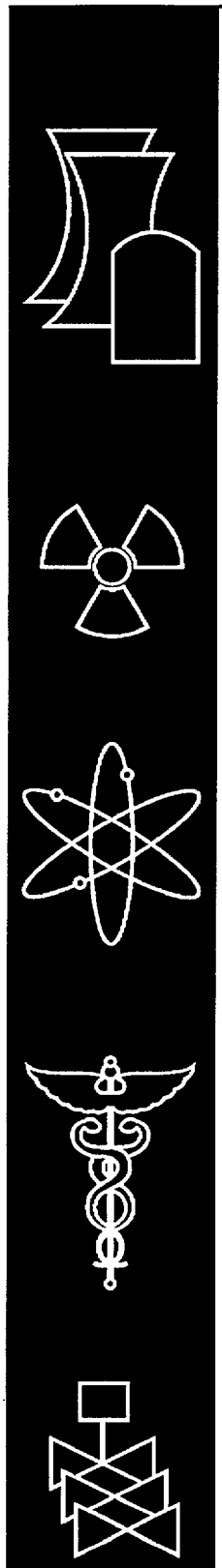
NUREG/CR-5500, Vol. 10
INEL/EXT-97-00740



Reliability Study: Combustion Engineering Reactor Protection System, 1984–1998

Idaho National Engineering and Environmental Laboratory

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

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

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

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

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

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

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

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

Non-NRC Reference Material

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

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

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

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

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

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

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

NUREG/CR-5500, Vol. 10
INEL/EXT-97-00740

Reliability Study: Combustion Engineering Reactor Protection System, 1984 –1998

Manuscript Completed: November 2001
Date Published: July 2002

Prepared by
T. E. Wierman, S. T. Beck, M. B. Calley,
S. A. Eide, C. D. Gentillon, W. E. Kohn

Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415

T. Wolf, NRC Project Manager

Prepared for
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code Y6214

ABSTRACT

This report documents an analysis of the safety-related performance of the reactor protection system (RPS) at U.S. Combustion Engineering commercial reactors during the period 1984 through 1998. The analysis is based on the four variations of Combustion Engineering reactor protection system designs. RPS-operational data were collected for all U.S. Combustion Engineering commercial reactors from the Nuclear Plant Reliability Data System and Licensee Event Reports. A risk-based analysis was performed on the data to estimate the observed unavailability of the RPS, based on fault tree models of the systems. An engineering analysis of trends and patterns was also performed on the data to provide additional insights into RPS performance. RPS unavailability results obtained from the data were compared with existing unavailability estimates from Individual Plant Examinations and other reports.

CONTENTS

Appendices

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This report documents an analysis of the safety-related performance of the reactor protection system (RPS) at U.S. Combustion Engineering (CE) commercial nuclear reactors during the period 1984 through 1998. The objectives of the study were (1) to estimate RPS unavailability based on operational experience data and compare the results with models used in probabilistic risk assessments and individual plant examinations, and (2) to review the operational data from an engineering perspective to determine trends and patterns, and to gain additional insights into RPS performance. The CE RPS designs covered in the unavailability estimation include four versions. Fault trees developed for this study were based on these four versions, which represent all CE plants.

Combustion Engineering RPS operational data were collected from Licensee Event Reports as recorded in the Sequence Coding and Search System and the Nuclear Plant Reliability Data System. The period covered 1984 through 1998. Data from both sources were evaluated by engineers with operational experience at nuclear power plants. Approximately 2400 events were evaluated for applicability to this study. Data not excluded were further characterized as to the type of RPS component, type of failure, failure detection, status of the plant during the failure, etc. Characterized data include both independent component failures and common-cause failures (CCFs) of more than one component. The CCF data were classified as outlined in the report *Common-Cause Failure Data Collection and Analysis System* (NUREG/CR-6268). Component demand counts were obtained from plant reactor trip histories and component test frequency information.

The risk-based analysis of the RPS operational data focused on obtaining failure probabilities for component independent failure and common-cause failure events in the RPS fault tree. The level of detail of the basic events includes channel trip signal sensor/transmitters and associated bistables, process switches and relays, and control rod drives and control rods. Common-cause failure events were modeled for all redundant, similar types of components.

Fault trees for each of the four designs of the CE RPS were developed and quantified using U.S. CE commercial nuclear reactor data from the period 1984 through 1998. All CE plants use the same channel through trip module design, except later plants use a digital core protection calculator. The Group 1 design uses trip contactors without any form of circuit breaker. The other three groups use either an eight-breaker design (Groups 2 and 3) or a four-breaker design (Group 4). Table ES-1 summarizes the RPS unavailability results of this study.

Table ES-1. Summary of Combustion Engineering RPS model results.

	5%	Mean	95%
Group 1 RPS Model			
No credit for manual trip by operator	1.2E-6	6.5E-6	1.8E-5
Credit for manual trip by operator	8.8E-7	5.7E-6	1.7E-5
Group 2 RPS Model			
No credit for manual trip by operator	1.9E-6	7.5E-6	1.9E-5
Credit for manual trip by operator	3.9E-7	1.9E-6	5.1E-6
Group 3 RPS Model			
No credit for manual trip by operator	1.9E-6	7.5E-6	1.9E-5
Credit for manual trip by operator	3.9E-7	1.9E-6	5.1E-6
Group 4 RPS Model			
No credit for manual trip by operator	1.6E-6	7.2E-6	1.9E-5
Credit for manual trip by operator	2.4E-7	1.6E-6	4.7E-6

The computed mean unavailabilities for the various CE design groups ranged from 6.5E-6 to 7.5E-6 (with no credit for manual trips). These are comparable to the values CE IPEs, which ranged from 3.7E-6 to 1.0E-5, and other reports. Common-cause failures contribute approximately 99 percent to the overall unavailability of the various designs. The individual component failure probabilities are generally comparable to failure probability estimates listed in previous reports.

The RPS fault tree was also quantified for manual trip by the operator (assuming an operator failure probability of 0.01). The mean unavailabilities improved 13 percent (Group 1) to 78 percent (Group 4), with a range of 1.6E-6 to 5.7E-6.

The study revealed several general insights:

- The dominant failure contribution to the Combustion Engineering RPS designs involve CCFs of the trip relays (K-1 through K-4, Groups 2, 3, and 4 or M-1 through M-4 Group 1) and the CCF of the mechanical portion of the trip breakers (except Group 1).

- Issues from the early 1980s that affected the performance of the reactor trip breakers (e.g., dirt, wear, lack of lubrication, and component failure) are not currently evident. Improved maintenance has resulted in improved performance of these components.

- Overall, the trends in unplanned trips, component failures, and CCF events decreased significantly over the time span of this study.

- The calculated unavailability of plants that have analog rather than digital core protection calculators shows no sensitivity to this design difference.

- The causes of the CE CCF events are similar to those of the rest of the industry. That is, over all RPS designs for all vendors for the components used in this study, the vast majority (80 percent) of RPS common-cause failure events can be attributed to either normal wear or out-of-specification conditions. These events, are typically degraded states, rather than complete failures. Design and manufacturing causes led to the next highest category (7 percent) and human errors (operations, maintenance, and procedures) were the next highest category (6 percent). Environmental problems and the state of other components (e.g., power supplies) led to the remaining RPS common-cause failure events. No evidence was found that these proportions are changing over time.

- The principle method of detection of failures of components in this study was either by testing or by observation during routine plant tours. Only two failures were detected by actual trip demands, neither of which was a CCF. No change over time in the overall distribution of detection method is apparent.

FOREWORD

This report presents information relevant to the reliability of the Combustion Engineering reactor protection system (RPS). It summarizes the event data used in the analysis. The results, findings, conclusions, and information contained in this study, the initiating event update study, and related system reliability studies conducted by the Office of Nuclear Regulatory Research are intended to support several risk-informed regulatory activities. This includes providing information about relevant operating experience that can be used to enhance plant inspections of risk-important systems, and information used to support staff technical reviews of proposed license amendments, including risk-informed applications. In the future, this work will be used in developing risk-based performance indicators that will be based largely on plant-specific system and equipment performance.

The Executive Summary presents findings and conclusions from the analyses of the Combustion Engineering RPS based on 1984–1998 operating experience. Sections 3 and 4, respectively, present the results of the quantitative analysis and engineering analysis. Table F-1 summarizes the information supporting risk-informed regulatory activities relating to the Combustion Engineering RPS. The table is an index of risk-important data and results presented in the discussions, tables, figures, and appendices of this report.

Table F-1. Summary of risk-important information specific to the Combustion Engineering RPS.

1.	General insights and conclusions regarding RPS unavailability	Section 5
2.	Dominant contributors to RPS unavailability	Table 3-4 and Table 3-5
3.	Dominant contributors to RPS unavailability by importance ranking	Appendix F
4.	Causal factors affecting dominant contributors to RPS unavailability	Sections 4.2 and 4.3
5.	Component-specific independent failure data used in the RPS fault tree quantification	Table 3-1
6.	Component-specific common-cause failure data used in RPS fault tree quantification	Table 3-2
7.	Failure information from the 1984-1998 operating experience used to estimate system unavailability (independent and common-cause failure events)	Tables B-1, B-2, and B-3
8.	Details of the common-cause failure parameter estimation	Appendix E
9.	Details of the failure event classification and parameter estimation	Appendix A
10.	Comparison with PRAs and IPEs	Figure 3-1, Section 3.3
11.	Trends in component failure occurrence rates	Section 4.2
12.	Trends in CCF occurrence rates	Section 4.3
13.	Trends in component total failure probabilities	Section 4.3

The application of results to plant-specific applications may require a more detailed review of the relevant Licensee Event Report (LER) and Nuclear Plant Reliability Data System (NPRDS) data than cited in this report. Such a review is needed to determine if generic experiences described in this report and specific aspects of the RPS events documented in the LER and NPRDS failure records are applicable to the design and operational features at a specific plant or site. Factors such as RPS design, specific components installed in the system, and test and maintenance practices would need to be considered in light of specific information provided in the LER and NPRDS failure records. Other documents, such as logs, reports, and inspection reports, that contain information about plant-specific experience (e.g., maintenance, operation, or surveillance testing) should be reviewed during plant inspections to supplement the information contained in this report.

Additional insights into plant-specific performance may be gained by examining specific events in light of overall industry performance. In addition, review of recent LERs and plant-specific component failure information in NPRDS or Equipment Performance Information and Exchange System (EPIX) may yield indications of whether performance has undergone any significant change since the last year of this report. Search of the LER database can be conducted through the NRC's Sequence Coding and Search System (SCSS) to identify RPS events that occurred after the reporting period covered by this report. The SCSS contains the full text LERs and is available to NRC staff on the SCSS home page (http://scss.ornl.gov/). Nuclear industry organizations and the general public can obtain information from the SCSS on a cost recovery basis by contacting the Oak Ridge National Laboratory directly.

Information in this report will be periodically updated, as additional data become available.

Scott F. Newberry, Director
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support and suggestions from H. Hamzehee, M. Harper, T. Wolf, D. Rasmuson, and S. Mays of the U.S. Nuclear Regulatory Commission.

ACRONYMS

ac	alternating current
ACRS	Advisory Committee on Reactor Safeguards (U.S. NRC)
ATWS	anticipated transient without scram
BME	trip breaker mechanical
BSN	trip breaker shunt trip device
BUV	trip breaker undervoltage device
BWR	boiling water reactor
CBI	channel bistable (trip unit)
CCF	common-cause failure
CEA	control element assembly
CEDM	control element assembly drive mechanism
CF	complete failure
CPA	core protection calculator, analog
CPD	core protection calculator, digital
CPR	channel pressure sensor/transmitter
CRD	control rod drive
CTP	channel temperature sensor/transmitter
dc	direct current
DNBR	departure from nucleate boiling ratio
FS	fail-safe (component failure not impacting safety function)
INEEL	Idaho National Engineering and Environmental Laboratory
IPE	Individual Plant Examination
MSW	manual scram switch
NF	no failure
NFS	non-fail-safe (component failure impacting safety function)
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission (U.S.)
PRA	probabilistic risk assessment
PWR	pressurized water reactor
RES	Office of Nuclear Regulatory Research
RMA	rod and control rod drive
ROD	control rod
RPS	reactor protection system
RTB	reactor trip breaker
RYL	logic relay
RYT	trip relay
SCSS	Sequence Coding and Search System
UC	unknown completeness (unknown if failure was CF or NF)

UKN	unknown (unknown if failure was NFS or FS)

TERMINOLOGY

Channel segment—The portion of the Combustion Engineering reactor protection system that includes trip signal sensor/transmitters and associated trip units (bistables) and other components distributed throughout the plant that monitor the state of the plant and generate automatic trip signals. There are four channels in the channel segment.

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

Common-cause failure model—A model for classifying and quantifying the probabilities of common-cause failures. The alpha factor model is used in this study.

Reactor protection system—The complex system comprising numerous electronic and mechanical components that provides the ability to produce an automatic or manual rapid shutdown of a nuclear reactor, given plant upset conditions that require a reactor trip.

Rod segment—The portion of the Combustion Engineering reactor protection system that includes the control rod drives and the control rods. There are generally 89 control rods and associated drives in Combustion Engineering plants.

Scram—Automatic or manual actuation of the reactor protection system, resulting in insertion of control rods into the core and shutdown of the nuclear reaction. A scram is also called a reactor trip.

Trip breaker/contactor segment—The portion of the Combustion Engineering reactor protection system that includes the reactor trip breakers or trip contactors. There are either four or eight trip breakers in the trip breaker segment. The trip breakers are arranged in two series/parallel paths. Both paths must be opened to complete a reactor trip. If the design has trip contactors (relays), there are four.

Trip matrix segment—The portion of the Combustion Engineering reactor protection system that includes the trip paths, logic matrices, matrix output relays, and the initiation relays (K or M relays) housed in cabinets in the control room. Each trip matrix receives signals from two of the four instrument channels. Each trip matrix energizes four of four initiation relays.

Unavailability—The probability that the reactor protection system will not actuate (and result in a reactor trip), given a demand for the system to actuate.

Unreliability—The probability that the reactor protection system will not fulfill its mission, given a demand for the system. Unreliability typically involves both failure to actuate and failure to continue to function for an appropriate mission time. However, the reactor protection system has no mission time. Therefore, for the reactor protection system, unreliability and unavailability are the same.

Reliability Study: Combustion Engineering Reactor Protection System, 1984–1998

1. INTRODUCTION

The U.S. Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) has, in cooperation with other NRC offices, undertaken to ensure that the NRC policy to expand the use of probabilistic risk assessment (PRA) within the agency is implemented consistently and predictably. As part of this effort, the Division of Risk Analysis and Applications has undertaken to monitor and report the functional reliability of risk-important systems in commercial nuclear power plants. The approach is to compare estimates and associated assumptions found in PRAs to actual operating experience. The first phase of the review involves identifying risk-important systems from a PRA perspective and the performance of reliability and trending analysis on these identified systems. As part of this review, a risk-related performance evaluation of the reactor protection system (RPS) in Combustion Engineering pressurized water reactors (PWRs) was performed.

An abbreviated U.S. history of regulatory issues relating to RPS and anticipated transient without scram (ATWS) begins with a 1969 concern[1] from the Advisory Committee on Reactor Safeguards (ACRS) that RPS common mode failures might result in unavailabilities higher than previously thought. At that time, ATWS events were considered to have frequencies lower than 1E-6/y, based on the levels of redundancy in RPS designs. Therefore, such events were not included in the design basis for U.S. nuclear power plants. This concern was followed by issuance of WASH-1270[2] in 1973, in which the RPS unavailability was estimated to be 6.9E-5 (median value). Based on this information and the fact that increasing numbers of nuclear reactors were being built and operated in the United States, it was recommended that ATWS events be considered in the safety analysis of nuclear reactors. In 1978, NUREG-0460[1] was issued. In that report, the RPS unavailability was estimated to be in the range 1E-5 to 1E-4. An unavailability of 3E-5 was recommended, allowing for some improvements in design and performance. In addition, it was recommended that consideration be given to additional systems that would help to mitigate ATWS events, given failure of the RPS. Two events: the 1980 boiling water reactor (BWR) Browns Ferry Unit 3 event, in which 76 of 185 control rods failed to insert fully; and the 1983 PWR Salem Unit 1 low-power ATWS event (failure of the undervoltage coils to open the reactor trip breakers), led to NUREG-1000[3] and Generic Letter 83-28.[4] These documents discussed actions to improve RPS reliability, including the requirement for functional testing of backup scram systems. Finally, 49FR26036[5] in 1984, Generic Letter 85-06[6] in 1985, and 10CFR50.62[7] in 1986 outlined requirements for diverse ATWS mitigation systems.

The risk-related performance evaluation in this study measures RPS unavailability using actual operating experience. To perform this evaluation, system unavailability was evaluated using two levels of detail: the entire system (without distinguishing components within the system) and the system broken down into components such as sensors, logic modules, and relays. The modeling of components in the RPS was necessary because the U.S. operating experience during the period 1984 through 1998 does not include any RPS system failures. Therefore, unavailability results for the RPS modeled at the system level provide limited information. Additional unavailability information is gained by working at the component level, at which actual failures have occurred. Failures and associated demands that occurred during tests of portions of the RPS are included in the component level evaluation of the RPS unavailability, although such demands do not model a complete system response for accident mitigation. This is in contrast to previous system studies, in which such partial system tests generally were not used.

RPS unavailability in this evaluation is concerned with failure of the function of the system to shut down the reactor given a plant-upset condition requiring a reactor trip. Component or system failures causing spurious reactor trips or not affecting the shutdown function of the RPS are not considered as failures in this report. However, spurious trips are included as demands where applicable.

Note that the RPS boundary for this study does not include ATWS mitigation systems added or modified in the late 1980s. For Combustion Engineering nuclear reactors, these systems use diverse trip parameters and trip the RPS motor generator set input breakers. In addition, the base case of this study models the automatic actuation of the RPS. However, RPS unavailability was also determined assuming credit for operator action.

The RPS unavailability study is based on U.S. Combustion Engineering RPS operational experience data from the period 1984 through 1998, as reported in both the Nuclear Plant Reliability Data System (NPRDS)[8] and Licensee Event Reports (LERs) found in the Sequence Coding and Search System (SCSS).[9]

The objectives of the study were the following:

1. Estimate RPS unavailability based on operation data and compare the results with the assumptions, models, and data used in PRAs and Individual Plant Examinations (IPEs).

2. Conduct an engineering analysis of the factors affecting system unavailability and determine if trends and patterns are present in the RPS operational data.

The body of this report is in six sections. After this introduction, Section 2 describes the fault tree models used in the analysis, the data collection, characterization, and analysis. Section 3 presents the unavailability results from the operational data and compares them with PRA/IPE RPS results. Section 4 presents the results of the engineering analysis of the operational data. Section 5 summarizes and presents conclusions. Section 6 presents references.

There are also seven appendices in this report. Appendix A explains in detail the methods used for data collection, characterization, and analysis. Appendix B summarizes the operational data. Appendix C presents detailed statistical analyses. Appendix D presents the fault tree model. Appendix E presents common-cause failure modeling information. Appendix F presents the fault tree quantification results, cut sets, and importance rankings. Appendix G presents sensitivity analysis results.

2. SCOPE OF STUDY

This study documents an analysis of the operational experience of the Combustion Engineering RPS from 1984 through 1998. The analysis focused on the ability of the RPS to automatically shut down the reactor given a plant upset condition requiring a reactor trip while the plant is at full power. The term *reactor trip* refers to a rapid insertion of control rods into the reactor core to inhibit the nuclear reaction. RPS spurious reactor trips or component failures not affecting the automatic shutdown function were not considered as failures. The Combustion Engineering RPS is described, followed by a description of the RPS fault tree used in the study. The section concludes with a description of the data collection, characterization, and analysis.

2.1 System Description

2.1.1 System Configurations

Four generic RPS configurations represent all Combustion Engineering plants. Each plant's RPS closely matches one of these four generic configurations. Among the individual plants, there are only minor variations of hardware and test practices. The most significant of these are noted in the applicable parts of the text. Table 2-1 shows which plants are grouped into the generic designs.

Table 2-1. Combustion Engineering RPS configuration table.

Plant Name	RPS Group
Palisades	1
Fort Calhoun	1
Calvert Cliffs 1, 2	2
Maine Yankee	2
Millstone 2	2
St. Lucie 1, 2	2
Arkansas 2	3
San Onofre 2, 3	3
Waterford 3	3
Palo Verde 1, 2, 3	4

The most important differences between these four RPS configurations are the use of analog or digital core protection calculators and the trip breaker configuration. Table 2-2 shows the four groups and the combinations that define these groups.

Table 2-2. Combustion Engineering RPS group descriptions.

RPS Group	Core Protection Calculator Type	Trip Breaker Configuration
1	Analog thermal margin/low pressure setpoint Calculator	Four trip contactors (relays)
2	Analog thermal margin/low pressure setpoint Calculator	Eight reactor trip breakers
3	Digital core protection calculator	Eight reactor trip breakers
4	Digital core protection calculator	Four reactor trip breakers

2.1.2 System Segment Description

The Combustion Engineering RPS is a complex control system comprising numerous electronic and mechanical components that combine in the ability to produce an automatic or manual rapid shutdown of the nuclear reactor, known as a reactor trip or scram. In spite of its complexity, the Combustion Engineering RPS components can be roughly divided into four segments—channels, trip matrices, trip breakers/relays/contactors, and rods—as shown in Table 2-3.

Table 2-3. Segments of Combustion Engineering RPS.

	RPS Segments			
RPS Group	Channel	Trip Matrices	Trip Breakers/Relays/ Contactors	Rods
1	Four channels (A – D). Each channel includes bistables and instrumentation to measure plant parameters. Thermal margin is calculated with an analog device.	Six trip matrices. Each trip matrix consists of contacts from two channel bistables and four output relays. Each output relay opens a contact in one of four initiation relays (M-1 to M-4). One out of six trip matrices is sufficient to trip the reactor trip switchgear.	Relays M-1 to M-4, also called trip contactors, open contacts in line with the CEDM power supplies.	Rod groups de-energized on successful RPS actuation.
2	Four channels (A – D). Each channel includes bistables and instrumentation to measure plant parameters. Thermal margin is calculated with an analog device.	Six trip matrices. Each trip matrix consists of contacts from two channel bistables and four output relays. Each output relay opens a contact in one of four initiation relays (K-1 to K-4). One out of six trip matrices is sufficient to trip the reactor trip switchgear.	Relays K-1 to K-4 open contacts in line with the eight trip circuit breakers.	Rod groups de-energized on successful RPS actuation.
3	Four channels (A – D). Each channel includes bistables and instrumentation to measure plant parameters. Thermal margin is calculated with a digital device.	Six trip matrices. Each trip matrix consists of contacts from two channel bistables and four output relays. Each output relay opens a contact in one of four initiation relays (K-1 to K-4). One out of six trip matrices is sufficient to trip the reactor trip switchgear.	Relays K-1 to K-4 open contacts in line with the eight trip circuit breakers.	Rod groups de-energized on successful RPS actuation.
4	Four channels (A – D). Each channel includes bistables and instrumentation to measure plant parameters. Thermal margin is calculated with a digital device.	Six trip matrices. Each trip matrix consists of contacts from two channel bistables and four output relays. Each output relay opens a contact in one of four initiation relays (K-1 to K-4). One out of six trip matrices is sufficient to trip the reactor trip switchgear.	Relays K-1 to K-4 open contacts in line with the four trip circuit breakers.	Rod groups de-energized on successful RPS actuation.

There are typically 89 control element assemblies (CEAs) grouped for control and safety purposes into nine banks (five regulating banks, two shutdown banks, and two part-length banks). Typical rod banking is shown in Table 2-4. The trip breakers/ trip contactors interrupt power to the control element assembly drive mechanisms (CEDM). When power is removed, the roller nuts disengage from the lead screw, allowing gravity to insert the control rod assembly.

Table 2-4. Typical rod banking arrangement.

CEA Type	Number of Control Element Assemblies
Shutdown 12-element full length CEA	Shutdown bank A – 16 Shutdown bank B – 20
12-element full length CEA	12
4-element full length CEA	28
4-element part length CEA (not held by the magnetic clutches)	13
Total	89
Total held by RPS	76

The shutdown banks A and B contain approximately 76 percent of the total rod worth and are sufficient to ensure shutdown at the beginning of life and at the end of life of the reactor core. SECY-83-293, Enclosure D, Appendix A. describes a rod failure criterion. In this reference, *rod success* is defined for all PWRs as the insertion of one-half or more of the control rods into the core in a roughly checkerboard pattern. For the purposes of this study, we will require 20 percent, 7 rods total, to fully insert to ensure shutdown. Appendix G presents a range of rod failure criteria and the effect on the overall RPS unavailability.

The shutdown banks A and B contain approximately 76 percent of the total rod worth and are sufficient to ensure shutdown at the beginning of life and at the end of life of the reactor core. Consistent with previous studies, the reported RPS unavailability is based on a rod success criterion of 20 percent. As noted in the statement of considerations (49FR26036)[5] for the ATWS reduction rule (10CFR50.62)[7], the insertion of 20 percent of the shutdown rods is needed to achieve hot, zero power provided that the inserted rods are suitably uniformly distributed. To demonstrate the effect of selecting a different rod success criterion, the overall RPS unavailability was computed for a range of rod failure percentages. The results of this sensitivity study are presented in Appendix G.

2.1.3 System Operation

The RPS system as shown in Figure 2-1 through Figure 2-3 consists of four identical protective channels. Each protective channel contains between ten and sixteen measurement channels, each capable of initiating protective actions by actuating a bistable. Each bistable includes three relays (included within the bistable component). The relay contacts are in three of the six logic matrices combined with relay contacts from one other channel in a two-out-of-two logic. When both channels trip, the logic matrix de-energizes removing power from the four matrix output relays. The four output relays open contacts supplying power to relays K-1, 2, 3, and 4 (M-1, 2, 3, and 4 in RPS Group 1). The trip parameters are shown in Table 2-5.

Figure 2-4 through Figure 2-8 show the logic of the four RPS-group designs.

2.1.3.1 Group 1 Trip Contactor Logic

Relays M-1 and M-2 contain contacts that supply ac power to two CRD clutch power supplies on one side of the two clutch power busses. Similarly, relays M-3 and M-4 contain contacts that supply ac power to the CRD clutch power supplies on the opposite side of the two clutch power buses. When the dc power supplies to a clutch power bus on both sides and are de-energized, the magnetic clutch holding coils release the full-length CEAs.

Either relay M-1 or M-2 is sufficient to remove ac power from one side of the CRD clutch power buses. Similarly, either relay M-3 or M-4 is sufficient to remove ac power from the other side of the CRD clutch power buses. Power must be removed from both sides of the CRD clutch buses in order to de-energize the magnetic clutch holding coils and release the full-length rods.

A reactor trip is accomplished by de-energizing the CEDM coils, allowing the shutdown and regulating CEAs to drop into the core by gravity.

2.1.3.2 Groups 2 and 3 Trip Circuit Breaker Logic

Relays K-1 through K-4 contain contacts that provide actuation of the undervoltage and shunt trips of the eight trip circuit breakers. De-energizing any one trip breaker control relay (K-x) opens one trip path and opens the two breakers controlled by that trip path.

The CEDMs are separated into two groups. The CEDM power supplies in each group are supplied with parallel ac power. The loss of either set does not cause a release of the CEAs. Each power supply source is separated into two branches. Each side of each branch line passes through two trip circuit breakers (each actuated by a separate trip path) in series so that, although both sides of the branch lines must be de-energized to release the CEAs, there are two separate means of interrupting each side of the line.

A reactor trip is accomplished by de-energizing the CEDM coils, allowing the shutdown and regulating CEAs to drop into the core by gravity.

2.1.3.3 Group 4 Trip Circuit Breaker Logic

Relays K-1 through K-4 contain contacts that provide actuation of the undervoltage and shunt trips of the four trip circuit breakers. De-energizing of any one trip breaker control relay (K-x) opens one trip path and opens the breaker controlled by that trip path.

The CEDMs are separated into two groups, but are supplied ac power from the same parallel power arrangement. The loss of either set does not cause a release of the CEAs. Each side of the branch lines pass through two trip circuit breakers (each actuated by a separate trip path) in series so that, although both sides of the branch lines must be de-energized to release the CEAs, there are two separate means of interrupting each side of the line.

A reactor trip is accomplished by de-energizing the CEDM coils, allowing the shutdown and regulating CEAs to drop into the core by gravity.

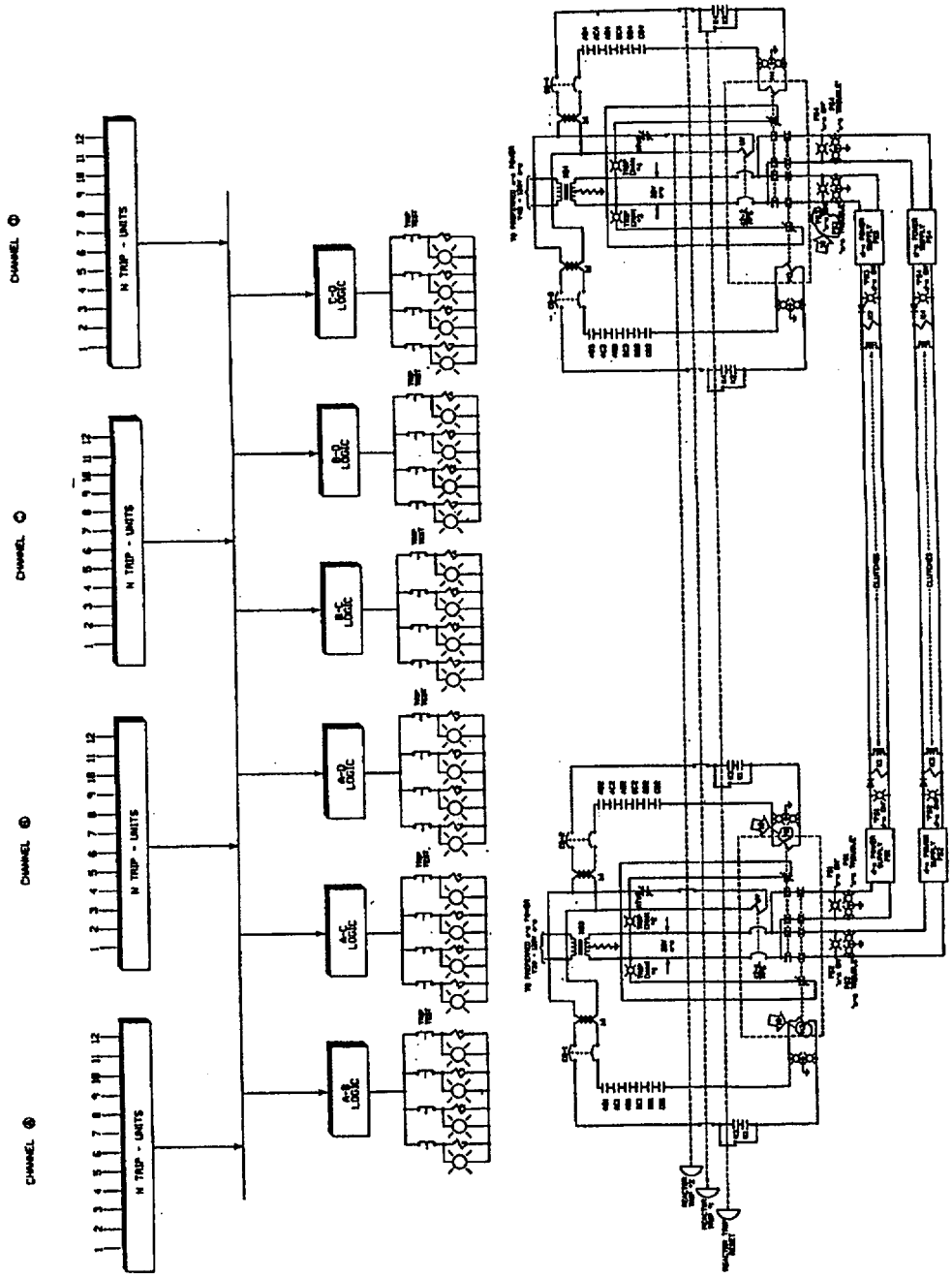


Figure 2-1. Group 1 Combustion Engineering RPS simplified schematic.

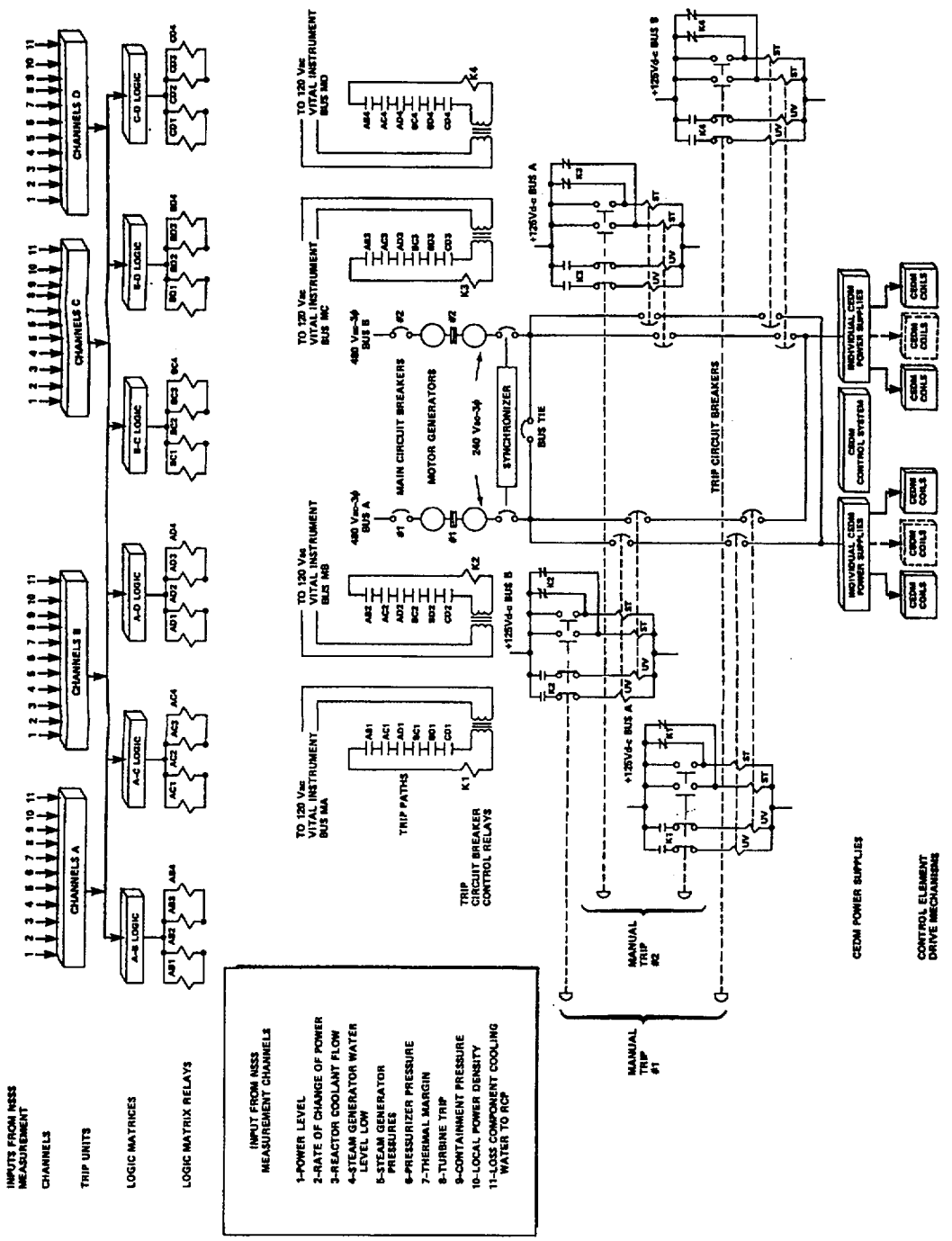


Figure 2-2. Groups 2 and 3 Combustion Engineering RPS simplified schematic.

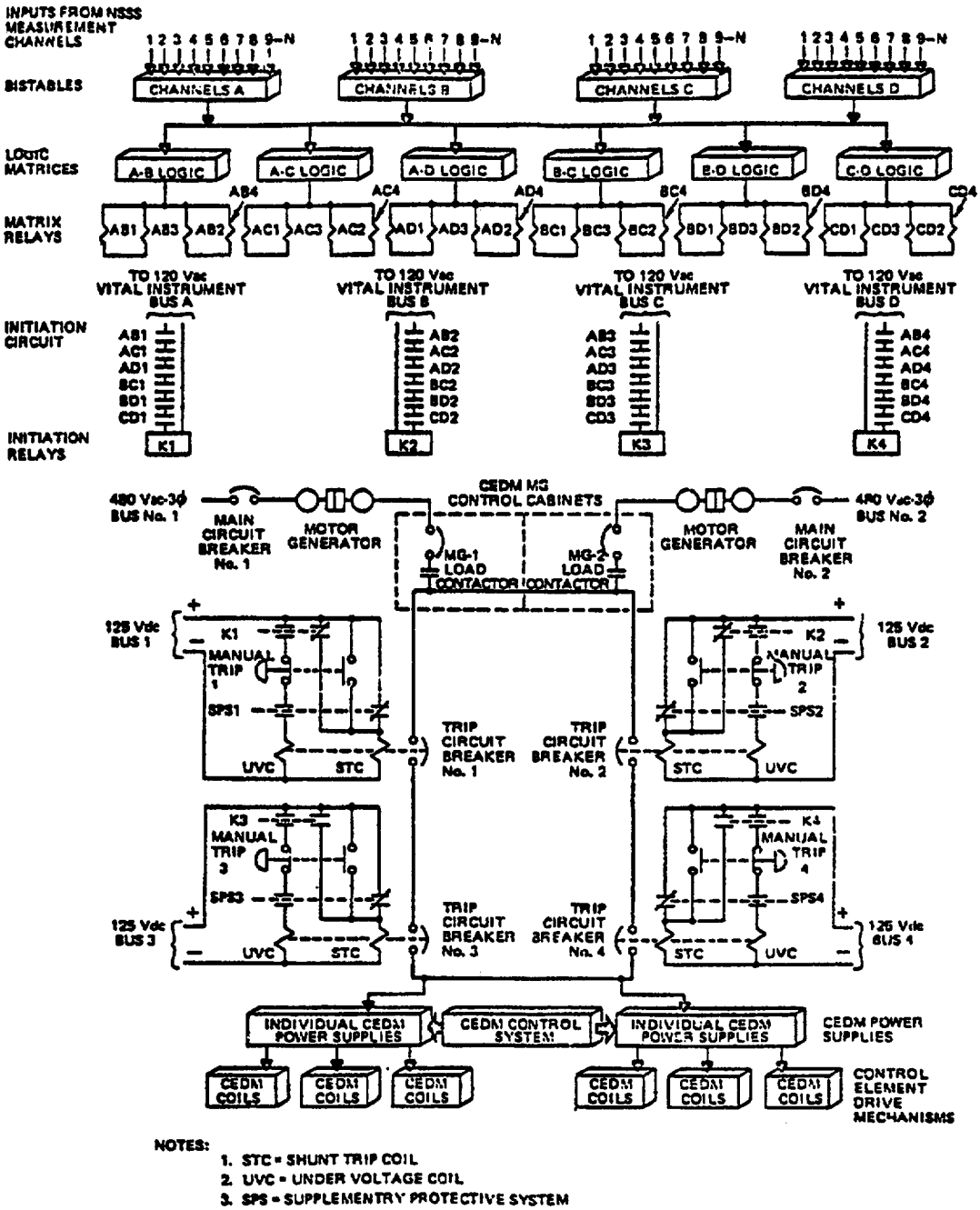


Figure 2-3. Group 4 Combustion Engineering RPS simplified schematic.

