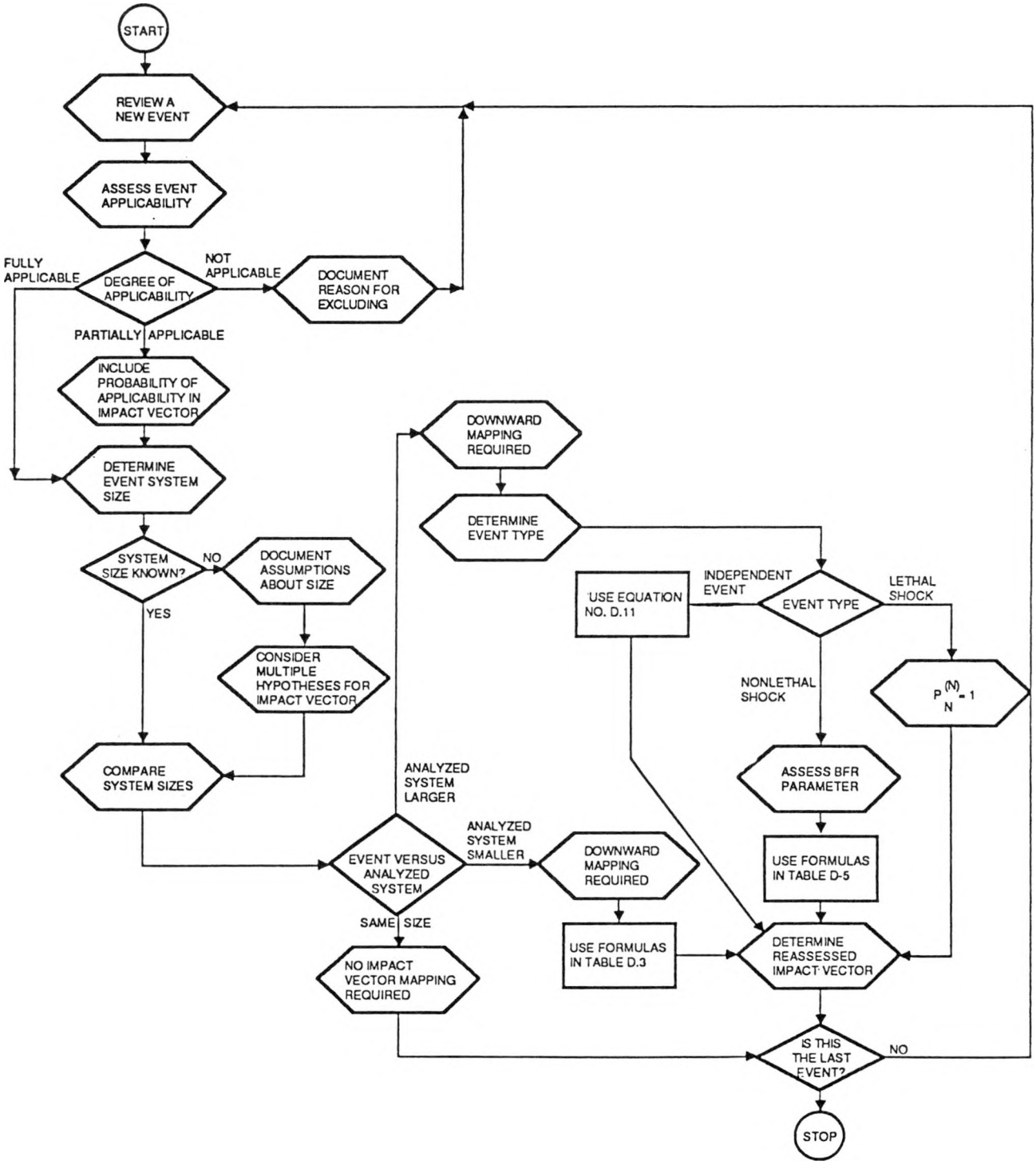


Figure D-1. Decision Tree for Assessing and Mapping Event Impact Vectors

Table D-6

EXAMPLES 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 ($\rho = .10$)				
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 - TWO TRAIN	.5	.5	—	—
	IDENTICAL - THREE TRAIN	.675	.5	.05	—
	IDENTICAL - FOUR TRAIN	.81	.5175	.095	.005
7	ORIGINAL - THREE TRAIN	.25	.5	.25	—
	IDENTICAL - FOUR TRAIN	.3	.475	.275	.025

EVENT NO.	SYSTEM-SIZE	IMPACT VECTOR P_1	P_2	P_3	P_4
	LETHAL SHOCK CASE				
8	ORIGINAL - ONE TRAIN	1	—	—	—
	IDENTICAL - TWO TRAIN	0	1	—	—
	IDENTICAL - THREE TRAIN	0	0	1	—
	IDENTICAL - FOUR TRAIN	0	0	0	1
	NONLETHAL SHOCK CASES ($\rho = .9$)				
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 ($\rho = .5$)				
10	ORIGINAL - ONE TRAIN	1	—	—	—
	IDENTICAL - TWO TRAIN	1	.5	—	—
	IDENTICAL - THREE TRAIN	.75	.75	.25	—
	IDENTICAL - FOUR TRAIN	.5	.75	.5	.125
11	ORIGINAL - TWO TRAIN	0	1	—	—
	IDENTICAL - THREE TRAIN	0	.5	.5	—
	IDENTICAL - FOUR TRAIN	0	.25	.5	.25
12	ORIGINAL - TWO TRAIN	.5	.5	—	—
	IDENTICAL - THREE TRAIN	.375	.50	.25	—
	IDENTICAL - FOUR TRAIN	.25	.4375	.375	.125
13	ORIGINAL - THREE TRAIN	.25	.5	.25	—
	IDENTICAL - FOUR TRAIN	.1667	.375	.375	.125

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

**(—) MEANS THE IMPACT CATEGORY IS INAPPLICABLE

APPENDIX E

STATISTICAL UNCERTAINTY DISTRIBUTION FOR MODEL PARAMETERS

E.1 INTRODUCTION

This appendix describes 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 this appendix 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 3, Volume I; e.g., 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 here for the analysis of uncertainty is the Bayesian approach, in which the distribution of a parameter, Θ, in light of evidence E, is obtained from

$$\pi(\Theta|E) = \frac{L(E|\Theta)\pi_0(\Theta)}{\int L(E|\Theta)\pi_0(\Theta)d\Theta} \qquad (E.1)$$

where

$\pi(\Theta|E) \equiv$ posterior distribution of Θ given evidence E.

$\pi_0(\Theta) \equiv$ distribution of Θ prior to the evidence.

$L(E|\Theta) \equiv$ 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, 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 distributions.

E.2 DISTRIBUTION OF THE BASIC PARAMETER MODEL

The demand based parameters of the basic parameter model are defined as:

$Q_k \equiv$ 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

$$E = \{n_k, k=1,\ldots,m \quad ; N_D\} \tag{E.2}$$

where n_k is the number of failures of events involving failure of k components in a common cause group of size m, and N_D is the number of system demands.

Assuming nonstaggered testing (see discussion in Appendix C), the number of times a group of k components is challenged in each test of a system of m components can be calculated from

$$N_k = \binom{m}{k} N_D \tag{E.3}$$

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

$$\pi(Q_k|n_k, N_k) = \frac{1}{C} L(n_k|Q_k, N_k)\, \pi_o(Q_k) \tag{E.4}$$

where

$$C \equiv \int_0^1 L(n_k|Q_k, N_k)\, \pi_o(Q_k)\, dQ_k$$

The binomial distribution

$$L(n_k|Q_k, N_k) = \binom{N_k}{n_k} Q_k^{n_k} (1-Q_k)^{N_k-n_k} \tag{E.5}$$

for the likelihood and its conjugate distribution, beta

$$\pi_o(Q_k) = \frac{\Gamma(A_k + B_k)}{\Gamma(A_k)\,\Gamma(B_k)} Q_k^{A_k-1} (1 - Q_k)^{B_k-1} \tag{E.6}$$

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

$$\Gamma(x) = \int_0^\infty z^{x-1} e^{-z}\, dz \tag{E.7}$$

The parameters of the posterior distribution that will also be a member of the beta family of distributions are

$$A_k' = A_k + n_k$$

$$B_k' = B_k + N_k - n_k \qquad \text{(E.8)}$$

The mean of the posterior distribution is given by

$$\overline{Q}_k = \frac{A_k'}{A_k' + B_k'} \qquad \text{(E.9)}$$

Therefore

$$\overline{Q}_k = \frac{n_k + A_k}{N_k + B_k + A_k} \qquad k=1,\ldots,m \qquad \text{(E.10)}$$

For a uniform prior with $A_k = B_k = 1$, we get

$$\overline{Q}_k = \frac{n_k + 1}{N_k + 2} \qquad \text{(E.11)}$$

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

$$Q_k = \frac{A_k' - 1}{A_k' + B_k' - 2} \qquad \text{(E.12)}$$

which, in terms of the prior distribution parameters and the data, is written as

$$Q_k = \frac{n_k + A_k - 1}{N_k + A_k + B_k - 2} \qquad \text{(E.13)}$$

For a uniform prior ($A_k = B_k = 1$), the above estimator reduces to a form commonly known as the maximum likelihood estimator (MLE):

$$Q_k = \frac{n_k}{N_k} \qquad \text{(E.14)}$$

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.

E.3 DISTRIBUTION OF THE ALPHA-FACTOR MODEL PARAMETERS

The parameters of the alpha-factor model are defined as:

α_k = fraction of basic events involving failure of any k components due to common cause.

