NUREG/CR-6268, Rev. 1
INL/EXT-07-12969

Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding

Idaho National Laboratory

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

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

Address: U.S. Nuclear Regulatory Commission
Office of Administration
Mail, Distribution and Messenger Team
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

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

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

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

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

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

NUREG/CR-6268, Rev. 1
INL/EXT-07-12969

Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding

Manuscript Completed: August 2007
Date Published: September 2007

Prepared by
T.E. Wierman/INL
D.M. Rasmuson/NRC
A. Mosleh/Univ. of MD

Idaho National Laboratory
Risk and Reliability Assessment Department
P.O. Box 1625
Idaho Falls, ID 83415-3850

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

A.D. Salomon, NRC Project Manager

**Prepared for
Division of Risk Assessment and Special Projects
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code Y6546**

ABSTRACT

This report on the Common-Cause Failure Database and Analysis System presents an overview of common-cause failure (CCF) analysis methods for use in the U.S. commercial nuclear power industry. Idaho National Laboratory staff identify equipment failures that contribute to CCF events through searches of Licensee Event Reports, Nuclear Plant Reliability Data System failure reports, and Equipment Performance and Information Exchange failure reports. The staff then enter the event information into a personal computer-based data analysis system (CCF system). This report summarizes how data are gathered, evaluated, and coded into the CCF system, and describes the process for using the data to estimate probabilistic risk assessment common-cause failure parameters.

FOREWORD

This report presents guidance for collecting, classifying, and coding common-cause failure (CCF) events. It updates NUREG/CR-6268, "Common-Cause Failure Database and Analysis System," published in 1998. The U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) and the Idaho National Laboratory (INL) maintain a CCF database for the U.S. commercial nuclear power industry. The CCF data effort consists of CCF event identification, CCF event coding and CCF parameter estimation.

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

The NRC draws from three data sources to select equipment failure reports for CCF event identification: (1) the Nuclear Plant Reliability Data System (NPRDS), which contains component failure information from 1980 through 1996; (2) the Equipment Performance and Information Exchange (EPIX) System, which contains component failure information since 1997; and (3) Licensee Event Reports (LERs). RES and INL data analysts review failure data to identify independent and CCF events.

The CCF data collection and analysis activity consists of CCF event identification, event coding, and loading the CCF events into a software system to estimate CCF parameters. The CCF event identification process includes reviewing failure data to identify independent and CCF events. The data analyst uses the guidance in this report to code the CCF events consistently and accurately. The data analysts then load the CCF events into the CCF database. The events are stored in a format that allows PRA analysts to review the events and develop an understanding of how they occurred and to estimate CCF parameters and their uncertainties.

The CCF database not only stores the CCF event descriptions but also event counts and information associated with the events. It also automates the estimation of CCF parameters. NRC risk analysts and senior reactor analysts use these CCF parameters estimates in Standardized Plant Analysis Risk models, reliability studies, and other PRA regulatory activities. The NRC staff also use CCF insights in inspection activities. The industry uses the CCF parameter estimates in their probabilistic safety assessments.

Farouk Eltawila, Director
Division of Risk Assessment
and Special Applications
Office of Nuclear Regulatory Research

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

This report presents guidance for collecting, classifying, and coding common-cause failure (CCF) events. It updates NUREG/CR-6268, "Common-Cause Failure Database and Analysis System," published in 1998. The U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) and the Idaho National Laboratory (INL) maintain a CCF database for the U.S. commercial nuclear power industry. The CCF data effort consists of CCF event identification, CCF event coding, and CCF parameter estimation.

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

Three data sources are used to select equipment failure reports to be reviewed for CCF event identification: (1) the Nuclear Plant Reliability Data System (NPRDS), which contains component failure information from 1980 through 1996; (2) the Equipment Performance and Information Exchange (EPIX), which contains component failure information since 1997; and (3) LER Search, which contains Licensee Event Reports (LERs). All events that meet the above criteria are identified as CCF events and are included in the CCF database. The database contains CCFs beginning in 1980 and is continuously updated to remain current.

The CCF material has been updated to include the coding guidance applicable to EPIX. It also contains corrections and changes that have been made to the data collection and coding process. Figure ES-1 shows the steps of the data analysis process. They are the following: collection of source data, identification of CCF events, coding of CCF events, database quality assurance, data analysis, and parameter estimation.

The initial step in the process is to identify the boundaries of the analysis, including the plant systems and components to be analyzed and operational event boundaries. The system and component combinations that have been selected for analysis are those addressed in PRA modeling for which CCF parameters are needed.

The next step is to perform searches for events using available data sources. The sources of component failure data most readily available to the NRC were the NPRDS failure reports, which have been replaced by EPIX failure reports, and LERs. For the first data searches, sophisticated algorithms were developed to locate and pre-process event data from NPRDS and LERs to compile potential CCF events. The current updates are of much smaller scope. Routine searches are performed that filter EPIX data to obtain failure reports for components of interest to the CCF study. All LERs submitted by licensees are reviewed for events applicable to the CCF program as well as other ongoing programs at the INL pertaining to plant performance indicators, system reliability studies, and initiating event studies.

Data analysts read the LER and EPIX report narratives of events to determine the system, component, failure mode, degree of degradation, and plant status. Event records that either have no failure or do not involve a component included in the CCF study are not considered. The LER events are then compared to EPIX events to eliminate any duplication of events.

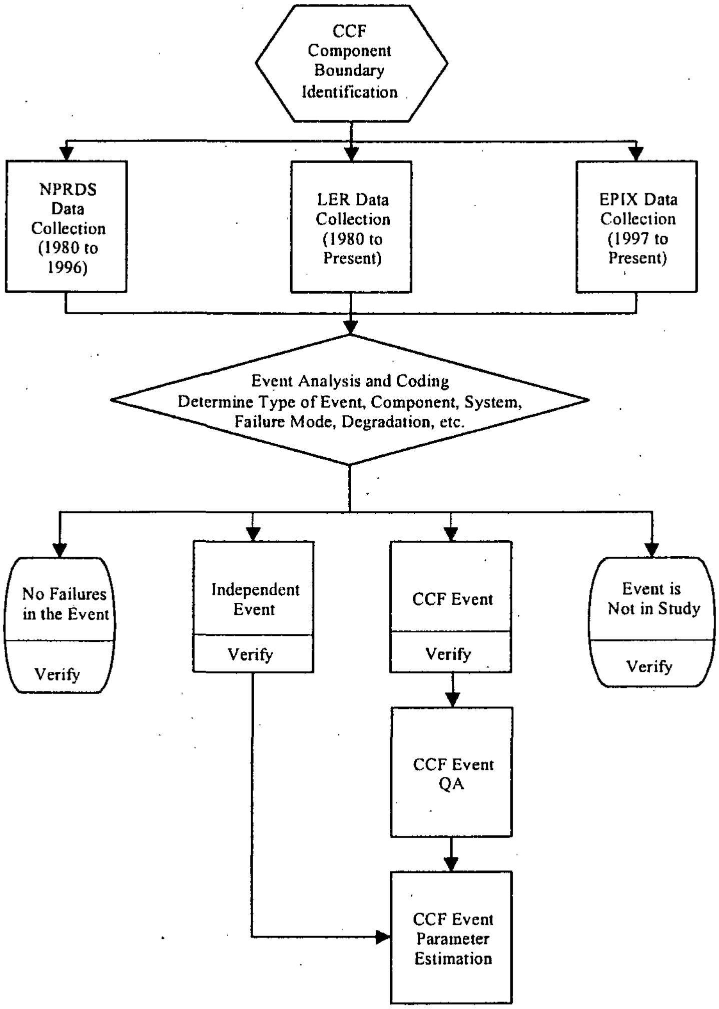

CCF Component Boundary Identification
NPRDS Data Collection (1980 to 1996)
LER Data Collection (1980 to Present)
EPIX Data Collection (1997 to Present)
Event Analysis and Coding Determine Type of Event, Component, System, Failure Mode, Degradation, etc.
No Failures in the Event
Verify
Independent Event
Verify
CCF Event
Verify
Event is Not in Study
Verify
CCF Event QA
CCF Event Parameter Estimation

Figure ES-1. CCF data analysis process.

All of the data analysis takes place external to the CCF database so that unreviewed data are not released. The data-loading step adds qualified data to the CCF database. After the CCF events have been reviewed, comments resolved, and duplicate events removed, the CCF and independent events are loaded into the CCF database.

Once the independent event count and CCF event information have been entered into the CCF database and quality assurance verification has been completed, the next step is the estimation of CCF parameters using the CCF software system. The parameter estimation software developed for this project uses the impact vector method based on physical characteristics of the event. These characteristics include component degradation parameter, timing factor, and shared cause factor. In addition, the software allows the user to modify the generic event impact factors for plant-specific applications, including mapping the impact vectors to account for differences in common-cause component group (CCCG) size between the plant in which the event occurred and the plant for which the data are being modified. Other software features include parameter estimations for both Alpha Factor and Multiple Greek Letter models.

In May 1998, the NRC published NUREG/CR-5497, "Common-Cause Failure Parameter Estimations." In September 2003, the NRC started publishing the common-cause parameter estimations on the NRC web site. The parameter estimations file contains the same information, but is updated on a yearly basis. The web page containing the common-cause parameter estimations downloadable file is http://nrcoe.inel.gov/results/.

- Uncertainties exist in the development of a statistical database from CCF event reports. These uncertainties can be categorized as follows:

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

- Uncertainty in translating event characteristics to numerical parameters for impact vector assessment

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

The guidelines provided in this report help to reduce the uncertainties by providing a reasonable level of accuracy and consistency and to reduce analyst-to-analyst variability.

ABBREVIATIONS

AFW	auxiliary feed water
BE	basic event
BWR	boiling water reactors
CCCG	common-cause component group
CCF	common-cause failure
CCW	component cooling water
CST	condensate storage tank
EDG	emergency diesel generator
EPIX	Equipment Performance and Information Exchange
HPCI	high-pressure coolant injection
INL	Idaho National Laboratory
IPE	individual plant examination
LER	Licensee Event Report
MGL	Multiple Greek Letter (model)
MOV	motor operated valve
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
PRA	probabilistic risk assessment
PWR	pressurized water reactors
RCIC	reactor core isolation cooling
RES	NRC's Office of Nuclear Regulatory Research
RHR	residual heat removal
RPS	reactor protection system
SRV	safety relief valve

Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding

1. INTRODUCTION

A general conclusion from probabilistic risk assessments (PRAs) of commercial nuclear power plants is that common-cause *failures*[a] (CCFs) are significant contributors to the unavailability of safety *systems*. A CCF *event* consists of *component* failures that meet the following four criteria: (1) two or more individual components fail, are *degraded* (including failures during demand or in-service testing), or have deficiencies that would result in component failures if a demand signal had been received, (2) components fail within a selected period of time such that success of the probabilistic risk assessment (PRA) mission would be uncertain, (3) components fail because of a single *shared cause mechanism* and coupling mechanism, and (4) components fail within the established *component boundary*.

Efforts in past years to improve understanding and modeling of CCF events have produced several models, procedures, computer codes, and databases. Some efforts have collected limited amounts of data for use in CCF analyses. Most of these efforts used operational experience data prior to 1984. Until recently, lack of CCF event data was a major problem, though significant progress was made with the publication of "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," EPRI NP-3967 (Ref. 1). Two known deficiencies of EPRI NP-3967 are the limited timeframe for the study and the lack of details regarding *independent events*. In the areas of data classification, analysis, and model parameter estimation, the detailed procedures of "Procedures for Treating Common-cause Failures in Safety and Reliability Studies," NUREG/CR-4780, Volumes 1 and 2 (Ref. 2), and "Procedure for Analysis of Common-cause Failures in Probabilistic Safety Analysis," NUREG/CR-5801 (Ref. 3), have been viewed as too time consuming, despite wide acceptance of the basic approach.

In response to these deficiencies, the Idaho National Laboratory (INL) staff and the U. S. Nuclear Regulatory Commission's (NRC's) Division of Risk Assessment and Special Projects have developed a CCF data collection and analysis system that includes a method for identifying CCF events, coding and classifying those events for use in CCF studies, and storing and analyzing the data. The system is based, in part, on previous CCF methods and models and is designed to run on a personal computer. The data collection effort added a substantial number of CCF events for use in CCF analyses above the previous industry efforts to collect CCF data. The generic data generated from these past studies have been divided by component type, with no allowance given for differences that might exist between systems. The current data collection effort has separated the data by system. The principal products of this CCF data collection and analysis system (CCF system) project are the method for identifying and classifying CCF events, the CCF database containing both CCF events and independent failure counts, and the CCF parameter estimation software. The computer software produced for this project uses the *impact vector* method introduced in Reference 2 and further refined in Reference 3.

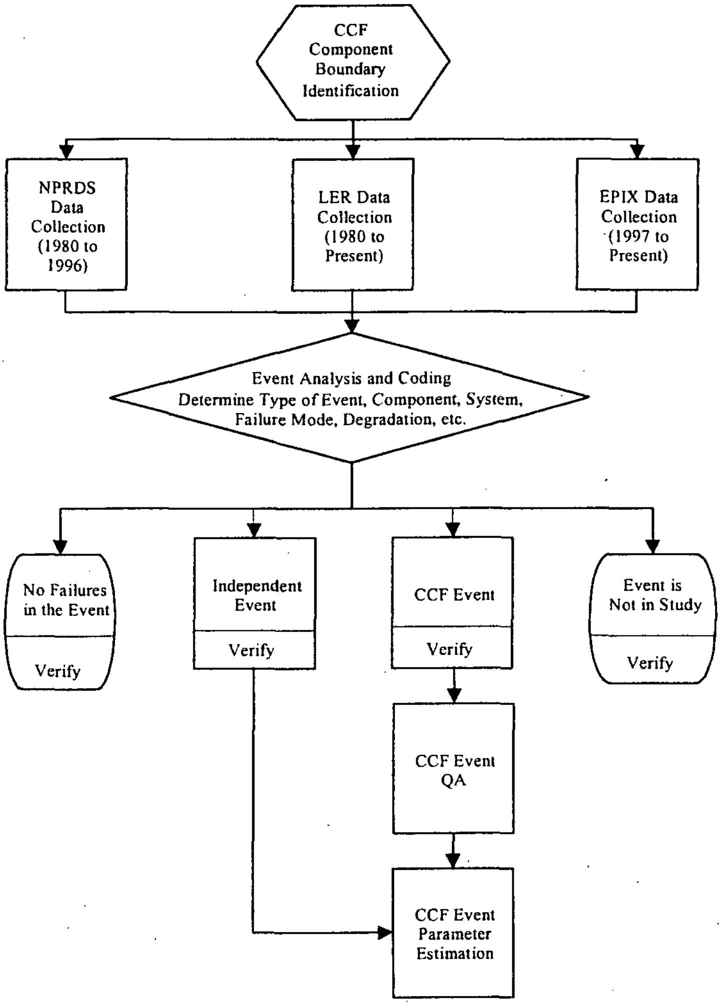
[a] Glossary terms are italicized at first use in the text.

Three data sources are used to select equipment failure reports to be reviewed for CCF event identification: the Nuclear Plant Reliability Data System (NPRDS), which contained component failure information prior to 1997; the Equipment Performance and Information Exchange (EPIX), which contains component failure information since 1997; and LER Search, which contains Licensee Event Reports (LERs). All events that meet the above criteria are identified as CCF events and are included in the CCF database. The database contains CCFs beginning in 1980 and is continuously updated to remain current. In 1997, the NRC published NUREG/CR-6268, "Common-Cause Failure Database and Analysis System" (Refs. 4, 5, 6, and 7). Volume 1 presented an overview of the data collection and classification process. Volume 2 contained background information for the coders. The coding guidelines were presented in Volume 3. Volume 4 was the user's guide for the software system.

In May 1998, the NRC published NUREG/CR-5497, "Common-Cause Failure Parameter Estimations" (Ref. 8). In September 2003, the NRC started publishing the common-cause parameter estimations on the NRC web site. The parameter estimations file contains the same information, but is updated on a yearly basis. The web page containing the common-cause parameter estimations downloadable file is http://nrcoe.inel.gov/results/.

This report is an update of NUREG/CR-6268 and combines Volumes 1, 2, and 3. The material has been updated to include the coding guidance applicable to EPIX. It also contains corrections and changes that have been made to the data collection and coding process. Figure 1-1 shows the steps in the data analysis process: collection of source data, identification of CCF events, coding of CCF events, database quality assurance, data analysis, and parameter estimation.

Section 2 of this report presents the definition of common-cause failures. Section 3 contains the description of the basic concepts for coding the CCF events. Section 4 provides an overview of the CCF data analysis process. The detailed coding guidance is presented in Section 5, and Section 6 contains examples of coded events. Section 7 provides an overview of the quantification process. CCF parameter estimation is contained in Section 8. Section 9 is a glossary. Section 10 lists the references.



CCF Component Boundary Identification
NPRDS Data Collection (1980 to 1996)
LER Data Collection (1980 to Present)
EPIX Data Collection (1997 to Present)
Event Analysis and Coding Determine Type of Event, Component, System, Failure Mode, Degradation, etc.
No Failures in the Event
Verify
Independent Event
Verify
CCF Event
Verify
Event is Not in Study
Verify
CCF Event QA
CCF Event Parameter Estimation

Figure 1-1. CCF data analysis process.

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, a definition of a dependent event is provided here . To simplify the presentation, consider two failure events, A and B.

Events A and B are said to be *dependent events* if

$$\begin{aligned} P[A \cap B] &= P[B \mid A]P[A] \\ &= P[A \mid B]P[B] \\ &\neq P[A]P[B] \end{aligned} \qquad (2\text{-}1)$$

where P[*X*] denotes 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, the 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 caused by 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 sub-classes of intrinsic dependencies depending on the type of influence that components have on each other. The sub-classifications 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
  - 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. The valve failure causes the pump to fail when a start signal is generated because of flashing in the suction line from a lack of flow. Because 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, 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 such as 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 failures from 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 that 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 CCFs.

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 25 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 PRA. NUREG/CR-4780 (Ref. 2) 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, because of a shared cause. Consistent with current practices in reliability analysis systems modeling, Reference 2 excludes failure or unavailability of other components as a shared cause of a CCF event. This is particularly 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 2, 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*, or (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 setpoints were set too high. The setpoint 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 because of 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 (Ref. 2) 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. In addition, the reference to a time interval between failures acknowledges the reliability significance of these events. Multiple component failures from a shared cause, but without affecting mission requirements, in a period 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 CCF (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 failure cause, coupling factor, and defense) is provided in the following sections, including a coding system for each of these elements.

