NUREG/CR-6268
Vol. 2
INEEL/EXT-97-00696

Common-Cause Failure Database and Analysis System: Event Definition and Classification

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

Idaho National Engineering and Environmental Laboratory

University of Maryland

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

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

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555-0001

2. The Superintendent of Documents, U.S. Government Printing Office, P. O. Box 37082, Washington, DC 20402-9328

3. The National Technical Information Service, Springfield, VA 22161-0002

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

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

The following documents in the NUREG series are available for purchase from the Government Printing Office: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grantee reports, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

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

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

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

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852-2738, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018-3308.

NUREG/CR-6268
Vol. 2
INEEL/EXT-97-00696

Common-Cause Failure Database and Analysis System: Event Definition and Classification

Manuscript Completed: June 1998
Date Published: June 1998

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

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

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

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

ABSTRACT

This volume of the Common Cause Failure Database and Analysis System report provides the definition and classification method used for identifying, coding, and quantifying common cause failure (CCF) probabilistic risk assessment (PRA) parameter estimates on the data that are stored in the CCF database.

Equipment failures that contribute to CCF events at commercial nuclear power plants in the U.S. will be identified during a search and review of Licensee Event Report (LER) and Nuclear Plant Reliability Data System (NPRDS) failure reports in accordance with the criteria specified in this document. The equipment failures that contribute to a CCF event are identified and coded for entry into a personal computer storage system using the method presented in this volume. The events stored in the system are used to perform CCF PRA parameter estimations using CCF quantification methods (also described in this volume).

The database resulting from coding CCF events is used to estimate CCF failure parameters for use in various CCF models used in PRAs.

CONTENTS

ABSTRACT ... iii

EXECUTIVE SUMMARY ... vii

ACRONYMS ... ix

1. INTRODUCTION ... 1

2. DEFINITION OF COMMON CAUSE FAILURES ... 3

   2.1 Intrinsic Dependency ... 3

   2.2 Extrinsic Dependency ... 4

3. CCF EVENT CLASSIFICATION ... 7

   3.1 Component States ... 7

   3.2 Failure Causes ... 7

      3.2.1 Proximate Cause ... 7
      3.2.2 Root Cause ... 8

   3.3 Coupling Factors ... 10

      3.3.1 Hardware Based ... 10
      3.3.2 Operational Based ... 12
      3.3.3 Environmental Based ... 13

   3.4 Defense Mechanisms ... 15

4. QUANTITATIVE ANALYSIS OF COMMON CAUSE FAILURE EVENTS ... 17

   4.1 Event Impact Vector ... 17

   4.2 Generic Impact Vector Assessment ... 19

      4.2.1 Case 1: Events Involving Degraded Component States ... 19
      4.2.2 Case 2: Events Involving Failures Distributed in Time ... 20
      4.2.3 Case 3: Events Involving Uncertainty about Shared Cause ... 23
      4.2.4 Cases Involving Degraded States, Time Delay, and Uncertain Shared Cause ... 23

   4.3 Specializing Impact Vectors for Plant Specific Analyses ... 24
      4.3.1 Adjustment Based on Qualitative Differences ... 24
      4.3.2 Adjustment for Quantitative Difference ... 26

4.4 Estimation of CCF Event Frequencies from Impact Vectors 27

4.5 Treatment of Uncertainties 27

5. INFORMATION NEEDED FOR COMMON CAUSE DATA CLASSIFICATION AND ANALYSIS 33

5.1 Event Description 33

5.2 Event Analysis 33

5.3 Application-Specific Analysis 34

6. REFERENCES 35

GLOSSARY 37

Appendix A—Overview of Impact Vector Mapping A-1

Appendix B—Commonly Used CCF Parametric Models B-1

FIGURES

1. Coding system for component states 8

2. Example of the assessment of impact vectors involving multiple interpretation of event 18

3. Schematic representation of the role of shared cause factor and root cause strength information of different classes of events 25

4. Example of changes in CCF uncertainty percentiles with changes in alpha factor uncertainty 31

TABLES

1. Failure cause codes 9

2. Coding system for shared cause factors 14

3. Defense mechanisms 16

4. Impact vector assessment for various degrees of component degradations 21

5. Suggested values for r_1 and r_2 25

EXECUTIVE SUMMARY

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

A CCF event consists of component failures that meet four criteria: (1) two or more individual components fail or are degraded, including failures during demand, in-service testing, or from deficiencies that would have resulted in a failure if a demand signal had been received; (2) components fail within a selected period of time, such that success of the PRA mission would be uncertain; (3) component failures result from a single shared cause and coupling mechanism; and (4) a component failure is not due to the failure of equipment outside the established component boundary.

Two data sources are used to select equipment failure reports to be reviewed for CCF event identification: the Nuclear Plant Reliability Data System (NPRDS), which contains component failure information, and the Sequence Coding and Search System (SCSS), which contains Licensee Event Reports (LERs). These sources served as the developmental basis for the CCF data collection and analysis system. The CCF data collection and analysis system consists of (1) CCF event identification methodology, (2) event coding guidance, and (3) a software system to estimate CCF parameters.

The CCF event identification process includes reviewing failure data to identify CCF events and counting independent failure events. The process allows the analyst to consistently screen failures and identify CCF events. The CCF event coding process provides guidance for the analyst to consistently code CCF events. Sufficient information is recorded to ensure accuracy and consistency. Additionally, the CCF events are stored in a format that allows PRA analysts to review the events and develop an understanding of how they occurred.

A software system stores CCF events, independent failure counts, and automates PRA parameter estimations. The system employs two quantification models: alpha factor and multiple Greek letter. These models are used throughout the nuclear industry. In addition, these parameter estimations can be utilized in a PRA to estimate basic event probability and uncertainty.

ACRONYMS

AEOD	Nuclear Regulatory Commission's (NRC's) Office for the Analysis and Evaluation of Operational Data
AFW	Auxiliary Feed Water
CCF	Common-Cause Failure
CCW	Component Cooling Water
CST	Condensate Storage Tank
ES	Engineering Safeguards
HPCI	High-Pressure Coolant Injection
HHSI	High-Head Safety Injection
INEEL	Idaho National Engineering and Environmental Laboratory
LHSI	Low-Head Safety Injection
MCC	Motor Control Center
MGL	Multiple Greek Letter
MLE	Maximum Likelihood Estimator
NRC	Nuclear Regulatory Commission
PM	Preventive Maintenance
PRA	Probabilistic Risk Assessment
RCIC	Reactor Core Isolation Cooling
RHR	Residual Heat Removal
RWST	Refueling Water Storage Tank

Common Cause Failure Database and Analysis System Volume 2—Event Definition and Classification

1. INTRODUCTION

The Nuclear Regulatory Commission's (NRC's) Office for the Analysis and Evaluation of Operational Data (AEOD) asked the Idaho National Engineering and Environmental Laboratory (INEEL) to assist in developing a common cause failure (CCF) database for the U.S. commercial nuclear power industry, including a method for identifying CCF events and a computer system for storing and analyzing the data. For this effort, CCF events are defined as "a subset of dependent failures in which two or more component and or functional fault states exist at the same time, or within a short interval, as a result of a shared cause." The fault states must exist in the same operating power plant to be considered a CCF event. Similar failures within a short time interval in different power plants of multiple power plant sites do not constitute a CCF event.

The INEEL staff developed a method for identifying CCF events and a personal computer (PC)-based system for storing and analyzing the data. This volume defines a CCF event, provides a method for classifying and analyzing a CCF event, describes the parameter estimation models, and describes the information necessary to reproduce the logic used to identify and analyze each CCF event.

2. DEFINITION OF COMMON CAUSE FAILURES

The definition of a CCF is closely tied to an understanding of the nature and significance of dependent events. Therefore, first a definition of a dependent event is provided. To simplify the presentation, consider two failure events, A and B.

Events A and B are said to be dependent if

$$P(A \cap B) = P(A)P(B|A)$$

$$= P(B)P(A|B) \neq P(A)P(B),$$

where P(X) is the probability of event X.

In the presence of dependencies, often, but not always, $P(A \cap B) > P(A)P(B)$. Therefore, if A and B represent failure of safety functions, the actual probability of both failures will be higher than the expected probability if that probability is calculated based on the assumption of independence. In cases where the systems provide multiple layers of defense against total system or functional failure, presence of dependence may translate into a reduced safety margin and over- estimation of the reliability level.

Dependencies that result in dependent failures can be classified in many ways. A classification useful in relating operational data to reliability characteristics of systems is offered below. In this classification, dependencies are first categorized based on whether they stem from intended intrinsic functional and physical characteristics of the system or are due to external factors and unintended characteristics. Therefore, the dependence is either intrinsic or extrinsic to the system.

2.1 Intrinsic Dependency

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

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

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

  Functional requirement dependency also includes cases where component B is required to perform its function in excess of its design because of the failure of A.

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

- **Cascade Failure.** A cascade failure refers to the cases where failure of A leads to failure of B, a cascading effect within a design.

An example is a valve on a pump suction line that fails to open, and this failure causes the pump to fail when a start signal is generated because of flashing in the suction line from a lack of flow. Since the pump may be physically damaged, even if the valve is made operable, the pump would remain inoperable.

Through the above dependencies, other types of intrinsic dependencies are created. A **Shared Equipment Dependency**, or when several components are functionally dependent on the same component, is one such type. An example of Shared Equipment Dependency is if both B and C are functionally dependent on A operating, then B and C have a shared equipment dependency.

Known intrinsic dependencies should be, and often are, modeled explicitly in the logic model (e.g., fault tree) of the system.