The data needed to estimate α_k's are of the following form:

$$E = \{ n_k; \quad k=1,\ldots,m \} \tag{E.15}$$

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

$$L(n_1,n_2,\ldots,n_m|\alpha_1,\alpha_2,\ldots,\alpha_m) = \frac{\Gamma(n_1+n_2+\ldots+n_m)}{\Gamma(n_1).....\Gamma(n_m)} \prod_{k=1}^{m} \alpha_k^{n_k} \tag{E.16}$$

where

$$\sum_{k=1}^{m} \alpha_k = 1 \tag{E.17}$$

This is a multinomial distribution.

Using a Dirichlet prior distribution of the form

$$\pi_o(\alpha_1,\ldots,\alpha_m) = \frac{\Gamma(A_1+A_2+\ldots A_m)}{\Gamma(A_1)\Gamma(A_2)\ldots\Gamma(A_m)} \prod_{k=1}^{m} \alpha_k^{A_k-1} \tag{E.18}$$

and the likelihood function given in Equation (E.16) in Bayes' theorem results in another Dirichlet distribution for the posterior distribution,

$$\pi(\alpha_1,\ldots,\alpha_m|E) = C^{-1}\, L(E|\alpha_1,\ldots,\alpha_m)\pi_o(\alpha_1,\ldots,\alpha_m) \tag{E.19}$$

where C is a normalization factor. The posterior distribution has the same form as Equation (E.18) with the following parameters

$$A_k' = A_k + n_k \qquad k=1,\ldots,m \tag{E.20}$$

The marginal distribution of α_k is a beta distribution with mean and mode given by

$$\text{mean:} \quad \bar{\alpha}_k = \frac{A_k + n_k}{\sum_{k=1}^{m} (A_k+n_k)} \qquad k=1,\ldots,m \tag{E.21}$$

$$\text{mode:}\quad \alpha_k = \frac{A_k + n_k - 1}{\sum_{k=1}^{m} (A_k + n_k - 1)} \qquad k=1,\ldots,m \tag{E.22}$$

For a uniform prior $A_k = 1$ $k=1,\ldots,m$, we have

$$\alpha_k = \frac{n_k}{\sum_{k=1}^{m} n_k} \qquad k=1,\ldots,m \tag{E.23}$$

which is the maximum likelihood estimator of α_k.

E.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.

E.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.

We first note that, based on the definition of the α-factors and the MGL parameters, we can establish the following relations.

$$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3} \tag{E.24}$$

$$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3} \tag{E.25}$$

Using the standard approach for change of variables, the distributions of the MGL and α-factor model parameters are related through the following equation:

$$\pi_{\alpha,\beta}(\beta,\gamma) = \frac{\pi_{\alpha_1, \alpha_2, \alpha_3}(\alpha_1, \alpha_2, \alpha_3)}{|J(\alpha_1, \alpha_2, \alpha_3)|} \tag{E.26}$$

where, defining a dummy parameter $\chi = \alpha_2$, the Jacobian is written as

$$J(\alpha_1, \alpha_2, \alpha_3) = \begin{vmatrix} \frac{\partial \beta}{a_1} & \frac{\partial \beta}{a_2} & \frac{\partial \beta}{a_3} \\ \frac{\partial \gamma}{\alpha_1} & \frac{\partial \gamma}{\alpha_2} & \frac{\partial \gamma}{\alpha_3} \\ \frac{\partial \chi}{\alpha_1} & \frac{\partial \chi}{\alpha_2} & \frac{\partial \chi}{\alpha_3} \end{vmatrix} \tag{E.27}$$

Since,

$$\frac{\partial \beta}{\partial \alpha_2} = \frac{\partial \beta}{\partial \alpha_2} = \frac{\partial \chi}{\partial \alpha_1} = \frac{\partial \chi}{\partial \alpha_3} = 0 \tag{E.28}$$

Then,

$$J(\alpha_1, \alpha_2, \alpha_3) = - \left(\frac{\partial \beta}{\partial \alpha_1}\right)\left(\frac{\partial \gamma}{\partial \alpha_3}\right) - \left(\frac{\partial \beta}{\partial \alpha_3}\right)\left(\frac{\partial \gamma}{\partial \alpha_1}\right) \tag{E.29}$$

From Equations (E.24) and (E.25), eliminating α_2, we have

$$\frac{\partial \beta}{\partial \alpha_1} = \frac{-\frac{9}{2} - \frac{9}{4}\alpha_3}{\left(3 - \frac{3}{2}\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{E.30}$$

$$\frac{\partial \beta}{\partial \alpha_3} = \frac{\frac{9}{4}\alpha_1}{\left(3 - \frac{3}{2}\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{E.31}$$

$$\frac{\partial \gamma}{\partial \alpha_1} = \frac{\frac{27}{2}\alpha_3}{\left(3 - 3\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{E.32}$$

$$\frac{\partial \gamma}{\partial \alpha_3} = \frac{\frac{27}{2} - \frac{27}{2}\alpha_1}{\left(3 - 3\alpha_1 + \frac{3}{2}\alpha_3\right)^2} \tag{E.33}$$

Using the above equations in Equation (E.29) and replacing α_1 and α_3 by

$$\alpha_1 = \frac{3(1-\beta)}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma} \tag{E.34}$$

$$\alpha_3 = \frac{\beta\gamma}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma} \tag{E.35}$$

$$J = \frac{2}{9\beta}\left(3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma\right)^3 \tag{E.36}$$

Therefore,

$$\pi_{\beta,\gamma}(\beta,\gamma) = \frac{9\beta}{2\left(3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma\right)^3}\,\pi_{\alpha_1,\alpha_2,\alpha_3}(\alpha_1,\alpha_2,\alpha_3) \tag{E.37}$$

Based on the discussion in Section E.3, for a uniform prior distribution, the distribution of α_1, α_2, and α_3 is given by

$$\pi_{\alpha_1,\alpha_2,\alpha_3}(\alpha_1,\alpha_2,\alpha_3) = \frac{\Gamma(n_1+n_2+n_3)}{\Gamma(n_1)\,\Gamma(n_2)\,\Gamma(n_3)}\,\alpha_1^{n_1-1}\,\alpha_2^{n_2-1}\,\alpha_3^{n_3-1} \tag{E.38}$$

Equations (E.34) and (E.35) give the relation between α_1 and α_3 and β and γ. The corresponding equation for α_2 is

$$\alpha_2 = \frac{\frac{3}{2}\beta\,(1-\gamma)}{3 - \frac{3}{2}\beta - \frac{1}{2}\beta\gamma} \tag{E.39}$$

We can now replace α_1, α_2, and α_3 in Equation (E.39) by Equations (E.35), (E.36), and (E.40). The resulting distribution can then be used in Equation (E.38) to obtain the distribution of β and γ:

$$\pi_{\beta,\gamma}(\beta,\gamma) = C\,\frac{\beta^{n_2+n_3-1}\,(1-\beta)^{n_1-1}\,\gamma^{n_3-1}\,(1-\gamma)^{n_2-1}}{3-\frac{3}{2}\beta - \frac{1}{2}\beta\gamma^{\,n_1+n_2+n_3}}$$

where

$$C = \frac{3^{n_1+n_2}}{2^{n_2}}\,\frac{(n_1+n_2+n_3)}{\Gamma(n_1)\,\Gamma(n_2)\,\Gamma(n_3)} \tag{E.41}$$

From Equation (E.40), 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 groups as described in step 2 of the procedure. In such cases, the approximate method described in the following section may be used.

E.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 $\{n_k\ k=1, \ldots, m\}$ where n_k is the number of events involving failure of k components due to common cause will be

interpreted as $\{kn_k;\ k=1, \ldots, m\}$ where kn_k is the number of components failed in common cause events involving k component falures, 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 a component being involved in a double failure.

$Z_3 \equiv \beta\gamma$ = conditional probability of a 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.

$$P(n_1,2n_2,3n_3,|Z_1,Z_2,Z_3) = \frac{(n_1 + 2n_2 + 3n_3)!}{(n_1)!(2n_2)!(3n_3)!} \; Z_1^{n_1} Z_2^{2n_2} Z_3^{3n_3} \qquad \text{(E.42)}$$

Rewriting Equation (E.43) in terms of β and γ gives

$$P(n_1,2n_2,3n_3|\beta,\gamma) = M\,\beta^{2n_2+3n_3}(1-\beta)^{n_1}\gamma^{3n_3}(1-\gamma)^{2n_2} \qquad \text{(E.43)}$$

where M is the multinomial multiplier as in Equation (E.42).

We now write Bayes' theorem as

$$\pi(\beta,\gamma|n_1,2n_2,3n_3) = \frac{1}{C} P(n_1,2n_2,3n_3|\beta,\gamma)\pi_0(\beta,\gamma) \qquad \text{(E.44)}$$

where π_0 and π are the prior and posterior distribution of β and γ and C is a normalizing factor defined as

$$C = \int_0^1 \int_0^1 P\,(n_1,2n_2,3n_3|\beta,\gamma)\pi_0(\beta,\gamma)d\beta\; d\gamma \qquad \text{(E.45)}$$

As the prior, one can use a multinomial distribution

$$\pi_0(\beta,\gamma) = h\,\beta^{A_0-1}(1-\beta)^{B_0-1}\gamma^{C_0-1}(1-\gamma)^{D_0-1} \qquad \text{(E.46)}$$

where h is given by

$$h = \frac{\Gamma(A_0 + B_0 + C_0 + D_0)}{\Gamma(A_0)\Gamma(B_0)\Gamma(C_0)\Gamma(D_0)} \tag{E.47}$$

A flat prior distribution is obtained by setting $A_0 = B_0 = C_0 = D_0 = 1$.