3.1 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. However, 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, NUREG/CR-5460 (Ref. 9) introduces the following concepts.

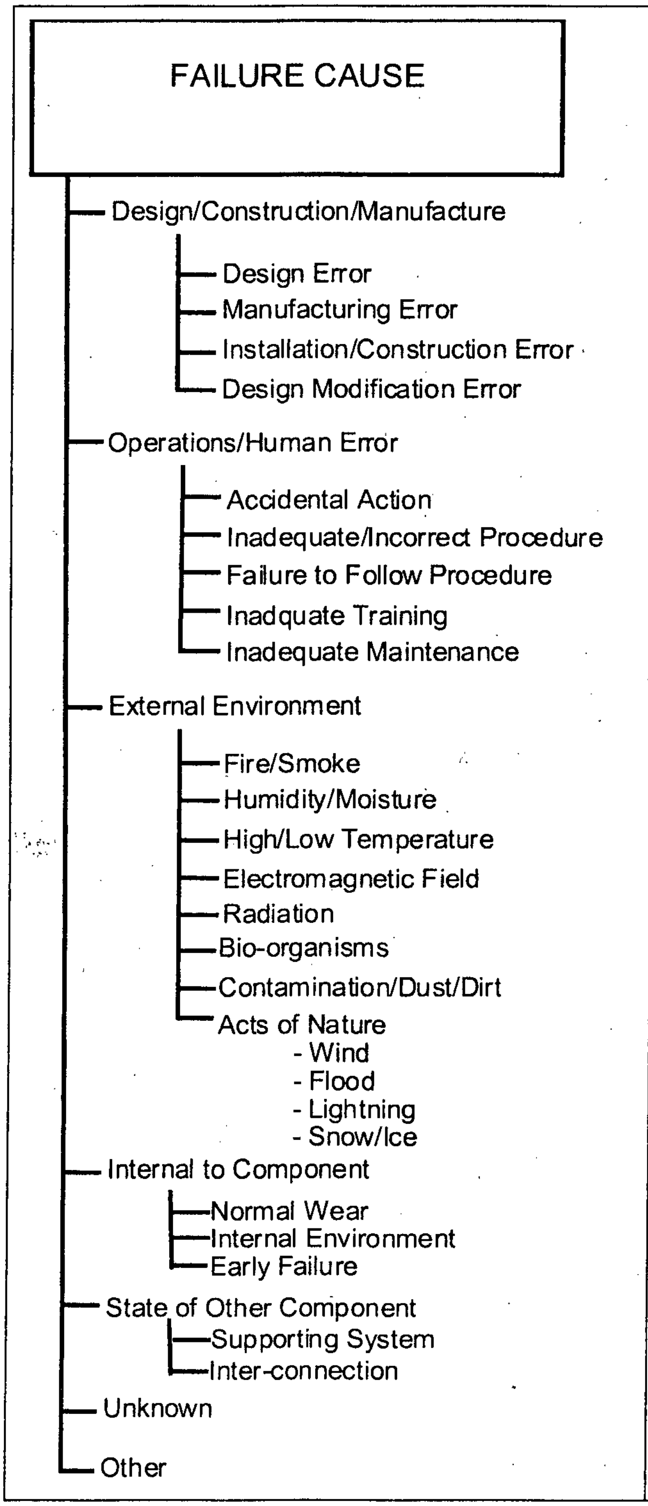
A *proximate cause* associated with a component failure event is a characterization of the condition that is readily identifiable as having led to the failure. In the pump example above, humidity could be identified as the proximate cause. The proximate cause is usually easy to identify and is adequate for identifying and classifying CCF events. However, the proximate cause can be regarded as a symptom of the failure cause and does not necessarily 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 aid in a systematic review of event data and are useful in analyzing component failures. For a single event, however, it is not always necessary to consider both concepts.

A conditioning event is an event that predisposes a component to fail or increases its susceptibility to fail. A conditioning event does not cause a failure. In the pump example, a conditioning event could have been the failure of maintenance personnel to seal the pump control cabinet properly after 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. A steam leak that led to high humidity in a room (and subsequent pump failure) would be considered 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 external event 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 that increase susceptibility to failure given the appropriate ensuing conditions.

The 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. The root cause may be determined to be the trigger event or the conditioning event. Often, failure investigations do not determine the root causes of failures even though this determination is crucial for judging defense adequacy. Additionally, the utility failure reports (LERs, EPIX reports, and NPRDS reports) often do not identify the actual root cause. Therefore, the failure cause coded into the CCF database is usually the proximate cause.

Causes are grouped into seven categories, which are then subdivided to provide a means of recording more detailed information when available. This failure cause classification scheme can be used for either the root or the proximate cause. The specific CCF database failure cause codes are identified in Section 5.1.6. The major failure cause categories are shown in Figure 3-1.



Design/Construction/Manufacture Inadequacy. Encompasses actions and decisions taken during design, manufacture, or installation of components both before and after the plant is operational.

Operations/Human Error (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. It also includes 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.

External Environment. Represents causes related to a harsh external environment that is not within component design specifications. Specific mechanisms include electromagnetic interference, fire/ smoke, impact loads, moisture (sprays, floods, etc.), radiation, abnormally high or low temperature, and acts of nature.

Internal to Component. Associated with the 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 internal environment of a component. Specific mechanisms include erosion/ corrosion, vibration, internal contamination, fatigue, and wear-out/end of life.

State of Other Component. The component is functionally unavailable because of failure of a supporting component or system. For example, an air supply line to a valve breaks or a fuse in a control circuit blows. CCF events exclude those events that have dependencies that would reasonably be expected to be modeled in an individual plant examination or PRA.

Unknown. Used when the cause of the component state cannot be identified.

Other. Used when the cause cannot be attributed to any of the previous cause categories. This category is most frequently used for cases of setpoint drift.

Figure 3-1. Proximate failure causes hierarchy.

3.2 Coupling Factors

As described earlier, for failures to originate from the same cause and 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 for a PRA mission. 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, operation, maintenance, and test procedures.

The report "On Quantitative Analysis of Common-cause Failure Data for Plant-Specific Probabilistic Safety Assessments" (Ref. 10) presents a coupling factor classification system, which is used as a systematic and consistent method for classifying coupling factors of multiple component unavailability. 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 five major classes:

- Quality based
- Design based
- Maintenance based
- Operation based
- Environment based.

These five classes are divided into subcategories to provide more detail for important parameters and attributes (see Figure 3-2). The multi-layered coding approach acknowledges that often during classification only major categories are identified because event descriptions do not have enough detail to allow distinction of subcategories. Details of the database coding system and coding guidance for coupling factors are contained in Section 5.1.14.

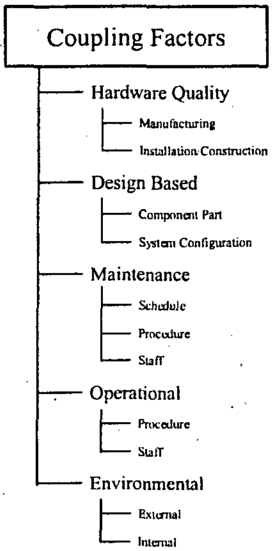


Figure 3-2. Categories for coupling factors.

3.2.1 Quality Based

Quality coupling factors refer to characteristics introduced as common elements for the quality of the hardware and include the following:

- Manufacturing Attributes. Refers to the same manufacturing staff, quality control procedure, manufacturing method, and material.

  Example: 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). Refers to the same construction/installation staff, construction/installation procedure, construction/installation testing/verification procedure, and construction/installation schedule.

Example: A reactor core isolation cooling (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 high-pressure coolant injection (HPCI) turbine.

3.2.2 Design Based

Design coupling factors result from common characteristics among components determined at the hardware 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 represent features within the boundary of each component. The following are coupling factors in the design category:

- System Layout/Configuration. Refers to the arrangement of components to form a system.

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

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

- Component Internal Parts. Refers to characteristics that could lead to several components failing because of the failure of similar internal parts or sub-components. This category is used when investigating the root cause of component failures and when the investigation is limited to identifying the sub-components or piece-part at fault, rather than the root cause of failure of the piece-part.

  Example: 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.

  Example: During normal operations, it was found that two AFW 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.

3.2.3 Maintenance Based

The maintenance based coupling factors propagate a failure mechanism from identical maintenance program characteristics among several components. The categories of maintenance based coupling factors are

- Maintenance/Test/Calibration Schedule. Refers to the maintenance/test/calibration activities on multiple components being performed simultaneously or sequentially during the same event.

  Example: 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 breakers were called on to operate. The maintenance requirements or cleaning schedules had not been established or identified as being necessary.

- Maintenance/Test/Calibration Procedures. Refers to 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.

  Example: During surveillance testing, two of five 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. The valves were bench tested to ensure operability before installation.

- Maintenance/Test/Calibration Staff. Refers to the same maintenance/test/calibration team being in charge of maintaining multiple systems/components.

  Example: Component cooling water (CCW) pump C sounded a high bearing temperature alarm. 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.

3.2.4 Operation Based

The operation based coupling factors propagate a failure mechanism from identical operational characteristics among several components. The categories of operation based coupling factors are

- Operating Procedure. 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 as shown in the first example. 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 second example. In other cases, a common procedure results in failure or multiple failures of multiple trains as demonstrated by the third example.

  Example: Two AFW 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 because of an error in the procedure.

  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. Mis-positioning the valves was due to operator error and an incomplete procedure.

  Example: Due to procedure and personnel errors, the nitrogen for the air-operated valves on two trains of the AFW 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.

- Operating Staff. 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.

  Example: 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 information that is more detailed and the operator training was enhanced on operating the trip devices.

3.2.5 Environment Based

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

- External Environment. Refers to all redundant systems/components exposed to the same external environmental stresses (e.g., flood, fire, high humidity, and earthquake). The impact of several of these environmental stresses is normally modeled explicitly in current PRAs (by analyzing the phenomena involved and incorporating their impact into the plant/system models). Other environmental causes such as high humidity and temperature fluctuations are typically considered in CCF analysis and treated parametrically.

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

- Internal Environment. Refers to commonality of multiple components in terms of the medium of their operation such as internal fluids (water, lube oil, gas, etc.).

  Example: Three of four service water pumps failed because of wear causing a high pump vibration. The ocean is the suction source for the pumps, and the failures were caused by excessive quantities of abrasive particles in the water. The pumps were replaced.

3.3 Defense Mechanisms

To understand a defense strategy against a CCF event, it is necessary to understand that defending against a CCF event is no different than defending against an independent failure that has a single root cause, except that more than one failure has occurred and the failures are related through a coupling mechanism. 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 defending against the CCF coupling factors. A summary of the defenses is provided in Table 3-1.

There are three methods of defense against a CCF: (1) defend against the failure proximate cause, (2) defend against the CCF coupling factor, or (3) defend against both items 1 and 2. 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. 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, a 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. For coupling factors, a defense strategy typically includes diversity (functional, equipment, and staff), barriers, and staggered testing and maintenance. With this defense strategy, component failures may occur that may not be related to any other failures.

A defense strategy addressing both the proximate cause and coupling factor is the most comprehensive.

Table 3-1. Defense mechanisms.

Defense Mechanism	Description
Functional Barrier	A CCF event could be prevented by modification of the equipment functional interconnections. Defenses involving system or component design changes would fall under this category.
Physical Barrier	A physical restriction, barrier, or separation could have prevented a CCF. An example would be installation of a watertight door to preclude flooding of an equipment room.
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. This would include modifications such as staggered testing and maintenance/operation staff diversity.
Component Identification	Improvements in component identification, especially between identical trains in a system and similar systems in multi-plant facilities. Examples of this would be more visible equipment identification, bar coding, and color-coding.
Diversity	A 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. THE CCF DATA ANALYSIS PROCESS

The CCF data analysis process consists of six activities: identification of analysis boundaries, data collection, failure event analysis and data coding, independent quality assurance verification, and CCF parameter estimation. Most of these activities are discussed in the following sections. Data coding is discussed in Section 5; CCF parameter estimation is discussed in Section 8. Figure 1-1 shows the major steps in the CCF data analysis process.

4.1 Identification of Analysis Boundaries

The initial step in the process is to identify the boundaries of the analysis, including the plant systems and components to be analyzed and operational event boundaries. The system and component combinations that have been selected for analysis are those addressed in PRA modeling for which CCF parameters are needed.

The data in the CCF database was coded based on predefined component boundaries that may include numerous sub-components. Component boundaries were defined before the data review so that each data analyst can consistently identify failure reports that should be included within a single component analysis. Examples of multiple sub-components within a component boundary include the actuator, valve, and power supply circuit breaker in a motor-operated valve (MOV) component; the turbine and pump for a turbine-driven pump component; and the engine, generator, starting/control air, and output breaker for an emergency diesel generator (EDG) component. Systems currently included in the CCF database and the boundaries for these components are described in detail in Section 5.1.5 of this report.

The system success criteria were identified by defining system and component *failure modes*. These are descriptions of how the system and components within the system are required to operate and accomplish their safety or PRA-specific mission. The failure modes defined were those that correspond primarily to the ones used in PRAs. For example, the safety function of a pump is to start on specific demand criteria and then run for a given length of time (mission time). Pump failure to start includes events such as the motor circuit breaker not racked in or failure to achieve rated pressure and flow. Pump failure to run events include failures such as erratic speed control, lubrication system problems, or high vibration that may prevent operation for the full duration of mission time. Analysts determine the failure modes for both the CCF events and the independent failures. The applicable failure modes for each component are defined in Section 5.1.13 of this report.

The component and system combinations are referred to as a *common-cause component group* (CCCG). The number of components in a CCCG is referred to as the size of the group, the CCCG size, or the redundancy level. Each CCCG (e.g., EDGs, AFW air-operated valves [AOVs]) is unique in the application of system and component boundaries, definition of failure, and the applicable failure modes. Before reviewing the failure records for identification of CCF events, it is necessary to understand the system configuration at each plant. Understanding the configuration enables the analyst to properly interpret the event and determine the impact of the reported failure on the system and component operability with respect to the PRA mission. The system configurations were determined using plant drawings, information in the plant final safety analysis reports, "Overview and Comparison of U.S. Commercial Nuclear Power Plants" (Ref. 11), and other available sources. The system configuration analysis consists of identifying the number of trains involved, the number of each type of component (CCCG), and component configuration.

Before performing any data searches and downloads, the analysts established the CCCG boundaries and defined the applicable failure modes to ensure that the data were properly collected and consistently analyzed. For example, the AFW pump boundary includes the driver (motor and circuit breaker or turbine and turbine governor) and the mechanical portion of the pump. Examples of possible failure events for each component set were given to the data analyst to assist in determining the applicability of the reported failure event to the CCF study. When a licensee reported degradation of a component, the analyst had to determine the effect of the degradation on the actual operability of the component. For example, failure of one indicator light on a valve position indicator was determined not to be a failure of the valve. Conversely, an incorrectly positioned pump circuit breaker that would have prevented a successful pump start was considered a failure, although the deficiency was identified before an actual demand.

4.2 Data Collection

After identifying the analysis boundaries, the next step is to perform searches for events using available data sources. The sources of component failure data most readily available to the NRC were the NPRDS failure reports, which were replaced by EPIX failure reports, and LERs. For the first data searches, sophisticated algorithms were developed to locate and pre-process event data from NPRDS and LERs to compile *potential CCF* events. The current updates are of much smaller scope. Routine searches are performed that filter EPIX data to obtain failure reports for components of interest to the CCF study. All LERs submitted by licensees are reviewed for events applicable to the CCF program as well as other ongoing programs at the INL pertaining to plant performance indicators, system reliability studies, and initiating event studies.

The NPRDS and EPIX reports contain detailed information about the failure of a single component; thus, they must be considered by groups of two or more records with specific characteristics to constitute CCF events. Conversely, LERs contain information about more complex plant events, and, because of the reporting criteria, often contain information about simultaneous failures in a single report.

4.3 Event Analysis

Once the event data are collected, data analysts read the LER and the NPRDS or EPIX report narratives of events to determine the system, component, failure mode, degree of degradation, and plant status. Event records that either have no failure or do not involve a component included in the CCF study are marked either NOF (no failure) or NIS (not in scope). The LER events are then compared to NPRDS or EPIX events to eliminate any duplication of events.

Once each failure record is categorized, all valid data are grouped by plant, system, component, failure mode, and failure *date*. The grouping is to assist the analyst in identifying NPRDS/EPIX/LER failure reports that occur within a specified time interval and may be associated with a CCF event.

The failure date for each report is compared to the failure date for all other failure reports at that plant to determine whether the failure date for one or more reports falls within the PRA mission time or the testing interval (plus the allowed 25%), as applicable per the method of detection. All reports within the applicable period are considered a possible CCF event and are grouped together for narrative screening. More discussion of this *timing factor* is in Section 5.1.7.

As part of the data grouping, two filters are applied to failure data to identify failure reports that do not fit the CCF event definition. If there is only one failure in the data set, then it is coded as an independent failure. If all failures in a group involve the same component, they are all coded as independent failures because there must be failures of at least two different components to qualify as a CCF event. In addition, for the specified period, only one failure of each component in the CCCG is counted for a CCF event; otherwise, counting multiple failures of one or more components in the CCCG would make the event appear to be more severe. For example, if two MOVs within a CCCG size of six each failed three times and six failures were counted in the CCF event, it would appear that the CCF event involved failure of all valves in the group. However, in this example it may be acceptable to classify the six failures into more than one CCF event, depending on the timing of the failures for each valve.

Groups of failures are identified as CCF events if they meet the following criteria:

1. Two or more similar components have failed or are degraded. The failures occurred on demand, during testing, or in situations where the equipment would have failed had it been called upon to operate.

2. The period of the failures is within or near the PRA mission time. For standby equipment, the time interval is assumed to be the surveillance testing interval plus 25%.

3. The failures share a single cause and are linked by a coupling mechanism.

4. The equipment failures are not caused by the failure of equipment outside the established component boundary, such as cooling water or AC power. These failures are dependent but are not CCF events.

Failure of shared equipment (e.g., common cooling water or AC power systems) is not considered a CCF event because these events are usually modeled explicitly in the *reliability logic models*. Another convention adopted in the initial effort of this project is that similar failures within a short time interval in different power plants of a multiple unit power plant site are not considered a CCF event. This is because an individual plant design typically does not rely on use of systems from another unit. Exceptions to this are the EDGs and ultimate heat sinks. In cases where similar failures (e.g., all four EDGs at a two-unit site with the same defective design) are detected at multiple plants, a CCF event is entered into the database for each unit affected.

