NUREG/CR-6268
Vol. 3
INEEL/EXT-97-00696

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

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

Idaho National Engineering and Environmental Laboratory

University of Maryland

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-6268
Vol. 3
INEEL/EXT-97-00696

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

Manuscript Completed: June 1998
Date Published: June 1998

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

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

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

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

ABSTRACT

This volume of the Common Cause Failure Database and Analysis System report documents the method used for coding common cause failure (CCF) events that are stored in the common cause failure database.

Equipment failures that contribute to common cause failure events at commercial nuclear power plants in the U.S. are identified during Licensee Event Report (LER) and Nuclear Plant Reliability Data System (NPRDS) failure report reviews. Once equipment failures that contribute to a common cause failure event are identified, the common cause failure events are coded for entry into a personal computer storage system using the method presented in this volume.

The database resulting from coding common cause failure events is used to estimate common cause failure parameters for use in various probabilistic risk assessment (PRA) CCF models.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

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

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

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

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

Sufficient information is recorded to ensure accuracy and consistency. Additionally, the CCF events are stored in a format that allows PRA analysts to review the events and develop an understanding on how they occurred.

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

ACRONYMS

AEOD	Nuclear Regulatory Commission's Office for the Analysis and Evaluation of Operational Data
AFW	Auxiliary Feedwater System
ASCII	American Standard Code for Information Interchange
BW	Babcock and Wilcox
CCF	Common Cause Failure
CCCG	Common Cause Component Group
CE	Combustion Engineering
ESF	Engineered Safety Feature
GE	General Electric
INEEL	Idaho National Engineering and Environmental Laboratory
INPO	Institute of Nuclear Power Operations
LERs	Licensee Event Reports
MOV	Motor Operated Valve
NOAC	Nuclear Operations Analysis Center
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
PC	Personal Computer
PRA	Probabilistic Risk Assessment
QA	Quality Assurance
RPS	Reactor Protection System
SCSS	Sequence Coding and Search System
W	Westinghouse

Common Cause Failure Database and Analysis System Volume 3—Data Collection and Event Coding

1. INTRODUCTION

1.1 Background

The Nuclear Regulatory Commission (NRC) Office for the Analysis and Evaluation of Operational Data (AEOD) and the Idaho National Engineering and Environmental Laboratory (INEEL) developed a common cause failure (CCF) database for the U.S. commercial nuclear power industry. It includes a method for identifying CCF events and a computer system for storing and quantifying the data for use in Probabilistic Risk Assessment (PRA) studies. CCF events are defined in Reference 1 as "a subset of dependent failures in which two or more component functional fault states exist at the same time, or within a short interval, as a result of a shared cause." Similar failures within a short time interval at multiple unit sites do not constitute a CCF event.

1.2 CCF System Summary

The INEEL staff developed methods to identify CCF events and a personal computer based system for storing and analyzing the events. This volume of the series describes the method for obtaining failure data, provides guidance for identifying CCF events, provides guidance for coding CCF events from either the Nuclear Plant Reliability Data System (NPRDS) database failure reports or Licensee Event Reports (LERs) obtained from the Sequence Coding and Search System (SCSS) database, and establishes a review process to ensure data quality. In addition, this volume explains CCF and independent event coding rules, and provides examples for applying the codes. A sample coding sheet, system list, and examples of CCF events are provided in the appendices. The CCF data analysis process is shown in Figure 1. The numbers in parentheses after each block correspond to the numbers given after the associated section number in the remainder of this volume. All segments of the process are discussed in this volume, except for parameter estimations, which are discussed in Volume2[1].

1.3 CCF Event Definition

For this project, a CCF event is defined by the following criteria:

1. Two or more components fail or are degraded at the same plant. Failures are discovered during equipment challenges to operate, surveillance testing, or design deficiencies that are detected prior to operating the equipment. In the case of a failure resulting from a design deficiency, a potential failure is considered to have the same severity as a failure that results from a challenge to the equipment, provided the design deficiency would have caused a component to fail on demand. For example, a wiring discrepancy that would prevent a pump start is considered to be a complete failure, even if no start was attempted.

2. Component failures occur within a selected period of time.

3. The component failures result from a single shared cause and are linked by a coupling mechanism such that other components in the group are susceptible to the same cause and failure mode.

4. The equipment failures are not caused by the failure of equipment outside the established component boundary.

All events that meet the above criteria are identified as CCF events and included in the CCF database. The collection of source data, identification of CCF events, coding of CCF events, and database quality assurance are described in the following sections of this volume.

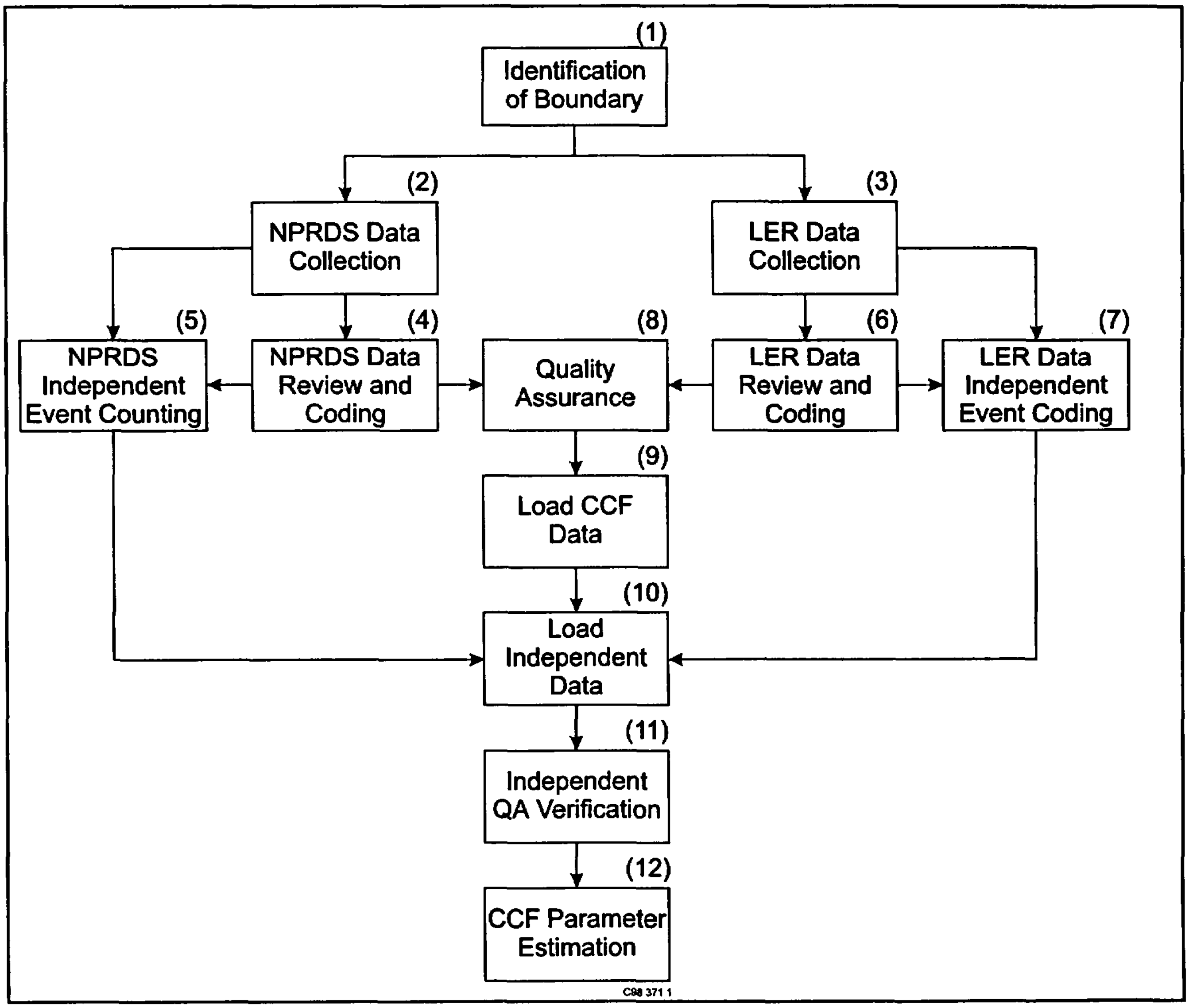

Figure 1. CCF data analysis process.

2. DATA COLLECTION

The INEEL staff has used the LER and NPRDS data for identifying CCF events. This section of the report provides criteria for obtaining the LER and NPRDS data used in CCF event analysis, and the criteria for identifying CCF events. Information on NPRDS data fields is located in the *NPRDS Reporting Guidance Manual*[2]. Information on LER data fields and SCSS search information is located in the *Sequence Coding and Search System for Licensee Event Reports*[3]. (It is assumed at this point that the reader is knowledgeable about NPRDS and LER data.)

This section documents the process used to gather and identify CCF events in NPRDS and LER data. This is a three step process: (1) data collection preparation, (2) data download, and (3)screening of text to identify CCF events. These steps are discussed in the remainder of Section 2.

2.1 Data Collection Preparation

The current CCF system was developed to analyze CCF events within a single system. To ensure that data are consistently gathered and analyzed to meet the PRA modeling requirements, search criteria have been developed to standardize data collection. The goal for developing data search criteria is to collect failure data that have the potential to contribute to a CCF event, and to eliminate data that are not relevant to PRA modeling.