Using Equation (E.46) in Equation (E.44) results in a posterior distribution for β and γ that is also multinomial, with parameters

$$A = A_0 + 2n_2 + 3n_3$$

$$B = B_0 + n_1$$

$$C = C_0 + 3n_3$$

$$D = D_0 + 2n_2 \tag{E.48}$$

The mode of the posterior distribution occurs at

$$\beta = \frac{A-1}{A+B-2} \tag{E.49}$$

$$\gamma = \frac{C-1}{C+D-2} \tag{E.50}$$

The mean values are calculated from

$$\overline{\beta} = \frac{A}{A+B} \tag{E.51}$$

$$\overline{\gamma} = \frac{C}{C+D} \tag{E.52}$$

Note that for the flat prior the mode of the posterior distribution is

$$\beta = \frac{2n_2 + 3n_3}{n_1+2n_2+3n_3} \tag{E.53}$$

$$\gamma = \frac{3n_3}{2n_2+3n_3} \tag{E.54}$$

which correspond to the point estimates developed in Section 3, Volume I 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 (References E-2 and E-3). The difference may not be significant, however, if other sources of uncertainty are accounted for in the development of these distributions.

E.5 DISTRIBUTIONS FOR BFR PARAMETERS

To obtain uncertainty distributions for the parameters of the BFR model, Bayes' theorem is used as follows (the method presented here is an extension of the method presented in Reference E-1):

$$P(Q_I,\lambda_t,\omega,p|data) = \frac{1}{C} L(data|Q_I,\lambda_t,\omega,p)\ P_o(Q_I,\lambda_t,\omega,p) \tag{E.55}$$

where

$$C \equiv \int_{Q_I} \int_{\lambda_t} \int_{\omega} \int_{p} L(data|Q_I,\lambda_t,\omega,p,)\ P_o(Q_I,\lambda_t,\omega,p) \tag{E.56}$$

and P_o and P are the prior and posterior distributions for the quantities, Q_I, λ_t, ω, and p. To obtain the likelihood term, we note that the data consists of (n_I, n_L, n_1, n_2, ..., n_m), where n_I is the number of single failures that were not due to common cause shocks, n_L is the number of occurrences of lethal shocks, and, finally, n_k, k=1, ..., m, is the number of occurrences of exactly k failures due to nonlethal shocks in t hours of operation.

In this model, times of occurrences of noncommon cause individual component failures, nonlethal shocks, and lethal shocks are assumed to be exponentially distributed. Therefore, n_I, n_t, and n_L have Poisson distributions with parameters Q_I, λ_t, and ω.

Now, the joint likelihood of the data can be decomposed into marginal distributions as follows:

$$\begin{aligned} L &= P[n_I,\ n_L,\ n_1,\ldots,n_m] \\ &= P[n_I]\ P[n_L]\ P[n_t]\ P[n_1,\ldots,n_m|n_t] \end{aligned} \tag{E.57}$$

Where the first three distributions on the left-hand side of the equation are Poisson,

$$P[n_I|Q_I] = \frac{(Q_I t)^{n_I}}{n_I!} e^{-Q_I t} \tag{E.58}$$

$$P[n_L|1] = \frac{(\omega t)^{n_L}}{n_L!} e^{-\omega t} \tag{E.59}$$

$$P[n_t|\lambda_t] = \frac{(\lambda_t t)^{n_t}}{n_t!} e^{-\lambda_t t} \tag{E.60}$$

The fourth term is multinomial distribution; i.e.,

$$P[n_1,n_2,\ldots,n_m|n_t,p] = \frac{n_t!}{n_1!\ldots n_m!} \prod_{i=1}^{m} Z_i^{n_i} \tag{E.61}$$

where

$$Z_i = \frac{m!}{(m-i)!\ i!} \frac{p^i q^{m-i}}{1-q^m} \tag{E.62}$$

where

$$q = 1 - p \tag{E.63}$$

The estimators provided in Section 3 are in fact the maximum likelihood estimator based on the likelihood function of Equations (E.58) through (E.62).

As we saw earlier, the likelihood function can be decomposed into likelihood functions for each of the four quantities. Similarly, the prior distribution, P_o, can be written as the product of four prior distributions,

$$P_o(Q_I,\lambda_t,\omega,p) = P_o(Q_I)P_o(\lambda_t)P_o(\omega)P_o(p) \tag{E.64}$$

As a result, the posterior distribution of Equation (E.55) can also be decomposed into the product of four distributions. Since the likelihood for the first three parameters are Poisson, a reasonable choice for the family of their corresponding priors is the gamma family of distributions, which has the following form

$$f(x) = \frac{b^a}{\Gamma(a)} x^{a-1} e^{-bx} \qquad x \geq 0 \tag{E.65}$$

where $a \geq 0$ and $b \geq 0$ are the two parameters of the distribution. Let (a,b), (a_t,b_t), and (a_ω,b_ω) be the parameters of the gamma prior distribution for Q_I, λ_t, and ω, respectively. If

$$a = a_t = a_\omega = \frac{1}{2}$$

$$b = b_t = b_\omega = 0 \tag{E.66}$$

then the resulting priors are noninformative for Q_I, λ_t, and ω.

Reference E-1 suggests the use of beta distribution for p,

$$f(p) = \frac{\Gamma(c+d)}{\Gamma(c)\Gamma(d)} p^{c-1} (1-p)^{d-1} \tag{E.67}$$

where c and d are the two parameters of the distribution. According to Reference E-1,

$$c = d = \frac{1}{2}$$

approximates a noninformative prior for p.

The general form of the posterior distribution is then

$$p(Q_I,\lambda_t,\omega,p) = C^{-1} Q_I^{a'} \lambda_t^{a_t'} \omega^{a_\omega'} e^{-(b' Q_I + b_t' \lambda_t + b_\omega' \omega)} \times \frac{p^{s+c-1} q^{mn_t-s+d-1}}{(1-q^m)^{m_t}} \quad \text{(E.68)}$$

where

$$a' = a + n_I - 1 \qquad b' = b + t$$

$$a_t' = a_t + n_t - 1 \qquad b_t' = b_t + t$$

$$a_\omega' = a_\omega + n_L - 1 \qquad b_\omega' = b_\omega + t \quad \text{(E.69)}$$

The mean values of λ, λ_t, and ω can be calculated analytically and are

$$\overline{Q}_I = \frac{n_I + a}{t + b} \quad \text{(E.70)}$$

$$\overline{\lambda}_t = \frac{n_t + a_t}{t + b_t} \quad \text{(E.71)}$$

$$\overline{\omega} = \frac{n_L + a_\omega}{t + b_\omega} \quad \text{(E.72)}$$

However, the mean of p can only be calculated by numerical integration.

Maximizing the posterior distribution [Equation (E.68)] to obtain the mode results in the following estimates:

$$Q_I = \frac{n_I + a - 1}{t + b} \quad \text{(E.73)}$$

$$\lambda_t = \frac{n_t + a_t - 1}{t + b_t} \quad \text{(E.74)}$$

$$\omega = \frac{n_L + a_\omega - 1}{t + b_\omega} \tag{E.75}$$

$$\hat{s}_1 = p \frac{m}{1-q} \frac{n_t}{m} + \hat{p}\,(d-1) - q\,(c-1) \tag{E.76}$$

E.6 REFERENCE

E-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.

E-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.

E-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 F

PRACTICAL CONSIDERATIONS

F.1 INTRODUCTION

The procedural framework described in Volume I allows application at varying levels of detail. It is recognized that it may not always be necessary or practical to perform the analysis to the level of detail discussed in Section 3 and applied in the auxiliary feedwater system example in Section 4. Indeed, the screening analysis, Stage 2 of the procedure, is included as an essential element in achieving a practical methodology in that it restricts the number of common cause failure events that have to be analyzed in detail. The purpose of this appendix is to discuss the various practical aspects of applying the procedure, to identify where simplifying assumptions are made, and where they can be made without loss of accuracy. The topics discussed here are entirely concerned with the analytical aspect, and not the qualitative screening or the data analysis.

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), large fault trees can result from the identification of large common cause component groups or many common cause component groups. 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 one-out-of-N (for success) systems that are comprised of N components so that system failure requires failure of all N components. Suppose that all N components are assigned to the same common cause group. The systematic procedures described in the guide suggest as one alternative 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 given by

$$n_e = \sum_{j=1}^{N} \binom{N}{j} = 2^N - 1 \qquad \text{(F.1)}$$

Values of n_e are listed in Table F-1 for selected values of N, 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. More than 6,000 minimal cutsets result from the 6 component-common cause fault tree. Even systems with 10 or 11 identical components (e.g., relief valves in a BWR ADS system) are well beyond the practical limit of a complete fault tree

TABLE F-1

SIZE PARAMETERS FOR COMMON CAUSE EVENT FAULT TREES OF ONE-OUT-OF-N SYSTEMS

N 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	(*)
100	6.3×10^{32}	1.3×10^{30}	(*)

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

(a) Determined from

$$n = N. \sum_{j=0}^{N} \binom{N-1}{j}$$

(b) Detemined from Equation F-1.
(c) As determined by fault tree solution with SETS.

analysis of all common cause events. In these situations, it is necessary to either simplify the model or apply algebraic formulas to component-level logic models, as more fully described below.

Section F.2 discusses analytical methods that are applicable in both the screening and the detailed analysis, while Section F.3 is concerned with methods that are specific to the detailed analysis of Stage 3 of the procedural framework. Section F.4 discusses briefly the iterative application of this framework to achieve an economical yet detailed system analysis that incorporates common cause failures.

F.2 ANALYTICAL METHODS APPLICABLE TO BOTH SCREENING AND DETAILED ANALYSES

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 model.