After all CCF events have been identified, they are entered into the CCF database. Section 5.1 describes the criteria for coding events into the CCF database. Independent failure events are coded into the independent failure database and counted because they are used in the overall CCF parameter estimation, as described in Section 5.2. Independent failure event data must be provided by system, component, failure mode, and docket. This information is determined for each independent failure identified during the review of the NPRDS, EPIX, and LER data. The NPRDS and EPIX failure reports and LERs for all events collected in the data searches are stored for quality assurance tractability.

4.4 Data Loading

All of the data analysis takes place external to the CCF database so that un-reviewed data are not released. The data-loading step adds qualified data to the CCF database. After the CCF events have been reviewed, comments resolved, and duplicate events removed, the CCF and independent events are loaded into the CCF database.

4.5 Quality Assurance

The primary goal of CCF quality assurance is to ensure consistency and accuracy in the data analysis and CCF event coding. The major steps of CCF analysis (data handling, screening, and coding activities) are based on engineering judgment, which all have a potential for error. The quality assurance process for CCF data includes (1) INL coding and review by PRA qualified data analysts and (2) independent quality assurance verification by a subcontractor not at the INL. A second INL data analyst evaluates every coded CCF event to ensure proper identification of the CCF event, verification of coding accuracy, and consideration of appropriate PRA concepts. The two data analysts resolve any differences between the first and second coding before data acceptance. During failure data analysis to identify CCF events, a large number of failure reports are downloaded and reviewed. To ensure that the failure report review is auditable and that the findings can be reproduced, all data for each system/component study are maintained. Included are

- All NPRDS failure records
- All EPIX failure records
- All LERs
- Coding disposition of each record (e.g., CCF, independent, or no failure)
- Quality assurance comments.

5. EVENT CODING GUIDANCE

This section provides guidance for the analyst for both CCF events and independent events.

5.1 CCF Event Coding

This sub-section describes the information coded into each CCF event data field and presents associated codes for most fields. Sample CCF coding forms are provided in Section 6, with several coding examples.

5.1.1 Event Name

The event name is a unique character string used to identify each CCF event. The format is

S-DDD-YY-####-FM

where

S = source document where the CCF event was identified (N represents NPRDS, L represents LER, and E represents EPIX)

DDD = plant's docket number

YY = year of the event

= sequential four digit event number assigned by the CCF system administrator

FM = two-character code for the failure mode of the event.

Detailed guidance regarding failure modes applicable to systems and components and a complete list of failure mode codes is contained in Section 5.1.13.

5.1.2 Plant Name

The plant name is the name of the nuclear power plant where the CCF event occurred. The full name is entered when the data are loaded into the database.

5.1.3 Power Level

The power field contains the plant power level at the time of the CCF event as a percentage of full power. For CCF events identified from NPRDS or EPIX, this information is not always available and the field may be left blank. At least two NPRDS or EPIX records are required to define a CCF event. If the power level identified for both failures is conflicting, the power reported for the first event is used. For CCF events identified from LERs, the power level is given in Block 10 on the LER form; this number may be changed if information within the LER contradicts it. If it is known that the event occurred at power but the actual power level is not given, 100% is used.

5.1.4 Event Title

The title field provides a 60-character space for a title or short description of the event.

5.1.5 System

System codes identify groups of components that work together to perform a specific function. The system code used in event coding represents the group that includes the failed components. The system codes are listed in Table 5-1.

5.1.6 Proximate Cause

The proximate cause field identifies the reason the components failed. Most failure reports address an immediate cause and an underlying cause. The appropriate code is the one representing the common-cause or, if all levels of causes are common, the most readily identifiable or proximate cause. The proximate cause codes and their descriptions are shown in Table 5-2. A detailed discussion of failure causes is contained in Section 3.1 of this report.

Table 5-1. CCF system codes.

Code	System Description[a]
ACP	AC power distribution
AFW	Auxiliary feedwater
CSS	Containment spray system
CVR	Containment vacuum relief
DCP	DC power
EPS	Emergency power system
ESW	Emergency/essential service water
HCI	High-pressure coolant injection (BWR)
HCS	High-pressure core spray
HPI	High-pressure safety injection (PWR)
ISO	Isolation condenser
LCS	Low-pressure core spray
MSS	Main steam system (applies to the steam generator and steam lines at a PWR and the boiler vessel and steam lines at a BWR)
RCI	Reactor core isolation cooling
RCS	Reactor coolant system
RHR	Residual heat removal (this includes the low pressure coolant injection and the low pressure injection systems in both BWRs and PWRs)
RPS	Reactor protection
SDC	Shutdown cooling system (only used for the stand-alone shutdown cooling system in some BWRs)
SLC	Standby liquid control

a. BWR = boiling water reactor, PWR = pressurized water reactor.

Table 5-2. Proximate cause codes.

Code	Cause	Description
DC	Construction/installation error or inadequacy	A construction or installation error was made during the original or modification installation, including an incorrect component or material installed or specification of incorrect component or material
DE	Design error or inadequacy	A design error was made
DM	Manufacturing error or inadequacy	A manufacturing error was made during component manufacture
HA	Accidental action (unintentional or undesired human errors)	A human error (during the performance of an activity) resulted in an unintentional or undesired action
HD	Wrong procedure followed	The wrong procedure was followed
HP	Failure to follow procedure	The correct procedure was not followed; applies to • Calibration/test staff • Construction/test staff • Maintenance staff • Operations staff • Other plant staff
HT	Inadequate training	Training was inadequate
IC	Internal to component, piece-part	The cause of the failure is the result of a failure internal to the component that failed; applies to • Erosion/corrosion • Equipment fatigue • Wear out/end of life • Internal contamination
IE	Ambient environmental stress	The cause of the failure is the result of an environmental condition from the location of the component; applies to • Chemical reactions • Electromagnetic interference • Fire/smoke • Impact loads • Moisture (spray, flood, etc.) • Acts of nature • Radiation (irradiation) • Temperature (abnormally high or low) • Vibration loads (excluding seismic events)

Table 5-2. (continued).

Code	Cause	Description
OT	Other (stated cause does not fit other categories)	The cause of the failure is provided but it does not meet any one of the descriptions
PA	Inadequate procedure	The cause of the failure is the result of an inadequate procedure; applies to • Calibration/test procedure • Administrative • Maintenance • Operational • Construction/modification • Other
QI	Setpoint drift	The cause of the failure is the result of setpoint drift
QP	State of other component	The cause of the failure is the result of a component state not associated with the component that failed
U	Unknown	The cause of the failure is not known

5.1.7 Timing Factor

This is a measure of how close in time multiple failures occurred. In general, the goal of the timing factor is to assign a weighting factor to the CCF event based on the time between individual failures. The acceptable input for this field is a decimal number from 0.1 to 1.0.

The definition of timing factor is presented in two parts based on whether failures are announced or unannounced. The two classes of failures are the following:

- Announced (Overt) Failures. Failures were announced, inspected for, or monitored before a demand or failure. It includes failures of operating components and self-revealing failures of components in standby state (e.g., low cooling water flow, low tank level, low oil level, or high exhaust temperature). If any of these conditions occurs during scheduled testing, the Unannounced or Latent failure class is appropriate. Announced failures and degradations are usually detected immediately (e.g., an operating pump alarms and is shut down by procedure during a non-test demand). Thus, the probability of failure is related to a mission time. Hence, the assignment of a value for the timing factor should be related to the mission time.

- Unannounced (Latent) Failures. Covers failures of components in a standby state that are not announced but are subsequently detected by testing or a valid demand (e.g., pump does not start on demand, EDG fails to produce required voltage on a test, residual heat removal [RHR] pump exhibits low suction pressure during a test, or a valve fails to completely open on a demand). Unannounced failures occur in equipment that is demanded without a prior indication of failure (e.g., standby safety pumps, valves being opened). Failure probabilities for such components are usually estimated by the number of failures and number of demands. Here, the assignment of a value should be based on the opportunity for a demand to detect the component degradations. Two basic means of detection are valid operational demands and surveillance testing.

As a simple but conservative rule for CCF events containing more than two components, the maximum value of timing factor values for each pair of consecutive component degradations in the event should be assigned to the event.

5.1.7.1 Announced Failures. For announced failures, the timing factor is based on a time-based model. Thus, the timing factor is assigned values based upon a PRA mission time (the period of time the component is usually required to perform its function in a PRA or individual plant examination [IPE], usually 24 hours). The following classifications may be used for two consecutive degradations of two components contained in a CCF event:

- High (1.0): The component events are separated by no more than the PRA mission time.
- Medium (0.5): The component events did not occur within the PRA mission time and two times the PRA mission time.
- Low (0.1): The component events are separated by more than two times the PRA mission time and less than three times the PRA mission time.
- Not CCF: More than three times the PRA mission time or during the interval between the component events, the component (which was detected, failed, or degraded later) has undergone maintenance, overhaul, or other action that can be regarded as a renewal event for the failure mechanisms. (Note: In this case, the event is not classified as a CCF event.)

The specification of the time intervals based on the PRA mission time indicates that there was one success between failures for "medium" events and two successes between failures for "low" events.

5.1.7.2 Unannounced Failures. Unannounced failures are related to two (redundant) component degradations (failure events) occurring and being detected during a demand situation. In the following, the term "challenge" means an opportunity to detect the considered failure mechanism with high probability. Test and demand events are the primary challenges. The following classification is for two consecutive failures/degradations of two components that are members of a CCF event:

- High (1.0): During the time interval between the degradation events of components 1 and 2, there was no successful challenge to component 2. For example
  - Two RHR pumps are tested and both fail to run for the required period of time. The tests are performed within the same surveillance cycle. (Success of other RHR pumps does not impact the timing of the two recorded failures.)
  - Two AFW MOVs fail to open during a valid operational demand. The demands are not separated by a valid success of one of the two MOVs before failure. (Success of another MOV does not provide a valid challenge.)
- Medium (0.5): During the time interval between the degradation events of components 1 and 2, there was one and only one successful challenge of component 2. For example
  - The EDGs were tested during testing cycle 1. One failure of the "A" EDG is recorded. (No failure records are found for the other EDGs.) In the next testing cycle, one failure of the "B" EDG is recorded.
  - The AFW pumps are all demanded during a scram event. The "A" AFW pump fails to start. Later, another demand is made of the AFW system. The "B" AFW pump fails to start. This set of circumstances may lead the analyst to code a CCF event with a "medium" timing factor if the analyst believes that no other successful demands of the AFW system occurred between these two recorded events. This will mostly fall on the calendar time

between the events. Very short times (< day, < week, etc.) may warrant this category.

- Low (0.1): During the time interval between the degradation events of components 1 and 2, there were two and only two successful challenges of component 2. For example
  - The EDGs were tested during testing cycle 1. One failure of the "A" EDG is recorded. (No failure records are found for the other EDGs.) In the next testing cycle, no failures of the EDGs are recorded. In the third testing cycle, one failure of the "B" EDG is recorded.
  - The AFW pumps are all demanded during a scram event. The "A" AFW pump fails to start. Later, another demand is made of the AFW system in which no failures are recorded. Later, another demand is made of the AFW system. The "B" AFW pump fails to start. This set of circumstances may lead the analyst to code a CCF event with a "low" timing factor if the analyst believes that no other successful demands of the AFW system occurred between these three recorded events. This will mostly fall on the calendar time between the events. Very short times (< day, < week, etc.) may warrant this category.
- Not CCF: During the interval between the degradation events of components 1 and 2, there were more than two successful challenges of component 2. (Note: In this case, the event is not classified as a CCF event.)

If the component time histories are not known in detail regarding actual test and maintenance timing and real demands, an assumed pattern can be used based on test interval and scheme of possible test staggering, time-based maintenance pattern, and typical pattern of demands. In practice, the analyst will have to have a very strong sense that something is going on. For example, the failure mechanism is very likely to occur within very few demands. The more successes between failures required, the more likely the analyst is to record the events as a CCF event.

The above classification scheme is independent of the type of testing scheme (e.g., staggered, sequential) and technical specifications considerations (testing redundant components when a component failure is detected). The key discriminating factor is the spacing of failures and opportunities to detect failures of the two components.

The majority of safety-related systems and components considered for CCF event analysis are normally in a standby condition. This implies that most system operation occurs during testing, which is when a large portion of the failures are discovered. The inservice testing requirements of 10 CFR 50.55a and the containment penetration leakage testing requirements of 10 CFR 50, Appendix J, govern most safety-related component testing (Refs. 12 and 13). Licensees are allowed to extend the testing interval by up to 25% to allow for scheduling. Testing intervals for each component set are considered individually. For example, EDGs have monthly testing requirements that are specified in the technical specifications. Considering the 25% extension, it is recommended that 39 days be used for EDG failure report grouping.

In addition, for most standby safety system components, technical specifications and limiting conditions of operation require that when a test or other source reveals that a component is inoperable, the other similar redundant components must be tested. If it is noted that the first failure triggers testing of the other components, then the next cycle may assume a success in between the failures.

5.1.8 Component

The component field describes the equipment that experienced the CCF event. The codes reflect operational system components that are normally modeled in a PRA. Table 5-3 provides a listing of available component codes and component descriptions.

Table 5-3. Component codes.

Code	Component	Description
AOV	Air operated valve, water	Controls flow of water
BAT	Battery	Provides DC power
BCH	Battery charger	Provides recharging DC power to batteries and DC buses
CB2	Reactor protection trip circuit breakers	Provides electrical power connection between power source and load, or opens on electrical fault or demand
CB3	6.9 k VAC circuit breakers	Provides electrical power connection between power source and load, or opens on electrical fault or demand
CB4	4160 V AC circuit breakers	Provides electrical power connection between power source and load, or opens on electrical fault or demand
CB5	480 V AC circuit breakers	Provides electrical power connection between power source and load, or opens on electrical fault or demand
CB7	DC distribution circuit breakers	Provides electrical power connection between power source and load, or opens on electrical fault or demand
CB8	13.2 kV circuit breaker	Provides electrical power connection between power source and load, or opens on electrical fault or demand
CKB	Vacuum breaker check valve	Closes or opens to isolate or permit flow on specific differential pressure
CKS	Stop check valve	Closes or opens to isolate or permit flow on specific differential pressure
CKV	Check valve	Closes or opens to isolate or permit flow on specific differential pressure
EDG	Emergency diesel generator	Provides electrical power with a diesel engine driver
HSV	Hydraulically operated main steam isolation valve	Hydraulically operated main steam isolation valve
HTX	Heat exchanger	Provides for heat transfer, allows flow, and contains process fluid
MDP	Motor-driven pump	Pump with an electrical driver
MOV	Motor-operated valve, water	Isolates water or permits flow on demand; operated by motor operator
MSV	Main Steam Isolation Valve	Air- or gas-operated main steam isolation valve
RAV	Air operated valve, recirculation	Controls flow of water through pump minimum flow recirculation lines
RVA	Relief valve, air or nitrogen operated	Provides process system pressure relief; operated by valve operator
RVE	Relief valve, solenoid operated	Provides process system pressure relief; operated by valve operator
RVH	Relief valve, hydraulic operator	Provides process system pressure relief; operated by valve operator
RVM	Relief valve, motor-operated	Provides process system pressure relief; operated by valve operator
STR	Strainer, main pump suction or discharge	Filters debris in main piping line
SVV	Safety valve	Provides process system pressure relief; operated by system pressure
TAV	Air operated valve, steam	Controls flow of steam to pump turbine
TMV	Motor-operated valve, steam	Isolates or permits steam flow to pump turbine; operated by motor operator

5.1.9 Sub-Component and Piece-Part

The sub-component and piece-part fields further identify which parts of the component failed. The list of sub-components and piece-parts, is shown in Table 5-4.

5.1.10 Shock Type

This field describes the relationship of one component failure to another. The allowable codes are L (lethal) or NL (non-lethal). Given one failure, a lethal *shock* type means that all other components in the CCCG will always fail as well, independent of the group size. The coding of a shock type as lethal requires that the *shared cause factor* = 1.0, the timing factor = 1.0 and all components in the group failed, and all *p-values* = 1.0. A non-lethal shock type means the cause of failure may affect all components in a CCCG or a subset of the CCCG within the PRA mission time.

5.1.11 CCF Event Operational Status

The CCF event operational status field indicates when the CCF event occurred or could occur. Allowable codes for this field are provided in Table 5-5.

5.1.12 CCF Event Detection Operational Status

This field is used to indicate the plant operational status when the CCF event was detected. Table 5-6 provides the allowable codes.

5.1.13 Failure Mode

The failure mode field describes which function the components did not perform. Proper coding of the failure mode is essential because the CCF events are sorted by failure mode for parameter estimations. The failure mode codes are shown in Table 5-7, along with a short discussion of each failure mode code. The table identifies the applicable component for each failure mode because some failure modes depend on the component being coded. The boundary identification includes specific guidance on the use of failure modes and PRA considerations for the system and component of interest.

It is possible for a component to fail in multiple ways; therefore, a CCF event may have multiple failure modes. In these cases, only one failure mode code is entered with an event record. To track multiple failure modes, a CCF record is created for each failure mode. An example is a loss of lubrication event for a pump. In most cases, the pump would start and operate. However, because the pump would eventually seize and fail, the failure mode is failure to run. Another pump may suffer a catastrophic loss of lubrication that prevents a successful start and the failure mode would be failure to start. Two CCF records would be entered into the database, with the *failure mode applicability* of 0.5 for each event.

5.1.14 Coupling Factor

The coupling factor field describes the mechanism that ties multiple components together resulting in susceptibility to the same-shared cause to create the CCF. The allowable codes and their descriptions are presented in Table 5-8. A detailed discussion of coupling factors is contained in Section 3.2 of this report.

5.1.15 Event Type

The event type field indicates which events should be included in the parameter estimation. Some dependent events are explicitly modeled in other areas of a PRA while some CCF events are not modeled in a PRA because they do not contribute significantly to plant risk. Other CCF events need to be considered as CCF events in PRA analysis. The allowable codes and their descriptions are given in Table 5-9.

Table 5-4. Component group, sub-component, and piece-part listing.