Performing search and data download criteria preparation includes identifying general boundaries for each system and component data set, and then developing boundaries that are specific to the data source. Each are discussed in the following sections. An example of the data collection information is shown in Figure 2.

2.1.1 Identification of Boundaries (1) Prior to obtaining data, INEEL staff developed search criteria. While developing NPRDS and SCSS database search criteria, specific restrictions on the searches are developed and documented in four steps: (1) identify the data set to be analyzed, (2) identify component boundaries, (3) identify operational event boundaries, including failure modes, and (4) perform a system characterization. Each step is documented and records kept for quality assurance (QA) traceability.

The first step is to identify the type of component to be evaluated. The system and component combinations that have been selected for analysis are those addressed in PRA modeling for which CCF parameters are needed. An example is the auxiliary feedwater (AFW) system at pressurized water reactors (PWRs); components of interest within this system are valves and pumps.

The second step is to identify component boundaries. It is necessary to identify if and how the components are partitioned into sub-components in PRA models.

Examples of components with sub-components are motor operated valves (MOV) and pumps (PMP). A failure data set for the analysis of AFW system MOVs includes failures of the valves, motor operators, and circuit breakers. Since the design, construction, and installation of all MOVs are essentially the same, the boundaries for each MOV in the system are the same.

The component boundaries for AFW pumps includes the pumps, drivers, circuit breakers, steam control valves, and turbine governors. AFW motor-driven pump boundaries include the motor and circuit breaker. Turbine-driven pumps include the steam control valves and turbine governor. Some CCF events affect only the mechanical pump, so the driver type is irrelevant, and all pump types are included.

1. Relevant NPRDS system codes are: BW plants HHB, W plants HHC, and CE plants HHJ.

2. The operational event boundary is defined as follows:

   The safety function (PRA mission) for auxiliary feedwater it to provide water to the steam generators for residual heat removal from the reactor coolant system. Using the PRA mission as a basis, the event boundary is a condition that does not permit flow from the pumps.

   Overall, the event boundary is any failure that renders pumps and pump drivers inoperable. This includes suction and discharge lines, pumps, pump drivers, and motive forces up to steam stops or supply breakers.

   Functional failure modes are failure-to-start (FS) and failure-to-run (FR).

3. Components identified for evaluation are as follows:

   Pumps
   Turbines and controllers (governors)
   Motors and motor circuit breakers

4. Component boundaries are defined as follows:

   Pumps—The pump and all internal parts: suction lines, pump driver bearings, equalizing lines, discharge lines, and lubrication system.

   Turbines—The turbine and all internal parts: governor, steam-stop-valve, lubrication system, control circuits, and cooling water heat exchangers.

   Motors—The motor and all internal parts: lubrication system, circuit breakers, and control circuits (including relays).

5. Component NPRDS application codes considered during analysis are listed by reactor vendor. For this system analysis, only application-code-specified components are considered.

Application	Description
AFPU	Auxiliary feedwater pump
AFPUMO	Auxiliary feedwater pump motor
AFPUMOCK	Auxiliary feedwater pump motor circuit breaker
AFPUTU	Auxiliary feedwater turbine
AFPUTUGOME	Auxiliary feedwater turbine governor

6. The time frame for the analysis is failure records input into the NPRDS database after January 1, 1984 and with failure start/discovery dates before December 31, 1995.

7. Incipient records are excluded.

8. Only safety-equipment records are included.

Figure 2. Example of AFW pump data collection preparation.

In some PRA analyses, pumps consist of the entire assembly, while in other analyses, pumps are partitioned into sub-components of pumps and drivers. The boundaries for each component and sub-component are established based on the partitions. Further partitioning of subcomponents may be necessary because of factors that cause a CCF event. For example, when analyzing pumps, generally the pumps are sub-divided into pumps and drivers because CCF events are different between pumps and drivers. However, in the case of AFW pumps, drivers are sub-divided further into turbines, diesel engines, and motors. This additional partitioning is performed because there are CCF events that affect only one type of pump driver. For example, failures that result in the loss of steam turbine operability generally cannot be analyzed with failures that result in a loss of electrical power to a motor.

The SCSS and NPRDS data searches are performed for each component, including the sub-components. The CCF analysis considers CCF factors that are common among various types of components and sub-components, such as oil supplies, maintenance practices, and cooling water. When failures resulting from common factors can be linked, the failures are characterized and coded as a CCF event, regardless of which sub-components are affected.

The third step is to identify system success criteria and identify associated system/component failure modes. System success criteria are the operating conditions required to satisfy system safety function (PRA mission). This assists the analyst in evaluating the failure report to determine the PRA impact of the failure. The failure modes are the ways a component fails that affects the ability of the component and system to perform the PRA mission. Examples of failure modes used in a PRA for AFW pumps are failure-to-start and failure-to-run. Failure modes can be used to differentiate between severity levels of similar events. For example, both 'LI' and 'VR' are valve leakage failure modes, but 'LI' is a lower severity event with no system effect. This allows the analyst to distinguish between event types for independent events.

The fourth step is to perform a system characterization analysis that includes plant-specific data about the system of interest. Understanding the system configuration allows an analyst to identify a CCF event and its associated common cause component group size (CCCG). The characterization analysis is performed using primarily the plant drawings. Additional sources used are the data recorded in the *Nuclear Power Plant System Sourcebooks*[4], plant Final Safety Analysis Reports, operator examination lesson plans, reports from previous studies, and research data compiled from operators and operator-examiners that have visited the plants. The characterization analysis consists of identifying the number of trains in the system and the number of each component type that could be exposed to a CCF event.

At the completion of the boundary identification, searches of NPRDS and SCSS (for LERs) are performed. Specific search criteria, developed for each data source, are discussed below.

2.1.2 NPRDS Specific Search Criteria. The NPRDS database is maintained by the Institute of Nuclear Plant Operations (INPO). The database consists of component failure records for U.S. commercial nuclear power plants, and is accessed by the INEEL for NRC sponsored studies.

NPRDS failure reports provide background information on the equipment and failure (cause, corrective action, how the failure was identified, failure narratives, etc.). The focus of an NPRDS failure report is the component, rather than the plant or system as a whole.

The NPRDS data search is based on establishing search boundaries as described in Section 2.1.1 and using the *NPRDS Reporting Guidance Manual*[2]. Search criteria are based on the following:

1. NPRDS manuals are used to identify NPRDS component, system, and application codes for the component and system being analyzed.

2. Data input to NPRDS prior to January 1, 1984 are not considered reliable and are excluded.

3. Incipient failure reports are excluded from the NPRDS data downloads because they are not consistently reported and are not considered to be failures.

4. Only safety related component failures are included.

2.1.3 LER Specific Search Criteria. The Nuclear Operations Analysis Center (NOAC) of Oak Ridge National Laboratory (ORNL) developed CCF and independent failure search algorithms of the SCSS database to locate LERs that document component failures for particular components and systems.

The SCSS database is a system that stores, in computer-searchable format, the sequence of occurrences described in each LER. LERs contain information regarding component failures, personnel errors, system/train failures, engineered safety feature (ESF) actuations, and reactor protection system (RPS) actuations (e.g., automatic and manual reactor shutdowns). The LER data focus primarily on plant events, and not individual component failures with the same level of detail as NPRDS.

For an SCSS search, the basic definition of a CCF event is to identify "any actual or potential failure of multiple pieces of equipment within a system, because of a common or similar cause, that could adversely impact the redundancy of a particular system." Using the system and component of interest and definitions, a complete search algorithm is developed.

The CCF search algorithm is constructed in segments: (1) any actual or potential failures of multiple similar components within one system, (2) any actual or potential failure of multiple trains within the same system, and (3) any fabrication/manufacturing deficiency for multiple components resulting in an actual or potential failure within the system. These search elements are sequentially executed in a mutually exclusive manner, so that any LERs retrieved in one part of the search are not duplicated in another part of the search. The LERs retrieved are combined into one group, resulting in a CCF search for the system or component of interest.

Once the CCF search algorithm is performed, the SCSS database is searched for independent failures to complement the CCF searches. This is accomplished by retrieving LERs that involve actual or potential failures or degradations of the component or system of interest that were not retrieved by any elements of the CCF search mentioned above.

2.1.4 Summary of Preparation. Following completion of the NPRDS and SCSS search criteria development, the results are documented and saved for quality assurance traceability. Figure 2 depicts the results of the data collection preparation. The next step is to download the data from the two data sources.

2.2 Data Download

The data download process is performed in two separate steps, one for each data source, and is discussed below.

2.2.1 NPRDS Data Download (2). The NPRDS database is searched and applicable data downloaded, using criteria established in Section 2.1.2, and guidance from the *NPRDS Information Retrieval Guide*[5]. The source data file is stored for quality assurance traceability.

2.2.2 LER Data Download (3). An LER search is performed on the SCSS by the ORNL staff using the search criteria established in Section 2.1.3 and Reference 3. These files are stored for quality assurance traceability.

2.3 Identification of CCF Events

Identification of CCF events is accomplished by reviewing NPRDS failure reports and LER abstracts.