2.2 Extrinsic Dependency

Extrinsic dependency refers to cases where the dependency or coupling is not inherent or intended in the functional characteristics of the system. The source and mechanism of such dependencies are often external to the system. Examples of extrinsic dependencies are:

- **Physical/Environmental.** Physical/ environmental dependency is caused by common environmental factors. Environmental factors include harsh or abnormal environments created by a component. For example, high vibration induced by A causes B to fail.

- **Human Interaction.** Human Interaction dependency is caused by man-machine interaction (e.g., multiple component failure due to the same maintenance error).

In nuclear power plant risk and reliability studies, a large number of extrinsic dependencies are treated through modeling of the phenomenology and the physical processes involved. Examples are fire and earthquake events which are physical/environment dependencies. Nevertheless, there are a large number of extrinsic mechanisms which are unpredictable (or misunderstood) and cannot be modeled. In many cases, even when the mechanisms are well-understood, it is not cost-effective to model the effects explicitly. In these cases, the combined probabilistic effect of dependencies is treated parametrically. This means that these types of events are treated together as one group known as **common-cause failure events**.

Viewed in this fashion, CCF events are inseparable from the class of dependent failures. The distinction is based on the level of treatment and choice of modeling approach in reliability analysis.

In the past 20 years, several definitions of **common-cause failures** have been suggested in literature. Some definitions are broad and essentially cover the entire set of dependent failures. Other definitions focus on dependent events in the context of a particular application, such as probabilistic risk assessment (PRA). Reference 1, NUREG/CR-4780, defines CCFs as a subset of dependent failures in which two or more component fault states exist at the same time, or within a short interval, as a result of a shared cause. Consistent with current practices in reliability analysis systems modeling, Reference 1 excludes failure or unavailability of other components as a shared cause of a CCF event. In particular, this is true where the failure of one component cascades down to the components being analyzed. This exclusion is based on the premise that functional dependencies are modeled explicitly in the logic models.

According to Reference 1, CCFs result from the coexistence of two main factors: (1) a susceptibility for components to fail or become unavailable because of a particular **root cause**, and (2) a **coupling factor** or mechanism that creates the condition for multiple components to be affected by the same cause. An example is two pressure relief valves that failed to open because the set-points were set too high. The set-point oversight was human error.

Overall, each component failed because of its susceptibility to the conditions created by the root cause and the role of coupling factors that created the conditions common to several components. Defenses against root causes improve the reliability of each component, but do not necessarily reduce the fraction of total failures that occur due to a common cause. The susceptibility of a system of components to dependent failures compared with independent failures is determined by coupling factors.

Characterization of CCF events, in terms of these main factors, enables effective engineering assessment of the CCF phenomenon. Characterization identifies plant vulnerabilities to CCFs and establishes a basis for the defenses against them. It is equally effective in the evaluation and classification of operational data and quantitative analysis of CCF frequencies.

The NUREG/CR-4780 definition of CCFs—in terms of root cause, coupling factor, and the timing of failures—expresses (explicitly or implicitly) the main features of CCFs for most applications. The concept of a shared cause of malfunction or change in component state is the key aspect of a CCF event. The use of the word "shared" implicitly includes the concept of coupling factor or mechanism. Also the reference to a time interval between failures acknowledges the reliability significance of these events. For some applications, however, the time characteristic may not be a critical discriminator. Multiple component failures due to a shared cause, but without affecting mission requirements, in a period of time required for performance, are of little or no significance from a reliability point of view. It is the correlation of failure times and their simultaneity in reference to the specified mission time that carries their reliability significance. Often when the same cause is acting on multiple components, failure times are also closely correlated. It should be mentioned that the term "common-mode failure" which was used in the early literature and is still used by some practitioners is more indicative of the most common symptom of common cause failure, i.e., failure of multiple components. As such, it is not a precise term for communicating the main character of CCF events.

3. CCF EVENT CLASSIFICATION

A classification system for the main elements of CCF events (specifically the component fault state, the cause, and coupling factor) is provided in the following sections. These sections include definitions and a coding system for component states, causes, and coupling factors.

3.1 Component States

In representing CCFs, an important aspect is the impact of the event on the state of components that failed; where a state is defined as the status of a component with respect to the function it is intended to provide. Various states of a component, as classified in Reference 2, EPRI NP-3967, are given in Figure 1. According to this classification, with regard to the intended function and in reference to a given performance criterion, a component could have two states: available or unavailable. The unavailable state includes two distinct substates: "failed" and "functionally unavailable," depending on whether the cause of the unavailability is damage to the component or lack of necessary support such as motive power. The state classification also recognizes that even though a component may be capable of performing its function, i.e., available, an incipient or degraded condition could exist in that component, or in a supporting component. These failure situations are termed "potentially failed" and "potentially functionally unavailable," respectively. These concepts have proven useful in CCF data analysis.

3.2 Failure Causes

In the context of the present discussion, the cause of a failure event is a condition or combination of conditions to which a change in the state of a component can be attributed. It is recognized that the description of a failure in terms of a single "cause: is often too simplistic. For example, for some purposes it may be adequate to identify that a pump failed because of high humidity. But to develop a complete understanding of the potential for multiple failures, it is necessary to identify why the humidity was high and why it affected the pump, i.e., it is necessary to identify the ultimate reason for the failure. There are many different paths by which the ultimate reason for failure could be reached. The sequence of events that constitute a failure path, or failure mechanism, is not necessarily simple. As an aid to considering failure mechanisms, Reference 3, NUREG/CR-5460, introduces the following concepts.

3.2.1 Proximate Cause

A proximate cause associated with a component failure event is a characterization of the condition that is identifiable as having led to the failure. In the pump example above, humidity could be identified as the proximate cause. The proximate cause can be regarded as a symptom of the failure cause, and does not provide a complete understanding of what led to that failed condition. As such, the proximate cause may not be the most useful characterization of failure events for the purposes of identifying appropriate corrective actions.

To expand the description of the causal chain of conditions resulting in a failure, it is useful to introduce the concepts of **conditioning events** and **trigger events**. These concepts are introduced to aid in a systematic review of event data and are useful in analyzing component failures. However, for a single event it is not always necessary to consider both concepts.

A **conditioning event** is an event which predisposes a component to fail, or increases its susceptibility to fail. A conditioning event does not cause a failure. In the pump example, the conditioning event could have been the failure of maintenance personnel to properly seal the pump

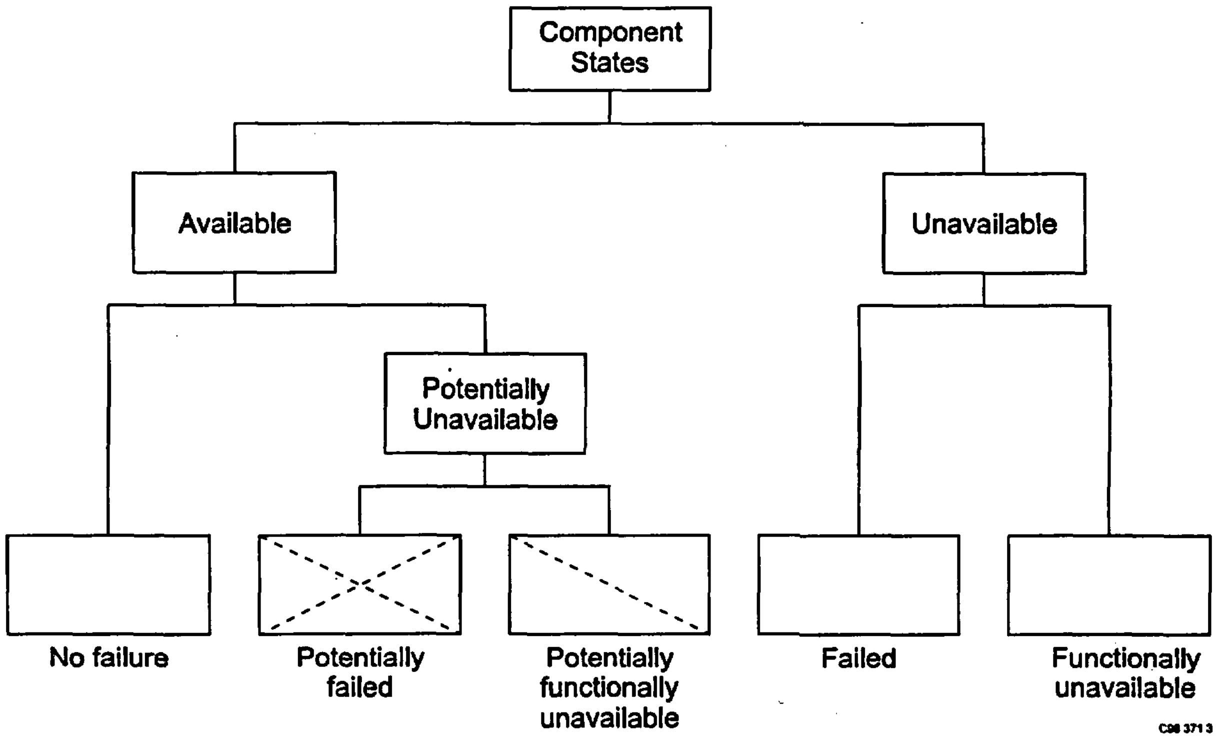

Figure 1. Coding system for component states (Reference 2).

control cabinet following maintenance. The effect of the conditioning event is latent, but contributes to the failure mechanism.