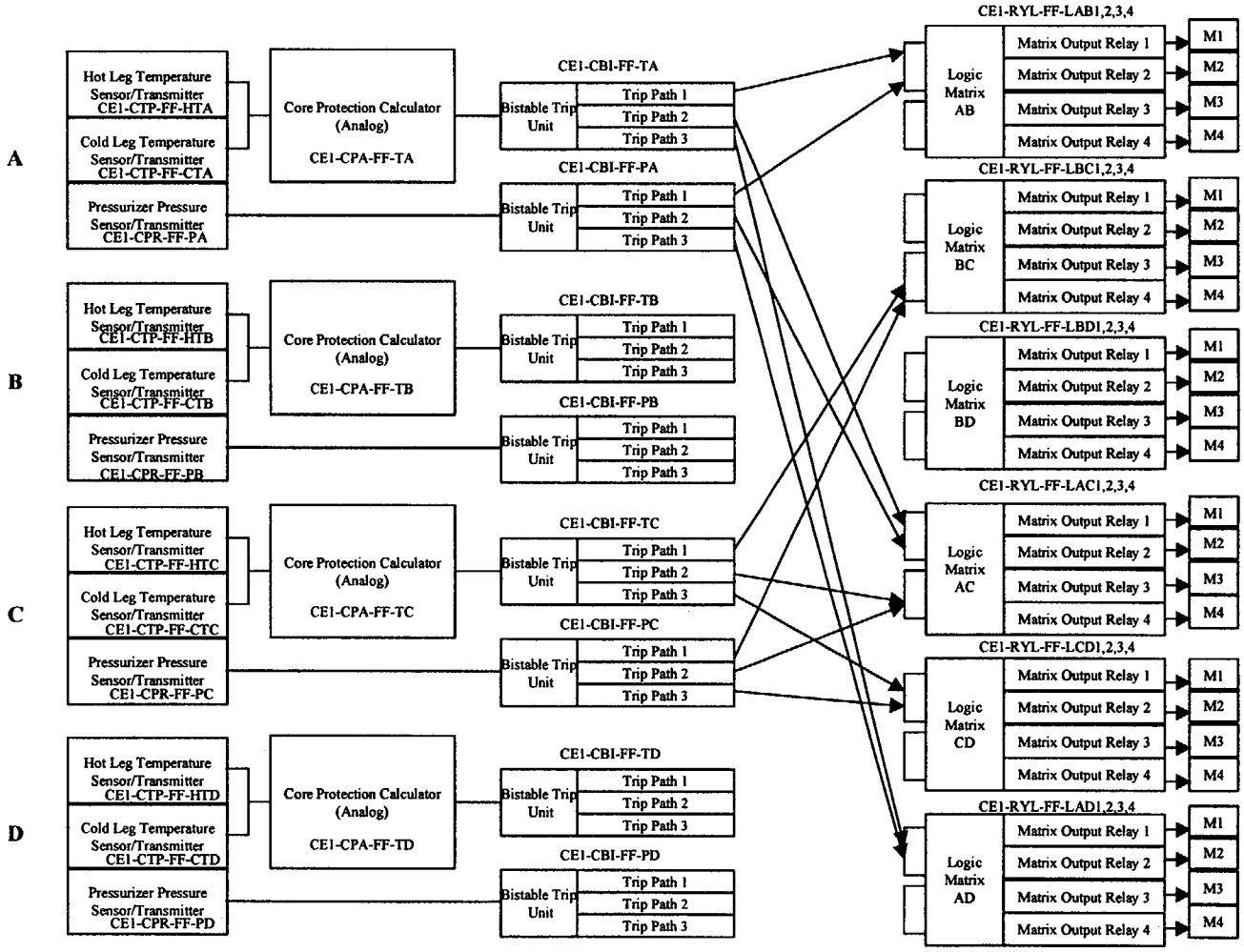


Figure 2-4. Group 1 Combustion Engineering RPS simplified diagram.

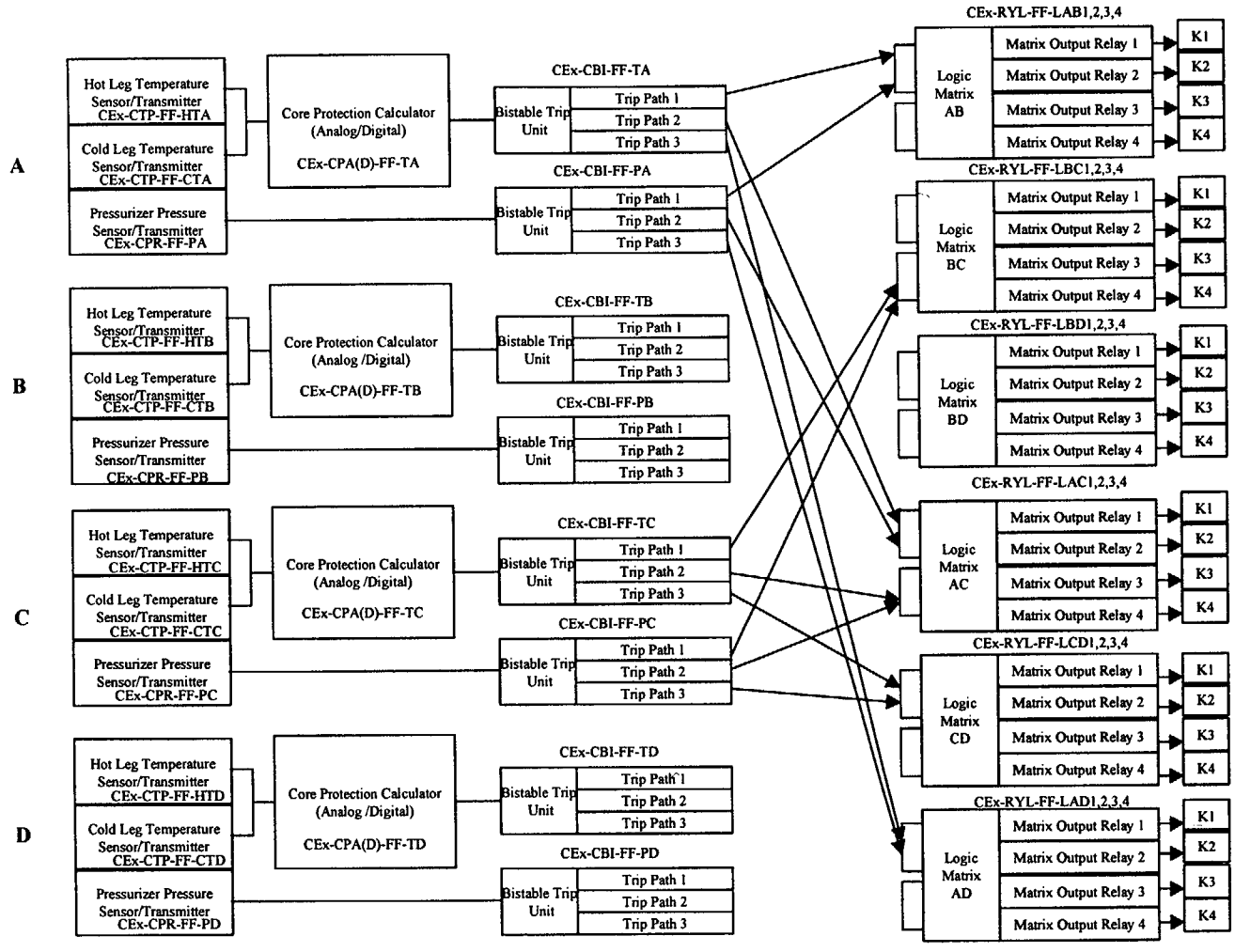


Figure 2-5. Groups 2, 3, and 4 Combustion Engineering RPS simplified diagram.

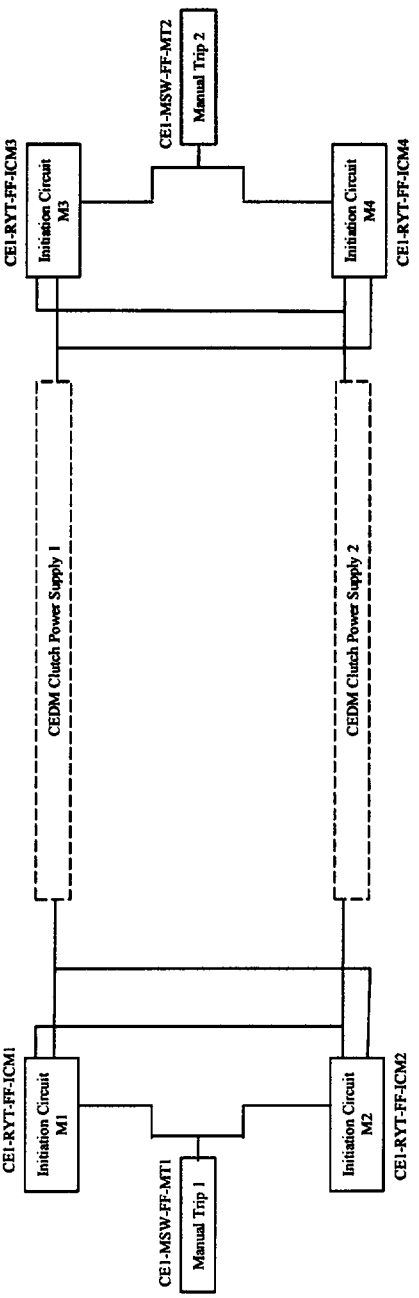


Figure 2-6. Group 1 Combustion Engineering RPS trip contactor and control element assemblies simplified diagram.

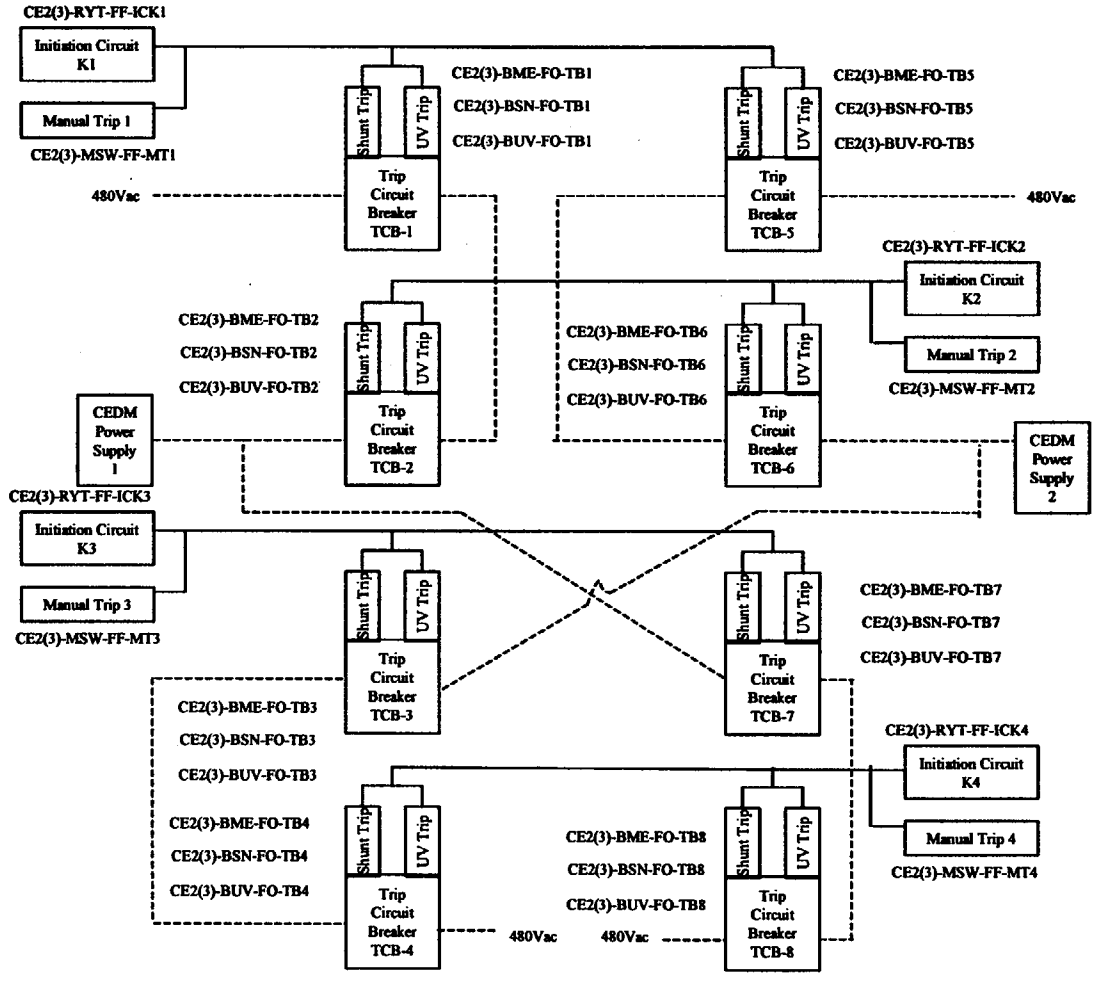


Figure 2-7. Group 2 & 3 Combustion Engineering RPS trip circuit breaker and control element assemblies simplified diagram.

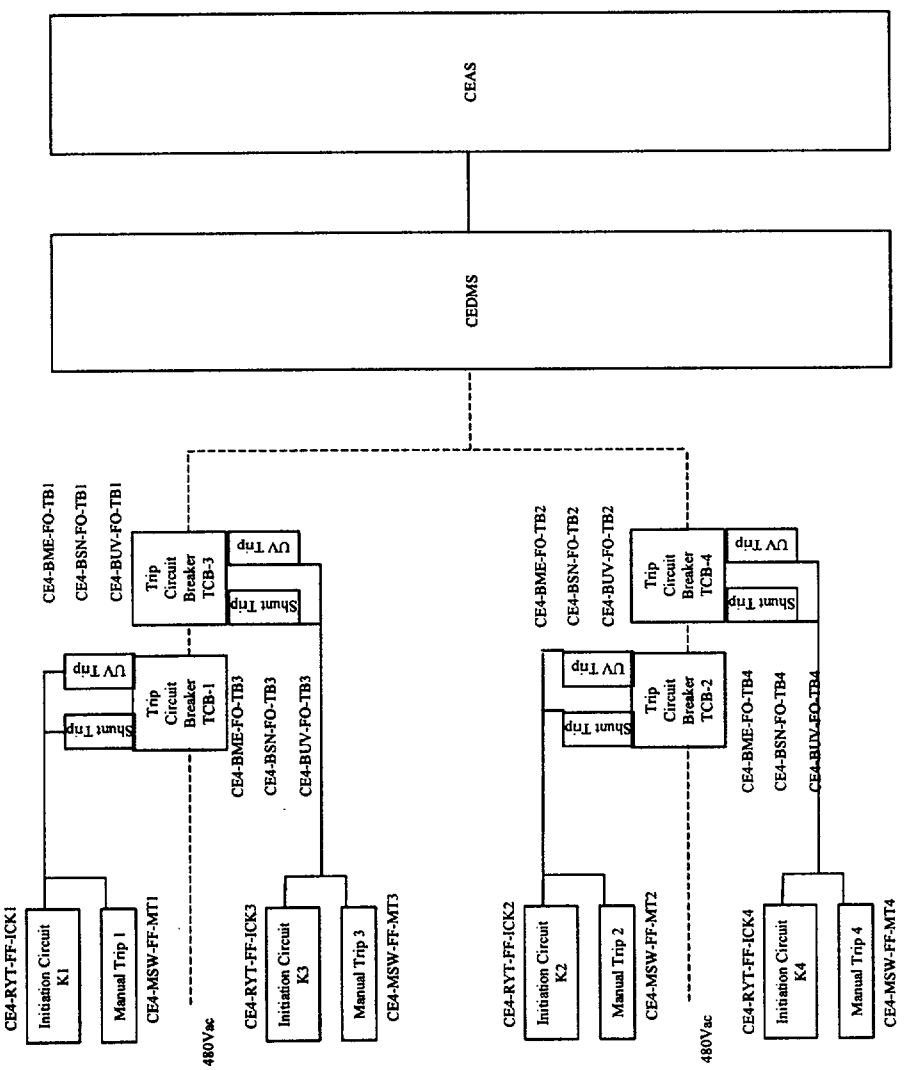


Figure 2-8. Group 4 Combustion Engineering RPS trip circuit breaker and control element assemblies simplified diagram.

Table 2-5. Generic Combustion Engineering RPS trip signals.

Trip Signal	Trip Logic	Purpose of Trip
1. High linear power	2-out-of-4 Coincident	Trip the reactor in the event of a reactivity excursion too rapid to be mitigated by the high-pressure trip without damage.
2. High thermal margin/low pressure [a]	2-out-of-4 Coincident	Two purposes: the thermal margin portion of the trip, in conjunction with the low reactor coolant flow trip, prevents violation of the safety limit on DNB during anticipated transients. The low-pressure portion of the trip functions to trip the reactor in case of a LOCA.
3. High local power density	2-out-of-4 Coincident	Prevent peak local power density in the fuel from exceeding limits.
4. High pressurizer pressure [a]	2-out-of-4 Coincident	Prevent excessive blowdown of the RCS by relief action through the pressurizer safety valves.
5. Low steam generator level	2-out-of-4 Coincident	Protect the reactor coolant system in case of a loss of feedwater and resultant loss in heat sink.
6. Low steam generator pressure	2-out-of-4 Coincident	Protect the RCS from the excessive rate of heat extraction from a steam line break.
7. Low reactor coolant flow	2-out-of-4 Coincident	Protect the core against exceeding departure from nucleate boiling (DNB).
8. High containment pressure	2-out-of-4 Coincident	Assure the trip of the reactor is concurrent with safety injection actuation.
9. Loss of load	2-out-of-4 Coincident	Minimize primary system upset on turbine trip.

a. These two signals are modeled in the RPS fault tree used for this study.

2.1.4 System Testing

Table 2-6 shows the components in the RPS system that are considered in the PRA model and indicates when these components are counted as being demanded based on reactor trips, testing, and operational demands.

Several different types of tests are performed periodically on the Combustion Engineering RPS. Channel checks are performed to detect variances between instruments. These checks ensure that redundant parameter indications, such as reactor pressure or temperature, agree within certain limits. These channel checks identify gross failures in the channel sensor/transmitters. When channel checks are performed, the channel is placed in a bypass mode.

Table 2-6. Combustion Engineering RPS components used in the probabilistic risk assessment.

Comp. code	Component	Testing Frequency [a]	Operating [b]	Demanded in each reactor trip	Count basis
Channel					
CPR	Pressure sensor/transmitter	Cyclic and quarterly [c]	Yes	No	One for the pressurizer & at least one per steam generator, per channel. The digital plants have two per SG/ channel. See Note d.
CTP	Temperature sensor/transmitter	Cyclic & quarterly [c]	Yes	No	2/loop/channel, except Maine Yankee with 1/loop/channel.
CPA	Analog core protection calculator	Quarterly	Yes	No	1 per channel (Model Groups 1, 2)
CPD	Digital core protection calculator	Quarterly	Yes	No	1 per channel (Model Groups 3, 4)
CBI	Bistable	Quarterly	No	No	12 to 16 per channel
Trains					
RYL	Logic relay	Quarterly	No	No	dc. 24 (from 6 logic matrices and 4 channels)
RYT	Trip relay	Quarterly [f]	No	No	4 K relays; except, at Group 1 plants, 4 M relays.
MSW	Manual scram switch	Quarterly	No	Yes [e]	4, except 2 at Model Group 1 plants.
Trip breakers and rods					
BME	Breaker mechanical	Quarterly & monthly [f]	No	Yes	8 for plants in Model Groups 2 and 3. 4 for Group 4.
BSN	Breaker shunt device	Quarterly [f]	No	No [g]	1 per breaker
BUV	Breaker undervoltage coil	Monthly [h]	No	No [g]	1 per breaker
RMA	Control element assembly & rod	Cyclic	No	Yes	Plant-specific. NPRDS data not collected after 3/15/94.

a. Information is from CEN-327-A. A Combustion Engineering owners group submittal in May 1986, argued for quarterly rather than monthly testing of channels. However, it is not known when particular plants switched to quarterly testing. This study assumes quarterly testing for the entire study period (1984-1995).

b. Operating components are those components whose safety function failures can be detected in time. Rates as well as probabilities of failure on demand are estimated for operating components. The instruments are visually checked in each shift, and the core protection calculators perform continuous internal checking for certain types of failures.

c. In the quarterly channel tests, responsiveness of the sensor/transmitter signal conditioning is verified.

d. Plant Model Groups 1 and 2 are analog, while Groups 3 and 4 are digital. See Table 3. There are two loops/plant, except for Maine Yankee, which has three.

e. Demanded in manual trips, not automatic trips.

f. Each quarterly test includes 6 demands, one associated with each logic matrix.

g. BSN or BUV failures that occur during a trip generally cannot be detected. Both BSN and BUV must fail in order for the failure to be detected.

h. Quarterly tests not included for BUV because the breaker actuation tests do not test UV and shunt mechanisms separately.

2.1.5 System Boundary

The RPS boundary for this study includes the four segments indicated in Table 2-3. Also included is the control room operator who pushes the manual reactor trip buttons. The supplementary protection system (SPS, an ATWS system) is not included in the analysis.

2.2 System Fault Tree

This section briefly describes the Combustion Engineering RPS fault trees developed for this study. Appendix D presents the actual fault trees. The analysis of the Combustion Engineering RPS is based on representative designs based on Groups 1, 2, 3, and 4, as defined in Table 2-2. Note that the RPS fault tree development represents a moderate level of detail, reflecting the purpose of this project—to collect actual RPS performance data and assemble the data into overall RPS unavailability estimates. The level of detail in the fault trees reflects the level of detail available from the component failure information in the NPRDS and the LERs.

The top event in the RPS fault tree is Reactor Protection System (RPS) Fails. RPS failure at this top level is defined as an insufficient number of shutdown rods inserting into the core to inhibit the nuclear reaction. Various plant upset conditions can result in differing requirements for the minimum number of shutdown rods to be inserted into the core, and the positions of the shutdown rods within the core can also be important. The shutdown rod failure criterion was chosen to be 20 percent (or more) of the shutdown rods fail to insert.

The level of detail in the RPS fault tree includes sensor/transmitters, bistable trip units, relays, trip contactors/trip circuit breakers with the undervoltage and shunt trip devices modeled separately, control rod drives, and control rods. The Loss of Main Feedwater event is the most severe event with respect to the Severe Condition 3 reactor coolant pressure limit. This event is modeled as high pressurizer pressure and high thermal margin/low pressure (see Table 2-5). These are two parameters that would detect several types of plant upset conditions while the plant is at power.

Common-cause failures (CCFs) across similar components were explicitly modeled in the RPS fault tree. Examples of such components include the sensor/transmitters, bistable trip units, relays, trip breakers with the undervoltage and shunt trip devices modeled separately, and CRD/rods. In general, the common-cause modeling in the RPS fault tree is limited to the events that fail enough components to fail that portion of the RPS. Lower-order CCF events are not modeled in the fault tree. Such events would have to be combined with independent failures to fail the portion of the RPS being modeled. Such combinations of events (not modeled in the fault tree) were reviewed to ensure that they would not have contributed significantly to the overall RPS unavailability.

Test and maintenance outages and associated RPS configurations are modeled for channel outages. For channel outages, the fault tree was developed based on the assumption that a channel out for testing or maintenance is placed into the bypass mode rather than a tripped mode. All channel test and maintenance outages are modeled in Channel A. There are no test and maintenance outages modeled for the trip modules or breakers, since these components are placed in a tripped state during testing and have no effect on the failure to insert rods.

2.3 Operational Data Collection, Characterization, and Analysis

The RPS data collection, characterization, and analysis process is shown in Figure 2-9. The major tasks include failure data collection and characterization, demand data collection, and data analysis. Each

of these major tasks is discussed below. Also discussed is the engineering analysis of the data. Appendix A presents a more detailed explanation of the process.

2.3.1 Inoperability Data Collection and Characterization

The RPS is a system required by technical specifications to be operable when the reactor vessel pressure is above 150 psig (some plants have a 90-psig requirement); therefore, all occurrences that result in the system not being operable are required by 10 CFR 50.73(a)(2)(i)(B) to be reported in LERs. In addition, 10 CFR 50.73(a)(2)(vii) requires the licensee to report all common-cause failures resulting in a loss of capability for safe shutdown. Therefore, the SCSS LER database should include all occurrences when the RPS was not operable and all common-cause failures of the RPS. However, the LERs will not normally report RPS component independent failures. Therefore, the LER search was supplemented by an NPRDS data search. NPRDS data were downloaded for all RPS and control rod drive system records for the years 1984 through 1995. The SCSS database was searched for all RPS failures for the period 1984 through 1998. In addition, the NRC's Performance Indicator Database and the 1987–1998 database used for the initiating events study [NUREG/CR-5750] were compared to obtain a list of unplanned RPS demands (reactor trips).

The NPRDS reportable scope for RPS and control rod drive systems includes the components modeled in the fault tree described in Section 2.2 and presented in Appendix D. Therefore, the NPRDS data search should identify all RPS component failures through the end of 1995. Failures for control rods, however, are only reported in the NPRDS through March 15, 1994.

In this report, the term *inoperability* is used to describe any RPS event reported by NPRDS or the LERs. The inoperabilities are classified as fail-safe (FS) or non-fail-safe (NFS) for the purposes of this study. The term *NFS* is used to identify the subset of inoperabilities for which the safety function of the RPS component was impacted. An example of an NFS event is a failure of the channel trip unit to open given a valid signal to open. The term *FS* is used to describe the subset of inoperabilities for which the safety function of the RPS component was not impacted. Using the trip unit as an example, a spurious opening of the trip unit is an FS event for the purposes of this study. For some events, it was not clear whether the inoperability is FS or NFS. In such cases, the event was coded as unknown (UKN).

Inoperability events were further classified with respect to the degree of failure. An event that resulted in complete failure of a component was classified as a Complete Failure (CF). The failure of a trip unit to open given a valid signal to open is a CF (and NFS) event. Events that indicated some degradation of the component, but with the component still able to function, were classified as No Failure (NF). An example of an NF event is a trip unit with its trip setting slightly out of specification, but which is still able to open (but late) when demanded. For some events, it was not clear, whether the inoperability was CF or NF. In such cases, the event was coded as Unknown Completeness (UC).

Table 2-7 summarizes the data classification scheme. In the table, the data can be placed into nine bins. These nine bins represent combinations of the three types of safety function impact (NFS, UKN, or FS) and the three degrees of failure completeness (CF, UC, or NF). As indicated by the shaded area in Table 2-7, the data classification results in one bin containing non-fail-safe complete failures (NFS/CF) and three bins (NFS/UC, UKN/CF, and UKN/UC) that contain events that are potentially NFS/CF. For these three bins, a lack of information in the data event reports did not allow the data analyst to determine whether the events were NFS/CF. These three bins are called collectively, "Uncertain Failures." The other five bins do not contain potential NFS/CF events, and generally were not used in the data analysis.

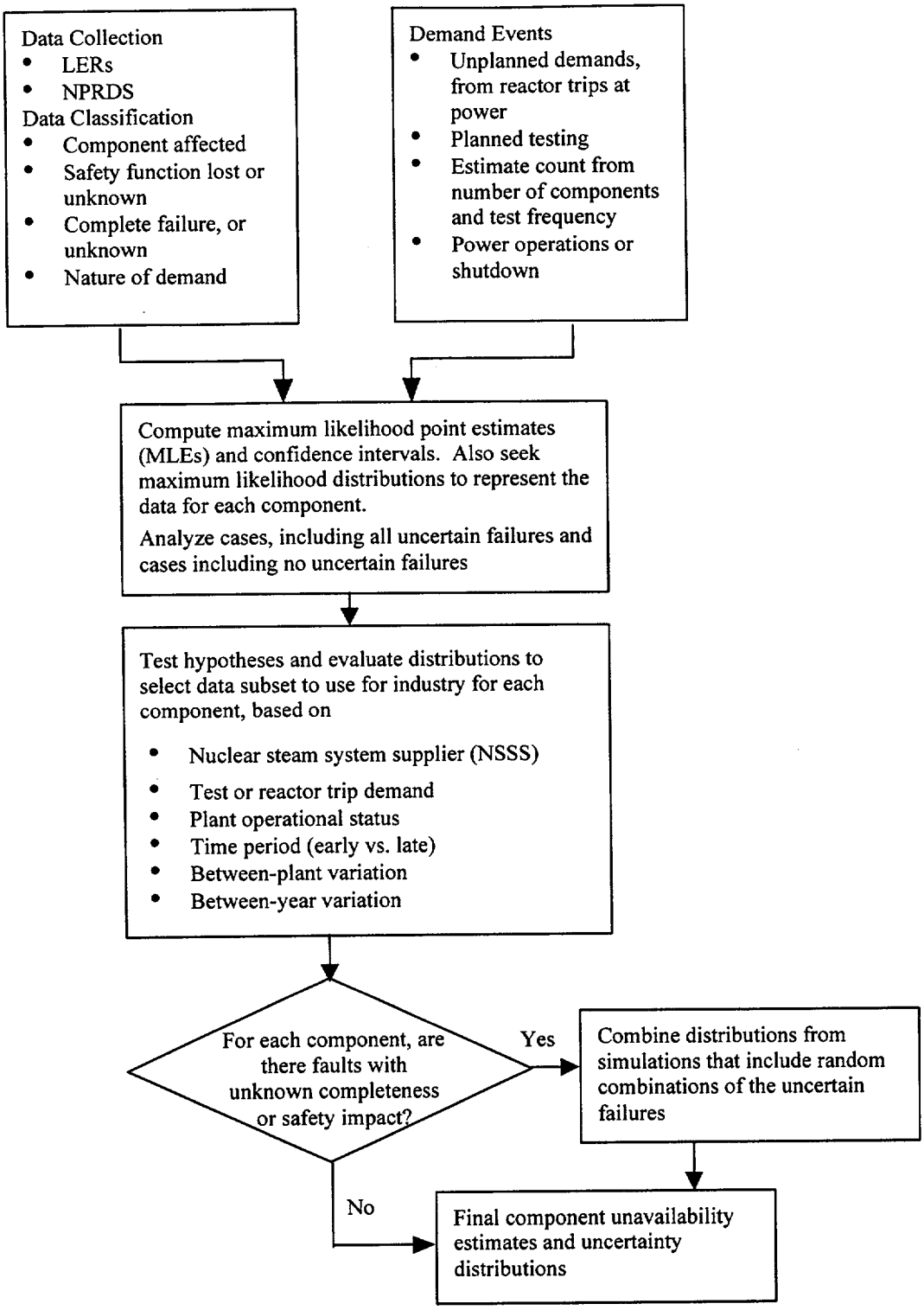


Figure 2-9. Data collection, characterization, and analysis process.

Table 2-7. Data classification scheme.

	Safety Function Impact		
Failure Completeness	NFS/CF (safety function impact, complete failure)	UKN/CF (unknown safety function impact, complete failure; potential NFS/CF)	FS/CF (no safety function impact, complete failure)
	NFS/UC (safety function impact, unknown completeness; potential NFS/CF)	UKN/UC (unknown safety function impact, unknown completeness; potential NFS/CF)	FS/UC (no safety function impact, unknown completeness)
	NFS/NF (safety function impact, no failure)	UKN/NF (unknown safety function impact, no failure)	FS/NF (no safety function impact, no failure)

The data characterization followed a three-step process: an initial review and classification by personnel with operator level nuclear plant experience, a consistency check by the same personnel (reviewing work performed by others), and a final, focused review by instrumentation and control and RPS experts. This effort involved approximately 2400 NPRDS and LER records.

2.3.2 Demand Data Collection and Characterization

Demand counts for the RPS include both unplanned system demands or unplanned reactor trips while the plant is at power, and tests of RPS components. These demands meet two necessary criteria: (1) the demands must be identifiable, countable, and associated with specific RPS components, and (2) the demands must reasonably approximate the conditions being considered in this study. Unplanned reactor trips meet these criteria for the following RPS components: breakers, manual switches (for manual trips), and the CRD/RODS. However, the reactor trips do not meet the first criterion for channel components, because it is not clear what reactor trip signals existed for each unplanned reactor trip. For example, not all unplanned reactor trips might have resulted from a reactor vessel high pressure.

The RPS component tests clearly meet the first criterion, though uncertainty exists in the association of RPS component failures with particular types of testing. For this report, any failures discovered in testing were assumed to be associated with the specific periodic testing described in Section 2.1.4. Because of the types of tests, the test demands also meet the second criterion, i.e., the tests are believed to adequately approximate conditions associated with unplanned reactor trips.

For unplanned demands, the LER Performance Indicator data describe all unplanned reactor trips while plants are critical. The reactor trip LERs were screened to determine whether the reactor trips were automatic or manual, since each type exercises different portions of the RPS. For RPS component tests, demands were counted based on component populations and the testing schedule described in Section 2.1.4. More details on the counting of demands are presented in Appendix A.

2.3.3 Data Analysis

In Figure 2-9, the data analysis steps shown cover the risk-based analysis of the operational data leading to the quantification of RPS unavailability. Not shown in Figure 2-9 is the engineering analysis of the operational data. The risk-based analysis involves analysis of the data to determine the appropriate subset of data for each component unavailability calculation. Then simulations can be performed to characterize the uncertainty associated with each component unavailability.

The risk-based analysis of the operational data (Section 3) and engineering analysis of the operational data (Sections 4.1 and 4.2) are largely based on two different data sets. The Venn diagram in Figure 2-10 illustrates the relationship between these data sets. Data set A represents all of the LER and NPRDS events that identified an RPS inoperability. Data set B represents the inoperabilities that resulted in a complete loss of the safety function of the RPS component, or the NFS/CF events (and some fraction of the NFS/UC, UKN/CF, and UKN/UC events). Finally, data set C represents the NFS/CF events (and some fraction of the NFS/UC, UKN/CF, and UKN/UC events) for which the corresponding demands could be counted. Data set C (or a subset of C) is used for the failure upon demand risk-based analysis of the RPS components. Data set C contains all NFS/CF events (and some fraction of the NFS/UC, UKN/CF, and UKN/UC events) that occurred during either an unplanned reactor trip while the plant was critical or a periodic surveillance test.

Since the instrumentation is continuously operating, it may experience failures that are detected and repaired on an ongoing basis. The failure modes for such failures differ from the failure modes that may be detected on demands or tests. Instrumentation failures in Set B that are not in Set C were used to estimate failure rates for the unavailability analysis for these components.

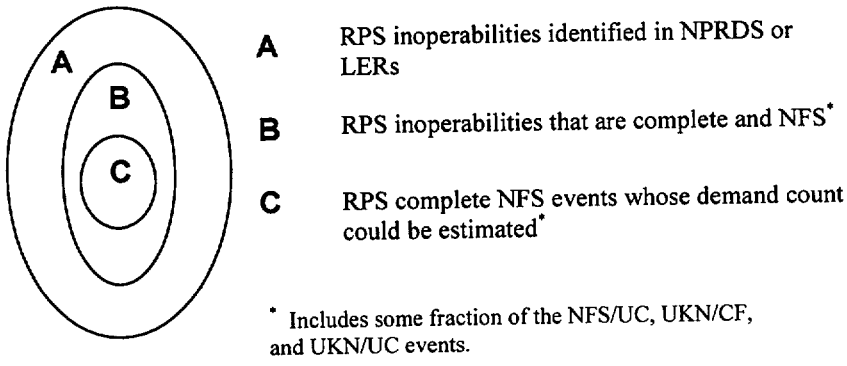


Figure 2-10. RPS data sets.

The purpose of the engineering analysis is to provide qualitative insights into RPS performance. The engineering analysis focused on data set B in Figure 2-10, which includes data set C as a subset. Data set A was not used for the engineering analysis because the additional FS events in that data set were not judged to be informative with respect to RPS failure to trip, which is the focus of this report.

In contrast to the risk-based analysis of operational data to obtain component failures upon demand, which used data set C, the CCF analysis used the entire data set B. This is appropriate because the CCF analysis is concerned with what fraction of all NFS events involved more than one component. Such an analysis does not require that the failures be matched to demands. The engineering analysis of CCF events, in Section 4, also used data set B.

3. RISK-BASED ANALYSIS OF OPERATIONAL DATA

3.1 Unavailability Estimates Based on System Operational Data

If the Combustion Engineering RPS evaluated at the system level, with no consideration of plant-to-plant variations in RPS designs, then a system failure probability should be able to be estimated based on the total system failures and total system demands. For the period 1984 through 1998, there were no RPS system failures in 612 demands (unplanned reactor trips). This data is too sparse to accurately estimate a system unavailability using a Jeffreys noninformative prior and applying a Bayesian update technique. Therefore, in order to obtain a realistic RPS unavailability estimate, an RPS fault tree was developed, as discussed in the following section. That approach permits the use of RPS component failure data.

3.2 Unavailability Estimates Based on Component Operational Data

3.2.1 Fault Tree Unavailability Results

The Combustion Engineering RPS fault trees presented in Appendix D and discussed in Section 2.2 were quantified using the SAPHIRE computer code.[10] Fault tree basic event probabilities are presented in the following tables. The basic events are divided into three groups: component independent failure events (Table 3-1), CCF events (Table 3-2), and other types of events, such as test and maintenance outages and operator errors (Table 3-3). Failure probabilities for the component independent failures were obtained from the Combustion Engineering RPS data and other PWR vendors as necessary. Failure data are discussed in Section 2.3. Details of the methodology are discussed in Appendix A, a summary of the data is presented in Appendix B, and the results of the analyses are presented in Appendix C. All of the component independent failure probabilities listed in Table 3-1 are based on component failure events during the period 1984 through 1998. Data collection is shown in Table C-1 in Appendix C.

The CCF event probabilities in Table 3-2 are based on the Combustion Engineering RPS CCF data during the period 1984 through 1998. However, the CCF event probabilities are also influenced by the prior used in the Bayesian updating of the common-cause α parameters. The prior for this study was developed from the overall PWR RPS CCF database. A summary of the Combustion Engineering CCF data is presented in Appendix B, while the actual details of the CCF calculations are in described in Appendix E. In general, the CCF events reflect multipliers (from the alpha equations) of 0.01 to 0.0002 on the total component failure probabilities in Table 3-2.

The other types of fault tree basic events in Table 3-3 involve test and maintenance outages and operator error. No credit was taken for operator action to manually actuate the RPS in the base case quantification, so the operator action has a failure probability of 1.0. However, the RPS was also quantified assuming an operator action failure probability of 1.0E-2, which is a typical value used in individual plant examinations (IPEs).

Table 3-1. Combustion Engineering RPS fault tree independent failure basic events.