Component Group	Component	Sub-Component/Type	Piece-Part
AOV	AOV	Actuator	Orifice
	TAV		Accumulator check valves
	RAV		Pressure regulator
			Instrument air
			Instrumentation & control
			Gasket/o-rings
			Diaphragm
			Bushings
			Air solenoid valve
			Stem
		Valve	Stem
			Valve body
BAT	BAT	Lead acid batteries	Cell
		Lithium batteries	Cell
BCH	BCH	AC breaker	Circuit breaker
			None
			Various
			Unknown
		Charger	Filter module
			Various
			Timer
			Silicon controlled rectifier
			Relay/contactor
			Power module
			None
			Gate module
			Firing module
			Voltage regulating module
			Current limiter module
			Control module
			Amplifier module
			Alarm module
			Fuse
			None
			Overcurrent relay
			Fuse
		DC breaker	Various
			Overvoltage relay
BKR	CB2	4160 Vac	Mechanical assembly
	CB3	480 Vac	UV trip assembly
	CB4	6.9 kVac	Stabs/connectors
	CB5		Spring charging motor
	CB6		Overcurrent relay
	CB7		Limit switch
	CB8		Latch assembly
			Instrumentation & control
			Closing coil
			Auxiliary contactor
			Arc chute
			Relay
			Fuse

Table 5-4. (continued).

Component Group	Component	Sub-Component/Type	Piece-Part
			Main contacts
		DC distribution	Control switch
			Mechanical assembly
			Overcurrent relay
		RPS trip breakers	Shunt trip
			Wires/connectors/board
			UV trip assembly
			Unknown
			Spring
			Mechanical assembly
			Latch assembly
			Auxiliary contactor
			Closing coil
			Relay
CKV	CKA	Valve	Hinge pin
	CKV		Various
	CKS		Unknown
	VAC		Stem
			Setpoint adjustment nut
			Seat & disk
			Seat
			Packing
			Hinge pin bearing/bushing
			Disk
			None
			Closure spring
			Disk anti-rotation device
			Disk nut/stud/pin
			Disk stop
			Gasket/seal
			Guide stud
			Hinge arm
			Body
EDG	EDG	Battery	Battery
		Breaker	Logic circuit
			Relay
			Switch
		Cooling	Miscellaneous
			Valve
			Heat exchanger
			Pump
			Piping
		Engine	Piping
			Valve
			Turbocharger
			Shaft
			Piston
			Miscellaneous
			Governor
			Fuel rack
			Fuel nozzles
			Bearing
			Sensors
		Exhaust	Valve

Table 5-4. (continued).

Component Group	Component	Sub-Component/Type	Piece-Part
		Fuel oil	Fuel rack
			Strainer
			Tank
			Valve
			Pump
			Miscellaneous
			Piping
		Generator	Casing
			Generator excitation
			Load sequencer
			Logic circuit
			Power resistor
			Relay
			Rotor
			Voltage regulator
		Instrumentation & control	Instrumentation
			Fuse
			Governor
			Load sequencer
			Miscellaneous
			Piping
			Relay
			Sensors
			Valve
			Voltage regulator
			Generator excitation
		Lube Oil	Tank
			Check valve
			Heat exchanger
		Starting	Valve
			Strainer
			Miscellaneous
			Motor
HTX		Heat exchanger	Head gasket
			None
			Piping
			Shell/baffles
			Tubes/tubesheet
			Various
MOV	MOV	Actuator	Torque switch
	TMV		Breaker
			Transmission
			Circuit
			Motor
			Limit switch
		Valve	Body
			Disk
			Packing
			Stem
MSV	MSV	Actuator	Stem
	HSV		Instrumentation & control
			Limit switch
			None
			O-rings/seals/gaskets

Table 5-4. (continued).

Component Group	Component	Sub-Component/Type	Piece-Part
			Pins/keys
			Pneumatic supply
			Relay
			Rupture disk
			Steam pilot
			Unknown
			Wiring
			Hydraulic plunger
			Solenoid pilot valve
			Actuator stanchions/guides
			Accumulator
			Actuator air piston
			Accumulator check valves
			Actuator linkage
			Hydraulic pilot valve
			Air metering valve
			Air pilot valve
			Control power
			Cylinder
			Fuse
			Hydraulic cylinders
			Hydraulic oil pumps
			Actuator guide screws
		Valve	Seat/disk
			Stuffing box
			Unknown
			Various
			Stem
			Poppet pilot assembly
			Packing/lubricant
			Disk
			Condensate drain
			Valve body
			Seat
PMP	PMP	Discharge	Check valve
	MDP		Piping
	TDP		Recirc
	MOT		Valve
		Driver	Bearing
			Supports
			Piping
			Packing/seals
			Motor
			Lubrication
			Breaker
			Instrumentation & control
		Pump	Packing
			Coupling
			Shaft
			Plunger/cylinder
			Packing/seals
			Bearing
			Impeller/wear rings
			Lubrication

Table 5-4. (continued).

Component Group	Component	Sub-Component/Type	Piece-Part
			Casing
			Breaker
		Suction	Valve
			Tank
			Strainer
			Piping
			Instrumentation & control
			Booster pump
SRV	RVA	Actuator	Packing
	RVE		Accumulator check valves
	RVH		Wires
	SVV		Unknown
			Tubing/fittings
			Spring
			Solenoid
			Seals/gaskets/o-rings
			Rings
			Pilot assembly
			Valve stem
			None
			Limit switches
			Instrumentation & control
			Gears
			Fuse
			Diaphragm
			Booster valve
			Air regulator/relay
			Air/nitrogen
			Nozzle rings
		Valve	Nozzle rings
			Valve yoke
			Valve stem
			Packing
			Guide bushing
			Bonnet drain
			Valve seat/disk
STR	SRS	Strainer	Various
	SRK		Backflush regulator
			Drive coupling
			Filters/screens
			Shear pin
			Strainer adjustment shoes
			Strainer basket
			Thrust collar
			Traveling screens

Table 5-5. Operating mode codes.

Code	Description
BO	The CCF event could occur during both power operations and shutdown conditions
OP	The CCF event could occur only during a power operation condition
SD	The CCF event could occur only during a shutdown operation condition

Table 5-6. Detection codes.

Code	Description
D	The event was detected during plant shutdown
O	The event was detected during power operations

Table 5-7. Failure mode codes.

Code	Description	Component	Discussion
CC	Fail to open (normally closed)	Circuit breaker, valve	A circuit breaker or valve does not open on demand
FR	Fail to run	Pump, EDGs	The component fails to continue running at rated conditions after reaching rated conditions
FS	Fail to start	Pump, EDGs	The component fails to start or reach rated conditions for the requirements at the time (test conditions may be different from operating conditions)
FX	Fail to stop	Pump, EDGs	The component fails to stop operating
HI	High voltage/ amperage output	Battery, charger	The component provides an output that is higher than designed
NO	No voltage/ amperage output	Battery, charger	A device, such as a battery or instrument, fails to provide an output signal
PG	No flow/plugged	Heat exchanger, strainer	Loss of flow or failure of a heat exchanger to transfer heat because of fouling or plugging
OO	Fail to close (normally open)	Circuit breaker, valve	A component fails to close within the required amount of time
SA	Spurious actuation	Circuit breaker, valve	A device trips to an unintended position because of an external cause (loose connection, lighting, human action)
VR	Fail to remain closed (detectable leakage)	Valve	A valve is leaking internally past the valve seat, with detectable system effect, including leakage in excess of technical specification or safety analysis limits; if evidence exists that the valve didn't close fully initially, the OO code is used

Table 5-8. Coupling factors.

Code	Description	Discussion
EE	Environment, external	Components are coupled by the external environment
EI	Environment, internal environment/working medium	The internal environment couples component failures
HDCP	Hardware design, component part (internal parts)	The same design and internal parts couples component failures
HDSC	Hardware design, system configuration (physical appearance)	Component failures are coupled by design features within the system in which they are located
HQIC	Hardware quality, installation/construction (initial or modification)	Component failures are coupled by installation or construction features, from initial installation, construction, or subsequent modifications
HQMM	Hardware quality, manufacturing	Component failures are coupled by hardware quality deficiencies from the manufacturing process
OMTC	Operational, maintenance/test schedule	Component failures are coupled by maintenance and test schedules
OMTP	Operational, maintenance/test procedure	Component failures are coupled by the same maintenance or test procedure
OMTS	Operational, maintenance/test staff	Component failures are coupled by maintenance staff personnel error
OOOP	Operational, operation procedure	Component failures are coupled by operations procedures
OOOS	Operational, operation staff	Component failures are coupled by operations staff personnel error

Table 5-9. CCF event types.

Code	Description	Discussion
CCF	CCF estimation	CCF events that are generally considered applicable to PRA CCF parametric modeling (e.g., the failure of both motors in an AFW pump system because of manufacturing flaws).
EXP	Explicitly modeled	Events that are modeled explicitly in system analyses include events caused by failure of support systems, cascade failures from system configuration, and certain types of operator actions. For example, a failure in the Engineered Safety Feature Actuation System caused the AFW pumps failure to start. This type of failure would be modeled as part of the Engineered Safety Feature Actuation System PRA model.
INS	Insignificant	Events involving failures or potential failures that do not have a significant impact on system performance and thus are not generally included in PRA models (e.g., component setpoint slightly outside of technical specification limits, packing leaks that were insignificant).

5.1.16 Failure Mode Applicability

Failure mode applicability represents the percentage of specific failure modes for multiple component failures involved in the CCF event. This is a weighting factor for parameter estimation for a CCF event involving multiple failure modes. Failure mode applicability is a decimal number from 0.0 to 1.0. If there is only one failure mode for multiple failure events, the failure mode applicability is 1.0 because only one failure mode resulted from all component failures. If there is more than one failure mode assigned to a single CCF event, the sum of failure mode applicabilities is equal to 1.0. Failure mode applicabilities for a multiple failure mode event is a percentage of failures affected by each failure mode. For example, if two pumps fail to start and one fails to run, the failure mode applicabilities are assigned 0.67 and 0.33, respectively.

5.1.17 Shared Cause Factor

By definition, a CCF event must result from a single, shared cause of failure. However, the event reports may not provide sufficient information to determine whether the multiple failures result from the same cause or different causes. Because of this, the analyst sometimes must make a subjective assessment about the potential of a shared cause. The shared cause factor allows the analyst to express a degree of assurance about the multiple failures resulting from the same cause. The acceptable input for this field is a decimal number from 0.1 to 1.0. To ensure consistency in the coding, 0.1, 0.5, and 1.0 are used. Guidance and examples are provided in the following:

1.0 Used when the analyst believes that the cause of the multiple failures is the same, often resulting in the same failure/degradation mechanism and affecting the same piece-parts in each of the components. The corrective action(s) taken for each of the components involved in the event is (are) also typically the same. The following illustrates an event with a shared cause factor of 1.0:

"Three turbine-driven steam-supply check valves failed to open. Investigation revealed similar internal damage to all three valves. The failures for each valve were due to steam system flow oscillations causing the valve discs to hammer against the seat. The oscillations were ultimately attributed to inadequate design. The valve internals were replaced, and a design review is being conducted to identify ways of reducing flow-induced oscillations."

Statements in the event report that indicate the same cause, failure mechanism, or failure symptoms are usually good indicators of a shared cause of failure. This is true even if little information is provided about the exact nature of the problem. Statements such as "investigation revealed similar damage to all three redundant valves," "loose screws found in five circuit breakers," and "several air-operated valves malfunctions because of moisture in the air supply," indicate a shared cause factor equal to 1.0.

Any information available that is not in the event narrative (the NPRDS or EPIX failure report or the LER abstract) is included in the Comments field.

0.5 This value is used when the event description does not directly indicate that multiple failures resulted from the same cause, involved the same failure mechanism, or affected the same piece-parts, but there is evidence that the underlying root cause of the multiple failures is the same. The following example illustrates a shared cause factor equal to 0.5:

"Binding was observed in two check valves. Wear of the hinge pin/pin bearing is suspected to have caused the binding of the valve disc, resulting in failure of the first valve. The hinge pins were binding in the second valve due to misalignment. Further investigation of the second valve failure revealed inadequate repair/maintenance instructions from the vendor and engineering department."

The event description presents two different causes of failure (wear and misalignment) for these valves. Therefore, these failures could be considered independent. However, it is clear that there is a programmatic deficiency associated with repair and maintenance of these valves. It is possible, for example, that the inadequate instructions from the vendor and engineering department resulted in the first valve being misaligned and the misalignment caused abnormal or excessive wear. It is also possible that the event descriptions were written by different mechanics and the difference in the cause description is simply a difference in their writing styles (one focused on the actual cause [misalignment], the other on the symptom [wear]). In either case, both valves would have failed because of misalignment, making this a CCF.

0.1 This value is used when the event description indicates that the multiple failures resulted from different causes, involved different failure mechanisms, or affected different piece-parts, but there is still some evidence that the underlying root cause of the multiple failures is the same. The following examples illustrate a shared cause factor equal to 0.1:

"Water was found in the lubricating oil for the motor of the RHR 'D' pump. The source of the water was a loose fitting at the motor cooling coil. The fitting was replaced."

"A severe seal water leak was observed at the RHR 'B' pump. The source of this leak was a missing ferrule in the seal water line purge fitting. The ferrule was possibly left out during a previous pump seal repair. A new pump seal fitting ferrule was installed."

These events involved different pump sub-components (motor cooling and seal water) and the specific causes of failure are different (loose fitting and missing ferrule). These are indications that the failures are independent. However, it can also be speculated that the utility has programmatic deficiencies (e.g., inadequate training and procedures) regarding water piping connections and fittings, particularly if there has been a history of similar events. If so, the root cause of the problem is lack of training, inadequate procedures, etc., making the cause of the multiple failures the same. Since this hypothesis is highly speculative, the shared cause factor is small.

5.1.18 CCF Event Level

The CCF event level field indicates whether events impact overall system operation or only affect specific components within the system. The allowable codes for this field and their descriptions are provided in Table 5-10.

5.1.19 Common-cause Component Group

This field indicates the size of the population that can be exposed to a CCF. The acceptable values for this field are integers from 2 to 16 with at least two being required to meet CCF event definition. If there are more than 16 components, 16 should be entered in the CCCG field and additional information should be included in the event comments. Each CCF event needs to be considered before assigning the CCCG. Some failures will not affect all similar components in the system, so the appropriate CCCG is the number of components susceptible to that specific failure event.

Table 5-10. CCF event levels.

Code	Description	Discussion
COM	Component Level	The CCF event is a component level failure (e.g., a CCF event that caused two valves in a single train of a three-train system to fail; in this example, the trains were available)
SYS	System Level	The CCF event is a system functional level failure (e.g., a CCF event that resulted in the failure of two trains of a three-train system)

5.1.20 Multiple Unit

This field is to indicate if the CCF event affects more than one power plant at a single site ("Y" or "N"). Very few events will be coded Y; most are for the EDGs. A CCF event will be coded for each unit, and both will have multi-unit = Y. Some licensees check operability of components at a second unit once they have found failures at one unit.

5.1.21 Defense Mechanism

This field describes the actions a licensee can take to eliminate the coupling factor and prevent the CCF event from recurring. The defense mechanism selection is based on an assessment of the coupling factor between the failures. The allowable defense mechanisms are provided in Table 5-11.

Table 5-11. Defense codes.

Code	Description	Discussion
DIV	Diversity	Increased diversity could have prevented a CCF; this includes diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.
FSB	Functional	A decoupling of a CCF event could have been accomplished if the equipment barrier (functional and/or physical interconnections) had been modified
IDE	Component identification	If the component identification had been modified by more clearly identifying equipment, a CCF event could have been prevented; examples of the modifications are better equipment identification, color coding, etc.
MAI	Maintenance staffing and scheduling	A maintenance program modification could have prevented a CCF; the modification includes items such as staggered testing and maintenance/operation staff diversity
MON	Monitoring/awareness	Increased monitoring, surveillance, or personnel training could have prevented a CCF
NON	No practical defense	No practical defense could be identified
PBR	Physical barrier	A physical restriction, barrier, or separation could have prevented a CCF
UKN	Unknown	Sufficient detail is not provided to make adequate defense mechanism identification

5.1.22 Safety Function

The safety function field represents the observed failure mode as it pertains to the safety function of the component as installed in the system. The allowable codes and their descriptions are given in Table 5-12.

Table 5-12. Safety function codes.

Code	Description	Discussion
FS	Fail-safe	Component failed and performed its safety function
NFS	Non-fail-safe	Normal safety function was impaired
UKN	Unknown	Safety function cannot be determined

5.1.23 Component Degradation Values

The *component degradation value* field indicates the extent of each component failure as a probability that the degree of degradation would have led to failure during system operation. If the shock type is "lethal," all components in the CCCG will have a degradation value equal to 1.0. The allowable values are decimal numbers from 0.0 to 1.0. There must be as many p-values as the number of components listed in the CCCG field. If some components are not degraded, their p-values are coded as 0.0, indicating no degradation. A potential failure (e.g., a design flaw that would have resulted in failure) will be coded as the actual degradation on the parallel failed component only if it is certain that the degradation would have occurred. For example, a wiring discrepancy that would have prevented a pump start is coded as p = 1.0 because it is certain the pump would not have started and it is a complete failure. If the CCF event only affected two of three pumps, $p_3 = 0.0$. Coding guidance for different values follows:

1.0 The component has completely failed and will not perform its specific function. For example, if a pump will not start, the pump has completely failed, and degradation is complete.

0.5 The component is capable of performing some portion of the safety function and is only partially degraded. For example, high bearing temperatures on a pump will not completely disable a pump but will increase the potential for failing within the duration of the PRA mission.

0.1 The component is only slightly degraded but component safety function is impacted. An example would be a safety valve with setpoint drift in excess of technical specification but still within the bounds of the plant safety analyses. This also includes *incipient* failures where some degradation or a degradation mechanism has become apparent, has not yet impacted component function, but has caused failures in other components. For example, casing bolt failures from corrosion lead to a pump failure. The cause of the corrosion is determined to be incorrect bolt material. Other pumps in the CCCG that had not failed would be considered degraded if they had the incorrect bolts installed, even if not severely corroded, and the failures would be considered incipient.

0.01 The component was considered inoperable in the failure report; however, the failure was so slight that failure did not seriously affect component function. An example would be a pump packing leak that would not prevent the pump from performing its function.

0.0 The component did not fail.

5.1.24 Use

The use field is marked with an X if the component applies to the parameter estimation analysis.

5.1.25 Date

This is the failure occurrence date or the date it was detected if the actual failure date is unknown. The format of the date field is YYYY/MM/DD.

5.1.26 Comments

This field contains the analyst's comments and assumptions on coding decisions. For example, if there were two different failure modes for two failures within the CCF event, the second failure mode would be discussed here, even though an additional record was created for the second failure mode. Coder assumptions about the applicability of an event to the CCF database are discussed here, as are assumptions about the CCCG or any other data field. For CCF events identified from LERs, the LER number is referenced here. A number is listed for NPRDS and EPIX as well; this is internal to the INL data tracking system and does not refer to anything specific in the NPRDS database.

5.1.27 Narrative

LER abstracts and NPRDS failure report narratives are in this field. EPIX narratives are too lengthy to replicate in the Narrative field. The analyst will paraphrase the event in this field.