2.3.1 Review of NPRDS Data (4). The process of reviewing NPRDS data for CCF events includes grouping the events by failure date and reviewing the failure narratives for similar event descriptions and causes.

2.3.1.1 Grouping NPRDS Data. The NPRDS data are loaded into a database and are electronically grouped by failure date. The grouping is to assist the analyst in identifying NPRDS failure reports that occur within a specified time interval and may be associated with a CCF event.

The time frame between failures was analyzed to develop a method to specify when the mission is compromised and at the same time specify a time frame when failures are routinely discovered. For example, the AFW pumps are required to operate for 24 hours following most design basis events. It is assumed that two failures occurring less than 24 hours apart could be expected to impact the PRA mission.

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 also when a large portion of the failures are discovered. The inservice testing requirements of 10 CFR 50 Appendix J govern most safety related component testing. 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, emergency diesel generators (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.

The failure date for each NPRDS failure report is compared to the failure date for all other failure reports at that plant. If, during comparison, the failure date for one or more reports falls within the testing interval (plus the allowed 25%) of the failure being considered, all reports within that time frame are considered a possible CCF event and grouped together for narrative screening.

As part of the data grouping, two filters are applied to failure data to eliminate failure reports (from the failure grouping) that do not fit the CCF event definition. First, failures from plants that have only one failure in the data set are eliminated. Second, if all failures in a group are for the same component, the group is eliminated because there must be failures of at least two different components to qualify as a CCF event.

2.3.1.2 Review of Narratives (4). Once the groups of NPRDS failure reports are determined, the next step is to identify CCF events by reading and comparing the narratives for the failures in each failure group. The narrative review is performed by personnel that are familiar with both power plant operations and PRA concepts.

During the screening process, groups of failure reports 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 or during situations where the equipment would fail had it been called upon to operate.

2. The time frame 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.

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.

2.3.2 Review of LER Data (6). INEEL staff reviews LER data for both the possible CCF events and the possible independent events.

During the SCSS search (described in Section 2.1.3), LER events are identified as possible CCF events if multiple failures of similar components in the system of interest are reported in a single LER. The printed LER abstracts are reviewed to identify component failures that meet the CCF criteria described in Section 2.3.1.2. Additional information about the event can be obtained from reviewing the complete LER text. The review eliminates failure reports that are not CCF events (i.e., there were no actual failures or the failures were independent). The remaining LERs are coded as CCF events.

The file of independent LER events are grouped by event date (using the same time frame criteria explained in Section 2.3.1.1) to assist in identifying CCF events from multiple similar failures reported in two separate LERs.

2.4 Data Collection Summary

Once all CCF events have been identified, they are coded for entry into the database. All non-CCF event records are reviewed to identify the independent events and the non-failure events. Section 3 describes the coding process for both CCF and independent events. The process is the same for both NPRDS and LER data.

The NPRDS failure reports and LER abstracts for all events collected in the data searches are stored for quality assurance traceability.

After all CCF events have been identified, the LER events are compared to NPRDS events. The purpose of the comparison is to identify and eliminate any duplicate CCF and independent events that were collected during both NPRDS and SCSS searches.

3. CCF DATABASE CODING GUIDANCE

This section of the report describes the information in the CCF database. The CCF database system is a personal computer (PC)-based data management and analysis system using SAGE-ST software[6]. It also provides guidance for the analyst in the selection of codes for both CCF and independent failure events. Guidance for loading data into the CCF database, searching the database, and performing CCF analyses is provided in Volume 4[7] of this report.

3.1 Event Coding

This sub-section of the report describes the information coded into each CCF event data field and presents associated codes for most fields. A sample CCF coding form is provided in Appendix A, with the coding examples.

3.1.1 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 is the source document where the CCF event was identified. An N as the first character represents NPRDS, L represents an LER, and E represents an EPRI report. The DDD portion is the plant's docket number. The YY portion is the year of the event. The #### portion is a sequential four digit event number, it is assigned by the CCF system administrator. The FM is a two character code for the failure mode of the event. A complete list of failure mode codes is provided in Table 1. The failure mode is the same failure mode discussed in Section 3.1.5.

3.1.2 Plant. 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.

3.1.3 Power. 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, this information is not always available, and the field may be left blank. At least two NPRDS 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 from Block 10 of the front page of the LER is used.

Table 1. Failure mode codes.

Failure Mode	Description	Component	Discussion
CC	Fail to open (normally closed)	circuit breaker, fuse, valve, relay	A circuit breaker, relay, or valve that does not open on demand, or a fuse that fails to blow at the correct rating.
FI	Functional inoperability	all	The component is incapable of performing its safety function, but there is no failure of the component. A circuit breaker that correctly trips open in response to a signal, but is subsequently incapable of supplying power to its associated component. A PORV that is not broken, but is isolated by a closed block valve.
FR	Fail to run	blower, compressor, fan, generator, motor, pump, turbine	The component fails to continue running at rated conditions, after reaching rated conditions.

Table 1. Failure mode codes (continued)

Failure Mode	Description	Component	Discussion
FS	Fail to start	blower, compressor, fan, generator, motor, pump, turbine	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	blower, compressor, fan, generator, motor, pump, turbine	The component fails to stop operating.
HI	High voltage/ amperage output	battery, charger, inverter, power supply	The component provides an output that is higher than designed.
LI	Internal leakage	heat exchanger, valve	In heat exchangers, tube to shell side (or vice versa) leakage. In valves, failure of the local leak rate test, with no system effect.
LK	Containment boundary leakage	demineralizer, heat exchanger, pump, strainer, valve	Internal fluid leaks to the environment external to the component.
MF	Reduced flow, no heat transfer effect	heat exchanger	Small reduction in flow that does not result in detectable loss of heat transfer.
NO	No voltage/ amperage output	battery, charger, instrument, inverter, power supply	A device, such as a battery or instrument that fails to provide an output signal.
PG	No flow/plugged	demineralizer, heat exchanger, strainer	Loss of flow or failure of a heat exchanger to transfer heat due to fouling or plugging.
OO	Fail to close (normally open)	circuit breaker, valve, relay	The component fails to close within the required amount of time.
SA	Spurious actuation	circuit breaker, instrumentation, relay, valve	A device that trips to an unintended position due to an unknown cause (possibly a loose connection).
SD	Setpoint drift	instrument, valve	A setpoint found outside the acceptable setpoint band, with no indication that the initial setting was incorrect.
VR	Fail to remain closed (detectable leakage)	valve	The valve is leaking internally past the valve seat, with detectable system effect. If there is evidence that the valve didn't close fully initially, the OO code will be used.
XA	Human error of alignment	all	Incorrect human action that leads to component unavailability (the wrong circuit breaker opened).

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

3.1.5 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 1, which provides some discussion of each failure mode code. The codes listed are based on "Review and Development of Common Nomenclature for Naming and Labeling Schemes for Probabilistic Risk Assessment", NUREG/CR-5905[8]. Some of the failure modes depend on the component being analyzed, so the table identifies the applicable component for each failure mode. The boundary identification, described in Section 2.1.1, 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 code is entered with an event record. To track multiple failure modes, a CCF record is developed 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, since 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 (Section 3.1.8) less than 1.0.

3.1.6 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 2 provides a listing of available component codes, definitions, and guidance for their use.

3.1.7 System. The system field identifies the group of components that work together to perform a specific function which includes failed components. Table 3 provides the system codes. The table in Appendix B provides a translation between NPRDS system codes and appropriate CCF system codes. Some systems have dual functions (Residual Heat Removal and Low Pressure Safety Injection), but only one system code is used. The system function lost because of the CCF event is the system code used in the CCF database.

3.1.8 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 0.00 to 1.00. If there is only one failure mode for multiple failure events, the failure mode applicability is 1.00 since 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 1.00. 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.

3.1.9 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 common cause failure event. The allowable codes are presented in Table 4, which provides definitions and guidance for using coupling factor codes.

3.1.10 Cause. The cause field identifies the reason the components failed. Most failure reports address an immediate cause and an underlying cause. For this project, the appropriate code is the one representing the common cause, or if all levels of causes are common, the most readily identifiable cause.

Table 2. Component codes.

Component	Code	Description
Air operated valve, water	AOV*	Controls flow of water.
Air operated valve, steam	TAV*	Controls flow of steam to pump turbine.
Air operated valve, recirculation	RAV*	Controls flow of water through pump minimum flow recirculation lines.
Battery	BAT*	Provides DC power.
Battery charger	BCH*	Provides recharging DC power to batteries and DC buses.
Blower/fan	BLW	Circulates gases for heat transfer or filtration.
Emergency diesel generator output circuit breaker	CB1*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
Reactor protection trip circuit breakers	CB2*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
6.9 k VAC circuit breakers	CB3*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
4160 V AC circuit breakers	CB4*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
480 V AC circuit breakers	CB5*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
120 V AC circuit breakers	CB6*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
DC distribution circuit breakers	CB7*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
13.2 kV circuit breaker	CB8*	Provides electrical power connection between power source and load, or opens on electrical fault or demand.
Air testable check valve	CKA*	Closes or opens to isolate or permit flow on specific differential pressure.
Vacuum breaker check valve	CKB*	Closes or opens to isolate or permit flow on specific differential pressure.
Stop check valve	CKS*	Closes or opens to isolate or permit flow on specific differential pressure.
Check valve	CKV*	Closes or opens to isolate or permit flow on specific differential pressure.
Compressor	MDC	Produces flow, pressure, and contains the process gas.
Controller	CON	Provides mechanical and electronic control signals for process control.
Damper	DMP	Isolates or permits flow on demand.
Engine	ENG	Provides motive power from a diesel engine.
Emergency diesel generator	EDG*	Provides electrical power with a diesel engine driver.
Electrical bus	BUS	Provides for electrical energy transmittal within electrical gear.
Electrical cable	CBL	Provides for electrical energy transmittal.
Filter/strainer/demineralizer	FLT	Removes materials from fluids, prevents fluid contamination, and contains process fluid.
Fuse	FUS	Passes electrical power or opens on electrical fault.
Generator unit	MGN	Provides electrical power with a electrical motor driver.
Heat exchanger	HTX*	Provides for heat transfer, allows flow, and contains process fluid.