A **trigger event** activates a failure or initiates the transition to the failed state. The trigger event is important whether the failure is revealed at the time the trigger event occurs or not. The event which led to high humidity in a room (and subsequent equipment failure) would be a trigger event. A trigger event is therefore a dynamic feature of the failure mechanism. A trigger event, particularly in the case of CCF events, is usually an event which is external relative to the components in question.

It is not always necessary or possible to define conditioning and trigger events for a failure. However, the concepts are useful in that they focus on immediate and subsidiary causes which function to increase susceptibility to failure, given the appropriate ensuing conditions.

3.2.2 Root Cause

Root cause is the basic reason why components fail. Correction of a root cause can prevent recurrence. The identification of root cause, therefore, can be tied to the implementation of defenses.

It should be noted that many proximate causes (moisture and vibration) are symptoms of the root cause, and that proximate causes do not provide an understanding of what led to a failure condition. Often, failure investigations do not determine the root causes of failures, even though this determination is crucial for judging defense adequacy.

Reference 2 provides a classification of possible causes of component unavailability. A modified version of this classification is presented in Table 1. The causes are grouped into eight categories which are then subdivided to provide a means of recording more detailed information when available. This classification can be used for either the root or proximate cause.

The major categories which can lead to a CCF include:

- **State of Other Component.** The cause of the state of the component under consideration is due to the state of another component. Examples are loss of power and loss of cooling.

Table 1. Failure cause codes.

State of a Component

(QP) State of Other Component

Design, Manufacture, and Construction Inadequacy

(DE) Designing Error or Inadequacy

(DC) Construction/Installation Error or Inadequacy

(DM) Manufacturing Error or Inadequacy

Abnormal Environmental Stress

(IE) Ambient Environmental Stress

Human Actions, Plant Staff

(HA) Accidental Action

(HD) Wrong Procedure Followed

(HP) Failure to Follow Procedure

(HT) Inadequate Training

Internal (Internal to component, piece-part)

(IC) Internal to Component, Piece-Part

Other

(OT) Other

(QI) Set Point Drift

Procedures Inadequacy

(PA) Inadequate Procedures

Unknown

(U) Unknown

C96 3714

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

- **Abnormal Environmental Stress.** Represents causes related to a harsh environment that is not within component design specifications. Specific mechanisms include chemical reactions, electromagnetic interference, fire/ smoke, impact loads, moisture (sprays, floods, etc.), radiation, abnormally high or low temperature, vibration load, and acts of nature.

- **Human Actions, Plant Staff Error.** Represents causes related to errors of omission and commission on the part of plant staff. An example is a failure to follow the correct procedure. This category includes accidental actions, and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing.

- **Internal.** Deals with malfunctioning of something internal to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the ambient environment on a component. Specific mechanisms include erosion/ corrosion, internal contamination, fatigue, and wearout/ end of life.

- **Other.** This category includes specific and general categories not covered by the other categories in this classification scheme. A specific category that is frequently used is setpoint drift. The general category is "Other" which is considered to be the cause of events for which the cause of the failures is known if, and only if, the cause does not fit one of the other categories in this classification scheme.

- **Procedure Inadequacy.** Refers to ambiguity, incompleteness, or error in procedures for operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test, and calibration procedures.

- **Unknown.** This cause category is used when the cause of the component state cannot be identified.

3.3 Coupling Factors

As described earlier, for failures to originate from the same cause and thus be classified as a CCF, the conditions for the trigger or conditioning events have to affect multiple components simultaneously. Simultaneity, in this context, refers to failures that occur close enough in time to lead to the inability of multiple components to perform their intended safety function. The condition or mechanism through which failures of multiple components are coupled is termed the coupling factor. The coupling factor is a characteristic of a group of components or piece-parts that identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission, operational, maintenance, and test procedures.

Reference 4 presents a coupling factor classification system which is used as a systematic and consistent method for classifying coupling factors of multiple component unavailabilities. A modified version of this classification system is used in the analysis of operational data and in evaluating plant-specific defenses against multiple failures.

The coupling factor classification format consists of three major classes:

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

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

3.3.1 Hardware Based

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

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

The following are coupling factors in the hardware design category.

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

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

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

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

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

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

    - On two occasions, both the HPCI and RCIC pumps tripped during tests. The cause was failed teflon rupture discs. The discs were inadequate for their intended purpose.

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

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

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

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

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

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

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

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

3.3.2 Operational Based

The operational based coupling factors are coupling factors that propagate a failure mechanism on account of identical operational characteristics among several components. For example, failure of three redundant HHSI pumps to start as a result breakers for all three pumps were racked-out as a result of operator error. The categories of operation based coupling factors are:

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

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

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

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

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

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

Mispositioning the valves was due to operator error and an incomplete procedure.

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

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

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

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

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

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

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

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

3.3.3 Environmental Based

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

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

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

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

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

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

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

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

For ease of representation and to facilitate communication of events classified as CCFs, a coding system for coupling factors has been developed as shown in Table 2. The hierarchical

Table 2. Coding system for coupling factors.

- H Hardware
  - HDCP Hardware Design: Component Part
  - HDSC Hardware Designing: System Configuration
  - HQIC Hardware Quality: Installation/Configuration
  - HQMM Hardware Quality: Manufacturing
- O Operational
  - OMTC Operational: Maintenance/Test Schedule
  - OMTP Operational: Maintenance/Test Procedure
  - OMTS Operational: Maintenance/Test Staff
  - OOOP Operational: Operation Procedure
  - OOOS Operational: Operation Staff
- E Environmental
  - EE Environment: External
  - EI Environment: Internal (e.g., Fluid)

C98 3714

structure of the coding system is particularly useful in event classification since the level of detail in available information can vary from event to event. In some cases, it may be possible to identify the coupling factor of the event at a high level of hardware-based, operational-based, or environmental-based information. In other situations a more detailed classification may be possible based on the specific information provided in the event description. In either case, the flexibility has been provided in the coding system to represent the event as closely as possible.

3.4 Defense Mechanisms

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

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

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

A defense strategy against proximate causes typically includes design control, use of qualified equipment, testing and preventive maintenance programs, procedure review, personnel training, quality control, redundancy, diversity, and barriers. For coupling factors, a defense strategy typically includes: diversity (functional, equipment, and staff), barriers, and staggered testing and maintenance. The defense mechanisms for the CCF system are functional barrier, physical barrier, monitoring and awareness, maintenance staffing and scheduling, component identification, diversity, no practical defense, and unknown. These defenses are constructed primarily based on coupling factors. A summary of the defenses is provided in Table 3.

Table 3. Defense mechanisms.

Defense Mechanism	Description
Functional Barrier	A decoupling of a CCF event could have been accomplished if the equipment functional interconnections had been modified.
Physical Barrier	A physical restriction, barrier, or separation could have prevented a CCF.
Monitoring/Awareness	Increased monitoring, surveillance, or personnel training could have prevented a CCF.
Maintenance Staffing and Scheduling	A maintenance program modification could have prevented a CCF. Modification includes items such as staggered testing and maintenance/operation staff diversity.
Component Identification	If component identification had been modified by more clearly identifying equipment, a CCF event could have been prevented. Examples of modification are better equipment identification and color coding.
Diversity	The modification to diversity could have prevented a CCF. This includes diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.
No Practical Defense	No practical defense could be identified.
Unknown	Adequate detail is not provided on the cause and coupling factor for a CCF event to make an adequate defense mechanism identification.

4. QUANTITATIVE ANALYSIS OF COMMON CAUSE FAILURE EVENTS

On account of the rarity of common cause events and the limited experience base for individual plants, the quantity of data for CCF analysis and plant-specific assessment of their frequencies is statistically insignificant. To overcome this difficulty, Reference 1 proposes creating plant-specific data through screening and evaluating generic data for plant-specific characteristics. Two techniques were presented in Reference 1 to facilitate the estimation of plant-specific CCF frequencies from generic industry experience. One technique proposed using an "event impact vector" to classify generic events according to the level of impact of common cause events and the associated uncertainties in numerical terms. The second was impact vector specialization in which generic event impact vectors were modified to reflect the likelihood of the occurrence of the event in the plant of interest, and the degree of its potential impact. These techniques would be an assessment of the differences between the original plant and the plant being analyzed (target plant) for susceptibility to various CCF events. Each technique is briefly described.

4.1 Event Impact Vector

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

[1, 0, 0] No components failed.

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

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

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

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

$0.9\, I_1 + 0.1\, I_2 = [0, 0, 0.9, 0.1]$.

The average impact vector for a set of N hypotheses is obtained by:

$$\bar{I} = \sum_{i=1}^{N} w_i I_i \qquad (4\text{-}1)$$

Event Description: Main Yankee, August 1977. Plant at power. Two diesel generators failed to run due to plugged radiators. The third unit radiator was also plugged.

Failure Mode: Fail to Run

Common Cause Component Group Size: 3

Hypothesis	Probability	Elements of Impact Vector			
		F_1	F_2	F_3	F_4
1. Two of three components fail	0.9	0	0	0	0
2. All three components fail	0.1	0	0	0	0
Average Impact Vector ($\bar{I}$)		$\overline{F_0}$	$\overline{F_1}$	$\overline{F_2}$	$\overline{F_3}$
		0	0	0.9	0.1

Figure 2. Example of the assessment of impact vectors involving multiple interpretation of event (Reference 1).