5.1.28 Insights Description

The analyst will compose a short but informative description of the event. This description will then be used to populate the event description tables in the Insights Studies. The description will be in sentence structure and will use correct grammar and spelling.

5.2 Independent Failure Coding

During the initial analysis of the failure events, all failures from both NPRDS/EPIX failure reports and LER text are characterized and counted as though they are independent failures. Common dependencies are determined later.

Five pieces of information, discussed below, are recorded for each failure: failure mode, system, component, number of failures, and p-value. The NPRDS or EPIX data set is compared to the LER data set to ensure that independent failures are not counted more than once. Once independent failure count data are developed, the independent event count data are entered into the CCF database for use in the parameter estimations.

5.2.1 System

The system code identifies the power plant system, which includes the individual failed components. Table 5-1 provides the system codes.

5.2.2 Component

The component code describes the equipment that experienced the failure. This code corresponds to the component code for the component analyzed for CCF events. The codes are intended to be operational system components and not piece-parts. The codes are defined in Table 5-3.

5.2.3 Sub-Component and Piece-Part

The sub-component and piece-part fields further identify which parts of the component failed. The appropriate sub-components and piece-parts are listed in Table 5-4.

5.2.4 Failure Mode

The failure mode describes the function the component did not perform. The codes are defined in Table 5-7.

5.2.5 Safety Function

The safety function field represents the observed failure mode as it pertains to the safety function of the component as installed in the system. If the normal safety function was impaired, the code will be Non-Fail-Safe (NFS). If the component failed and performed its safety function, the code will be Fail-Safe (FS). If it cannot be determined, the event shall be code as Unknown (UKN).

5.2.6 Component Degradation Values

This is the same as the CCF component degradation value, discussed in the Section 5.1.23, but applied here to single failures.

5.2.7 Number of Failures

This is the number of failures discussed in a single report for each combination of system, component, and failure mode. An NPRDS or EPIX record generally reports only one failure for one component. LERs, however, can report several failures of either the same component type or multiple component types in a single LER.

5.2.8 Event Type

The appropriate event types are as follows:

- Independent (IND): The event is a valid failure event for the CCF study.

- Common-cause Failure (CCF): The event either contains multiple failures that qualify as a CCF or the event is one of a set of events that are part of a CCF event.

- No Failure (NOF): The event is not a valid failure.

- Not in Study (NIS): The event describes the failure of a component that is not in the list of components for which data is being collected.

- Duplicate Event (DUP): The event document is a duplicate record of a component failure. This usually occurs when an LER has been written for a failure that is also recorded in NPRDS or EPIX. By convention, the EPIX or NPRDS event should be the one selected as a duplicate.

5.2.9 Detection Method

This field denotes the circumstances under which the failure was detected. Four categories are provided:

- Discovered during Surveillance. These events are detected during the performance of scheduled surveillance tests. In some cases, the surveillance test is performed to ensure that previous maintenance was performed correctly; these are not counted as valid failures because the component has not yet been declared operable.

- Discovered during Inspection. The inspection detection method includes alarms, walk downs, observation, etc.

- Discovered during a Demand. Component demand means that the component was started, opened, closed, or operated for either normal plant operations or in response to a safety signal. Spurious demands are included in this category.

- Discovered during Maintenance. Maintenance activities generally detect latent conditions. The analyst must ensure that the failure is not detected before the component is declared operable.

5.2.10 Comments

The comments memo field is provided so the analyst can paraphrase the event and record observations about the coding.

6. EVENT CODING EXAMPLES

This section contains six examples of coded events. Sample coding forms are also shown:

1. Boiling water reactor (BWR) safety relief valve corrosion bonding
2. Low-suction pressure trips on AFW pumps
3. Loss of power to safety injection valves
4. Excessive packing leaks
5. Start relay on AFW pumps
6. Aging/wear.

6.1 Coding Example 1: BWR Safety-Relief Valve Corrosion Bonding

Testing of the main steam safety relief valves (SRVs) revealed twelve of the fourteen valves failed to lift within technical specification acceptance limits because of corrosion bonding of the pilot seat and disk. Setpoint drift is caused by (potentially) numerous and often indeterminate random variables. Valve failures from corrosion bonding of the seat and disk are specifically design-related failures involving material selection, operating conditions, and system design. The following codes were assigned:

System = BWR main steam system (MSS).

Proximate cause = DC (construction/installation error or inadequacy) because the corrosion bonding phenomena is related to the material selection for the pilot valve seat and disk.

Timing factor = 1.0 because all valves failed during the same test.

Component = RVA (relief valve, air)

Shock type = NL (non-lethal) because the prevalent failure mechanism did not affect all components.

CCF event operational status = BO because this event can occur in operation or shutdown.

CCF event detection operational status = D because the event can only be detected during shutdown.

Failure mode = CC (fail to open) because the setpoints were significantly out of tolerance (high) from corrosion bonding of the pilot seat and disk. Technical specification tolerance is +/– 1%. The valves lifted in the range of 3% to 9% above the allowable tolerance.

Coupling factor = HDCP (Hardware Design: Component Parts) because the failures are linked by the same valve designs.

CCF event type = CCF because this type of event is considered during a CCF parameter estimation.

Failure mode applicability = 1.0 because there is only one failure mode that is appropriate for this event and all valves failed in this mode.

Shared cause factor = 1.0 because the failure mechanism is the same for all valves.

CCF event level = SYS because the majority of the SRVs failed.

CCCG = 14 because there are fourteen SRVs.

Multiple unit = N because the event only affected Limerick 1

Defense mechanism = FSB because design modifications could have prevented the CCF event.

Use field = "X" for all 14 events because they all apply to the parameter estimation analysis.

Degradation factor = 0.1 for SRVs numbers 1–12, which were slightly degraded, and 0.0 for SRV numbers 13 and 14, which were unaffected.

Name E-352-00-0366-CC Plant Limerick 1 Power 0

Title Twelve of Fourteen SRVs Failed High Due to Corrosion Bonding

System MSS Cause DC Timing Factor 1.0

Component RVA Shock Type NL Op. Status BO Det. Status D

Failure Mode CC Coupling Factor HDCP Event Type CCF

FMA 1.0 Shared Cause Factor 1.0 Event Level SYS

CCCG 14 Multiple Units N Defense Mech. FSB

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	0.1	04/04/00		9	X	0.1	04/04/00	
2	X	0.1	04/04/00		10	X	0.1	04/04/00	
3	X	0.1	04/04/00		11	X	0.1	04/04/00	
4	X	0.1	04/04/00		12	X	0.1	04/04/00	
5	X	0.1	04/04/00		13	X	0.0		
6	X	0.1	04/04/00		14	X	0.0		
7	X	0.1	04/04/00		15				
8	X	0.1	04/04/00		16				

Comments:

The cause was attributed to corrosion bonding of the pilot seat and disk. 12/14 SRVs fail to open within technical specification tolerance. As-found lifts ranged 3.6 to 9.7% above the required setpoint.

6.2 Coding Example 2: Low-Suction Pressure Trips on AFW Pumps

During surveillance testing, two of three AFW pumps tripped on low-suction pressure. It was determined that the trips were the result of momentary drops in suction pressure as the pumps were started. The pump vendor felt that the trips were not needed and should be removed. The trips were originally designed and installed to protect the pumps, and the low-pressure trips were not considered to have a safety-related function. The following codes were assigned:

System = The AFW system.

Proximate cause = DE (design error or inadequacy). The failure is the result of a design error because the trip circuits were erroneously installed and the design not adjusted.

Timing factor = 1.0 because both pumps failed closely in time.

Component = MDP (motor-driven pump). The component boundary is pumps including the suction lines and control circuitry. With the low-suction pressure trips in operation, the pumps were considered failed because they tripped. The component is MDP because the LER indicates that only the motor-driven pumps were affected.

Shock type = NL (non-lethal). The shared cause factor is applicable to the entire component population. However, the failures were random and not consistent.

CCF event operational status = BO because the condition could have been noted during shutdown or operation.

CCF event detection operational status = O because the event was detected during testing at power.

Failure mode = FR (fail to run) because the pump would not run long enough to fulfill its safety function, even though it actuated and started.

Coupling factor = HDCP (Hardware Design: Component Part [Internal Parts: Ease of Maintenance & Operation])) because it is a design error in the component part.

CCF event type = CCF because this type of event is considered during a CCF parameter estimation.

Failure mode applicability = 1.0 because there is only one failure mode and it is applicable to both failures.

Shared cause factor = 1.0 because the failures of both pumps are of the same design and installation.

CCF event level = SYS because two parallel pumps failed.

CCCG = 2 because at this plant there are two motor-driven pumps in the AFW system with low suction pressure trips. The LER indicates that only the motor-driven pumps were affected, so the turbine-driven pump is not included.

Multiple unit = N because the event only affected Millstone 3.

Defense mechanism = FSB (functional physical barrier) because the shared cause factor is the system design.

Use = "X" for the two failures that occurred because they both apply to the parameter.

Degradation factor = 0.5 for both events because both motor-driven pumps would perform their function intermittently and therefore are partially degraded.

Name L-423-87-0047-FR Plant Millstone 3 Power 100

Title Both Motor-Driven Aux. Feedwater Pumps Tripped due to Suction Pressure Fluctuations

System AFW Cause DE Timing Factor 1.0

Component MDP Shock Type NL Op. Status BO Det. Status O

Failure Mode FR Coupling Factor HDCP Event Type CCF

FMA 1.0 Shared Cause Factor 1.0 Event Level SYS

CCCG 2 Multiple Units N Defense Mech. FSB

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	0.5	01/27/87		9				
2	X	0.5	01/27/87		10				
3					11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments:

Both motor-driven auxiliary feedwater pumps tripped due to fluctuations in suction pressure. This trip function was not safety-related so it was removed. The turbine driven pump was not affected.

6.3 Coding Example 3: Loss of Power to Safety Injection Valves

An overload condition resulted in loss of power to a load center that supplied two safety injection valves. The following codes were assigned:

System = The HPI system.

Proximate cause = QP (state of other component) because the state of the injection valves are caused by another component failure.

Timing factor = 1.0 because both injection valves failed simultaneously.

Component = MOV and the boundary includes the circuit breaker.

Shock type = NL (non-lethal) because the prevalent failure mechanism did not affect all components and trains.

The CCF event operational status = OP because this event can only occur during an operational condition.

CCF event detection operational status = O because the event was detected at operation.

Failure mode = CC (fail to open) because the injection valves are normally closed and failed to open because of not receiving an actuation signal.

Coupling factor = HDSC (hardware design, system configuration) because the electrical source is shared by the two components.

CCF event type = EXP (explicitly modeled) because this type of event is explicitly modeled in PRA in combination with electric power. Coding this event in this manner will allow the analyst the ability to develop PRA specific parameter estimations.

Failure mode applicability = 1.0 because there is only one failure mode that is appropriate for this event and both valves failed in this mode.

Shared cause factor = 1.0 because the failure of both injection valves is closely linked because of shared equipment dependence.

CCF event level = COM (component level) because this event affected only one train.

CCCG = 6 because there are six injection valves, two on each train.

Multiple units = N because the event only affects San Onofre 1

Defense mechanism = FSB (functional/physical barrier) because a decoupling of the CCF event could have accomplished if functional barriers were administered.

Use = "X" for all six events because they all apply to the parameter estimation analysis.

Degradation factor = 1.0 for the two failed injection valves and 0.0 for the unaffected injection valves in the other trains.

Name	L-206-85-0556-CC	Plant	San Onofre 1	Power	92
Title	Loss of Power to MCC Caused Loss of High Pressure Safety Injection Valves				
System	HPI	Cause	QP	Timing Factor	1.0

Component	MOV	Shock Type	NL	Op. Status	OP	Det. Status	O

Failure Mode	CC	Coupling Factor	HDSC	Event Type	EXP
FMA	1.0	Shared Cause Factor	1.0	Event Level	COM
CCCG	6	Multiple Units	N	Defense Mech.	FSB

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	1.0	06/16/85		9				
2	X	1.0	06/16/85		10				
3	X	0.0			11				
4	X	0.0			12				
5	X	0.0			13				
6	X	0.0			14				
7					15				
8					16				

Comments:

An overload condition on the motor control center, caused by a faulty vacuum pump breaker, resulted in the loss of power to 2 HPSI valves.

6.4 Coding Example 4: Excessive Packing Leaks

The packing in two pumps failed because of normal wear and aging. The leakage was reported by the licensee as "excessive." The following codes were assigned:

System = AFW system.

Proximate cause = IC (internal to the component, piece-part) The failure resulted from wear-out.

Timing factor = 0.1 because the failures occurred more than a month apart.

Component = PMP (pump). With the pump packing failing, the pumps failed. Although only the motor-driven pumps were affected in this event, there's no indication that turbine-driven pumps are not susceptible to the same causal factors.

Shock type = NL (non-lethal) because failures are loosely coupled and not likely to affect the entire component population.

CCF event operational status = BO because the CCF event can occur during operating or shutdown conditions.

CCF event detection operational status = O because it was detected while the plant was at power.

Failure mode = FR (fail to run) because the pumps would start but would not continue to operate.

Coupling factor = OMTC (Operational: Maintenance/Test Schedule) because it is assumed that more frequent maintenance would have replaced the packing before it leaked.

CCF event type = CCF because this type of event is included in a PRA system model. The report indicated that the leakage was excessive, and would impact pump operation. A leak not indicated to be "excessive" would be considered "INS."

Failure mode applicability = 1.0 because there is only one failure mode and it applies to both failures.

Shared cause factor = 0.5 because the failure of both pumps is linked by maintenance schedules. It is uncertain if more frequent maintenance may eliminate the coupling between these components with respect to this cause.

CCF event level = COM because this is a component-level type failure because parallel pumps were degraded, but multiple trains were not disabled simultaneously.

CCCG = 3 because there are three pumps.

Multiple units = N because the event only affected San Onofre 1.

Defense mechanism = MAI because the shared cause factor is operating and maintenance schedule, where a change in the maintenance staffing or scheduling may have prevented the CCF event.

Use = "X" for three events, two that occurred and one that did not occur (one pump did not fail).

Degradation factor = 0.1 for the two failures, because these failures did not significantly affect the operation of the pumps. A degradation factor of 0.0 was assigned to the pump that did not fail.

Name N-206-90-0050-FR Plant San Onofre 1 Power 100

Title Both Motor-Driven Auxiliary Feedwater Pumps had Excessive Leakage

System AFW Cause IC Timing Factor 0.1

Component PMP Shock Type NL Op. Status BO Det. Status O

Failure Mode FR Coupling Factor OMTC Event Type CCF

FMA 1.0 Shared Cause Factor 0.5 Event Level COM

CCCG 3 Multiple Units N Defense Mech. MAI

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	0.1	04/24/90		9				
2	X	0.1	07/03/90		10				
3	X	0.0			11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments:

Both motor-driven auxiliary feedwater pumps had excessive packing leakage resulting in degraded system operation. The cause of the leakage was determined to be normal wear.

6.5 Coding Example 5: Start Relay on Auxiliary Feedwater Pumps

The circuit breakers on the motor-driven pumps failed to operate properly. In one case, it was unclear whether or not the breaker had closed and the motor started; in the second case the breaker did not close. Both cases were the result of broken or dirty switch contacts. The following codes were assigned:

System = AFW system.

Proximate cause = IE because the failure is the result of an environmental condition external to the component.

Timing factor = 1.0 because the failures occurred simultaneously.

Component = MOT (motor). The component boundary is the motor, including the motor, breaker, and control circuit. When the control switches fail, the motors are considered failed.

Shock type = L (lethal) because the failures are tightly coupled.

CCF event operational status = BO because the event can occur during either operating or shutdown conditions.

CCF event detection operational status = D because it was detected during a refueling outage.

Failure mode = FS (fail to start) because neither motor started.

Coupling factor = EE (external environment) because of the shared external environment.

CCF event type = CCF because this event is considered important during a CCF parameter estimation.

Failure mode applicability = 1.0 because there is only one failure mode and it applies to both failures.

Shared cause factor = 1.0 because failure of both motors is linked by a factor that will always affect the components in a similar manner.

CCF event level = SYS because this is a system type failure.

CCCG = 2 because there are two motor-driven pumps.

Multiple units = N because the event only affected Indian Point 2.

Defense mechanism = PBR (physical barrier) because the shared cause factor is an environmental factor where separation between the two components could have prevented the CCF event.

Use = "X" for both events because they apply to the parameter estimation analysis.

Degradation factor = 1.0 for both failures because the motors did not start.

Name	L-247-84-0001-FS	Plant	Indian Point 2	Power	0
Title	Two Auxiliary Feedwater Pumps Failed due to Start Relay Failure				
System	AFW	Cause	IE	Timing Factor	1.0

Component	MOT	Shock Type	L	Op. Status	BO	Det. Status	D

Failure Mode	FS	Coupling Factor	EE	Event Type	CCF
FMA	1.0	Shared Cause Factor	1.0	Event Level	SYS
CCCG	2	Multiple Units	N	Defense Mech.	PBR

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	1.0	09/10/84		9				
2	X	1.0	09/10/84		10				
3					11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments:

Both motor-driven auxiliary feedwater pumps failed to start on demand. One relay for each pump motor had failed due to insulation degradation.

6.6 Coding Example 6: Aging/Wear

The AFW pumps were susceptible to corrosion cracking of their bushings. A different material was needed for the shaft sleeves. All four pumps at the two units were affected. A separate record was input for Unit 2. The following codes were assigned:

System = AFW system

Proximate cause = DE (design deficiency). It was determined that the stainless steel material used for the sleeve material was too hard, which resulted in higher stress-related corrosion susceptibility.

Timing factor = 1.0 because the degraded condition existed in all components simultaneously.

Component = PMP (pump). The component boundary is the pump, including the pump shaft.

Shock type = L (lethal) because the failure is applicable to the entire population.

CCF event operational status = BO because the event can occur in operation or shutdown mode.

CCF event detection operational status = D because detection occurred and is most likely to occur when the plant is shut down.

Failure mode = FR (fail to run) because it is assumed that the pump shaft will fail during stress loading when the pump is running. This would disable the pump from continuing to deliver discharge pressure after it had been successfully started.

Coupling factor = (HDCP) hardware/design of the component (HDCP). All components used the same material.

CCF event type = CCF because it would not typically be modeled explicitly in a PRA and should be included in an estimation of the CCF *basic event* (BE) for the AFW pump.

Failure mode applicability = 1.0 because there is only one failure mode and it is applicable to both failures and potential failures in the record.