Comp-onent Code	Component Type	Fault Tree Basic Event	Number of Failures [a]	Number of Demands	Modeled Variation [b]	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
BME[c]	Breaker mechanical	CE2-BME-FO-TB-1,2,3,4,5,6,7,8 CE3-BME-FO-TB-1,2,3,4,5,6,7,8 CE4-BME-FO-TB-1,2,3,4	1 (1.0)	83,813	Sampling	Lognormal	4.3E-6 1.8E-5 4.5E-5	Trip breaker local hardware faults
BSN	Shunt trip device	CE2-BSN-FF-TB-1,2,3,4,5,6,7,8 CE3-BSN-FF-TB-1,2,3,4,5,6,7,8 CE4-BSN-FF-TB-1,2,3,4	3 (3.5)	25,270	Year	Lognormal	6.3E-6 1.5E-4 5.5E-4	Shunt trip device local faults
BUV	Undervoltage device	CE2-BUV-FF-TB-1,2,3,4,5,6,7,8 CE3-BUV-FF-TB-1,2,3,4,5,6,7,8 CE4-BUV-FF-TB-1,2,3,4	10 (13.6)	12,635	Plant	Lognormal	1.4E-4 1.1E-3 3.5E-3	Undervoltage coil device local faults
CBI	Trip unit (bistable)	CE1-CBI-FF-PA,B,C,D CE1-CBI-FF-TA,B,C,D CE2-CBI-FF-PA,B,C,D CE2-CBI-FF-TA,B,C,D CE3-CBI-FF-PA,B,C,D CE3-CBI-FF-TA,B,C,D CE4-CBI-FF-PA,B,C,D CE4-CBI-FF-TA,B,C,D	5 (7.0)	15,262	Plant	Lognormal	3.4E-5 5.0E-4 1.8E-3	Channel trip unit (bistable) fails to trip at its setpoint
CPA	Analog core protection calculator	CE1-CPA-FF-TA,B,C,D CE2-CPA-FF-TA,B,C,D	3(8.2)	1082	Plant	Lognormal	1.6E-3 7.6E-3 2.0E-2	Channel analog core protection calculator fails to send a signal to the trip unit
CPD	Digital core protection calculator	CE3-CPD-FF-TA,B,C,D CE4-CPD-FF-TA,B,C,D	1(1.0)	548	Sampling	Lognormal	6.5E-4 2.7E-3 6.8E-3	Channel digital core protection calculator fails to send a signal to the trip unit

Table 3-1. (Continued)

Comp -onent Code	Component Type	Fault Tree Basic Event	Number of Failures [a]	Number of Demands	Modeled Variation [b]	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
CPR	Pressure sensor/ transmitter	CE1-CPR-FF-PA,B,C,D CE2-CPR-FF-PA,B,C,D CE3-CPR-FF-PA,B,C,D CE4-CPR-FF-PA,B,C,D	0 (0.0)	4,678	Plant	Lognormal	1.1E-5 1.1E-4 3.5E-4	Channel reactor vessel pressure sensor/ transmitter fails to detect a high pressure and sends a signal to the trip unit
CTP	Temperatur e sensor/ transmitter	CE1-CTP-FF-C(H)TA,B,C,D CE2-CTP-FF-C(H)TA,B,C,D CE3-CTP-FF-C(H)TA,B,C,D CE4-CTP-FF-C(H)TA,B,C,D	2 (4.2)	12,530	Sampling	Lognormal	4.2E-4 8.4E-4 1.5E-3	Channel reactor vessel temperature/ transmitter (cold or hot leg) fails to detect a low level and sends a signal to the trip unit
MSW [c]	Manual scram switch	CE1-MSW-FF-MT1,2 CE2-MSW-FF-MT1,2,3,4 CE3-MSW-FF-MT1,2,3,4 CE4-MSW-FF-MT1,2,3,4	2 (2.0)	19,789	Sampling	Lognormal	4.1E-5 1.3E-4 2.8E-4	Manual scram switch fails to operate upon demand
RMA [c] (ROD and CRD)	Control rod and associated control rod drive	None (supports ROD CCF event in fault tree)	1 (2.9)	189,536	Plant	Lognormal	3.4E-7 1.7E-5 6.4E-5	Control rod (or associated control rod drive) fails to insert fully into core upon demand
RYL	Logic Relay	CE1-RYL-FF-LA,B,C,D – 1,2,3,4 CE2-RYL-FF-LA,B,C,D – 1,2,3,4 CE3-RYL-FF-LA,B,C,D – 1,2,3,4 CE4-RYL-FF-LA,B,C,D – 1,2,3,4	2 (4.2)	16,160	Plant	Lognormal	2.2E-5 2.6E-4 8.8E-4	Channel logic relay fails to de-energize upon demand

Table 3-1. (Continued)

Comp -onent Code	Component Type	Fault Tree Basic Event	Number of Failures [a]	Number of Demands	Modeled Variation [b]	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
RYT	Trip Relay	CE1-RYT-FF-ICM1,2,3,4 CE2-RYT-FF-ICK1,2,3,4 CE3-RYT-FF-ICK1,2,3,4 CE4-RYT-FF-ICK1,2,3,4	1 (1.5)	16,160	Sampling	Lognormal	3.3E-5 1.2E-4 3.0E-4	Trip system trip relay fails to de-energize upon demand

a. Includes uncertain events and CCF events. The number in parentheses is the weighted average number of failures, resulting from the inclusion of uncertain events from data bins NFS/UC, UKN/CF, and UKN/UC (explained in Section 2.3.1).
b. Modeled variation indicates the type of data grouping used to determine the uncertainty bands. For example, for the plant-to-plant variation, data were organized by plant to obtain component failure probabilities per plant. Then, the plant failure probabilities were combined to obtain the mean and variance for the component uncertainty distribution. See Appendix A for more details.
c. The failure data and demand counts for this component are based on pooling of two or more plant vendor designs. See Appendix C Table C-9 for more detail on which vendors were pooled.

Table 3-2. Combustion Engineering RPS fault tree CCF basic events.

Component Code	Component Type	Basic Event(s)	Number of CCF Events	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
BME [a]	Breaker mechanical	CE2-BME-CF-TB2OF8 CE3-BME-CF-TB2OF8	3	Lognormal	1.9E-7 1.0E-6 2.7E-6	CCF 2 of 8 trip breaker local hardware faults
		CE4-BME-CF-TB2OF4	3	Lognormal	8.0E-8 7.1E-7 2.2E-6	CCF 2 of 4 trip breaker local hardware faults
BSN	Shunt trip device	CE2-BSN-CF-TB2OF8 CE3-BSN-CF-TB2OF8	2	Lognormal	3.9E-7 1.1E-6 4..0E-5	CCF 2 of 8 shunt trip device local faults

Table 3-2. (Continued)

Component Code	Component Type	Basic Event(s)	Number of CCF Events	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
		CE4-BSN-CF-TB2OF4	2	Lognormal	2.5E-7 8.7E-6 3.3E-5	CCF 2 of 4 shunt trip device local faults
BUV	Undervoltage device	CE2-BUV-CF-TB2OF8 CE3-BUV-CF-TB2OF8	2	Lognormal	5.1E-6 5.4E-5 1.8E-4	CCF 2 of 8 undervoltage coil device local faults
		CE4-BUV-CF-TB2OF4	2	Lognormal	2.3E-6 3.7E-5 1.3E-4	CCF 2 of 4 undervoltage coil device local faults
CBI	Trip unit (bistable)	CE1-CBI-CF-P(T)2OF3TM CE2-CBI-CF-P(T)2OF3TM CE3-CBI-CF-P(T)2OF3TM CE4-CBI-CF-P(T)2OF3TM	27	Lognormal	1.1E-6 2.6E-5 9.5E-5	CCF specific 2 of 3 bistables associated with either a pressure (P) or temperature (T) signal (T&M)
		CE1-CBI-CF-P(T)3OF4 CE2-CBI-CF-P(T)3OF4 CE3-CBI-CF-P(T)3OF4 CE4-CBI-CF-P(T)3OF4	27	Lognormal	1.4E-7 7.2E-6 2.8E-5	CCF specific 3 of 4 bistables associated with either a pressure (P) or temperature (T) signal
		CE1-CBI-CF-4OF6TM CE2-CBI-CF-4OF6TM CE3-CBI-CF-4OF6TM CE4-CBI-CF-4OF6TM	27	Lognormal	3.7E-8 1.7E-6 6.6E-6	CCF specific 4 of 6 bistables (T&M)
		CE1-CBI-CF-6OF8 CE2-CBI-CF-6OF8 CE3-CBI-CF-6OF8 CE4-CBI-CF-6OF8	27	Lognormal	7.1E-9 7.7E-7 2.9E-6	CCF specific 6 of 8 bistables
CPA	Analog core protection calculator	CE1-CPA-CF-T2OF3TM CE2-CPA-CF-T2OF3TM	7	Lognormal	4.9E-5 3.8E-4 1.2E-3	CCF 2 of 3 analog core protection calculators (T&M)

Table 3-2. (Continued)

Component Code	Component Type	Basic Event(s)	Number of CCF Events	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
		CE1-CPA-CF-T3OF4	7	Lognormal	1.3E-5	CCF 3 of 4 analog core protection
		CE2-CPA-CF-T3OF4			1.7E-4	calculators
					5.6E-4	
CPD	Digital core protection calculator	CE3-CPD-CF-T2OF3TM	9	Lognormal	2.3E-5	CCF 2 of 3 digital core protection
		CE4-CPD-CF-T2OF3TM			1.4E-4	calculators (T&M)
					3.8E-4	
		CE3-CPD-CF-T3OF4	9	Lognormal	6.3E-6	CCF 3 of 4 digital core protection
		CE4-CPD-CF-T3OF4			5.7E-5	calculators
					1.8E-4	
CPR	Pressure sensor/ transmitter	CE1-CPR-CF-P2OF3TM	6	Lognormal	3.0E-7	CCF 2 of 3 pressure sensor/ transmitters
		CE2-CPR-CF-P2OF3TM			5.0E-6	(T&M)
		CE3-CPR-CF-P2OF3TM			1.8E-5	
		CE4-CPR-CF-P2OF3TM				
		CE1-CPR-CF-P3OF4	6	Lognormal	4.0E-8	CCF 3 of 4 pressure sensor/ transmitters
		CE2-CPR-CF-P3OF4			1.5E-6	
		CE3-CPR-CF-P3OF4			5.8E-6	
		CE4-CPR-CF-P3OF4				
CTP	Temperature sensor/ transmitter	CE1-CTP-CF-C(H)T2OF3TM	10	Lognormal	8.0E-6	CCF 2 of 3 temperature sensor/ transmitters
		CE2-CTP-CF-C(H)T2OF3TM			3.7E-5	(T&M)
		CE3-CTP-CF-C(H)T2OF3TM			9.8E-5	
		CE4-CTP-CF-C(H)T2OF3TM				
		CE1-CTP-CF-C(H)T3OF4	10	Lognormal	7.5E-7	CCF 3 of 4 temperature sensor/ transmitters
		CE2-CTP-CF-C(H)T3OF4			1.0E-5	
		CE3-CTP-CF-C(H)T3OF4			3.5E-5	
		CE4-CTP-CF-C(H)T3OF4				
MSW [a]	Manual Trip Switch	CE2-MSW-CF-2OF4	0	Lognormal	7.4E-7	CCF specific 2 of 4 manual trip switches
		CE3-MSW-CF-2OF4			5.0E-6	
		CE4-MSW-CF-2OF4			1.5E-5	

Table 3-2. (Continued)

Component Code	Component Type	Basic Event(s)	Number of CCF Events	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
PWR	dc power	CE2-PWR-CF-TB2OF4	N/A	Lognormal	2.3E-7	CCF specific 2 of 4 trip breaker shunt trip device power
		CE3-PWR-CF-TB2OF4			2.5E-6	
		CE4-PWR-CF-TB2OF4			8.3E-6	
RMA (ROD and CRD) [a]	Control rod and associated control rod drive	CE1-ROD-CF-RODS	2	Lognormal	7.5E-10	CCF 50% (18 of 36) or more CRD/rods fail to insert
		CE2-ROD-CF-RODS			3.6E-8	
		CE3-ROD-CF-RODS			1.4E-7	
		CE4-ROD-CF-RODS				
RYL	Logic Relay	CE1-RYL-CF-LM6OF12TM	0	Lognormal	4.8E-9	CCF specific 6 of 12 logic relays (T&M)
		CE2-RYL-CF-LM6OF12TM			1.6E-7	
		CE3-RYL-CF-LM6OF12TM			6.0E-7	
		CE4-RYL-CF-LM6OF12TM				
		CE1-RYL-CF-LM12OF24	0	Lognormal	5.3E-10	CCF specific 12 of 24 logic relays
		CE2-RYL-CF-LM12OF24			4.3E-8	
		CE3-RYL-CF-LM12OF24			1.7E-7	
		CE4-RYL-CF-LM12OF24				
		CE1-RYL-CF-1,2,3,4LM3OF3TM	0	Lognormal	4.8E-9	CCF 3 of 3 logic relays (T&M)
		CE2-RYL-CF-1,2,3,4LM3OF3TM			4.7E-7	
		CE3-RYL-CF-1,2,3,4LM3OF3TM			1.8E-6	
		CE4-RYL-CF-1,2,3,4LM3OF3TM				
		CE1-RYL-CF-1,2,3,4LM6OF6	0	Lognormal	8.2E-10	CCF 6 of 6 logic relays
		CE2-RYL-CF-1,2,3,4LM6OF6			2.0E-7	
		CE3-RYL-CF-1,2,3,4LM6OF6			7.2E-7	
		CE4-RYL-CF-1,2,3,4LM6OF6				

Table 3-2. (Continued)

Component Code	Component Type	Basic Event(s)	Number of CCF Events	Distribution	Bayes 5%, Mean, 95%	Basic Event Description
RYT	Trip Relay	CE1-RYT-CF-TR2OF4	0	Lognormal	5.7E-7	CCF 2 of 4 trip relays
		CE2-RYT-CF-TR2OF4			4.8E-6	
		CE3-RYT-CF-TR2OF4			1.5E-5	
		CE4-RYT-CF-TR2OF4				

a. These CCF events were pooled with the same vendors and components as the independent events. See Table 3-1.

Table 3-3. Combustion Engineering RPS fault tree other basic events.

Basic Event	Distribution	Lower Bound, Mean, Upper Bound	Basic Event Description	Notes
CE1-RPS-TM-CHA CE2-RPS-TM-CHA CE3-RPS-TM-CHA CE4-RPS-TM-CHA	Uniform	0.0 1.6E-2 3.2E-2	Channel A through D bypassed because of testing or maintenance	Assumes 3 hours per monthly test (outages for each of the four channels combined into channel A). The upper bound assumes 6 hours.
CE1-XHE-XE-SCRAM CE2-XHE-XE-SCRAM CE3-XHE-XE-SCRAM CE4-XHE-XE-SCRAM	None	1.0 or 1.0E-2	Operator fails to manually actuate RPS	No credit is given for operator action for the base case quantification.
CE2,3-PWR-FF-TB15 CE2,3-PWR-FF-TB26 CE2,3-PWR-FF-TB37 CE2,3-PWR-FF-TB48	Lognormal	2.3E-6 6.0E-5 2.3E-4	TCB-1, TCB-5 Shunt Trip Device DC Power Fails TCB-2, TCB-6 Shunt Trip Device DC Power Fails TCB-3, TCB-7 Shunt Trip Device DC Power Fails TCB-4, TCB-8 Shunt Trip Device DC Power Fails	125 Vdc power to the shunt trip fails (1.0E-5/h * 6h repair time)[a]
CE4-PWR-FF-TB1 CE4-PWR-FF-TB2 CE4-PWR-FF-TB3 CE4-PWR-FF-TB4	Lognormal	2.3E-6 6.0E-5 2.3E-4	TCB-1 Shunt Trip Device DC Power Fails TCB-2 Shunt Trip Device DC Power Fails TCB-3 Shunt Trip Device DC Power Fails TCB-4 Shunt Trip Device DC Power Fails	125 Vdc power to the shunt trip fails (1.0E-5/h * 6h repair time)[a]

a. Power failure data were not analyzed as part of this study. The failure rate per hour was obtained from Reference 11 (Table 4, p. 23). The six-hour repair time was estimated from the reactor trip breaker maintenance duration in Reference 12.

Using the RPS basic event mean probabilities presented in Table 3-1 through Table 3-3, the Combustion Engineering RPS mean unavailability (failure probability upon demand) is shown as the Total Group RPS in Table 3-4 with and without operator action to manually trip. The cut sets from the RPS fault tree quantification performed using SAPHIRE are presented in Appendix F. Basic event importance rankings are also presented in Appendix F. The dominant failures for the Combustion Engineering RPS design involve CCFs of the trip relays (K-1 through K-4, Groups 2, 3, and 4 or M-1 through M-4 Group 1) and the mechanical portion of the breaker (except Group 1). The rods, channel, and trip module segments each have a small, but measurable contribution. The RPS fault tree was also quantified, allowing credit for manual trip by the operator (with a failure probability of 0.01). If the model takes credit for manual trip by the operator, then the contribution of the channel trip unit CCFs are significantly reduced. Operator action reduces the RPS unavailability by approximately 13 percent (Group 1), to 75 percent (Groups 2 and 3), to 78 percent (Group 4).

Table 3-4. Combustion Engineering RPS segment contribution.

	Unavailability (Point Estimate) with No Credit for Manual Scram by Operator		**Unavailability (Point Estimate) with Credit for Manual Scram by Operator**	
RPS Segment	**Percent**	**Unavailability**	**Percent**	**Unavailability**
		Group 1 RPS Model		
Channel	12.0%	7.8E-07	0.1%	7.8E-09
Trip Modules	0.7%	4.5E-08	0.0%	4.2E-10
Trip Contactors	74.4%	4.8E-06	85.1%	4.8E-06
Rods	12.9%	8.4E-07	14.8%	8.4E-07
Total Group 1 RPS	100.0%	6.5E-06	100.0%	5.7E-06
		Group 2 RPS Model		
Channel	10.4%	7.8E-07	0.4%	7.5E-09
Trip Modules	0.6%	4.5E-08	0.2%	2.9E-09
Trip Breakers/Trip Relays	77.9%	5.8E-06	55.2%	1.0E-06
Rods	11.2%	8.4E-07	44.2%	8.4E-07
Total Group 2 RPS	100.0%	7.5E-06	100.0%	1.9E-06
		Group 3 RPS Model		
Channel	10.4%	7.8E-07	0.4%	7.5E-09
Trip Modules	0.6%	4.5E-08	0.2%	2.9E-09
Trip Breakers/Trip Relays	77.9%	5.8E-06	55.2%	1.0E-06
Rods	11.2%	8.4E-07	44.2%	8.4E-07
Total Group 3 RPS	100.0%	7.5E-06	100.0%	1.9E-06
		Group 4 RPS Model		
Channel	10.8%	7.8E-07	0.5%	7.5E-09
Trip Modules	0.6%	4.2E-08	0.0%	4.2E-10
Trip Breakers/Trip Relays	77.0%	5.6E-06	47.2%	7.6E-07
Rods	11.6%	8.4E-07	52.3%	8.4E-07
Total Group 4 RPS	100.0%	7.2E-06	100.0%	1.6E-06

The small reduction in unavailability by operator action for Group 1 is because of the point at which the manual trip enters the logic. In Group 1, the manual trip removes coil power to the M relays (see Figure 2-4). This leaves the trip contactor (M relays) event at the top of the cutset listing. In Groups 2, 3, and 4, the manual trip bypasses the K relays and directly initiates the trip breakers (see Figure 2-5).

Table 3-4 summarizes the RPS segment (channel, trip module, trip breaker/trip contactors, and rods) contributions to the overall demand unavailability. The trip breakers and trip contactors are the dominant segments in all models.

To quantify the exact difference between the two breaker configurations, a sensitivity study was performed. The results of this study are shown in Appendix G, Section G-3. The four-trip-breaker configuration is about 41 percent (7.1E-7 versus 1.0E-6) more reliable than the eight-trip-breaker configuration based on an analysis of the fault trees. This is due to the presence of more valid combinations of trip breaker failures in the eight-trip-breaker configuration that will not de-energize the control rod clutches.

Another way to segment the Combustion Engineering RPS unavailability is to identify the percentage of the total unavailability contributed by independent failures versus CCF events. Such a breakdown is not exact, because RPS cut sets can include combinations of independent failures and CCF events. However, if one splits cut sets with CCF events and independent events, then the breakdown can show the contribution of independent events to the overall unavailability. The results are presented in Table 3-5. The CCF contribution is between 99.5 and 99.6 percent for the case with no operator action and between 99.5 and greater than 99.9 percent when operator action is included.

Table 3-5. Combustion Engineering RPS failure contributions (CCF and independent failures).

	No Credit for Manual Scram by Operator		Credit for Manual Scram by Operator	
RPS Segment	**Contribution from CCF Events**	**Contribution from Independent Failures**	**Contribution from CCF Events**	**Contribution from Independent Failures**
		Group 1 RPS Model		
Channel	12.0%	<0.1%	0.1%	<0.1%
Trip Modules	0.7%	<0.1%	0.0%	<0.1%
Trip Contactors	74.0%	0.4%	84.6%	0.5%
Rods	12.9%	<0.1%	14.8%	<0.1%
Total Group 1	99.6%	0.4%	99.5%	0.5%
		Group 2 RPS Model		
Channel	10.4%	<0.1%	0.4%	<0.1%
Trip Modules	0.6%	<0.1%	0.2%	<0.1%
Trip Breakers/Trip Relays	77.2%	0.6%	55.2%	0.1%
Rods	11.2%	<0.1%	44.2%	<0.1%
Total Group 2	99.4%	0.6%	99.9%	0.1%
		Group 3 RPS Model		
Channel	10.4%	<0.1%	0.4%	<0.1%
Trip Modules	0.6%	<0.1%	0.2%	<0.1%
Trip Breakers/Trip Relays	77.2%	0.6%	55.2%	0.1%
Rods	11.2%	<0.1%	44.2%	<0.1%
Total Group 3	99.4%	0.6%	99.9%	0.1%
		Group 4 RPS Model		
Channel	10.8%	<0.1%	0.5%	<0.1%
Trip Modules	0.6%	<0.1%	0.0%	<0.1%
Trip Breakers/Trip Relays	76.4%	0.6%	47.2%	<0.1%
Rods	11.6%	<0.1%	52.3%	<0.1%
Total Group 4	99.4%	0.6%	>99.9%	<0.1%

Sensitivity analyses were performed on the RPS fault tree quantification results. These sensitivity analyses are discussed in Appendix G of this report.

3.2.2 Fault Tree Uncertainty Analysis

An uncertainty analysis was performed on the Combustion Engineering RPS fault tree cut sets listed in Appendix F using the SAPHIRE code. To perform the analysis, uncertainty distributions for each of the fault tree basic events are required. The uncertainty distributions for the basic events involving independent failures of RPS components were obtained from the data statistical analysis presented in Appendix C. The component demand failure probabilities were modeled by lognormal distributions.

Uncertainty distributions for the CCF basic events required additional calculations. Each CCF basic event is represented by an equation involving the component total failure probability, Q_T, and the CCF α's and their coefficients. See Appendix E for details. The uncertainty distributions for Q_T were obtained from the statistical analysis results in Appendix C. Uncertainty distributions for the component-specific α's were obtained from the methodology discussed in Appendix E. Each of the α's was assumed to have a beta distribution. The uncertainty distributions for each CCF basic event equation were then evaluated and fit to lognormal distributions. This information was then input to the SAPHIRE calculations. The results of the uncertainty analysis of the Combustion Engineering RPS fault tree model are shown in Table 3-6.

Table 3-6. Combustion Engineering fault tree model results with uncertainty.

	5%	Median	Mean	95%
Group 1 RPS Model				
No credit for manual trip by operator	1.2E-6	4.4E-6	6.5E-6	1.8E-5
Credit for manual trip by operator	8.8E-7	3.7E-6	5.7E-6	1.7E-5
Group 2 RPS Model				
No credit for manual trip by operator	1.9E-6	5.5E-6	7.5E-6	1.9E-5
Credit for manual trip by operator	3.9E-7	1.3E-6	1.9E-6	5.1E-6
Group 3 RPS Model				
No credit for manual trip by operator	1.9E-6	5.5E-6	7.5E-6	1.9E-5
Credit for manual trip by operator	3.9E-7	1.3E-6	1.9E-6	5.1E-6
Group 4 RPS Model				
No credit for manual trip by operator	1.6E-6	5.1E-6	7.2E-6	1.9E-5
Credit for manual trip by operator	2.4E-7	9.5E-7	1.6E-6	4.7E-6

Note: These results were obtained using a Latin Hypercube simulation with 10,000 samples.

3.3 Comparison with PRAs and Other Sources

Similar to the approaches used in this study, RPS unavailability has been estimated previously from overall system data or from data for individual components within the system. The component approach requires a logic model such as a fault tree to relate component performance to overall system

performance. This section summarizes early RPS unavailability estimates using both methods and more recent PWR (Combustion Engineering) IPE estimates.

WASH-1270, published in 1973, estimated the RPS unavailability to be 6.9E-5 (median), based on two RPS failures (N-Reactor and German Kahl reactor events) in 1627 reactor-years of operation. Of this combined experience, approximately 1000 reactor years were from naval reactors. The Electric Power Research Institute (EPRI) ATWS study in 1976 estimated the RPS unavailability to be 7.0E-7 (median), based on no failures in 110,000 reactor trips (75,000 of these were naval reactor trips).[13] Finally, NUREG-0460[1] in 1978 estimated the RPS unavailability to be 1.1E-4 (median), based on one failure (German Kahl reactor event) in approximately 700 reactor-years. However, that document recommended a value of 3E-5 to account for expected improvements in design and operation, with 1E-5 from the mechanical (rod) portion of the RPS and 2E-5 from the electrical (signal) portion of the RPS. Therefore, early RPS unavailabilities based on system level data ranged from 7.0E-7 (median) to 1.1E-4 (median), depending upon the types of nuclear reactor experience included and the inclusion or exclusion of RPS failure events.

An early RPS unavailability estimate using component data and fault tree logic models is contained in WASH-1400. WASH-1400 estimated the RPS unavailability to be 1.3E-5 (median). The dominant contributors were rod failures (three or more control rods failing to insert was considered a RPS failure) and channel switch failures. The RPS model used in this report assumed 7 or more of 36 safety group shutdown rods must fail to insert in order to fail to achieve a hot shutdown state, which is a less conservative failure criterion. This is one reason why the RPS unavailability presented in this report is much lower than the WASH-1400 result.

Also, Combustion Engineering in 1986 analyzed the channel and trip system portion of the RPS (excluding the CRD and control rod portions) and obtained RPS mean unavailabilities from 1.3E-7 to 3.3E-6.[14] A summary of the results based on the 30-day testing period is shown in Table 3-7. These results do not include an operator action event to trip the reactor.

Table 3-7. Combustion Engineering calculated unavailabilities from CEN-327-A.[14]

Group	Single Trip Parameter Unavailability (TM/LP or DNBR 30-day test interval)
1	1.3E-7
2	3.3E-6
3	3.3E-6
4	2.6E-6

The Combustion Engineering study[14] did not include the CRD and control rod portions of the RPS, which contribute 11.2 to 12.9 percent to the RPS unavailability in the present study.

Finally, RPS unavailability estimates from the PWR IPEs are presented in Table 3-8. The RPS unavailability estimates range from 1.0E-5 (mean) to 3.7E-6 (mean). Details concerning modeling and quantification of RPS unreliability in these IPEs are generally limited. Figure 3-1 shows the Combustion Engineering RPS unavailability distributions obtained in this study compared to the IPE results. This studies' RPS unavailability estimates, with no operator action, lie below the reported Combustion Engineering IPE unavailability estimates except for the Calvert Cliffs IPE estimate. The estimates with operator action are lower than the IPEs for Combustion Engineering RPS Groups 2, 3, and 4 and lie within the IPEs range of values for Combustion Engineering RPS Group 1. It is not clear whether the

Combustion Engineering IPE estimates include an operator action to trip the reactor, except for Arkansas Unit 2, which has an operator error value of 0.5.

When comparing the IPE results to the results presented in this study, several items should be considered. The IPE models are not as detailed as the model in this study. CCF is insufficiently treated in each of the IPEs. When CCF is considered, it is not based on observed failure data. The rod failure criteria is conservatively estimated or not defined. Despite these differences, the reported values are within an order of magnitude of this study's result.

Table 3-8. Summary of plant review for Combustion Engineering RPS unavailability values.

PLANT	IPE/PRA RPS Unavailability	Notes
Arkansas 2[15]	1.0E-5 (mechanical) 1.0E-6 (electrical)	A RPS fault tree is not provided in the IPE. The RPS unavailability has been separated into two categories; electrical and mechanical. The RPS electrical failure unavailability used in the IPE is 1.0E-6. This estimate is based on a predicted electrical failure probability of 2.0E-6 times 0.5 for operator recovery. The mechanical failure to scram in the IPE is defined as the inability of the control rods to physically drop into the core due to sticking. Based on other PRA studies, the probability of mechanical failure is estimated to be 1.0E-5.
Calvert Cliffs Units 1 & 2[16]	3.66E-6	RPS is represented in the model as split fractions. A RPS description is provided in the IPE, but a detailed model of the RPS is not provided.
Fort Calhoun Unit 1[17]	1.0E-5 (mechanical) 1.04E-6 (signal) 1.3E-6 (fail to remove relay jumpers prior to power escalation)	The IPE does describe the RPS and provides a simplified RPS fault tree. The top gate is Failure to Scram Reactor with basically three inputs: mechanical failure, RPS signal failure, and a failure to remove RPS interposing relay jumpers prior to power operation. Mechanical failure is the failure of two or more control element assemblies to drop.
Maine Yankee[18]	1.0E-5	The IPE does describe the RPS system, which states that "Several previous PRAs throughout the industry have shown that RPS failures are not significant contributors to plant risks nor significant contributors to failure to trip the reactor." The IPE also states that "The Maine Yankee RPS is a fairly typical Combustion Engineering two-out-of-four, 'fail safe' system. Plant history does not reveal any unique problems. For these reasons, the PRA will not model the RPS; it is assumed to be insignificant to risk." However, the ATWS sequences state the scram failure probability to be 1.0E-5.
Millstone Unit 2[19]	1.0E-5	The IPE has a reactor trip (RT) event in the event tree and the value used for the RT event is 1.0E-5. The IPE does not describe in detail the RT event or the RPS.
Palisades[20]	NA	The IPE does not describe the RPS, but an electrical reactor trip failure (RXE) and a mechanical reactor trip failure (RXM) are discussed for the ATWS sequences. However, the IPE does not provide values for these two top events.
Palo Verde Unit 1, 2, & 3[21]	NA	Although the RPS discusses the IPE, a system fault tree or RPS unavailability was not provided in the IPE.
San Onofre Units 2 & 3[22]	1.0E-5 (mechanical)	The IPE provides a description and figure for the RPS, but an RPS fault tree or results are not provided. However, a basic event importance measure report is provided, and a basic event for a mechanical failure of the RPS to scram is listed. The value of the basic event is 1.0E-5.

Table 3-8. (Continued)

PLANT	IPE/PRA RPS Unavailability	Notes
St. Lucie Units 1 & 2[23]	NA	The IPE does not describe the RPS, but the function of the RPS is discussed and a partial fault tree is provided for the top event "Failure of making Reactor Subcritical Using Rods." Mechanical and electrical failures are represented, but the top event unavailability or basic event values are not given in the IPE.
Waterford 3[24]	NA	The IPE does not describe the RPS, and a RPS unavailability is not given.

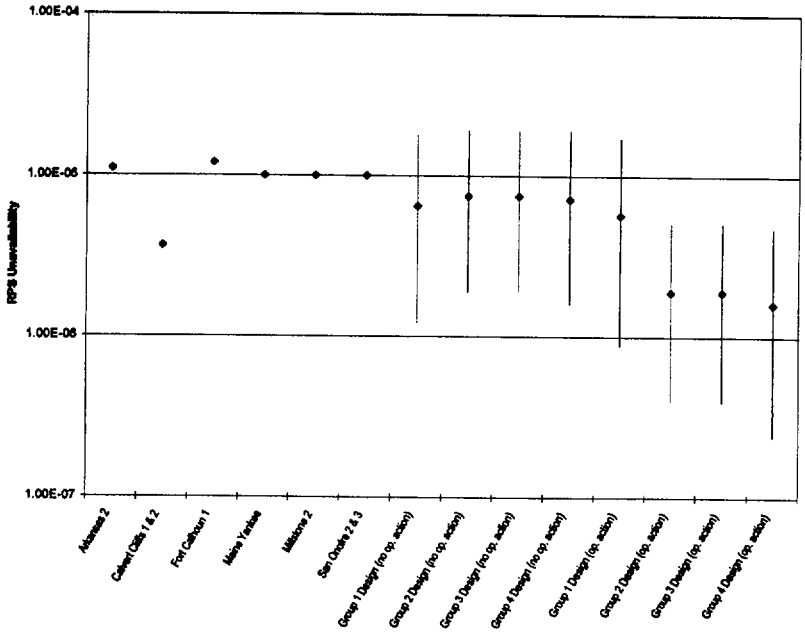


Figure 3-1. Combustion Engineering IPE and RPS Study RPS unavailabilities.[1]

3.4 Regulatory Implications

The regulatory history of the RPS can be divided into two distinct areas: general ATWS concerns, and RPS component or segment issues. The general ATWS concerns are covered in NUREG-0460, SECY-83-293,[25] and 10 CFR 50.62. NUREG-0460 outlined the U.S. NRC's concerns about the potential for ATWS events at U.S. commercial nuclear power plants. That document proposed several alternatives for commercial plants to implement in order to reduce the frequency and consequences of ATWS events. SECY-83-293 included the proposed final ATWS rule, while 10 CFR 50.62 is the final ATWS rule. In those three documents, the assumed Combustion Engineering RPS unavailabilities ranged from 1.5E-5 to 6.0E-5. The Combustion Engineering RPS unavailabilities obtained in this report ranged from 6.5E-6 to 7.5E-6, with no credit for manual trip by the operator. These values are slightly lower than the values

[1] The range shown is the 5th and 95th percentiles. All other data points are mean values.

used in the development of the ATWS rule. Because this study did not analyze RPS data from the late 1970s and early 1980s, it is not known what RPS unavailability estimate would have been obtained by this type of study for the ATWS rulemaking period.

With respect to RPS components or segments, issues were identified from the document review discussed previously: reactor trip breaker unavailability and channel test intervals. The reactor trip breaker unavailability issue arose from the Salem low-power ATWS events in 1983. The issue is discussed in detail in NUREG-1000. Recommendations resulting from this issue included better breaker testing and maintenance programs, and automatic actuation of the shunt trip coil. (The Salem ATWS events would not have occurred if the shunt trip coils had automatically actuated from the reactor trip signals.) Using Westinghouse reactor trip breaker (DB-50 and DS-416 designs) data through 1982, the breaker unavailability was determined to be 4E-3. In addition, SECY-83-293 indicated a CCF (two reactor trip breakers) unavailability of 2E-4 without automatic actuation of the shunt trip coils and 5E-5 with automatic actuation. The corresponding unavailabilities based on the component failure probabilities used in this study are 1.8E-5 for a reactor trip breaker (undervoltage coil and shunt trip failure, or mechanical failure) and 1.2E-6 for CCF of two of four breakers (undervoltage coil and shunt trip failure, or mechanical failure). Both of the study results are significantly lower than the 1983 document values. Therefore, the observed reactor trip breaker performance has improved considerably since 1983.

In 1989, Combustion Engineering obtained approval to change RPS channel testing procedures.[26] The approval recommended a change of the channel test interval from one month to six months (using a staggered testing scheme). In addition, during testing the channel could be placed in the bypass mode, rather than the tripped mode. Both of these changes have the potential to increase the unavailability of the RPS. The base case (no operator action) RPS results, obtained with only two trip signals modeled, indicate that the channels contributed between 10.4 and 12.0 percent to the overall RPS unavailability. In addition, a sensitivity analysis presented in Appendix G indicates that if three trip signals had been modeled, the channel contribution would have dropped to between 4.3 and 5.0 percent. Because at least three trip signals are expected for almost all plant upset conditions requiring a reactor trip, the 4.3 to 5.0 percent contributions from channels is considered more appropriate.

4. ENGINEERING ANALYSIS OF THE OPERATIONAL DATA

This section presents an analysis of trends based on overall system performance, total component performance, and CCF component performance. Section A-3 presents the methodology for evaluating the trends.

4.1 System Evaluation

At a system level, the change in RPS performance over time can be roughly characterized by examining the trends with time of component failures and CCFs. A review of the component independent failure counts in Table B-1 of Appendix B indicates a drop in RPS component failures, from a high of 44 failures in 1988 to a low of 11 in 1994. In addition, a review of CCF counts in Table B-2 of Appendix B indicates a high of 16 CCF events in 1985 to a low of one CCF event in 1988, 1991, and 1994. Detailed analyses of trends with time for component failure probabilities and CCFs, presented in Sections 4.2 and 4.3, respectively, indicate decreasing trends in events that dominate the RPS unavailability.

As indicated in Section 3.1, there were no RPS failures during 1984 through 1995. This also implies that there were no complete failures of the RPS trip system.

No complete channel failures during unplanned reactor trips were identified during the review of the RPS data. However, because of the complexity and diversity of RPS channels and the uncertainty in determining associated trip signals, it is difficult to determine whether an entire channel failed during an unplanned reactor trip. Therefore, it is possible that some complete channel failures have occurred and were not identified as such in the data review.

Since unplanned reactor trips are reported in LERs, data from the full study period are available for the study of demands on the RPS system. The data were examined for a trend over the time frame spanned by this study. However, the reactor trip count among CE plants for 1984 was unusually high (approximately 25 scrams per plant), so 1984 data were omitted from this analysis. Data for the remaining years are shown in Figure 4-1. A single trend line does not fully represent these data, particularly before and after 1988, and the data could be analyzed in two or three groupings on the time axis. However, the purpose of the current assessment is just to see whether a decreasing trend exists, and the plot shows this clearly. The rate of demands among Combustion Engineering plants has decreased since the middle 1980s, even with the exclusion of 1984 data. This trend is similar to the trend among Westinghouse, Babcock & Wilcox, and General Electric plants.

4.2 Component Evaluation

Over 1600 LER and NPRDS records were reviewed for the Combustion Engineering RPS study. Data analysts classified these events into the nine bins shown in Table 2-7 in Section 2. The highlighted NFS/CF bin contains events involving complete failure of the component's safety function of concern. The other three highlighted bins contain events that may be NFS/CF, but insufficient information prevented the data analysts from classifying the events as NFS/CF. (In the quantification of RPS unavailability discussed in Section 3, a fraction of the events in the three bins was considered to be NFS/CF and was added to the events already in the NFS/CF bin.) Combustion Engineering RPS component failure data used in this study are summarized in Table B-1 in Appendix B (independent failures only) and Table C-1 in Appendix C (independent and CCF events).

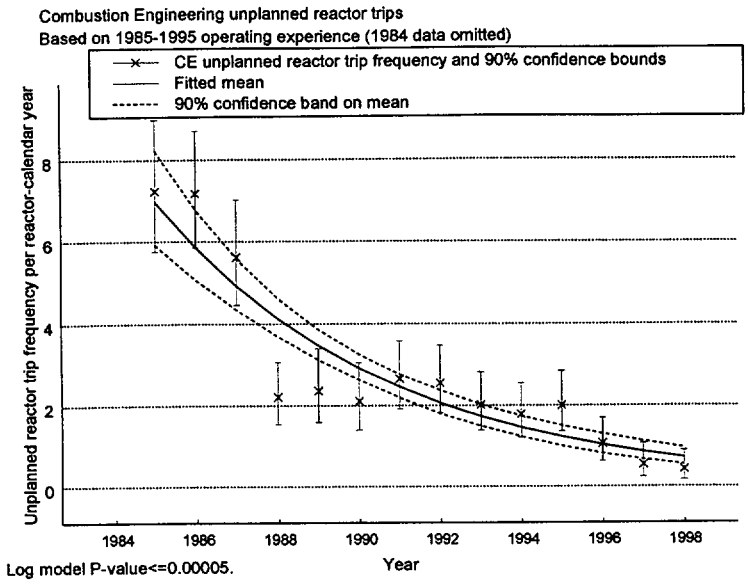


Figure 4-1. Trend analysis for Combustion Engineering unplanned reactor trips, per plant operating year, from 1985 to 1998.

Evaluations were performed for the overall frequency of component failure for each of the components used in the unavailability analysis and modeled from the failure data. The evaluations considered failures without regard to the method of detection. Two primary cases were analyzed for each component, one using all complete losses of a component's RPS safety function, and one that included the upper bound case of counting partial failures (with an assessed 0.5 probability of being complete) and counting failures that might have involved loss of a component's RPS safety function:

Failure data from tests on each component that did not involve a loss of a train or channel are not in general reportable for LERs but are seen in NPRDS data. However, the NPRDS data system stopped at the end of 1996, and the completeness of plant reporting during 1996 is not known. Therefore, an adequate new test data set for 1996-1998 was not available for this study. The trend analysis for these Combustion Engineering components was therefore restricted to 1984–1995.