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

$$\bar{I} = [\overline{F_0}, \overline{F_1}, \cdots, \overline{F_m}] \; . \qquad (4\text{-}2)$$

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

Both are equal to [0, 1, 0]. If the weight for hypothesis one is 0.6 and 0.4 for hypothesis two, the average impact vector equals

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

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

4.2 Generic Impact Vector Assessment

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

For many events, assigning a single impact category (i.e., $F_k = 1$ for some k) is not possible. This was also illustrated in the previous section. Such cases generally involve one or both of the following factors (References 4, 5, and 6):

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

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

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

1. Events involving degraded component states,

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

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

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

4.2.1 Case 1: Events Involving Degraded Component States

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

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

- Failed p = 1.00,
- Highly degraded p = 0.50,

- Degraded p = 0.10,
- Incipient p = 0.01, and
- No Failure p = 0.00.

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

4.2.2 Case 2: Events Involving Failures Distributed in Time

In this case, the presence of a shared cause for the component states is determined. However, component states (failure, degraded, etc.) do not occur, or are not detected, simultaneously. Rather they are recorded at different, but closely correlated times (or test cycles). In this case, a probability q can be assigned that reflects the degree the events (component degradations) represent a CCF event during the mission time of interest (e.g., typical PRA mission times). The following guidelines are suggested for assessing q for different operational characteristics. The values used in assigning q are in part based on the probability of failures given a successive number of trials using a binomial distribution.

4.2.2.1 Operating Components. For operating components, assigning the time delay probability q is straightforward, and it is based solely on the reported time of the failures. There is no assumption about the time of failure or whether the multiple failures, or degraded states, occurred at the same time.

- For component failures that occur within the PRA mission time and for standby components whose failures were discovered during testing, but within half the test interval, the event is interpreted as a CCF event and q = 1.00.
- For k components that fail more than the (PRA) mission time apart, but within 1 month of each other and for standby components whose failures were discovered during testing, but within a time interval (T/2, T), q = 0.50.
- For component failures that occur more than one month apart and for standby component failures that were discovered during testing outside the test interval, q = 0.10.
- For component failures that occur more than one test interval apart, events are considered as independent, thus q = 0.00.

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

Approach Using the Standby Failure Rate Model. If non-staggered testing is adopted, it is possible for the components to fail immediately following the test, in which case, the latent CCF state could exist for the test interval. However, the average time a latent CCF state could exist is half the test interval.

Table 4. Impact vector assessment for various degrees of component degradations.

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

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

- If components fail, or are reported failed, within half the test interval, the event is interpreted as CCF with q = 1.00,

- If component failures are separated by a time interval longer than $T_I/2$, but shorter than T_I, the event is interpreted as a CCF with q = 0.50,

- If component failures are separated by a time interval longer than T_I, but shorter than 3/2 T_I, the event is interpreted as a CCF with q = 0.10, and

- If the component failures are separated by a time interval longer than 3/2 T_I, the event is interpreted as two (or m) independent failures.

Since test intervals vary between plants and systems for like components, some average values may have to be assumed. A month is appropriate for diesel generators in U.S. plants, but is too short for most other components. Test intervals must be determined for each individual system/component combination.

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

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

- If the failures are separated by one successful challenge, then using the binomial concept, a point estimate for the probability of failure of the second component given the failure of the first one is 1/2 (one failure in two challenges). In this case, the event is interpreted as a CCF with q = 0.50.

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

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

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

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

For common cause failure,

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

For independent failure of component 1,

$$I_{c_1} = (1\text{-}q)\,[0,1,0,0] = [0,\ 1\text{-}q,\ 0,\ 0] \text{ for component 1}$$

and

For independent failure of component 2,

$$I_{c_2} = (1\text{-}q)\,[0,1,0,0] = [0,\ 1\text{-}q,\ 0,\ 0] \text{ for component 2.}$$

The average impact vector for this specific case is:

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

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

I_{CCF} = [0, 0,..., q, ..., 0], where q is the k+1 element of the vector,

$$I_{c_1} = [0,\ 1\text{-}q,\ 0,\ \ldots,\ 0] \text{ for component 1}$$

$$\vdots \quad = [0,\ 1\text{-}q,\ 0,\ \ldots,\ 0] \text{ for component k.} \quad (4\text{-}3)$$

$$I_{c_k}$$

The average impact vector in this case is:

$\bar{I}$ = [0, k(1-q), ..., q, ..., 0], where q is the k+1 element of the vector.

4.2.3 Case 3: Events Involving Uncertainty about Shared Cause

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

- Very High $c = 1.0$,
- High $c = 0.50$,
- Moderate $c = 0.10$,
- Low $c = 0.01$, and
- No coupling $c = 0.00$.

The effect of this factor on the event impact vector can be obtained similarly to the timing factor q. More specifically, the set of equations (4-3) can be used after replacing q with c.

I_{CCF} = [0, 0, ..., c,..., 0], where c is the k+1 element of the vector,

I_{c_1} = [0, (1-c), 0, ..., 0] for component 1,

⋮

I_{c_k} = [0, (1-c), 0, ..., 0] for component k. (4-4)

The average impact vector in this case is:

$\bar{I}$ = [0, k(1-c), ..., c,..., 0], where c is the k+1 element of the vector.

4.2.4 Cases Involving Degraded States, Time Delay, and Uncertain Shared Cause

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

I_{CCF} = $[cqF_0, cqF_1, \ldots, cqF_m]$,

I_{c_1} = $[(1\text{-}cq)(1\text{-}P_1), (1\text{-}cq)P_1, 0, \ldots, 0]$ for component 1,

⋮

I_{c_m} = $[(1\text{-}cq)(1\text{-}P_m), (1\text{-}cq)P_m, 0, \ldots, 0]$ (4-5)

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

Note that the product of cq represents an overall measure of coupling strength. The decomposition of this measure, in terms of c and q, is merely an aid to the analyst's subjective assessment of the strength based on different manifestations of the degree of coupling presence. As can be seen from equation 4-5, the quantity modifying the impact vectors for shared cause strength is cq, which could be replaced by a single parameter.

4.3 Specializing Impact Vectors for Plant Specific Analyses

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

4.3.1 Adjustment Based on Qualitative Differences

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

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

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

$$I_r = r * I. \qquad (4\text{-}6)$$

The modified application-specific impact vector is then written as: The r factor may be written as the product of two factors r_1 and r_2, which are measures of applicability of the root cause and coupling factor of the event, respectively (References 4, 5, and 6). The "strength" of a root cause manifests itself in the degree to which each of the components is affected. Therefore, on the arbitrary scale of zero to one, a root cause of zero strength results in no failure. The likelihood of a failure increases as the root cause strength moves towards one. In contrast, the coupling factor strength represents the degree to which multiple failures share a common-cause. Coupling strength of zero means failures are independent, while CCFs are characterized by coupling strength of one. The role of these two factors in creating various types of events is shown schematically in the diagram of Figure 3.

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

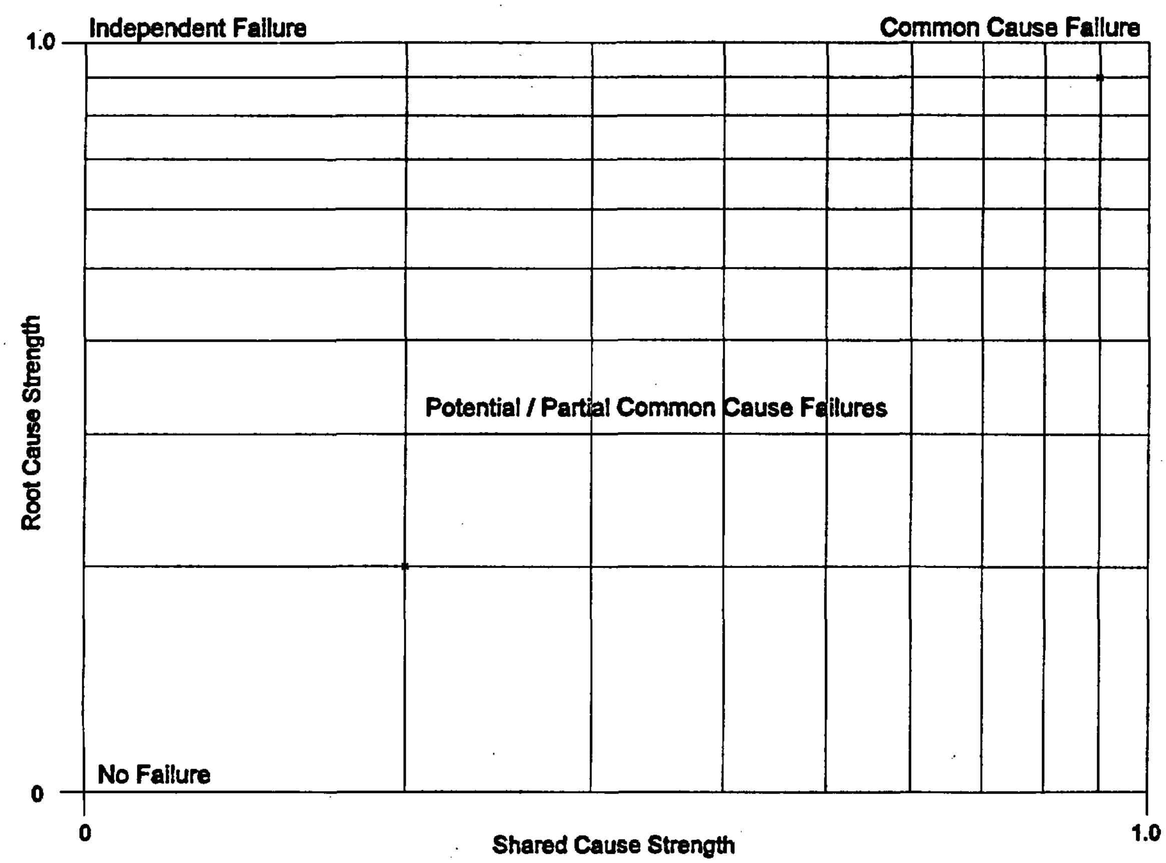

Figure 3. Schematic representation of the role of shared cause factor and root cause strength information of different classes of events (the density of vertical and horizontal lines represents the degree of strength for illustrative purposes).