Table 2. Component codes (continued)

Component	Code	Description
Instrumentation and/or control circuit	ICC	Senses process parameters, provides signals of process parameters, transmits signals of process parameters, indicates process conditions, provides control signals for process controllers, and provides trip signals for abnormal process conditions.
Instrument channel	CNL	The instrument train, from sensor to output.
Instrument transmitter	IST	Senses and transmits signals on process parameters.
Inverter	INV	Provides electrical power by changing DC power to AC power.
Load/relay unit	LOD	Provides signals on changes in process state.
Local power supply	LPS	Provides electrical power.
Main Steam Isolation Valve	MSV*	Air or gas operated main steam isolation valve.
	HSV*	Hydraulically operated main steam isolation valve.
Motor-driven pump	MDP*	Pump with an electrical driver.
Motor	MOT*	Provides motive power from electrical energy.
Motor-operated valve, water	MOV*	Isolates water or permits flow on demand; operated by motor operator.
Motor-operated valve, steam	TMV*	Isolates or permits steam flow to pump turbine; operated by motor operator.
Motor-operated valve, both	BMV*	A CCF event that affects a steam MOV and a water MOV.
Pipe segment	PSP	Sections of pipe.
Pump	PMP*	Produces flow, pressure, and contains the process fluid.
Relief valve: air or nitrogen operated	RVA*	Provides process system pressure relief; operated by valve operator.
Relief valve: solenoid operated	RVE*	Provides process system pressure relief; operated by valve operator.
Relief valve: hydraulic operator	RVH*	Provides process system pressure relief; operated by valve operator.
Relief valve: motor operated	RVM*	Provides process system pressure relief; operated by valve operator.
Safety valve	SVV*	Provides process system pressure relief; operated by system pressure.
Strainer, main pump suction or discharge	STR*	Filters debris in main piping line.
Strainer, secondary application	SRS*	Filters debris in secondary or minor piping line.
Strainer, trash racks	SRK*	Stops debris at pump house, "traveling screens."
Sump	SMP	Provides fluid collection location.
Tank	TNK	Provides containment of process fluids.
Transformer	TFM	Provides electrical power while changing the power ratings (amperage and voltage).
Turbine	TUR*	Provides motive power from fluid systems.
Turbine-driven pump	TDP*	Pump with a steam turbine driver.
Valve	VLV	Isolates or permits flow on demand.
Valve operator	VOP	Provides motive force to operate a valve.

*Components for which CCF events are in the CCF database.

Table 3. Systems list (CCF system codes).

CCF system code	CCF system description
ACP	AC power distribution
ADS	Automatic depressurization
AFW	Auxiliary feedwater
ARF	Air return fan
AVS	Annulus ventilation
CAC	Containment atmosphere clean up
CCS	Containment cooling
CCW	Containment emergency fan cooling
CDS	Condensate
CFS	Core flood
CGC	Containment combustible gas control
CHP	Charging pump
CHR	Containment heat removal
CHW	Chilled water
CIS	Containment isolation
CLS	Consequence limiting control
CPC	Charging pump cooling
CPS	Containment penetration
CRD	Control rod drive
CSC	Closed cycle cooling
CSR	Containment spray recirculation
CSS	Containment spray mode of residual heat removal
CVC	Chemical volume and control
DCP	DC power
DGX	Diesel cross-tie
DRY	Drywell
DWS	Drywell (wetwell) spray mode of residual heat removal
EHV	Emergency heating, ventilation, and air conditioning
EPS	Emergency power
ESF	Engineered safety feature actuation
ESW	Emergency/essential service water
FHS	Fuel handling
FWS	Firewater
HCI	High pressure coolant injection (BWR)
HCS	High pressure core spray
HPI	High pressure safety injection (PWR)
HPR	High pressure coolant recirculation
IAS	Instrument air
ICS	Ice condenser
IGS	Integrated control
IPS	Instrument AC power
ISO	Isolation condenser
ISR	Inside containment spray recirculation
LCI	Low pressure coolant injection (BWR)
LCS	Low pressure core spray
LMS	Let down purification and makeup
LPI	Low pressure safety injection (PWR)
LPR	Low pressure coolant recirculation

Table 3. Systems list (CCF system codes) (continued)

CCF system code	CCF system description
MCW	Main circulating water
MFW	Main feedwater
MSS	Main stream
NHV	Normal heating, ventilation, and air conditioning
NSS	Nuclear steam supply shutoff
OEP	Offsite electrical power
OTS	Other systems
PCS	Power conversion
PPR	Primary pressure relief (safety/relief valves)
PVS	Penetration room ventilation
PZR	Pressurizer
RBC	Reactor building cooling water
RBS	Reactor building penetration
RCI	Reactor core isolation cooling
RCS	Reactor coolant
RGW	Radioactive gaseous waste
RHR	Residual heat removal
RLW	Radioactive liquid waste
RMT	Recirculation mode transfer
RPS	Reactor protection
RRS	Reactor recirculation
RWC	Reactor water cleanup
RWS	Refueling water storage tank
SDC	Shutdown cooling mode of residual heat removal
SGT	Standby gas treatment
SIS	Safety injection actuation
SLB	Steam line break control subsystem
SLC	Standby liquid control
SPC	Suppression pool cooling mode of residual heat removal
SPM	Suppression pool makeup
SPR	Secondary pressure relief (safety/relief valves)
TBC	Turbine building cooling water
VSS	Vapor suppression

The proximate cause codes are shown in Table 5, which provides definitions and guidance on use of the cause codes.

3.1.11 Shock Type. This field describes the relationship of one component failure to another. Given one failure, a lethal shock type means that other components in the common cause component group will fail as well. The allowable codes and their descriptions are:

L	Lethal	The cause of failure will result in the failure of all components in the population within the PRA mission time.
NL	Non-Lethal	The cause of failure will affect only a subset of the entire component population within the PRA mission time.

Table 4. Coupling factor codes.

Code	Coupling factor	Description
EE	Environment: external	Components share the external environment. For example, the room that houses the component was too hot.
EI	Environment: internal environment/working medium	Components share an internal environment. For example, the process fluid flowing through the component was too hot.
HDCP	Hardware design: component part (internal parts)	Components share the same design and internal parts.
HDSC	Hardware design: system configuration (physical appearance)	CCF event is the result of design features within the system in which the components are located.
HQIC	Hardware quality: installation/construction (initial or modification)	Components share installation or construction features, from initial installation, construction, or subsequent modifications.
HQMM	Hardware quality: manufacturing	Components share hardware quality deficiencies from the manufacturing process.
OMTC	Operational: maintenance/test schedule	Components share maintenance and test schedules. For example, the component failed because maintenance was delayed until failure.
OMTP	Operational: maintenance/test procedure	Components are affected by the same inadequate maintenance or test procedure. For example, the component failed because the maintenance procedure was incorrect or a calibration setpoint was incorrectly specified.
OMTS	Operational: maintenance/test staff	Components are affected by a maintenance staff personnel error.
OOOP	Operational: operation procedure	Components are affected by an inadequate operations procedure. For example, the component failed because the operational procedure was incorrect and the pump was operated with the discharge valve closed.
OOOS	Operational: operation staff	Components are affected by the same operations staff personnel error.

3.1.12 Shared Cause Factor. By definition, a CCF event must result from a single, shared cause of failure (see Item 3, Section 1.3). However, the failure reports (LERs or NPRDS records) may not provide sufficient information to determine whether the multiple failures result from the same cause or different causes. Because of this lack of detailed description of the causes in the event reports, the analyst 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 0.0 to 1.0. To ensure consistency in the coding, four numbers are used. Examples are the following:

1.0 This value is used when the analyst believes that the cause of the multiple failures is the *same*, whatever the nature of the cause. A shared cause factor of 1.0 implies multiple failures from the same root cause of failure, often resulting in the same failure/degradation mechanism and affecting the same piece-parts of each of the multiple components. The corrective action(s) taken for each of the multiple components involved in the event is (are) also typically the same. The following example illustrates a shared cause factor equal to 1.0:

Table 5. Cause codes.