Figure 4-2 shows the total Combustion Engineering failure count for this period, normalized by the number of reactor-calendar years in the period. An overall decreasing trend in these failures was evident in the data, with a statistically significant[2] p-value[3] (less than 0.00005). A decreasing trend remains significant; even when the uncertain failures are omitted (p-value less than 0.00005).

The individual component failure frequencies, computed from the failure counts and the number of components in the Combustion Engineering plants in each year from 1984 to 1995, were also evaluated for trends. Significant trends were seen for digital core protection calculators (p-value 0.0003), bistables (p-value 0.0003), logic relays (p-value 0.003), temperature sensor/transmitters (p-value 0.003), breaker

[2] The term "statistically significant" means that the data are too closely correlated to be attributed to chances and consequently have a systematic relationship.

[3] A p-value is a probability, with a value between zero and one, that is a measure of statistical significance. The smaller the p-value, the greater the significance. A p-value of less than 0.05 is generally considered to be statistically significant.

undervoltage devices (p-value 0.046), and the pressure sensor/transmitters (p-value 0.046) (see Figure 4-3 through Figure 4-8). All trends were significant both with and without the uncertain failures.

A final Combustion Engineering failure frequency evaluation was performed that considered the entire study period (1984–1998). Since only LER data were available during the 1996–1998 period, this entire study was restricted to events for which an LER number was available. As Figure 4-9 shows, the overall failure frequencies were too sparse to observe trends in this data set (p-value 0.31). For the twelve Combustion Engineering components evaluated for the unavailability analysis, just five complete losses of the components' safety-function and eight uncertain failures were reported in the LERs. The component-specific LER-reported failure frequencies were even sparser and showed no trends.

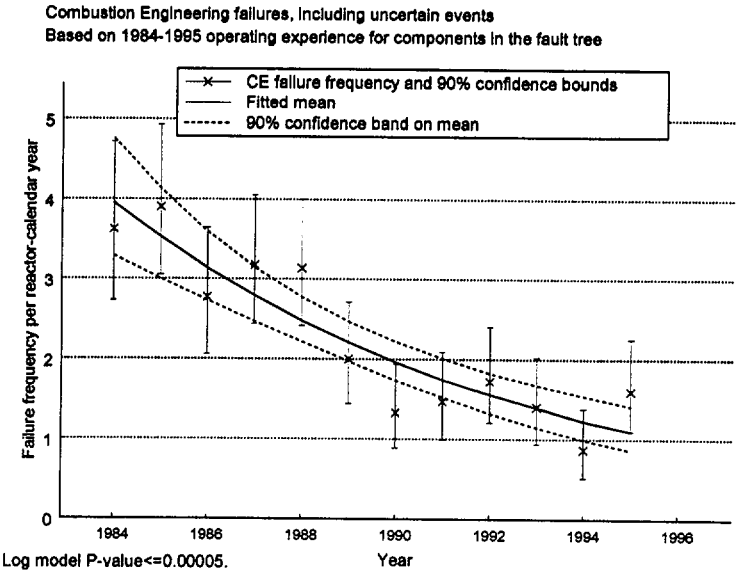


Figure 4-2. Trend analysis for frequency of Combustion Engineering failures of components in unavailability analysis, per plant year, including uncertain failures.

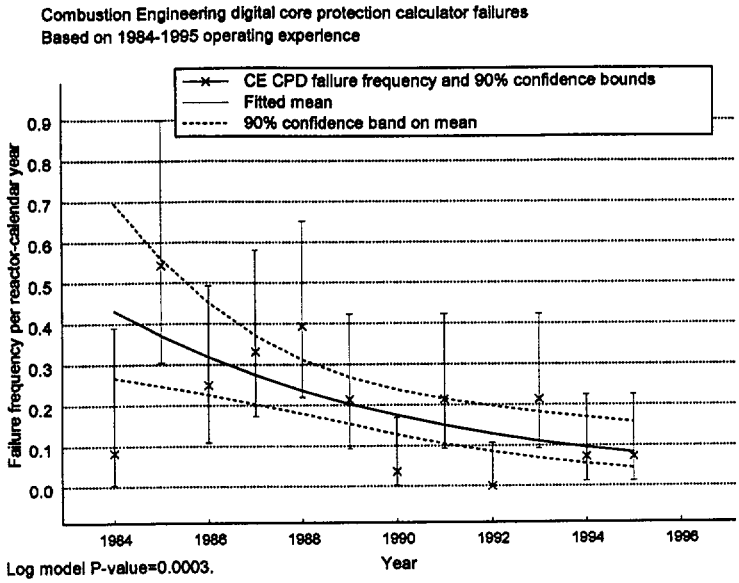


Figure 4-3. Trend analysis for frequency of Combustion Engineering digital core protection calculator failures, including uncertain failures.

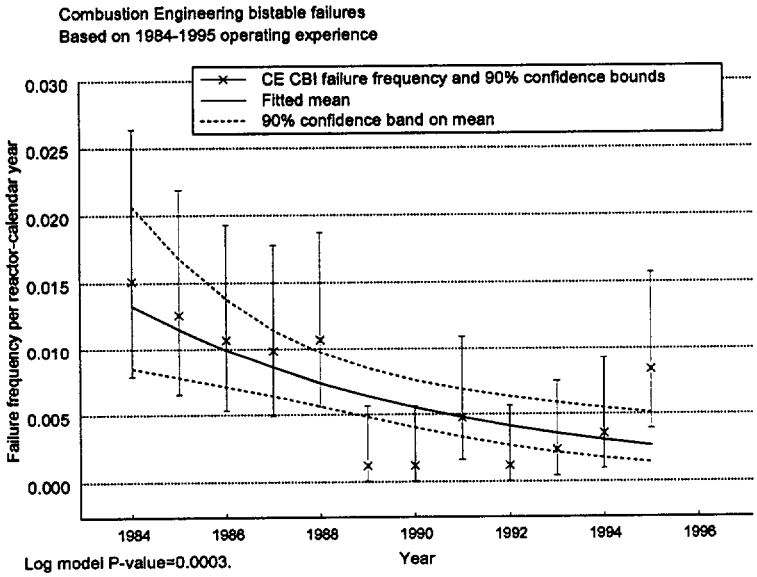


Figure 4-4. Trend analysis for the Combustion Engineering bistable failure frequency.

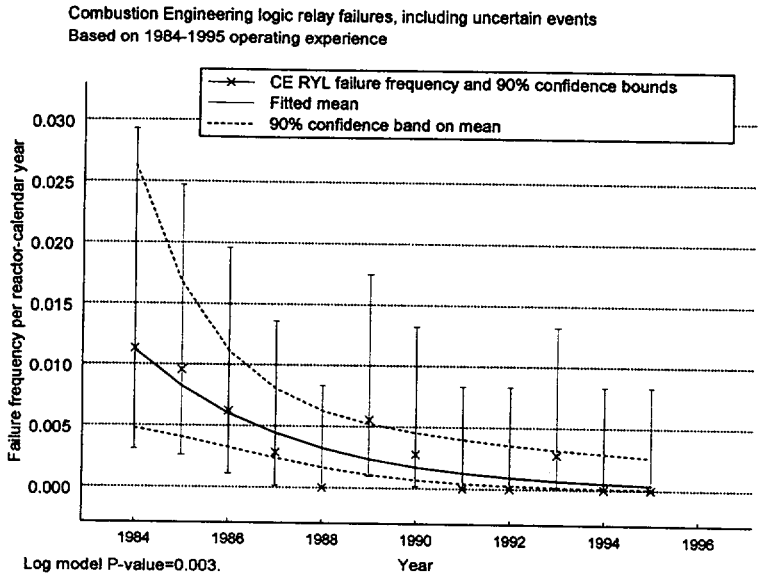


Figure 4-5. Trend analysis for the Combustion Engineering logic relay failure frequency.

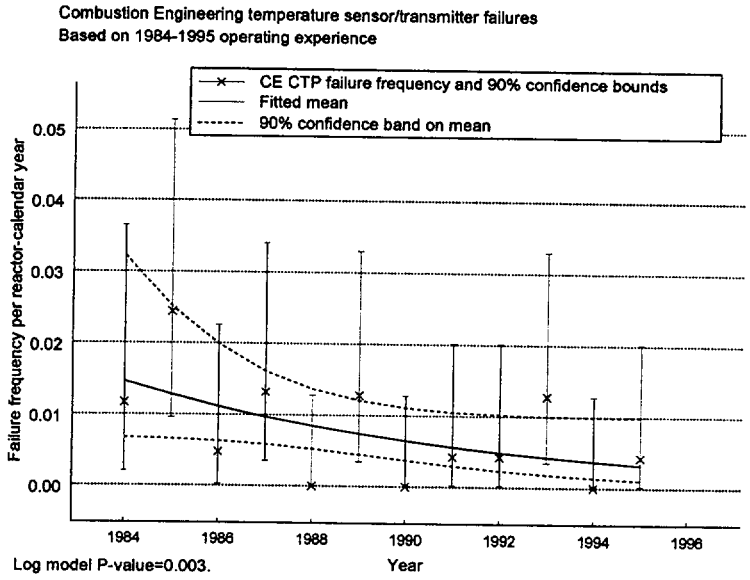


Figure 4-6. Trend analysis for the Combustion Engineering temperature sensor/transmitter failure frequency.

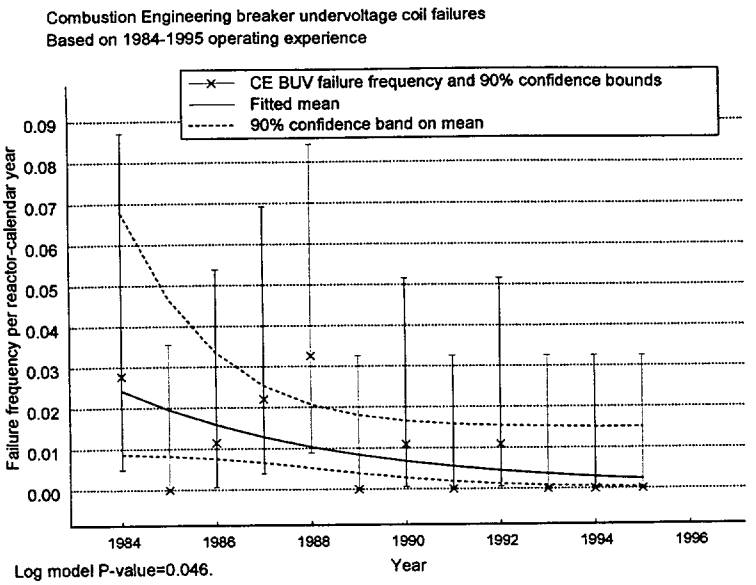


Figure 4-7. Trend analysis for the Combustion Engineering breaker undervoltage coil failure frequency.

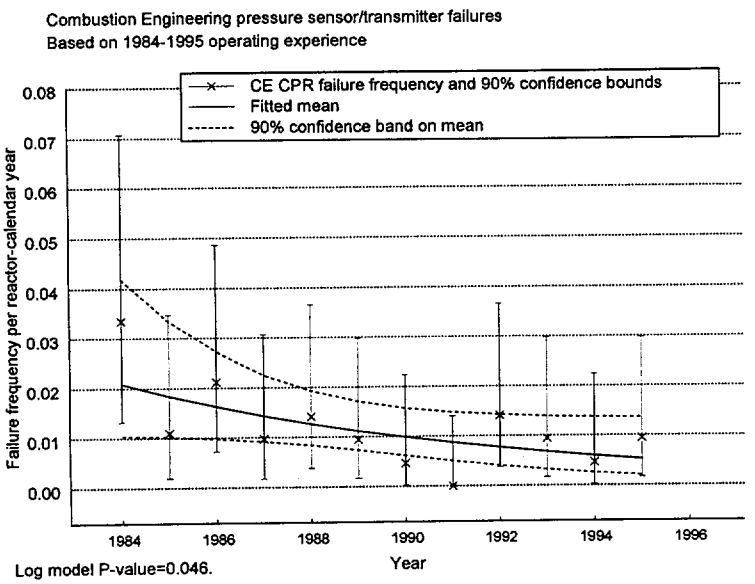


Figure 4-8. Trend analysis for the Combustion Engineering pressure sensor/transmitter failure frequency.

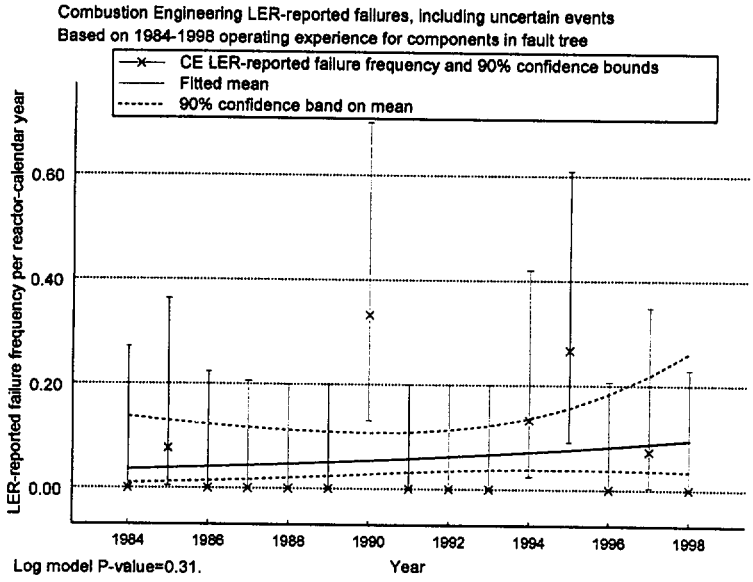


Figure 4-9. Trend analysis for frequency of LER-reported failures of Combustion Engineering components in the data analysis, per plant year, including uncertain failures.

4.3 Common-Cause Failure Evaluation

The Combustion Engineering RPS CCF data involve CCF and potential CCF events. A complete CCF event involves failure (degradation factor of 1.0) of each of the components in the common-cause component group, with additional factors such as shared cause and timing assigned values of 1.0. (See Appendices B and E for additional discussions of the CCF model and failure degradation and other factors.) Other CCF events involve failure of several (but not all) of the components in the common-cause component group. Finally, potential CCFs involve events in which one or more of the degradation or other factors has a value of less than 1.0.

Combustion Engineering RPS CCF data are summarized in Tables B-2 and B-3 in Appendix B. There were no observed complete CCF failures of the RPS components modeled in this study. Sixty-five potential CCF events were identified for the period 1984 through 1998.

The following is a list of the more interesting CCF events found at Combustion Engineering plants:

- Incomplete restoration from a test left the shunt trip leads removed from half of the RTBs.

- Four times over a 5-year period, the coils of bistable trip unit dual coil relays shorted together, causing current to be added to the measurement loop. The first time it occurred, three of the bistables were affected. The second time, eleven bistables were affected. The third and fourth time, two bistables were affected. These appeared to be caused by a breakdown of properties associated with normal degradation related to hours of service.

- Over a 3-day period, three of four core protection calculator/control element assembly controller channels had memory parity errors, caused by faulty memory boards. One of the failure records indicated that the memory board had been installed just 2 days prior.

Following are comments on the general findings over all the RPS studies. The vast majority (80 percent) of RPS CCF events can be attributed to either normal wear or out-of-specification failure reports. These events fall into the potential CCF event category and do not appreciably contribute to the calculated CCF basic event probabilities. Design and manufacturing causes led to the next highest category (7 percent) and human errors (operations, maintenance, and procedures) were the next highest category (6 percent). Environmental problems and the state of other components (e.g., power supplies) led to the remaining RPS CCF events. No evidence was found that these proportions are changing over time.

The detection of failures of components in this study either was by testing or by observation with a small majority detected by testing. Very few failures were detected by trip demands. No change in the overall distribution of detection is apparent.

The most subtle CCF mechanisms are the design modifications and the procedures. These two mechanisms have the highest potential to completely fail all components in the common-cause component group (e.g., modification to all four containment pressure transmitters that prevented a high containment pressure trip, or a calibration procedure that gives an incorrect calibration parameter). While neither of these events occurred at a Combustion Engineering plant, the mechanisms are generic enough to apply to all vendor designs.

4.3.1 CCF Event Trends

Figure 4-10 shows the Combustion Engineering CCF event frequency plotted based on the year when each event occurred. A decreasing trend was observed for the 65 events (p-value less than 0.00005). As shown in Figure 4-11 through Figure 4-13, the trend was also seen in CCF events for temperature transmitter/sensors (p-value 0.008), digital core protection calculators (p-value 0.005), and bistables (p-value 0.0008).

To form a starting point for assessing the Combustion Engineering operational data, the CCF evaluation in this study used the pattern of CCF failures shown by the set of all PWR CCF events that occurred in the component types in the Combustion Engineering model. Figure 4-14 shows the significant decreasing trend in the overall PWR CCF event frequency (p-value less than 0.00005).

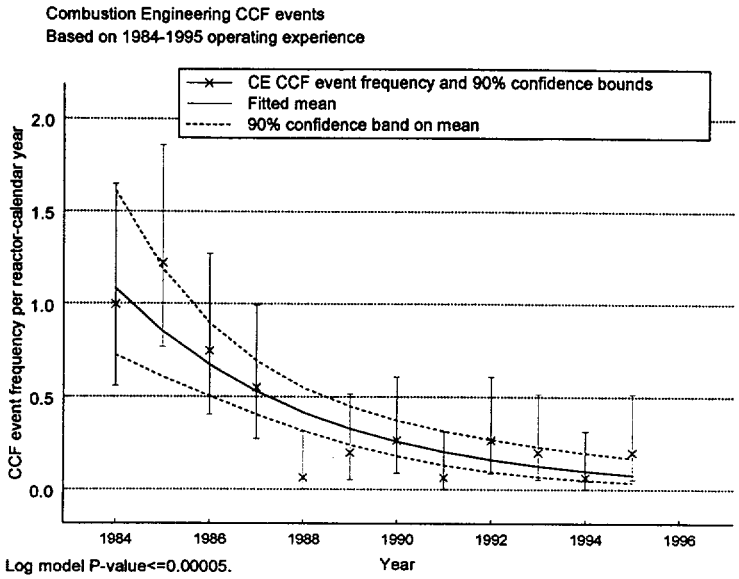


Figure 4-10. Trend analysis for Combustion Engineering CCF events per plant calendar year.

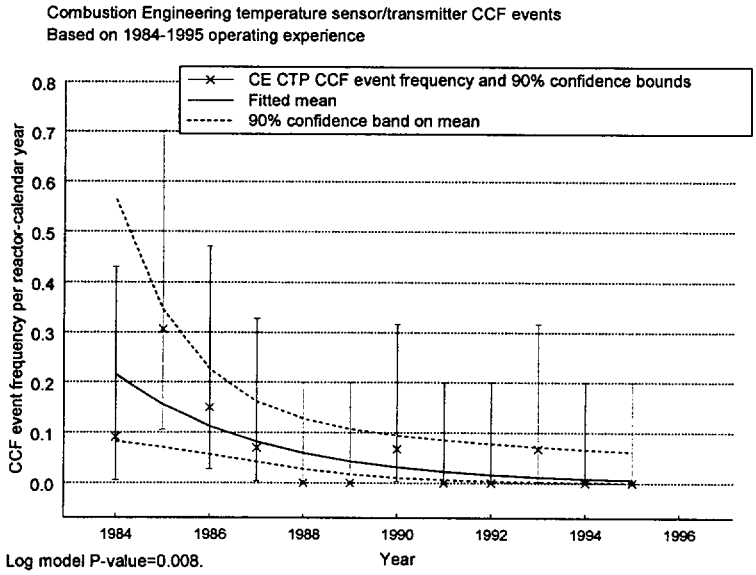


Figure 4-11. Trend analysis for Combustion Engineering temperature sensor/transmitter CCF events.

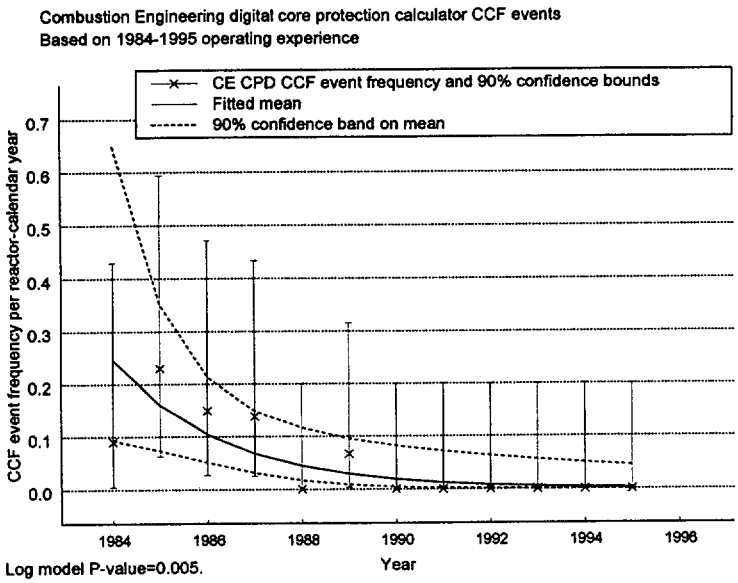


Figure 4-12. Trend analysis for Combustion Engineering digital core protection calculator CCF events.

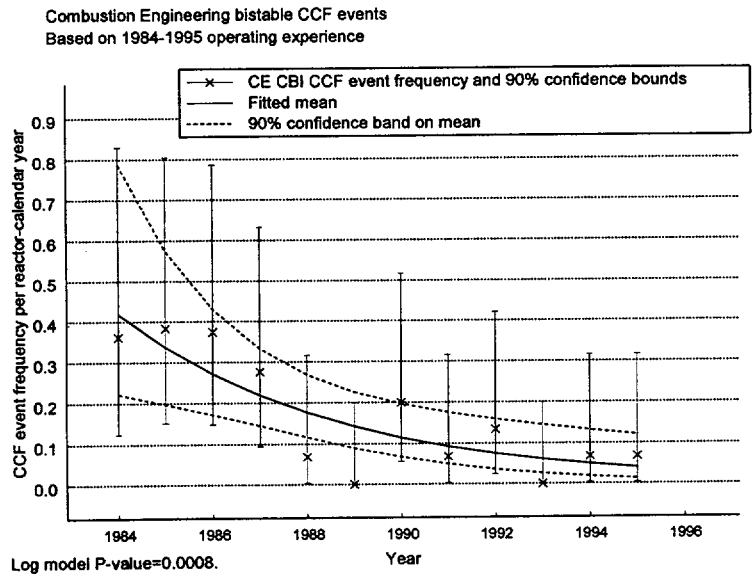


Figure 4-13. Trend analysis for Combustion Engineering CCF bistable events.

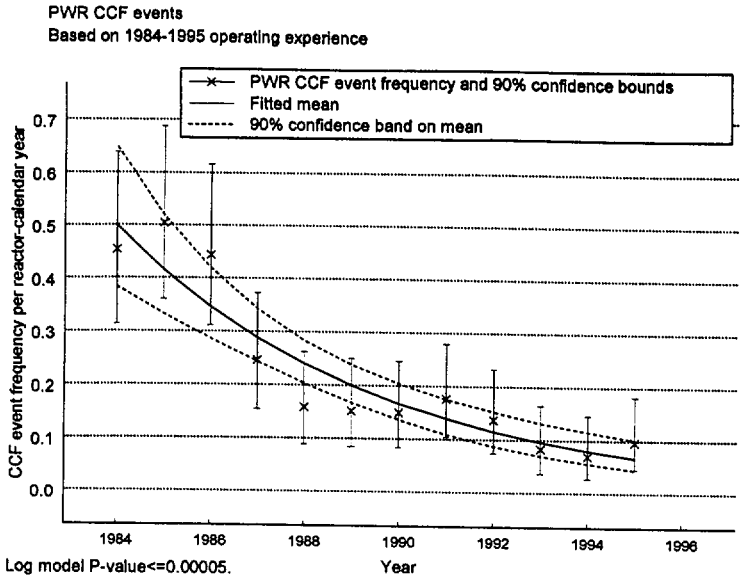


Figure 4-14. Trend analysis for PWR CCF events among the components in the Combustion Engineering data analysis, per reactor calendar year.

4.3.2 Total Failure Probability Trends

In estimating the probability of CCF events, factors representing the level of loss of redundant components were multiplied by overall total failure probability estimates. Possible trends were evaluated for the data going into these total failure estimates. For the two sensor/transmitter and two core protection calculator components in the fault tree models, the unavailability from failures detected during routine operation and the unavailability from failure modes detected during testing were estimated separately. The routine operation unavailability was estimated from the data by assuming a specified downtime and computing a failure rate.

The resulting four rate estimates and the 12 probability estimates computed for the Combustion Engineering RPS unavailability assessment were each evaluated for trends. The evaluations were repeated with and without the inclusion of uncertain failures. In some cases, observations from one or both other PWR vendors were included in addition to the Combustion Engineering data. Conversely, in some cases the shutdown data are excluded. In both of these determinations, the selected data set corresponds to the data set used for input in computing the unavailability estimate (Q_T).

Four of the estimates showed decreasing trends. As shown in Figure 4-15 through Figure 4-19, the decreasing trends were observed for pressure sensor/ transmitter rates with the plant operating (p-value 0.022), for digital core protection calculator rates (p-value 0.032), for bistable failure probabilities with the plant operating (p-value 0.0004), for temperature sensor/transmitter rates (p-value 0.008), and for breaker undervoltage coil probabilities (p-value 0.038). Each of these was estimated using data from Combustion Engineering plants only. For all of these components, the trends remained significant, even with uncertain failures excluded.

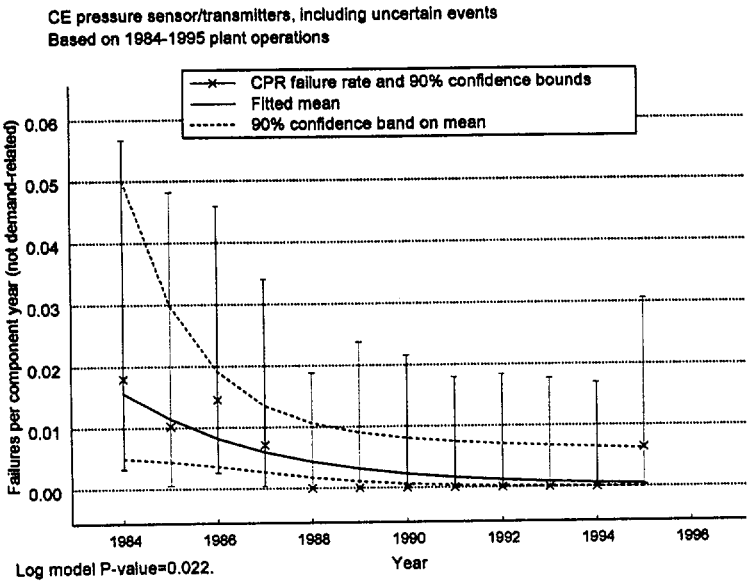


Figure 4-15. Trend analysis for Combustion Engineering pressure sensor/transmitter total failure rate, including uncertain failures, while the plants were operating.

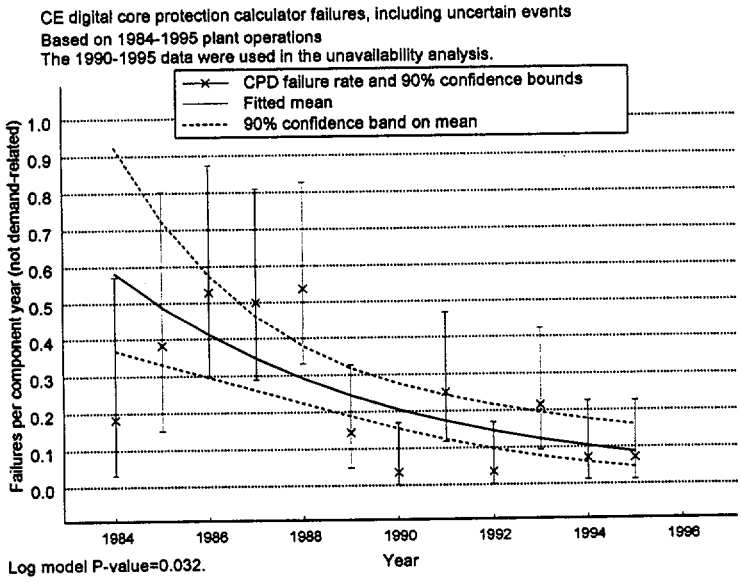


Figure 4-16. Trend analysis for Combustion Engineering digital core protection calculator total failure rate, including uncertain failures.

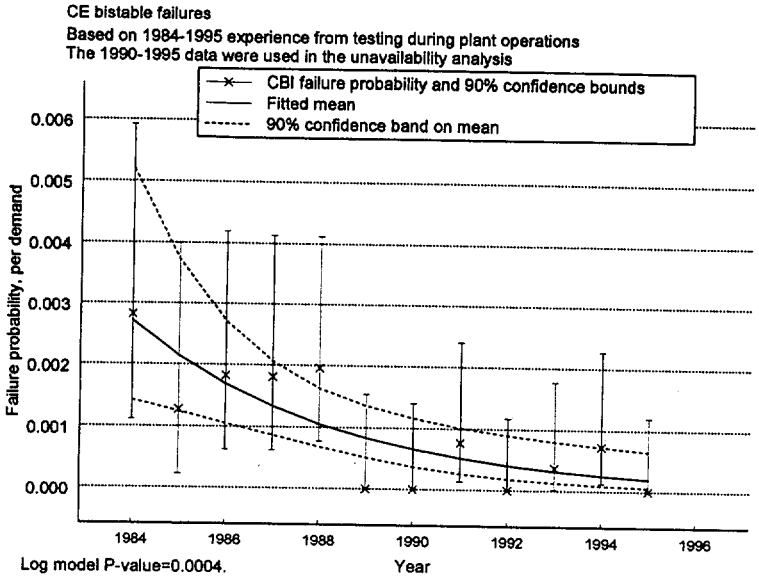


Figure 4-17. Trend analysis for Combustion Engineering bistable total failure probability, based on failures detected in testing during plant operations (including uncertain failures).

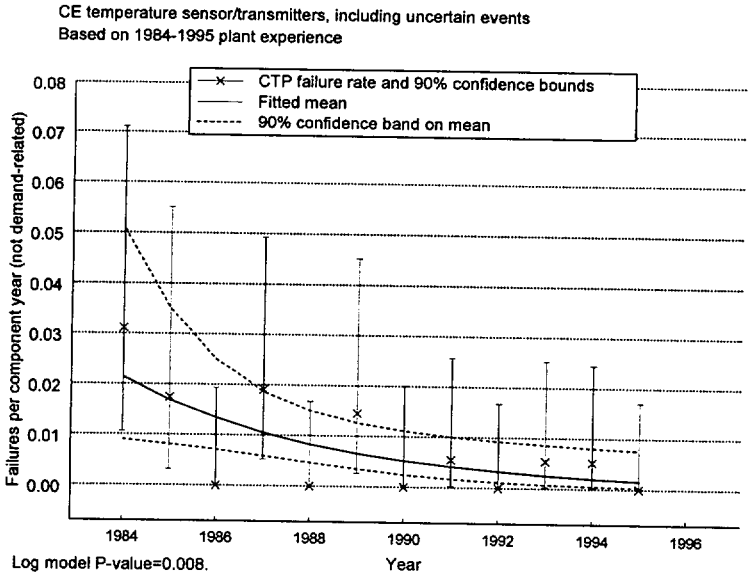


Figure 4-18. Trend analysis for Combustion Engineering temperature sensors/transmitter failures that are not demand-related, including uncertain failures.

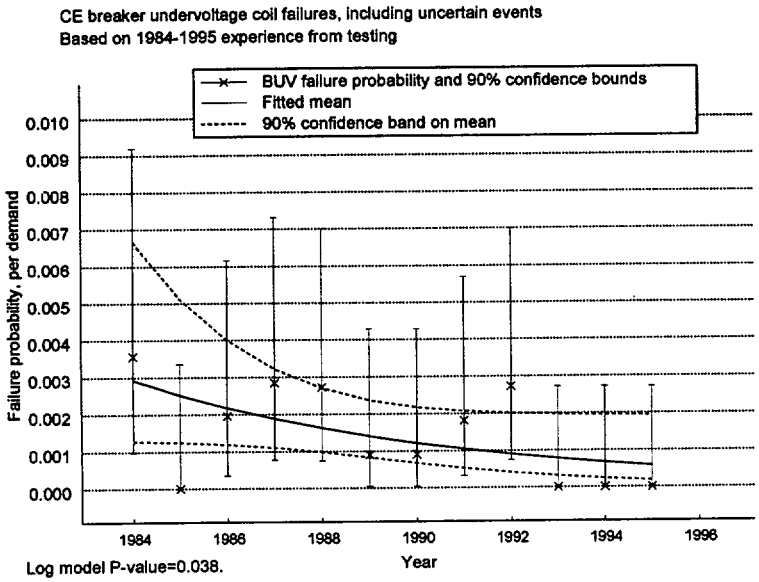


Figure 4-19. Trend analysis for Combustion Engineering breaker undervoltage coil total failure probability, including uncertain failures.

Since other statistical tests showed a difference between the data for the 1980s and the 1990s, only the 1990–1995 data were used in the unavailability analysis for the digital core protection calculator failure rate and for the bistable failure probability. For pressure sensor/transmitters, logic relays, temperature sensor/transmitters, and breaker undervoltage coils the entire period was used in the estimates because the performance without the uncertain failures showed no significant difference between the 1984–1989 and 1990–1995 periods.

5. SUMMARY AND CONCLUSIONS

Fault trees for each of the four designs of the CE RPS were developed and quantified using U.S. CE commercial nuclear reactor data from the period 1984 through 1998. All CE plants use the same channel through trip module design, except later plants use a digital core protection calculator. The Group 1 design uses trip contactors without any form of circuit breaker. The other three groups use either an eight-breaker design (Groups 2 and 3) or a four-breaker design (Group 4). Table 5-1 summarizes the results of this study.

Table 5-1. Summary of Combustion Engineering RPS model results.

	5%	Mean	95%
Group 1 RPS Model			
No credit for manual trip by operator	1.2E-6	6.5E-6	1.8E-5
Credit for manual trip by operator	8.8E-7	5.7E-6	1.7E-5
Group 2 RPS Model			
No credit for manual trip by operator	1.9E-6	7.5E-6	1.9E-5
Credit for manual trip by operator	3.9E-7	1.9E-6	5.1E-6
Group 3 RPS Model			
No credit for manual trip by operator	1.9E-6	7.5E-6	1.9E-5
Credit for manual trip by operator	3.9E-7	1.9E-6	5.1E-6
Group 4 RPS Model			
No credit for manual trip by operator	1.6E-6	7.2E-6	1.9E-5
Credit for manual trip by operator	2.4E-7	1.6E-6	4.7E-6

The computed mean unavailabilities for the various CE design groups ranged from 6.5E-6 to 7.5E-6 (with no credit for manual trips). These are comparable to the values CE IPEs, which ranged from 3.7E-6 to 1.0E-5, and other reports. Common-cause failures contribute approximately 99 percent to the overall unavailability of the various designs. The individual component failure probabilities are generally comparable to failure probability estimates listed in previous reports.

The RPS fault tree was also quantified for manual trip by the operator (assuming an operator failure probability of 0.01). The mean unavailabilities improved 13 percent (Group 1) to 78 percent (Group 4), with a range of 1.6E-6 to 5.7E-6.

The study revealed several general insights:

- The dominant failure contribution to the Combustion Engineering RPS designs involve CCFs of the trip relays (K-1 through K-4, Groups 2, 3, and 4 or M-1 through M-4 Group 1) and the CCF of the mechanical portion of the trip breakers (except Group 1).

- Issues from the early 1980s that affected the performance of the reactor trip breakers (e.g., dirt, wear, lack of lubrication, and component failure) are not currently evident. Improved maintenance has resulted in improved performance of these components.

- Overall, the trends in unplanned trips, component failures, and CCF events decreased significantly over the time span of this study.

- The calculated unavailability of plants that have analog rather than digital core protection calculators shows no sensitivity to this design difference.

- The causes of the CE CCF events are similar to those of the rest of the industry. That is, over all RPS designs for all vendors for the components used in this study, the vast majority (80 percent) of RPS common-cause failure events can be attributed to either normal wear or out-of-specification conditions. These events, are typically degraded states, rather than complete failures. Design and manufacturing causes led to the next highest category (7 percent) and human errors (operations, maintenance, and procedures) were the next highest category (6 percent). Environmental problems and the state of other components (e.g., power supplies) led to the remaining RPS common-cause failure events. No evidence was found that these proportions are changing over time.

- The principle method of detection of failures of components in this study was either by testing or by observation during routine plant tours. Only two failures were detected by actual trip demands, neither of which was a CCF. No change over time in the overall distribution of detection method is apparent.

6. REFERENCES

1. U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, *Anticipated Transients Without Scram for Light Water Reactors*, NUREG-0460, Vol. 1, April 1978.

2. U.S. Atomic Energy Commission, *Technical Report on Anticipated Transients without Scram for Water-Cooled Power Reactors,* WASH-1270, September 1973.

3. U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, *Generic Implications of ATWS Events at the Salem Nuclear Power Plant, NUREG-1000,* Vol. 1, April 1983.

4. Generic Letter 83-28, *Required Actions Based on Generic Implications of Salem ATWS Events*, U.S. Nuclear Regulatory Commission, July 8, 1983.

5. 49 FR 124, *Considerations Regarding Systems and Equipment Criteria*, Federal Register, U.S. Nuclear Regulatory Commission, June 26, 1984, p. 26036.

6. Generic Letter 85-06, *Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related*, U.S. Nuclear Regulatory Commission, April 16, 1985.

7. 10 CFR 50.62, *Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants*, February 25, 1986.

8. The Institute of Nuclear Power Operations, *NPRDS Reportable System and Component Scope Manual, Combustion Engineering Pressurized Water Reactors*, INPO 83-020G, Rev. 5, November 1994.

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

10. K. D. Russell et al., *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0*, NUREG/CR-6116, Vol. 1, December 1993.

11. S. A. Eide et al., *Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs*, EGG-SSRE-8875, February 1990.

12. Westinghouse Electric Corporation, Energy Systems Division, *Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System*, WCAP-10271-P-A, May 1986.

13. R. R. Fullwood et al., *ATWS: A Reappraisal Part I: An Examination and Analysis of WASH-1270, Technical Report on ATWS for Water-Cooled Power Reactors,* EPRI NP-251, August 1976.

14. *RPS/ESFAS Extended Test Interval Evaluation*, prepared for the C-E Owners Group, CEN-327-A Topical Report, May 1986.

15. *Arkansas Nuclear One Unit 2 Probabilistic Risk Assessment Individual Plant Examination*, Entergy Operations, Inc., August 1992.

16. *Calvert Cliffs Nuclear Power Plant Probabilistic Risk Assessment Individual Plant Examination Summary Report*, Baltimore Gas and Electric, December 1993.

17. *Fort Calhoun Station Individual Plant Examination Submittal*, Omaha Public Power District, December 1993.

18. *Maine Yankee Probabilistic Risk Assessment Individual Plant Examination*, Yankee Atomic Electric Company, August 1992.

19. *Millstone Unit 2 Individual Plant Examination for Severe Accident Vulnerabilities*, Northeast Utilities Service Co., December 1993.

20. *Palisades Nuclear Plant Individual Plant Examination*, Consumers Power, January 1993.