Table 5. Suggested values for r_1 and r_2.

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

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

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

4.3.2 Adjustment for Quantitative Difference

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

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

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

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

$$\rho = \sum_{i=1}^{m} \frac{i}{m} F_i \qquad (4\text{-}7)$$

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

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

4.4 Estimation of CCF Event Frequencies from Impact Vectors

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

$$n_k = \sum_{i=1}^{m} \overline{F}_k(i) \ , \qquad (4\text{-}8)$$

where

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

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

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

$$\hat{\alpha}_k = \frac{n_k}{\sum_{j=1}^{m} n_j} . \qquad (4\text{-}9)$$

4.5 Treatment of Uncertainties

From earlier discussions it is evident that there are potentially significant uncertainties in the development of a statistical database from CCF event reports. These uncertainties can be categorized as follows:

1. Uncertainty because of lack of sufficient information in the event reports for unambiguous event classification and impact vector assessment,

2. Uncertainty in translating event characteristics to numerical parameters for impact vector assessment, and

3. Uncertainty in determining the applicability of an event to a specific plant design and operating characteristics.

In these cases, significant amounts of judgment are required. Analysts are likely to have different interpretations of the events, and make different assumptions about what is missing from both the event reports and physical and operational descriptions of the plants involved. This is true even though specific guidelines have been provided in this report to ensure, as a minimum, a reasonable level of accuracy and consistency and to reduce analyst-to-analyst variabilities.

Nevertheless, the potential for major variabilities in the results exist. It is essential that the uncertainties in the estimated CCF probabilities be assessed. This requires a systematic procedure to capture the magnitude of variabilities in the estimated impact vectors. Similarly, potential incompleteness and biases in the raw data (event reports) should be considered and their magnitude estimated. Finally statistical techniques should be applied to measure the effect of uncertainties on the distribution of CCF frequencies.

The method described in Section 4.4 develops statistical evidence needed for parameter estimation by averaging event impact vectors over multiple hypotheses and corresponding probabilities. The averaging procedure leads, as described in Reference 1 to an underestimation of uncertainties, while producing nearly exact mean values. Reference 1 proposed a formal uncertainty analysis method to account for the impact of the multiple-hypothesis approach to data classification.

Limited exercise with typical data sets (Reference 9) has indicated the difference between the results of the formal approach and those based on average impact vectors is not significant, particularly when compared with the impact of other sources of uncertainty, such as plant-to-plant and analyst-to-analyst variabilities of impact vector values. The computational complexity and relatively small impact of the formal method add to the appeal of the average impact vector approach as the method of choice implemented in the CCF software.

Certain formal and rigorous methods for handling uncertainties in CCF frequencies, as a function of analyst uncertainty in the impact vector assessment, have been suggested and applied to a small data sample. These methods, however, tend to be tedious for large databases. A rough approximation of the range of uncertainty in CCF frequency estimates can be developed through ad-hoc techniques, such as bounding of the uncertainties. For example, the analyst assesses the impact vectors "optimistically" (tends to judge events "independent" when in doubt) and, then, assesses the impact vectors "pessimistically" (tends to judge events as common cause). Distributions of CCF frequency are then developed from the statistics obtained from each of the two sets of impact vectors, according to the methods described in Reference 1. These distributions are combined to obtain the overall range of uncertainty in the CCF frequency estimate.

Among the models discussed in Appendix B and implemented in the CCF software, the full uncertainty treatment is only provided for the alpha-factor model. This is because the sampling model (on which the alpha factor model can be based) is simple, and can be justified with very few assumptions regarding the process through which the data are generated. This is not the case, however, for the Multiple Greek Letter (MGL) model (see Appendix B; also see Reference 1, Appendix E).

The statistical uncertainty distribution of the alpha-factor model parameters can be developed using Bayesian techniques as described in Reference 1 and summarized in the following.

Start with the set of event data developed based on Equation 4-8:

$$Data = [\, n_1, \ldots, n_m], \qquad (4\text{-}10)$$

where n_k is the number of *events* involving failure of k components. The likelihood of observing this data can be modeled by a multinomial distribution for given values of α_k's:

$$P(n_1, \ldots, n_m \mid \alpha_1, \ldots, \alpha_m) = \frac{\Gamma(n_1 + n_2 + \cdots + n_m)}{\Gamma(n_1) \cdots \Gamma(n_m)} \alpha_1^{n_1} \alpha_2^{n_2} \cdots \alpha_m^{n_m - 1} \qquad (4\text{-}11)$$

This distribution is based on the assumption that n_k's are generated independently with probabilities given by α_k's subject to the constraint that the sum of α's is one. By using equation 4-11 as the likelihood function in Bayes theorem and choosing a Dirichlet distribution function as the prior for α's, a posterior distribution function, which is also Dirichlet in form, is obtained:

$$\pi(\alpha_1, \ldots, \alpha_m) = \frac{\Gamma(A_1 + A_2 + \cdots + A_m)}{\Gamma(A_1) \cdots \Gamma(A_m)} \alpha_1^{A_1 - 1} \alpha_2^{A_2 - 1} \cdots \alpha_m^{A} \qquad (4\text{-}12)$$

where A_k's [k = 1,...,m] are the parameters of the posterior distribution and are related to a similar set of prior distribution parameters [A_{o1}, ..., A_{om}] through the following relationship:

$$A_k = A_{ok} + n_k. \qquad (4\text{-}13)$$

Note that $0 \le A_k < \infty$ for all k.

The general form of marginal distribution of each α_j is:

$$\Pi_j(\alpha_j) = \frac{\Gamma(A_T)}{\Gamma(A_j)\Gamma(A_T - A_j)} \alpha_j^{A_j - 1}(1 - \alpha_j)^{(A_T - A_j) - 1} \quad (4\text{-}14)$$

The mean value is calculated from:

$$\bar{\alpha}_j = \frac{A_j}{A_T}\ , \quad (4\text{-}15)$$

where

$$A_T \equiv \sum_j A_j\ .$$

The equivalent of the maximum likelihood estimators is obtained as the mode of the posterior distribution when the value of all prior distribution parameters is set to 1. This gives the posterior mode for α_j, which is

$$\hat{\alpha}_j = \frac{n_j}{n_t} \quad (4\text{-}16)$$

where

$$n_t = \sum_{j=1}^{m} n_j.$$

The above treatment assumes that once the CCF events are reinterpreted and impact vectors mapped in a particular application, a homogeneous population of events is created. That is, after the specialization of the CCF event impact vectors, the events are considered as belonging in the same population and coming from the plant under consideration. If on the other hand, this potential population variability (plant-to-plant variability) of CCF events are considered, a different statistical model (one based on non-homogenous population) applies.

In this approach average impact vector elements are summed for each impact category for each plant. A data set is thus generated for each of the N plants in the database. That is,

$$D^{(i)} = [n_1^{(i)}, n_1^{(i)}, \ldots, n_1^{(i)}], \quad i = 1, \ldots, N \quad (4\text{-}17)$$

Note that the data set of equation 4-10 is formed by summing the $D^{(i)}$ for all plants.

The plant-to-plant variability distribution of each α_j can be obtained through the following steps. First we assume that the distribution can be represented by a beta distribution:

$$\pi_j(\alpha_j) = \frac{\Gamma(a_j + b_j)}{\Gamma(a_j)\Gamma(b_j)} \alpha_j^{a_j}(1 - \alpha_j)^{b_j} \quad (4\text{-}18)$$

where a_j and b_j are two (unknown) parameters. The distribution of a_j and b_j can be obtained using the following data set developed from equation 4-17:

$$D_j = [n_j^{(i)}, n_t^{(i)}; i = 1, \ldots, N] \quad (4\text{-}19)$$

where

$$n_t^{(i)} = \sum_{j=1}^{m} n_j^{(i)} \quad (4\text{-}20)$$

We use D_j in Bayes Theorem:

$$f(a_j, b_j | D_j) = \frac{L(D_j | a_j, b_j) f_0(a_j, b_j)}{\int\int L(D_j | a_j, b_j) f_0(a_j, b_j) da_j db_j} \quad (4\text{-}21)$$

where the likelihood function is

$$L(D_j ; a_j, b_j) = \prod_{i=1}^{N} [\int B(n_j^{(i)}, n_t^{(i)} | \alpha_j) \pi_j(\alpha_j) d\alpha_j] \quad (4\text{-}22)$$

In equation 4-22, $B(n_j^{(i)}, n_t^{(i)} | \alpha_j)$ is a binomial distribution corresponding to the data from the plant I. The final step is to use the posterior distribution of equation 4-21 to find various estimates of the desired distribution of α_j, including a mean density function:

$$\bar{\pi}_j(\alpha_j) = \int\int \pi_j(\alpha_j | a_j, b_j) f(a_j, b_j | D_j)\, da_j\, db_j \qquad (4\text{-}23)$$

Both the homogeneous and nonhomogeneous models are available in the CCF software. The non-homogeneous option can be used to develop generic and global assessment of the ranges of CCF parameters across the industry. It can also be used as a prior distribution in plant-specific estimations. For this use the data from the plant being analyzed should be excluded from the non-homogeneous data base, equation 4-17, to be used as plant-specific data in the Bayesian updating process. The resulting distribution form this procedure is expected to be wider than the distribution obtained based on the non-homogeneous assumption (equation 4-14). We also note that common cause failure frequencies, Q_k's, are calculated by multiplying α-factors and total component failure frequency, Q_t:

$$Q_k \propto \alpha_k Q_k \qquad (4\text{-}24)$$

The spread of the distribution of Q_k is, therefore, also influenced by the spread of the distribution of Q_t, which often includes uncertainties due to plant-to-plant variability. The distributions of α and Q_t are usually skewed to the left (i.e., the long tail in closer to zero), and their mean values are greater than the median. Therefore, the distribution of Q_k is also skewed to the left and its mean is greater than the median. Thus, its upper percentiles do not change as much as the lower percentiles.