Description	Code	Discussion
Construction/installation error or inadequacy Incorrect component/material installed	DC	Used when a construction or installation error is made during the original or modification installation. This includes specification of incorrect component or material.
Design error or inadequacy	DE	Used when a design error is made.
Manufacturing error or inadequacy	DM	Used when a manufacturing error is made during component manufacture.
Accidental action (unintentional or undesired human errors)	HA	Used when a human error (during the performance of an activity) results in an unintentional or undesired action.
Wrong procedure followed	HD	Used when the wrong procedure is followed.
Failure to follow procedure Calibration/test staff Construction/test staff Maintenance staff Operations staff Other plant staff	HP	Used when the correct procedure is not followed. For example: when a missed step in a surveillance procedure results in a component failure.
Inadequate training	HT	Used when training is inadequate.
Other (stated cause does not fit other categories)	OT	Used when the cause of a failure is provided but it does not meet any one of the descriptions.
Internal to component, piece-part Erosion/corrosion Equipment fatigue Wear out/end of life Internal contamination	IC	Used when the cause of a failure is the result of a failure internal to the component that failed.
Ambient environmental stress 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)	IE	Used when the cause of a failure is the result of an environmental condition from the location of the component.

Table 5. Cause codes (continued)

Description	Code	Discussion
Inadequate procedure Calibration/test procedure Administrative Maintenance Operational Construction/modification Other	PA	Used when the cause of a failure is the result of an inadequate procedure.
Setpoint drift	QI	Used when the cause of a failure is the result of setpoint drift.
State of other component	QP	Used when the cause of a failure is the result of a component state that is not associated with the component that failed. An example would be the diesel failed due to no fuel in the fuel storage tanks.
Unknown	U	Used when the cause of the failure is not known.

"Three turbine-driven steam-supply check valves failed to open. Investigation revealed similar internal damage to all three valves. The cause of failure for each valve was 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. The following examples illustrate statements that indicate a shared cause factor equal to 1.0:

"investigation revealed similar damage to all three redundant valves"

"loose screws found in five circuit breakers"

"several air-operated valves malfunctions because of moisture in the air supply."

If the event report contains no information about the causes of failure, the analyst should assign a value of 1.0. To change this value requires evidence or an indication that the causes were different. This evidence need not come from the event description itself, but may result from a more general knowledge of the plant and its operational history. If the information is not in the event narrative (the NPRDS failure report or the LER abstract), explanation of the additional information should be included in the comments field.

0.50 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 strong evidence that the underlying root cause of the multiple failures is the same. The following example illustrates a shared cause factor equal to 0.50:

"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/maintenance of these valves. It is possible, for example that the inadequate instructions from the vendor/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 example illustrates 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 event involved different pump subcomponents (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., thereby making the cause of the multiple failures the same. Since this hypothesis is highly speculative, the shared cause factor is small.

0.0 This value is used when the analyst believes that the multiple failures resulted from clearly different causes. (This value is rarely used because events with shared cause values equal to 0.0 are typically not included in the CCF database.)

3.1.13 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 0.00 to 1.00. Specific values to be used are:

1.00 Multiple failures that occur within the PRA mission time. For standby components whose failures were discovered during testing or observance, but within half of the testing interval, the timing factor is 1.00.

0.50 Multiple failures that do not occur within the PRA mission time, but within a month of each other. For standby components whose failures were discovered during testing, but within a time interval (T/2, T), the timing factor is 0.50.

0.10 Multiple failures that occur more than one month apart. For standby components whose failures were discovered during testing, outside the test interval, the timing factor is 0.10. The test interval is discussed in Section 2.3.1.1.

3.1.14 Common Cause Component Group (CCCG). This field indicates the size of the population that can be exposed to a common cause failure event. 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 prior to 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.

3.1.15 Defense Mechanism. This field describes the actions a licensee can take to eliminate the coupling factor, to 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 6, which presents definitions, codes, and guidance on use of defense mechanisms. The table in Appendix C provides guidance on assigning defense mechanism codes based on coupling factor codes.

3.1.16 Event Type. The event type field indicates which events should and should not 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. Volume 2[1] of the series discusses dependent events and what is included in the subset of dependent events called `CCF'. The allowable entries and codes for this field are provided in Table 7, which presents definitions and guidance for assigning this code.

3.1.17 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 entries and codes for this field are provided in Table 8, which presents definitions and guidance for assigning this code.

Table 6. Defense mechanisms.

Code	Defense mechanism	Description
FSB	Functional	A decoupling of a CCF event could have been accomplished if the equipment barrier (functional and/or physical interconnections) had been modified.
PBR	Physical barrier	A physical restriction, barrier, or separation could have prevented a CCF.
MON	Monitoring/awareness	Increased monitoring, surveillance, or personnel training could have prevented a CCF.
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.
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.
DIV	Diversity	Increased diversity could have prevented a CCF. This includes diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.
NON	No practical defense	No practical defense could be identified.
UKN	Unknown	Adequate detail is not provided to make an adequate defense mechanism identification.

3.1.18 CCF Event Operational Status. The CCF event operational status field indicates when the CCF event occurred or could occur. Allowable entries and codes for this field are provided in Table 9, which presents definitions and guidance for assigning this code.

3.1.19 CCF Event Detection Operational Status. This field is used to indicate the plant operational status when the CCF event was detected. Table 10 provides the allowable codes and discussion of each.

3.1.20 Component Degradation Values (p). This 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 greater than zero. The allowable values are decimal numbers from 0.00 to 1.00. 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 0.00, 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, $p_3 = 0.00$. Coding guidance for different values follows:

1.00 The component has completely failed and will not perform any function. If the cause prevented a pump from starting, the pump has completely failed and degradation would be complete. If the description is vague, p = 1.0 is assigned in order to be conservative.

Table 7. CCF event types.

Code	Event types	Description
CCF	CCF estimation	Common cause failure events that are generally considered applicable to PRA CCF parametric modeling (e.g., the failure of both motors, in an auxiliary feedwater 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 due to system configuration, and certain types of operator actions (e.g., a failure in the Engineered Safety Feature Actuation System caused the auxiliary feedwater pumps failure to start). This type 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).

Table 8. CCF event levels.

Code	Event level	Description
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 other 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).

Table 9. CCF event operational status.

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

Table 10. CCF event detection operational status.

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

0.50 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 it increases the potential for failing within the duration of the PRA mission.

0.10 The component is only slightly degraded or failure is incipient. If parts were replaced on some components due to failures of parallel components, 0.1 is used for the components that didn't actually experience a failure.

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. For a pump packing leak that would not prevent the pump from performing its function, p=0.01. Setpoint drift that the licensee determined did not render the component inoperable is also coded as p = 0.01.

0.00 The component did not fail.

3.1.21 Use. There is an analysis use field preceding the 'p' field (in the data input screen) for the coder/analyst to indicate which eight (of the possible 16) events are used as primary events in the parameter estimations. An "X" is entered in the desired spaces. If there are eight or less component degradation values given, all are designated with an "X," and all will be used in parameter estimations.

3.1.22 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.

3.1.23 Time. This is the time of failure. The format is HH:MM:SS. If the CCF event is identified from an LER, the time information may be unknown and the field may be left blank. For CCF events identified from NPRDS records, the Failure Start Time is used.

3.1.24 Comments. This field contains the analyst's comments and assumptions on coding decisions. For example, if there are 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 as well; this is internal to the INEEL data tracking system and does not refer to anything specific in the NPRDS database.

3.1.25 Narrative. LER abstracts and NPRDS failure report narratives are in this field.

3.1.26 Multiple Unit. This field is to indicate ('Y' or 'N') if the CCF event affects more than one power plant at a single site. Very few events will be coded 'Y;' most are for the emergency diesel generators. 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.

3.2 Independent Failure Coding Rules

Following the identification of CCF events, independent failures from both NPRDS failure reports and LER text are characterized and counted. Independent failures are equipment failures that are not involved in the common cause failure events.

Five pieces of information, discussed below, are recorded for each independent failure: failure mode, system, component, the number of failures, and the p-value. The NPRDS dataset is compared to the LER dataset 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.

3.2.1 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 2.

3.2.2 System. The system code identifies the power plant system which includes the individual failed components. Table 3 provides the system codes, and the table in Appendix B provides a translation between NPRDS system codes and appropriate CCF system codes.

3.2.3 Failure Mode. The failure mode describes the function the component did not perform. The codes are defined in Table 1.

3.2.4 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 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.

3.2.5 Component Degradation Values (p). This is the same as the CCF component degradation value, discussed in Section 3.1.20, but applied here to single failures.

3.3 Quality Assurance (QA)

Data handling, screening, and coding activities are based on engineering judgment, which has a potential for error. To reduce this potential, a two-step quality assurance program has been developed: (1) screening and coding quality assurance and (2) independent quality assurance. The results of the CCF analysis and the quality assurance review results are stored with each set of source data.

3.3.1 Screening and Coding Quality Assurance (8).

3.3.1.1 Coding QA. Both second CCF coding analyst and a PRA analyst at the INEEL evaluate the coded events to ensure that the events were coded consistently. Any differences between the first and second codings are mutually resolved by the two coders.

The second review entails the following:

- Reviewing a copy of the coded events and source data used during the first review to determine whether CCF events were correctly identified.

- Evaluating coded events to determine if coding information was correctly identified and documented.

- Resolving differences between coder and reviewer, and implementing corrections to the events in the CCF database.

3.3.1.2 Data Tracking. 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 in a file. Included are:

- Boundary definitions.

- All NPRDS failure records, with date of down- load and search criteria.

- All LER abstracts.