21. *Palo Verde Nuclear Generating Station Units 1, 2, & 3 Individual Plant Examination*, Palo Verde Nuclear Generating Station, April 1992.

22. *Individual Plant Examination Report for San Onofre Nuclear Generating Station Units 2 and 3*, Southern California Edison, April 1993.

23. *St. Lucie Units 1 and 2 Individual Plant Examination Submittal*, Florida Power and Light Company, December 1993.

24. *Waterford Generating Station Unit 3 Probabilistic Risk Assessment Individual Plant Examination*, Entergy Operations, Inc., August 1992.

25. U.S. Nuclear Regulatory Commission, *Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram (ATWS) Events*, SECY-83-293, July 19, 1983.

26. Thadani, A.C., *NRC Evaluation of CEOG Topical Report CEN-327, RPS/ESFAS Extended Test Interval Evaluation*, included in the latest issue of CEN-327-A Topical Report, November 6 1989.

Appendix A

RPS Data Collection and Analysis Methods

Appendix A

RPS Data Collection and Analysis Methods

To characterize reactor protection system (RPS) performance, operational data pertaining to the RPS from U.S. commercial nuclear power plants from 1984 through 1998 were collected and reviewed. In this study of the RPS, the fifteen Combustion Engineering (CE) pressurized water reactor (PWR) plants were considered. Reported inoperabilities and unplanned actuations were characterized and studied for these plants from the perspective of overall trends and the existence of patterns in the system performance. Unlike other operational data-based system studies sponsored by the Nuclear Regulatory Commission (NRC) at the Idaho National Engineering and Environmental Laboratory (INEEL), the inoperabilities were component failures. Redundancy in the RPS and interconnections between the RPS channels and the trip logic and breakers that deenergize and release the control rods requires a more detailed analysis than just viewing the RPS, even at a train level.

Descriptions of the methods for the basic data characterization and the estimation of unavailability are presented below. In addition to discussing the methods, the descriptions summarize the quality assurance measures used and the reasoning behind the choice of methods. Appendix E explains the probabilities coming from the common-cause data analysis.

A-1 DATA COLLECTION AND CHARACTERIZATION

The subsections below describe the methods for acquiring the basic operational data used in this study. The data are inoperabilities and the associated demands and exposure time during which the events may occur.

A-1.1 Inoperabilities

Because RPS is a multiple-train system, most failures in RPS components are not required by 10 CFR 50.73 to be reported in Licensee Event Reports (LERs). Accordingly, the primary data source for RPS inoperabilities is the Nuclear Plant Reliability Data System (NPRDS). NPRDS failure data were downloaded for components in the RPS and control rod drive systems. Immediate/catastrophic and degraded events were included; incipient events were omitted.

For this study, events prior to 1984 were excluded for two reasons. First, nuclear power plant (NPP) industry changes related to the RPS occurred in response to the 1983 Salem Unit 1 low-power ATWS event. Second, the failure reporting system changed significantly with the January 1, 1984 institution of the LER Rule (10 CFR 50.73). The LER rule shifted the emphasis in LER reporting away from single component failures to focus on significant events, leaving NPRDS to cover component failures. Failure reporting to NPRDS has been voluntary. As manager of the NPRDS, the Institute for Nuclear Power Operations (INPO) has taken many measures to encourage complete failure reporting to the system during the period from 1984 through 1996. The NPP

industry has relied on the NPRDS for the routine reporting of single component failures during that period.

In 1997 and 1998, an industry-sponsored initiative to report failure data to a system called "EPIX" has been underway. Because development for the EPIX database continues, the EPIX RPS data were not available for this study. Furthermore, the NPRDS data for 1996 are possibly not complete, since the NPRDS was known to be ending at that point. Therefore, no source for reliable reporting of failures discovered in system testing (with many redundant components) was available for the 1996–1998 period for this study.

To ensure that the failure data set is as complete as possible, the Sequence Coding and Search System (SCSS) LER database was searched for any RPS inoperabilities reported in LERs from 1984 through 1998. Particularly, any inoperabilities discovered during unplanned reactor scrams should be reported. The 1996–1998 LER data have been reviewed for CE plants and for Babcock & Wilcox (B&W) plants, but not for Westinghouse (W) or General Electric (GE) plants. Table A-1 summarizes the availability of various types of data for the CE RPS analysis.

Table A-1. Availability of RPS reliability data for this study.

Type of component	Reporting in LERs	Reporting in NPRDS
Component demanded in every reactor trip, other than rods	Failures during unplanned trips should be reported. 1984–1998 data. Data from testing and routine observation would not be reported due to system redundancy. Westinghouse LER data from 1996—1998 has not been reviewed for this study.	Failures occurring during trips, tests, and routine operations should be reported. For this study, data from 1984 through 1995.
Component used in some but not all reactor trips	LER trip data cannot be used because there is no way to estimate the number of demands.	Same as above.
Rods and control rod drives [a]	LERs provide reactor trip data, as above.	Rod failures were not reported after 3/15/1994.

a. Treated as one unit in this study.

The NPRDS and SCSS data searches were used to identify events for screening. The major areas of evaluation to support the analysis in this report were as follows:

- What part of the RPS, if any, was affected? Some events pertained to the ATWS Mitigation System Actuation Circuitry (AMSAC), or to support systems that are not within the scope of the RPS. Other RPS events were in parts of the system not directly critical to the performance of its safety function, such as failures in indicators and recording devices. Such events were marked as nonfailures and were not considered further.
- For events within the scope of RPS, the specific component affected by the event was indicated. For CE plants, the following distinctions were made (codes for the associated components are in parentheses):
  - Channels (instrumentation rack): sensors and transmitters [power (CPN), source (CSR), and intermediate range (CIR) neutron detectors, temperature sensor/transmitters (CTP), pressure sensor/transmitters (CPR) flow (CPF) and level (CPL) sensor/transmitters, pump monitors (CPM), and pressure (CPS) switches], analog or digital core protection calculators (CPC and CPD, respectively), power supplies (CPW), and bistables (BIS).

  - Trains (logic cabinet): logic relays (RYT), trip relays(RYL), and the manual scram switch (MSW).
  - Trip breakers: ac breakers (mechanical/electrical) (BME) and the associated RTB undervoltage coil (BUV) and shunt trip (BSN) devices.
  - Rods: rod control cluster assemblies/control rod drive mechanisms (ROD and CRD).

- Whether the event contributed to a possible loss of the RPS design safety function of shutting down the reactor. This distinction classifies each inoperability as either a failure, or just a fault. *Faults* are occurrences that might lead to spurious RPS actuation such as high-pressure set points that have drifted low. *Failures*, on the other hand, are losses at a component level that would contribute to loss of the safety function of RPS; i.e., that would prevent the deenergizing and insertion of the control rods. For the RPS, another way of stating this distinction is that faults are inoperabilities that are fail-safe, while failures are those that are not fail-safe. The RPS events were flagged as fail-safe (FS), not fail-safe (NFS), or unknown (UNK). The latter designation applies, for example, when a failure report does not distinguish whether a failed transmitter monitors for high pressure or for low pressure.

- Whether the event was a common-cause failure (CCF). In this case, several other fields were encoded from the event record: CCF Number, CCF shock type, time delay factor, coupling strength, and a brief event description. These assessments are described further in Appendixes B and E.

- Whether the failure was complete. Completeness is an issue, particularly for failed timing tests and cases where components are out of tolerance but might still perform their safety function if called upon. Completeness is also an issue when component boundary definitions differ and NPRDS reports the complete failure of a component that is a piece part with regard to the RPS fault tree model. The probability of the modeled RPS component functioning given the degradation reported in the LER or NRPDS was assessed as either 1.0, 0.5, 0.1, or 0.01. In the basic failure analysis, the 0.5-assessed events were treated as unknown completeness, while the 0.1- and 0.01-assessed events were treated as nonfailures. These assessments were also used in developing impact vectors for the common-cause assessment, as discussed in Appendix E.

- The method of discovery of the event [unplanned demand (i.e., reactor trip), surveillance test, other]. For the NPRDS data, "other" includes annunciated events. For surveillance tests, the test frequency was determined if it was clear from the event narrative. Failures discovered during reactor trips were identified from the LERs and from matching the reactor trip LERs (described in the next section) with the NPRDS failures. Narratives from the few matching records were reviewed. If the failure caused the reactor trip, it was flagged as a fail-safe fault discovered during operations. If it did not cause the reactor trip but was observed during the course of the reactor trip event, it was flagged as being discovered by the reactor trip.

- Plant operational state ("mode"): up or down. RPS actuation, after the control rods have already been inserted, is not required to be reported[A-18] since 1992. Thus, for reported events, the plant is defined as up. The test events may occur while the plant is up or while it is down. An issue is whether the failure occurrence probabilities (failures per demand) are the same for both situations, and which scenario is the most realistic for the unavailability analysis if they differ. The assessment of plant state for failures during testing and operation was based on the NPRDS and LER narratives, if possible. The data were then compared with the outage information used in the NRC Performance Indicator Program to resolve plant state issues in

some cases. When the plant state was unknown, it was treated as operating since the plants spend more time in an operating state than shut down.

- The plant and event date for each failure, as presented in the source databases, were preserved and used in the data analysis.

Other attributes were also considered, such as the event cause and failure mode. Some of these fields are described in Appendix B. The screening associated with the common-cause analysis is described further in Appendix E.

The RPS inoperability evaluation differs from previous NRC system operational unreliability studies (References A-1 through A-6) in several aspects. A greater emphasis on common-cause failure analysis applies due to the many redundant aspects of the system. The system redundancy also leads to the use of NPRDS data, since few unplanned reactor trips reveal problems within the RPS itself. That is, unlike the auxiliary feedwater system, the RPS does not have a sufficient failure data set for analysis from just the LERs from unplanned reactor trips. Given the use of NPRDS data and the focus on components rather than trains or segments, the completeness issue is more dynamic for the RPS. The inability to distinguish whether a failure is fail-safe adds additional uncertainty to the data evaluation. Unlike previous NRC system operational unreliability studies, the failure events were not screened to determine if the events were recoverable, since the RPS performs its mission on demand and has no extended mission time. The lack of a mission time means also that there is no need to evaluate the components based on different failure modes, such as starting and running.

The treatment of maintenance unavailability is also different for the RPS than for the previous system studies. Although the SCSS data search included timing codes such as "actual preexisting" and "potential," both previously detected and not previously detected, incidents of a channel of the RPS being out-of-service for maintenance or testing when demanded during an unplanned reactor trip are not routinely reported. The primary instances found in the data for such preexisting maintenance were when the maintenance contributed to causing a spurious reactor trip and was thus fail-safe. Since neither the NPRDS nor the LER data provide the needed information on planned maintenance unavailabilities, the maintenance unavailabilities in the fault tree were estimated using the maintenance times specified in the operating procedures.

The data characterization for the events was based on reading the associated NPRDS event narratives and LER abstracts. Engineers with commercial nuclear power plant experience classified the data and reviewed each other's work for consistency. A final, focused review was performed by instrumentation and control and RPS experts on a subset of the approximately 20000 NPRDS and LER records.

Several additional checks and filters were applied to the RPS failure event data:

- For each plant, the data were constrained to lie between the plant's commercial operation date and its decommission date (if applicable; 8/6/1997 for Maine Yankee). NPRDS data reporting for a plant begins with its commercial operation date.

- Events and operating time/demands during NRC-enforced *regulatory outages*, as defined in the NRC Performance Indicator (PI) Program, were excluded as being atypical. Among CE plants, this restriction removed Palisades during the last half of 1986 and the first third of 1987, and Millstone 2 from the middle of 1996 onward.
- A date check ensured that no control rod demands or events from testing were counted after March 15, 1994, the date on which the NPRDS reporting scope changed to omit these components (among others) from the NPRDS.
- NPRDS and LER data were matched by plant, event date, and component, and checked to ensure that no event was counted twice.

Further details of the inoperability characterization and database structure are included in Appendix B.

A-1.2 Demands and Exposure Times

For the reliability estimation process, two models are typically used to estimate unavailability. The first is based simply on failures and demands. The probability of failure on demand is estimated simply as the number of failures divided by the number of demands. The resulting estimate is useful if the demands are complete and unbiased, and the counts of demands and failures are complete. This is the primary model used for the components in the RPS.

For the channel neutron monitors, pressure sensor/transmitters, and temperature sensor/ transmitters, however, failures occur other than the ones routinely monitored by testing. These failures are detected either by annunciators or during periodic walkthroughs by plant operators, and thus are not present during the quarterly and cyclic surveillance tests. The method of discovery thus distinguishes these failures from the others. The downtime for discovering these failures and repairing them is small, typically 8 hours or less. To ensure that this contribution to the unavailability is not overlooked, the nontesting failure rate in time is estimated for the subset of these components that appear in the fault tree. For each of these components, a gamma uncertainty distribution for the rate is combined with an 8-hour downtime to obtain an unavailability. If this unavailability is much greater than the unavailability from the demand events, it is used in the fault model quantification. If, on the other hand, it is much smaller, the unavailability estimated from the failures on demand is used. If the two unavailabilities are comparable, they are summed for the fault model quantification.

In the engineering analysis portion of this study, general failure occurrence frequencies in time are estimated for the assessment of trends. These frequencies are based on all the failures and the associated calendar time for the components.

Estimation of both demands and operating times requires knowledge of the number of each type of RPS component at each plant. The next three sections discuss estimates of component counts, demands, and operating times.

A-1.2.1 Component Counts

For each plant, the number of each type of RPS component listed in the second bullet in Section A-1.1 was estimated. These component counts are the exposed population of RPS system components installed at each plant that could fail. The "Count Basis" column of Table A-2 contains the results for the components used in the fault trees. Note that these counts are estimates; exact information on each plant was not available. Plant-specific engineering records in the NPRDS are intended to provide a profile of the number of components for which failures are to be reported to the NPRDS system. These records were studied to identify component counts, but they were not directly useful because the component boundary definitions used for this study are different.

Table A-2. CE RPS components used in the PRA.

Comp. code	Component	Testing Frequency [a]	Operating [b]	Demanded in each reactor trip	Count basis
Channels					
CPR	Pressure sensor/transmitter	Cyclic & quarterly [c]	Yes	No	One for the pressurizer and at least one per steam generator, per ch. Digital plants have two per SG/ch. See Note d.
CTP	Temperature sensor/transmitter	Cyclic & qtrly. [c]	Yes	No	2/loop/channel, except Maine Yankee with 1/loop/channel.
CPA	Analog core protection calculator	Quarterly	Yes	No	1 per channel (Model Groups 1, 2)
CPD	Digital core protection calculator	Quarterly	Yes	No	1 per channel (Model Groups 3, 4)
CBI	Bistable	Quarterly	No	No	12 to 16 per channel
Trains					
RYL	Logic relay	Quarterly	No	No	dc. 24 (from 6 logic matrices and 4 channels)
RYT	Trip relay	Quarterly [f]	No	No	4-K relays; except, at Group 1 plants, 4-M relays.
MSW	Manual scram switch	Quarterly	No	Yes [e]	4, except 2 at Model Group 1 plants.
Trip breakers and rods					
BME	Breaker mechanical	Qtrly.& monthly [f]	No	Yes	8 for plants in Model Groups 2 and 3. 4 for Group 4.
BSN	Breaker shunt device	Quarterly [f]	No	No [g]	1 per breaker
BUV	Breaker undervoltage coil	Monthly [h]	No	No [g]	1 per breaker
RMA	Control element assembly & rod	Cyclic	No	Yes	Plant-specific. NPRDS data not collected after 3/15/94.

a. Information from CEN-327-A. A CE Owners Group submittal in May, 1986, argued for quarterly rather than monthly testing of channels. However, it is not known when particular plants switched to quarterly testing. This study assumes quarterly testing for the entire study period (1984-1995).

b. Operating components are those components whose safety function failures can be detected in time. Rates as well as probabilities of failure on demand are estimated for operating components. The instruments are visually checked in each shift, and the core protection calculators perform continuous internal checking for certain types of failures.

c. In the quarterly channel tests, responsiveness of the sensor/transmitter signal conditioning is verified.

d. Plant Model Groups 1 and 2 are analog, while Groups 3 and 4 are digital. See Table 3. There are two loops/plant, except Maine Yankee with three.

e. Demanded in manual trips, not automatic trips.

f. Each quarterly test includes six demands, one associated with each logic matrix.

g. BSN or BUV failures that occur during a trip generally cannot be detected. Both BSN and BUV must fail in order for the failure to be detected.

h. Quarterly tests are not included for BUV because the breaker actuation tests do not test UV and shunt mechanisms separately.

A-1.2.2 Demands

For RPS, the demand count assessment for unavailability estimates based on failures per demand is more uncertain than in previous NRC system studies. In previous NRC system studies, possible sets of demands were considered, such as demands from unplanned actuations of the system and demands from various types of periodic surveillance tests (monthly, quarterly, or cyclic). Demands at plant startup or shutdown might also be considered. The selection of the sets of events with particular system demands determines the set of failures to be considered in the reliability estimation (namely, the failures occurring during those demands).

In evaluating the possible sets of demands, the following criteria are sought:

1. An ability to count, or at least estimate, the number of demands
2. An ability to estimate the number of failures. Completeness is sought in the failures, so that they will not be underestimated. Conversely, the failures are to be matched with the demands, so that failures only on the type of demand being considered are counted. Then the number of successes on the type of demand being considered will not be underestimated.
3. The demands need to be complete and rigorous, like an unplanned demand on the system, so that all the relevant failure modes will be tested.

For RPS, the requirement that the demand event set be *countable* is not always met. Although a fairly accurate count of unplanned reactor trips is available from the LERs since 1984, the reactor trips themselves do not exercise the complete RPS. Particularly for the channel components, different reactor trips come from different out-of-bound parameters. For example, the number of unplanned reactor trips for which the pressurizer low pressure setpoint was exceeded is unknown. Unplanned reactor trip demand data are not used in this report for channel data since these demands are not countable. For the same reason, unplanned demands are also not used for the logic and trip relays. Unplanned reactor trip demands are not used for the RTB shunt trip and undervoltage coils because these events demand at least one of these two components but not necessarily both.

Most of the estimates in this report are therefore based on test data. For CE plants, quarterly tests apply for train (trip logic) components and breakers, and channel components. In addition, the channel instruments are tested and calibrated during refueling outages and cyclic tests. The breakers have monthly tests in addition to the quarterly tests. The control rod assemblies and control rod drives are tested during cyclic tests associated with refueling. Based on calendar time and the number of installed components of each type in each plant, estimates for these demands are calculated in this report. The estimates are calculated also based on the fact that, in some of the tests, a component is demanded more than once. Table A-2 and its footnotes show the testing assumptions that were made for each component used in the fault tree.

The completeness of the failure count for the RPS testing data depends on two attributes. First, the failures need to be reported, either through the LERs or NPRDS. In the August 7, 1991 NRC Policy Issue, SECY-91-244, the NRC staff estimated overall NPRDS completeness at 65 to 70%, based on a comparison of 1990 NPRDS failure data and component failures reported in LERs. As mentioned, the LERs themselves are not expected to be complete for RPS failures since

single failures on testing are not required to be reported through the LER system. Thus, the failures may be undercounted.

The second attribute probably leads to an overcounting of the RPS testing failures. This attribute concerns the ability to distinguish whether a failure is detected during testing, or, more specifically, during the type of testing being considered. In this regard, the brief NPRDS failure narratives usually are insufficient to distinguish periodic surveillance tests from postmaintenance tests or other types of testing. Since the testing frequency often is not mentioned, no attempt is made in this study to restrict the set of testing failures to a particular type of test. An example of the influence of this uncertainty in the data is that all failures on testing for temperature sensor/transmitters are used in the unavailability analysis, though the quarterly testing occurs only four times per year, and the calibration testing occurs on average only once every eighteen months. No attempt has been made in this study to associate the failure times with the plant refueling outage times. This source of uncertainty is not currently quantified.

The completeness of the periodic surveillance testing for RPS components is believed to be statistically adequate, realistically mimicking the demand that an unplanned reactor trip using this portion of the RPS would place on the system. The demands are believed to be rigorous enough that successes as well as failures provide meaningful system performance information. However, in some of the demand data, differences have been noted between tests that are conducted while the plant is operating and tests conducted during shutdown. The failure probability in some cases is observed to be higher during shutdown. This phenomenon is attributed to the additional complications introduced by maintenance during shutdowns rather than to an inadequacy in the quarterly and monthly testing that occurs at power.

The remaining subsections of this section outline additional details of the methods for estimating the various types of demand counts.

A-1.2.2.1 Unplanned Demands. The NRC Performance Indicator (PI) databases maintained at the INEEL were used as the source for a list of unplanned actuations of the RPS. Unplanned reactor trips have been a reporting requirement for LERs since the 1984 LER rule. The PI databases have been maintained since 1985 and are a reliable source of LER reactor trip data. The databases include manual as well as automatic reactor trips, though only the latter are currently a performance indicator.

Reactor trip data for 1984 were obtained from the Sequence Coding and Search System. Nine LER number lists with associated event dates for 1984 were obtained. Seven corresponded to each combination of three attributes: required versus spurious reactor trips, automatic versus manual reactor trips, and during operation versus during startup (there were no LERs for the combination of manual spurious reactor trips during startup). The other two files described automatic, spurious reactor trips. The eighth file was for LERs reporting reactor trips at a different unit at the site than the unit reporting the LER. The ninth was for LERs reporting multiple reactor trips. These lists were consolidated, and records for a second unit's reactor trip were added for LERs reporting multiple reactor trips, including reactor trips at another unit. The plant identifier field was adjusted to the unit with the reactor trip for LERs with single reactor trips at different units. Finally, records with multiple reactor trips at single units were examined. If multiple records

were already present (e.g., reflecting a manual reactor trip and an automatic reactor trip on the same date), no changes were made. If no multiple records were present, the demand field (for number of reactor trips) was changed to two. Since the SCSS did not provide a simple list of reactor trip dates and counts for each unit, uncertainties are associated with this process; but the process is believed to be quite accurate.

The unplanned demands were used for three components in the fault tree: reactor trip breakers, the manual scram switch (manual scrams only), and the control rod assemblies/control rod drives. In each of these cases, for each plant and year, the number of relevant reactor trips was multiplied by the assumed number of components to get the number of component demands. Unlike other recent NRC system studies (References A-1 through A-6), there was no concern that failures of particular components would preclude demands on other components. The changes in demand counts that the few failures discovered in the unplanned demands might make on the few other RPS components considered in the unplanned demands is negligible compared with the total number of demands.

A-1.2.2.2 Surveillance Tests. Quarterly test counts were estimated at a plant-year level by assuming 4 tests per full plant year. On the year of the plant's commercial service date, and the year of the plant's decommission date (if any), the demands were reduced in proportion to the plant's in-service time.

Cyclic surveillance test demands at a plant level were counted using the NRC's OUTINFO database. This database is based on plant Monthly Operations Reports, and is maintained for the NRC PI program. It lists the starting and ending dates of all periods when the main generator is off-line for a period spanning at least two calendar days. Plausible test dates were estimated based on the ending dates for refueling outages. If the period from the startup after a refueling outage to the beginning of the next refueling outage exceeds 550 days (approximately 18 months), then a plausible date for a mid-cycle test is assigned. The resulting dates are summed by plant and year. For the 1984–1985 period for which the refueling outage information is not available, plausible testing dates are projected back in time from known refuelings.

For each type of periodic surveillance test, the estimated plant counts were prorated between plant operation time and plant shutdown time. For each plant and year, the outage time represented in the OUTINFO database was summed, including the days on which outages started and ended. The down time was summed separately and excluded for regulatory-imposed outages (as observed above, Palisades for a selected period in the early years of the study and Millstone 2 for the ending part of the study period). The remaining time between a plant's low power license date and its decommission date or the study end date was treated as operational (up) time. The demands were then prorated on a plant and year-specific basis. For example, the operational demands were taken to be the total demand times the fraction of the year the plant was up, divided by the sum of the up fraction and the shutdown fraction.

For the current study, the period covers 1984–1998. Outage data for the period prior to 1986, however, are not readily available. The OUTINFO database has gaps for periods before 1986. For periods during 1984 and 1985 between a plant's low-power license date and the start of OUTINFO

data on the plant, the outage and operational data split was estimated by summing the plant's operational and shutdown time from 1986–1995 and prorating the 1984 and 1985 time to reflect the same percentages.

The plant-year demands were multiplied by the number of components to obtain estimates of component demands. After this multiplication, the estimates for demands during shutdown and demands during operations were rounded up to whole numbers. There was no concern that failures of particular components would preclude demands on other components, because the tests are conducted on the components individually and are staggered across channels and breakers.

A-1.2.3 Operating Time

For failure rate assessments, outage and operational time were estimated in fractions of calendar years for each plant and year, as discussed in the previous section. These fractions were multiplied by the estimated number of components for which failure data has been reported for each plant and year to obtain exposure times in years for operating and shutdown periods for each component type. As needed, these times were converted to hours.

A-2. ESTIMATION OF UNAVAILABILITY

The subsections below describe the statistical analysis for each separate component, then address the combining of failure modes to characterize the total system unavailability and its uncertainty.

A-2.1 Estimates for Each Failure Mode

The RPS unavailability assessment is based on a fault tree with three general types of basic events: independent failures, common-cause failures (CCF), and miscellaneous maintenance/operator action events.

The CCF modes tend to contribute the most to the unavailability, because they affect multiple redundant components. With staggered testing, the estimation of each CCF probability is a product of a **total** failure event probability (Q_T) and one or more factors derived from the analysis of the failure events, as explained in Appendix E.

Since every RPS component involved in the unavailability analysis is in a train whose function is also provided by at least one more train, every component occurs in the CCF events. Therefore, the focus in the individual component analysis for this report was on total failure probabilities rather than probabilities just for independent events. Separate independent estimates with the common-cause events removed were not evaluated, nor were independent probabilities estimated as $\alpha_1 * Q_T$. The fault tree results were reviewed, and the use of Q_T in place of $\alpha_1 * Q_T$ for the independent events introduces less than 3% error.

This section addresses the estimation of the total failure probability and its uncertainty for virtually all of the RPS components appearing in the fault tree. For the RPS basic failure data analysis for the unavailability assessment, 12 failure modes were identified, one for each of the 12 component types listed in Table A-2. Each is based on the nonfail-safe failures of a particular type of component. Component failure data from the NPRDS and LERs were not available for just one

component, namely the 125-Vdc power supply to the shunt trip coils (DCP). The power supply failures in the databases were fail-safe, tending to cause rather than prevent RPS actuation. Generic data were used for DCP failure estimates for the fault tree. The failure data also do not address the RPS maintenance unavailabilities.

The contribution of the operator is another aspect of the system operation that tends currently to fall outside the scope of the operational data analysis. At the system level, manual reactor trips are a form of recovery from failure of the automatic reactor trip function. However, no credit was assumed in this study for operator recovery in the base case.

Table A-2 shows the components for which estimates were obtained. It also indicates which data sets might be applicable for each component. For the components marked in the table as operating, both a probability on demand and a rate were estimated. The demand probability was based on the number of tests and the failures discovered during testing, while the rate was based on the remaining failures in calendar time.

The subsections below describe the processes of selecting particular data sets and estimating probability distributions that reflect uncertainty and variation in the data. Finally, a simulation method is described for quantifying the uncertainty concerning whether particular failures were complete losses of the component's safety function.

A-2.1.1. Data-Based Choice of Data Sets

To determine the most representative set of data for estimating each total failure probability or rate, statistical tests were performed to evaluate differences in the following attributes (as applicable):

- Differences between PWR vendors
- Differences in reactor trip data and testing data
- Differences in test results during operations and during shutdown periods (plant mode differences)
- Differences across time. In particular, the initial 12-year frame of the study was separated into two periods, from 1984 through 1989 and from 1990 through 1995, and differences were evaluated.

To determine which data to use in particular cases, each component failure probability and the associated 90% confidence interval were computed separately in each data set. For failures and demands, the confidence intervals assume binomial distributions for the number of failures observed in a fixed number of demands, with independent trials and a constant probability of failure in each data set. For failures and run times, the confidence intervals assume Poisson distributions for the number of failures observed in a fixed length of time, with a constant failure occurrence rate in each data set. In evaluating the differences, statistical tests were used that do not require large sample sizes.

A premise for the statistical tests is that variation between subgroups in the data be less than the sampling variation, so that the data can be treated as having constant probabilities of failure

across the subgroups. When statistical evidence of differences across a grouping is identified, this hypothesis is not satisfied. For such data sets, confidence intervals based on overall pooled data are too narrow, not reflecting all the variability in the data. However, the additional between-subgroup variation is likely to inflate the likelihood of rejecting the hypothesis of no significant systematic variation between data sets, rather than to mask existing differences.

A further indication of differences among the data sets was whether empirical Bayes distributions were fitted for variation between the testing and unplanned demands or between the two plant modes or the two times frames. This topic is discussed further in Section A-2.1.2.

These evaluations were not performed in the common-cause analysis. The CCF analysis addresses the probability of multiple failures occurring, given a failure, rather than the actual occurrence rate of multiple failures. The occurrence of multiple failures among failures may be less sensitive to the type of demand, plant operational state, and time than the incidence of failure itself. In any case, the CCF data are too sparse for such distinctions.

The four attributes used to determine the data sets for the total failure probabilities for the unreliability analysis are discussed further in the paragraphs below.

Pooling across Vendors. The consideration of pooling across vendors for CE and B&W differs from the RPS system studies for W and GE plants. Differences are likely in the operating environment and testing/maintenance routines for similar components in plants from different vendor's designs. CE and B&W plants represent less operating experience. As the experience decreases, the uncertainty in the estimation of the probability of rare events increases. With homogeneous data, over 30 demands, and two failures, the upper confidence bound on the probability of failure is approximately 3.15 times the maximum likelihood estimate (number of failures divided by the number of demands). When there are fewer failures, the ratio of the upper bound to the point estimate becomes much larger. Therefore, the possibility of including data from more than one vendor is considered for the CE analysis.

The pooling across vendor was considered only under the following three conditions. First, there had to be less than three failures in the CE data for the estimate, so that pooling to refine the estimate might be worthwhile. Second, the pooling had to be feasible from an engineering viewpoint. That is, the components had to be physically similar for the different vendors, and with a similar operating environment. Finally, the pooling had to be feasible from a statistical viewpoint. Pooling was not considered if the statistical test for homogeneity across vendors rejected the hypothesis of homogeneity. However, when differences were found among the three PWR vendors, pairwise comparisons were made to see if one vendor differed from the other three, so that perhaps data from two vendors could be combined.

The pooling of vendors was the first consideration in the data-based choice of data sets. Further subsetting of the data was considered, as described below, to identify the most appropriate data for the unreliability analysis. In pooling the vendor data, only PWR data were considered. In computing the number of testing demands, the type of testing assessed for each separate vendor was applied to the data for that vendor. Thus, the quarterly and monthly testing of Table A-2 was used for the CE trip breaker data, but bimonthly testing was used for the W breakers, and monthly

testing was used for B&W breakers. Furthermore, the pooling decision was made separately for each quantity to be estimated. Thus, pooling might be used for a rate estimate and not used for the probability of failure on demand for the same instrument, because each of these estimates represents a different failure mode for the component. The statistical decision about pooling across vendors was made using exact statistical tests that did not assume a large population size.

Subsetting Based on Reactor Trip Data or Testing Data. Restricting the data for an estimate to trip data only, or testing data only, was applicable only for the few components known to be demanded in each reactor trip. Since few failures were detected during reactor trips, the data were generally insufficient to reveal differences in performance for the unplanned system demand and the testing data sets. Where unplanned demands were listed in Table A-2 for a component, they were used, since they were genuine demands on the RPS. When differences were observed, the testing data were generally used likewise, due to concerns about the adequacy of reporting the failures that might have been revealed in the reactor trips. That is, differences between the unplanned and testing data sets were noted, but the data were pooled in spite of such differences.

Subsetting Based on Plant Modes. The plant operational mode during testing was considered because the duration of RPS maintenance outages during plant operations is limited by plant technical specifications. During plant outages, the technical specifications are much less restrictive, and the tests might be more detailed. Conversely, failure modes, if any, that can only occur during operations might be revealed in the tests conducted during operations.

All unplanned demands occurred when the reactor was at power. Reactor trip signals passing through the system when the plant is not at power have not been reportable as LERs since mid-1993, and were never performance indicators. Thus, no analysis with regard to plant operating mode was performed for the unplanned demand data set.

Where differences were seen between the operational and shutdown testing data sets, and both were potentially applicable for the component, the operational data set was used. This is the set that corresponds to the goal of the unavailability analysis, which is to quantify RPS unavailability during operations.

Subsetting Based on Differences in Time. As in the W and GE RPS system studies, data for the period from 1984 through 1989 were compared with more recent data, and the more recent data were used to estimate the failure probability or rate when significant differences were seen. In this evaluation, the added set of data from 1996 through 1998 was included in the new period if applicable. However, it rarely applied. The newest data apply only to unplanned demands, not to the testing data nor to the occurrences in time, since no NPRDS data were assessed for this period. The Westinghouse unplanned demand data for 1996 through1998 were not available, since these LERs have not yet been reviewed. Therefore, extending the study to 1998 did not shift the January 1, 1990 boundary between old and new data for the assessment.

Summary. The following guidelines were used to select the data set for the unavailability analysis:

1. When no significant differences occurred between vendors and less than three CE failures, data from different PWR vendors was pooled.

2. Where unplanned demands were listed in Table A-2 for a component, they were used, since they were genuine demands on the RPS. Applicable testing data were also used, due to concerns about the adequacy of reporting the failures that might have been revealed in the reactor trips. Thus, differences between the unplanned and testing data sets were noted, but the data were pooled in spite of such differences.
3. Where differences were seen between the operational and shutdown testing data sets, and both were potentially applicable for the component, the operational data set was used.
4. When differences were found between the older and more recent data, the more recent data set was selected.
5. When the data were restricted to plant operations or to the newer time period, and data from more than one vendor was in an assessment, a test for differences in vendors was performed for the subset to ensure that the vendor data could still be pooled.

The final selections were also checked using a statistical model that simultaneously considers the effect of vendor, operational state, and the two times. The model was log linear for rates. For probabilities, the ratio of the probability of failure to the probability of success was taken to be log linear (this is called a *logit* model). SAS procedure GENMOD was used to estimate parameters and evaluate their significance. The models confirmed the consistency of the subset selections.

A-2.1.2. Estimation of Distributions Showing Variation in the Data

To further characterize the failure probability or rate estimates and their uncertainties, probabilities or rates and confidence bounds were computed in each data set for each year and each plant unit. The hypothesis of no differences across each of these groupings was tested in each data set, using the Pearson chi-square test. Often, the expected cell counts were small enough that the asymptotic chi-square distribution was not a good approximation for the distribution of the test statistic; therefore, the computed p-values were only rough approximations for the likelihood of observing as large a chi-square test statistic when no between-group differences exist. The tests are useful for screening, however. Variation in the rates or probabilities from plant to plant or from year to year is identified in order to describe the resulting variation in the unavailability estimates. Identifying the impact of particular plants or years on the estimates is useful in determining whether the results of the unavailability analysis are influenced by possible outliers. The existence of plant outliers is addressed in this report, though the identity of the plants is not, since the NPRDS data are proprietary.

Three methods of modeling the failure/demand or failure in time data for the unavailability calculations were employed. They all use Bayesian tools, with the unknown probability or rate of failure for each failure mode represented by a probability distribution. An updated probability distribution, or *posterior* distribution, is formed by using the observed data to update an assumed *prior* distribution. One important reason for using Bayesian tools is that the resulting distributions for individual failure modes can be propagated easily, yielding an uncertainty distribution for the overall unavailability.

In all three methods, Bayes Theorem provides the mechanics for this process. Details are highlighted for probabilities and for rates in the next two subsections.

A-2.1.2.1. Estimation of Failure Probability Distributions Using Demands. The prior distribution describing failure probabilities is taken to be a *beta* distribution. The beta family of distributions provides a variety of distributions for quantities lying between 0 and 1, ranging from bell-shape distributions to J- and U-shaped distributions. Given a probability (p) sampled from this distribution, the number of failures in a fixed number of demands is taken to be binomially distributed. Use of the beta family of distributions for the prior on p is convenient because, with binomial data, the resulting output distribution is also beta. More specifically, if a and b are the parameters of a prior beta distribution, a plus the number of failures and b plus the number of successes are the parameters of the resulting posterior beta distribution. The posterior distribution thus combines the prior distribution and the observed data, both of which are viewed as relevant for the observed performance.

The three methods differ primarily in the selection of a prior distribution, as described below. After describing the basic methods, a summary section describes additional refinements that are applied in conjunction with these methods.

Simple Bayes Method. Where no significant differences were found between groups (such as plants), the data were pooled, and modeled as arising from a binomial distribution with a failure probability p. The assumed prior distribution was taken to be the Jeffreys noninformative prior distribution.[A-7] More specifically, in accordance with the processing of binomially distributed data, the prior distribution was a beta distribution with parameters, a=0.5 and b=0.5. This distribution is diffuse, and has a mean of 0.5. Results from the use of noninformative priors are very similar to traditional confidence bounds. See Atwood[A-8] for further discussion.

In the simple Bayes method, the data were pooled, not because there were no differences between groups (such as years), but because the sampling variability within each group was so much larger than the variability between groups that the between-group variability could not be estimated. The dominant variability was the sampling variability, and this was quantified by the posterior distribution from the pooled data. Therefore, the simple Bayes method used a single posterior distribution for the failure probability. It was used both for any single group and as a generic distribution for industry results.

Empirical Bayes Method. When between-group variability could be estimated, the *empirical Bayes* method was employed.[A-9] Here, the prior beta (a, b) distribution is estimated directly from the data for a failure mode, and it models between-group variation. The model assumes that each group has its own probability of failure, p, drawn from this distribution, and that the number of failures from that group has a binomial distribution governed by the group's p. The likelihood function for the data is based on the observed number of failures and successes in each group and the assumed beta-binomial model. This function of a and b was maximized through an iterative search of the parameter space, using a SAS routine.[A-8] In order to avoid fitting a degenerate, spike-like distribution whose variance is less than the variance of the observed failure counts, the parameter space in this search was restricted to cases where the sum, a plus b, was less than the total number of observed demands. The a and b corresponding to the maximum likelihood were taken as estimates of the generic beta distribution parameters representing the observed data for the failure mode.

The empirical Bayes method uses the empirically estimated distribution for generic results, but it also can yield group-specific results. For this, the generic empirical distribution is used as a prior, which is updated by group-specific data to produce a group-specific posterior distribution. In this process, the generic distribution itself applies for modes and groups, if any, for which no demands occurred (such as plants with no unplanned demands).

A chi-square test was one method used to determine if there were significant differences between the groups. But because of concerns about the appropriateness and power of the chi-square test, discomfort at drawing a fixed line between significant and nonsignificant, and an engineering belief that there were real differences between the groups, an attempt was made for each failure mode to estimate an empirical Bayes prior distribution over years and plants. The fitting of a nondegenerate empirical Bayes distribution was used as the index of whether between-group variability could be estimated. The simple Bayes method was used only if no empirical Bayes distribution could be fitted, or if the empirical Bayes distribution was nearly degenerate, with smaller dispersion than the simple Bayes posterior distribution. Sometimes, an empirical Bayes distribution could be fitted even though the chi-square test did not find a between-group variation that was even close to statistically significant. In such a case, the empirical Bayes method was used, but the numerical results were almost the same as from the simple Bayes method.

If more than one empirical Bayes prior distribution was fitted for a failure mode, such as a distribution describing variation across plants and another one describing variation across years, the general principle was to select the distribution with the largest variability (highest 95th percentile). Exceptions to this rule were based on engineering judgment regarding the most logical and important sources of variation, or the needs of the application.