Consider the following numerical example as an illustration of these concepts. Let Q_t be distributed as a lognormal random variable with mean equal to 0.001 and error factor equal to 5. For α_k we consider a set of lognormal distributions, each with a mean equal to 0.05 and error factors that vary from 2 to 10. Figure 4 contains a plot of the mean CCF probability, Q_k, the 95th percentile, the 50th percentile (median), and the 5th percentile obtained from equation 4-24. (Note that an error factor of 1 is equivalent to multiplying by a constant value.) Typical error factors for α_k range from 2 to 4. The plot shows that the 95th percentile is relatively constant, as expected. The 95th percentile of the distribution of α_k with an error factor of 10 is only 1.25 times as large as the 95th percentile of the distribution of Q_t. Similar results are obtained when beta distributions or combinations of beta and lognormal distributions are used. Note, however, that the changes in the lower tail are more pronounced.

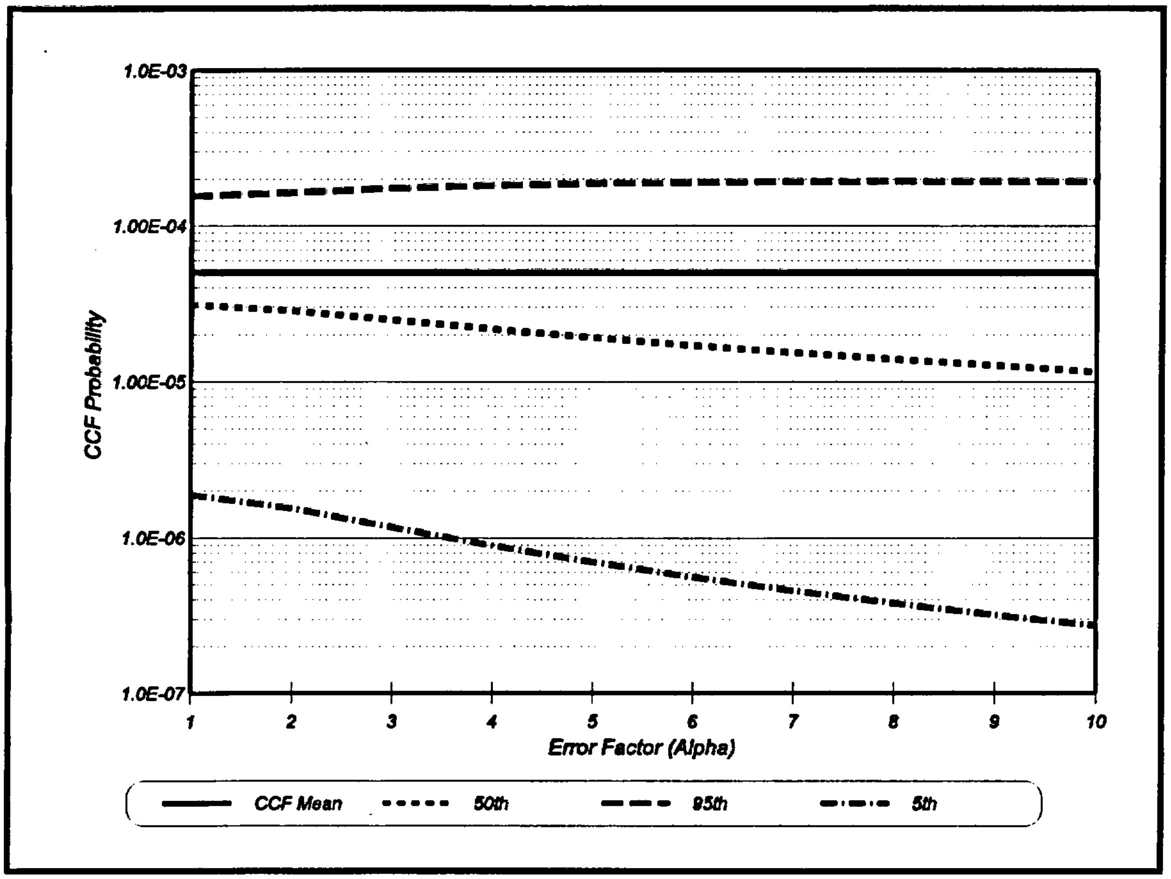

Figure 4. Example of changes in CCF uncertainty percentiles with changes in alpha factor uncertainty (lognormal distribution).

5. INFORMATION NEEDED FOR COMMON CAUSE DATA CLASSIFICATION AND ANALYSIS

The following is a list of important information needed to identify, classify, and analyze CCF events. Some of this list was presented in prior studies, References 7 and 8. The list has three parts: (1) Event Description: the information that can come directly from the event reports as factual and ideally requiring no analytical interpretation, (2) Event Analysis: classification of key characteristics of the event such as component states, causes, coupling factors, and statistical interpretation of the event, and (3) Application-Specific Analysis: identification or assessment of the event for a specific analysis such as a plant-specific PRA.

5.1 Event Description

1. REPORT NUMBER—Identifies the source of the event under consideration, and is a unique character string identifier.

2. NAME—The name of the plant and the unit(s) in which the event occurred.

3. DATE—The date(s) of the failure(s) discovery.

4. STATUS—The plant or unit operational status at the time of the event.

5. SYSTEM—The system in which the failure occurred.

6. FAILURE MODE—The failure mode associated with the function that the component was actually or potentially unavailable to perform. The degree of unavailability to perform the function is coded as "Component Degradation Parameter."

7. COMMON CAUSE COMPONENT GROUP SIZE—Refers to the number of similar components in the system considered to be susceptible to a CCF. This is sometimes identical to the level of redundancy in the system.

8. EVENT DESCRIPTION—A summary (or full) description of the event under consideration.

9. TIME OF FAILURE—The time of failure and discovery of condition (for each component involved in the event).

5.2 Event Analysis

10. CAUSE—There are three factors that constitute a common-cause event: proximate cause, trigger event, and conditioning event. The proximate cause is the immediate origin of component failure, while the trigger event initiates the failure or the transition to the failed state. The conditioning event predisposes a component to fail, but does not itself cause the failure.

11. COUPLING FACTOR—A postulation of why and how a failure is systematically induced in several components.

12. SHARED CAUSE FACTOR—This reflects the analyst's uncertainty about the existence of coupling between the failures, i.e., whether a shared cause of failures can be identified (see also the Timing Factor).

13. SHOCK TYPE—Characterization of the impact mechanism of the cause of the event on the population of components exposed to it. There are two types of shocks:

    Lethal Shock: This refers to causes of failure that fail all components in the population.

Nonlethal Shock: Refers to causes that can affect any subset or the entire population.

14. MODE OF DISCOVERY—The way the condition in the component(s) was discovered. This is used in determining if the time delay factor should be evaluated based on operational/observation events or a scheduled test interval.

15. DEFENSES—The defenses that could have been implemented against recurrence at the plant. These are assigned based on whether they were primarily defending against the cause or the coupling factor.

16. COMPONENT DEGRADATION PARAMETER—The assessed probability that a degraded component would lead to failure to complete the mission.

17. TIMING FACTOR—The probability that two or more component failures (or degraded states), separated in time, represent a CCF. This can be viewed as an indication of the strength-of-coupling in synchronizing failure times.

18. FAILURE MODE APPLICABILITY FACTOR—The degree (or probability) that the functional mode of component(s) failure is the mode specified under the failure mode code.

19. AVERAGE IMPACT VECTOR—Records the average of impact vectors for different hypotheses regarding the number of components failed in the event. This calculation is based upon other attributes (e.g., time delay factor, degradation values).

5.3 Application-Specific Analysis

20. COMMON CAUSE COMPONENT GROUP SIZE—Refers to the number of similar components in the system considered to be susceptible to CCFs. This is sometimes identical to the level of redundancy in the system.

21. CAUSE APPLICABILITY FACTOR—The probability that the cause of the event applies to the plant/system which uses the data. This is a measure of the defenses relative strength against the cause of the event at the original plant/system and target plant/system.

22. COUPLING APPLICABILITY FACTOR—The probability that the coupling factor of the event applies to the plant/system which uses the data. This is a measure of the defenses' relative strength at the original plant/system and target plant/system against the coupling factor of the event.

23. MAPPING UP FACTOR—The parameter needed for adjusting the impact vector of the event for application to a larger size system (see Appendix A).

24. PLANT APPLICATION SPECIFIC IMPACT VECTOR—The application specific impact vector (representing the interpretation of the data to a specific plant or system) would be recorded. Calculation of this quantity is based upon the average impact vector and other attributes (e.g., cause applicability factors).