Shared cause factor = 1.0 because a design error in the manufacturing process will closely tie the components together.

CCF event level = Component level failure since other trains were *available* for AFW.

CCCG = 2 because there are two pumps affected by this event at each unit.

Multiple units = Y because the event also affected South Texas 2.

Defense mechanism = DIV (diversity). This defense mechanism states that an increase in the diversity of the pumps could have prevented a similar CCF.

Use = "X" for both components because they both apply to the analysis.

Degradation value = 1.0 for one of the pumps because it failed. The other pumps contained the same material that failed. One of the three remaining pumps at the two units was inspected and revealed that similar cracking to the sleeve shaft had occurred; therefore, the second degradation value was assigned 0.1 to indicate potential cracking and failure of the pump.

Name L-498-88-0048-FR Plant South Texas 1 Power 0

Title Stress Corrosion Cracking/Hydrogen Embrittlement of AFP Shaft Sleeve

System AFW Cause DE Timing Factor 1.0

Component PMP Shock Type NL Op. Status BO Det. Status D

Failure Mode FR Coupling Factor HDCP Event Type CCF

FMA 1.0 Shared Cause Factor 1.0 Event Level COM

CCCG 2 Multiple Units Y Defense Mech. DIV

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	1.0	02/28/88		9				
2	X	0.1	05/12/88		10				
3					11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments:

An AFW pump failed its performance test because of internal damage, including a split in the shaft sleeve. A second pump, used as a replacement for the first one, also had the same damage. The cause was determined to be stress corrosion cracking/hydrogen embrittlement of the sleeve material. All pumps at both units were considered affected and the sleeve material in all pumps was replaced.

7. QUANTITATIVE ANALYSIS OF COMMON-CAUSE FAILURE EVENTS

Because 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 2 proposes creating plant-specific data through screening and evaluating generic data for plant-specific characteristics. Two techniques were presented in Reference 2 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.

7.1 Event Impact Vector

An impact vector is a numerical representation of a CCF event. According to Reference 2, 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 with each representing a different interpretation of the event.

Consider the event depicted in Figure 7-1, which 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 1 is

$I_1 = [0, 0, 1, 0]$

and the impact vector for hypothesis 2 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 2. That is, he believes that there is a 90% chance that hypothesis 1 is true and only a 10% chance that hypothesis 2 is true. To use these in a CCF analysis, the average or weighted impact vector is calculated. The weighted impact vector for this example is

$$0.9I_1 + 0.1I_2 = [0, 0, 0.9, 0.1] \quad (7\text{-}1)$$

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_0	F_1	F_2	F_3
Two of three components fail	0.9	0	0	1	0
All three components fail	0.1	0	0	0	1
Average Impact Vector ($\bar{I}$)		$\bar{F}_0$	$\bar{F}_1$	$\bar{F}_2$	$\bar{F}_3$
		0	0	0.9	0.1

Figure 7-1. Example of the assessment of impact vectors involving multiple interpretation of event.

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

$$\bar{I} = \sum_{i=1}^{N} w_i I_i \tag{7-2}$$

where

N = number of hypotheses

w_i = weight or probability of hypothesis *I*

I_i = impact vector.

The average impact vector is given by

$$\bar{I} = \left[\bar{F}_0, \bar{F}_1, \cdots \bar{F}_m\right] \tag{7-3}$$

Some events occur where judging whether multiple failures occurred because of 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 1 is [0, 0, 1]. For hypothesis 2, the analyst postulates independent failures of two components. Therefore, two impact vectors exist for this hypothesis—one for each component—because two components failed independently. Both are equal to [0, 1, 0]. If the weight for hypothesis 1 is 0.6 and 0.4 for hypothesis 2, the average impact vector equals

$$0.6\,[0, 0, 1] + 0.4\,[0, 1, 0] + 0.4\,[0, 1, 0] \tag{7-4}$$
$$= [0, 0.8, 0.6]$$

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. 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.

7.2 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., Fk = 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 (Refs. 3, 10, and 14):

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 may be lacking (e.g., the number of components affected, their functional state, and root causes of the event).

In general, three event types require multiple hypotheses:

1. Events involving degraded component states

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

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 event types are discussed separately.

7.2.1 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 (i.e., 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 during a typical system mission as defined in PRAs. This is called the component degradation value. It is denoted by pk and takes values in the range of $0 \leq p_k \leq 1$ (see Section 5.1.23 for recommended values).

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 7-1 shows how the various elements of the average impact vector may be calculated for components groups of sizes 2, 3, and 4. This technique does not require the formulation of multiple hypotheses, but it uses the information about the degraded component states to obtain the average impact vector.

7.2.2 Case 2: Events Involving Failures Distributed in Time

In this case, the presence of a shared cause for the component states is determined but the 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).

Table 7-1. 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	$(1-p_1)(1-p_2)$ $(1-p_3)(1-p_4)$	$p_1(1-p_2)(1-p_3)(1-p_4)$ $+ p_2(1-p_1)(1-p_3)(1-p_4)$ $+ p_3(1-p_1)(1-p_2)(1-p_4)$ $+ p_4(1-p_1)(1-p_2)(1-p_3)$	$p_1p_2(1-p_3)(1-p_4)$ $+ p_1p_3(1-p_2)(1-p_4)$ $+ p_1p_4(1-p_2)(1-p_3)$ $+ p_2p_3(1-p_1)(1-p_4)$ $+ p_2p_4(1-p_1)(1-p_3)$ $+ p_3p_4(1-p_1)(1-p_2)$	$p_1p_2p_3(1-p_4)$ $+ p_1p_2p_4(1-p_3)$ $+ p_1p_3p_4(1-p_2)$ $+ p_2p_3p_4(1-p_1)$	$p_1p_2p_3p_4$

Specific guidelines for assigning values of q are contained in Section 5.1.7. 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.

The values for q are impacted by operational characteristics. 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 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, test strategies for generic events are usually not known to the analyst; therefore, conservative assumptions may be made based on the following two approaches.

7.2.2.1 Standby Failure Rate Model Approach. If non-staggered testing is adopted, it is possible for the components to fail immediately following the test; in this 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.

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

7.2.2.2 Probability of Failure on Demand Model Approach. For standby systems where a CCF is considered for failure on demand, the value chosen for probability 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. If the second component fails on the first challenge after failure of the first component, the event is interpreted as CCF with $q = 1.0$.

Using the binomial concept, if the failures are separated by one successful challenge then 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 $q = 0.5$. If the failures were 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 $q = 0.1$. Failures separated by more than two successful challenges can be assumed independent. Because generic failure reports usually do not provide the number of successful challenges between demands, the Probability of Failure on Demand Model was not used for coding the timing factor of events in the NRC CCF database.

7.2.2.3 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

$$I_{CCF} = q\,[0,0,1,0] = [0,0,q,0] \qquad (7\text{-}5)$$

For independent failure of component 1

$$I_{c_1} = (1-q)\,[0,1,0,0] = [0,\ 1-q,\ 0,\ 0] \qquad (7\text{-}6)$$

For independent failure of component 2

$$I_{c_2} = (1-q)\,[0,1,0,0] = [0,\ 1-q,\ 0,\ 0] \qquad (7\text{-}7)$$

The average impact vector for this specific case is

$$\bar{I} = [0, 2(1-q), \ldots, q, \ldots, 0] \qquad (7\text{-}8)$$

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:

$$I_{CCF} = [0, 0, \ldots, q, \ldots, 0] \qquad (7\text{-}9)$$

where q is the $k+1$ element of the vector,

$$I_{c_1} = [0,\ 1-q,\ 0, \ldots, 0] \text{ for component 1,} \qquad (7\text{-}10)$$

$$\vdots$$

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

The average impact vector in this case is

$$\bar{I} = [0, k(1-q), \ldots, q, \ldots, 0\,] \qquad (7\text{-}11)$$

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

7.2.3 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, 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 because it relates to an important and distinct element of CCF events (i.e., the coupling factor). For this reason, a parameter called the "shared cause factor," c, is introduced as the analyst's degree of confidence about the presence of a shared cause in the event. The values of c may range from $0 \leq c \leq 1$ (see Section 5.1.17 for recommended values).

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

$$I_{CCF} = [0, 0, ..., c, ..., 0] \qquad (7\text{-}12)$$

where c is the $k+1$ element of the vector,

$$I_{c_1} = [0, (1-c), 0, ..., 0] \text{ for component 1,}$$
$$\vdots$$
$$I_{c_k} = [0, (1-c), 0, ..., 0] \text{ for component } k.$$

The average impact vector in this case is

$$\bar{I} = [0, k(1-c), ..., c, ..., 0] \qquad (7\text{-}13)$$

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

7.2.4 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

$$I_{CCF} = [cqF_0, cqF_1, ..., cqF_m], \qquad (7\text{-}14)$$
$$I_{c_1} = [(1-cq)(1-P_1), (1-cq)P_1, 0, ..., 0]$$
for component 1,
$$\vdots$$
$$I_{c_m} = [(1-cq)(1-P_m), (1-cq)P_m, 0, ..., 0]$$

where

P_i = degree of degradation of the i^{th} component

F_i = calculated from P_i according to the relations in Table 7-1 for $m = 2$, 3, and 4, or similar ones for $m > 4$.

The average impact vector is obtained by adding I_{CCF} and the I_c values.

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 (7-14), the quantity modifying the impact vectors for shared cause strength is cq, which could be replaced by a single parameter.

7.3 Specializing Impact Vectors for Plant Specific Analyses

The discussions to this point have addressed using industry data to perform generic analyses. According to Reference 2, 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.

7.3.1 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 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. Because 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 2, in this situation, the analyst can multiply the original impact vector by an event applicability factor r ($0 \leq r \leq 1$), which is subjectively assessed and is a measure of applicability of the cause and coupling factor of the event to the target system. The r number is a measure of the physical, operational, and environmental differences between the original and the target system, as well as the analyst's uncertainty as to whether such differences exist. The modified *application*-specific impact vector is then written as

$$I_r = r * I \qquad (7\text{-}15)$$

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 (Refs. 3, 10, and 14). 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 toward 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 a coupling strength of one. The role of these two factors in creating various types of events is shown schematically in the diagram of Figure 7-2.

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 7-2 are suggested values for r_1 and r_2.

Another issue which influences the applicability factor and is often encountered in data analysis is what to do with events that 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 because 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, because of the potential for introduction of new problems and failure mechanisms.

Table 7-2. Suggested values for r_1 and r_2.

Strength of Target Plant Defenses Compared with Original/Average Plant	Applicability Factor	
	Root Cause (r_1)	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

Both sides of this debate have valid points. The essential 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 that 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 because the level of detail contained in current data compilations does not support this type of estimation.

7.3.2 Adjustment for Quantitative Difference

7.3.2.1 Exposed Population versus Component Group Size. There is a difference between the concepts of exposed population and the CCCG size. The exposed population is a data analysis concept and CCCG size is a modeling concept. An example of the difference is provided in the context of the Reactor Protection System (RPS).

Pressurized water reactor (PWR) plants contain up to 40 bistables in the RPS. The actual number of bistables in a particular plant represents the exposed population and remains the same for a given plant. For a given scram scenario, one or more bistables are required to function in each channel. The CCCG size is the number of bistables required per channel times the number of channels. This varies as the number of modeled scram parameters change, depending upon the channel design. Therefore, it is possible to have events with in-plant populations of up to 24 components; modeled events have a CCCG from two to the exposed population. In the case of a maintenance event, one channel's worth of components is removed from the CCCG.

An impact vector represents a CCF in a specific group of components of exposed population size *m*. A collection of impact vectors used to calculate the *CCF BE* probability for a particular component may contain impact vectors of many different exposed population sizes (i.e., events that occur in different plants or different systems). In this case, the impact vectors are mapped to the CCCG size of interest.

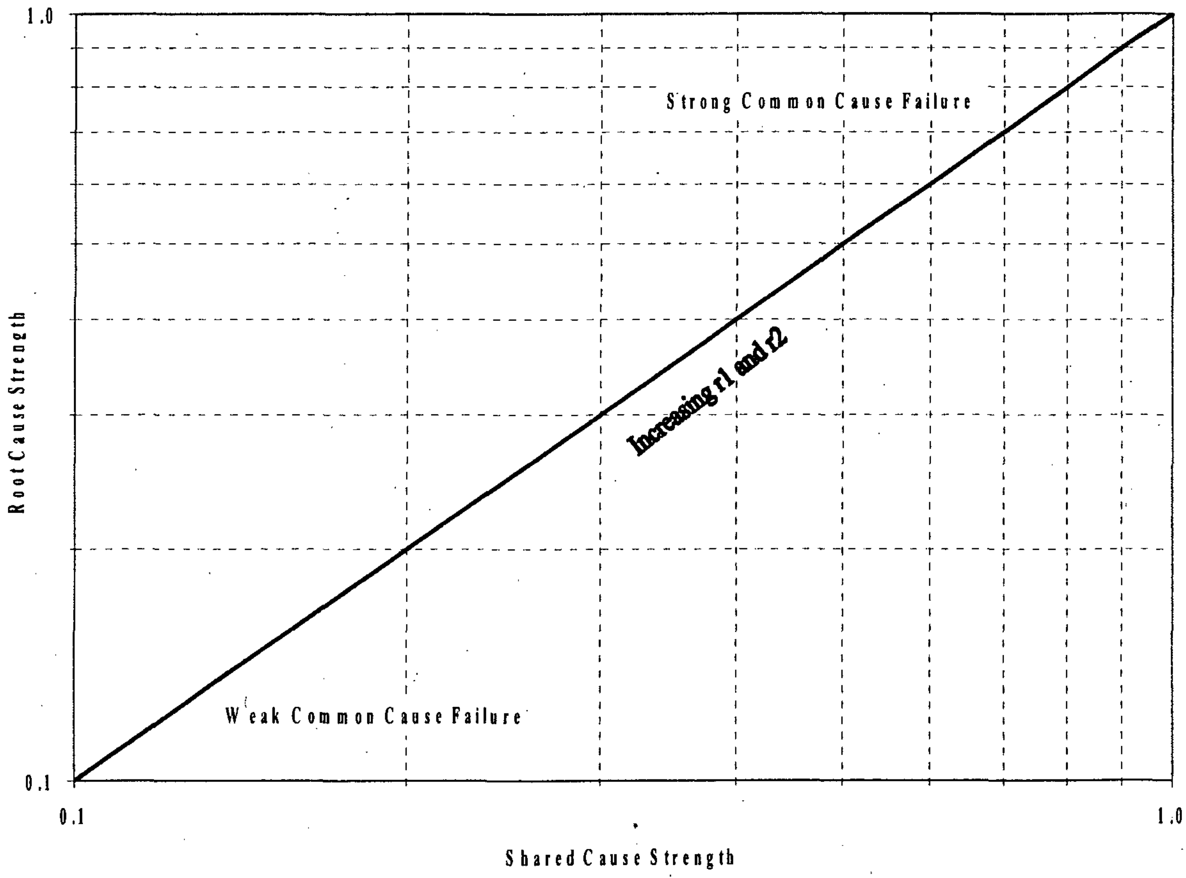


Figure 7-2. Schematic representation of the role of shared cause factor and root cause strength information of different classes of events.

7.3.2.2 Mapping of Data. The level impact of the event on the target system is analyzed because of the difference that may exist between the level of exposed populations in 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 2 provides *mapping* rules for the following cases:

- *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).
- *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).

The parameter ρ in Equation (7-16) is called the mapping up parameter. It is the probability that the non-lethal shock or cause would have failed a single component added to the system. One method for estimating ρ is given by the following equation (Ref. 15):

$$\rho = \frac{\sum_{i=1}^{m} i(i-1)f_i}{(m-1)\sum_{i=1}^{m} i(f_i)} \qquad (7\text{-}16)$$

where

m = the number of elements in the group (CCCG)

f_i = the i^{th} element of the generic impact vector.

This method works well when the system sizes are close to one another (e.g., mapping from size 2 to size 3 or 4) or when at least one of the component degradation values is less than 1.0. When all of the component degradation values are equal to 1.0, ρ is also equal to 1.0. When used in the mapping up equations for the RPS data, this method tends to overestimate the probability that components added to a system will exhibit the same lethal shock-like behavior. Examination of trends in the unmapped RPS data shows that as the number of components in a system increases, the likelihood of lethal behavior in that group of components decreases rapidly. Based on these observed trends and empirical studies, a maximum value of 0.85 was established for ρ.

7.3.2.3 Mapping Techniques. 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 7-3. 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.

It is evident from the information presented above that downward mapping is "deterministic"; that is, 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 Ref. 2, 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 common-cause model (Ref. 1). The concept is that all events can be classified into one of three categories:

- Independent Events. Causal events that act on components singly and independently.
- Non-lethal 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, non-lethal shocks can occur when a causal event acts only on a subset of the components in the system.
- Lethal Shocks. Causal events that fail all the components in the system.

When enough is known about the cause of a given event (i.e., root cause and coupling mechanism), 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 non-lethal.

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 non-lethal shocks that an added element of uncertainty is introduced in mapping upward. How each event is handled is summarized below.

Table 7-3. Formulas for mapping down event impact vectors.

		Size of System Mapping To (Number of Identical Trains)				
		5	4	3	2	1
Size of System Mapping From	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		$f_1^{(4)}=(4/5)f_1^{(5)}+(2/5)f_2^{(5)}$ $f_2^{(4)}=(3/5)f_2^{(5)}+(3/5)f_3^{(5)}$ $f_3^{(4)}=(2/5)f_3^{(5)}+(4/5)f_4^{(5)}$ $f_4^{(4)}=(1/5)f_4^{(5)}+f_5^{(5)}$	$f_1^{(3)}=(3/5)f_1^{(5)}+(3/5)f_2^{(5)}+(3/10)f_3^{(5)}$ $f_2^{(3)}=(3/10)f_2^{(5)}+(3/5)f_3^{(5)}+(3/5)f_4^{(5)}$ $f_3^{(3)}=(1/10)f_3^{(5)}+(2/5)f_4^{(5)}+f_5^{(5)}$	$f_1^{(2)}=(2/5)f_1^{(5)}+(3/5)f_2^{(5)}+(3/5)f_3^{(5)}$ $+(2/5)f_4^{(5)}$ $f_2^{(2)}=(1/10)f_2^{(5)}+(3/10)f_3^{(5)}$ $+(3/5)f_4^{(5)}+f_5^{(5)}$	$f_1^{(1)}=(1/5)f_1^{(5)}+(2/5)f_2^{(5)}+(3/5)f_3^{(5)}$ $+(4/5)f_4^{(5)}+f_5^{(5)}$
	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					$f_1^{(1)}=(1/2)f_1^{(2)}+f_2^{(2)}$

7.3.2.4 Mapping up Independent Events. Because the number of independent events in the database is proportional to the number of components in the system, in the case of independent events, 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:

$$F_I^{(l)} = (l/k)\, F_I^{(k)} \qquad (7\text{-}17)$$

7.3.2.5 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

$$F_l^{(l)} = F_j^{(j)} \qquad (7\text{-}18)$$

Hence, for lethal shocks, the impact vector is mapped directly. The probability that j components in a system of j components have failed because of a lethal shock is mapped directly to the probability of failing all l components in an l component system.