Alternate Method for Some Group-Specific Investigations. The data for each component were modeled by year to see if trends due to time existed. The above methods tend to mask any such trend. The simple Bayes method pools all the data, and thus yields a single generic posterior distribution. The empirical Bayes method typically does not apply to all of the failure modes, and so masks part of the variation. When empirical Bayes distributions are fitted, and year-specific updated distributions are obtained, the Bayes distribution may smooth the group-specific results and pull them toward the generic fitted distribution, thus masking trends.

It is natural, therefore, to update a prior distribution using only the data from the one group. The Jeffreys noninformative prior is suitably diffuse to allow the data to drive the posterior distribution toward any probability range between 0 and 1, if sufficient data exist. However, when the full data set is split into many groups, the groups often have sparse data and few demands. Any Bayesian update method pulls the posterior distribution toward the mean of the prior distribution. More specifically, with beta distributions and binomial data, the estimated posterior mean is $(a+f)/(a+b+d)$. The Jeffreys prior, with $a = b = 0.5$, thus pulls every failure probability toward 0.5. When the data are sparse, the pull toward 0.5 can be quite strong, and can result in every group having a larger estimated unavailability than the population as a whole. In the worst case of a group and failure mode having no demands, the posterior distribution mean is the same as that of the prior, 0.5, even though the overall industry experience may show that the probability for the particular failure mode is, for example, less than 0.1. Since industry experience is relevant for the performance of a particular group, a more practical prior distribution choice is a diffuse prior

whose mean equals the estimated industry mean. Keeping the prior diffuse, and therefore somewhat noninformative, allows the data to strongly affect the posterior distribution; and using the industry mean avoids the bias introduced by the Jeffreys prior distribution when the data are sparse.

To do this, a generalization of the Jeffreys prior called the *constrained noninformative prior* was used. The constrained noninformative prior is defined in Reference A-10 and summarized here. The Jeffreys prior is defined by transforming the binomial data model so that the parameter p is transformed, approximately, to a location parameter, ϕ. The uniform distribution for ϕ is noninformative. The corresponding distribution for p is the Jeffreys noninformative prior. This process is generalized using the maximum entropy distribution[A-11] for ϕ, constrained so that the corresponding mean of p is the industry mean from the pooled data, $(f+0.5)/(d+1)$. The maximum entropy distribution for ϕ is, in a precise sense, as flat as possible, subject to the constraint. Therefore, it is quite diffuse. The corresponding distribution for p is found. It does not have a convenient form, so the beta distribution for p having the same mean and variance is found. This beta distribution is referred to here as the constrained noninformative prior. It corresponds to an assumed mean for p but to no other prior information. For various assumed means of p, the noninformative prior beta distributions are tabulated in Reference A-10.

For each failure mode of interest, every group-specific failure probability was found by a Bayesian update of the constrained noninformative prior with the group-specific data. The resulting posterior distributions were pulled toward the industry mean instead of toward 0.5, but they were sensitive to the group-specific data because the prior distribution was so diffuse.

Additional Refinements in the Application of Group-Specific Bayesian Methods. For both the empirical Bayes distribution and the constrained noninformative prior distribution using pooled data, beta distribution parameters are estimated from the data. A minor adjustment[A-12] was made in the posterior beta distribution parameters for particular years to account for the fact that the prior parameters a and b are only estimated, not known. This adjustment increases the group-specific posterior variances somewhat.

Both group-specific failure probability distribution methods use a model, namely, that the failure probability p varies between groups according to a beta distribution. In a second refinement, lack of fit to this model was investigated. Data from the most extreme groups (plants or years) were examined to see if the observed failure counts were consistent with the assumed model, or if they were so far in the tail of the beta-binomial distribution that the assumed model was hard to believe. The test consisted of computing the probability that as many or more than the observed number of failures for the group would occur given the beta posterior distribution and binomial sampling. If this probability was low, the results were flagged for further evaluation of whether the model adequately fitted the data. This test was most important with the empirical Bayes method, since the empirical Bayes prior distribution might not be diffuse. See Atwood[A-8] for more details about this test.

Group-specific updates were not evaluated with the simple Bayes approach because this method is based on the hypothesis that significant differences in the groups do not exist.

Note that, for the RPS study, Combustion Engineering generic distributions were sought rather than distributions updated with plant-specific data. Plant-specific evaluations are not within the scope of this study.

A-2.1.2.2. Estimation of Failure Probability Distributions Using Operating Time. Failure rates were estimated for the three operating components using the failures that occurred in time, excluding those detected in testing. Chi-square test statistics were computed and Bayesian methods similar to those described above for probabilities were used to characterize the variation in the rates. The analyses for rates are based on event counts from Poisson distributions, with gamma distributions that reflect the variation in the occurrence rate across subgroups of interest or across the industry. The *simple Bayes* procedure for rates results in a gamma distribution with shape parameter equal to $0.5+f$, where f is the number of failures, and scale parameter 1/T, where T is the total pooled running time. An *empirical Bayes* method also exists. Here, gamma distribution shape and scale parameters are estimated by identifying the values that maximize the likelihood of the observed data. Finally, the *constrained noninformative prior* method was applied in a manner similar to the other failure modes but again resulting in a gamma distribution for rates. These methods are described further in References A-13 and A-10.

From the rates, failure probability distributions are estimated in the fault tree software. In addition to the gamma distribution for a rate, the software uses an estimate of the average downtime when a failure occurs. For the RPS components, this time is short, since the failures are quickly detected and most corrective actions involve simple replacements and adjustments.

A-2.1.2.3. Estimation of Lognormal Failure Probability Distributions. For simplicity, the uncertainty distributions used in the fault tree analysis were lognormal distributions. These distributions produced more stable results in the fault tree simulations, since the lognormal densities are never J- or U-shaped. For both probabilities and rates, lognormal distributions were identified that had the same means and variances as the original uncertainty distributions.

A-2.1.3. Treatment of Uncertain Failures

In the statistical analysis of Section A-1.2.2, uncertainty is modeled by specifying probability distributions for each input failure probability or rate. These distributions account for known variations. For example, a simple event probability calculated from an observed number of events in an observed number of demands will vary as a result of the random nature of the events. The effect of this sampling variation on the system unavailability is modeled in the simple Bayes method.

For the RPS data, however, the number of events itself was difficult to determine from the often vague NPRDS failure reports. Uncertain information for two particular aspects of the event records has been flagged. The first is whether the safety function was lost. Many of the failure reports for components such as calculators and sensors do not describe their exact usage. The reports often state how the component failed but not whether the nature of the failure would cause a reactor trip or delay a reactor trip. For example, failing high could have either impact, depending on the particular process being monitored. In the failure data, the records were marked as safety function lost, not lost, or unknown.

The second source of uncertainty that has had a significant effect on the data for the RPS is whether the failure represents a total loss of function for the component. In the common-cause methodology, the data analyst assesses his or her confidence in whether a failure represents a total loss. The resulting completeness value represents the probability that, among similar events, the component's function would be completely lost. Assessed values of 1.0, 0.5, 0.1, and 0.01 were used in this field. For the uncertainty analysis, records with 1.0 were treated as complete; those with 0.5 were treated as unknown completeness, and those with lesser values were treated as not complete.

Since they were flagged in the data, these two sources of uncertainty in the RPS failure data were explicitly modeled in the RPS study. This section provides further details on the treatment of these uncertainties.

In the RPS modeling, each assessed common-cause fraction (alpha) was multiplied by the corresponding total failure probability for the component. This probability was based on the total number of failures (both independent and common-cause) that represent complete losses of the safety function of the component. For each component, potentially nine sub-sets of failures could be identified:

1. Complete, safety function lost, failures
2. Complete failures that were fail-safe (safety function not lost)
3. Complete failures for which the impact on the safety function (plant shutdown) is unknown
4. Incomplete failures that would result in the safety function being lost, if they were more severe
5. Incomplete failures that would be fail-safe if they were more severe
6. Incomplete failures with unknown impact on the safety function
7. Failures with unknown completeness that tend to prevent a trip (safety function lost)
8. Failures with unknown completeness that were fail-safe (safety function not lost)
9. Failures with unknown completeness and unknown impact on the safety function.

Failures in Categories 3, 7, and 9 were, potentially, complete failures with the safety function lost.

In past NRC system studies, uncertainties in data classification or the number of failures or demands have been modeled by explicitly assigning a probability for every possible scenario in the uncertain data. The data set for each scenario was analyzed, and the resulting output distributions were combined as a mixture distribution, weighted according to the assigned probabilities. This process was used to account for uncertain demands for system restart in the High Pressure Core Injection Study (Reference A-1), and to account for whether certain failures to run occurred in the early, middle, or late period in the Emergency Diesel Generator Study (Reference A-2). This method has also been described in the literature (see References A-14 through A-16).

For each component in the RPS study, too many possible combinations of outcomes exist to separately enumerate each one. There are three types of uncertain data, and in some cases over 100 uncertain events for a component. Therefore, the well-known Monte Carlo simulation method was used to assess the impact of the uncertain failures. Probabilities were assigned for whether to treat

each set of uncertain failures as complete failures with the safety function lost. After sampling from probability distributions based on the assigned probabilities, the failure probability or failure rate of the RPS component being studied was characterized as described in Section A-2.1.2. This process was repeated 1000 times, and the variation in the output was used to assess the overall uncertainty for the failure probability or failure rate. As with the previous NRC system uncertainty models, the resulting output distributions were combined as a mixture distribution. Since these distributions arise from simulations, they were equally weighted in forming the final output distribution.

More details on the selection of the probabilities, the nature of the simulations, and the combining of the output distributions are presented in the subsections below.

A-2.1.3.1. Selection of Uncertainty Distributions. Three uncertainties were considered, corresponding to Categories 3, 7, and 9 in the list above. Probabilities for these events were developed using engineering judgment, as follows.

The average or best estimate of the probability that the safety function was lost was estimated from the data in each data set. Among complete failures, the ratio of the number of events with known safety function lost to events with safety function either known to be lost or known to be fail-safe was used for the probability of counting a complete event with uncertain safety function loss. Similarly, among failures with uncertain completeness, a probability of the safety function actually being lost in questionable cases was estimated by the ratio of the number of events with known safety function lost to events with safety function either known to be lost or known to be fail-safe, among events with uncertain completeness.

For the probability that an event with uncertain completeness would be a complete loss of the safety function of the component, 0.5 was the selected mean value. This choice corresponds to the assessments of the engineers reviewing the failure data. For the uncertain events under consideration, the assessment was that the probability of complete function loss among similar events is closer to 0.5 than to 1.0 or to a value less than or equal to 0.1.

In the simulations, beta distributions were used to model uncertainty in these probabilities. More specifically, the family of constrained noninformative distributions described under Alternate Methods in Section A-2.1.2 was selected. For both the probability of the safety function being lost and the probability of complete losses, the maximum entropy distribution constrained to have the specified mean probability was selected. The maximum entropy property results in a broad distribution; for the probability of an event with uncertain completeness being complete, the 5^{th} and 95^{th} percentile bounds are, respectively, 0.006 and 0.994. Thus, these distributions model a range of probabilities for the uncertain data attributes.

For events in Category 9, for which both the safety function status and the completeness were unknown, the probability of complete failures with loss of the safety function was taken to be the product of the two separate probabilities. While the completeness and safety function loss status may not be completely independent among events with both attributes unknown, use of the product ensures that the modeled probability for these events will be as low, or lower, than the probability that the events with only one uncertain factor were complete losses of the safety function.

A-2.1.3.2. Nature of the Simulations. The simulations occurred in the context of the ordinary statistical analysis described in Sections A-2.1.1 and A-2.1.2. The first step in completing the analysis was to identify the best data subset, using the methods of Section A-2.1.1. The variation in the data was bounded by completing the analysis of Section A-2.1.1 using two cases:

- Lower bound case: counting no uncertain failures.
- Upper bound case: counting all uncertain failure (i.e., counting all the failures in Categories 3, 7, and 9 as complete losses of the safety function).

When differences were found between data sets in either of these bounding analyses, the differences were preserved for the simulation. That is, a subset was selected to best represent a RPS component's failure probability or failure rate for Combustion Engineering plants if the rules given in Section A-2.1.1 applied in either the upper bound or the lower bound case.

In the simulation, the selected data subset was analyzed using the simple Bayes method and also the empirical Bayes method for differences between plants and years. In each iteration, the data set itself differs according to the number of uncertain failures included. That is, for each selected set of data, the simulation proceeds as follows. First, a simulated number of failures was calculated for each combination of plant, year, plant mode, and method of discovery present in the data. Then, a simple Bayes or empirical Bayes distribution was sought. The results were saved and combined, as described in the next subsection.

The calculation of the simulated number of failures was simple. Suppose a cell of data (plant/year/plant operational mode/method-of-discovery combination) had f failures that were known to be complete losses of the safety function, s failures for which the impact on the safety function was unknown, c failures for which the completeness was unknown, and b failures for which both the safety function impact and completeness were unknown. In the simulation, a p_{sc} for complete failures with unknown safety function status and a p_{su} for unknown completeness failures with unknown safety function status were obtained by sampling from the beta distributions discussed above. A p_c was obtained by sampling from the beta distribution discussed above with mean 0.5. A simulated number of failures with the safety function lost among the s failures with unknown impact was obtained by sampling from a binomial distribution with parameters s and p_{sc}. Here, the first parameter of a binomial distribution is the number of opportunities for an outcome, and the second is the probability of the outcome of interest in each independent trial. Similarly, a simulated number of complete failures among the c failures with unknown completeness was obtained by sampling from a binomial distribution with parameters c and p_c. A simulated number of complete failures with safety function lost was generated from among the b failures with both uncertainties by sampling from a binomial distribution with parameters b and $p_{su}*p_c$. The total number of failures for the cell was f plus the values obtained from sampling from the three binomial distributions. This process was repeated for each cell of data.

A-2.1.3.3. Combining Output Distributions. The resulting beta or gamma distributions from the simulation cases were weighted equally and combined to produce distributions reflecting both the variation between plants or other specifically analyzed data sources, and the underlying uncertainty in the two attributes of the classification of the failure data. Two details of this process bear mention.

In some of the simulated data sets, empirical Bayes distributions were not fitted to the data; the maximum likelihood estimates of the empirical Bayes distribution parameters did not exist. An outcome of the simulation was the percentage of the iterations for which empirical Bayes distributions were found. When no empirical Bayes distribution was fit to the simulated data, the simulated data were treated as being homogenous. The simple Bayes method represented the data using the updated Jeffrey's noninformative prior distribution. The mean was taken to be the number of simulated failures plus 0.5, divided by the number of demands plus 1 (for probabilities) or by the exposure time (for rates). The resulting distribution goes into the mix along with the other distributions computed for the attribute under study in the simulations.

For each studied attribute, the simulation distributions were combined by matching moments. A lognormal distribution was obtained that has the same mean and variance as the mixture distribution arising from the simulation.

An option in the last step of this analysis would be to match the mean and the 95th percentile from the simulation instead of the mean and variance. Two lognormal distributions can generally be found that match a specified mean and upper 95th percentile (the error factors are roots of a quadratic equation). For the RPS data, the 95th percentiles from the simulation were relatively low, and the mean and upper bound match led to unrealistic error factors (generally less than 1.5 or greater than 100). Therefore, lognormal distributions that matched the means and variances of the simulation data were used rather than distributions based on the mean and 95th percentiles.

A-2.2 The Combination of Failure Modes

The failure mode probabilities were combined to obtain the unavailability. The primary tool in this assessment was the SAPHIRE analysis of the fault trees for the four CE plant model groups (with analog or digital core protection calculators, and two different reactor trip breaker/contactor configurations in each of these categories).

Algebraic methods, described briefly here, were used to compute overall common-cause failure probabilities and their associated uncertainties. The CCF probabilities were linear combinations of selected high-order CCF alpha factors, multiplied by the total failure probability or rate coming from the analysis of Section A-2.1. The CCF alpha factors, described in Appendix E, indicate the probability that, given a failure, a particular number of redundant components will fail by common-cause. For example, the probability of 6 of 8 components failing depends on the alpha factors for levels 6, 7, and 8. The linear combination of these terms was multiplied by Q_T, the total failure probability, to get the desired common-cause failure probability.

The following algebraic method is presented in more generality by Martz and Waller.[A-17] The CCF probability was an expression of the form

(aX+bY)*Z

where X, Y, and Z are events or failure modes or alpha factors that each had an uncertainty distribution, and a and b are positive constants between 0 and 1 that reflect a subset of CCF events

of a given order meeting the particular criterion of the RPS fault tree. A combined distribution was obtained by repeatedly rewriting the expression using the facts that

Prob(kA) = k Prob(A) for the subsetting operation

Prob(A*B) = Prob(A and B) = Prob(A)*Prob(B)

Prob(A+B) =Prob(A or B) = 1 - Prob(not A)*Prob(*not* B) = 1 - [1 - Prob(A)]*[1 - Prob(B)]

where A and B are any independent events. Because the resulting algebraic expressions were linear in each of the failure probabilities, the estimated mean and variance of the combination were obtained by propagating the failure probability means and variances. These means and variances were readily available from the beta distributions. Propagation of the means used the fact that the mean of a product is the product of the means, for independent random variables. Propagation of variances of independent factors was also readily accomplished, based on the fact that the variance of a random variable is the expected value of its square minus the square of its mean.

In practice, estimates were obtained by the following process:

- Compute the mean and variance of each beta distribution
- Compute the mean and variance of the combination for each case using simple equations for expected values of sums for "or" operations and of products for "and" operations
- Compute parameters for the lognormal distribution with the same mean and variance
- Report the mean and the 5th and 95th percentiles of the fitted lognormal distribution.

The means and variances calculated from this process were exact. The 5th and 95th percentiles were only approximate, however, because they assume that the final distribution is a lognormal distribution. Monte Carlo simulation for the percentiles is more accurate than this method if enough Monte Carlo runs are performed, because the output uncertainty distribution is empirical and not required to be lognormal.

A-3. METHODS FOR THE TREND ANALYSIS

Trend analyses were performed for unplanned demands (reactor trips), failures, common cause events, and failures within the data used to estimate the total failure probabilities for the unreliability assessment. In each set of data, the failures or events were binned by calendar year along with the associated exposure time. Trends were generally not analyzed, however, in data groupings with fewer than five failures or with fewer than three years in the study period with at least one failure.

Rates were tested for log trends. The log model is preferred over a simple linear model because it does not allow the data to be negative. The log model trends were fitted using the SAS procedure, "GENMOD," which fits *generalized linear models.*[A-18] In these models, a probability structure is assumed for the data, and a linear model [e.g., log(rate)=a + b t] applies to the mean of the rates rather than to the rates themselves. Parameters in these models are estimated by

maximizing the likelihood of the observed data assuming the specified structure, rather than by minimizing the sum of the squares of the differences between observed and model-predicted rates. The GENMOD rate model is based on the assumptions of random occurrences in time (as in a Poisson process). It thus allows the significance of the trend line to be estimated without requiring the assumption of normally-distributed data. A second major advantage of the method over least squares methods is that it uses zero counts for the log model without requiring any adjustment.

The generalized linear model also supports the estimation of simultaneous confidence bounds for the mean of a rate. When the model adequately fits the data, the probability is 0.90 that the true curve describing the mean of the rates across years lies within the plotted band. The method also provides goodness-of-fit tests that show whether the data has the type of variation expected for random event counts. When the data have either much more or much less than expected variation, the model does not fit well. In the case of more variation in the data, the simultaneous confidence band will tend to be tighter than a similar band derived from a model that does fit the data. Since the trend models of this report are primarily for descriptive purposes and for identifying overall patterns, rather than for predictions or other detailed investigations, better-fitting models were not needed. Further technical details of the method are given in Reference A-20.

The final trend analysis was performed on the total failure probabilities (Q_T) used in the unavailability analysis. Common-cause failure probabilities are largely driven by these probabilities, since the CCF probabilities are estimated by multiplying a function of the estimated alpha parameters (which are too sparse for trend analysis) and Q_T. For each component in the unreliability analysis, annual data were trended using the same methods as described above. The failures and demands entering this calculation were from the subset used for the Q_T analysis, with the exception that the entire time period was used even for components for which the unreliability estimates were based on data from the 1990-1995 or 1990-1998 period. The RPS demand count estimates are large in comparison to the failures for these components. Therefore, the trending methods applicable for rates were also applicable to these probabilities, and the demands were treated like the exposure times. The means of the uncertainty distributions were trended, and significant trends were highlighted and plotted using the same regression methods as for the frequencies.

A-4. REFERENCES

A-1. G. M. Grant, W. S. Roesener, D. G. Hall, C. L. Atwood, C. D. Gentillon, and T. R. Wolf, *High Pressure Coolant Injection (HPCI) System Performance, 1987-1993*, INEEL-94/0158, February, 1995.

A-2. G. M. Grant, J. P. Poloski, A. J. Luptak, C. D. Gentillon and W. J. Galyean, *Emergency Diesel Generator Power System Reliability, 1987-1993*, INEEL-95/0035, February, 1996.

A-3. G. M. Grant, J. P. Poloski, C. D. Gentillon and W. J. Galyean, *Isolation Condenser System Reliability*, 1987-1993, INEEL-95/0478, March, 1996.

A-4. J. P. Poloski, G. M. Grant, C. D. Gentillon, W. J. Galyean, W. S. Roesener, *Reactor Core Isolation Cooling System Reliability*, 1987-1993, INEEL-95/0196, September, 1996.

A-5. J. P. Poloski, G. M. Grant, C. D. Gentillon, W. J. Galyean, J. K. Knudsen, *Auxiliary/Emergency Feedwater System Reliability, 1987-1995* (Draft), INEEL/EXT-97-00740, November, 1997.

A-6. J. P. Poloski, G. M. Grant, C. D. Gentillon, and W. J. Galyean, *Historical Reliability of the High-Pressure Core Spray System*, 1987-1993, INEEL/EXT-95-00133, January, 1998.

A-7. George E. P. Box and George C. Tiao, *Bayesian Inference in Statistical Analysis*, Reading, MA: Addison Wesley, 1973, Sections 1.3.4–1.3.5.

A-8. Corwin L. Atwood, *Hits per Trial: Basic Analysis of Binomial Data*, EGG-RAAM-11041, September 1994.

A-9. Harry F. Martz and Ray A. Waller, *Bayesian Reliability Analysis*, Malabar, FL: Krieger, 1991, Section 7.6.

A-10. Corwin L. Atwood, "Constrained Noninformative Priors in Risk Assessment," *Reliability Engineering and System Safety*, 53:37-46, 1966.

A-11. B. Harris, "Entropy," *Encyclopedia of Statistical Sciences, Vol. 5*, S. Kotz and N. L Johnson, editors, 1982, pp. 512–516.

A-12. Robert E. Kass and Duane Steffey, "Approximate Bayesian Inference in Conditionally Independent Hierarchical Models (Parametric Empirical Bayes Models)," *Journal of the American Statistical Association*, 84, 1989, pp. 717–726, Equation (3.8).

A-13. M. E. Engelhardt, *Events in Time: Basic Analysis of Poisson Data*, EGG-RAAM-11088, Sept. 1994.

A-14. H. F. Martz and R. R. Picard, "Uncertainty in Poisson Event Counts and Exposure Time in Rate Estimation," *Reliability Engineering and System Safety*, 48:181-190, 1995.

A-15. C. L. Atwood and C. D. Gentillon, "Bayesian Treatment of Uncertainty in Classifying Data: Two Case Studies," *Proceedings of the ESREL'96/PSAM-III International Conference on Probabilistic Safety Assessment and Management, June 24–28, 1996*, Crete, Greece.

A-16. H. F. Martz, P. H. Kvam, and C. L. Atwood, "Uncertainty in Binomial Failures and Demands with Applications to Reliability," *International Journal of Reliability, Quality, and Safety Engineering*, Vol. 3, No. 1 (1996).

A-17. H. F. Martz and R. A. Waller, "Bayesian Reliability Analysis of Complex Series/Parallel Systems of Binomial Subsystems and Components," *Technometrics, 32*, 1990, pp. 407-416.

A-18. U.S. NRC, *Event Reporting Guidelines 10 CFR 50.72 and 50.73*, NUREG-1022, Rev. 1, Section 3.3.2, January 1998.

A-19. SAS/STAT© Software: The GENMOD Procedure, Release 8.01, SAS Institute, Cary, NC.

A-20. J. P. Poloski, et.al, *Rates of Initiating Events at U. S. Nuclear Power Plants: 1987-1995*, NUREG/CR-5750, February, 1999.

Appendix B

Data Summary

Appendix B
Data Summary

This appendix summarizes the data evaluated in the common-cause failure (CCF) data collection in support of the Combustion Engineering RPS study. Table B-1 lists Combustion Engineering independent failure counts by type of component from the source data files, summarized yearly. Table B-2 lists the Combustion Engineering CCF failure event counts by type of component from the CCF file, again summarized yearly. Table B-3 summarizes in detail the Combustion Engineering CCF events. The tables show only records for components in the dataset.

The data presented in this appendix represent a subset of the data collected and analyzed for this study. The first screening was to exclude data prior to 1984 and to include only data from Combustion Engineering plants. The second screening separated out the components of interest for the RPS study. The following lists the components included in this summary, with a short description of each:

Component	Description
BME	Breaker mechanical
BSN	Breaker shunt trip coil
BUV	Breaker undervoltage coil
CBI	Channel bistable
CPA	Analog core protection calculator
CPD	Digital core protection calculator
CPR	Channel pressure sensor/transmitter
CTP	Channel temperature sensor/transmitter
CRD	Control rod drive mechanism
MSW	Manual scram switch
ROD	Control rod
RYL	Logic Relay
RYT	Trip Relay
TLR	Trip Logic Relay (used in the pooled studies)

The third screening was for the safety function significance of the failure. The data collection classified failures into three categories: fail-safe (FS), which represents a failure that does not affect the component's safety function; nonfail-safe (NFS), which represents a failure of the component's safety function; and unknown (UKN), which represents a failure that cannot be classified as FS or NFS because of insufficient information concerning the failure. Only those failures designated as NFS or UKN are included in these attachments.

The fourth screening was for the failure completeness (degradation) value. Events were categorized as complete failures (CF)(P=1.0), nonfailures (NF)(P=0.1 or lower), or unknown completeness (UC)(P=0.5). Events with failure completeness (degradation) values less than 0.5 are excluded from the counts of independent events in Table B-1.

The Table B-3 headings are listed and described below:

Component	The component three-character identifier.
Fail Mode	Failure mode. The failure mode is a two-character designator describing the mode of failure. The following list shows the failure modes applicable to this report:

FM	Description
IO	Instrument inoperability
IS	Instrument setpoint drift
CO	Breaker fails to open
FO	Functionally failed (applies to RODs)

CCF Number	Unique identifier for each common-cause failure event. For this nonproprietary report, the docket number portion of the CCF number has been replaced with 'XXX'.
Event Year	The calendar year that the event occurred in.
Event Description	The description field for the CCF.
Safety Function	Determination of the type of failure as related to the safety function. Allowable entries are NFS, UKN, and FS.
TDF	Time Delay Factor. The probability that two or more component failures separated in time represent a CCF. Allowable values are between 0.1 and 1.0. (Called the Timing Factor in Appendix E.)
Coupling Strength	The analyst's uncertainty about the existence of coupling among the failures of two or more components. Allowable values are between 0.1 and 1.0. (Called the Shared Cause Factor in Appendix E.)
CCCG	The common-cause component group size.
Shock Type	An indication of whether or not all components in a group can be expected to fail. Allowable entries: 'L' for lethal shock and 'NL' for nonlethal.
Date	The date of the event.
No. Failures	The number of failure events included in the data record.
Degraded Value	This field indicates the extent of each component failure. The allowable values are decimal numbers from 0.0 to 1.0. Coding guidance for different values follows:

1.0 (CF)	The component has completely failed and will not perform its safety function.
0.5 (UC)	The completeness of the component failure is unknown.
0.1 (NF)	The component is only slightly degraded or failure is incipient.
0.01 (NF)	The component was considered inoperable in the failure report; however, the failure was so slight that failure did not seriously affect component function.
0.0	The component did not fail (given a CCF event).

Table B-1. Combustion Engineering RPS independent failure yearly summary, 1984 to 1998.

SYSTEM	ROD																
Component[a]	**Safety Function**	**1984**	**1985**	**1986**	**1987**	**1988**	**1989**	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**Total**
CRD	UKN							1									1
ROD	NFS					1		1	1						1		4
Summary for 'SYSTEM' = ROD																	
Sum						1		2	1						1		5

SYSTEM	RPS																
Component[a]	**Safety Function**	**1984**	**1985**	**1986**	**1987**	**1988**	**1989**	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**Total**
BME	NFS									1		1					2
BSN	NFS	2					2										4
BUV	NFS	3			3	3	1	1	1	2							14
BUV	UKN			1					1	1							3
CBI	NFS	6	12	5	9	8	1	1	5	4	2	3	2				58
CBI	UKN	2	3		1	4	1	1		1							13
CPA	NFS	3			3	3	2	3		1	3		2				20
CPA	UKN	1	1		4	1	2		1	1		1	2				14
CPD	NFS	1	9	10	7	19	5	1	7		7	2	2				70
CPD	UKN	2	1	3	6	2			1	1			1				17
CPR	NFS	3	1		1	2				1			1				9
CPR	UKN	2	1	4	1	1	2	1		1		1	1				15
CTP	NFS	3		1	4		3	3	3	3	1		1				22
CTP	UKN	3	1	3	2	1	1			2	1	2	1				17
MSW	NFS	1										1					2
RYL	NFS			1							1						2
RYL	UKN	3	3	1	1		2	1									11
RYT	NFS			1									1				2
Summary for 'SYSTEM' = RPS																	
Sum		35	32	30	42	44	22	12	19	19	15	11	14				295

a. Components listed are those that have failure records with degradation values greater than 0.1.

Table B-2. Combustion Engineering RPS common-cause failure yearly summary, 1984 to 1998.

SYSTEM	RPS																
Component[a]	**Safety Function**	**1984**	**1985**	**1986**	**1987**	**1988**	**1989**	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**Total**
BME	NFS	1	2														3
BSN	NFS	1															1
BUV	NFS			1													1
BUV	UKN		1														1
CBI	NFS	4	4	5	3	1		3		1		1	1				23
CBI	UKN		1		1				1	1							4
CPA	NFS	1									1		1				3
CPA	UKN						2			1			1				4
CPD	NFS		1	1	1		1										4
CPD	UKN	1	2	1	1												5
CPR	NFS	1	1		1						1						4
CPR	UKN	1								1							2
CTP	NFS	1	4		1			1			1						8
CTP	UKN			2													2
Summary for 'SYSTEM' = RPS																	
Sum		11	16	10	8	1	3	4	1	4	3	1	3				65
Study Total		11	16	10	8	1	3	4	1	4	3	1	3				65

a. Components listed are those that have CCF records.

Table B-3. Combustion Engineering RPS common-cause failure detailed summary, 1984 to 1998.

Component	Fail Mode	CCF Number	Event Year	Event Description	Safety Function	TDF	Coupling Strength	CCCG	Shock Type	Date	No. Failures[a]	Degraded Value
BME	CO	N-XXX-84-1118-CO	1984	BREAKERS DID NOT CHANGE STATE IN THE REQUIRED	NFS	0.10	0.50	8	NL	9/25/1984	1	0.10
										7/13/1984	1	0.10
BME	CO	N-XXX-85-1120-CO	1985	RTB FAILED (UV) TIME RESPONSE TIME TEST, FRONT FRAME	NFS	0.10	1.00	8	NL	4/8/1985	1	0.10
										2/19/1985	1	0.10
BME	CO	N-XXX-85-1104-CO	1985	FRONT FRAME ASSEMBLIES WORN AND LACKING LUBRICATION	NFS	1.00	1.00	8	NL	1/3/1985	1	0.10
										1/3/1985	1	0.10
BSN	CO	L-XXX-84-1094-CO	1984	DISCONNECTED LEADS REMOVED THE AUTOMATIC SHUNT TRIP FEATURE	NFS	1.00	1.00	8	NL	2/27/1984	4	1.00
BUV	CX	L-XXX-85-1090-CX	1985	ARMATURES ON UV DEVICES FOR TCBS 4 AND 8 WERE IN A MID-POSIT	UKN	1.00	0.50	8	NL	12/17/1985	2	0.10
BUV	CO	N-XXX-86-1121-CO	1986	UNDER VOLTAGE DEVICE ARMATURE EXTENSION DID NOT PICK UP	NFS	0.10	0.50	8	NL	10/31/1986	1	0.10
										9/5/1986	1	1.00
CBI	IS	N-XXX-84-0609-IS	1984	PRE-TRIP BISTABLE SETPOINT HAD DRIFTED	NFS	1.00	0.50	56	NL	8/23/1984	1	0.10
										8/23/1984	1	0.10
CBI	IS	N-XXX-84-0688-IS	1984	CONTAINMENT PRESSURE SWITCHES OOS	NFS	1.00	0.50	48	NL	4/21/1984	1	0.10
										4/21/1984	1	0.10
										4/21/1984	1	0.10
										4/21/1984	1	0.10
CBI	IO	N-XXX-84-0644-IO	1984	TRIP MODULE FAILED TO RESPOND	NFS	1.00	0.10	56	NL	12/4/1984	1	1.00
										12/4/1984	1	1.00
CBI	IO	N-XXX-84-0718-IS	1984	BISTABLE GREATER THAN 15% POWER 'TRIP PERMISSIVE' OUT OF SPE	NFS	1.00	1.00	56	NL	1/13/1984	1	0.10
										1/13/1984	1	0.10
CBI	IS	N-XXX-85-0617-IS	1985	TRIP (ASGT) TRIP UNIT WAS FOUND OUT OF	NFS	0.50	0.50	56	NL	12/20/1985	1	0.10
										11/25/1985	1	0.10
CBI	IO	N-XXX-85-0611-IO	1985	TRIP UNIT POWER SUPPLYS FOUND UNSTABLE	UKN	1.00	1.00	56	NL	4/10/1985	1	1.00
										4/10/1985	1	1.00
										4/10/1985	1	1.00
										4/10/1985	1	1.00
										4/10/1985	1	1.00
										4/10/1985	1	1.00

Table B-3. Combustion Engineering RPS common-cause failure detailed summary, 1984 to 1998 (continued).

Component	Fail Mode	CCF Number	Event Year	Event Description	Safety Function	TDF	Coupling Strength	CCCG	Shock Type	Date	No. Failures[a]	Degraded Value
										4/10/1985	1	1.00
CBI	IS	N-XXX-85-0614-IS	1985	BISTABLE TRIP UNIT OUT OF SETPOINT CALIBRATION	NFS	1.00	0.50	56	NL	5/6/1985	1	0.10
										5/4/1985	1	0.10
CBI	IS	N-XXX-85-0616-IS	1985	TRIP UNIT'S PRETRIP SETPOINT WAS FOUND OUT OF SPECIFICATION	NFS	1.00	0.50	56	NL	10/25/1985	1	0.10
										10/25/1985	1	0.10
										10/2/1985	1	0.10
										10/2/1985	1	0.10
										9/20/1985	1	0.10
CBI	IS	N-XXX-85-0615-IS	1985	TRIP UNIT SETPOINT OUT OF SPECIFICATION LOW	NFS	1.00	0.50	56	NL	5/25/1985	1	0.10
										5/25/1985	1	0.10
CBI	IO	N-XXX-86-0649-IO	1986	BISTABLE COMPARATOR CARDS FOUND TO BE BAD	NFS	1.00	0.50	56	NL	8/13/1986	1	1.00
										8/13/1986	1	1.00
CBI	IS	N-XXX-86-0618-IS	1986	STEAM GENERATOR TRIP WAS FOUND OUT OF SPECIFICATION HIGH	NFS	0.50	0.50	56	NL	5/14/1986	1	0.10
										5/13/1986	1	0.10
										4/17/1986	1	0.10
CBI	IS	N-XXX-86-0619-IS	1986	TRIP UNIT'S SETPOINT HAD DRIFTED	NFS	1.00	0.50	56	NL	7/16/1986	1	0.10
										7/7/1986	1	0.10
CBI	IO	N-XXX-86-1144-IO	1986	VARIABLE SETPOINT CARDS FOUND TO BE BAD	NFS	1.00	0.50	56	NL	10/7/1986	1	1.00
										9/29/1986	1	1.00
CBI	IS	N-XXX-86-0633-IS	1986	TRIP BISTABLE TRIP UNIT OUT OF SPEC LOW	NFS	0.50	0.50	56	NL	12/17/1986	1	0.10
										11/21/1986	1	0.10
CBI	IO	N-XXX-87-0680-IO	1987	BISTABLE TRIP UNIT DUAL COIL RELAY HAD SHORTED	NFS	1.00	1.00	48	NL	2/21/1987	1	1.00
										2/21/1987	1	1.00
										2/21/1987	1	1.00
CBI	IO	N-XXX-87-0681-IO	1987	BISTABLE TRIP UNIT DUAL COIL RELAY COILS HAD SHORTED TOGETHE	NFS	1.00	1.00	48	NL	3/18/1987	1	1.00
										3/18/1987	1	1.00
										3/18/1987	1	1.00
										3/18/1987	1	1.00
										3/18/1987	1	1.00
										3/17/1987	1	1.00
										3/17/1987	1	1.00
										3/17/1987	1	1.00

Table B-3. Combustion Engineering RPS common-cause failure detailed summary, 1984 to 1998 (continued).

Component	Fail Mode	CCF Number	Event Year	Event Description	Safety Function	TDF	Coupling Strength	CCCG	Shock Type	Date	No. Failures[a]	Degraded Value
										3/17/1987	1	1.00
										3/17/1987	1	1.00
										3/17/1987	1	1.00
CBI	IS	N-XXX-87-0621-IS	1987	BISTABLE TRIP UNIT'S SETPOINTS WERE FOUND OUT OF SPECIFICATI	NFS	1.00	0.50	56	NL	1/27/1987	1	0.10
										1/16/1987	1	0.10
										1/16/1987	1	0.10
										1/16/1987	1	0.10
CBI	IS	N-XXX-87-0634-IS	1987	TRIP BISTABLE TRIP UNIT OUT OF SPEC LOW	UKN	1.00	0.50	56	NL	2/27/1987	1	0.10
										2/27/1987	1	0.10
										2/13/1987	1	0.10
										1/21/1987	1	0.10
										1/21/1987	1	0.10
										1/21/1987	1	0.10
CBI	IO	N-XXX-88-0684-IO	1988	DUAL COIL RELAY COILS HAD SHORTED TOGETHER	NFS	1.00	1.00	48	NL	11/8/1988	1	1.00
										11/8/1988	1	1.00
CBI	IS	N-XXX-90-0735-IS	1990	BISTABLES FOUND OUT OF SPEC. HIGH ON CHANNELS A , B , AND C	NFS	1.00	0.50	56	NL	6/13/1990	1	0.10
										6/13/1990	1	0.10
										6/13/1990	1	0.10
CBI	IS	N-XXX-90-0624-IS	1990	SET POINT WAS OUT OF SPECIFICATION IN THE TRIP UNIT	NFS	1.00	0.50	56	NL	10/9/1990	1	0.10
										10/5/1990	1	0.10
										10/1/1990	1	0.10
										9/28/1990	1	0.10
										9/19/1990	1	0.10
										9/11/1990	1	0.10
										9/8/1990	1	0.10
CBI	IO	L-XXX-90-1149-IO	1990	ALL 4 POWER RANGE BISTABLES WERE FOUND TO BE OOS	NFS	1.00	1.00	56	NL	10/2/1990	4	0.50
CBI	IO	N-XXX-91-0689-IO	1991	DUAL COIL RELAY COILS HAD SHORTED TOGETHER	UKN	1.00	1.00	48	NL	2/17/1991	1	1.00
										2/11/1991	1	1.00
CBI	IS	N-XXX-92-0638-IS	1992	BI-POLAR AMPLIFIER HAD A SLIGHTLY LOW OUT-OF-SURVEILLANCE TE	UKN	0.10	0.50	56	NL	3/13/1992	1	0.10
										3/12/1992	1	0.10
										2/10/1992	1	0.10

Table B-3. Combustion Engineering RPS common-cause failure detailed summary, 1984 to 1998 (continued).