F.2.1 Model Simplification

In the most rigorous application of the procedures 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 $2^N - 1$ such combinations in a group of N 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 original beta factor model incorporated this technique by modeling only the purely independent events and the global common cause events; i.e., the event that fails all N components in a common cause group.

There are natural variations on the beta factor model within this class of techniques 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 "rigorous" approach. One such variation, for groups having five or more components, might be 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. In practical situations with five or more components, there is no real technical justification in light of data analysis uncertainties to have a greater degree of freedom than that included in this type of model.

When the model is simplified using one of these approaches, it is very important to analyze the data in a consistent manner. If care is taken, the analyst can ensure that any errors introduced by event deletion are controlled in a conservative manner. For example, if using the above model in a system of, say, 12 components, any event that involved failure of 4 or more components would be counted in the data analysis as failing all 12 components, or, if the original beta factor model is being used, any common cause event would be counted as failing all N components.

For example, if the truncated model described above is being used to analyze a 12-component system, suppose that the following data were developed (after screening the events and performing the necessary upward and downward mapping of applicable data from different sized systems).

$$n_1 = 100$$
$$n_2 = 4$$
$$n_3 = 2$$
$$n_{\geq 4} = 1$$

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 also not make the distinction. So, for estimation of the β-factor, the following approach would be used to estimate the mean of the β-factor uncertainty distribution (see Section E.3, Appendix E, Volume I).

$$\beta = \frac{2n_2 + 3n_3 + 12n_{\geq 4}}{n_1 + 2n_2 + 3n_3 + 12n_{\geq 4}} = \frac{26}{126} \simeq .2$$

If the β-factor model was being used to analyze some system with the same data as above, the following approach would ensure that the modeling truncation error is conservative. Assume all common cause events (i.e., $n_2 + n_3 + n_{\geq 4}$) fail all 12 components, and estimate β as

$$\beta = \frac{(n_2 + n_3 + n_{\geq 4})\ (12)}{n_1 + (n_2 + n_3 + n_{\geq 4})\ (12)} = \frac{84}{184} \simeq .45$$

The quantitative screening proposed in this guide has adopted the most simple and conservative approach of using the beta factor type of model; that is, using only the global common cause terms. The use of the global common cause term will be revisited in terms of the detailed analysis in Section F.3.

F.2.2 Truncation

When all the common cause events are included in the logic model, or when some are omitted and the 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 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 4.1, Volume I, 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 2, with single failures of components in a given component group, any cutsets of events within the same group of order 3 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.

A variation on this approach is to truncate certain types of cutsets within a given order. For example, the approach followed in the COMCAN software (Reference F-1) includes three types of cutsets: (1) purely independent events of any order, (2) cutsets with one independent event, a common cause event, and (3) first-order cutsets that are global events.

An alternative approach is one in which cutsets or algebraic model terms are truncated, based on estimates, or bounds, on their probabilities. 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. To best control this approach, it is highly desirable that the estimates, or bounds, on the probability of truncated cutsets be saved for comparison to the final result. This comment also applies to the cutset order truncation technique.

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 to fault tree analysts and is incorporated into such fault tree computer programs as WAME and SETS. It was employed in the U.S. contribution to the Common Cause Reliability Benchmark Exercise (Reference F-2). The system that was 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 independent events fault tree 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 "rigorous" approach described in this procedures guide, 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 whatsoever. 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 fault tree not simplified in this way.

F.2.3 Incorporation of Common Cause Events into the Plant Model

There are basically two different approaches to plant modeling: the fault tree linking and the support state model approach. 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 fault trees for the support systems and frontline systems before solution for the cutsets. However, the inclusion of many additional events into fault trees can make their solution cumbersome. Two alternatives are discussed here. This approach is to solve for the cutsets without the common cause events and to substitute into the resulting minimal cutsets expressions, which expand the component events into independent and common cause events. The latter approach can be 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 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 illustrated below.

F.2.3.1 Basic Event Substitution

Suppose a system is composed of four components, X, Y, Z, and W. The first three of these are identical and belong to a common cause group, and the fourth, component W, is independent of the first three. Let all the causal events in this system be denoted by C_j, where j denotes the particular impact of that cause in terms of a component, or combination of components, that is affected. All the basic events in the resultant fault tree are listed as follows:

Independent Cause Events	Common Cause Events
C_X	C_{XY}
C_Y	C_{XZ}
C_Z	C_{YZ}
C_W	C_{XYZ}

Assume that the system success criterion dictates that there are two minimal cutsets for the system in the component-level Boolean for the normal alignment. The minimal cutsets are given by

{X,Y} and {Z,W}

Therefore, the solution to the problem with component level basic events is

$$\boxed{T = X^*Y + Z^*W}^{*} \qquad (F.2)$$

*All equations with boxes are Boolean algebra; those without are normal algebra.

Incorporation of the common cause basic events into the fault tree is equivalent to the Boolean substitution

$$X = C_{XY} + C_{XZ} + C_{XYZ} + C_X$$
$$Y = C_{XY} + C_{YZ} + C_{XYZ} + C_Y$$
$$Z = C_{YZ} + C_{XZ} + C_{XYZ} + C_Z$$
$$W = C_W$$

Consequently Equation (F.2) becomes

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

After Boolean reduction

$$T = C_{XY} + C_{XYZ} + C_{XZ}*C_Y + C_X*C_Y + C_{XZ}*C_{YZ} + C_{YZ}*C_W + C_{XZ}*C_W + C_Z*C_W + C_X*C_{YZ} \quad \text{(F.13)}$$

The final equation is equivalent to the following list of minimal cutsets:

Singles: $\{C_{XY}\}$[a] ; $\{C_{XYZ}\}$

Doubles: $\{C_{XZ}*C_{YZ}\}$[a] ; $\{C_{XZ}*C_Y\}$; $\{C_X*C_Y\}$; $\{C_X*C_{YZ}\}$

$\{C_{YZ}*C_W\}$; $\{C_{XZ}*C_W\}$; $\{C_Z*C_W\}$

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

$$P(T) \simeq P\{C_{XY}\} + P\{C_{XYZ}\} + P\{C_{XZ}\} \cdot P\{C_{YZ}\} + P\{C_{XZ}\} \cdot P\{C_Y\} + P\{C_X\} \cdot [P\{C_Y\} + P\{C_{YZ}\}] + P\{C_W\}[P\{C_{YZ}\} + P\{C_{XZ}\} + P\{C_Z\}] \quad \text{(F.4)}$$

Applying the assumption of symmetry, i.e., that

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

(a)For a discussion of these controversial cutsets, refer to Section C.1 of this volume.

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

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

we obtain

$$P(T) = Q_2 + Q_3 + Q_2^{2*} + 2Q_1Q_2 + Q_1^2 + Q_W(Q_1 + 2Q_2) \qquad (F.5)$$

F.2.3.2 A "Support State" Model

The support state model suggests an alternative approach to the inclusion of common cause events. This model uses a conditional probability formalism to account for all dependencies. Thus

$$P(T) = \sum_{j=i}^{N} P(S_j)\ P(T|S_j) \qquad (F.6)$$

where

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

T = top event of the system fault tree.

S_j = one of N mutually exclusive and exhaustive conditions under which the top event can occur.

$T|S_j$ = fault tree modified to reflect the condition S_j; i.e., given Prob $(S_j) = 1$.

The common cause events can be included in such a model by associating a common cause failure occurrence with one of a set of states, S_j. Since the common cause dependency is explicitly accounted for in the term $P(S_j)$, the events constituting $T|S_j$ are now independent and, therefore,

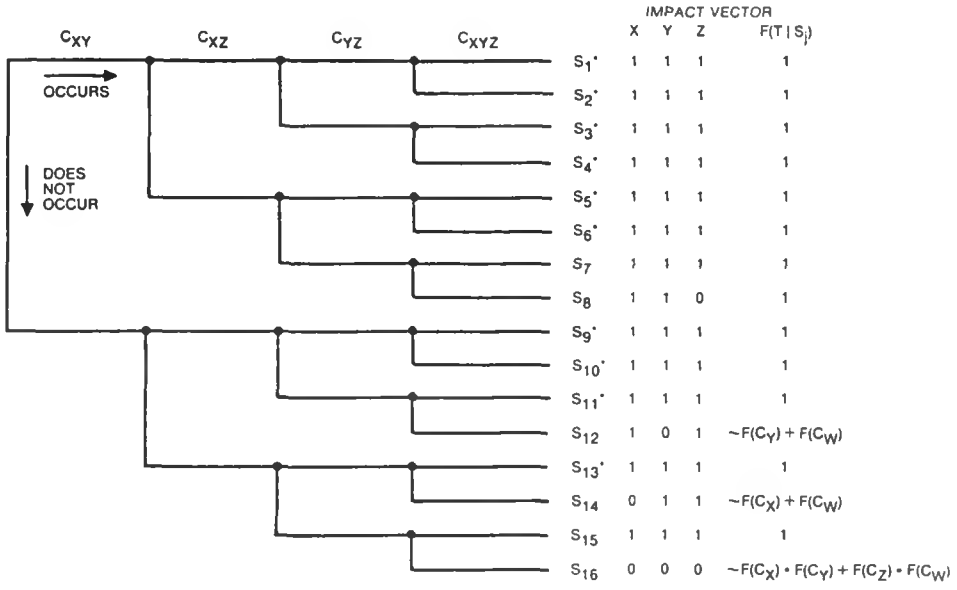
$$P(T|S_j) = P(X|S_j)\cdot P(Y|S_j) + P(Z|S_j)\cdot P(W|S_j) - P(X|S_j)\cdot(P(Y|S_j)P(Z|S_j)P(W|S_j) \qquad (F.7)$$

What this means in practice is that each term in the right-hand side can be expressed as the following for $P(X|S_j)$

$$P(X|S_j) = \begin{cases} P(C_X), & \text{states that do not impact component X} \\ 1, & \text{states that impact component X} \end{cases}$$

The use of an event tree to generate all the common cause event states is illustrated as follows.