- Coding disposition of each record (e.g., CCF, independent, or no failure).

- CCF coding sheets.

- QA comments.

- Computer disks with source files.

3.3.2 Independent QA Verification (11). The independent QA activity is a review of coded CCF events and the CCF method. The independent QA is performed by two or more people independent of the organization performing the initial evaluation. The reviewers are recognized as industry experts on CCF issues. The goals for independent evaluation are to: (a) validate coded CCF events, and (b) ensure that the codes documented on the coding sheets are correct and consistent.

The independent QA review includes the following:

- Coded CCF events and supporting documentation are transmitted to the personnel doing the QA verification.

- The independent QA staff reviews the events and identifies potential changes. The changes are transmitted back to the INEEL database staff for resolution of differences and implementation.

3.4 Data Loading

After the CCF events have been reviewed, comments resolved, and duplicate events removed, the CCF events are loaded into the CCF database. The database structure is shown in Table 11. The fields followed by "1-16" are to be filled out for each individual component failure, or each component in the CCCG, included in the CCF event.

As the independent failure counts are completed, including elimination of duplicate records, the independent failure event totals are entered into the CCF database, grouped by plant, system, component, and failure mode. Volume 4[7] provides guidance on the data loading interface for the CCF software.

Table 11. CCF database file structure.

CCF file data structure	Field length
Event	16
Plant name	16
Power	3
Title	60
Failure mode	2
Component	3
System	3
Coupling factor	4
Cause	4
Shock type	2
Shared cause factor	4 (Format of X.XX)
Timing factor	4 (Format of X.XX)
CCCG level	2 (Up to a value of 16)
Failure mode applicability	4 (Format of X.XX)
Defense mechanism	3
Event type	3
CCF level	3
Event operational status	2
Event detection operational status	1
Multiple units	1
Use, 1-16	1 each
Component degradation value (P), 1-16	4 (Format of X.XX)
Date, 1-16	10 each
Time, 1-16	8 each
Comments	Unlimited
Narrative	Unlimited

4. SUMMARY

The data from two sources (NPRDS and SCSS) have been analyzed to identify CCF events using the three-step process: selection and definition of the component to be analyzed, collection of data, and reviewing the failure records to identify CCF events. The events have been coded, reviewed, and entered into the database.

At this time, the CCF parameter estimations are performed to provide input for PRA modeling. Volume 4[7] provides guidance on how to search the database, group the events, and perform the estimations. Following this activity, a summary report is prepared for each system/component dataset that has been analyzed to disseminate the results of the data analysis. The summary reports include background information on the definition of the system and component boundaries, the failure events considered, the applicable failure modes, and the quantitative results of the parameter estimations.

Following the independent QA review, events are revised as necessary, parameter estimations are revised, and the summary reports are finalized for publication.

5. REFERENCES

1. U.S. Nuclear Regulatory Commission, *Common Cause Failure Database and Analysis System, Volume 2, Event Definition and Classification*, NUREG/CR-62698, June 1998, INEEL/EXT-97-00696.

2. Institute of Nuclear Power Operations, *NPRDS Reporting Guidance Manual*, INPO 89-001, Revision 05, December 1994.

3. Oak Ridge National Laboratory, *Sequence Coding and Search System for Licensee Event Reports*, NUREG/CR-3905, Volumes 1-4, Nuclear Operations Analysis Center, Oak Ridge, TN, April 1985.

4. Science Applications International Corporation, SAIC, San Diego, California, *Nuclear Power Plant System Sourcebook*, 1989.

5. Institute of Nuclear Power Operations, *NPRDS Information Retrieval Guide*, INPO 87-024, Revision 04, July 1991.

6. Idaho National Engineering Laboratory, EG&G Idaho, Inc., *AdaSAGE Reference Manual*, Version 4.1.1.

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

8. U. S. Nuclear Regulatory Commission, "Review and Development of Common Nomenclature for Naming and Labeling Schemes for Probabilistic Risk Assessment," NUREG/CR-5905, August, 1992.

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

GLOSSARY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix A

Coding Examples

Appendix A

Coding Examples

A-1. CODING EXAMPLES

To enhance coding consistency and reduce subjectivity, the following examples demonstrate how common cause failure events are analyzed and codes logically assigned. Completed coding sheets are provided to demonstrate coding.

A-1.1 Coding Example 1: Main Steam Safety Valve Setpoints

Testing of the main steam safety valves revealed two valves with set points slightly above tolerance. The following codes were assigned:

- The evaluation is on the secondary pressure relief (SPR) system.
- The failure mode is setpoint drift (SD) since the setpoints were out of tolerance.
- The proximate cause is QI since the cause of failure was setpoint drift.
- The coupling factor is operational maintenance or test scheduling (OMTC) because setpoint drift for the two valves are most likely linked together through maintenance or test scheduling operational errors.
- The shock type is non-lethal, since the prevalent failure mechanism did not affect all components.
- The shared cause factor is 1.00 because the failure mechanism is most likely a procedural or schedule error.
- The timing factor is 1.00 because both valves drifted out of tolerance closely in time.
- The component group size is 6 since there are six MSIVs.
- Failure mode applicability is 1.00 because there is only one failure mode that is appropriate for this event and both valves failed in this mode.
- The defense mechanism is MAI since modification of the maintenance program could have prevented the CCF event. Monitoring and awareness (MON) is also an appropriate defense mechanism for this event.
- The CCF event type is INS because this type of event has limited PRA significance due to a negligible impact on system.
- The CCF event level is COM since this event affected only two components and not the entire system.
- The CCF event operational status is BO since this event can occur in operation or shutdown.
- The CCF event detection operational status is D because the event can only be detected during shutdown.
- The analysis use field is marked with an "X" for all six events since they all apply to the parameter estimation analysis.
- The degradation factor is 0.10 for the two MSIVs which were slightly degraded and 0.00 for the unaffected MSIVs.

CODING EXAMPLE 1: CCF Coding Sheet

Name	L-029-87-1487-SD	Plant	Yankee Rowe	Power	0%
Title	Main Steam Safety Valves Setpoint Too High				
System	SPR	Cause	QI	Timing Factor	1.00
Component	SVV	Shock Type	NL	Op. Status	BO
Det. Status	D				
Failure Mode	SC	Coupling Factor	OMTC	Event Type	INS
Fl.Md.Appl.	1.00	Shared Cause Factor	1.00	Event Level	COM
CCCG	6	Multiple Units	N	Defense Mech.	MAI

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	0.10	1987/05/02		9				
2	X	0.10			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

NPRDS/LER number: 029-87-005 (Circle one)

Assumptions: CCCG

Coupl. Factor

Cause

Failed Sub-component:

Event Text: Testing of MSSVs revealed two valves with setpoints slightly higher than the acceptable limit. The cause was determined to be setpoint drift.

A-1.2 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.

- The evaluation is on the AFW system.

- 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 motor-driven pump (MDP) because the LER indicates that only the motor-driven pumps were affected.

- The failure mode is fail to run (FR) because the pump would not run long enough to fulfill its safety function, even though actuated and started.

- The failure is the result of a design error because the trip circuits were erroneously installed and the design not adjusted. As a result, this event is a Design Error or Inadequacy (DE) cause.

- The coupling factor is Hardware Design: Component Part (Internal Parts: Ease of Maintenance & Operation) (HDCP) because it is a design error in the component part.

- The shared cause factor is 1.00 because the failures of both pumps are closely linked due to the same design and installation.

- The timing factor is 1.00 because both pumps failed closely in time.
- Since at this plant there are two motor-driven pumps in the AFW system with low suction pressure trips, the CCCG size is 2. The LER indicates that only the motor-driven pumps were affected, so the turbine-driven pump is not included.

- Failure mode applicability is 1.00 because there is only one failure mode and it is applicable to both failures.

- The shared cause factor is applicable to the entire component population. However, the failures were random and not consistent. Therefore, the shock type was non-lethal.

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

- The CCF event detection operational status is O because the event was detected during testing at power.

- The defense mechanism is assigned as functional physical barrier (FSB) because the shared cause factor is the system design.

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

- The CCF event level is SYS because two parallel pumps failed.

- The degradation factor is 0.5 for both events because both motor-driven pumps would perform their function intermittently, and therefore are partially degraded.

- The analysis use field is marked with an "X" for the two failures that occurred.

CODING EXAMPLE 2: CCF Coding Sheet

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	1.00
Component	MDP	Shock Type	NL	Op. Status	BO	Det. Status	O
Failure Mode	FR		Coupling Factor	HDCP		Event Type	CCF
Fl.Md.Appl.	1.00		Shared Cause Factor	1.00		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	1987/01/27	04:58	9				
2	X	0.5	1987/01/29	05:05	10				
3					11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments

NPRDS/LER number: 423-87-004 (Circle one)

Assumptions: CG

Coupl. Factor

Cause

Failed Sub-component:

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

A-1.3 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:

- The evaluation is on the HPI system.
- The component analyzed is MOV, and the boundary includes the circuit breaker.
- The failure mode is fail to open (CC) since the injection valves are normally closed and failed to open due to not receiving an actuation signal.
- The proximate cause is QP since the state of the injection valves are caused by another component failure.
- The coupling factor is hardware design, system configuration (HDSC) because the electrical source is shared by the two components.
- The shock type is non-lethal, since the prevalent failure mechanism did not affect all components and trains.
- The shared cause factor is 1.00 because the failure of both injection valves is closely linked due to shared equipment dependence.
- The timing factor is 1.00 because both injection valves failed simultaneously.
- The component group size is 6 since there are six injection valves, two on each train.
- Failure mode applicability is 1.00 because there is only one failure mode that is appropriate for this event and both valves failed in this mode.
- The defense mechanism is functional/physical barrier (FSB) since a decoupling of the CCF event could have accomplished if functional barriers were administered.
- The CCF event type is EXP 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.
- The CCF event level is COM since this event affected only one train.
- The CCF event operational status is OP since this event can only occur during an operational condition.
- The CCF event detection operational status is O since the event was detected at operation.
- The analysis use field is marked with an "X" for all six events since they all apply to the parameter estimation analysis.
- The degradation factor is 1.00 for the two failed injection valves and 0.00 for the unaffected injection valves in the other trains.