Component	Fail Mode	CCF Number	Event Year	Event Description	Safety Function	TDF	Coupling Strength	CCCG	Shock Type	Date	No. Failures[a]	Degraded Value
CBI	IS	N-XXX-92-0639-IS	1992	TRIP UNIT HAD DRIFTED SLIGHTLY OUT OF SURVEILLANCE TEST SPEC	NFS	1.00	0.50	56	NL	4/10/1992	1	0.10
										4/8/1992	1	0.10
CBI	IO	N-XXX-94-0687-IO	1994	THE STEAM GENERATOR LOW LEVEL BISTABLE TRIP UNIT DID NOT SHU	NFS	1.00	1.00	48	NL	10/5/1994	1	0.50
										10/4/1994	1	0.50
CBI	IO	L-XXX-95-0589-IO	1995	NONE OF THE FOUR CONTAINMENT HIGH PRESSURE CHANNELS WOULD IN	NFS	1.00	1.00	56	NL	7/28/1995	4	1.00
CPA	IS	N-XXX-84-0631-IS	1984	CALCULATOR MINIMUM HIGH POWER TRIP SETPOINT VOLTAGE OUT OF S	NFS	1.00	0.50	12	NL	12/18/1984	1	0.10
										12/18/1984	1	0.10
CPA	IS	N-XXX-89-0732-IS	1989	A FAULTY DUAL AMPLIFIER MODULES FOUND WITHIN THE CORE PROTEC	UKN	1.00	0.50	4	NL	3/5/1989	1	0.50
										3/5/1989	1	0.50
CPA	IO	N-XXX-89-0733-IO	1989	DUAL AMPLIFIER MODULES FOUND BAD	UKN	1.00	0.50	4	NL	3/15/1989	1	1.00
										3/14/1989	1	1.00
										3/13/1989	1	1.00
										3/6/1989	1	1.00
CPA	IO	N-XXX-92-0729-IO	1992	FLUX TRIP INTEGRATOR CALCULATOR DRAWER WAS NOT PRODUCING ANY	UKN	1.00	0.50	12	NL	4/7/1992	1	1.00
										4/7/1992	1	1.00
										4/7/1992	1	1.00
										4/7/1992	1	1.00
										4/7/1992	1	1.00
										4/7/1992	1	1.00
CPA	IO	N-XXX-93-0700-IO	1993	COMPUTATION MODULE HAD FAILED	NFS	1.00	0.50	12	NL	9/9/1993	1	1.00
										9/9/1993	1	1.00
CPA	IO	N-XXX-95-0701-IO	1995	18 VOLT POWER SUPPLY VOLTAGE BELOW THE ACCEPTABLE TOLERANCE	NFS	0.50	1.00	4	NL	2/22/1995	1	1.00
										2/9/1995	1	0.50
CPA	IO	N-XXX-95-0703-IO	1995	TRIP CALCULATOR DRAWER POTENTIOMETER WOULD NOT ADJUST AS REQ	UKN	1.00	0.50	4	NL	12/30/1995	1	1.00
										12/28/1995	1	1.00
										12/26/1995	1	1.00
CPD	IO	N-XXX-84-0691-IO	1984	CPC / CEAC INDICATED CHANNEL PROBLEMS	UKN	1.00	0.50	12	NL	11/14/1984	1	1.00

Table B-3. Combustion Engineering RPS common-cause failure detailed summary, 1984 to 1998 (continued).

Component	Fail Mode	CCF Number	Event Year	Event Description	Safety Function	TDF	Coupling Strength	CCCG	Shock Type	Date	No. Failures[a]	Degraded Value
										11/10/1984	1	1.00
CPD	IO	N-XXX-85-0645-IO	1985	CORE PROTECTION CALCULATOR WAS FOUND TO READ LOW	UKN	0.50	0.50	4	NL	5/1/1985	1	1.00
										4/15/1985	1	1.00
CPD	IO	N-XXX-85-0694-IO	1985	(CPC / CEAC) HAD INTERMITTANT MEMORY PARITY ERRORS	NFS	1.00	1.00	4	NL	11/19/1985	1	1.00
										11/12/1985	1	1.00
										11/9/1985	1	1.00
CPD	IO	N-XXX-85-0693-IO	1985	CPC/CEA POWER SUPPLY HAD REACHED ITS END OF	UKN	0.50	0.50	12	NL	10/8/1985	1	1.00
										9/8/1985	1	1.00
CPD	IS	N-XXX-86-0647-IS	1986	PUMP INPUT WOULD NOT ADJUST, CORE PROTECTION CALCULATOR	NFS	1.00	0.50	4	NL	6/23/1986	1	0.50
										6/18/1986	1	0.50
CPD	IO	N-XXX-86-0650-IO	1986	CONTROL ELEMENT ASSEMBLY CALCULATOR WAS NOT OPERATING	UKN	1.00	0.50	4	NL	9/10/1986	1	1.00
										9/9/1986	1	1.00
CPD	IO	N-XXX-87-0669-IO	1987	(CPC / CEAC) DATA LINK FAILED	NFS	1.00	0.50	4	NL	9/23/1987	1	1.00
										9/19/1987	1	1.00
CPD	IO	N-XXX-87-0656-IO	1987	CEAC DEVIATION SENSOR FAILED	UKN	1.00	1.00	12	NL	9/9/1987	1	0.50
										9/9/1987	1	0.50
CPD	IO	N-XXX-89-0671-IO	1989	CORE PROTECTION CALCULATOR (CPC) FAILED DURING PERFORMANCE	NFS	1.00	0.50	4	NL	8/15/1989	1	1.00
										8/14/1989	1	1.00
CPR	IS	N-XXX-84-0629-IS	1984	PRESSURE TRANSMITTER HAD DRIFTED LOW	NFS	1.00	0.50	16	NL	6/24/1984	1	0.10
										6/24/1984	1	0.10
										6/24/1984	1	0.10
CPR	IS	N-XXX-84-0630-IS	1984	SPAN OF THE TRANSMITTER HAD DRIFTED	UKN	1.00	0.50	16	NL	7/14/1984	1	0.10
										7/14/1984	1	0.10
CPR	IS	L-XXX-85-0587-IS	1985	7 PZR PRESSURE TRANSMITTERS WERE OUT OF THE REQUIRED CALIBRA	NFS	1.00	0.50	16	NL	9/14/1985	7	0.10
CPR	IS	N-XXX-87-1441-IS	1987	PRESSURE TRANSMITTERS OUT OF SPECIFICATION LOW	NFS	1.00	0.50	16	NL	3/31/1987	1	0.10
										3/31/1987	1	0.10
CPR	IS	N-XXX-92-0724-IS	1992	POWER SUPPLY WAS FOUND TO HAVE HIGH OUT OF SPECIFICATION AC	UKN	1.00	0.50	16	NL	3/4/1992	1	0.10
										2/3/1992	1	0.10

Table B-3. Combustion Engineering RPS common-cause failure detailed summary, 1984 to 1998 (continued).

Component	Fail Mode	CCF Number	Event Year	Event Description	Safety Function	TDF	Coupling Strength	CCCG	Shock Type	Date	No. Failures[a]	Degraded Value
										2/3/1992	1	0.10
										2/3/1992	1	0.10
										2/3/1992	1	0.10
										2/1/1992	1	0.50
CPR	IO	N-XXX-93-0641-IO	1993	STEAM GENERATOR PRESSURE HAD FAILED HIGH DUE TO A FAILED HIG	NFS	1.00	0.50	16	NL	5/10/1993	1	1.00
										5/10/1993	1	1.00
CTP	IO	L-XXX-84-0593-IO	1984	12 RTDS EXCEEDED THE TECH SPEC LIMIT OF 8 SECS	NFS	1.00	1.00	16	NL	2/13/1984	12	0.10
CTP	IS	N-XXX-85-0613-IS	1985	TEMPERATURE TRANSMITTER'S SPAN HAD DRIFTED LOW	NFS	1.00	0.50	16	NL	5/1/1985	1	0.10
										5/1/1985	1	0.10
CTP	IO	N-XXX-85-0722-IO	1985	RESISTANCE TEMPERATURE DETECTORS HAD A CRACK IN IT DUE TO MA	NFS	1.00	1.00	16	NL	6/28/1985	1	0.10
										6/28/1985	1	0.10
										6/28/1985	1	0.10
										6/25/1985	1	1.00
CTP	IO	N-XXX-85-0728-IO	1985	RESISTANCE TEMPERATURE DETECTORS FOUND TO PRODUCE INTERMITTE	NFS	1.00	0.50	12	NL	9/7/1985	1	1.00
										9/7/1985	1	1.00
CTP	IO	N-XXX-85-0646-IO	1985	RESISTANCE TEMPERATURE DETECTOR HAD FAILED	NFS	1.00	0.50	16	NL	7/30/1985	1	1.00
										7/30/1985	1	1.00
CTP	IS	N-XXX-86-0652-IS	1986	TEMPERATURE TRANSMITTERS OUT OF CALIBRATION	UKN	1.00	0.50	16	NL	10/3/1986	1	0.10
										10/3/1986	1	0.10
										10/3/1986	1	0.10
CTP	IS	N-XXX-86-0651-IS	1986	TEMPERATURE TRANSMITTERS OUT OF CALIBRATION	UKN	1.00	0.50	16	NL	9/29/1986	1	0.10
										9/29/1986	1	0.10
										9/29/1986	1	0.10
CTP	IS	N-XXX-87-0657-IS	1987	THREE TEMPERATURE TRANSMITTERS IN THE CPC CHANNEL 'B' WERE O	NFS	1.00	0.50	16	NL	12/29/1987	1	0.10
										12/29/1987	1	0.10
										12/29/1987	1	0.10
CTP	IO	N-XXX-90-0736-IO	1990	RTDS FAILED ITIME RESPONSE TEST	NFS	1.00	1.00	16	NL	9/11/1990	1	0.50
										9/11/1990	1	0.50
CTP	IO	N-XXX-93-0699-IO	1993	HOT LEG TEMPERATURE DETECTOR HAD FAILED WITH AN OPEN CIRCUIT	NFS	1.00	1.00	16	NL	11/27/1993	1	1.00
										11/27/1993	1	1.00

Note: a. This value represents the number of failures in the event record that is part of the CCF.

Appendix C

Quantitative Results of Basic Component Operational Data Analysis

Appendix C

Quantitative Results of Basic Component Operational Data Analysis

This appendix displays relevant RPS component counts and the estimated probability or rate for each failure mode, including distributions that characterize any variation observed between portions of the data. The analysis is based primarily on data from Combustion Engineering plants during the period 1984 through 1998. However, since relatively few CE plants exist, and similar components exist in the RPS system for other PWR plants, the data were supplemented with data from other PWR vendors when such data were applicable and the CE data were sparse.

Table C-1 lists the components from the RPS unreliability analysis whose total failure probability or rate was estimated from the failure data. The components are listed in sequence across the RPS, beginning with the channel sensor/transmitters and core protection calculator, then the channel bistables, then the logic relays, trip relays, breakers, and rods. For each quantity that is to be estimated, the CE operational data experience is listed (failures and demands or operating times). When fewer than three failures were observed, and other PWR vendors have possibly relevant failure data, the table contains additional rows showing the operational experience with all PWRs, CE and B&W data combined, and CE and Westinghouse data combined.

The quantitative analysis of the RPS failure data was also influenced by the uncertainty in the number of complete failures for which the safety function of the associated component was lost. In each row in Table C-1, a range is given for the number of failures when uncertain failures occurred.

Additional columns in Table C-1 show the results of statistical tests on whether the vendor data can be pooled. In the final column, the vendor data set selected for the analysis of this study is specified. The conclusion of the vendor analysis is that pooling for CE data will be done for manual switch failures, for breaker mechanical failures, and for failures associated with control rods/drives. The pooling is over all three PWR vendors, unless the statistical tests show one vendor to be different from CE and the third vendor.

A final comment with regard to pooling across vendors is that the determination is made at the level of a particular estimate for the unreliability analysis. Each estimate identifies a different failure mode or way for the RPS system to become degraded. Thus, for example, the three breaker-related components are treated in two different ways. CE data are combined with B&W data for the mechanical part of the breaker, but are not combined with other vendors for the shunt trip and the undervoltage trip. CE and B&W have similar data for the mechanical part of the breaker and the CE data set is sparse, so pooling is considered. The CE data sets for shunt and UV trips each contain at least three complete failures. Thus, these sets are not regarded as sparse. Therefore, because the failure mode behaves differently, different estimations are used for the CE trip breaker performance.

Table C-1. Vendor differences applicable to CE RPS components used in the PRA (upper failure count includes uncertain failures).

Comp. code	Component	Data set	Vendor(s) [a]	Failures [b]	Demands or Years	Test Statistic P-value [c]	Conclusion
Channel components							
CPR	Pressure sensor/ transmitter	Cyclic and quarterly testing failures and demands	C	8 to 19	11,188 d	—	No need to pool. Use C data alone.
		Occurrences in time	C	6 to 12	2,360.9 y	—	No need to pool. Use C data alone.
CTP	Temperature sensor/ transmitter	Cyclic and quarterly testing failures and demands	C	9 to 21	12,530 d	—	No need to pool. Use C data alone.
		Occurrences in time	C	11 to 25	2,645.4 y	—	No need to pool. Use C data alone.
CPA	Analog core protection calculator	Cyclic and quarterly testing failures and demands	C	8 to 41	1,524 d	—	No need to pool. Use C data alone.
		Occurrences in time	C	3 to 11	380.5 y	—	No need to pool. Use C data alone.
CPD	Digital core protection calculator	Cyclic and quarterly testing failures and demands	C	23 to 37	1,171 d	—	No need to pool. Use C data alone.
		Occurrences in time	C	38 to 68	292.9 y	—	No need to pool. Use C data alone.
CBI	Bistable	Quarterly testing failures and demands	C	45 to 76	37,453 d	—	No need to pool. Use C data alone.
Trains (trip logic)							
RYL	Logic relay	Quarterly testing failures and demands	C	2 to 8	16,160 d	—	Use C data alone (higher failure probability than other vendors)
			BCW	45 to 58	849,025 d	<1.E-5 (all f.)	
			CB	3 to 9	74,504 d	<=0.01	
			CW	44 to 57	790,682 d	<1.E-5 (all f.)	
RYT	Trip relay	Quarterly testing failures and demands	C	1 to 2	16,160 d	—	Used in CE RPS. Not comparable with other vendors.
MSW	Manual scram switch	Manual trips & quarterly testing failures and demands	C	1	3,426 d	—	Pool data from all three PWR vendors
			BCW	2	19,790 d	0.23	
			CB	1	5,538 d	1.0 [d]	
			CW	2	17,677 d	0.35	

Table C-1. (Continued)

Comp. code	Component	Data set	Vendor(s) [a]	Failures [b]	Demands or Years	Test Statistic P-value [c]	Conclusion
Reactor trip breakers							
BME	Breaker mechanical	Trips and quarterly and monthly testing failures and demands	C	1	42,013 d	—	Pool C and B data
			BCW	4 to 6	113,585 d	0.006 (all f)	
			CB	1	83,813 d	1.0	
			CW	4 to 6	71,785 d	0.05 (all f)	
BSN	Breaker shunt device	Quarterly testing failures and demands (6 tests per quarter)	C	3 to 4	25,270 d	—	No need to pool. Use C data alone.
BUV	Breaker undervoltage coil	Monthly testing failures and demands	C	10 to 18	12,635 d	—	No need to pool. Use C data alone.
Control rod drive and rod							
RMA	Control rod drive and rods	Trips and cyclic testing failures and demands	C	1 to 3	58,006 d	—	Pool B, C, and W data.
			BCW	1 to 5	189,536 d	>0.10	
			CB	1 to 3	77,092 d	>0.58	
			CW	1 to 5	170,450 d	>0.17	

Notes:

a. B = Babcock and Wilcox; C = Combustion Engineering, W = Westinghouse.

b. When a range is given, the lower number is the number of certain failures (complete, with safety function lost), and the upper number is the upper bound that counts all the failures, including the ones with unknown completeness and/or unknown safety impact.

c. Low p-values (<0.05) show data that should not be pooled. When certain failures and all failures differ, there are two possible p-values. If both are relatively high, showing no observed difference between the vendors, the result is stated as greater than or equal to the lower of the two values. Conversely, if both are near zero, showing data that should not be pooled, the result is stated as less than or equal to the larger of the values. If one of the p-values is low, showing data that should not be pooled, that value will be cited with a parethetical note on which case it was ("failures," or "all f").

d. When only two groups are compared, one with no failures and the other with one failure, and the group with no failures has less demands than the other group, the p-value will always be 1.0. The group with no failures has insufficient data to be able to discern a difference in the two groups.

Table C-2 breaks down the failures within the selected vendor groups for each component. It shows the number of events fully classified as known, complete failures, and the number of uncertain events within various subsets of the data. Within each component grouping, subsets in Table C-2 are based on the assessed method of discovery and the plant status (operations or shutdown) for each event (note that uncertainty in these two attributes of the data was not quantified in the data assessment). In addition, rows in Table C-2 show breakdowns for whether the failures occurred during the first part of the study period (1984–1989) or during the second part (1990–1998). For testing data, the second part range is 1990–1995, since only CE and B&W LER data were available for 1996–1998.

The choice of the most representative subset of data to use for each component for the fault tree was a major part of the statistical data analysis. Where operations and shutdown data differ significantly, the subset of operations data was selected, since the unavailability analysis describes risk during operations. Similarly, when the newer data differed significantly from the data earlier in the study period, the newer data were used for the analysis. The analysis also considered whether the test data and data from unplanned scrams differ, for the limited number of components that are always demanded in a trip and whose failures would be detected. Rules for subset selection are discussed further in Section 2.1.1 of Appendix A.

Tables C-1 and C-2 show that the observed number of failures for each component potentially lies between two bounds: a lower bound that excludes all the uncertain failures, and an upper bound that includes them. The initial analysis of the RPS failure data, to select the subsets, was based on these two extreme cases. The next four tables present information on how the subsets were selected using these two sets of data. Figure C-1 overviews the selection process and how the results feed into these tables.

As shown in Figure C-1, the analysis first considered the lower bound (LB) case of no uncertain failures. These data correspond to the first failure count in Table C-1. Table C-3 provides these counts for several subsets, along with the associated denominators and simple calculated probabilities or rates. It also gives confidence bounds for the estimates. Note that the confidence bounds do not consider any special sources of variation (e.g., year or plant). The maximum likelihood estimates and bounds are presented for simple comparisons. They are not used directly in the unavailability analysis.

Table C-4 summarizes the results from testing the hypothesis of constant probabilities or, as applicable, constant rates, across groupings for each basic component failure mode in the RPS fault trees having data. The table provides probability values (p-values) for the hypothesis tests, rounded to the nearest 0.001. When the hypothesis is rejected, the data show evidence of variation. The tests are for possible differences based on method of discovery or data source (unplanned reactor trips or testing), on plant mode (operations or shutdown), on the time period (1984–1989 versus 1990–1995), on different plant units, and on different calendar years. Like Table C-3, Table C-4 applies to the LB data. The results are subdivided according to the method of discovery whenever this distinction is applicable. In the table, finding empirical Bayes distributions for differences in plant mode or finding a p-value less than 0.05 for differences in plant mode resulted in the generation of lines describing the operational and shutdown data separately. Similarly, a finding of an empirical Bayes distribution or small p-value in the time period data groupings produced additional separate evaluations of the older and more recent data.

In Table C-4, low p-values point to variation and lack of homogeneity in the associated data groupings. For example, in Table C-4 the entire row of p-values for data from quarterly tests of CE digital core protection calculators is marked as "<5.E-4." The first of these values indicates that the data

Table C-2. Summary of RPS total failure counts and weighted average total failures (independent and common-cause failures) for PWR vendor groups used in the CE unavailability analysis.

Basic event (component)	Data set[a]	Lower bound: known failures only	Uncertain failure counts			Upper bound: all failures counted	Total failure weighted average[b]
			Uncertain loss of safety function	Uncertain complete-ness	Both uncertainties		
Channel components							
Pressure sensor/ transmitter (CPR)	C cyclic and quarterly tests	8	3	1	7	19	13.7
	—(op)	1	1	0	3	5	2.3
	—(s/d)	7	2	1	4	14	10.9
	(1984-1989)	2	2	1	4	9	5.3
	—(1984-1989 op)	1	1	0	3	5	2.3
	—(1984-1989 s/d)	1	1	1	1	4	2.6
	(1990-1995) (all s/d)	6	1	0	3	10	7.7
	C occurrences in time	6	3	0	3	12	7.1
	—(op)	2	3	0	2	7	2.6
	—(s/d)	4	0	0	1	5	4.3
	(1984-1989)	4	2	0	3	9	4.8
	—(1984-1989 op)	2	2	0	2	6	2.6
	—(1984-1989 s/d)	2	0	0	1	3	2.3
	(1990-1995)	2	1	0	0	3	2.3
	—(1990-1995 op)	0	1	0	0	1	0.1
	—(1990-1995 s/d)	2	0	0	0	2	2.0
Temperature sensor/ transmitter (CTP)	C cyclic and quarterly tests	9	2	7	3	21	15.1
	—(op)	4	2	3	1	10	7.4
	—(s/d)	5	0	4	2	11	7.6

Table C-2. (Continued.)

Basic event (component)	Data set[a]	Lower bound: known failures only	Uncertain failure counts			Upper bound: all failures counted	Total failure weighted average[b]
			Uncertain loss of safety function	Uncertain complete-ness	Both uncertainties		
Temperature sensor/ transmitter, continued	(1984-1989)	6	1	1	0	8	7.2
	—(1984-1989 op)	3	1	0	0	4	3.7
	—(1984-1989 s/d)	3	0	1	0	4	3.5
	(1990-1995)	3	1	6	3	13	8.1
	—(1990-1995 op)	1	1	3	1	6	3.7
	—(1990-1995 s/d)	2	0	3	2	7	4.2
	C occurrences in time	11	8	4	2	25	16.4
	—(op)	8	4	1	1	14	10.0
	—(s/d)	3	4	3	1	11	6.6
	(1984-1989)	8	6	1	2	17	11.4
	—(1984-1989 op)	6	3	1	1	11	7.9
	—(1984-1989 s/d)	2	3	0	1	6	3.6
	(1990-1995)	3	2	3	0	8	5.0
	—(1990-1995 op)	2	1	0	0	3	2.3
	—(1990-1995 s/d)	1	1	3	0	5	2.9
Analog core protection calculator (CPA)	C quarterly tests	8	19	6	8	41	22.9
	—(op)	3	6	3	3	15	8.2
	—(s/d)	5	13	3	5	26	14.9
	(1984-1989)	2	9	2	5	18	10.2
	—(1984-1989 op)	1	4	2	2	9	4.6
	—(1984-1989 s/d)	1	5	0	3	9	5.5
	(1990-1995)	6	10	4	3	23	13.5
	—(1990-1995 op)	2	2	1	1	6	3.7
	—(1990-1995 s/d)	4	8	3	2	17	10.0

Table C-2. (Continued)

Basic event (component)	Data set[a]	Lower bound: known failures only	Uncertain failure counts			Upper bound: all failures counted	Total failure weighted average[b]
			Uncertain loss of safety function	Uncertain complete-ness	Both uncertainties		
Analog core protection calculator, continued	C occurrences in time	3	1	7	0	11	6.7
	—(op)	2	0	6	0	8	5.0
	—(s/d)	1	1	1	0	3	1.9
	(1984-1989)	1	1	6	0	8	4.3
	—(1984-1989 op)	1	0	5	0	6	3.5
	—(1984-1989 s/d)	0	1	1	0	2	0.8
	(1990-1995)	2	0	1	0	3	2.5
	—(1990-1995 op)	1	0	1	0	2	1.5
	—(1990-1995 s/d)	1	0	0	0	1	1.0
Digital core protection calculator (CPD)	C quarterly tests	23	7	1	6	37	31.6
	—(op)	7	2	0	1	10	8.8
	—(s/d)	16	5	1	5	27	23.2
	(1984-1989)	21	6	1	6	34	28.6
	—(1984-1989 op)	6	2	0	1	9	7.8
	—(1984-1989 s/d)	15	4	1	5	25	21.3
	(1990-1995)	2	1	0	0	3	2.8
	—(1990-1995 op)	1	0	0	0	1	1.0
	—(1990-1995 s/d)	1	1	0	0	2	1.8
	C occurrences in time	38	12	15	4	69	54.0
	—(op)	33	7	12	3	55	44.0
	—(s/d)	5	5	3	1	14	10.4
	(1984-1989)	23	10	13	4	50	36.7
	—(1984-1989 op)	20	5	10	3	38	28.9
	—(1984-1989 s/d)	3	5	3	1	12	7.9

Table C-2. (Continued.)

Basic event (component)	Data set[a]	Lower bound: known failures only	Uncertain failure counts			Upper bound: all failures counted	Total failure weighted average[b]
			Uncertain loss of safety function	Uncertain complete-ness	Both uncertainties		
Digital core protection calculator, continued	(1990-1995)	15	2	2	0	19	17.3
	—(1990-1995 op)	13	2	2	0	17	15.2
	—(1990-1995 s/d)	2	0	0	0	2	2.0
Bistable (CBI)	C quarterly tests	45	15	14	2	76	63.7
	—(op)	25	3	6	1	35	30.3
	—(s/d)	20	12	8	1	41	34.7
	(1984-1989)	33	12	4	2	51	45.1
	—(1984-1989 op)	20	3	2	1	26	23.4
	—(1984-1989 s/d)	13	9	2	1	25	22.4
	(1990-1995)	12	3	10	0	25	18.8
	—(1990-1995 op)	5	0	4	0	9	7.0
	—(1990-1995 s/d)	7	3	6	0	16	12.3
Trains (trip logic)							
Logic relay (RYL)	C quarterly tests	2	6	0	0	8	4.1
	—(op)	1	4	0	0	5	2.5
	—(s/d)	1	2	0	0	3	1.8
	(1984-1989)	1	5	0	0	6	2.5
	—(1984-1989 op)	1	3	0	0	4	2.5
	—(1984-1989 s/d)	0	2	0	0	2	0.3
	(1990-1995)	1	1	0	0	2	1.5
	—(1990-1995 op)	0	1	0	0	1	0.3
	—(1990-1995 s/d)	1	0	0	0	1	1.0

Table C-2. (Continued)

Basic event (component)	Data set[a]	Lower bound: known failures only	Uncertain failure counts			Upper bound: all failures counted	Total failure weighted average[b]
			Uncertain loss of safety function	Uncertain complete-ness	Both uncertainties		
Trip relay (RYT)	C quarterly tests (all op)	1	0	1	0	2	1.5
	(1984-1989)	1	0	0	0	1	1.0
	(1990-1995)	0	0	1	0	1	0.5
Manual scram switch (MSW)	PWR quarterly tests and manual scrams (all 1990-1998)	2	0	0	0	2	2.0
	—(op)	1	0	0	0	1	1.0
	—(s/d)	1	0	0	0	1	1.0
Reactor trip breakers							
Breaker mechanical (BME)	Unplanned reactor trips	0	0	0	0	0	0.0
	BC quarterly and monthly tests (1990-1995 op)	1	0	0	0	1	1.0
Breaker shunt device (BSN)	C quarterly tests (1984-1989 op)	3	0	1	0	4	3.5
Breaker undervoltage coil (BUV)	C monthly tests	10	1	5	2	18	13.6
	—(op)	5	1	4	2	12	8.1
	—(s/d)	5	0	1	0	6	5.5
	(1984-1989)	8	0	3	1	12	9.9
	—(1984-1989 op)	4	0	2	1	7	5.4
	—(1984-1989 s/d)	4	0	1	0	5	4.5
	(1990-1995)	2	1	2	1	6	3.7
	—(1990-1995 op)	1	1	2	1	5	2.6
	—(1990-1995 s/d)	1	0	0	0	1	1.0

Table C-2. (Continued.)

Basic event (component)	Data set[a]	Lower bound: known failures only	Uncertain failure counts			Upper bound: all failures counted	Total failure weighted average[b]
			Uncertain loss of safety function	Uncertain complete-ness	Both uncertainties		
Control rod drive and rod							
Control element assembly & rod (RMA)	Unplanned reactor trips (both failures were in 1990-1998) [c]	0	0	2	0	2	1.0
	PWR cyc. tests (all in 1984-1989, s/d)	1	0	2	0	3	2.0

a. NSSS vendor abbreviations: C, CE (only); BC, CE, and B&W pooled; CW, CE, and W pooled; and PWR, B&W, CE, and W all pooled. Testing frequency abbreviations: mon., monthly; qtr., quarterly; cyc., cyclic. The frequency of testing applies to the demand count estimations. The failure data are classified as being discovered on testing, unplanned demands or observation (occurrences in time). Plant status abbreviations: op, operating; s/d, shut down. The stated testing applies to the CE components. Other vendors have different testing schedules for some of the components.

b. Suppose there are NFS = 8 complete failures for a component (CPR, for example) with the safety function lost, and FS = 1 complete fault that is known from the failure reports to be fail-safe. For this report, the estimated probability (pcNFS) of safety function loss for a complete fault with unknown safety impact is (NFS+0.5)/(NFS+FS+1) = 0.85. A similar ratio, (pucNFS), is estimated using the faults with unknown completeness and either known or unknown safety impact. For example, for CPR with 1 safety function lost event with unknown completeness, and 0 fail safe reported events with unknown completeness, (pucNFS) is (1+0.5)/(1+0+1) =0.75. 0.5 was assumed for the completeness probability for an event with uncertain completeness. Therefore, the total failure weighted average is the number of "known failures only" (8 complete and with known safety impact) plus pcNFS times the number (3) of complete failures that might have had a safety impact, plus 0.5 times the number (1) of safety impact failures that might have been complete, plus pucNFS times 0.5 times the number (7) of failures that might have had a safety impact and might have been complete. Thus, for CPR as an example, the total weighted failures is 13.7 = 8 + 3 * 0.85 + 1 * 0.5 + 7 * 0.75 *0.5.

c. The 1996–1998 period considers only CE and B&W demands from trips. Note that any failures that occur during these demands are assumed to be reported in the LERs that explain the reactor trips. This applies to single failures as well as multiple failures. Problems with breakers and control rod drives and rods that occur during trips should be discussed in the LER (they might have a potential common-cause effect).

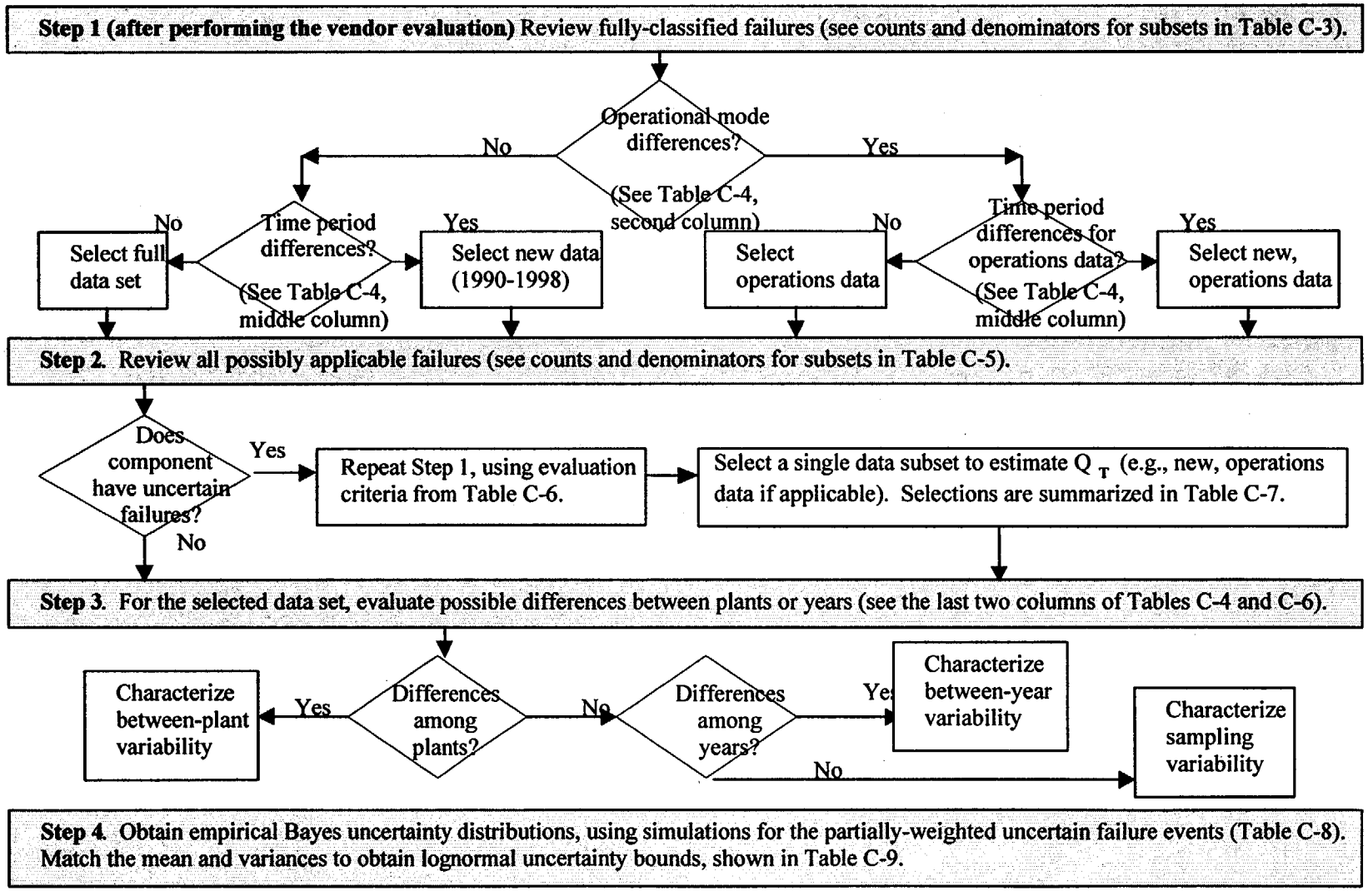


Figure C-1. Decision algorithm for uncertainty distribution selection (applied for each component).

Table C-3. Point estimates and confidence bounds for component groups used in the assessment of CE RPS total failure probabilities and rates (complete failures with safety function lost, only).

Failure mode (component)	Data set	Failures f	Denominator d or T	Probability or rate [a] and 90% confidence interval
Channel components				
Pressure sensor/transmitter (CPR)	C cyclic & qtrly. tests	8	11188	(3.6E-04, 7.2E-04, 1.3E-03)
	C cyclic & qtrly. tests (op)	1	8296	(6.2E-06, 1.2E-04, 5.7E-04)
	C cyclic & qtrly. tests (s/d)	7	2892	(1.1E-03, 2.4E-03, 4.5E-03)
	C tests, 1984-1989 (s/d)	1	1446	(3.5E-05, 6.9E-04, 3.3E-03)
	C tests, 1990-1995 (s/d)	6	1446	(1.8E-03, 4.1E-03, 8.2E-03)
	C occurrences in time	6	2360.9 [c]	(1.1E-03, 2.5E-03, 5.0E-03)
	C occurrences in time (op) [b]	**2** [b]	**1740.4** [b,c]	**(2.0E-04, 1.1E-03, 3.6E-03)** [b]
	C occurrences in time (s/d)	4	620.6 [c]	(2.2E-03, 6.4E-03, 1.5E-02)
Temperature sensor/transmitter (CTP)	C cyclic & qtrly. tests	9	12530	(3.7E-04, 7.2E-04, 1.3E-03)
	C cyclic & qtrly. tests (op)	**4**	**9266**	**(1.5E-04, 4.3E-04, 9.9E-04)**
	C cyclic & qtrly. tests (s/d)	5	3264	(6.0E-04, 1.5E-03, 3.2E-03)
	C occurrences in time	11	2645.4 [c]	(2.3E-03, 4.2E-03, 6.9E-03)
Analog core protection calculator (CPA)	C quarterly tests	8	1524	(2.6E-03, 5.2E-03, 9.5E-03)
	C quarterly tests (op)	**3**	**1082**	**(7.6E-04, 2.8E-03, 7.2E-03)**
	C quarterly tests (s/d)	5	442	(4.5E-03, 1.1E-02, 2.4E-02)
	C occurrences in time	**3**	**380.5** [c]	**(2.2E-03, 7.9E-03, 2.0E-02)**
Digital core protection calculator (CPD)	C quarterly tests	23	1171	(1.3E-02, 2.0E-02, 2.8E-02)
	C quarterly tests (op)	7	894	(3.7E-03, 7.8E-03, 1.5E-02)
	C qtr. tests, 1984-1989 (op)	6	346	(7.6E-03, 1.7E-02, 3.4E-02)
	C qtr. tests, 1990-1995 (op)	**1**	**548**	**(9.4E-05, 1.8E-03, 8.6E-03)**
	C quarterly tests (s/d)	16	277	(3.7E-02, 5.8E-02, 8.6E-02)
	C qtr. tests, 1984-1989 (s/d)	15	153	(6.1E-02, 9.8E-02, 1.5E-01)
	C qtr. tests, 1990-1995 (s/d)	1	124	(4.1E-04, 8.1E-03, 3.8E-02)
	C occurrences in time	38	292.9 [c]	(9.9E-02, 1.3E-01, 1.7E-01)
	C occurrences in time, 1984-1989	23	124.9 [c]	(1.3E-01, 1.8E-01, 2.5E-01)
	C occurrences in time, 1990-1995	**15**	**168.0** [c]	**(5.6E-02, 8.9E-02, 1.3E-01)**
Bistable (CBI)	C quarterly tests	45	37453	(9.2E-04, 1.2E-03, 1.5E-03)
	C quarterly tests (op)	25	27494	(6.3E-04, 9.1E-04, 1.3E-03)
	C qtr. tests, 1984-1989 (op)	20	12232	(1.1E-03, 1.6E-03, 2.4E-03)
	C qtr. tests, 1990-1995 (op)	**5**	**15262**	**(1.3E-04, 3.3E-04, 6.9E-04)**
	C quarterly tests (s/d)	20	9959	(1.3E-03, 2.0E-03, 2.9E-03)
Trains (trip logic)				
Logic relay (RYL)	**C quarterly tests**	**2**	**16160**	**(2.2E-05, 1.2E-04, 3.9E-04)**
Trip relay (RYT)	**C quarterly tests**	**1**	**16160**	**(3.2E-06, 6.2E-05, 2.9E-04)**

Table C-3. (Continued.)