7.3.2.6 Mapping up Non-lethal Shocks. Non-lethal shock failures are viewed as the result of a non-lethal 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 non-lethal shock that occurs in a one-component system up to a four-component system is illustrated in Reference 2. Table 7-4 includes formulas to cover all upward mapping possibilities with system sizes up to four. In the limiting cases of $\rho = 0$ and $\rho = 1$, the formulas in Table 7-4 become identical to the equations for mapping up independent events and the equations for mapping up lethal shocks, respectively.

A special case occurs when a complete common-cause failure event involves a non-lethal shock (i.e., all $P_i = 1.0$, the timing factor equals 1.0 and the shared cause factor equals 1.0). For this case, ρ given by Equation (7-16) equals 1. Thus, Equation (7-16) treats non-lethal shock complete failure events as lethal shock events. Examination of the *complete CCF* events shows that this is overly conservative because the number of complete CCF events decreases as the CCCG size increases. Empirical studies show that using a value of $\rho = 0.5$ is a good choice for the non-lethal shock complete CCF events.

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 non-lethal shock or cause would have failed a single hypothetical component added to the system.

7.4 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,

$$n_k = \sum_{i=1}^{m} \overline{F}_k(i) \qquad (7\text{-}19)$$

where

n_k = total number of BEs involving failure of k similar components

m = number of elements in the group (CCCG)

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

Table 7-4. Formulas for upward mapping of events classified as non-lethal shocks.

		Size of System Mapping To (Number of Identical Trains)				
		2	3	4	5	6
Size of System Mapping From	1	$f_1^{(2)}=2(1-\rho)f_1^{(1)}$ $f_2^{(2)}=\rho f_1^{(1)}$	$f_1^{(3)}=3(1-\rho)^2f_1^{(1)}$ $f_2^{(3)}=3\rho(1-\rho)f_1^{(1)}$ $f_3^{(3)}=\rho^2f_1^{(1)}$	$f_1^{(4)}=4(1-\rho)^3f_1^{(1)}$ $f_2^{(4)}=6\rho(1-\rho)^2f_1^{(1)}$ $f_3^{(4)}=4\rho^2(1-\rho)f_1^{(1)}$ $f_4^{(4)}=\rho^3f_1^{(1)}$	$f_1^{(5)}=5(1-\rho)^4f_1^{(1)}$ $f_2^{(5)}=10\rho(1-\rho)^3f_1^{(1)}$ $f_3^{(5)}=10\rho^2(1-\rho)^2f_1^{(1)}$ $f_4^{(5)}=5\rho^3(1-\rho)f_1^{(1)}$ $f_5^{(5)}=\rho^4f_1^{(1)}$	$f_1^{(6)}=6(1-\rho)^5f_1^{(1)}$ $f_2^{(6)}=15\rho(1-\rho)^4f_1^{(1)}$ $f_3^{(6)}=20\rho^2(1-\rho)^3f_1^{(1)}$ $f_4^{(6)}=15\rho^3(1-\rho)^2f_1^{(1)}$ $f_5^{(6)}=6\rho^4(1-\rho)f_1^{(1)}$ $f_6^{(6)}=\rho^5f_1^{(1)}$
	2		$f_1^{(3)}=(3/2)(1-\rho)f_1^{(2)}$ $f_2^{(3)}=\rho f_1(2)+(1-\rho)f_2^{(2)}$ $f_3^{(3)}=\rho f_2^{(2)}$	$f_1^{(4)}=2(1-\rho)^2f_1^{(2)}$ $f_2^{(4)}=(5/2)\rho(1-\rho)f_1^{(2)}+(1-\rho)^2f_2^{(2)}$ $f_3^{(4)}=\rho^2f_1^{(2)}+2\rho(1-\rho)f_2^{(2)}$ $f_4^{(4)}=\rho^2f_2^{(2)}$	$f_1^{(5)}=(5/2)(1-\rho)^3f_1^{(2)}$ $f_2^{(5)}=(9/2)\rho(1-\rho)^2f_1^{(2)}+(1-\rho)^3f_2^{(2)}$ $f_3^{(5)}=(7/2)\rho^2(1-\rho)f_1^{(2)}+3\rho(1-\rho)^2f_2^{(2)}$ $f_4^{(5)}=\rho^3f_1^{(2)}+3\rho^2(1-\rho)f_2^{(2)}$ $f_5^{(5)}=\rho^3f_2^{(2)}$	$f_1^{(6)}=3(1-\rho)^4f_1^{(2)}$ $f_2^{(6)}=7\rho(1-\rho)^3f_1^{(2)}+(1-\rho)^4f_2^{(2)}$ $f_3^{(6)}=8\rho^2(1-\rho)^2f_1^{(2)}+4\rho(1-\rho)^3f_2^{(2)}$ $f_4^{(6)}=(9/2)\rho^3(1-\rho)f_1^{(2)}+6\rho^2(1-\rho)^2f_2^{(2)}$ $f_5^{(6)}=\rho^4f_1^{(2)}+4\rho^3(1-\rho)f_2^{(2)}$ $f_6^{(6)}=\rho^4f_2^{(2)}$
	3			$f_1^{(4)}=(4/3)(1-\rho)f_1^{(3)}$ $f_2^{(4)}=\rho f_1^{(3)}+(1-\rho)f_2^{(3)}$ $f_3^{(4)}=\rho f_2^{(3)}+(1-\rho)f_3^{(3)}$ $f_4^{(4)}=\rho f_3^{(3)}$	$f_1^{(5)}=(5/3)(1-\rho)^2f_1^{(3)}$ $f_2^{(5)}=(7/3)\rho(1-\rho)f_1^{(3)}+(1-\rho)^2f_2^{(3)}$ $f_3^{(5)}=\rho^2f_1^{(3)}+2\rho(1-\rho)f_2^{(3)}+(1-\rho)^2f_3^{(3)}$ $f_4^{(5)}=\rho^2f_2^{(3)}+2\rho(1-\rho)f_3^{(3)}$ $f_5^{(5)}=\rho^2f_3^{(3)}$	$f_1^{(6)}=2(1-\rho)^3f_1^{(3)}$ $f_2^{(6)}=4\rho(1-\rho)^2f_1^{(3)}+(1-\rho)^3f_2^{(3)}$ $f_3^{(6)}=(10/3)\rho^2(1-\rho)f_1^{(3)}+3\rho(1-\rho)^2f_2^{(3)}$ $+(1-\rho)^3f_3^{(3)}$ $f_4^{(6)}=\rho^3f_1^{(3)}+3\rho^2(1-\rho)f_2^{(3)}+3\rho(1-\rho)^2f_3^{(3)}$ $f_5^{(6)}=\rho^3f_2^{(3)}+3\rho^2(1-\rho)f_3^{(3)}$ $f_6^{(6)}=\rho^3f_3^{(3)}$
	4				$f_1^{(5)}=(5/4)(1-\rho)f_1^{(4)}$ $f_2^{(5)}=\rho f_1^{(4)}+(1-\rho)f_2^{(4)}$ $f_3^{(5)}=\rho f_2^{(4)}+(1-\rho)f_3^{(4)}$ $f_4^{(5)}=\rho f_3^{(4)}+(1-\rho)f_4^{(4)}$ $f_5^{(5)}=\rho f_4^{(4)}$	$f_1^{(6)}=(3/2)(1-\rho)^2f_1^{(4)}$ $f_2^{(6)}=(9/4)\rho(1-\rho)f_1^{(4)}+(1-\rho)^2f_2^{(4)}$ $f_3^{(6)}=\rho^2f_1^{(4)}+2\rho(1-\rho)f_2^{(4)}+(1-\rho)^2f_3^{(4)}$ $f_4^{(6)}=\rho^2f_2^{(4)}+2\rho(1-\rho)f_3^{(4)}+(1-\rho)^2f_4^{(4)}$ $f_5^{(6)}=\rho^2f_3^{(4)}+2\rho(1-\rho)f_4^{(4)}$ $f_6^{(6)}=\rho^2f_4^{(4)}$
	5					$f_1^{(6)}=(6/5)(1-\rho)f_1^{(5)}$ $f_2^{(6)}=\rho f_1^{(5)}+(1-\rho)f_2^{(5)}$ $f_3^{(6)}=\rho f_2^{(5)}+(1-\rho)f_3^{(5)}$ $f_4^{(6)}=\rho f_3^{(5)}+(1-\rho)f_4^{(5)}$ $f_5^{(6)}=\rho f_4^{(5)}+(1-\rho)f_5^{(5)}$ $f_6^{(6)}=\rho f_5^{(5)}$

In order to provide estimates of the probability of a common-cause event involving *k* specific components in a CCCG of size *m*, a model needed to be selected from among the available models. The available models included the Basic Parameter model, the Beta model, the *Multiple Greek Letter* (MGL) model, and the *Alpha Factor* model.

The parametric Alpha Factor model was chosen because it is (1) a multi-parameter model that can handle any redundancy level, (2) based on ratios of failure rates that make the assessment of its parameters easier when no statistical data are available, and (3) a simpler statistical model and produces more accurate point estimates as well as uncertainty distributions compared to other parametric models that have the above two properties.

Event statistics are used to develop estimates of *CCF model* parameters. The Alpha Factor model estimates CCF frequencies from a set of ratios of failures and the total component failure rate. The parameters of the model are

Q_T ≡ The total failure frequency of each component (includes independent and common-cause events)

α_k ≡ The fraction of the total frequency of failure events that occur in the system involving the failure of *k* components in a system of *m* components because of a common-cause

$$\sum_{k=1}^{m} \alpha_k = 1 \qquad (7\text{-}20)$$

The parameters of the Alpha Factor model can be estimated using the following maximum likelihood estimators:

$$\hat{\alpha}_k = \frac{n_k}{\sum_{j=1}^{m} n_j} \qquad (7\text{-}21)$$

7.5 CCF Basic Event Equation Development

With the alpha factors calculated for the target component, the next step is to develop the BE equation. The CCF BE equation depends on the failure criterion and the number of redundant components in the system. The most basic failure criterion is that any *k* of *m* components fail and the function of the system of components fails (e.g., three of four (3/4) pumps fail to start, meaning that two of the four pumps are sufficient). Other criteria typically used in systems that are more complicated include specific failure criteria (e.g., three of four channels and two out of two components to fail a channel) and a special case of specific logic, one-out-of-two-twice failure criteria.

7.5.1 Any-*k*-of-*m* Combinations

The form of the CCF BE equation for any *k* out of *m* components failing is given by following equation for staggered testing:

$$Q_{CCF} = Q_T \sum_{i=k}^{m} \frac{\binom{m}{i}}{\binom{m-1}{i-1}} \alpha_i = Q_T \sum_{i=k}^{m} \frac{m}{i} \alpha_i \qquad (7\text{-}22)$$

where

Q_{CCF} = the failure probability of *k* and greater than *k* components due to CCF

Q_T = the random failure rate (total)

m = the number of total rods in the component group

k = the failure criteria for a number of rod failures in the component group

α_i = the ratio of *i* and only *i* CCFs to total failures.

7.5.2 Specific Failure Criterion

In terms of the Alpha Factor model, the BE probability for a specific k failures out of a system of m components (assuming a staggered testing scheme) is shown in the following equation:

$$BE_{CCF} = Q_T \sum_{i=k}^{m} C_i \frac{(m-i)!(i-1)!}{(m-1)!} \alpha_i^{(m)} \tag{7-23}$$

where

C_i ≡ number of combinations of k component failures that will fail the system.

A specific failure criterion is represented by the C_i term in Equation (7-23). An example of a specific failure criterion is shown in Figure 7-3. This example applies to the 6/8 bistable CCF event used in some RPS fault trees. In this example, the failure criterion is described in shorthand as 6/8. This is based on specific criteria of failure of two of two components to fail a channel and failure of at least three of four channels to fail the system or function. Some of the combinations of six component failures will fail three channels (e.g., those combinations where two failures are in each of three channels). Some combinations of six will fail only two channels (e.g., those combinations that have less than two failures in a channel). The valid failure combinations are counted and the sum becomes the Ci term in the BE equation. When a channel is taken out of service for maintenance, it is placed in a non-tripped status. The criteria then become two of two components and two or more of the remaining three channels. This maintenance event is described in shorthand as 4/6 |8.

7.5.3 One-Out-of-Two-Twice Logic

In one-out-of-two-twice logic, Equation (7-23) is used again but the counting of the C_i term is based on a different system. An example of this failure criterion is shown in Figure 7-4. This example applies to the two of four reactor trip breaker CCF events used in some RPS fault trees. In this example, the failure criterion is described in shorthand as 2/4. This is based on failure of two of two components to fail a channel and failure of one of two channels to fail a train. Some of the combinations of four component failures will fail two channels but no trains (e.g., those combinations where two failures are in each of two trains). Some combinations of four will fail an entire train (an example is shown in the failure side of Figure 7-4). The valid failure combinations are counted and the sum becomes the C_i term in Equation (7-23). When a component is taken out of service for maintenance, it is placed in a non-tripped (bypassed) status. The possible combinations are counted with the component always failed. This maintenance event is described in shorthand as 1/3 |4.

7.5.4 CCF Basic Event Probability Equations

Table 7-5 shows some CCF BE probability equations used in various fault trees. All of the equations are based on staggered testing.

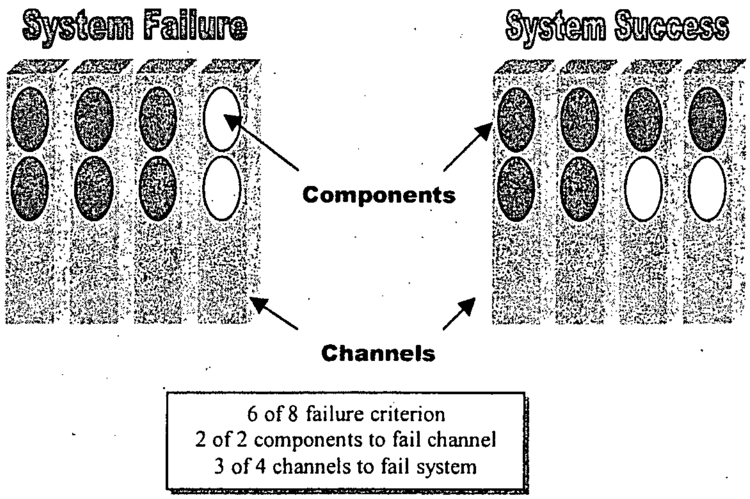
7.6 Treatment of Uncertainties

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:

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

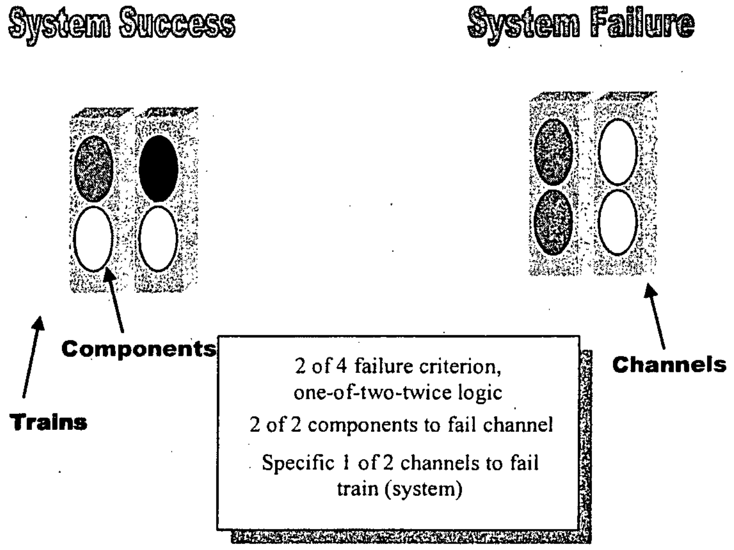
- Uncertainty in translating event characteristics to numerical parameters for impact vector assessment

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



Note: Black ellipses => failure
White ellipses => success

Figure 7-3. Example of a specific failure criterion.


System Success
System Failure
Components
Trains
Channels
2 of 4 failure criterion,
one-of-two-twice logic
2 of 2 components to fail channel
Specific 1 of 2 channels to fail
train (system)

Note: Black ellipses => failure
White ellipses => success

Figure 7-4. Example of a one-out-of-two-twice logic failure criterion for a 2-out-of-4 system.

Table 7-5. Failure criteria and basic event equation table.

Failure Criteria			
Channel or Train Level	Component (within channel or train)	Shorthand Criterion[a]	Basic Event Probability Equations
1/2	2/2	2/4 [b]	$(\alpha_4 + 4\alpha_3/3 + 2\alpha_2/3) * Q_T$
3/4	1/1	3/4 [c]	$(\alpha_4 + 4/3\ \alpha_3) * Q_T$
3/4	1/1	2/3 |4	$(\alpha_4 + 4/3\ \alpha_3 + 3/3\ \alpha_2) * Q_T$
3/4	2/2	6/8 [d]	$(\alpha_8 + 8\alpha_7/7 + 4\alpha_6/21) * Q_T$
3/4	2/2	4/6 |8 [d]	$(\alpha_8 + 8\alpha_7/7 + 16\alpha_6/21 + 12\alpha_5/35 + 3\alpha_4/35) * Q_T$
6/6	1/1	6/6 [c]	$(\alpha_6) * Q_T$

a. Shorthand criteria with the form x/y |z are maintenance events involving one channel or train taken out of service due to maintenance.

b. This criterion is based on the one-out-of-two logic described in Section 7.5.3.

c. This criterion is based on the any-*k*-of-*m* logic described in Section 7.5.1.

d. This criterion is based on the specific failure criterion described in Section 7.5.2.

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 although 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 variability. Nevertheless, the potential for major variability 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 variability 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 7.4 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 2, to an underestimation of uncertainties while producing nearly exact mean values. Reference 2 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 (Ref. 16) has indicated the difference between the results of the formal approach and those based on average impact vectors is not significant. This is particularly true when compared with the impact of other sources of uncertainty, such as plant-to-plant and analyst-to-analyst variability 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 2. These distributions are combined to obtain the overall range of uncertainty in the CCF frequency estimate.