*See discussion in Section C.1 of this volume regarding terms involving overlapping components in basic events.



Using the event tree to help calculate the $P(S_j)$ terms in Equation (F.2) and the impact vectors to help calculate the $P(T|S_j)$ terms, the top event frequency, $P(T)$, can be written as

$$P(T) \simeq P(C_{XYZ}) + P(C_{XY}) + P(C_{XZ})[P(C_{YZ})^{**} + P(C_Y) + P(C_W)]$$

$$+ P(C_{YZ})\cdot[P(C_X) + P(C_W)] + P(C_X)P(C_Y) + P(C_Z)\cdot P(C_W)$$

$$= Q_2 + Q_3 + Q_2^{2**} + 2Q_1Q_2 + Q_1^2 + Q_W(Q_1 + 2Q_2) \qquad \text{(F.10)}$$

where the approximations are valid for all frequencies $P(\alpha)<<1$.

Equation (F.10) is identical to Equation (F.6), which demonstrates the feasibility of this alternative approach to solving the example problem. In larger problems, it may be easier to follow the decomposition method, or vice versa.

F.3 DETAILED MODELING

Three topics are presented in this section. The first is a useful table of results that can be used directly or as a means to check that an analysis has been done correctly. It is called here "the pattern recognition approach." The second topic concerns the merits of using the global common cause

*If the events are considered mutually exclusive, these states cannot exist.
**This basic event would not exist if the basic events involving overlapping components are considered mutually exclusive.

terms only in the detailed modeling, and the third topic is that of refinement of common cause grouping when components are potentially a common cause group but some feature, perhaps of their operation, introduces some asymmetry.

F.3.1 The Pattern Recognition Approach

When the systematic procedures of this report are followed, it is not necessary to know the algebraic formulas for relating the system failure logic to the common cause model parameters. It is only necessary to know the formulas 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 rather large "library" of formulas for different systems and situations. This "library" of formulas can be used to support an alternative approach to common cause analysis, which the authors have termed the "pattern recognition approach."

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 pattern to one in his library, the analyst synthesizes the appropriate algebraic formulas 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 entrusts whoever developed the formulas that these steps have been properly performed and relies on the 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 omit or double count important cutsets and key contributors, as explained more fully in Section 4, Volume I. 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, the authors recognize that there may be some resistance to adopting the recommended "rigorous" approach, even when its application is feasible. Therefore, the authors provide guidance in this section on the proper use of formulas for common cause analysis when the pattern recognition approach is followed.

The chief difficulty with 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 then be made to decompose the system into independent subsystems for pattern matching. Independence implies here that there are no shared components between two or more subsystems and that the boundaries of all the common cause component groups 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 formulas for independent and common cause events in some simple, frequently encountered configurations is provided in Table F-2. For each model, formulas are provided for the basic parameter model on the assumption that the common cause basic events are manually exclusive. Additional terms are required if independence is assumed and indicated in the comments column. All the formulas account for all the first and second order minimal cutsets in the fault trees that include the common cause events. In some models, the technique of omitting or disallowing some common cause events is applied.

Models 1 through 8 cover all the simple "K out of N" (for success) situations for N up to four, and "one out of N" (for success) situations for N up to six. In each of these model formulas, the only approximations made are the rare event approximation and the truncation of cutsets of order 3 and higher. Otherwise, all possible common cause events are accounted for.

Models 9, 10, and 11 cover selected four-component configurations that exhibit some asymmetries that have been accounted for in selecting common cause events for inclusion in the models. Models 12 and 13 cover general parallel-series and series-parallel configurations of identical redundant components. These models and model 14 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.

There are pitfalls when formulas are applied to a list of minimal cutsets obtained from a component-level fault tree. To illustrate, suppose the minimal cutsets of a system 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 5. 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 4. 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 (i.e., the lethal shocks) are multiply accounted for. Additional pitfalls in applying formulas are described in Section 4, Volume I.

F.3.2 USE OF SIMPLIFIED MODELS

It is not always necessary to include all possible common cause events associated with a common cause component group containing many (more than two) components. The example in Section 4.1 illustrated that neglect of all terms other than the global common cause term resulted in an underestimate of the system unavailability that was negligible particularly when taking into account the uncertainties in the parameter estimates.

It should be pointed out however that 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 one has failed.

Currently, this appears to be the case in most evaluations. The reason is possibly that the data base, even after expansion to include industry wide experience, is small for multiple failure events, leading to potentially conservative estimates of the conditional probabilities of three, given two; four, given three; etc., failures.

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

F.3.3 Modeling Asymmetrical Common Cause Events

Most of the common cause event models presented in this guidebook use an assumption regarding the symmetry of causes acting on a group of causes. The basic parameter, multiple Greek letter, and binomial failure rate models in Table F-2 all assume, with a few exceptions, 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. In a three-train system, for example, the basic parameter model assumes that

$$Q_{AB} = Q_{BC} = Q_{AC} = Q_2 \qquad (F.11)$$

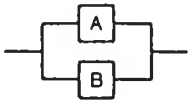
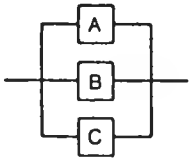
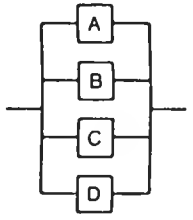
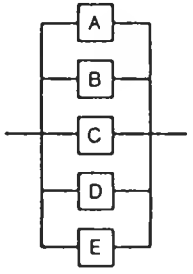
There are many situations in practice in which the common cause events would be expected to exhibit asymmetries. An example is the case of certain so-called alternating systems, of which component cooling water is one where one train is normally operating, while the others are in standby. Some of these situations were envisioned in models 9, 10, and 11 in Table F-2. In model 9, a mix of normally operating and standby components produces an asymmetry. In models 10 and 11, 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; e.g., those affecting a pair of components, each in a different system.

The basic approach to modeling asymmetries is to incorporate them into the system logic model by either adding to or subtracting from the model as appropriate to model the asymmetry. Because the common cause events affect the determination of minimal cutsets, this is highly preferable to manipulating algebraic formulas directly to add or delete the appropriate events. In Table F-2, models 1 through 8 include fully symmetric causes, whereas models 10 through 11 incorporate asymmetries by the deletion of events from the system's logic model.

Another example of an asymmetrical model was developed by adding events to the logic model that initially included all the symmetric causes. This occurred in the case of a three-train auxiliary feedwater system that included three identical mechanical pumps. During the screening of common cause event data some of the events could act on the pumps in a symmetric fashion, whereas

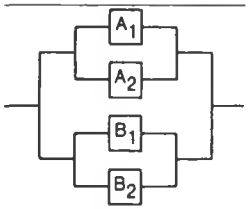
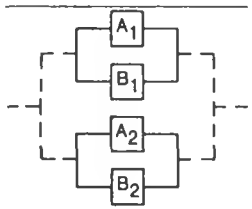
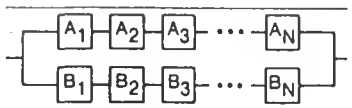
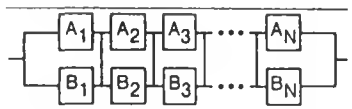
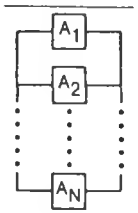
Table F-2

ALGEBRAIC FORMULAS FOR COMMON CAUSE EVENTS IN SOME SIMPLE SYSTEM CONFIGURATIONS

RELIABILITY BLOCK DIAGRAM	MODEL NO.	MODEL DESCRIPTION/ SUCCESS CRITERIA	APPROXIMATE FORMULAS BASIC PARAMETER MODEL*	KEY ASSUMPTIONS
	1	TWO UNITS IN STANDBY; ONE OF TWO MUST OPERATE ON DEMAND	$Q_2 + Q_1^2$	NONE
	2	TWO UNITS IN OPERATION; ONE OF TWO MUST OPERATE AT LEAST t HOURS	$\lambda_2 t + (\lambda_1 t)^2$	
	3	THREE UNITS IN STANDBY, TWO OF THREE MUST OPERATE ON DEMAND	$3Q_1^2 + 3Q_2 + Q_3$	NONE
	4	THREE UNITS IN STANDBY; ONE OF THREE MUST OPERATE ON DEMAND	$3Q_1Q_2 + 4Q_3 + Q_1^3$	ADD $3Q_2^2$ IF UNITS ARE ASSUMED INDEPENDENT NOT MUTUALLY EXCLUSIVE
	5	FOUR UNITS IN STANDBY; THREE OF FOUR MUST OPERATE ON DEMAND	$6(Q_1^2 + Q_2) + 4Q_3 + Q_4$	NONE
	6	FOUR UNITS IN STANDBY; TWO OF FOUR MUST OPERATE ON DEMAND	$12Q_1Q_2 + 3Q_2^2 + 4(Q_3 + Q_1^3) + Q_4$	ADD $12Q_2^2$ IF EVENTS ARE ASSUMED INDEPENDENT NOT MUTUALLY EXCLUSIVE
	7	FOUR UNITS IN STANDBY; ONE OF FOUR MUST OPERATE ON DEMAND	$3Q_2^2 + 4Q_1Q_3 + Q_4 + 6Q_1Q_2^2 + Q_1^4$	
	8	FIVE UNITS IN STANDBY; ONE OF FIVE MUST OPERATE ON DEMAND	$10Q_2Q_3 + 5Q_1Q_4 + Q_5$	ADD $15Q_3^2 + 20Q_2Q_4 + 30Q_3Q_4 + 20Q_4^2$ IF EVENTS ARE ASSUMED INDEPENDENT NOT MUTUALLY EXCLUSIVE

ENTED BY Q AND λ, RESPECTIVELY. THE MISSION TIME IS t WHEN APPLICABLE.