CODING EXAMPLE 3: CCF Coding Sheet

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	1.00

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

Failure Mode	CC	Coupling Factor	HDSC	Event Type	EXP
Fl.Md.Appl.	1.0	Shared Cause Factor	1.00	Event Level	COM
CCCG	6	Multiple Units	N	Defense Mech.	FSB

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	1.00	1985/06/16		9				
2	X	1.00	1985/06/16		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

NPRDS/LER number: 206-85-012 (Circle one)

Assumptions: CCCG

Coupl. Factor

Cause

Failed Sub-component:

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

A-1.4 Coding Example 4: 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.

- The evaluation is for the AFW system.

- The component boundary is pumps. With the pump packing failing, the pumps were failed. The component assigned is pump (PMP). 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.

- The failure mode is fail to run (FR) because the pumps would start, but would not continue to operate.

- The failure resulted from wearout and was assigned the internal to the component, piece-part (IC) cause.

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

- Since failures are loosely coupled and not likely to affect the entire component population, the shock type is non-lethal (NL).

- The shared cause factor is 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.

- The timing factor is 0.1 because the failures occurred greater than a month apart.

- Since there are three pumps, the CCCG size is 3.

- Failure mode applicability is 1.00 because there is only one failure mode and it applies to both failures.

- The defense mechanism is 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.

- The CCF event type is 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'.

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

- The CCF event operational status is BO because the CCF event can occur during operating or shutdown conditions.

- The CCF event detection operational status is O since it was detected while the plant was at power.

- The analysis use field is marked with an "X" for three events, two that occurred and one that did not occur (one pump did not fail).

- The degradation factor is 0.1 for the two failures, because these failures did not significantly affect the operation of the pumps. A degradation factor of 0.00 was assigned to the pump that did not fail.

CODING EXAMPLE 4: CCF Coding Sheet

Name	N-DDD-90-0050-FR	Plant	Plant Name	Power	100%
Title	Both Motor-Driven Aux. Feedwater Pumps had Excessive Leakage				

System	AFW	Cause	IC	Timing Factor	0.10
Component	AFW	Shock Type	NL	Op. Status	BO
Det. Status	O				
Failure Mode	FR	Coupling Factor	OMTC	Event Type	CCF
Fl.Md.Appl.	1.00	Shared Cause Factor	0.50	Event Level	COM
CCCG	3	Multiple Units	N	Defense Mech.	MAI

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	0.10	1990/04/24		9				
2	X	0.10	1990/07/03		10				
3	X	0.00			11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments

NPRDS/LER number: 206-85-012 (Circle one)

Assumptions: CCCG

Coupl. Factor

Cause

Failed Sub-component:

Event Text: Both motor-driven auxiliary feedwater pumps had excessive packing leakage resulting in degraded system operation. The cause was determined to be normal wearout.

A-1.5 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:

- The evaluation is on the AFW system.
- The component boundary is the motor, including the motor, breaker, and control circuit. When the control switches fail, the motors are considered failed. The component is motor (MOT).
- The failure mode is fail to start (FS) because neither motor started.
- The failure is the result of an environmental condition (IE) external to the component.
- The coupling factor is External Environment (EE) because of the shared external environment.
- Since the failures are tightly coupled, the shock type is lethal (L).
- The shared cause factor is 1.0 because failure of both motors is linked by a factor that will always affect the components in a similar manner.
- The timing factor is 1.00 because the failures occurred simultaneously.
- Since there are two motor-driven pumps, the CCCG size is 2.
- Failure mode applicability is 1.00 because there is only one failure mode and it applies to both failures.
- The defense mechanism is PBR because the shared cause factor is an environmental factor where separation between the two components could have prevented the CCF event.
- The CCF event type is CCF because this event is considered important during a CCF parameter estimation.
- The CCF event level is SYS because this is a system type failure.
- The CCF event operational status was BO because the event can occur during either operating or shutdown conditions.
- The CCF event detection operational status is D because it was detected during a refueling outage.
- The analysis use field is marked with an "X" for both events.
- The degradation factor for both failures is 1.00 because the motors did not start.

CODING EXAMPLE 5: CCF Coding Sheet

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	1.00
Component	AFW	Shock Type	L	Op. Status	BO
Det. Status	D				
Failure Mode	FS	Coupling Factor	EE	Event Type	CCF
Fl.Md.Appl.	1.00	Shared Cause Factor	1.00	Event Level	SYS
CCCG	2	Multiple Units	N	Defense Mech.	PBR

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	1.00	1984/09/10		9				
2	X	1.00	1984/09/10		10				
3					11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments

NPRDS/LER number: 247-84-012 (Circle one)

Assumptions: CCCG

Coupl. Factor

Cause

Failed Sub-component:

Event Text: Both motor-driven auxiliary feedwater pumps failed to start on demand.

One relay on each pump motor had failed due to insulation degradation.

A-1.6 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 evaluation is on the AFW system
- The component boundary is the pump, including the pump shaft. The component assigned to the failure is the pump (PMP).
- The failure mode is fail to run (FR) since 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.
- The failure is a result of a design deficiency, DE. It was determined that the stainless steel material used for the sleeve material was too hard which resulted in higher stress related corrosion susceptibility.
- The failure is applicable to the entire population so it is a lethal shock.
- The coupling factor is hardware/design of the component (HDCP). All components used the same material.
- The shared cause factor is 1.00 due to a design error in the manufacturing process will closely tie the components together.
- The timing factor is 1.00 because the degraded condition existed in all components simultaneously.
- There are two pumps affected by this event at each unit-therefore the CCCG is two.
- Failure mode applicability is 1.00 because there is only one failure mode and it is applicable to both failures and potential failures in the record.
- The defense mechanism is DIV. This defense mechanism states that an increase in the diversity of the pumps could have prevented a similar common cause failure.
- The event type is a CCF since it would not typically be modeled explicitly in a PRA and should be included in an estimation of the CCF basic event for the AFW pump.
- The CCF event level is a component level failure since other trains were available for AFW.
- The CCF event operational status is BO because the event can occur in operation or shutdown mode.
- The CCF event detection operational status is D, since detection occurred and is most likely to occur when the plant is shut down.
- The analysis use field is marked with an "X" for both components because they both apply to the analysis.
- The degradation factors for one of the pumps was 1.00 since it failed. The other pumps contained the same material that failed, and one of the three remaining pumps at the 2 units was inspected to reveal similar cracking to the sleeve shaft had occurred, so the second degradation value was assigned 0.1 to indicate potential cracking and failure of the pump.

CODING EXAMPLE 6: CCF Coding Sheet

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	1.00
Component	PMP	Shock Type	L	Op. Status	BO
Det. Status	D				
Failure Mode	FR	Coupling Factor	HDCP	Event Type	CCF
Fl.Md.Appl.	1.00	Shared Cause Factor	1.00	Event Level	COM
CCCG	2	Multiple Units	Y	Defense Mech.	DIV

Component Degradation Values

	Use	P	Date	Time		Use	P	Date	Time
1	X	1.00	1988/02/28		9				
2	X	0.10	1988/05/12		10				
3					11				
4					12				
5					13				
6					14				
7					15				
8					16				

Comments

NPRDS/LER number: 498-88-032 (Circle one)

Assumptions: CCCG

Coupl. Factor

Cause

Failed Sub-component:

Event Text: 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 pump sleeves was replaced.

Appendix B

NPRDS/CCF System List

Appendix B

NPRDS/CCF System List

Table B-1. Systems list (system codes: NPRDS codes and corresponding CCF system codes).