Failure mode (component)	Data set	Failures *f*	Denominator *d* or *T*	Probability or rate [a] and 90% confidence interval
Manual scram switch (MSW)	PWR unplanned trips	0	2222	(0.0E+00, 0.0E+00, 1.3E-03)
	PWR quarterly tests	2	17567	(2.0E-05, 1.1E-04, 3.6E-04)
	PWR pooled trips & tests	**2**	**19789**	**(1.8E-05, 1.0E-04, 3.2E-04)**
Reactor trip breakers				
Breaker mech. (BME)	BC unplanned trips	0	5416	(0.0E+00, 0.0E+00, 5.5E-04)
	BC quarterly tests	1	78397	(6.5E-07, 1.3E-05, 6.1E-05)
	BC pooled trips & tests	**1**	**83813**	**(6.1E-07, 1.2E-05, 5.7E-05)**
Breaker shunt device (BSN)	C quarterly tests	3	25270	(3.2E-05, 1.2E-04, 3.1E-04)
	C quarterly tests, 1984-1989	3	12022	(6.8E-05, 2.5E-04, 6.4E-04)
	C quarterly tests, 1990-1995	**0**	**13248**	**(0.0E+00, 0.0E+00, 2.3E-04)**
Breaker under-voltage coil (BUV)	**C monthly tests**	**10**	**12635**	**(4.3E-04, 7.9E-04, 1.3E-03)**
	C monthly tests, 1984-1989	8	6011	(6.6E-04, 1.3E-03, 2.4E-03)
	C monthly tests, 1990-1995	2	6624	(5.4E-05, 3.0E-04, 9.5E-04)
Control rod drive and rod				
Control element assembly & rod (RMA)	PWR unplanned trips	0	161514	(0.0E+00, 0.0E+00, 1.9E-05)
	PWR cyclic tests	1	28022	(1.8E-06, 3.6E-05, 1.7E-04)
	PWR pooled trips & tests	**1**	**189536**	**(2.7E-07, 5.3E-06, 2.5E-05)**

a. The middle number is the point estimate, *f*/*d*, or f/T, and the two end numbers form a 90% confidence interval. For demands, the interval is based on a binomial distribution for the occurrence of failures, while it is based on a Poisson distribution for the rates. Rates are identified from the "occurrences in time" data set, and a footnote in the denominator column. Note that these maximum likelihood estimates may be zero and are not used directly in the unavailability analysis.

b. Highlighted rows show the data sets selected for the unavailability analysis. In sections where no row is highlighted, see Table C-5.

c. Component years. The associated rates are failures per component year.

should not be pooled over plant mode. From Table C-3, more failures occurred during shutdown periods than during operational periods. Furthermore, from the prorating assumption used to estimate the number of test demands, many fewer test demands were counted for shutdown periods than for operations. The p-value is a measure of the likelihood of the observed difference or a more extreme difference if the two groups had the same failure probability. The low statistical p-value means that either a "rare" (probability less than 0.0005) situation occurred, or the two sets of failures and demands have different failure probabilities (the actual p-value was 3.15E-6). The statistical test for time period differences is similar. Only two of 23 failures occurred during the 1990–1995 period. This phenomenon is even less likely under the assumption of homogeneity than the observed difference with regard to plant state (the actual p-value was 1.2E-6). The low p-values in the last two columns similarly indicate differences, first between plants, and then between years.

Throughout these tables, p-values that are less than or equal to 0.05 are highlighted. The tables show many cases where differences in plant unit reporting were observed.

Table C-4. Evaluation of differences between groups for CE RPS failure modes (based only on complete failures with safety function lost).[a]

Failure mode (component)	Data set [b]	P-values for test of variation [c]				
		Rx. trip vs. tests	In plant modes	In time periods	In plant units	In years
Channel components and bistables						
Pressure sensor/ transmitter (CPR)	C cyclic & qtrly. tests	—	**<5.E-4 (E)**	0.306	**<5.E-4 (E)**	**0.001 (E)**
	C cyclic & qtrly. tests (op)	—	—	0.436	0.240	0.148
	C cyclic & qtrly. tests (s/d)	—	—	0.125 (E)	**0.010 (E)**	**<5.E-4 (E)**
	C tests, 1984-1989 (s/d)	—	—	—	0.151	0.434
	C tests, 1990-1995 (s/d)	—	—	—	**0.002 (E)**	**0.005 (E)**
	C occurrences in time	—	**0.025 (E)**	0.313	0.395	0.254 (E)
	C occurrences in time (op)	—	—	0.113	0.746	0.358
	C occurrences in time (s/d)	—	—	0.964	0.414 (E)	**0.020 (E)**
Temperature sensor/ transmitter (CTP)	C cyclic & qtrly. tests	—	0.058 (E)	0.316	**0.017 (E)**	0.052 (E)
	C cyclic & qtrly. tests (op)	—	—	0.328	0.853	0.521
	C cyclic & qtrly. tests (s/d)	—	—	0.686	**0.001 (E)**	0.093 (E)
	C occurrences in time	—	0.955	0.081	0.731	0.491
Analog core protection calculator (CPA)	C quarterly tests	—	**0.050 (E)**	0.288	**0.005 (E)**	**<5.E-4 (E)**
	C quarterly tests (op)	—	—	0.624	0.754	0.169 (E)
	C quarterly tests (s/d)	—	—	0.374	**0.003 (E)**	**0.004 (E)**
	C occurrences in time	—	0.861	0.575	0.669	0.113 (E)
Digital core protection calculator (CPD)	C quarterly tests	—	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**
	C quarterly tests (op)	—	—	**0.015 (E)**	0.095 (E)	**0.050 (E)**
	C qtr. tests, 1984-1989 (op)	—	—	—	0.495	0.366
	C qtr. tests, 1990-1995 (op)	—	—	—	0.439	0.412
	C quarterly tests (s/d)	—	—	**0.001 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**
	C qtr. tests, 1984-1989 (s/d)	—	—	—	**<5.E-4 (E)**	**<5.E-4 (E)**
	C qtr. tests, 1990-1995 (s/d)	—	—	—	0.386	0.387
	C occurrences in time	—	0.125	**0.026 (E)**	**<5.E-4 (E)**	0.092 (E)
	C occurrences in time, 1984-1989	—	0.067	—	**<5.E-4 (E)**	0.675
	C occurrences in time, 1990-1995	—	0.599	—	**<5.E-4 (E)**	**0.038 (E)**
Bistable (CBI)	C quarterly tests	—	**0.010 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**	**0.009 (E)**
	C quarterly tests (op)	—	—	**<5.E-4 (E)**	**<5.E-4 (E)**	**0.014 (E)**
	C qtr. tests, 1984-1989 (op)	—	—	—	**<5.E-4 (E)**	0.404
	C qtr. tests, 1990-1995 (op)	—	—	—	**0.029 (E)**	0.390
	C quarterly tests (s/d)	—	—	0.264	**<5.E-4 (E)**	0.547
Trains (trip logic)						
Logic relay (RYL)	C quarterly tests	—	0.461	1.000	0.592	0.504
Trip relay (RYT)	C quarterly tests	—	1.000	0.465	0.501	0.336

Table C-4. (Continued.)

Failure mode (component)	Data set [b]	P-values for test of variation [c]				
		Rx. trip vs. tests	In plant modes	In time periods	In plant units	In years
Manual scram switch (MSW)	PWR unplanned trips	—	0 F	0 F	0 F	0 F
	PWR quarterly tests	—	—	0.505	0.503	0.634
	PWR pooled trips & tests	1.000	—	0.500	0.728	0.769
Reactor trip breakers						
Breaker mechanical (BME)	BC unplanned trips	—	0 F	0 F	0 F	0 F
	BC monthly tests	—	1.000	1.000	**<5.0E-4** [d]	0.464
	BC pooled trips & tests	0.793	1.000	0.495	**<5.0E-4** [d]	0.673
Breaker shunt device (BSN)	CW quarterly tests	—	0.574	0.108 (E)	0.788	0.035 (E)
	CW quarterly tests, 1984-1989	—	0.566	—	0.827	0.138 (E)
	CW quarterly tests, 1990-1995	—	0 F	—	**0 F**	0 F
Breaker undervoltage coil (BUV)	C monthly tests	—	0.139	0.055 (E)	**0.008 (E)**	0.199 (E)
	C monthly tests, 1984-1989	—	0.227	—	0.054 (E)	0.380
	C monthly tests, 1990-1995	—	0.427	—	0.228	0.549
Control rod drive and rod						
Control element assembly & rod (RMA)	PWR unplanned trips	—	0 F	0 F	0 F	0 F
	PWR cyclic tests	—	0.244	0.500	0.979	0.561
	PWR pooled trips & tests	0.148	**0.036**	1.000	0.978	0.499

a. This table describes components in the fault tree whose failure probability or rate was estimated from the RPS data. Unplanned demands are considered for some components, as indicated in Table A-2. Additional rows for subsets based on plant status or time period appear if significant differences in these attributes were found in the larger groups of data.

b. —, a subset of the test data for the component based on plant state (operating or shut down) and/or year. In the first line of data for an estimate, vendor groups are given as follows: C, CE (only); BC, CE, and B&W pooled; CW, B&W, and W pooled; and PWR, CE, B&W, and W all pooled.

c. —, not applicable; 0 F, no failures (thus, no test); All F, no successes (thus, no test). P-values less than or equal to 0.05 are in a bold font. For the evaluation columns other than "Rx. trip vs. tests," an "E" is in parentheses after the p-value if and only if an empirical Bayes distribution was found accounting for variations in groupings. Low p-values and the fitting of empirical Bayes distributions are indications of variability between the groupings considered in the column.

d. The chi-square test statistic is only an approximation. In this case, the actual p-value for the pooled data is 0.015. A single failure occurred at a plant with 1.5% of the total demands, while twenty other plants each had more demands and no failures.

In each of the first three main evaluation columns in Table C-4, two entities or data groupings are being compared (reactor trips versus tests, operational versus shutdown, and older versus more recent). In the leftmost evaluation column, where applicable, the reactor trip data were compared with the data from testing. This evaluation is for information only, since both sets of data were pooled for the unavailability analysis.

The plant operating mode and time period evaluations in Table C-4 also reflect the comparison of pairs of attributes. "Step 1" in Figure C-1 shows how these evaluations are used in the selection of a subset of data for analysis. The selections were also dictated by the allowed component combinations listed in Table A-2.

Step 2 in the data selection process is to repeat Step 1 using the upper bound (UB) data from the fifth data column in Table C-1. Table C-5 is similar to Table C-3, and gives denominators, probabilities or rates, and confidence intervals. Table C-6 shows the p-values computed for the tests of differences in groups for the UB data.

The subset selection results for the LB and UB cases agreed for all but three of the estimates. For cyclic and quarterly tests of pressure sensor/transmitters, both runs showed higher probabilities for shutdown tests than for tests during operation, but only the upper bound case showed differences according to the two time periods. For the rate evaluation of failures detected during routine operations for pressure sensor/transmitters, the strongest difference was found between plant operational states in the lower bound run (with just two of six failures during operations) and between the two time periods in the upper bound run (with just three of twelve failures in the more recent period). The third estimate having differences between the two bounding runs was the temperature sensor/transmitter rate. Here, significant differences for both plant state and time period were seen in the upper bound run.

The general principle that subsets are used if either of the bounding analyses showed a need for them was used for the first and third estimates just discussed. This point is explained in the last Step 2 box in Figure C-1. The decision process thus reduced the data in these two cases to plant operations in the 1990-1995 period.

For the pressure sensor/transmitter *rates*, the LB and UB differences led to different sets for consideration, rather than to more detailed subsets. For the UB case, four of the six uncertain failures considered in addition to the known failures occurred in the earlier period, during operations. These events thus reduced the impact of plant state differences, while increasing the impact of the two different time periods. The subset selection for the pressure sensor/ transmitters rate evaluation was based on plant state, and not on the two time periods, because the p-value for plant state differences in the LB case was lower (and thus more significant) than the p-value for time period differences in the UB case. Also, the LB case has more impact in the evaluation since less than half of the added failures in the UB case are counted as complete with safety function lost.

Table C-5. Point estimates and confidence bounds for component groups used in the assessment of CE RPS total failure probabilities and rates (including all failures with unknown completeness and/or unknown loss of the safety function).

Failure mode (component)	Data set	Failures f	Denominator d or T	Probability or rate [a] and 90% confidence interval
Channel components				
Pressure sensor/ transmitter (CPR)	C cyclic & qtr. tests	19	11188	(1.1E-03, 1.7E-03, 2.5E-03)
	C cyclic & qtr. tests (op)	5	8296	(2.4E-04, 6.0E-04, 1.3E-03)
	C cyc. & qtr. tests, 1984-1989 (op)	5	3618	(5.4E-04, 1.4E-03, 2.9E-03)
	C cyc. & qtr. tests, 1990-1995 (op) [b]	**0** [b]	**4678** [b]	**(0.0E+00, 0.0E+00, 6.4E-04)** [b]
	C cyclic & qtr. tests (s/d)	14	2892	(2.9E-03, 4.8E-03, 7.6E-03)
	C occurrences in time	12	2360.9 [c]	(2.9E-03, 5.1E-03, 8.2E-03)
	C occurrences in time, 1984-1989	9	1088.9 [c]	(4.3E-03, 8.3E-03, 1.4E-02)
	C occurrences in time, 1990-1995	3	1272.0 [c]	(6.4E-04, 2.4E-03, 6.1E-03)
Temperature sensor/ transmitter (CTP)	C cyclic & qtr. tests	21	12530	(1.1E-03, 1.7E-03, 2.4E-03)
	C cyclic & qtr. tests (op)	**10**	**9266**	**(5.9E-04, 1.1E-03, 1.8E-03)**
	C cyclic & qtr. tests (s/d)	11	3264	(1.9E-03, 3.4E-03, 5.6E-03)
	C occurrences in time	25	2645.4 [c]	(6.6E-03, 9.5E-03, 1.3E-02)
	C occurrences in time (op)	14	1943.9 [c]	(4.4E-03, 7.2E-03, 1.1E-02)
	C occur. in time, 1984-1989 (op)	11	872.2 [c]	(7.1E-03, 1.3E-02, 2.1E-02)
	C occur. in time, 1990-1995 (op)	3	1071.7 [c]	(7.6E-04, 2.8E-03, 7.2E-03)
	C occurrences in time (s/d)	11	701.5 [c]	(8.8E-03, 1.6E-02, 2.6E-02)
Analog core protection calculator (CPA)	C quarterly tests	41	1524	(2.0E-02, 2.7E-02, 3.5E-02)
	C quarterly tests (op)	**15**	**1082**	**(8.6E-03, 1.4E-02, 2.1E-02)**
	C quarterly tests (s/d)	26	442	(4.2E-02, 5.9E-02, 8.1E-02)
	C occurrences in time	11	380.5 [c]	(1.6E-02, 2.9E-02, 4.7E-02)
Digital core protection calculator (CPD)	C quarterly tests	37	1171	(2.4E-02, 3.2E-02, 4.1E-02)
	C quarterly tests (op)	10	894	(6.1E-03, 1.1E-02, 1.9E-02)
	C qtr. tests, 1984-1989 (op)	9	346	(1.4E-02, 2.6E-02, 4.5E-02)
	C qtr. tests, 1990-1995 (op)	**1**	**548**	**(9.4E-05, 1.8E-03, 8.6E-03)**
	C quarterly tests (s/d)	27	277	(7.0E-02, 9.7E-02, 1.3E-01)
	C qtr. tests, 1984-1989 (s/d)	25	153	(1.2E-01, 1.6E-01, 2.2E-01)
	C qtr. tests, 1990-1995 (s/d)	2	124	(2.9E-03, 1.6E-02, 5.0E-02)
	C occurrences in time	68	292.9 [c]	(1.9E-01, 2.3E-01, 2.8E-01)
	C occurrences in time, 1984-1989	49	124.9 [c]	(3.2E-01, 3.9E-01, 4.7E-01)
	C occurrences in time, 1990-1995	19	168.0 [c]	(7.5E-02, 1.1E-01, 1.6E-01)
Bistable (CBI)	C quarterly tests	76	37453	(1.7E-03, 2.0E-03, 2.5E-03)
	C quarterly tests (op)	35	27494	(9.4E-04, 1.3E-03, 1.7E-03)
	C qtr. tests, 1984-1989 (op)	26	12232	(1.5E-03, 2.1E-03, 2.9E-03)
	C qtr. tests, 1990-1995 (op)	**9**	**15262**	**(3.1E-04, 5.9E-04, 1.0E-03)**
	C quarterly tests (s/d)	41	9959	(3.1E-03, 4.1E-03, 5.3E-03)

Table C-5. (Continued).

Failure mode (component)	Data set	Failures f	Denominator d or T	Probability or rate [a] and 90% confidence interval
Trains (trip logic) [d]				
Logic relay (RYL)	**C quarterly tests**	**8**	**16160**	**(2.5E-04, 5.0E-04, 8.9E-04)**
Trip relay (RYT)	**C quarterly tests**	**2**	**16160**	**(2.2E-05, 1.2E-04, 3.9E-04)**
Reactor trip breakers				
Breaker shunt device (BSN)	C quarterly tests	4	25270	(5.4E-05, 1.6E-04, 3.6E-04)
	C quarterly tests, 1984-1989	4	12022	(1.1E-04, 3.3E-04, 7.6E-04)
	C quarterly tests, 1990-1995	**0**	**13248**	**(0.0E+00, 0.0E+00, 2.3E-04)**
Breaker under-voltage coil (BUV)	**C monthly tests**	**18**	**12635**	**(9.2E-04, 1.4E-03, 2.1E-03)**
Control rod drive and rod				
Control element assembly & rod (RMA)	PWR unplanned trips	2	161514	(2.2E-06, 1.2E-05, 3.9E-05)
	PWR cyclic tests	3	28022	(2.9E-05, 1.1E-04, 2.8E-04)
	PWR cyclic tests (op)	0	21179	(0.0E+00, 0.0E+00, 1.4E-04)
	PWR cyclic tests (s/d)	3	6843	(1.2E-04, 4.4E-04, 1.1E-03)
	PWR cyclic tests, 1984-1989	3	14003	(5.8E-05, 2.1E-04, 5.5E-04)
	PWR cyclic tests, 1990-1998	0	14019	(0.0E+00, 0.0E+00, 2.1E-04)
	PWR pooled trips & tests	**5**	**189536**	**(1.0E-05, 2.6E-05, 5.5E-05)**
	PWR pooled trips & tests (op)	2	182693	(1.9E-06, 1.1E-05, 3.4E-05)

a. The middle number is the point estimate, f/d, or f/T, and the two end numbers form a 90% confidence interval. For demands, the interval is based on a binomial distribution for the occurrence of failures, whereas it is based on a Poisson distribution for the rates. Rates are identified from the "occurrences in time" data set, and a footnote in the denominator column. Note that these maximum likelihood estimates may be zero and are not used directly in the unavailability analysis. Note also that manual switches, silicon-controlled rectifiers, and breaker mechanical are not included in this table, since they had no uncertain failure data in the subsets under consideration for the unavailability analysis (see Table C3).

b. Highlighted rows show the data sets selected for the unavailability analysis. No rows are highlighted among the occurrences in time because the unavailability associated with each rate and an 8-hour per year down time is an order of magnitude lower than the unavailability computed from the test data.

c. Component years. The associated rates are failures per component year.

d. No row for manual switches. There were no uncertain failures for this component.

Table C-6. Evaluation of differences between groups for CE RPS failure modes, including failures with unknown completeness and/or unknown loss of safety function. [a]

Failure mode (component)	Data set [b]	P-values for test of variation [c]				
		Rx. trip vs. tests	In plant modes	In time periods	In plant units	In years
Channel components						
Pressure sensor/ transmitter (CPR)	C cyclic & qtrly. tests	—	**<5.E-4 (E)**	1.000	**0.001 (E)**	0.122 (E)
	C cyclic & qtrly. tests (op)	—	—	**0.016 (E)**	**0.001 (E)**	**0.026 (E)**
	C cyc. & qtr. tests, 1984-1989 (op)	—	—	—	**0.003 (E)**	0.245
	C cyc. & qtr. tests, 1990-1995 (op)	—	—	—	0 F	0 F
	C cyclic & qtrly. tests (s/d)	—	—	0.179	**0.001 (E)**	0.073 (E)
	C occurrences in time	—	0.226	**0.045 (E)**	**0.001 (E)**	0.389
	C occurrences in time, 1984-1989	—	0.781	—	0.228 (E)	0.746
	C occurrences in time, 1990-1995	—	0.082	—	**0.023 (E)**	0.221
Temperature sensor/ transmitter (CTP)	C cyclic & qtrly. tests	—	**0.011 (E)**	0.520	**0.002 (E)**	0.357
	C cyclic & qtrly. tests (op)	—	—	1.000	0.608	0.492
	C cyclic & qtrly. tests (s/d)	—	—	0.548	**0.007 (E)**	0.301 (E)
	C occurrences in time	—	**0.048 (E)**	**0.031 (E)**	0.164 (E)	0.191 (E)
	C occurrences in time (op)	—	—	**0.011 (E)**	0.123 (E)	**0.022 (E)**
	C occur. in time, 1984-1989 (op)	—	—	—	0.440	0.133 (E)
	C occur. in time, 1990-1995 (op)	—	—	—	0.517	0.749
	C occurrences in time (s/d)	—	—	0.810	**0.001 (E)**	0.545
Analog core protection calculator (CPA)	C quarterly tests	—	**<5.E-4 (E)**	0.528	**<5.E-4 (E)**	**0.001 (E)**
	C quarterly tests (op)	—	—	0.605	0.085 (E)	0.479
	C quarterly tests (s/d)	—	—	0.163	**<5.E-4 (E)**	**<5.E-4 (E)**
	C occurrences in time	—	0.914	0.124	0.290	0.074 (E)
Digital core protection calculator (CPD)	C quarterly tests	—	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**
	C quarterly tests (op)	—	—	**0.001 (E)**	0.116 (E)	**0.002 (E)**
	C qtr. tests, 1984-1989 (op)	—	—	—	0.457	0.165
	C qtr. tests, 1990-1995 (op)	—	—	—	0.439	0.412
	C quarterly tests (s/d)	—	—	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**
	C qtr. tests, 1984-1989 (s/d)	—	—	—	**<5.E-4 (E)**	**<5.E-4 (E)**
	C qtr. tests, 1990-1995 (s/d)	—	—	—	**0.046**	0.570
	C occurrences in time	—	0.370	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**
	C occurrences in time, 1984-1989	—	0.215	—	**<5.E-4 (E)**	0.115 (E)
	C occurrences in time, 1990-1995	—	0.365	—	**<5.E-4 (E)**	0.051 (E)

Table C-6. (Continued.)

Failure mode (component)	Data set [b]	P-values for test of variation [c]				
		Rx. trip vs. tests	In plant modes	In time periods	In plant units	In years
Bistable (CBI)	C quarterly tests	—	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**	**<5.E-4 (E)**
	C quarterly tests (op)	—	—	**<5.E-4 (E)**	**<5.E-4 (E)**	**0.007 (E)**
	C qtr. tests, 1984-1989 (op)	—	—	—	**<5.E-4 (E)**	0.291
	C qtr. tests, 1990-1995 (op)	—	—	—	**0.001 (E)**	0.245
	C quarterly tests (s/d)	—	—	0.213	**<5.E-4 (E)**	0.001 (E)
Trains (trip logic)						
Logic relay (RYL)	C quarterly tests	—	0.445	0.157	**<5.E-4 (E)**	0.690
Trip relay (RYT)	C quarterly tests	—	1.000	1.000	0.592	0.504
Reactor trip breakers						
Breaker shunt device (BSN)	C quarterly tests	—	0.578	**0.051 (E)**	0.860	0.021 (E)
	C quarterly tests, 1984-1989	—	0.581	—	0.892	0.126 (E)
	C quarterly tests, 1990-1995	—	**0 F**	—	**0 F**	0 F
Breaker undervoltage coil (BUV)	C monthly tests	—	0.431	0.155	0.001 (E)	0.259 (E)
Control rod drive and rod						
Control element assembly & rod (RMA)	PWR unplanned trips	—	—	0.077	0.667	0.209
	PWR cyclic tests	—	**0.015 (E)** [d]	0.125 (E)	**<5.E-4 (E)**	0.101 (E)
	PWR cyclic tests (op)	—	—	0 F	0 F	0 F
	PWR cyclic tests (s/d)	—	—	0.254	**0.002 (E)**	0.118 (E)
	PWR cyclic tests, 1984-1989	—	**0.018 (E)** [d]	—	**<5.E-4 (E)**	0.263
	PWR cyclic tests, 1990-1998	—	0 F	—	0 F	0 F
	PWR pooled trips & tests	**0.026** [d]	**<5.E-4 (E)** [d]	0.649	**0.001 (E)**	0.585 (E)
	PWR pooled trips & tests (op)	1.000	—	0.092	0.571	0.364

a. This table describes components in the fault tree whose failure probability or rate was estimated from the RPS data including uncertain failures. Unplanned demands are considered for some components as indicated in Table A-2. Additional rows for subsets based on plant status or time period appear if significant differences in these attributes were found in the larger groups of data. Note that manual switches, silicon-controlled rectifiers, and breaker mechanical are not included in this table since they had no uncertain failure data in the subsets under consideration for the unavailability analysis. See Table C-4 for these components.

b. —, a subset of the test data for the component based on plant state (operating or shut down) and/or year. In the first line of data for an estimate, vendor groups are given as follows: C, CE (only); BC, CE and B&W pooled; CW, CE and W pooled; and PWR, CE, B&W, and W all pooled.

Table C-6. (Continued.)

Failure mode (component)	Data set [b]	P-values for test of variation [c]				
		Rx. trip vs. tests	In plant modes	In time periods	In plant units	In years

Table C-6 notes, continued

c. —, not applicable; 0 F, no failures (thus, no test); All F, no successes (thus, no test). P-values less than or equal to 0.05 are in a bold font. For the evaluation columns other than "Rx. trip vs. tests," an "E" is in parentheses after the p-value if and only if an empirical Bayes distribution was found accounting for variations in groupings. Low p-values and the fitting of empirical Bayes distributions are indications of variability between the groupings considered in the column.

d. Pooled trips and tests were used for the unavailability analysis, in spite of statistical tests showing differences in the unplanned demands and tests and between tests in operations and tests while shut down. The reactor trip experience is like the RPS demand being modeled for this study. The cyclic rod drop tests are also believed to be relevant, representing failure modes that could occur on an unplanned demand, regardless of whether they were conducted during operations or during shutdown periods.

In both Tables C-3 and C-5, lines are highlighted corresponding to the subsets selected. Table C-7 concisely summarizes the data in the selected subsets.

Within each selected subset, the next evaluation focused on the two remaining attributes for study of data variation, namely differences between plants and between calendar years. Tables C-4 and C-6 include results from these evaluations in the last two columns. These evaluations are used in Step 3 in Figure 1. In nearly every instance where a significant p-value appears in these columns, empirical Bayes distributions reflect the associated variability. One exception to this finding is for one mechanical breaker (BME) failure at a CE plant. The result stands out because this plant had less than half as many BME demands as estimated for most of the other plants. However, the data were too sparse for estimation of an empirical Bayes distribution. The only other exception was for similar sparse data with two breaker shunt device failures that occurred at different Westinghouse plants.

In the Table C-6 data, the rod and control rod drive component show a higher probability from testing failures than from trips (p-value=0.026). One failure and one possible failure were found in nearly 162,000 trip demands, and the three possible failures were identified in an estimated 12,000 operational cyclic tests. The trip data are directly relevant to the study of operational reliability, but confidence in the detection of all failures occurring during trips is not as high as for the periodic testing failures. The tests are also believed to be complete. Pooling the trip and test data sets is conservative.

The evaluation of data groupings resulted in no failures in the final data set considered from testing CE pressure sensor/transmitters. Seven of the eight known failures (and 7 of the 11 uncertain failures) occurred while the plants were shutdown. The p-value for the test of equality across plant state among the known failures was less than 5.E-4. Since operational unreliability is the focus of this study, the CPR test data were restricted to plant operational periods. Furthermore, all the failures during plant operation

Table C-7. Point estimates of failure probabilities and rates for CE RPS unavailability analysis.

Basic Event (component)	Data set [a]	No uncertain failures	Failure count with uncertain failures included	Probability applied to uncertainty in whether the safety function is lost[b]		Weighted average total failures	Denominator (demands or hours)	Failures per demand or hour	Update of Jeffreys Noninformative Prior [c]
				Among complete failures	Among uncertain completeness failures				
Channel components									
Pressure sensor/ transmitter (CPR)	C cyc. & qtr. tests, 1990-1995 (op)	0	0	—	—	0.0	4678	0.0E+00	1.1E-04
	C occurrences in time (op)	2	7	0.147	0.167	2.6	15245553 h	1.7E-07	2.0E-07
Temperature sensor/ transmitter (CTP)	C cyc. & qtr. tests (op)	4	10	0.750	0.700	7.4	9266	7.9E-04	8.5E-04
	C occurrences in time, 1990-1995 (op)	2	3	0.250	—	2.3	9387636 h	2.4E-07	2.9E-07
Analog core protection calculator (CPA)	C qtr. tests (op)	3	15	0.438	0.700	8.2	1082	7.6E-03	8.0E-03
	C occurrences in time	3	11	0.233	—	6.7	3333109 h	2.0E-06	2.2E-06
Digital core protection calculator (CPD)	C qtr. tests, 1990-1995 (op)	1	1	—	—	1.0	548	1.8E-03	2.7E-03
	C occurrences in time, 1990-1995	15	19	0.646	—	17.3	1471680 h	1.2E-05	1.2E-05
Bistable (CBI)	C qtr. tests, 1990-1995 (op)	5	9	—	—	7.0	15262	4.6E-04	4.9E-04
Trains (trip logic)									
Logic relay (RYL)	C qtr. tests	2	8	0.313	0.5	3.8	16160	2.6E-04	2.9E-04
Trip relay (RYT)	C qtr. tests	1	2	—	—	1.5	16160	9.3E-05	1.2E-04
Manual scram switch (MSW)	PWR unplanned scrams & qtr. tests	2	2	—	—	2.0	19789	1.0E-04	1.3E-04

Table C-7. (Continued)

Basic Event (component)	Data set [a]	No uncertain failures	Failure count with uncertain failures included	Probability applied to uncertainty in whether the safety function is lost[b]: Among complete failures	Probability applied to uncertainty in whether the safety function is lost[b]: Among uncertain completeness failures	Weighted average total failures	Denominator (demands or hours)	Failures per demand or hour	Update of Jeffreys Noninformative Prior [c]
Reactor trip breakers									
Breaker mechanical (BME)	BC unplanned scrams & qtr. & mon. tests	1	1	—	—	1.0	83813.	1.2E-05	1.8E-05
Breaker shunt device (BSN)	C qtr. tests	3	4	0.700	—	3.5	25270	1.4E-04	1.6E-04
Breaker undervoltage coil (BUV)	C mon. tests	10	18	0.318	0.786	13.6	12635	1.1E-03	1.1E-03
Control rod drive and rod									
Control element assembly & rod (RMA)	PWR unplanned scrams & cyc. tests	1	5	—	—	3.0	189536	1.6E-05	1.8E-05

a. Vendor groups are given as follows: C, CE (only); BC, CE and B&W pooled; CW, CE and W pooled; and PWR, CE, B&W, and W all pooled. Denominators were computed separately for each vendor, according to the testing schedule of the vendors.
b. "—" when there were no applicable uncertain events. The probability used for uncertainty in completeness is 0.5.
c. (Failures + 0.5)/(Denominator+1) for probabilities; (Failures + 0.5)/Denominator for rates.

occurred during the 1984–1989 period. When the old and new data differ significantly (p-value 0.016), the most recent block of data is selected as the most applicable.

The upper and lower bound empirical Bayes analyses included tests of goodness of fit for the resulting beta-binomial model for probabilities or the associated gamma-Poisson model for rates. Each grouping level (each plant, or each year) was evaluated to see if it was a high outlier compared with the fitted GE model for each component. For the subsets of data used in the unreliability analysis, no outliers were found.

Within each selected subset for which differences exist in the LB and UB data, a simulation was conducted to observe the variation in the composite data, which includes the fully classified failures and a fraction of the uncertain failures. This evaluation, referenced in Step 4 of Figure 1, also focused on the two attributes for study of data variation that remain after considering the data subsets, namely differences between plants and between calendar years. In the simulation, the probability of being complete failures for events whose completeness was unknown was determined by a fixed distribution with a mean of 0.5. The probability that events with unknown safety function status were losses of the safety function was estimated based on the failure data within each subset, including the events (not shown in Table C-1) that were assessed as fail-safe. The last column of Table C-1 shows the weighted average of the events that would be complete losses of the safety function.

Table C-8 presents the final results of the basic quantitative component data analysis, most of which come from the simulation. Table C-8 describes the Bayes distributions initially selected to describe the statistical variability in the data used to model the basic RPS events. Table C-8 differs from Tables C-3 and C-5 because it gives Bayes distributions and intervals, not confidence intervals. This choice allows the results for the failure modes to be combined to give an uncertainty distribution on the unavailability. When distributions were fit for both plant variation and year variation, the distribution for differences between plants had greater variability and was selected. Where empirical Bayes distributions were not found, the simple Bayes method was used to obtain uncertainty distributions.

In the unreliability analysis, the means and variances of the generic Bayes distributions were fitted to lognormal distributions, listed in Table C-9. As applicable, these distributions describe the total failure probabilities (Q_T) associated with the common-cause fault tree events.

Table C-8. Results of uncertainty analysis. [a]

Failure Mode (Component)	Fail-ures[b]	Denom-inator [c]	Modeled variation [d]	Distribution [e]	Bayes mean and interval [f]
Channel components					
Pressure sensor transmitter (CPR)	0	4678	Sampling (only) [g]	Beta(0.5,4678.5)	(4.20E-07,1.07E-04,4.10E-04)
	2.6	1740.4 [h]	Sampling	Gamma(2.7,1497.2)	(4.42E-04,1.79E-03,3.89E-03)
Temperature sensor/ transmitter (CTP)	7.3	9266	Sampling	Beta(6.5,7781.7)	(3.82E-04,8.41E-04,1.44E-03)
	2.2	1071.6 [h]	Sampling	Gamma(2.6,1009.8)	(6.07E-04,2.56E-03,5.61E-03)
Analog core protection calculator (CPA)	8.2	1082	Between plant	Beta(1.3,162.5)	(6.50E-04,7.64E-03,2.11E-02)
	6.8	380.5 [h]	Between year	Gamma(0.8,45.2)	(5.20E-04,1.80E-02,5.80E-02)
Digital core protection calculator (CPD)	1	548	Sampling (only) [g]	Beta(1.5,547.5)	(3.21E-04,2.73E-03,7.11E-03)
	17.3	168.0 [h]	Between plant	Gamma(0.4,3.9)	(1.03E-04,1.03E-01,4.28E-01)
Bistable (CBI)	7.0	15262	Between plant	Beta(0.3,613.4)	(6.53E-08,5.00E-04,2.27E-03)
Trains (trip logic)					
Logic relay (RYL)	3.8	16160	Between plant	Beta(0.5,1951.1)	(7.57E-07,2.45E-04,9.56E-04)
Trip relay (RYT)	1.5	16160	Sampling	Beta(1.8,14351)	(1.84E-05,1.23E-04,3.03E-04)
Manual scram switch (MSW)	2	19789	Sampling (only) [g]	Beta(2.5,19788)	(2.89E-05,1.26E-04,2.80E-04)
Reactor trip breakers					
Breaker mechanical (BME)	1	83813	Sampling (only) [g]	Beta(1.5,83813)	(2.10E-06,1.79E-05,4.66E-05)
Breaker shunt device (BSN)	3.5	25270	Between Year	Beta(0.2,1259.4)	(1.00E-09,1.49E-04,7.79E-04)
Breaker undervoltage coil (BUV)	13.6	12635	Between plant	Beta(0.6,544.8)	(1.25E-05,1.14E-03,4.05E-03)
Control rod drive and rod					
Control element assembly & rod (RMA)	2.9	189536	Between plant	Beta(0.1,5157.9)	(8.18E-20,1.66E-05,9.70E-05)

a. When results consist of two lines, the first is for failures in demand; the second is for a rate of failure in time.
b. Number of failures, averaged over 1000 simulation iterations, each of which had an integral number of failures.
c. Estimated number of demands or exposure time, based on the selected data sets or subsets shown in Table C-7.
d. In addition to variation from unknown completeness and/or from unknown loss of safety function.
e. Beta distributions for probabilities and gamma distributions for rates. The simple and empirical Bayes distributions are initially either beta or gamma distributions. See Table C-9 for lognormal bounds.
f. Aggregate of Bayes distributions from simulation, unless otherwise noted. Obtained by matching the mean and variance of the simulation output distribution. If the variation is not just sampling, empirical Bayes distributions were found in each simulated iteration, except for the following: CPR probability, 7% of the time; CPR rate, 16%; CPA rate, 28%; CPA probability, 74%; RYL, 75%; and RMA, 52% of the time. Sampling variation (from the simple Bayes method) entered the simulation mixture when EB distributions were not found.
g. Simple Bayes distribution not based on the simulations. No uncertain events were in the selected subsets.
h. Component years rather than demands. Also, the rates in the Bayes mean column are per year. The rates were not used in fault tree assessment, because the unavailability associated with the failure rates was much lower than the unavailability estimated from the testing data.

Table C-9. Lognormal uncertainty distributions used for CE RPS total failure probabilities (Q_T).

Failure Mode (Component)	Data set [a]	Median	Error factor [b]	Lognormal distribution mean and interval [c]
Channel components				
Pressure sensor/ transmitter	C cyc. & qtr. tests, 1990–1995 (op)	6.2E-05	5.6	(1.1E-05, 1.1E-04, 3.5E-04)
	C occurrences in time (op)	1.5E-03 /y	2.5	(6.1E-04, 1.8E-03, 3.9E-03)
	Probability from rate [d]	1.4E-06	2.5	(5.5E-07, 1.6E-06, 3.5E-06)
Temperature sensor/ transmitter	C cyc. & qtr. tests (op)	7.8E-04	1.9	(4.2E-04, 8.4E-04, 1.5E-03)
	C occurrences in time, 1990–1995 (op)	2.2E-03/y	2.6	(8.6E-04, 2.6E-03, 5.6E-03)
	Probability from rate [d]	2.0E-06	2.6	(7.8E-07, 2.3E-06, 5.1E-06)
Analog core protection calculator	C qtr. tests (op)	5.7E-03	3.5	(1.6E-03, 7.6E-03, 2.0E-02)
	C occurrences in time	1.2E-02/y	4.4	(2.7E-03, 1.8E-02, 5.2E-02)
	Probability from rate [d]	1.1E-05	4.4	(2.5E-06, 1.6E-05, 4.8E-05)
Digital core protection calculator	C qtr. tests, 1990–1995 (op)	2.1E-03	3.2	(6.5E-04, 2.7E-03, 6.8E-03)
	C occurrences in time, 1990–1995	5.5E-02/y	6.3	(8.7E-03, 1.0E-01, 3.5E-01)
	Probability from rate [d]	5.0E-05	6.3	(8.0E-06, 9.4E-05, 3.2E-04)
Bistable	C qtr. tests, 1990–1995 (op)	2.4E-04	7.2	(3.4E-05, 5.0E-04, 1.8E-03)
Trains (trip logic)				
Logic relay	C qtr. tests	1.4E-04	5.7	(2.4E-05, 2.5E-04, 8.0E-04)
Trip relay	C qtr. tests	9.8E-05	3.0	(3.3E-05, 1.2E-04, 3.0E-04)
Manual scram switch	PWR unplanned scrams & qtr. tests	1.1E-04	2.6	(4.1E-05, 1.3E-04, 2.8E-04)
Reactor trip breakers				
Breaker mechanical	BC unplanned scrams & qtr. & mon. tests	1.4E-05	3.2	(4.3E-06, 1.8E-05, 4.5E-05)
Breaker shunt device	C qtr. tests	5.9E-05	9.3	(6.3E-06, 1.5E-04, 5.5E-04)
Breaker undervoltage coil	C mon. tests	7.1E-04	5.0	(1.4E-04, 1.1E-03, 3.5E-03)
Control rod drive and rod				
Control element assembly & rod	PWR unplanned scrams & cyc. tests	4.7E-06	13.8	(3.4E-07, 1.7E-05, 6.4E-05)

a. C: Combustion Engineering. B: B&W. W: Westinghouse.
b. Lognormal error factor corresponding to 5% and 95% bounds.
c. Mean and lognormal distribution 5th and 95th percentiles. Obtained by matching the mean and variance of the distributions from Table C-8, which are used in the unreliability analysis.
d. Probability computed from rate using an 8-hour downtime. This probability was not used in the fault tree assessment since it is much lower than the probability computed from failures and demands.