Table F-2 (Sheet 2 of 2)

RELIABILITY BLOCK DIAGRAM	MODEL NO.	MODEL DESCRIPTION/ SUCCESS CRITERIA	APPROXIMATE FORMULAS BASIC PARAMETER MODEL*	KEY ASSUMPTIONS
	9	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	$(\lambda_1 t)^4 + Q_1{}^2(\lambda_1 t)^2 + 2Q_1(\lambda_1 t)^3 + (\lambda_2 t)^2 + \lambda_4 t + 2\lambda_2 t(Q_1 + \lambda_1 t)(\lambda_1 t)$	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.
	10	FOUR REDUNDANT UNITS IN STANDBY; TWO IN UNIT 1 AND TWO IN UNIT 2; ONE OF FOUR MUST OPERATE ON DEMAND	$2Q_1Q_2 + Q_4$	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.
	11	SAME AS MODEL VII EXCEPT UNITS ARE ALL IN OPERATION AND ONE MUST OPERATE FOR t HOURS	$2\lambda_1\lambda_2 t^2 + \lambda_4 t$	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.
	12	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.
	13	SAME AS MODEL 13 WITH CROSSTIES; AT LEAST ONE OF TWO IN EACH OF N STAGES MUST 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.
	14	N COMPONENTS IN STANDBY; AT LEAST K COMPONENTS OUT OF N, K < N MUST OPERATE ON DEMAND	$\left\{ \sum_{j=N-k+1}^{N} \binom{N}{j} Q_1{}^j(1-Q_1)^{N-j} + Q_N \right\}$	WHEN A COMMON CAUSE FAILURE OCCURS, ALL N COMPONENTS ARE ASSUMED TO FAIL.

*FAILURES ON DEMAND AND DURING OPERATION ARE REPRESENTED BY Q AND λ, RESPECTIVELY. THE MISSION TIME IS t WHEN APPLICABLE.

others, due to the scoping layout, could only affect two specific pumps. A model of this system that accounts for both the symmetric and asymmetric causes was developed using the systematic procedures of this guidebook. A fault tree was constructed by separating the symmetric and asymmetric causes, as shown in Figure F-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 4 in Table F-2 whose MGL formula for system failure probability is

$$Q_S \simeq \frac{3}{4}(1-\gamma)\beta Q^2[2 + (1-\gamma)\beta]^* + \gamma\beta Q \qquad (F.12)$$

The minimal cutsets of the fault tree in Figure F-1 are:

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

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

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

$\{X, C_I\}$; $\{X, C_{AC}\}$; $\{X, C_{BC}\}$

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

where each set of braces represents a single minimal cutset. It is important to note that in setting up the impact vectors 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 4 in Table F-2 that include purely symmetric cause events, plus three second-order cutsets that include the asymmetric cause event. In terms of the basic parametric model, the formula for the system in Figure F-1 can be developed using

$$Q_S \simeq 3Q_1Q_2 + 3Q_2^{2*} + Q_3 + Q_X(Q_1 + 2Q_2)$$

which, according to the MGL formulas becomes

$$Q_S \simeq \frac{3}{4}(1-\gamma)\beta Q^2[1 + (1-\gamma)\beta]^* + \gamma\beta Q + Q_X(1-\beta\gamma)$$

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 systematic procedures of this guidebook to incorporate asymmetries into the models. 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. This approach is preferable to the

*See discussion in Appendix C regarding cutsets involving basic events with overlapping components.

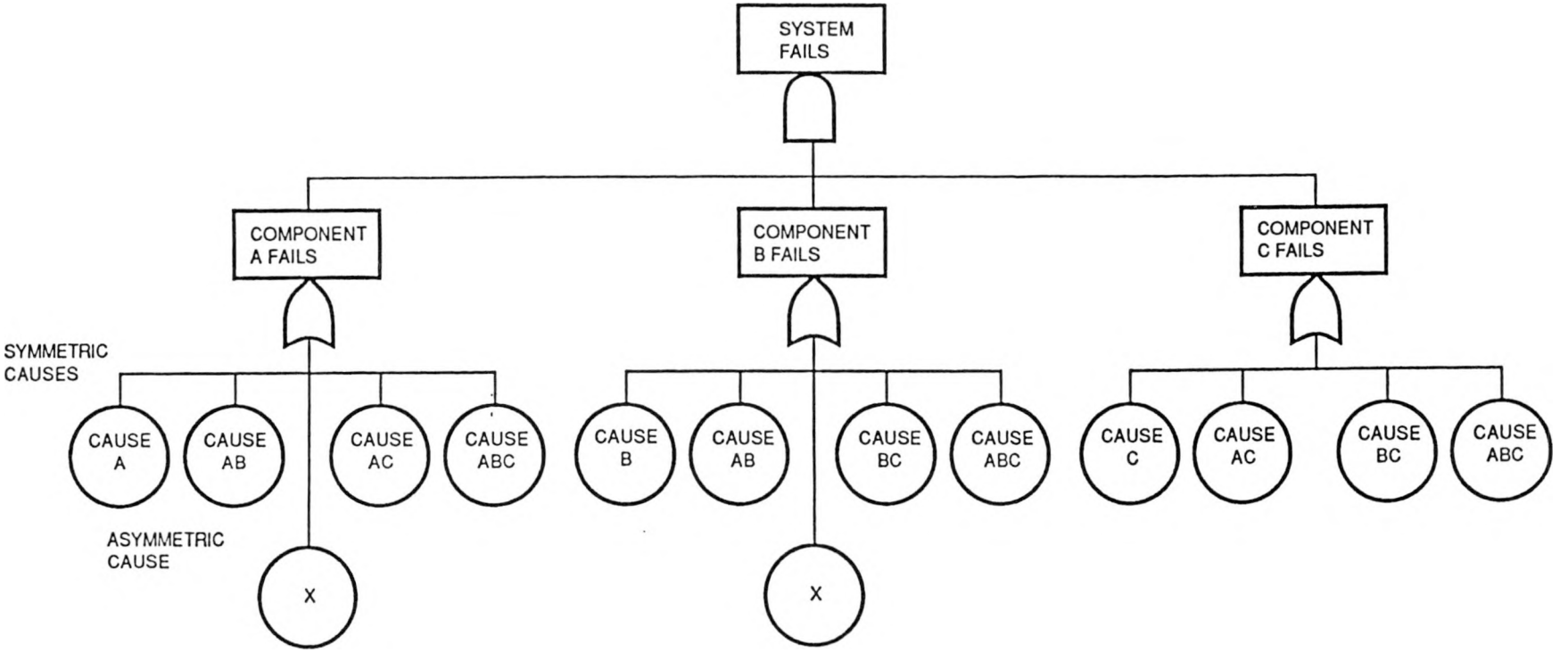


Figure F-1. Fault Tree of Common Cause Events Acting on ts Symmetrically and Nonsymmetrically

development of a generalized asymmetric model. Such a model would include common cause events, linking any and all combinations of components that may be difficult to enumerate, not to mention impractical to quantify.

Yet another example results in modeling the common cause failure of the safety relief valves in a BWR. There are many of these valves (typically on the order of 14 or so) and a large number have to fail to propagate an accident. Because of the lack of data on high multiplicity groups of components and the natural tendency to be conservative in this situation, the data analysis approach discussed at length in Section 3 would result in the higher order parameters in the MGL or alpha model being essentially unity, and the global common cause term clearly dominates. This will lead to unrealistically high common cause failure probabilities. One of the authors has used an approach based on asymmetry to argue, subjectively, for lower failure probabilities. The asymmetry was that which resulted from the maintenance policy of the plant where one-third of the valves were stripped down and rebuilt every refueling outage. This results, therefore, in an asymmetry of the valves with respect to the state of degradation as a result of the environment in which they are located. Therefore, for those causes that result in degradation, the valves are divided into three separate common groups with a less than complete coupling. Since it was judged from looking at failure event data that the failure modes of such valves were dominated by causes that can be attributed to gradual deterioration, a lower common cause failure probability than would otherwise be assigned was judged to be acceptable. This type of asymmetry is, therefore, dealt with in a different way, by its incorporation in the estimation of a common cause probability, rather than being represented explicitly in the model.

F.4 ITERATION AS AN INTEGRAL PART OF THE PROCEDURE

One of the features of the procedure discussed in this report, but perhaps not stressed enough, is that its application is necessarily iterative. The first iteration is clear; the procedure calls for a quantitative screening, which uses a conservative treatment to identify the important common cause failure terms. As common cause failure events are analyzed in more detail and as refinements to the system analysis, such as addition of recovery actions, are incorporated, the relative importance of the various terms changes and a further iteration is required. Of course, the second time around the model is already set up for screening. After the first screening, those common cause terms not requiring reevaluation should not be deleted from the model. The results of the screening merely imply that, at that stage in the analysis, it does not appear that reevaluation would be beneficial to producing a more realistic result. However, as stated above, as the analysis becomes more refined, these same terms may, in their turn, become important.

F.5 REFERENCES

F-1. Rasmuson, D. M., et al., "Use of COMCAN III in System Design and Reliability Analysis," EG&G Idaho, Inc., EGG-2187, October 1982.

F-2. Fleming, K. N., J. K. Liming, T. J. Mikschl, and A. Mosleh, "Common Cause Failure Reliability Benchmark Exercise, United States Team Contribution," prepared for Electric Power Research Institute, PLG-0426, July 1985.

APPENDIX G

RECOVERY CONSIDERATIONS IN A CCF ANALYSIS

Several factors involved in the analysis of accident sequences will affect the contribution of CCFs to the accident sequence frequency. Some of these factors tend to affect different CCF contributors in different ways. A particularly important example is that of the incorporation of recovery actions. Reference G-1 provides specific guidance on performing a recovery analysis. Two examples are given below showing how recovery considerations affect the relative contribution of CCF scenarios to accident sequence frequencies. Because of this, recovery considerations (even if only of a preliminary nature) can play an important role in the quantitative screening step (Section 3.2.2) since the purpose of this step is to focus on dominant CCF scenarios as early in the analysis as possible.

As can be seen in the examples that follow, recovery considerations depend on the specific accident sequence minimal cutsets. Thus, recovery considerations cannot be incorporated at the system level but must be addressed in connection with the accident sequence analysis.

Example 1: Station Blackout Scenarios. This example consists of accident scenarios initiated by a loss of offsite power at a BWR plant (see, for example, Reference G-2). Two CCF events that, if either existed following LOSP would, without recovery, result in a core damage, are (1) CCF of the emergency diesel generator and (2) CCF of the station batteries.

Consider Case 1 first without regarding possible recovery actions. Loss of the EDGs results in a station blackout (loss of all AC power). The station batteries provide DC power to the HPCI and RCIC systems. In the plant being analyzed, it is supposed that these systems maintain adequate core cooling (barring no additional failures) for about 6 hours. After this time, the batteries deplete and so become unable to supply enough power to HPCI and RCIC to keep the systems operable. Once these systems become functionally unavailable, it is supposed that core damage occurs within 3 hours.

Recovery from this "long-term" (9-hour) scenario is modeled by either restoration of one of the EDGs or by recovery of offsite power. Either recovery action would avoid core damage (barring any additional failures) if accomplished in time. The overall recovery potential for this scenario is high mainly because offsite power is likely to be recovered in time to avoid core damage. Data on recovery of offsite power or an EDG at U.S. nuclear power plant sites indicate that the probability of recovery is about 0.98 (Reference G-2). By far the most likely recovery action is that of offsite power.

For Case 2, loss of the station batteries is assumed to result in failure to start and load the EDGs and, therefore, loss of all AC and DC power. Core damage will occur, unless AC or DC power is recovered, in about 30 to 40 minutes. The recovery of the station batteries is difficult in such a short period of time, and the recovery of AC power is severely affected by the DC power loss. (Plant instrumentation is also significantly degraded under these circumstances.) Thus, the probability of recovering AC or DC power in this "short-term" blackout scenario is small and assumed to have no impact on scenario frequency.

Table G-1 shows the frequencies of these long-term and short-term blackout scenarios with and without recovery considerations taken directly from Reference G-2. The core damage scenario involving a CCF of the EDGs is, without recovery, about four times more likely to occur than the scenario involving a CCF of the station batteries. However, the EDG core damage scenario becomes about 11 times less likely to cause core damage than the station battery scenario when recovery is considered. Since these two CCF scenarios are the dominant contributors to the emergency power supply system unavailability, the results presented in Table G-1 also represent the impact of recovery considerations on system unavailability.

Since recovery considerations can substantially affect the relative importance of CCF contributors to system unavailability (in this case, a support system-emergency power supply unavailability), they should be incorporated into the quantitative screening step. If this is not possible, the results should be revisited when recovery terms have been included at a later stage in the analysis.

Example 2: Loss of Service Water Scenario. Figure G-1 shows a simplified schematic of a hypothetical SWS at a PWR power plant.* The system continuously operates with both pumps running and supplying the normal plant loads through normally open MOVs MOV-1A and MOV-2A. The system automatically realigns to the emergency configuration on an engineered safeguards actuation system signal expand by closing MOV-1A and MOV-2A and opening the normally closed motor-operated valves MOV-1B and MOV-2B. The MOVs in the crossover line are normally closed, and the manual valves in the pump discharge lines are locked open during power operations.

Only one CCF event is addressed in this example: a CCF of MOV-1B and MOV-2B to open on demand. However, two types of initiating events will be considered to illustrate how recovery considerations concerning the same CCF event differ for different sequences. The two types of initiators considered are (1) LOSP or another transient involving LOSP and (2) transients with loss of main feedwater. (In this second case, the EDGs are not required.)

To further define accident scenarios, assume that, for both initiating events, in addition to losing main feedwater, auxiliary feedwater has failed leading to the requirement for the use of the high pressure safety injection system in the feed and bleed mode to extract decay heat from the reactor.

*Although this SWS is hypothetical, the information and data presented in this example are fairly typical of U.S. nuclear power plants.

Table G-1

IMPACT OF RECOVERY CONSIDERATIONS ON SELECTED BLACKOUT SCENARIOS

Core Damage Scenario	Frequency ($year^{-1}$)		Factor of Reduction on Scenario Frequency when Recovery Is Considered
	Without Recovery	With Recovery	
LOSP followed by CCF of EDGs.	1.65-5*	3.3-7	50
LOSP followed by CCF of station batteries.	3.7-6	3.7-6	1

*All frequency values in this table were taken from Reference G-2.

NOTE: Exponential notation is indicated in abbreviated form; i.e., 1.65-5 = 1.65×10^{-5}.

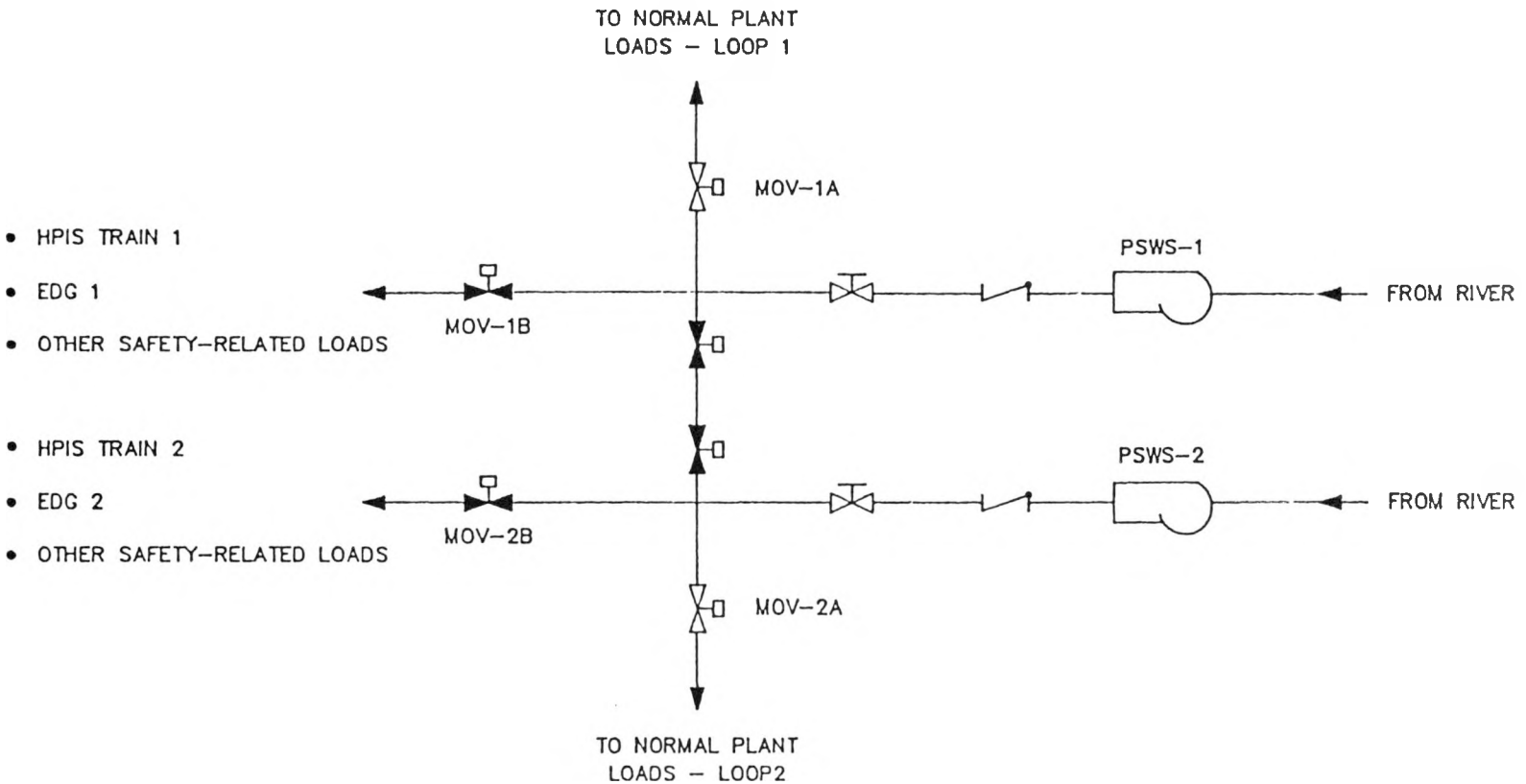


Figure G-1. Simplified Schematic of a Service Water System

The CCF of MOV-1B and MOV-2B results in loss of service water to all safety-related loads. With the loss of offsite power as an initiating event, the load of most importance initially is the emergency diesel generators and for other transients it is the cooling to the HPIS pumps.

The HPIS pumps at the plant can operate for a little more than 1 hour without lube oil cooling. Thus, whenever the initiating event does not involve LOSP, the safety-related system failures due to the CCF of interest can be avoided if the service water supply is restored within 1 hour. The probability that the operators would restore the service water supply within 1 hour is assumed to be 0.96 (see discussion later).