6. REFERENCES

1. U.S. Nuclear Regulatory Commission, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies,* Volume 1, *Procedural Framework and Examples*, and Vol. 2, *Analytical Background and Techniques*, NUREG/CR-4780, EPRI NP-5613, 1989.

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

3. U.S. Nuclear Regulatory Commission, *A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures*, NUREG-CR-5460, (SAND 89-2368), March 1990.

4. Mosleh , A. et al, *On Quantitative Analysis of Common Cause Failure Data for Plant-Specific Probabilistic Safety Assessments*, University of Maryland Nuclear Engineering Report UMNE-92-004, Prepared for the U.S. Nuclear Regulatory Commission, August 1992.

5. Mosleh, A., G. Parry, and A.F. Zikria, *An Approach to the Analysis of Common Cause Failure Data for Plant-Specific Application*, accepted for publication in Nuclear Engineering and Design, 1994.

6. U.S. Nuclear Regulatory Commission, *Procedure for Analysis of Common Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801 (SAND91-7087), April 1993.

7. U.S. Nuclear Regulatory Commission, *Enhancements to Data Collection and Reporting of Single and Multiple Failure Elements*, NUREG/CR 5471 (SAND89-2562), February 1993.

8. Paula, H. M., *Data Base Features That are Needed to Support Common Cause Failure Analysis and Prevention: An Analyst's Perspective*, Nuclear Safety, Volume 31, No. 2, April-June 1990.

9. Siu, N. and A. Mosleh, *Treating Data Uncertainties in Common Cause Failure Analysis*, Nuclear Technology, 84 (1989) 265-281.

GLOSSARY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- *Degraded*—The component is in such a state that it exhibits reduced performance but insufficient degradation to declare the component unavailable according to the specified success criterion.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Shock—A shock is an event that occurs at a random point in time and acts on the system; i.e., all the components in the system simultaneously. There are two kinds of shocks distinguished by the potential impact of the shock event, i.e., *lethal* and *nonlethal*.

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

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

Appendix A
Overview of Impact Vector Mapping

Appendix A
Overview of Impact Vector Mapping

This appendix provides a summary of the procedure recommended by Reference 1 for modifying generic impact vectors for size (exposed population) difference between the original plant (the plant in which the event has occurred) and the target plant (the plant for which the generic data are specialized).

A-1. MAPPING DOWN IMPACT VECTORS

A complete set of formulas for mapping down data from systems having four, three, or two components to a system having fewer components is presented in Table A-1. In this table, $F_k(m)$ represents the k-th element of the average impact vector in a system (or component group) of size m. The formulas show how to obtain the elements of the impact vector for smaller size systems when the elements of the impact vector of a larger system are known.

A-2. MAPPING UP IMPACT VECTORS

It is evident from the information presented above that downward mapping is "deterministic;" i.e., given an impact vector for a system having more components than the system being analyzed, the impact vector for the same size system can be calculated without introducing new uncertainties. Mapping up, however, (see Reference 1, Volume 2), is not deterministic.

To reduce the uncertainty inherent in upward mapping of impact vectors, use is made of a concept that is the basis of the binomial failure rate (BFR) common-cause model (Reference 5). The 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 only on a subset of the components in the system.

3. **Lethal Shocks.** Causal events that 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. 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 reduced (but not eliminated). To categorize an event, the analyst needs to understand the nature of the cause. Random, independent failures (category 1) are usually due to internal or external causes. Lethal shocks can often be identified as impacting all components present. Design errors and procedural errors are examples of causes that could result in lethal shocks. The remaining causes are external causes that have an uncertain impact on each component and can be either lethal or nonlethal.

Table A-1. Formulas for mapping down event impact vectors.

	Size of System Mapping to (Number of Identical Trains)				
SIZE OF SYSTEM MAPPING FROM	5	4	3	2	1
6	$f_1(5)=(5/6)f_1(6)+(1/3)f_2(6)$ $f_2(5)=(2/3)f_2(6)+(1/2)f_3(6)$ $f_3(5)=(1/2)f_3(6)+(2/3)f_4(6)$ $f_4(5)=(1/3)f_4(6)+(5/6)f_5(6)$ $f_5(5)=(1/6)f_5(6)+f_6(6)$	$f_1(4)=(2/3)f_1(6)+(8/15)f_2(6)+(1/5)f_3(6)$ $f_2(4)=(2/5)f_2(6)+(3/5)f_3(6)+(2/5)f_4(6)$ $f_3(4)=(1/5)f_3(6)+(8/15)f_4(6)+(2/3)f_5(6)$ $f_4(4)=(1/6)f_4(6)+(1/3)f_5(6)+f_6(6)$	$f_1(3)=(1/2)f_1(6)+(3/5)f_2(6)+(9/20)f_3(6)$ $+(1/5)f_4(6)$ $f_2(3)=(1/5)f_2(6)+(9/20)f_3(6)+(3/5)f_4(6)$ $+(1/2)f_5(6)$ $f_3(3)=(1/20)f_3(6)+(1/5)f_4(6)+(1/2)f_5(6)$ $+f_6(6)$	$f_1(2)=(1/3)f_1(6)+(8/15)f_2(6)$ $+(3/5)f_3(6)+(8/15)f_4(6)+(1/3)f_5(6)$ $f_2(2)=(1/15)f_2(6)+(1/5)f_3(6)$ $+(2/5)f_4(6)+(2/3)f_5(6)+f_6(6)$	$f_1(1)=(1/6)f_1(6)+(1/3)f_2(6)+(1/2)f_3(6)$ $+(2/3)f_4(6)+(5/6)f_5(6)+f_6(6)$
5		$f_1(4)=(4/5)f_1(5)+(2/5)f_2(5)$ $f_2(4)=(3/5)f_2(5)+(3/5)f_3(5)f$ $f_3(4)=(2/5)f_3(5)+(4/5)f_4(5)$ $f_4(4)=(1/5)f_4(5)+f_5(6)$	$f_1(3=(3/5)f_1(5)+(3/5)f_2(5)+(3/10)f_3(5)f_2$ $(3)=(3/10)f_2(5)+(3/5)f_3(5)+(3/5)f_4(5)$ $f_3(3)=(1/10)f_3(5)+(2/5)f_4(5)+f_5(5)$	$f_1(2)=(2/5)f_1(5)+(3/5)f_2(5)+(3/5)f_3(5)$ $+(2/5)f_4(5)$ $f_2(2)=(1/10)f_2(5)+(3/10)f_3(5)$ $+(3/5)f_4(5)+f_5(5)$	$f_1(1)=(1/5)f_1(5)+(2/5)f_2(5)+(3/5)f_3(5)$ $+(4/5)f_4(5)+f_5(5)$
4			$f_1(3)=(3/4)f_1(4)+(1/2)f_2(4)$ $f_2(3)=(1/2)f_2(4)+(3/4)f_3(4)$ $f_3(3)=(1/4)f_3(4)+f_4(4)$	$f_1(2)=(1/2)f_1(4)+(2/3)f_2(4)+(1/2)f_3(4)$ $f_2(2)=(1/6)f_2(4)+(1/2)f_3(4)+f_4(4)$	$f_1(1)=(1/4)f_1(4)+(1/2)f_2(4)+(3/4)f_3(4)$ $+f_4(4)$
3				$f_1(2)=(2/3)f_1(3)+(2/3)f_2(3)$ $f_2(2)=(1/3)f_2(3)+f_3(3)$	$f_1(1)=(1/3)f_1(3)+(2/3)f_2(3)+f_3(3)$
2					$f_1(1)=(1/2)f_1(2)+f2$

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

Mapping up independent events: In the case of independent events (since the number of independent events in the database is proportional to the number of components in the system), it can be shown that $F_I(l)$ and $F_I(k)$ (the number of independent events in systems with sizes l and k, respectively) are related by the following equation:

$$F_I^{(l)} = (l/k)\, F_I^{(k)}$$

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

$$F_l 0 = F_j^{(j)}$$

Hence, for lethal shocks, the impact vector is mapped directly. The probability that 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.

Mapping up nonlethal shocks: Nonlethal shock failures are viewed as the result of a nonlethal shock that acts on the system at a rate that is independent of system size. For each shock, the quantity ρ is the conditional probability of each component failure (given a shock).

The process of mapping a nonlethal shock that occurs in a one-component system up to a four-component system is illustrated in Reference 1. Table A-2 includes formulas to cover all upward mapping possibilities with system sizes up to four. In the limiting cases of ρ = 0 and ρ = 1, the formulas in Table A-2 become identical to the equations for mapping up independent events, and the equations for mapping up lethal shocks, respectively.

By using this model, the uncertainty inherent in mapping up impact vectors is reduced to the uncertainty in estimating the parameter ρ, which is the probability that the nonlethal shock or cause would have failed a single hypothetical component added to the system.

Table A-2. Formulas for upward mapping of events classified as nonlethal shocks.