NPRDS system code	NPRDS system description	CCF system code[a]
CBA	Reactor recirculation—GE	RRS
CBD	Reactor coolant—BW	RCS
CBG	Reactor coolant and control instrumentation—CE	RCS
CBH	Reactor coolant—W	RCS
CCA	Main steam—GE	MSS
CEA	Reactor core isolation cooling—GE	RCI
CFA	Residual heat removal—GE	RHR
CFA	Low pressure injection—GE	LCI
CFASCK	Containment spray—GE	CSS
CFB	Isolation condenser—GE	ISO
CFC	Decay heat removal—BW	RHR
CFC	Low pressure injection—BW	LPI
CFCSFE	Decay heat removal—BW	RHR
CFCSFE	LPI core flood subsystem—BW	LPI
CFD	Low pressure safety injection—CE	LPI
CFD	Shutdown cooling—CE	RHR
CFF	Residual heat removal—W	RHR
CFF	LP safety injection—W	LPI
CHA	Feedwater—GE	MFW
EBA	Plant AC distribution—GE	ACP
EBE	Plant AC power—BW	ACP
EBF	Plant AC power—W	ACP
EBG	Instrument AC power—BW	IPS
EBH	Instrument AC power—CE	IPS

Table B-1. Systems list (continued)

NPRDS system code	NPRDS system description	CCF system code[a]
EBI	Plant AC power—CE	ACP
EBJ	Instrument AC power—GE	IPS
EBK	Instrument AC power—W	IPS
ECB	DC power—GE	DCP
ECC	DC power—W	DCP
ECD	DC power—BW	DCP
ECE	DC power—CE	DCP
EEA	Emergency power—GE	EPS
EEADAA	Diesel starting air—GE	EPS
EEADCA	Diesel cooling water—GE	EPS
EEAFOA	Diesel fuel oil—GE	EPS
EEALOA	Diesel lube oil—GE	EPS
EEB	Emergency power—W	EPS
EEBDAA	Diesel starting air—W	EPS
EEBDCA	Diesel cooling water—W	EPS
EEBFOA	Diesel fuel oil—W	EPS
EEBLOA	Diesel lube oil—W	EPS
EEC	Emergency power—BW	EPS
EECDAA	Diesel starting air—BW	EPS
EECDCA	Diesel cooling water—BW	EPS
EECFOA	Diesel fuel oil—BW	EPS
EECLOA	Diesel lube oil—BW	EPS
EED	Emergency power—CE	EPS
EEDDAA	Diesel starting air—CE	EPS
EEDDCA	Diesel cooling water—CE	EPS
EEDFOA	Diesel fuel oil—CE	EPS
EEDLOA	Diesel lube oil—CE	EPS

Table B-1. Systems list (continued)

NPRDS system code	NPRDS system description	CCF system code[a]
EEE	High pressure core spray power—GE	HCS
EEEDAA	HPCS power—diesel starting air—GE	HCS
EEEDCA	HPCS power—diesel cooling water—GE	HCS
EEEFOA	HPCS power—diesel fuel oil—GE	HCS
EEELOA	HPCS power—diesel lube oil—GE	HCS
HBA	Main steam—BW	MSS
HBASLB	Main steam line break control—BW	NSS
HBB	Main steam—CE	MSS
HBC	Main steam—W	MSS
HBG	Main feedwater—CE	MFW
HGA	Condensate—CE	CDS
HHA	Feedwater—BW	MFW
HHB	Emergency feedwater—BW	AFW
HHC	Auxiliary feedwater—W	AFW
HHD	Condensate—GE	CDS
HHE	Condensate—W	CDS
HHF	Main feedwater system—W	MFW
HHH	Condensate—BW	CDS
HHJ	Auxiliary/emergency feedwater—CE	AFW
IBA	Reactor protection—GE	RPS
IBAIAA	Reactor protection—neutron monitoring—GE	RPS
IBB	Reactor protection—BW	RPS
IBC	Engineered safety features actuation—BW	ESF
IBD	Reactor protection—CE	RPS
IBE	Engineered safety features actuation—CE	ESF
IBG	Reactor protection—W	RPS
IBK	Engineered safety features actuation—W	ESF

Table B-1. Systems list (continued)

NPRDS system code	NPRDS system description	CCF system code[a]
IEC	Integrated control system—BW	IGS
PCA	Standby liquid control—GE	SLC
PCB	Letdown/purification and makeup—BW	LMS
PCF	Chemical and volume control—CE	CVC
PCG	Chemical and volume control—W	CVC
	Pressurizer—W, BW, CE	PZR
RBA	Control rod drive—GE	CRD
RBB	Control rod drive—BW	CRD
RBC	Control element assembly (rod drive)—CE	CRD
RBK	Control rod drive—W	CRD
SAA	Suppression pool support—GE	SPM
SAB	Reactor building penetration—BW	RBS
SAC	Reactor building penetration—W	RBS
SAD	Containment penetration—CE	CPS
SAG	Containment penetration—GE	CPS
SBA	Containment atmosphere cooling—GE	CHR
SBB	Reactor building cooling—BW	RBC
SBE	Containment cooling—CE	CHR
SBF	Ice condenser—W	ICS
SBG	Containment fan cooling—W	CCW
SCADIL	Combustible gas control—dilution subsystem—GE	CGC
SCAREC	Combustible gas control—recombiner subsystem—GE	CGC
SCB	Annulus ventilation—CE	AVS
SCC	Reactor building spray—BW	CSR
SCD	Containment spray—CE	CSR
SCF	Annulus ventilation—W	AVS
SCH	Penetration room ventilation—BW	PVS

Table B-1. Systems list (continued)

NPRDS system code	NPRDS system description	CCF system code[a]
SCJ	Containment spray—W	CSR
SDA	Containment isolation—BW	CIS
SDB	Containment isolation—W	CIS
SDC	Nuclear steam supply shutoff (NSSSS)—GE	NSS
SDCMCA	Steam shutoff—radiation monitoring—GE	NSS
SDE	Containment isolation—CE	CIS
SEA	Standby gas treatment—GE	SGT
SECDIL	Combustible gas control—dilution subsystem—BW	CGC
SECREC	Combustible gas control—recombiner subsystem—BW	CGC
SEDDIL	Combustible gas control—dilution subsystem—W	CGC
SEDIGN	Combustible gas control—ignitor subsystem—W	CGC
SEDREC	Combustible gas control—recombiner subsystem—W	CGC
SEEDIL	Combustible gas control—dilution subsystem—CE	CGC
SEEREC	Combustible gas control—recombiner subsystem—CE	CGC
SFA	Low pressure core spray—GE	LCS
SFB	High pressure core spray—GE	HCS
SFC	High pressure coolant injection—GE	HCI
SFD	High pressure injection—BW	HPI
SFG	High pressure safety injection—CE	HPI
SFK	High pressure safety injection—W	HPI
SFKUHI	HPSI—upper head injection subsystem—W	HPI
SHA	Penetration room ventilation—CE	PVS
SHB	Penetration room ventilation—W	PVS
WAA	Essential service water—GE	ESW
WAB	Low pressure service water—BW	ESW
WAC	Nuclear service water—CE	ESW
WAD	Nuclear service water—W	ESW

Table B-1. Systems list (continued)

NPRDS system code	NPRDS system description	CCF system code[a]
WBA	Reactor building closed cooling water—GE	RCW
WBB	Component cooling water—BW	CSC
WBC	Component cooling water—CE	CSC
WBD	Component cooling water—W	CSC

[a] If two CCF system codes are listed, the correct one is the system name of the function that was lost due to the CCF event.

Appendix C

Defense Mechanism/Coupling Factor Coding

Appendix C

Defense Mechanism/Coupling Factor Coding

Table C-1. Defense mechanism mapping from coupling factors.

Defense code	Defense description	Coupling factor code	Coupling factor description
		Defense Mechanism Mapping to Coupling Factors	
FSB	Functional barrier	HDCP[a]	Hardware design: component part (internal parts: ease of maintenance and operation)
		HDSC[a]	Hardware design: system configuration (physical appearance: identification, size or system layout)
		HQIC[a]	Hardware quality: installation construction (initial or modification)
		EI	Environment: internal fluid
PBR	Physical barrier	HQIC[a]	Hardware quality: installation/construction (initial or modification)
		EE	Environment: external
MON	Monitoring/ awareness	HQIC[a]	Hardware quality: installationl construction (initial or modification)
		OMTC[a]	Operational: maintenance/test schedule
		OMTP[a]	Operational: maintenance/test procedure
		OMTS[a]	Operational: maintenance/test staff
MAI	Maintenance staffing and scheduling	OMTC[a]	Operational: maintenance/test schedule
		OMTP[a]	Operational: maintenance/test procedure
		OMTS[a]	Operational: maintenance/test staff
		OOOP	Operational: operation procedure
		OOOS	Operational: operation staff
IDE	Component identification	HDSC[a]	Hardware design: system configuration (physical appearance: identification, size, or system layout)
DIV	Diversity	HQIC[a]	Hardware quality: installation/construction (initial or modification)
		HQMM	Hardware quality: manufacturing
		HDCP[a]	Hardware design: component part (internal parts: ease of maintenance and operation)
NON	No practical defense	HDCP[a]	Hardware design: component part (internal parts: ease of maintenance and operation)
UKN	Unknown		

[a] More than one defense mechanism can be used against any one of these coupling factors, so judgment is used to select the appropriate defense mechanisms for the specific event.

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

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

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

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

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

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This volume of the Common Cause Failure Database and Analysis System report documents the method used for coding common cause failure (CCF) events that are stored in the common cause failure database.

Equipment failures that contribute to common cause failure events at commercial nuclear power plants in the U.S. are identified during Licensee Event Report (LER) and Nuclear Plant Reliability Data System (NPRDS) failure report reviews. Once equipment failures that contribute to a common cause failure event are identified, the common cause failure events are coded for entry into a personal computer storage system using the method presented in this volume.

The database resulting from coding common cause failure events is used to estimate common cause failure parameters for use in various probabilistic risk assessment (PRA) CCF models.

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

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001