The EDGs however will fail within a few minutes following loss of SWS cooling. Thus, whenever the initiating event involves LOSP, the EDGs will be lost (realistically assuming a negligible probability of restoring SWS cooling to the EDGs within a few minutes), and the only recovery action that can be taken to avoid core damage is to restore offsite power within about 30 minutes, the time assumed to be available to restore HPIS flow without irreversible core damage. Data on recovery of offsite power at U.S. nuclear power plant sites indicates that the appropriate probability of recovery is about 0.6 (Reference G-2).

Table G-2 shows the impact of recovery considerations in both of the scenarios analyzed in this example. Recovery decreases the estimated frequencies of SWS failure scenarios (frequency estimates are not shown in Table G-2) by a factor of about 2.5., if LOSP is involved, and by a factor of about 25, if LOSP is not involved.

In this second example, the recovery action of interest was associated with the basic event representing the common cause failure itself and as such is part of the detailed analysis that would be performed. This is to be contrasted with the first example where the recovery action was largely associated with another event, the recovery of the offsite power source. What this second example shows is that the credit for recovery is dependent on the sequence as that determines the amount of time available. For this example, the probability of accomplishing this recovery action was obtained by (1) identifying all failure modes for the equipment of interest (e.g., valve motor-operator fails, valve plugs, circuit breaker fails, circuit breaker control circuit fails, etc.), (2) evaluating the probability of recovery for each failure mode [e.g., plugging of a valve is unrecoverable within 1 hour, motor-operator failure is moderately recoverable (requires local operation of the valve), and circuit breaker control circuit failure is more easily recoverable (requires pushing a button in the control room)], and (3) determining an appropriate average probability of recovery, weighted by the contribution of each failure mode to the CCF event probability. Reference G-1 provides specific guidance on evaluating recovery probabilities, and References G-2 through G-4 provide several additional examples of these evaluations.

The option remains open to the analyst: to apply these recovery factors in screening the data, so that only events that could not be recovered in the allowable time are retained for parameter estimation purposes, or to have a general common cause parameter and explicitly apply a recovery factor. The amount of work is the same; it is only a matter of preference in displaying the results.

REFERENCES

G-1. Carlson, D. D., et al., "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728, SAND82-1100, prepared for U.S. Nuclear Regulatory Commission by Sandia National Laboratories, January 1983.

Table G-2

IMPACT OF RECOVERY CONSIDERATIONS ON SELECTED SWS SCENARIOS

Type of Initiating Event	Probability of CCF of MOV-1B and MOV-2B To Open on Demand*		Factor of Reduction on CCF Probability when Recovery Is Considered
	Without Recovery	With Recovery	
Not Involving LOSP	~ 7-4	~ 3-5	~ 25
Involving LOSP	~ 7-4	~ 3-4	~ 2.5

*The probability of CCF without recovery considerations was obtained by multiplying the probability of an independent MOV failure to open on demand (Reference G-1) by a generic beta factor for MOVs (Reference G-5).

NOTE: Exponential notation is indicated in abbreviated form; i.e., 7-4 = 7 x 10^{-4}.

G-2. Kolaczkowski, A. M., F. T. Harper, A. L. Camp, et al., "Analysis of Core Damage Frequency from Internal Events: Peach Bottom, Unit 2," NUREG/CR-4550/4 of 10, SAND86-2084, prepared for U.S. Nuclear Regulatory Commission by Sandia National Laboratories, September 1986.

G-3. JBF Associates, Inc., "Plant Risk Status Information Management System (PRISIM) Version 2.0 User's Guide," JBFA-108-86, prepared for U.S. Nuclear Regulatory Commission, October 1986.

G-4. Kolb, G. J., et al., "Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant," NUREG/CR2787, SAND82-0978, prepared for U.S. Nuclear Regulatory Commission by Sandia National Laboratories, June 1982.

G-5. Fleming, K. N., A. Mosleh, et al., "Classification and Analysis of Reactor Operating Experience Involving Dependent Events, "EPRI-NP-3967, prepared for Electric Power Research Institute by Pickard, Lowe and Garrick, Inc., June 1986.

APPENDIX H

REFERENCES FOR BETA FACTOR ESTIMATES

This appendix was originally intended to be a compilation of generic beta factors that have been derived worldwide from nuclear, chemical, aircraft, and other industries.

The motivation was that the β-factor model has been the most widely used quantitative CCF model and that "generic" values might be useful, either as screening values or to provide a benchmark against which screening values could be judged. Although several extensions of the β-factor model (e.g., the basic parameter, the MGL, and the shock models described in Volume I and Appendices C and E) have been developed and are in current use in risk and reliability analyses, the β-factor model is still likely to play an important role in future studies; e.g., the quantitative screening step proposed in Volume I recommends using the β-factor model for obtaining preliminary estimates.

However, one of the problems with using generic beta factors is the difficulty of determining the criteria used for screening data (if any) and the component and failure mode definitions. As has been stressed throughout this report these have a direct influence on the estimates. It was decided therefore simply to supply a list of references (References H-1 through H-19) in which beta factor estimates can be found. Before using a particular estimate, the analyst should make every effort to determine compatibility with his model, and even then they should only be used as screening values or as a benchmark.

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

REFERENCES

H-1. Fleming, K. N., "A Reliability Model for Common Mode Failures in Redundant Safety Systems," General Atomic Corporation, GA-A13284, December 1974.

H-2. Montague, D. F., and H. M. Paula, "A Survey of Beta-Factor and C-Factor Application," JBF Associates, Inc., JBFA-LR-104-84, September 1984.

H-3. Edwards, G. T., and I. A. Watson, "A Study of Common Mode Failures," U.K. Atomic Energy Authority, Safety and Reliability Directorate, SRD R146, July 1979.

H-4. Edwards, G. T., and I. A. Watson, "Common Mode Failures in Redundancy Systems," Nuclear Technology, Vol. 46, December 1979.

H-5. U.S. Nuclear Regulatory Commission, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants," NUREG/CR-2300, April 1982.

H-6. Wright, R. I., "Some Data on Common Cause Failures in Redundancy Industrial Computer Systems," Systems Reliability Service, European Workshop on Industrial Computer Systems.

H-7. Table 3-7, Volume I.

H-8. Apostalakis, G., and P. Moieni, "A Model for Common Cause Failures," ANS Transactions, Vol. 45, Winter Meeting, October 30-November 3, 1983.

H-9. Fleming, K. N., et al., "HTGR Accident Initiation and Progress Analysis Status Report: Phase II Risk Assessment," General Atomic Corporation, GA-A15000, April 1978.

H-10. Fleming, K. N., and P. H. Raabe, "A Comparison of Three Methods for the Quantitative Analysis of Common Cause Failures," General Atomic Corporation, GA-A14568, May 1978.

H-11. Fleming, K. N., et al., "HTGR Accident Initiation and Progress Analysis Status Report - Volume II," General Atomic Corporation, GA-A13617, October 1975.

H-12. Fleming, K. N., et al., "On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation," Nuclear Safety, Vol. 24, No. 5, September-October 1983.

H-13. Lydell, B., "Dependent Failure Analysis in System Reliability: A Literature Survey," Chalmers University of Technology, Sweden, RE05-79, March 1979.

H-14. Baranowsky, P. W., et al., "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, NUREG-0666, April 1981.

H-15. Fleming, K. N., et al., "Event Classification and Systems Modeling of Common Cause Failures," ANS 1984 Annual Meeting, New Orleans, Louisiana, June 3-7, 1984.

H-16. Atwood, C. L., "Common Cause Fault Rates for Pumps: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, January 1, 1972 through September 30, 1980," prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., NUREG/CR-2098 (EGG-EA-5289), February 1983.

H-17. Melvin, J. G., and R. B. Maxwell, "Reliability and Maintainability Manual," Chalk River Nuclear Laboratories, prepared for U.S. Atomic Energy Commission, AECL-4607, January 1979.

H-18. Steverson, J. A., and C. L. Atwood, "Common Cause Fault Rates for Valves: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1980," prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-2770, EGG-EA-5485, February 1983.

H-19. Meachum, T. R., and C. L. Atwood, "Common Cause Fault Rates for Instrumentation and Control Assemblies: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1981," prepared for U.S. Nuclear Regulatory Commission, NUREG/CR-3289, EGG-2258, May 1983.

NRC FORM 335 (11-81) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-4780, Vol. 2
EPRI NP-5613
PLG-0547

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
Procedures for Treating Common Cause Failures in Safety and Reliability Studies
Analytical Background and Techniques

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
A. Mosleh, K. Fleming, G. Parry, H. Paula, D. Worledge, and D. Rasmuson

5. DATE REPORT COMPLETED
MONTH: October YEAR: 1988

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Pickard, Lowe, and Garrick, Inc.
2260 University Drive
Newport Beach, California 92660

DATE REPORT ISSUED
MONTH: January YEAR: 1989

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory
Washington, D.C. 20555

Electric Power
Research Institute
3412 Hillview Ave.
Palo Alto, CA 94303

10. PROJECT/TASK/WORK UNIT NO.

11. FIN NO.
FIN A1384

13. TYPE OF REPORT

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)* This report presents a framework for the inclusion of the impact of common cause failures in risk and reliability evaluations. Common cause failures are defined as that subset of dependent failures for which causes are not explicitly included in the logic model as basic events. The emphasis here is on providing procedures for a practical, systematic approach that can be used to perform and clearly document the analysis.

The framework comprises four major stages: (1) system logic model development, (2) identification of common cause component groups, (3) common cause modeling and data analysis, and (4) system quantification and interpretation of results.

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

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

Dependent Failures
Common Cause Failures
Common Mode Failures

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*
Unclassified

22. PRICE
S