Size of System Mapping From		Size of System Mapping to (Number of Identical Trains): 2	3	4	5	6
SIZE	1	$f_1(2)=2(1-\rho)f_1(1)$ $f_2(2)=\rho f_1(1)$	$f_1(3)=3(1-\rho)^2f_1(1)$ $f_2(3)=3\rho(1-\rho)f_1(1)$ $f_3(3)=\rho^2f_1(1)$	$f_1(4)=4(1-\rho)^3f_1(1)$ $f_2(4)=6\rho(1-\rho)^2f_1(1)$ $f_3(4)=4\rho^2(1-\rho)f_1(1)$ $f_4(4)=\rho^3f_1(1)$	$f_1(5)=5(1-\rho)^4f_1(1)$ $f_2(5)=10\rho(1-\rho)^3f_1(1)$ $f_3(5)=10\rho^2(1-\rho)^2f_1(1)$ $f_4(5)=5\rho^3(1-\rho)f_1(1)$ $f_5(5)=\rho^4f_1(1)$	$f_1(6)=6(1-\rho)^5f_1(1)$ $f_2(6)=15\rho(1-\rho)^4f_1(1)$ $f_3(6)=20\rho^2(1-\rho)^3f_1(1)$ $f_4(6)=15\rho^3(1-\rho)^2f_1(1)$ $f_5(6)=6\rho^4(1-\rho)f_1(1)$ $f_6(6)=\rho^5f_1(1)$
OF	2		$f_1(3)=(3/2)(1-\rho)f_1(2)$ $f_2(3)=\rho f_1(2)+(1-\rho)f_2(2)$ $f_3(3)=\rho f_2(2)$	$f_1(4)=2(1-\rho)^2f_1(2)$ $f_2(4)=(5/2)\rho(1-\rho)f_1(2)+(1-\rho)^2f_2(2)$ $f_3(4)=\rho^2f_1(2)+2\rho(1-\rho)f_2(2)$ $f_4(4)=\rho^2f_2(2)$	$f_1(5)=(5/2)(1-\rho)^3f_1(2)$ $f_2(5)=(9/2)\rho(1-\rho)^2f_1(2)+(1-\rho)^3f_2(2)$ $f_3(5)=(7/2)\rho^2(1-\rho)f_1(2)+3\rho(1-\rho)^2f_2(2)$ $f_4(5)=\rho^3f_1(2)+3\rho^2(1-\rho)f_2(2)$ $f_5(5)=\rho^3f_2(2)$	$f_1(6)=3(1-\rho)^4f_1(2)$ $f_2(6)=7\rho(1-\rho)^3f_1(2)+(1-\rho)^4f_2(2)$ $f_3(6)=8\rho^2(1-\rho)^2f_1(2)+4\rho(1-\rho)^3f_2(2)$ $f_4(6)=(9/2)\rho^3(1-\rho)f_1(2)+6\rho^2(1-\rho)^2f_2(2)$ $f_5(6)=\rho^4f_1(2)+4\rho^3(1-\rho)f_2(2)$ $f_6(6)=\rho^4f_2(2)$
SYSTEM	3			$f_1(4)=(4/3)(1-\rho)f_1(3)$ $f_2(4)=\rho f_1(3)+(1-\rho)f_2(3)$ $f_3(4)=\rho f_2(3)+(1-\rho)f_3(3)$ $f_4(4)=\rho f_3(3)$	$f_1(5)=(5/3)(1-\rho)^2f_1(3)$ $f_2(5)=(7/3)\rho(1-\rho)f_1(3)+(1-\rho)^2f_2(3)$ $f_3(5)=\rho^2f_1(3)+2\rho(1-\rho)f_2(3)+(1-\rho)^2f_3(3)$ $f_4(5)=\rho^2f_2(3)+2\rho(1-\rho)f_3(3)$ $f_5(5)=\rho^2f_3(3)$	$f_1(6)=2(1-\rho)^3f_1(3)$ $f_2(6)=4\rho(1-\rho)^2f_1(3)+(1-\rho)^3f_2(3)$ $f_3(6)=(10/3)\rho^2(1-\rho)f_1(3)+3\rho(1-\rho)^2f_2(3)$ $+(1-\rho)^3f_3(3)$ $f_4(6)=\rho^3f_1(3)+3\rho^2(1-\rho)f_2(3)+3\rho(1-\rho)^2f_3(3)$ $f_5(6)=\rho^3f_2(3)+3\rho^2(1-\rho)f_3(3)$ $f_6(6)=\rho^3f_3(3)$
MAPPING	4				$f_1(5)=(5/4)(1-\rho)f_1(4)$ $f_2(5)=\rho f_1(4)+(1-\rho)f_2(4)$ $f_3(5)=\rho f_2(4)+(1-\rho)f_3(4)$ $f_4(5)=\rho f_3(4)+(1-\rho)f_4(4)$ $f_5(5)=\rho f_4(4)$	$f_1(6)=(3/2)(1-\rho)^2f_1(4)$ $f_2(6)=(9/4)\rho(1-\rho)f_1(4)+(1-\rho)^2f_2(4)$ $f_3(6)=\rho^2f_1(4)+2\rho(1-\rho)f_2(4)+(1-\rho)^2f_3(4)$ $f_4(6)=\rho^2f_2(4)+2\rho(1-\rho)f_3(4)+(1-\rho)^2f_4(4)$ $f_5(6)=\rho^2f_3(4)+2\rho(1-\rho)f_4(4)$ $f_6(6)=\rho^2f_4(4)$
FROM	5					$f_1(6)=(6/5)(1-\rho)f_1(5)$ $f_2(6)=\rho f_1(5)+(1-\rho)f_2(5)$ $f_3(6)=\rho f_2(5)+(1-\rho)f_3(5)$ $f_4(6)=\rho f_3(5)+(1-\rho)f_4(5)$ $f_5(6)=\rho f_4(5)+(1-\rho)f_5(5)$ $f_6(6)=\rho f_5(5)$

Appendix B
Commonly Used CCF Parametric Models

Appendix B
Commonly Used CCF Parametric Models

This appendix provides a brief description of three of the most commonly used models for quantification of probabilities of common cause failures in systems reliability assessments. The models are the Basic Parameter (BP) model, the Alpha Factor model and the Multiple Greek Letter (MGL) model. More information about the basis and statistical characteristics of these models can be found in Reference 1.

B-1. THE BASIC PARAMETER MODEL

From the basic events corresponding to a common cause group of m components, the following probabilities can be defined:

Q_k's = probability of a basic event involving k specific components:

$(1 \leq k \leq m)$. (B-1)

The model that uses Q_k's defined in Equation (B-1) to calculate system failure probability is called the basic parameter model.

B-2. ALPHA FACTOR MODEL

The alpha-factor model develops common cause failure frequencies from a set of failure ratios and the total component failure rate. The parameters of the alpha-factor model are defined as:

Q_t ≡ total failure frequency of each component because of all independent and common-cause events

α_k ≡ fraction of the total frequency of failure events that occur in the system involving the failure of k components due to a common cause

and

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

In terms of the α-factor model parameter, the three basic event probabilities of a system of m components (assuming a staggered testing scheme) are written as:

$$Q_k^{(m)} = \frac{(m-k)!\,(k-1)!}{(m-1)!}\,\alpha_k^{(m)} Q_t\ .$$

B-3. MULTIPLE GREEK LETTER MODEL

The MGL parameters consist of the total component failure frequency (which includes the effects of all independent and common cause contributions to the component failure, and a set of failure fractions which are used to quantify the conditional probabilities of the possible ways a common cause failure of a component can be shared with other components in the same group) given a component failure has occurred.

For a system of m redundant components and for each given failure mode, m different parameters are defined. For example, the first four parameters of the MGL model are:

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

plus:

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

γ = conditional probability that the common cause of a component failure that is shared by one or more components will be shared by two or more components additional to the first.

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

To see how these parameters can be used in developing the probabilities of common-cause basic events, consider the system of three redundant components.

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

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

$$Q_3 = \beta\gamma Q_t.$$

Note that the beta factor model is a special case of the MGL model. For this example, the MGL model reduces to beta.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202	U.S. NUCLEAR REGULATORY COMMISSION **BIBLIOGRAPHIC DATA SHEET** (See Instructions on the reverse)	1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.) NUREG/CR-6268 INEEL/EXT-97-00696
2. TITLE AND SUBTITLE Common Cause Failure Database and Analysis System Volume 2 – Event Definition and Classification		3. DATE REPORT PUBLISHED MONTH: June YEAR: 1998 4. FIN OR GRANT NUMBER E8247
5. AUTHOR(S) F. M. Marshall, A. Mosleh, University of Maryland, D. M. Rasmuson, USNRC		6. TYPE OF REPORT Technical 7. PERIOD COVERED (Inclusive Dates) N/A

8. PERFORMING ORGANIZAITON - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Idaho National Engineering and Environmental Laboratory
Lockheed Martin Idaho Technologies Co.
P.O. Box 1625
Idaho Falls, ID 83415-3129

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

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above"; If contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This volume of the Common Cause Failure Database and Analysis System report provides the definition and classification method used for identifying, coding, and quantifying common cause failure (CCF) probabilistic risk assessment (PRA) parameter estimates on the data that are stored in the CCF database.

Equipment failures that contribute to CCF events at commercial nuclear power plants in the U.S. will be identified during a search and review of Licensee Event Report (LER) and Nuclear Plant Reliability Data System (NPRDS) failure reports in accordance with the criteria specified in this document. The equipment failures that contribute to a CCF event are identified and coded for entry into a personal computer storage system using the method presented in this volume. The events stored in the system are used to perform CCF PRA parameter estimations using CCF quantification methods (also described in this volume).The database resulting from coding CCF events is used to estimate CCF failure parameters for use in various CCF models used in PRAs.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)	
Common cause failure	13. AVAILABILITY STATEMENT Unlimited
	14. SECURITY CLASSIFICATION (This page) Unclassified (This report) Unclassified
	15. NUMBER OF PAGES
	16. PRICE

NRC FORM 335 (2-89)

Printed on recycled paper

Federal Recycling Program