Among the models available, 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 used to generate the data. (This is not the case, however, for the MGL model.) The statistical uncertainty distribution of the Alpha Factor model parameters can be developed using Bayesian techniques as described in Reference 2.

Both the homogeneous and non-homogeneous 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 database. The resulting distribution from this procedure is expected to be wider than the distribution obtained based on the non-homogeneous assumption.

8. CCF PARAMETER ESTIMATION

After independent event count and CCF event information have been entered into the CCF database and quality assurance verification completed, the next step is the estimation of CCF parameters using the software developed for performing quantifications. The parameter estimation software developed for this project uses the impact vector method described in Reference 2; the approach introduced in Reference 3 is used to evaluate the event impact vector based on physical characteristics of the event. These physical characteristics include component degradation parameter, timing factor, and shared cause factor. In addition, the software allows the user to modify the generic event impact factors for plant-specific applications, including mapping the impact vectors to account for differences in CCCG size between the plant in which the event occurred and the plant for which the data are being modified. Other software features include parameter estimations for both Alpha Factor and MGL models.

The CCF database system was developed for the personal computer. It contains the CCF events in a searchable database and options to estimate CCF parameters. It provides a number of capabilities to users with different interests and levels of expertise in CCF event analysis. The parameter estimation process is a three-step process: (1) search the CCF database to obtain the events of interest, usually sorted by system, component, and failure mode, (2) analyze the data from the search, and (3) estimate the CCF parameters. Mechanics of using the software to perform parameter estimations is contained in the CCF database software help file. The CCF system has two main options, allowing users to perform either generic analyses or plant-specific analyses of CCF events included in the database.

Generic analysis uses data pooled from multiple plants. Generic analysis of CCF events in the database includes a qualitative analysis of causes and severity of CCF events and a quantification of generic CCF parameters (Alpha Factor and MGL models). These can be used in risk and reliability studies or other applications such as trending of industry performance with respect to a single class of failures.

Plant-specific analysis allows users to specialize (modify) the CCF events in the database for application to a specific plant by considering design and operational differences between the plant where the event occurred and the plant of interest (target plant), and to estimate CCF parameters that reflect the specific features of the plant being studied. This is recommended in Reference 2 as the preferred approach for plant-specific analyses.

Flexibility is built into the CCF system to enable the PRA analyst to add or remove CCF events from a set of data (application) provided by the database search capability in recognition that a precise definition of a CCF may vary from one PRA study to another. The events in the database, therefore, include more events than those that might be appropriate for use in a given PRA or other studies.

The classification of events (both CCFs and independent failure data) represents the best judgment of experienced analysts who have applied a set of carefully designed rules to ensure consistency and minimize subjectivity. The PRA analyst, however, can modify various attributes of the events in a copy of the database, leaving the original database intact as a reference point. This type of modification requires a relatively high degree of experience and is not expected to be the primary application of the CCF system.

While in the CCF system, an analyst may search CCF database to obtain information on various aspects of the CCF data, such as the distribution of proximate causes (collectively or component by component). The software allows the user to specify a subset of the attributes of the events as the search criteria to obtain a subset of the database having those attributes. This enables the user to develop a statistical base for the study of generic differences among different classes of plants or systems, as well as a trend of CCF events by plant or across the industry.

8.1 Database Search

The CCF events that have been entered into the database cover a large range of systems and components and vary in importance from a PRA perspective. Searches for CCF events to be included in parameter estimations can be structured to prevent inclusion of events irrelevant to an individual study. For example, before searching for AFW pump events (which include either motor-driven pump CCF events, turbine-driven pump CCF events, or CCF events that include both pump types), the analyst must decide to include either all pump types (searching for motors, turbines, and pumps) or only one pump type and then search the CCF database accordingly.

Using the search option, the PRA analyst can select the data fields of interest (system, component, failure mode, shared cause factor, cause, type, etc.), search the database based on the coded event information entered in those fields, and identify the events whose fields meet the specified search criteria. For example, to search the database for the AFW pumps that fail to start on demand and the events that are important from a PRA perspective, the search criteria would specify

- System code for AFW
- Component code for motor-driven pumps; turbine-driven pumps; motors, turbines, and pumps
- Failure mode of failure to start
- Event type of CCF.

Following the search, the events are saved in an application for analysis. The search criteria are also saved in each user's profile. When new data are distributed to users, the applications can be updated to include new data without having to recreate the search criteria.

8.2 Data Analysis

Once the analyst selects the events to be included in the analysis, the CCF database system performs all calculations for the parameter estimations. Because of the relative rarity of CCF events in operational experience, CCF events from similar plants can be pooled together to obtain enough data for use in reliability and risk studies; these are the "generic" estimations. The analysis uses CCF data that involve degradations as well as those involving total failures. The data from any search can be saved for future reference and can be used with either the generic or plant-specific software options.

All CCF event data saved from a search can be reviewed for applicability for specific studies. Some events may be coded in a manner that does not reflect the PRA analyst's perception of the events. Each event can be reviewed to give the analyst an opportunity to modify or delete a copy of the event from consideration in the specific application. The data fields that can be modified are component degradation level, timing factor, shared cause factor, and average impact vector. The software system defaults to not modifying the data. Once the PRA analyst has determined and entered the data modifications, the software calculates the average impact vector for the selected set of CCF events. During sensitivity studies, the average impact vector values can be changed and saved for calculating parameter estimates.

Additionally, the PRA analyst may want to analyze the CCF data for applicability to a particular plant using the plant-specific option. In this case, some data may not be applicable because of a difference in plant configuration or in shared cause factors between the original event and the target plant. As in the generic option, event data can be modified or an event may be deleted from the analysis. The fields that can be modified are cause, shock type, component degradation level, shared cause factor, map up factor, event type, timing factor, shared cause factor, average impact vector, and application-specific impact vector. Once the analyst has determined and entered the applicability of an event, the software calculates the specific impact vector. Similar to the average impact vector values, the specific impact vector values can be modified and stored for use in parameter estimations.

8.3 Estimation of CCF Parameters

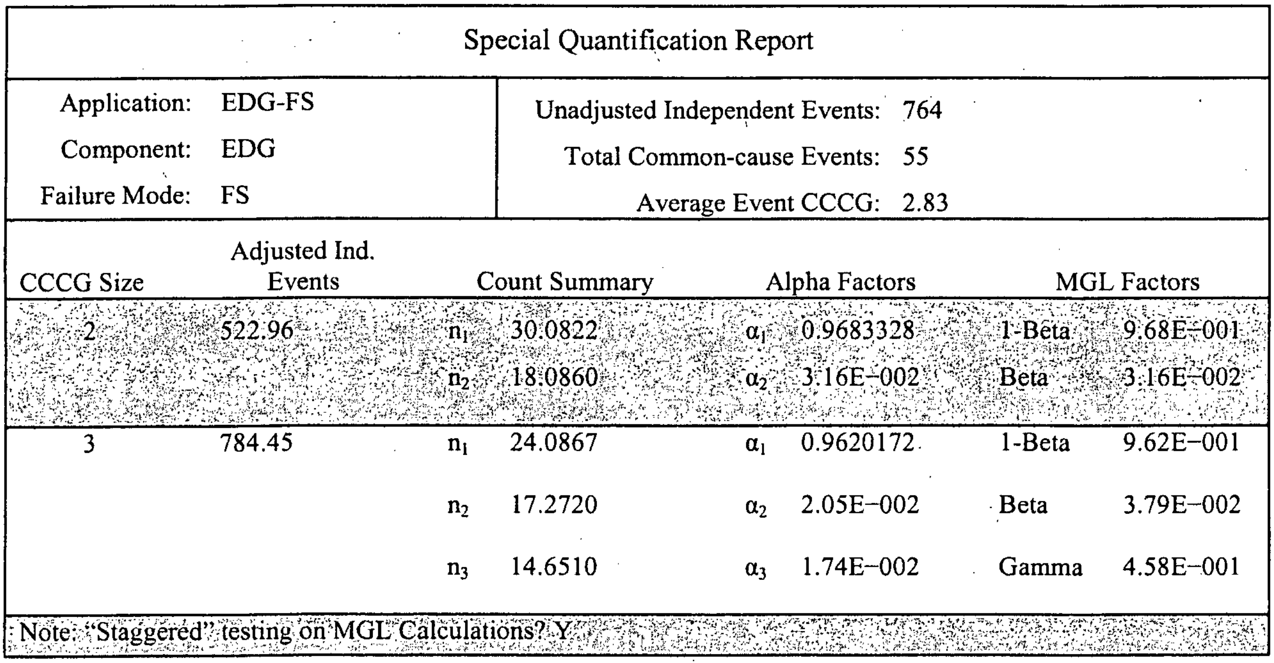
After event data are prepared for parameter estimation, the final analytical step is to perform the parameter estimation using either of the two different quantification methods (generic or specific). In both options, a CCF parametric model is selected (Alpha Factor, MGL, or both) and the calculations are performed.

The output of the parameter estimations is displayed in several ways: tabular, graphically, or electronically for transfer to other software applications. Uncertainty calculations are also provided. Figure 8-1 displays an example of output from the CCF system showing summary results of an EDG analysis, including generic estimates of the CCF frequency parameters for the failure-to-start mode.

The parameter estimation software uses the impact vector approach. Reference 2 discusses the use of event impact vectors. Using the assessments from the event coding, this method classifies the individual CCF events according to the level of their impact on the overall CCF effect on the PRA study and the associated uncertainties in numerical terms. These impact vectors represent the certainty that each event is a CCF event. They are based on the component degradation factor, timing factor, and shared cause factor. Once the individual event impact vectors are determined, the average impact vector for the CCCG of interest (e.g., EDGs) is calculated. The independent event counts are included in the CCF database and are sorted by system, component, failure mode, source (LER, NPRDS, or EPIX), and docket. The user has the option of modifying the independent event value if there is uncertainty about the number provided or if there are additional assumptions or information to be used in the analysis.

The generic analysis option of the CCF software performs an estimation of CCF parameters from pooled plant data, which can be used in risk and reliability studies, or other applications such as trending of industry performance with respect to specific types of failures. CCF data are used in the Accident Sequence Precursor Program, safety system reliability studies, Standardized Plant Analysis Risk models, and for resolution of NRC generic issues.

The plant-specific analysis option of the CCF software allows the analyst to modify event coding to adjust CCF event data for design or operational differences between the plant where the actual CCF event occurred and the plant to which the data are applied. The software allows the analyst to review each event and modify various attributes of the event or delete the event from consideration in parameter estimations. Two adjustment factors, the cause applicability factor and the shared cause factor applicability, can be used to reflect the analyst's interpretation of the differences between the two plants. The changes are saved in a copy of the database for the particular application for later use, while the data in the original database are not changed. As with the generic estimations, the analyst may use the independent events that are in the CCF database by individual plant or the analyst may choose another value based on knowledge of the target plant. Additionally, the software includes the capability to adjust the size of the CCCG (using mapping factors) so that an event that occurred at a plant with *n* similar components may be applied to a plant that has *m* such components.



Special Quantification Report

Application:	EDG-FS	Unadjusted Independent Events:	764
Component:	EDG	Total Common-cause Events:	55
Failure Mode:	FS	Average Event CCCG:	2.83

CCCG Size	Adjusted Ind. Events	Count Summary		Alpha Factors		MGL Factors	
2	522.96	n_1	30.0822	α_1	0.9683328	1-Beta	9.68E−001
		n_2	18.0860	α_2	3.16E−002	Beta	3.16E−002
3	784.45	n_1	24.0867	α_1	0.9620172	1-Beta	9.62E−001
		n_2	17.2720	α_2	2.05E−002	Beta	3.79E−002
		n_3	14.6510	α_3	1.74E−002	Gamma	4.58E−001

Note: "Staggered" testing on MGL Calculations? Y

Figure 8-1. Parameter estimation example.

9. GLOSSARY

Alpha Factor: The fraction of the total frequency of failure events that occur in the system involving the failure of *k* components in a system of *m* components due to a common-cause.

Application: A particular set of CCF events selected from the CCF database for use in a specific study.

Available: Describes a component that is capable of performing its function according to a specified success criterion. (Note: available is not the same as availability.)

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 components (in mission, manufacturer, maintenance, environment, etc.) that are considered to have a high potential for failure because of 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, Basic Parameter, and 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: 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: The component status concerning its intended function. Two general categories of component states are defined as available and unavailable.

Coupling Factor: The condition or mechanism through which failures of multiple components are coupled.

Failure: Describes a component not capable of performing its specified operation according to a success criterion.

Functionally Unavailable: Describes a component that is capable of operation, but the function normally provided by the component is unavailable because of lack of proper input, lack of support function from a source outside the component (i.e., motive power, actuation signal), maintenance, testing, improper interference of a person, etc.

Degraded: Describes a component in such a state that it exhibits reduced performance but insufficient degradation to declare the component unavailable according to the specified success criterion.

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 CCFs.

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

$$P[A \cap B] = P[B \mid A]P[A] = P[A \mid B]P[B] \neq P[A]P[B]$$

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

Event: 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 CCF 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 determined 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.

Incipient: Describes a component in a condition that, if left un-remedied, could ultimately lead to a degraded or unavailable state.

Independent 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 CCF. The result of mapping an impact vector is an adjusted impact vector applicable to the target plant.

Mapping Down Factor: A factor used to adjust the impact vector of an event when the exposed population of the target plant is lower than that of the original plant that experienced the CCF.

Mapping Up Factor: A factor used to adjust the impact vector of an event when the exposed population of the target plant is higher than that of the original plant that experienced the CCF.

Multiple Greek Letter: For a system of *m* redundant components and for each given failure mode, *m* different parameters are defined. Each parameter represents the conditional probability that the common-cause of a component failure will be shared by *n* or more additional components.

p-value: A probability that indicates a measure of statistical significance. The smaller the p-value, the greater the significance. A p-value of less than 0.05 is generally considered statistically significant.

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

Potentially Unavailable: Describes a component that is capable of performing its function according to a success criterion but an incipient or degraded condition exists. (Note:

Potentially unavailable is not synonymous with hypothetical.)

Mission Time: The time period (usually in hours) that a component is generally required to successfully operate to mitigate an event when modeled in a PRA or IPE. Most PRA mission times are assumed to be 24 hours.

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).

Shared Cause Mechanism: A set of causes and factors characterizing why and how a failure is systematically induced in several components.

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: lethal and non-lethal.

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 CCF. This can be viewed as an indication of the strength-of-coupling in synchronizing failure times.

Unavailable: Describes a component that is unable to perform its intended function according to a stated success criterion. Two subsets of unavailable states are failure and functionally unavailable.

10. REFERENCES

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

2. U.S. Nuclear Regulatory Commission, "Procedures for Treating Common-cause Failures in Safety and Reliability Studies," NUREG/CR-4780, Volume 1, January 1988, and Volume 2, January 1989.

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

4 U.S. Nuclear Regulatory Commission, "Common-Cause Failure Database and Analysis System: Overview," NUREG/CR-6268 (INEEL/EXT-97-00696), Volume 1, June 1988.

5 U.S. Nuclear Regulatory Commission, "Common-Cause Failure Database and Analysis System: Event Definition and Classification," NUREG/CR-6268 (INEEL/EXT-97-00696), Volume 2, June 1998.

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

7 U.S. Nuclear Regulatory Commission, "Common-Cause Failure Database and Analysis System: Software Reference Manual," NUREG/CR-6268 (INEEL/EXT-97-00696), Volume 4, June 1998.

8. U.S. Nuclear Regulatory Commission, "Common-Cause Failure Parameter Estimations," NUREG/CR-5497 (INEEL/EXT-97-01328), October 1998.

9. 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.

10. Mosleh, A., et al., "On Quantitative Analysis of Common-cause Failure Data for Plant-Specific Probabilistic Safety Assessments," UMNE-92-004, University of Maryland Nuclear Engineering, prepared for the U.S. Nuclear Regulatory Commission, August 1992.

11. U.S. Nuclear Regulatory Commission, "Overview and Comparison of U.S. Commercial Nuclear Power Plants," NUREG/CR-5640 (SAIC 89/1541), September 1990.

12. *U.S. Code of Federal Regulations*, Subpart 55a, "Codes and Standards," Part 50, "Domestic Licensing of Production and Utilization Facilities," Chapter I, Title 10, "Energy."

13. *U.S. Code of Federal Regulations*, Appendix J, "Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors," Part 50, "Domestic Licensing of Production and Utilization Facilities," Chapter I, Title 10, "Energy."

14. Mosleh, A., G. Parry, and A. F. Zikria, "An Approach to the Analysis of Common-cause Failure Data for Plant-Specific Application," *Nuclear Engineering and Design*, 150:25–47, 1994.

15. Kvam, P., "Estimation Techniques for Common-cause Failure Data with Different System Sizes," *Technometrics*, 38(4):382–388, 1996.

16. Siu, N., and A. Mosleh, "Treating Data Uncertainties in Common-cause Failure Analysis," *Nuclear Technology*, 84:265–281, 1989.

NRC FORM 335
(9-2004)
NRCMD 3.7

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, Rev. 1

2. TITLE AND SUBTITLE

Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding

3. DATE REPORT PUBLISHED

MONTH	YEAR
September	2007

4. FIN OR GRANT NUMBER

Y6546

5. AUTHOR(S)

T.E. Wierman, INL; D.M. Rasmuson, NRC; A. Mosleh, University of Maryland

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

NA

8. PERFORMING ORGANIZATION - 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 Laboratory, Risk & Reliability Assessment , P.O. Box 1625, Idaho Falls ID 84315-3850
University of Maryland, 2181 Glenn L. Martin Hall, College Park, MD 20742

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.)*

Division of Risk Assessment and Special Projects
Office of Nulcear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

10. SUPPLEMENTARY NOTES

A.D. Salomon, Project Manager

11. ABSTRACT *(200 words or less)*

This report on the Common Cause Failure Database and Analysis System presents an overview of common cause failure (CCF) analysis methods for use in the U.S. commercial nuclear power industry. Idaho National Laboratory staff identify equipment failures that contribute to CCF events through searches of Licensee Event Reports, Nuclear Plant Reliability Data System failure reports, and Equipment Performance and Information Exchange failure reports. The staff then enter the event information into a personal computer-based data analysis system (CCF system). This report summarizes how data are gathered, evaluated, and coded into the CCF system, and describes the process for using the data to estimate probabilistic risk assessment common cause failure parameters.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

common-cause failure, CCF, shared cause, proximate cause, timing factor, dependent failure, data collection

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)
Unclassified

(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS