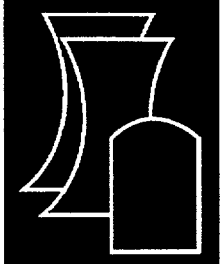
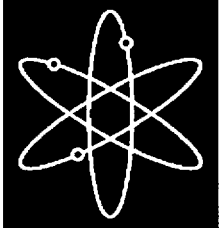
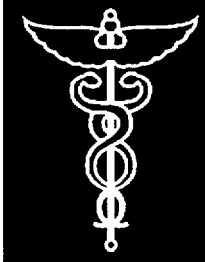
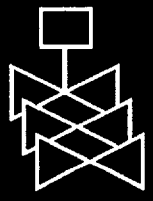
NUREG/CR-5500, Vol. 11
INEL/EXT-97-00740









Reliability Study: Babcock & Wilcox 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. 11
INEL/EXT-97-00740

Reliability Study: Babcock & Wilcox 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. Babcock & Wilcox commercial reactors during the period 1984 through 1998. The analysis is based on the Oconee and Davis-Besse plant designs. RPS operational data were collected for all U.S. Babcock & Wilcox 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. Babcock & Wilcox (B&W) commercial nuclear reactors during the period 1984 through 1998. The objectives of the study were the following: (1) to estimate RPS unavailability based on operational experience data and compare the results with models used in probabilistic risk assessments (PRAs) and individual plant examinations (IPEs), 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 B&W RPS designs covered in the unavailability estimation include two versions. Fault trees developed for this study were based on these two versions, which are representative of all B&W plants.

Babcock & Wilcox 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 600 events were evaluated for applicability to this study. Those 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 CCF events in the RPS fault tree. The level of detail of the basic events includes the following: channel trip signal sensor/transmitters and associated bistables, relays, and control rod drives and control rods. CCF events were modeled for all redundant, similar types of components.

Fault trees for the two versions of the B&W RPS were developed and quantified using U.S. B&W commercial nuclear reactor data from the period 1984 through 1998. All B&W plants use a design similar to the Oconee RPS except the Davis-Besse plant. The Davis-Besse design is unique to Davis-Besse and was modeled separately. Table ES-1 summarizes the results of this study.

Table ES-1. Babcock & Wilcox fault tree model results with uncertainty.

	5%	Mean	95%
Oconee Model			
No credit for manual trip by operator	1.3E-7	7.8E-7	2.4E-6
Credit for manual trip by operator	1.8E-9	8.7E-9	2.5E-8
Davis-Besse Model			
No credit for manual trip by operator	2.6E-7	1.6E-6	4.8E-6
Credit for manual trip by operator	3.1E-8	8.4E-7	3.2E-6

The computed mean unavailability estimates were 7.8E-7 and 1.6E-6 (with no credit for manual trips). These are comparable to the values given in B&W IPEs, which ranged from 1.0E-6 to 5.0E-6, and other similar reports. Common-cause failures contribute greater than 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 allowing credit for manual scram by the operator (with a failure probability of 0.01). Operator action reduces the RPS unavailability by approximately 99 percent (8.7E-9, Oconee design) and 48 percent (8.4E-7, Davis-Besse design).

Several general insights were obtained from this study:

- Neither design shows a significant contribution from the trip breakers/diverse trip segment.

- The Oconee design shows no contribution from the rods segment but the Davis-Besse design shows a significant contribution from this segment. This is because of the separation of the rods that are dropped by the diverse electronic trip. The Oconee design trips the safety rods with the trip breakers and the regulating rods with the diverse trip. This has the effect of having both a diverse means of tripping rods and a diverse group of rods that are tripped in the Oconee model. The Davis-Besse design trips all rods with both means.

- 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. Automatic actuation of the shunt trip mechanism within the reactor trip breakers and improved maintenance have resulted in improved performance of these components.

- Overall, trends in unplanned trips at B&W reactors decreased significantly over the time span of this study. Due to sparse data, trends in component failure probabilities and counts of CCF events are not significant in the B&W data. Trends for the pooled PWR overall CCF rate of occurrence used in this study showed a statistically significant decreasing trend. Relays, pressure sensor/transmitters, and undervoltage coils all showed significant decreasing trends.

- The causes of the Babcock & Wilcox CCF events are similar to those of the rest of the industry. That is, over all RPS designs for all vendors for all of the components 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 principal method of detection of failures of components in this study was either by testing or by observation during routine plant tours. No failures were detected by actual trip demands. No change over time in the overall distribution of the detection method is apparent.

FOREWORD

This report provides information relevant to the reliability of the Babcock & Wilcox 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 the development of risk-based performance indicators that will be based largely on plant-specific system and equipment performance.

Findings and conclusions from the analyses of the Babcock & Wilcox RPS, which are based on 1984–1998 operating experience, are presented in the Executive Summary. The results of the quantitative analysis and engineering analysis are presented in Sections 3 and 4, respectively. The information to support risk-informed regulatory activities related to the Babcock & Wilcox RPS is summarized in Table F-1. This table provides a condensed index of risk-important data and results presented in discussions, tables, figures, and appendices.

Table F-1. Summary of risk-important information specific to the Babcock & Wilcox 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 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 cited in this report. This 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 may be gained about plant-specific performance by examining the specific events in light of the overall industry performance. In addition, a 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. A search of the LER database can be conducted through the NRC's Sequence Coding and Search System (SCSS) to identify the RPS events that occurred after the period covered by this report. SCSS contains the full text LERs and is accessible by NRC staff from 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.

Periodic updates to the information in this report will be performed, as additional data become available.

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

ACKNOWLEDGMENTS

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

ACRS	Advisory Committee on Reactor Safeguards (U.S. NRC)
ARTS	anticipated reactor trip system
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
CF	complete failure
CPR	channel pressure sensor/transmitter
CRD	control rod drive
CRDM	control rod drive motor
CRDCS	control rod drive control system
CTP	channel temperature sensor/transmitter
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
MSIV	main steam isolation valve
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.)
NSSS	nuclear steam supply system
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
SCR	silicon-controlled rectifier
SCSS	Sequence Coding and Search System
TLR	trip logic relay

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 Babcock & Wilcox 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.

Diverse electronic trip–An alternate and varied means of de-energizing the holding power to the control rod drive motors.

Gating power–This term is used in conjunction with the silicon-controlled rectifiers (SCRs) to describe the control signal applied to a SCR to place the SCR in a closed state. When the gating power is interrupted, the SCR will revert to its open state on the next negative half-cycle of the applied ac voltage, thus removing all power at the outputs of the motor power supplies.

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 Babcock & Wilcox reactor protection system than includes the control rod drives and the control rods. There are generally 69 control rods and associated drives in Babcock & Wilcox 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 segment—The portion of the Babcock & Wilcox reactor protection system that includes the reactor trip breakers. There are four 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.

Trip module segment—The portion of the Babcock & Wilcox reactor protection system that includes the reactor trip relays housed in cabinets in the control room. There are four trains in the trip system segment. Each train receives signals from four of the four instrument channels. Each train energizes one of the four trip breakers.

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: Babcock & Wilcox 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 an effort to ensure that the stated NRC policy to expand the use of probabilistic risk assessment (PRA) within the agency is implemented in a consistent and predictable manner. As part of this effort, the Division of Risk Analysis & Applications has undertaken to monitor and report upon 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 the identification of 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 Babcock & Wilcox pressurized water reactors (PWRs) was performed.

An abbreviated U.S. history of regulatory issues related 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 U.S., 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.

It should be noted that the RPS boundary for this study does not include ATWS mitigation systems added or modified in the late 1980s. For Babcock & Wilcox nuclear reactors, these systems use diverse trip parameters and remove gating power to the SCRs through separate relays. 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. Babcock & Wilcox 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 operational data, and compare the results with the assumptions, models, and data used in PRAs and Individual Plant Examinations (IPEs).

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

The remainder of this report is arranged in five sections. Section 2 describes the scope of the study, including a system description for the RPS, description of the fault tree models used in the analysis, and descriptions of the data collection, characterization, and analysis. Section 3 contains the unavailability results from the operational data and comparisons with PRA/IPE RPS results. Section 4 provides the results of the engineering analysis of the operational data. A summary and conclusions are presented in Section 5. Finally, Section 6 contains the references.

There are also seven appendices in this report. Appendix A provides a detailed explanation of the methods used for data collection, characterization, and analysis. Appendix B gives a summary of the operational data. The detailed statistical analyses are presented in Appendix C. The fault tree model is included in Appendix D. Common-cause failure modeling information is presented in Appendix E. The fault tree quantification results, cut sets and importance rankings, are in Appendix F. Finally, sensitivity analysis results are presented in Appendix G.

2. SCOPE OF STUDY

This study documents an analysis of the operational experience of the Babcock & Wilcox 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 are not included in the models. A Babcock & Wilcox RPS description is provided followed by a description of the RPS fault trees 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

Two generic RPS configurations are representative of all Babcock & Wilcox plants. Each plant's RPS closely matches one of these two generic configurations. Among the individual plants there are only minor variations of hardware and test practices and the most significant of these are noted in the applicable parts of the text. These two designs are based on the Davis-Besse RPS design and the Oconee RPS design. Table 2-1 shows which plants are grouped into the generic designs:

Table 2-1. Babcock & Wilcox RPS configuration table.

Plant Name	Design Group
Oconee Units 1, 2, and 3	Oconee
Three Mile Island Unit 1	Oconee
Crystal River Unit 3	Oconee
Arkansas Unit 1	Oconee
Davis-Besse	Davis-Besse

The RPS trips the reactor by removing holding power from the control rod drive motors (CRDMs). Each holding power supply receives dc power from a Main and a Secondary power source. In order to release the rods, both the main and secondary power supplies must be interrupted. This is accomplished by either; opening trip breakers on both power supplies, or by removing gating power (gating power controls the operation of the SCRs to move or hold the rods) from the silicon-controlled rectifiers (SCRs).

The most important difference between these RPS configurations is the trip breaker and SCR configurations. The Oconee design uses two ac trip breakers (one on each power supply to all the CRDMs) and four dc trip breakers (each dc trip breaker consists of two dc contacts). The dc trip breakers supply holding power to CRDMs on the safety rod groups 1–4. The four dc trip breakers are arranged so that each breaker supplies one side of the power to two safety rod group CRDM holding power supplies. The diverse electronic trip in the Oconee design removes gating power to the SCRs that provide holding power to the regulating rods.

The Davis-Besse design uses four ac trip breakers (two in series on each holding power supply to the CRDMs). These supply power to the CRDMs of control rod groups 1–8. The Davis-Besse design also provides a diverse electronic trip to all rod groups utilizing the SCRs, which remove gating power to the SCRs that provide holding power to all rods.

2.1.2 System Segment Description

The Babcock & Wilcox RPS is a complex control system comprising numerous electronic and mechanical components that combine to provide 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 Babcock & Wilcox RPS components can be roughly divided into four segments—channels, trip modules, trip breakers/diverse trip, and rods—as shown in Table 2-2.

Table 2-2. Segments of Babcock & Wilcox RPS.

	RPS Segments			
RPS Group	Channels	Trip Modules	Trip Breakers/Diverse Trip	Rods
Oconee	Four channels (A–D). Each channel includes instrumentation and bistables to measure plant parameters provide a trip output.	Four trip modules, one for each channel. Each trip module consists of four relays energized by each of the four channels. The relays are configured so that any two-out-of-four will trip its associated breaker(s) or SCR relays.	Two ac breakers and four dc breakers. Each breaker consists of the mechanical portion, the undervoltage device, and shunt trip device. Channels C & D remove gating power from SCRs in rod groups 5, 6, and 7 for the diverse electronic trip.	Rod groups 1–4 de-energized on successful RPS actuation. Rod groups contain 8–12 rods. The diverse electronic trip uses rod groups 5, 6, and 7.
Davis-Besse	Four channels (A–D). Each channel includes instrumentation and bistables to measure plant parameters provide a trip output.	Four trip modules, one for each channel. Each trip module consists of four relays energized by each of the four channels. The relays are configured so that any two-out-of-four will trip its associated breaker or SCR relays.	Four ac trip breakers. Two in series for each CRDM power supply. Each breaker consists of the mechanical portion, the undervoltage device, and shunt trip device. Channels C & D remove gating power from SCRs in Rod groups 1–8 for the diverse electronic trip.	Rod groups 1 – 8 de-energized on successful RPS actuation. Rod groups contain 8–12 rods.

There are typically 69 control rod assemblies grouped for control and safety purposes into eight groups. Four rod-groups function as safety groups, three rod-groups function as regulating rods, and one group serves to regulate axial power peaking. A typical rod grouping is shown in Table 2-3. The trip breakers interrupt power to the CRD mechanisms. When power is removed, the roller nuts disengage from the lead screw allowing gravity to insert the control rod assembly.

One rod group has been shown to maintain the Reactor Coolant System pressure below the ASME Service Condition C limits (approximately 3000 psi) for anticipated transients evaluated by Anticipated Transient Without Scram (ATWS) studies.[10] Consistent with previous studies, the reported RPS unavailability is based on a safety 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 control rods is needed to achieve hot, zero power provided that the inserted rods are suitably uniformly distributed. This is more conservative than the ASME Service Condition C limits. 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.

Table 2-3. Typical rod grouping arrangement.

Group Identifier	Number Of Control Rod Assemblies
Safety Group 1	8
Safety Group 2	12
Safety Group 3	9
Safety Group 4	12
Regulating Group 5	12
Regulating Group 6	4
Regulating Group 7	4
Axial Power Shaping Group 8	8
Total	69

2.1.3 System Operation

The RPS system as shown in Figure 2-1 (Oconee) and Figure 2-2 (Davis-Besse) consists of four identical protective channels, each terminating in a trip relay within a reactor trip module. In the normal untripped state, each protective channel passes current to the channel trip relay holding it energized as long as all inputs are in the normal energized (untripped) state. Should any one or more inputs become de-energized (tripped), the channel trip relay in that protective channel de-energizes. Each channel trip relay controls power to one of four trip module relays in its own channel and one in each other channel. When the trip relay de-energizes, each corresponding trip module relay de-energizes, opening two of eight contacts in each trip module. It will take at least one more channel trip relay to complete a trip signal to the breakers.

The channel portion of the RPS, channels A through D, includes many different types of trip signals, as shown in Table 2-4. The trip signals include various neutron flux indications, reactor pressure, temperature, flow, primary containment pressure, and others. Most of the signals involve four sensor/transmitters (or process switches). Shown in the simplified RPS diagrams in Figure 2-3 and Figure 2-5 are sensor/transmitters and trip units associated with the reactor vessel high pressure and high temperature trip signals. (These two signals, along with others, are appropriate for several plant upset conditions, such as main steam isolation valve (MSIV) closure, loss of feedwater, and various losses of electrical loads.) Also shown in the figures are the manual scram switches. The sensor/transmitters are located throughout the plant, while the bistable trip units and relays are located in the RPS cabinets in the control room. A loss of electrical power to a sensor/transmitter or bistable trip unit would result in a trip signal.

The reactor trip modules are given the same designation as the protective channel whose trip relay they contain and in whose cabinet they are physically located. Thus, the protective channel A reactor trip module is located in protective channel A cabinet, etc. The coincidence logic in each reactor trip module

controls one breaker in the control rod drive (CRD) power system. Channels C and D also control gating power to SCRs through another set of relays.

2.1.3.1 Oconee Group Breaker Logic.

Figure 2-1 shows a simplified diagram of the Oconee RPS system and Figure 2-3 shows a functional logic diagram of the Oconee RPS system. The coincidence logic contained in RPS channel A reactor trip module controls breaker A in the CRD. Channel B reactor trip module controls breaker B, channel C reactor trip module controls dc breaker pair C1 and C2, and channel D reactor trip module controls dc breaker pair D1 and D2. In addition, channels C and D control gating power to silicon-controlled rectifiers (SCRs). Breakers A and B control all the 3-phase main and secondary power to the CRDs. Breakers C1, C2, D1, and D2 control the dc power to rod groups 1 through 4. The diverse electronic trip uses relays to remove gating power from SCRs that control the regulating rod groups 5 through 7.

The undervoltage coils of the CRD breakers receive their power from the protective channel associated with each breaker. The manual reactor trip switch is interposed in series between each reactor trip module logic and the assigned breaker's undervoltage coil.

Each reactor trip breaker contains a relay installed with its operating coil in parallel with the existing undervoltage device. The output contacts of these relays control the power to the shunt trip devices. Thus, when power is removed from the breaker undervoltage trip attachment on either a manual or automatic trip signal, the shunt trip attachment is energized to provide an additional means to trip the breaker.

The Oconee electronic SCR trip is shown in Figure 2-4. The electronic SCR trip is a diverse means of interrupting power to the CRDMs. The CRD control system is made up of nine power supplies. Four of these power supplies supply power to the safety rod groups 1 – 4. Four of these power supplies supply power to the regulating rod groups 5 – 7 and the axial shaping rods (group 8). One of the power supplies is the auxiliary power supply, which is used for control of selected rods in place of the group power supplies. The electronic SCR trip removes gating power to the regulating rods (groups 5 – 7) by the trip of channels C and D.

The electronic SCR trip does not remove power from the safety rod groups and instead removes power from the regulating rods. In the case where the trip of the safety rods is unavailable, and the electronic SCR trip functions, all regulating rods (groups 5 – 7, 20 rods) are assumed to be required to insert.

2.1.3.2 Davis-Besse Group Breaker Logic.

The coincidence logic contained in RPS channel A reactor trip module controls breaker A in the CRD system as shown in Figure 2-2, which shows a simplified diagram of the Davis-Besse RPS system and Figure 2-5, which shows a functional logic diagram of the Davis-Besse RPS system. Channel B reactor trip module controls breaker B, channel C reactor trip module controls breaker C, and channel D reactor trip module controls breaker D. In addition, channels C and D control gating power to SCRs. Breakers A, B, C, and D control all the three phase primary power to the CRDs. SCRs control the gating power to all rod groups as a diverse method of removing power from the CRDs.

The undervoltage coils of the CRD breakers receive their power from the protective channel associated with each breaker. The manual reactor trip switch is interposed in series between each reactor trip module logic and the assigned breaker's undervoltage coil.

Each reactor trip breaker contains a relay installed with its operating coil in parallel with the existing undervoltage device. The output contacts of these relays control the power to the shunt trip devices. Thus, when power is removed from the breaker undervoltage trip attachment on either a manual or automatic trip signal, the shunt trip attachment is energized to provide an additional means to trip the breaker.

The electronic SCR trip is shown in Figure 2-6. The electronic SCR trip is a diverse means of interrupting power to the CRDMs. The CRD control system is made up of nine power supplies. Four of these power supplies supply power to the safety rod groups 1 – 4. Four of these power supplies supply power to the regulating rod groups 5 – 7 and the axial shaping rods (group 8). One of the power supplies is the auxiliary power supply, which is used for control of selected rods in place of the group power supplies. SCRs are also used to control return power from all rod groups.

When Channel C sends a trip signal to trip breaker C, it also sends a trip signal to a group of ten relay coils (channel D functions similarly). The first nine of these coils control gating power to each of the nine power supplies. Both sides of power must be removed to disengage a rod group (e.g., relay C1 and D1 must open to disengage safety rod group 1). The tenth relay coil removes gating power from its corresponding return power SCR.

Table 2-4. Oconee RPS trip signals.

Trip Signal	Trip Logic	Purpose of Trip
1. Over power	2-out-of-4 coincidence	Prevent an inadvertent power increase at power
2. Nuclear over power based on flow and imbalance	2-out-of-4 coincidence	Prevent operation with a departure from nucleate boiling ratio (DNBR) <1.30
3. Reactor coolant pump power	2-out-of-4 coincidence	Redundant to low flow reactor trip
4. Reactor outlet temperature [a]	2-out-of-4 coincidence	Prevent operation with a DNBR <1.30
5. Pressure/Temperature	2-out-of-4 coincidence	Prevent excessive power density
6. Reactor coolant pressure [a]	2-out-of-4 coincidence	Protect integrity of the reactor coolant system (RCS) pressure boundary
7. Reactor building pressure	2-out-of-4 coincidence	Anticipate loss of coolant
8. Main turbine trip	2-out-of-4 coincidence	Minimize primary system upset on turbine trip
9. Loss of main feedwater	2-out-of-4 coincidence	Prevent loss of heat sink

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

2.1.3.3 Channel Bypass

A channel bypass is provided to allow maintenance and periodic testing to be performed on individual channels. When initiated, the channel bypass prevents the terminating relay of the bypassed channel from de-energizing (tripping). Therefore, when a channel is bypassed, the overall system trip coincidence is two-out-of-three. If two of the remaining three channels trip, all four RPS channels will de-energize their associated CRDM trip channels. The bypass is initiated using key-switches and when one channel is bypassed, an interlock prevents the other channels from being bypassed.

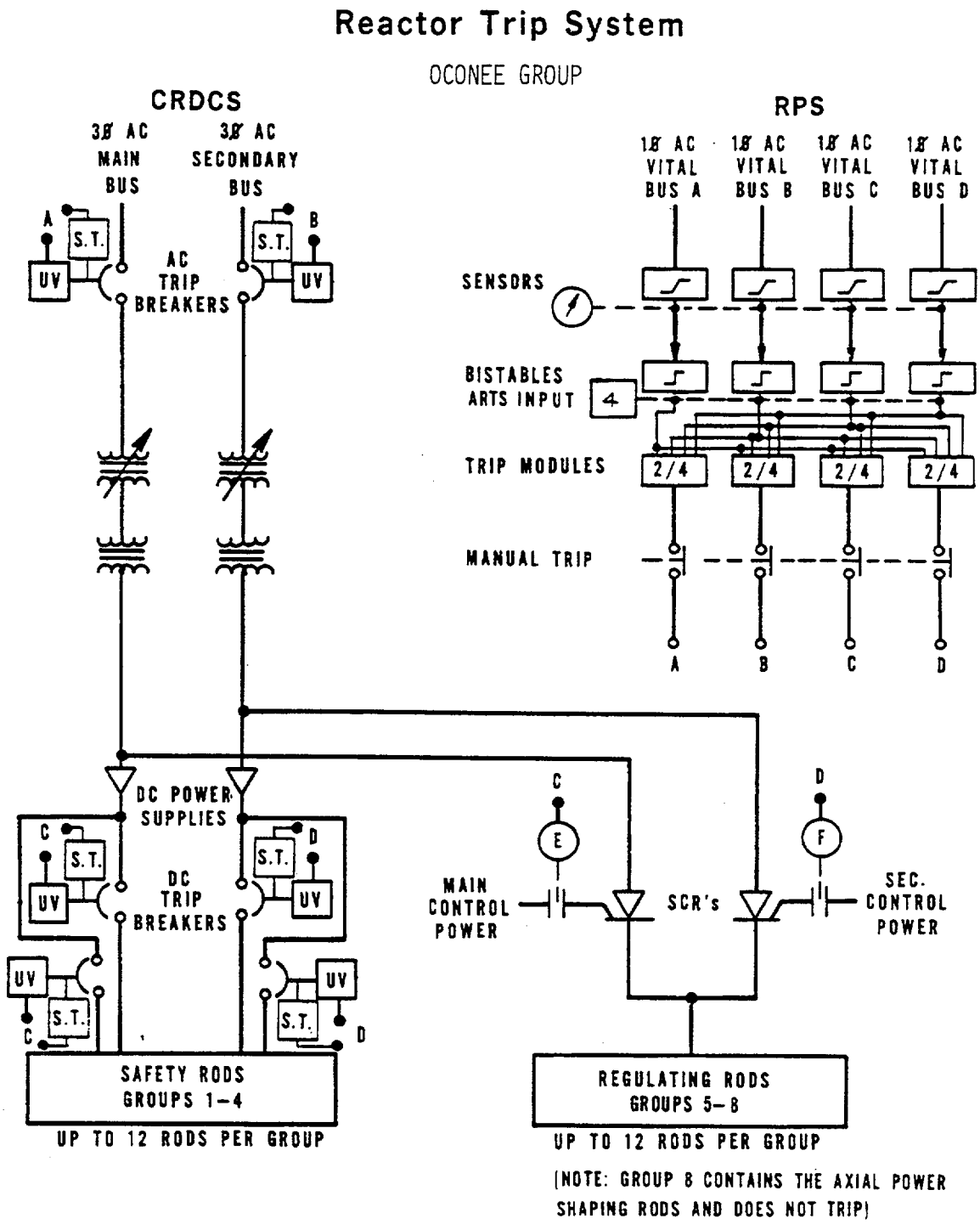


Figure 2-1. Babcock & Wilcox Oconee RPS integrated system diagram.

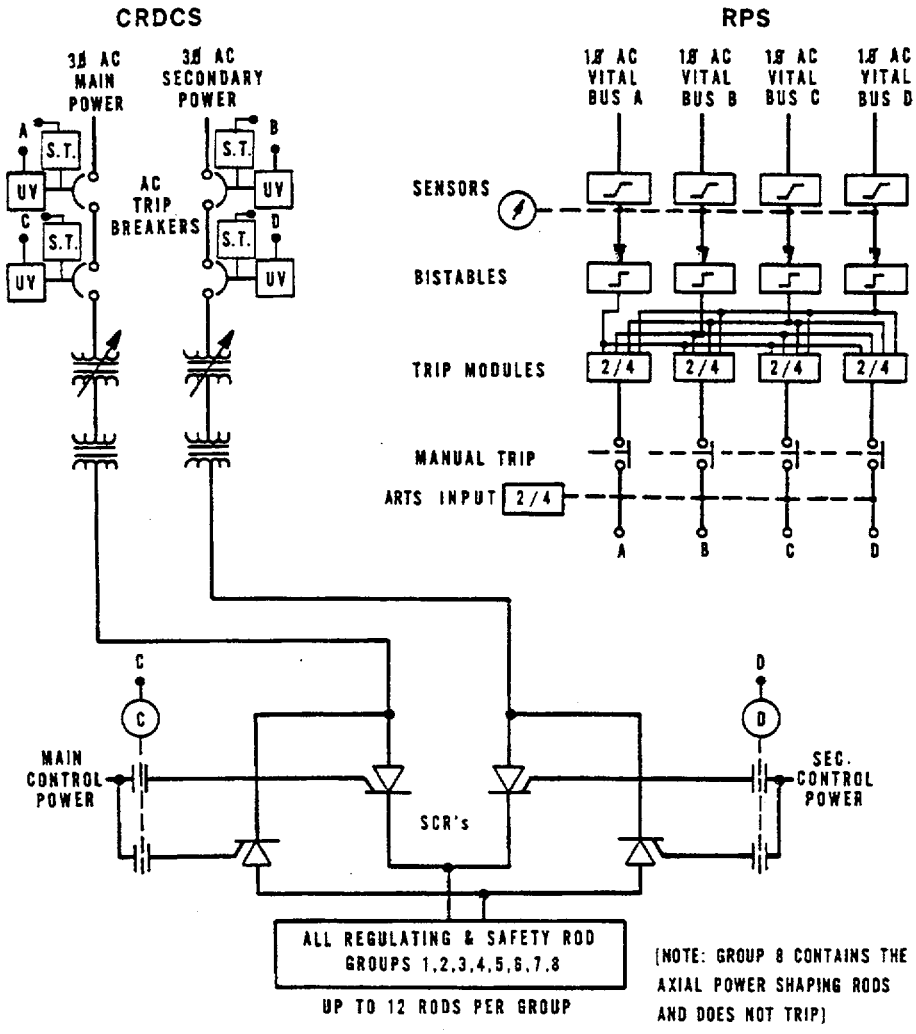


Figure 2-2. Babcock & Wilcox Davis-Besse design RPS integrated system diagram.

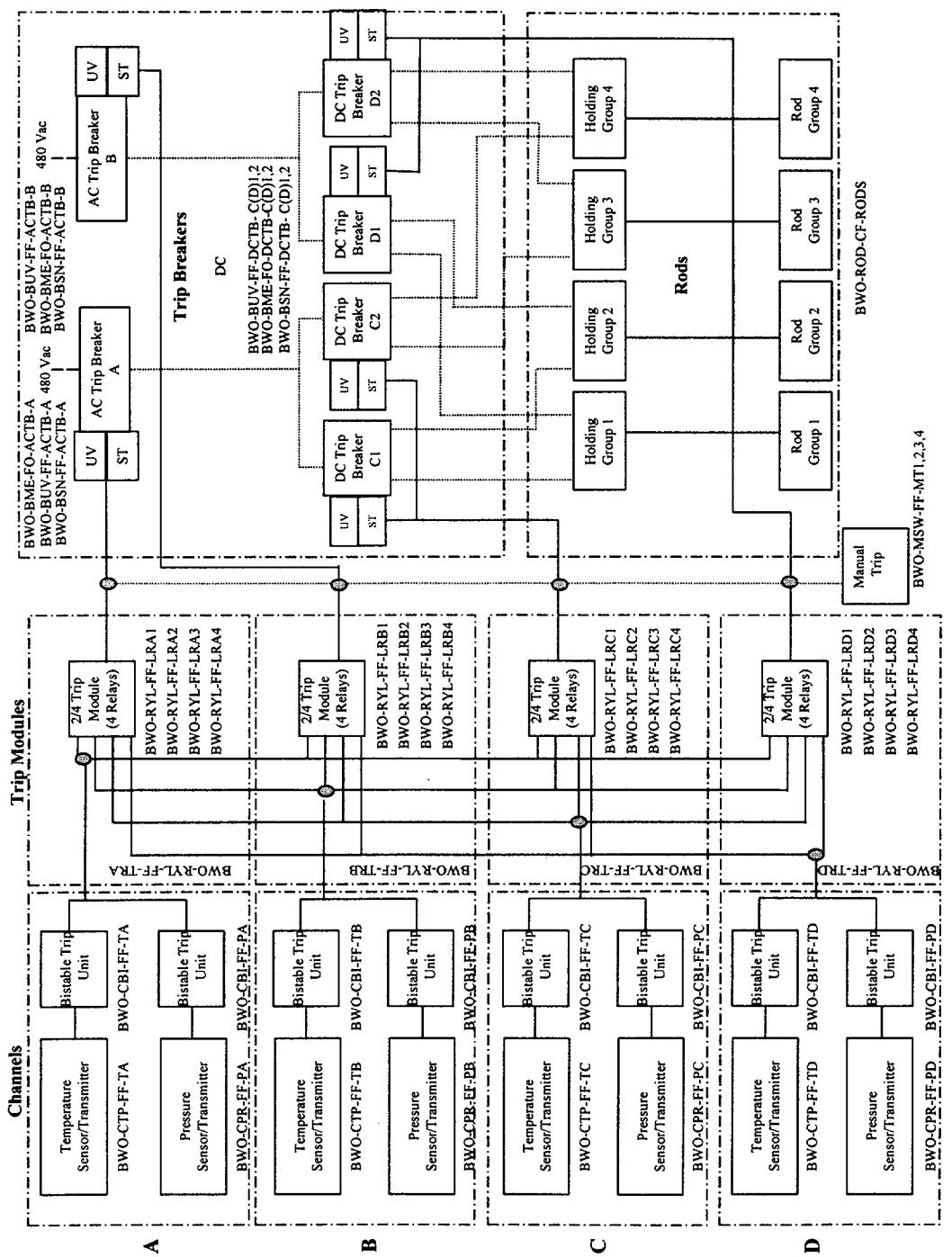


Figure 2-3. Babcock & Wilcox Oconee RPS simplified diagram.

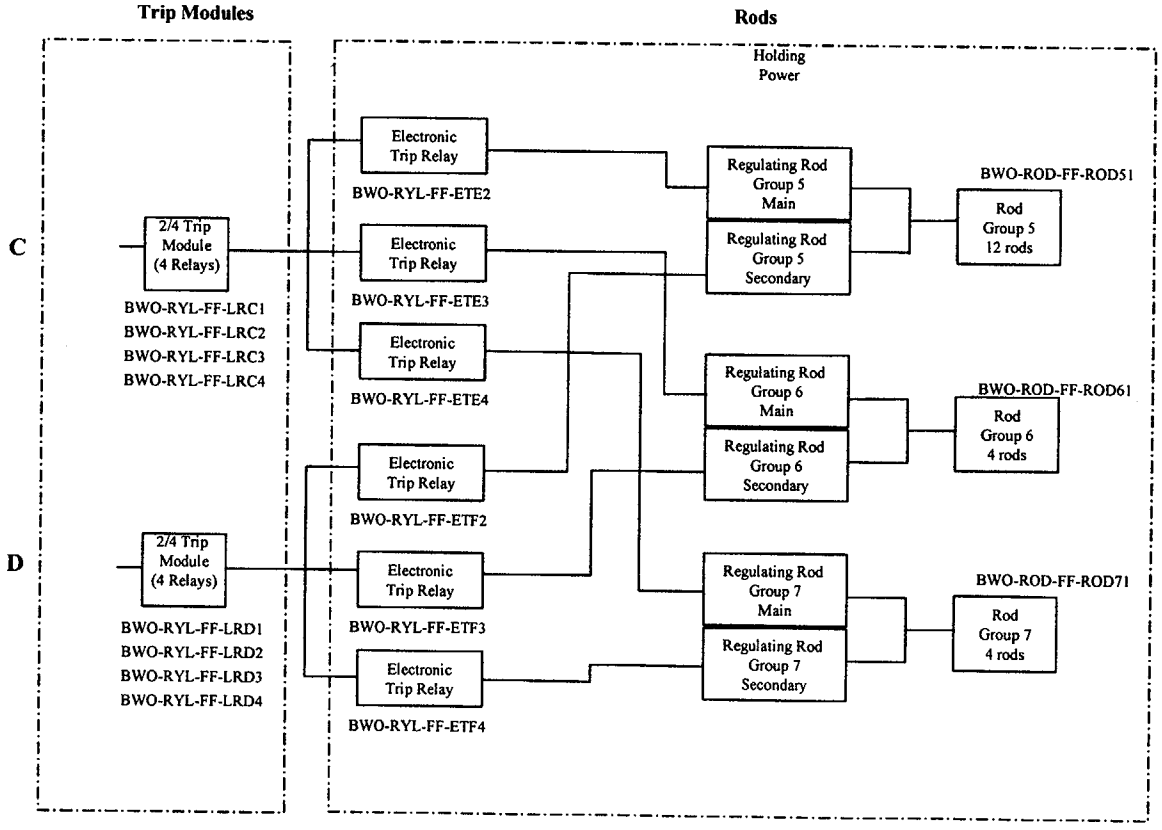


Figure 2-4. Babcock & Wilcox Oconee SCR electronic trip simplified diagram.

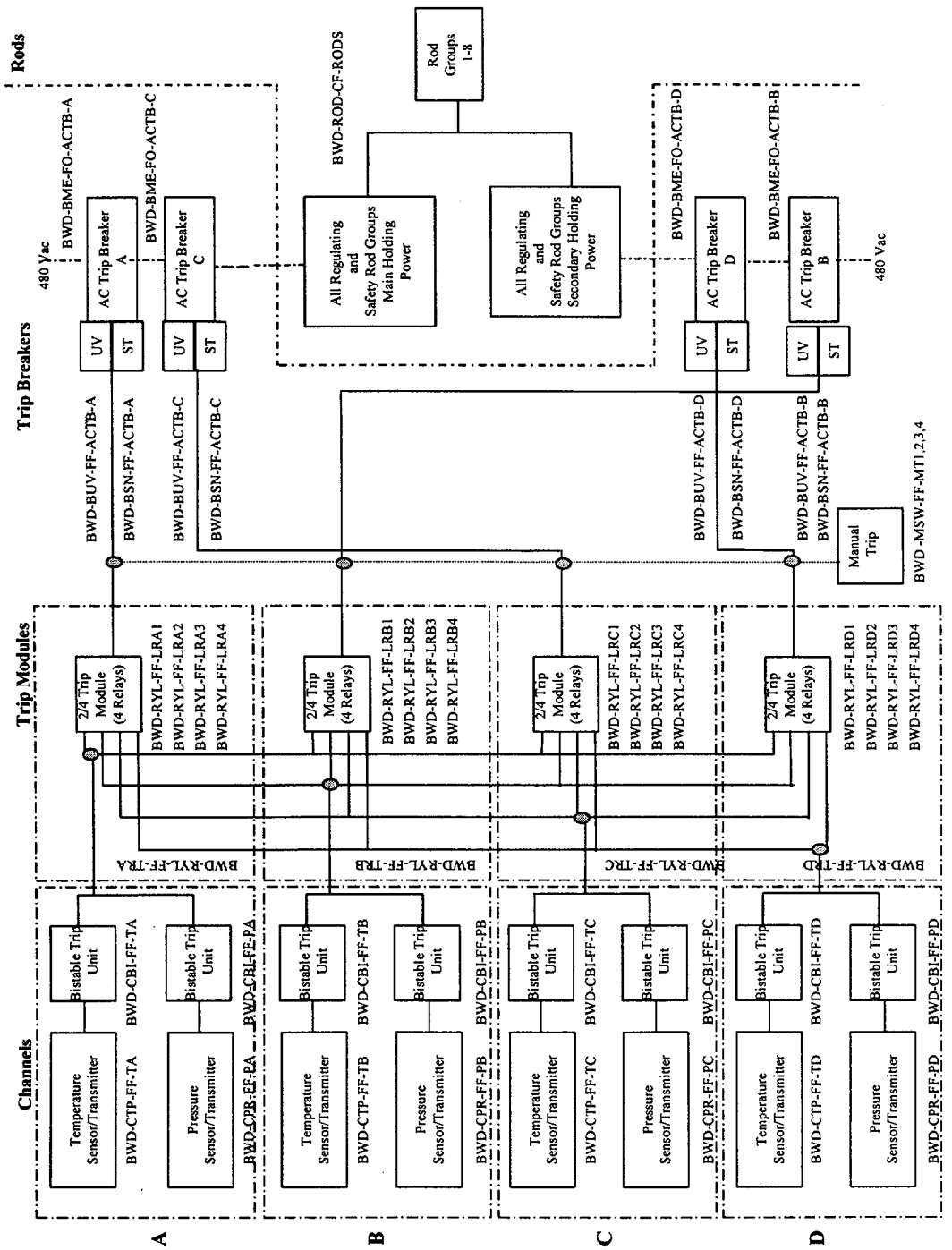


Figure 2-5. Babcock & Wilcox Davis-Besse RPS simplified diagram.

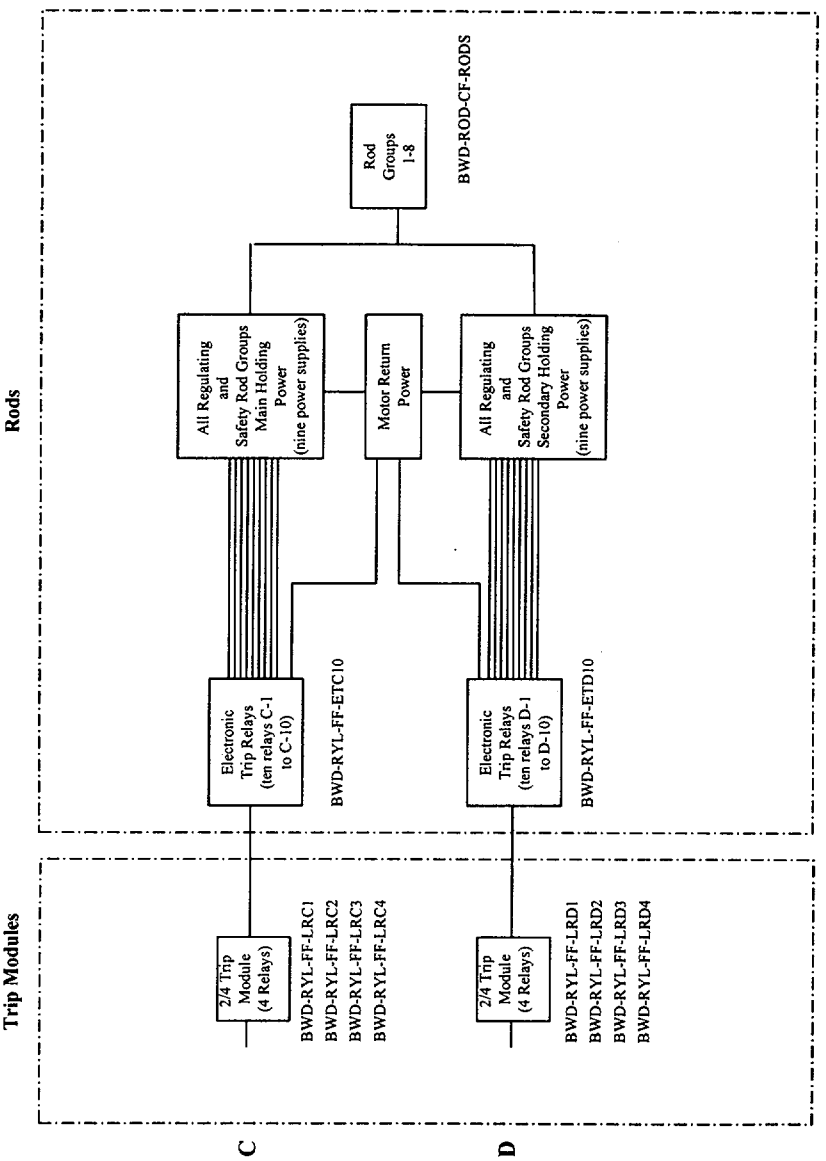


Figure 2-6. Babcock & Wilcox Davis-Besse SCR electronic trip simplified diagram.

2.1.4 System Testing and Component Population

Table 2-5 shows the components in the RPS system, and when these components are counted as being demanded based on reactor trips and testing. The table also flags operating components. These components have certain failure modes that are detected and repaired on an ongoing basis, unrelated to testing.

Several different types of tests are performed periodically on the Babcock & Wilcox 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 will identify gross failures in the channel sensor/transmitters.

Table 2-6 shows the counts of the components, which are used for the calculation of demands on those components.

2.1.5 System Boundary

The RPS boundary for this study includes the four segments indicated in Table 2-2. Also included is the control room operator who pushes the manual reactor trip buttons. The Anticipatory Reactor Trip System (ARTS), which is shown as a trip input in Figure 2-1 and Figure 2-2, is not included in the analysis.

Table 2-5. Babcock & Wilcox RPS component demand and count basis.

Comp. code	Component	Testing Frequency [a]	Operating [b]	Demanded in each reactor trip	Count Basis
Channel					
CPR	Pressure sensor/transmitter	Cyclic & monthly[c]	Yes	No	1 per channel
CTP	Temperature sensor/transmitter	Cyclic & monthly[c]	Yes	No	2 per loop per channel
CBI	Bistable	Monthly	No	No	9 trips per channel
Trains					
RYL	Logic relay	Monthly [d]	No	No	5 per channel
SCR	Silicon-controlled rectifier	Monthly [e]	No	No	6*4 safety rod groups+12*4 reg. rod groups
MSW	Manual scram switch	Monthly	No	Yes [f]	4
Trip breakers and rods					
BME	Breaker mechanical	Monthly [g]	No	Yes	6; 2 ac, 4 dc Oconee design 4 ac Davis-Besse design
BSN	Breaker shunt device	Monthly	No	No [h]	1 per breaker, 6 total Oconee design, 4 total Davis-Besse design
BUV	Breaker undervoltage coil	Monthly [g]	No	No [h]	1 per breaker, 6 total Oconee design, 4 total Davis-Besse design
RMA	Control rod drive and rods	Cyclic	No	Yes	61 to 69 NPRDS failure data not collected after 3/15/1994

Notes:

a. Information from BAW-10167A, V1 Section 2 (May 1986). This report justifies a switch from monthly to semiannual testing of channels on a staggered basis. However, after a check of all B&W plants, none have adopted this change for the period covered by this report.
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.
c. In the monthly channel tests, responsiveness of the sensor/transmitter signal conditioning is verified.
d. Four relays (one in each trip module unit) each receive three demands in each monthly test. The fifth relay receives one demand in each monthly test.
e. Each monthly test includes 3 demands (from combinations of 2/4 channel test inputs).
f. Demanded in manual trips, not automatic trips.
g. Seven breaker demands/month: one from the shunt and six from the UV.
h. 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.

Table 2-6. Babcock & Wilcox RPS component counts for components used in the model.

Plant	Model group	Component Code									
		CPR	CTP	CBI	RYL [a]	MSW	BME [b]	BSN	BUV	SCR	RMA
Arkansas 1	1	4	16	36	20	4	6	6	6	72	69
Crystal River 3	1	4	16	36	20	4	6	6	6	72	68
Davis-Besse	2	4	16	36	20	4	4	4	4	72	61
Oconee 1	1	4	16	36	20	4	6	6	6	72	69
Oconee 2	1	4	16	36	20	4	6	6	6	72	69
Oconee 3	1	4	16	36	20	4	6	6	6	72	69
Rancho Seco	1	4	16	36	20	4	6	6	6	72	69
Three Mile Isl 1	1	4	16	36	20	4	6	6	6	72	69

a. Counted as one logic relay for each of the four trip module units, plus four dc logic relays within each unit.
b. The breakers are four paired dc breakers and two ac breakers in the Model group 1 plants; and four ac breakers at Davis-Besse.

2.2 System Fault Tree

This section contains a brief description of the Babcock & Wilcox RPS fault trees developed for this study. The actual fault trees are presented in Appendix D. The analysis of the Babcock & Wilcox RPS is based on representative Oconee and Davis-Besse designs. It should be noted 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 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 safety rods inserting into the core to inhibit the nuclear reaction. Various plant upset conditions can result in differing requirements for the minimum number of control rods to be inserted into the core, and the positions of the control rods within the core can also be important. One rod group has been shown to maintain the Reactor Coolant System pressure below the ASME Service Condition C limits (approximately 3000 psi) for anticipated transients evaluated by Anticipated Transient Without Scram (ATWS) studies.[10] The safety rod failure criterion was chosen to be 20 percent (or more) of the safety rods fail to insert following the removal of power to all rod holding power supplies. In the case of the Oconee diverse electronic trip, all of the regulating rods are required to insert.

The level of detail in the RPS fault tree includes sensor/transmitters, bistable trip units, relays, trip 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 Service Condition 3 reactor coolant pressure limit. This representative event is modeled in the fault tree as reactor coolant pressure and reactor outlet temperature (see Table 2-4). These are two parameters that would also detect several types of other 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 assuming that a channel out for testing or maintenance is placed into the bypass mode, rather than a tripped mode. Channel test and maintenance outages are modeled in Channel A. There is no test and maintenance outage 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.

The diverse electronic trips are modeled for both RPS designs. The electronic SCR trip in the Oconee model is based on the trip of the logic relays in channels C and D. While the success of channels A and B to open the ac trip breakers will remove power from the regulating rods in the diverse section, these same two trip breakers will remove power from the safety rod groups. Modeling the special situations where either A or B fails and C or D fails introduces significant complexity to the model without a corresponding reduction in the overall unavailability.

The electronic SCR trip section of the Davis-Besse fault tree model is also based on the trip of the logic relays in channels C and D, which removes power from the electronic trip relays (ten per channel). The ten electronic trip relays individually remove gating power from each groups main and secondary power supplies and a motor-return power supply. It was decided to model only the motor-return supply portion of the trip. This part of the trip de-energizes all rod groups. More sophisticated rod/relay failure criteria are not necessary to quantify the electronic SCR trip segment.

2.3 Operational Data Collection, Characterization, and Analysis

The RPS data collection, characterization, and analysis process is shown in Figure 2-7. 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. A more detailed explanation of the process is presented in Appendix A.

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 a 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 a 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 a NF event is a trip unit with its trip setting slightly out of specification, but which is still able to open 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).

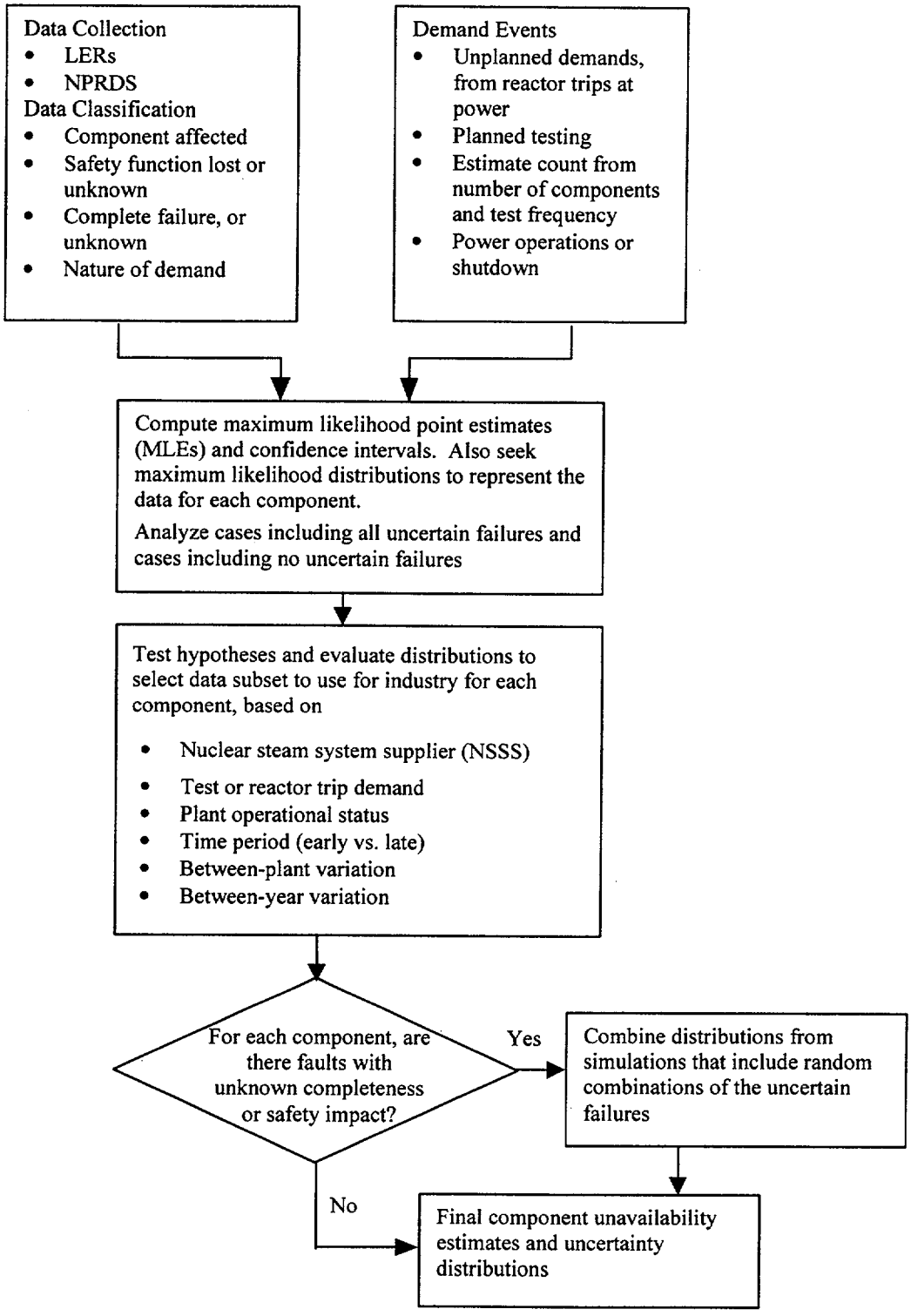


Figure 2-7. Data collection, characterization, and analysis process.

A summary of the data classification scheme is presented in Table 2-7. 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.

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 600 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, although 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 felt 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 2-7, 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 2-7 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 2-8 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.

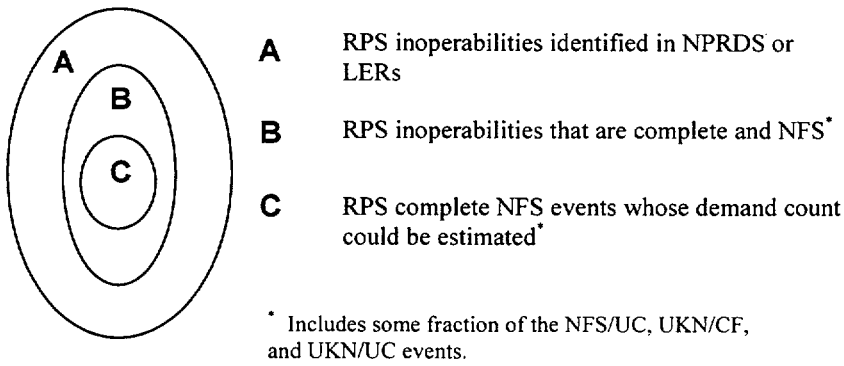


Figure 2-8. RPS data sets.

The purpose of the engineering analysis is to provide qualitative insights into RPS performance. The engineering analysis focused on data set B in Figure 2-8, 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 Babcock & Wilcox RPS is evaluated at the system level, with no consideration of plant-to-plant variations in RPS designs, then a system failure probability can 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 231 demands (unplanned reactor trips). Assuming a Jeffreys noninformative prior and applying a Bayesian update with this evidence results in an RPS mean unavailability of 2.2E-3, with a lower 5th percentile of 8.5E-6 and an upper 95th percentile of 8.3E-3. (See Appendix A for more details on the Bayesian update process. The Jeffreys noninformative prior assumes one-half failure in one demand if no failures occurred.) Because no failures occurred, the uncertainty bound on this estimate is broad. In addition, the estimate is most likely a conservative upper bound on RPS performance during that period, given previous estimates of RPS unavailabilities (Section 3.3).

This system level, Jeffreys noninformative prior, failure estimate is based on no system failures and a limited number of system demands. Therefore, the estimated unavailability is believed to be conservatively high. In order to obtain a more realistic RPS unavailability estimate with a smaller uncertainty band, an RPS fault tree was developed, as discussed in the following section. That approach could make use of additional RPS component failure data.

3.2 Unavailability Estimates Based on Component Operational Data

3.2.1 Fault Tree Unavailability Results

The Babcock & Wilcox RPS fault trees presented in Appendix D and discussed in Section 2.2 were quantified using the SAPHIRE computer code.[11] 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 Babcock & Wilcox RPS data and other PWR vendors as necessary. Failure data is 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. Vendor pooling is shown in Table C-1 in Appendix C.

Table 3-1. Babcock & Wilcox RPS fault tree independent failure basic events.

Component 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	BWD-BME-FO-ACTB-A,B,C,D BWO-BME-FO-ACTB-A,B BWO-BME-FO-DCTB-C1,C2,D1,D2	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	BWD-BSN-FF-ACTB-A,B,C,D BWO-BSN-FF-ACTB-A,B BWO-BSN-FF-DCTB-C1,C2,D1,D2	3 (3.0)	5,786	Sampling	Lognormal	2.3E-4 6.1E-4 1.2E-3	Shunt trip device local faults
BUV	Undervoltage device	BWD-BUV-FF-ACTB-A,B,C,D BWO-BUV-FF-ACTB-A,B BWO-BUV-FF-DCTB-C1,C2,D1,D2	6 (7.5)	34,708	Plant	Lognormal	1.1E-4 2.3E-4 4.0E-4	Undervoltage coil device local faults
CBI	Trip unit (bistable)	BWO(BWD)-CBI-FF-PA,B,C,D BWO(BWD)-CBI-FF-TA,B,C,D	4 (4.0)	15,571	Year	Lognormal	1.3E-4 2.9E-4 5.5E-4	Channel trip unit (bistable) fails to trip at its setpoint
CPR[c]	Pressure sensor/ transmitter	BWO(BWD)-CPR-FF-PA,B,C,D	1 (2.3)	17,536	Plant	Lognormal	4.0E-6 1.6E-4 6.0E-4	Channel reactor vessel pressure sensor/ transmitter fails to detect a high pressure and send a signal to the trip unit

Table 3-1 (Continued)

Component 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
CTP	Temperature sensor/ transmitter	BWO(BWD)-CTP-FF-TA,B,C,D	0 (1.5)	17,070	Plant	Lognormal	6.3E-6 1.2E-4 4.1E-4	Channel reactor vessel level sensor/ transmitter fails to detect a low level and send a signal to the trip unit
MSW[c]	Manual scram switch	BWO(BWD)-MSW-FF-MT1,2,3,4	2 (2.0)	19,789	N/A	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 (2.0)	189,536	Plant	Lognormal	3.5E-7 1.7E-5 6.4E-5	Control rod (or associated control rod drive) fails to insert fully into core upon demand
RYL[c]	Logic Relay	BWO(BWD)-RYL-FF-LRA,B,C,D –1,2,3,4 BWO(BWD)-RYL-FF-TRA,B,C,D BWO-RYL-FF-ETE2, ETE3, ETE4, ETF2, ETF3, ETF4 BWD-RYL-FF-DC10, DD10	7 (7.2)	362,420	Plant	Lognormal	6.8E-6 2.1E-5 4.6E-5	Channel or trip system logic 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-7 for more detail on which vendors were pooled.

Table 3-2. Babcock & Wilcox 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	BWD-BME-CF-TB2OF4	3	Lognormal	8.0E-8 7.1E-7 2.2E-6	CCF 2 of 4 trip breaker local hardware faults
		BWO-BME-CF-TB2OF6-4G	3	Lognormal	1.7E-7 1.0E-6 3.0E-6	CCF 2 or More of 6 Trip Breakers That Fail Two or More Groups
BSN	Shunt trip device	BWD-BSN-CF- TB2OF4	0	Lognormal	3.8E-6 2.3E-5 6.7E-5	CCF 2 of 4 shunt trip device local faults
		BWO-BSN-CF-TB2OF6-4G	0	Lognormal	5.6E-6 5.5E-6 1.8E-5	CCF 2 or More of 6 Trip Breaker Shunt Trip Devices That Fail Two or More Groups
BUV	Undervoltage device	BWD-BUV-CF- TB2OF4	0	Lognormal	1.4E-6 7.5E-6 2.1E-5	CCF 2 of 4 undervoltage coil device local faults
		BWO-BUV-CF-TB2OF6-4G	0	Lognormal	3.5E-6 1.2E-5 2.9E-5	CCF 2 or More of 6 Trip Breaker Undervoltage Trip Devices That Fail Two or More Groups
CBI	Trip unit (bistable)	BWO(BWD)-CBI-CF-CBI4OF6TM	71	Lognormal	7.3E-8 8.7E-7 2.9E-6	CCF specific 4 of 6 CBIs (T&M)
		BWO(BWD)-CBI-CF-CBI6OF8	71	Lognormal	1.3E-8 4.0E-7 1.5E-6	CCF specific 6 of 8 CBIs
CPR[a]	Pressure sensor/ transmitter	BWO(BWD)-CPR-CF-P2OF3TM	36	Lognormal	2.8E-6 6.4E-6 1.2E-5	CCF 2 of 3 CPRs (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
		BWO(BWD)-CPR-CF-P3OF4	36	Lognormal	4.4E-7 2.1E-6 5.4E-6	CCF 3 of 4 CPRs
CTP	Temperature sensor/ transmitter	BWO(BWD)-CTP-CF- T2OF3TM	0	Lognormal	1.7E-7 5.0E-6 1.9E-5	CCF 2 of 3 CTPs (T&M)
		BWO(BWD)-CTP-CF- T3OF4	0	Lognormal	2.4E-8 1.5E-6 5.8E-6	CCF 3 of 4 CTPs
MSW[a]	Manual Trip Switch	BWO(BWD)-MSW-CF-2OF4	0	Lognormal	6.4E-7 5.4E-6 1.7E-5	CCF specific 2 of 4 manual trip switches
PWR	dc power	BWO(BWD)-PWR-CF-TB2OF4	N/A	Lognormal	2.3E-7 2.5E-6 8.3E-6	CCF specific 2 of 4 trip breaker shunt trip device power
RMA (ROD and CRD)[a]	Control rod and associated control rod drive	BWO(BWD)-ROD-CF-RODS	2	Lognormal	1.2E-9 4.1E-8 4.6E-7	CCF 50% or more CRD/rods fail to insert
RYL[a]	Logic Relay	BWO(BWD)-RYL-CF-LR6OF12TM	0	Lognormal	7.0E-9 5.9E-8 1.8E-7	CCF specific 6 of 12 logic relays (T&M)
		BWO(BWD)-RYL-CF-LR9OF16	0	Lognormal	2.4E-9 3.3E-8 1.2E-7	CCF specific 9 of 16 logic relays
		BWO(BWD)-RYL-CF-TR2OF3TM	0	Lognormal	1.6E-7 1.1E-6 3.2E-6	CCF 2 of 3 trip relays (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
		BWO(BWD)-RYL-CF-TR3OF4	0	Lognormal	1.9E-8 3.3E-7 1.2E-6	CCF 3 of 4 trip relays
		BWD-RYL-CF-LR3OF8	0	Lognormal	1.5E-7 8.4E-7 2.3E-6	CCF specific 3 of 8 logic relays for diverse trip
		BWD-RYL-CF-LR2OF6TM	0	Lognormal	6.3E-7 2.5E-6 6.2E-6	CCF specific 2 of 6 logic relays for diverse trip (T&M)

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

Table 3-3. Babcock & Wilcox RPS fault tree other basic events.

Basic Event	Distribution	Lower Bound, Mean, Upper Bound	Basic Event Description	Notes
BWO(BWD)-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.
BWO(BWD)-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.

Table 3-3 (Continued)

Basic Event	Distribution	Lower Bound, Mean, Upper Bound	Basic Event Description	Notes
BWO-RMA-FF-1OF20REG		7.1E-6 3.4E-4	1 Regulating Rod out of 20 Fails to Insert	Represents a pre-calculated OR gate for any 1 of 20 regulating rods to insert (20 * 1.7E-5)
BWO-RMA-FF-1OF20SAF		1.3E-3	1 Safety Rod out of 20 Fails to Insert	
BWD-PWR-FF-ACTB-A BWD-PWR-FF-ACTB-B BWD-PWR-FF-ACTB-C BWD-PWR-FF-ACTB-D	Lognormal	2.3E-6 6.0E-5 2.3E-4	AC Trip Breaker A,B,C,D Shunt Trip Device DC Power Fails	125 Vdc power to the shunt trip fails (1.0E-5/h * 6h repair time)[a]
BWO-PWR-FF-ACTB-A BWO-PWR-FF-ACTB-B BWO-PWR-FF-DCTB-C1,2 BWO-PWR-FF-DCTB-D1,2	Lognormal	2.3E-6 6.0E-5 2.3E-4	AC Trip Breaker A,B Shunt Trip Device DC Power Fails DC Trip Breaker C1, C2, D1, D2 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 12 (Table 4, p. 23). The six-hour repair time was estimated from the reactor trip breaker maintenance duration in Reference 13.

The CCF event probabilities in Table 3-2 are based on the Babcock & Wilcox RPS CCF data during the period 1984 through 1998 pooled with other vendors using the same pooling described in Table C-1 in Appendix C. However, the CCF event probabilities are also influenced by the prior used in the Bayesian updating of the common-cause alpha parameters. The prior for this study was developed from the overall PWR RPS CCF database. A summary of the Babcock & Wilcox 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 0.12 to 0.001 on the total component failure probabilities in Table 3-1.

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).

Using the RPS basic event mean probabilities presented in Table 3-1 through Table 3-3, the Babcock & Wilcox RPS mean unavailability (failure probability upon demand) is 7.8E-7 (Oconee design) and 1.6E-6 (Davis-Besse design) with no credit for manual trip by the operator. If credit is taken for manual trip, then the RPS mean unavailability is 8.7E-9 (Oconee design) and 8.4E-7 (Davis-Besse design). Operator action reduces the RPS unavailability by approximately 99 percent in the Oconee model and by 37 percent in the Davis-Besse model. 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.

RPS segment (channel, trip module, trip breaker/electronic trip, and rods) contributions to the overall demand unavailability are summarized in Table 3-4. Surprisingly, neither model shows significant contribution from the trip breakers/diverse trip segment. All cutsets with the trip breakers also have an event with the failure of the electronic trip relays, which reduces the cutset probability to a small value and decreases its importance. Otherwise, the results for the two models are different. The Oconee model shows no contribution from the rods segment and the Davis-Besse model shows a significant contribution from this segment. This is because of the separation of the rods that are dropped by the diverse electronic trip. The Oconee design trips the safety rods with the trip breakers and the regulating rods with the diverse trip. This has the effect of having both a diverse means of tripping rods and a diverse group of rods that are tripped in the Oconee model. Oconee cutsets with the safety rods also have an event for the failure of at least one of the regulating rods. The Davis-Besse design trips the entire rod holding power with both means. The cutsets with the safety rods have no other failures. When the diverse trip is removed from both models, the overall RPS unavailability and segment contributions are similar for both models. See Appendix G for further details.

Another way to segment the Babcock & Wilcox 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 to the overall unavailability. The results are presented in Table 3-5. For the Babcock & Wilcox Oconee RPS design, the CCF contribution to overall RPS unavailability is >99.9 percent. For the Babcock & Wilcox Davis-Besse RPS design, the CCF contribution to overall RPS unavailability is >99.9 percent.

Table 3-4. Babcock & Wilcox RPS unavailability.

RPS Segment	Unavailability (Point Estimate) with No Credit for Manual Scram by Operator		Unavailability (Point Estimate) with Credit for Manual Scram by Operator	
	Percent	Unavailability	Percent	Unavailability
	Oconee RPS Model			
Channel	51.9%	4.1E-07	46.5%	4.1E-09
Trip Modules	48.0%	3.7E-07	42.9%	3.7E-09
Trip Breakers/Diverse Trip	0.0%	0.0E+00	7.2%	6.2E-10
Rods	0.0%	2.9E-10	3.3%	2.9E-10
Total Oconee RPS	100.0%	7.8E-07	100.0%	8.7E-09
	Davis-Besse RPS Model			
Channel	25.1%	4.1E-07	0.5%	4.0E-09
Trip Modules	23.0%	3.7E-07	0.4%	3.7E-09
Trip Breakers/Diverse Trip	0.0%	3.0E-11	0.0%	3.0E-11
Rods	52.0%	8.4E-07	99.1%	8.4E-07
Total Davis-Besse RPS	100.0%	1.6E-06	100.0%	8.5E-07

Table 3-5. Babcock & Wilcox RPS failure contributions (CCF and independent failures).

RPS Segment	No Credit for Manual Scram by Operator		Credit for Manual Scram by Operator	
	Contribution from CCF Events	Contribution from Independent Failures	Contribution from CCF Events	Contribution from Independent Failures
	Oconee RPS Model			
Channel	51.9%	<0.1%	46.5%	<0.1%
Trip Modules	48.0%	<0.1%	42.9%	<0.1%
Trip Breakers/Diverse Trip	0.0%	<0.1%	7.2%	<0.1%
Rods	0.0%	<0.1%	3.3%	<0.1%
Total Oconee RPS	>99.9%	<0.1%	>99.9%	<0.1%
	Davis-Besse RPS Model			
Channel	25.1%	<0.1%	0.5%	<0.1%
Trip Modules	23.0%	<0.1%	0.4%	<0.1%
Trip Breakers/Diverse Trip	0.0%	<0.1%	0.0%	<0.1%
Rods	52.0%	<0.1%	99.1%	<0.1%
Total Davis-Besse RPS	>99.9%	<0.1%	>99.9%	<0.1%

Various 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 Babcock & Wilcox RPS fault tree cut sets listed in Appendix F. The fault tree uncertainty analysis was performed 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 alpha'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 alpha's were obtained from the methodology discussed in Appendix E. Each of the alphas 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 Babcock & Wilcox RPS fault tree model are shown in Table 3-6.

Table 3-6. Babcock & Wilcox fault tree model results with uncertainty.

	5%	Median	Mean	95%
Oconee Model				
No credit for manual trip by operator	1.3E-7	4.6E-7	7.8E-7	2.4E-6
Credit for manual trip by operator	1.8E-9	5.5E-9	8.7E-9	2.5E-8
Davis-Besse Model				
No credit for manual trip by operator	2.6E-7	9.6E-7	1.6E-6	4.8E-6
Credit for manual trip by operator	3.1E-8	2.9E-7	8.4E-7	3.2E-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 (Babcock & Wilcox) 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).[14] 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 8 or more of 41 safety group rods must fail to insert in order to fail to achieve a hot shutdown state, which is a much less conservative failure criterion. In addition, the RPS models in this report include the diverse electronic trip function, which is unique to the B&W RPS models.

Also, Babcock & Wilcox in 1986 analyzed the channel and trip system portion of the RPS (excluding the CRD and control rod portions) and obtained RPS mean unavailabilities of 1.1E-6 for the Oconee design and 1.1E-9 for the Davis-Besse design.[15] The RPS results from the Oconee and Davis-Besse designs in the present study indicate an unavailability of 7.8E-7 to 1.6E-6 respectively, which is slightly lower than the Oconee result and significantly larger than the Davis-Besse result. The referenced results from Reference 15 are based on an hourly rate, which is calculated for a month's unavailability. In addition, common-cause failures of relays are considered insignificant and the model only contains multiple independent failures of relays and did not include the CRD and control rod portions of the RPS. Therefore, comparisons between the results of this study and the results in Reference 15 are not appropriate.

The CRD and safety rod segment contributes less than 0.1 percent to the Oconee and 52 percent to the Davis-Besse RPS unavailability in the present study (see Table 3-4).

Finally, RPS unavailability estimates from the PWR IPEs are presented in Table 3-7 and Figure 3-1. The RPS unavailability estimates range from 1.0E-6 (mean) to 5.0E-6 (mean). Details concerning modeling and quantification of the RPS unreliability in these IPEs are generally limited. In addition, Figure 3-1 shows the Babcock & Wilcox RPS unavailability distributions obtained in this study. The Crystal River 3 and Three Mile Island 1 IPEs assumed success of the RPS.

Table 3-7. Summary of plant review for Babcock & Wilcox RPS unavailability values.

Plant	IPE/PRA RPS Unavailability	Notes
Arkansas Nuclear One Unit 1[16]	5.00E-6	Electrical portion estimated at 1E-5, which does not include the diverse electronic trip. The diverse electronic trip was estimated at 0.1. Operator non-recovery was estimated at 0.5.
Davis-Besse[17]	1.00E-6	Based on predicted values without a detailed model. The failure is only based on a common-cause failure of the control rods.
Oconee 1, 2, and 3[18]	1.01E-6	A fault tree is presented in the IPE with rods, breakers, operator action, and logic relays to the breakers. Operator error was estimated at 0.001. Rods estimated at 1.0E-6.
Three Mile Island Unit 1	N/A	RPS success assumed.
Crystal River	N/A	RPS success assumed.

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. Operator error varies from 0.5 to 0.001. Despite these differences, the reported values are within an order of magnitude of this studies result.

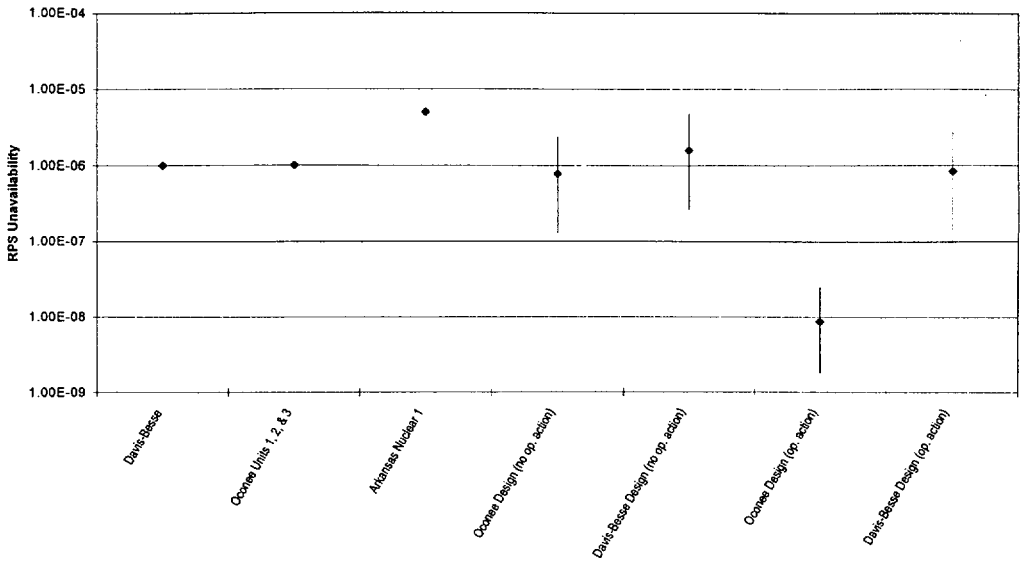


Figure 3-1. Babcock & Wilcox IPE and RPS Study RPS unavailabilities.[1]

3.3.1 Arkansas Nuclear One Unit 1 (ANO-1)

The RPS system unavailability used in the ANO-1 IPE was not specifically analyzed and is based on predicted values. The discussion for the RPS unavailability is presented in Appendix B, Section B.4.1, of the ANO-1 IPE.[16] The RPS unavailability in the ANO-1 IPE is separated into an electrical and a mechanical category. The ANO-1 IPE states that an electrical failure in the RPS was predicted by NRC contractors to be 4.2E-6 in the ANO Interim Report Evaluation Program (IREP). This RPS unavailability was estimated prior to the installation of the Diversified Scram System (DSS) in response to the NRC ATWS Rule. For the ANO-1 IPE, it was estimated that the electrical failure was 1E-5, the DSS failure was conservatively estimated to be 0.1, and the operator recovery (failure to manually trip the reactor) was 0.5. Thus, the RPS unavailability in the ANO-1 IPE for the electrical category was estimated to be 5.0E-6.

The ANO-1 IPE states that the mechanical failure to trip is defined as the inability of the control rods to physically drop into the core due to sticking. The ANO-1 IPE goes on to state that the RPS unavailability due to mechanical failure was found to be from one-half to one-fifth of that due to electrical failure before operator recovery was considered for the Sequoyah and Surry plants evaluated in NUREG/CR 4500. A value of 5.0E-6 was chosen for the RPS mechanical failure probability in the ANO-1 IPE.

3.3.2 Davis-Besse

The RPS unavailability used in the Davis-Besse IPE was not specifically analyzed and is based on predicted values and a detailed model was not developed for the RPS or DSS. The discussion for the RPS unavailability is presented in Section 2.2.11 of the Davis-Besse IPE.[17] The RPS unavailability in the Davis-Besse IPE is based on previous reliability studies of the trip signals and operation of the system components. The IPE indicated that the reliability of the trip systems is expected to be very high.

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

However, previous system investigations did not specifically address the potential for common-cause failure of the control rod assemblies to insert due to mechanical binding. Therefore, the failure of the RPS and DSS was reflected in the sequence logic by a single event representing common-cause failure of the control rod assemblies to insert following a trip signal. The probability of RPS failure was estimated based on a review of PWR operating experience and treatment of the common-cause failure mode used in other PRAs. An RPS unavailability of 1.0E-6 was estimated for this failure mode.

3.3.3 Oconee 1, 2, and 3

The RPS unavailability used in the Oconee IPE is estimated by a detailed model (i.e., fault tree) developed for the RPS. The model includes only the rods, breakers, operator action, and logic relays to the breakers. A detailed discussion and fault tree model for the Oconee RPS is presented in Appendix A of the Oconee IPE.[18] A diagram of the RPS, operating conditions, RPS trip summary, surveillance requirements, and operating incidents are included in the detailed discussion contained in Appendix A of the Oconee IPE. The reliability data for the basic events contained in the RPS fault tree as well as the fault tree cut sets result are also presented in the appendix. Operator error is estimated at 0.001. From the RPS fault tree results, the RPS unavailability for the Oconee IPE is estimated to be 1.01E-6. The cut set results for the RPS fault tree are dominated by the rods cut set, which represents an insufficient number of control rods drop into the core upon trip which is estimated by a failure probability of 1.0E-6.

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,[19] 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 Babcock & Wilcox RPS unavailabilities ranged from 1.5E-5 to 6.0E-5. The Babcock & Wilcox RPS unavailability obtained in this report is 7.8E-7 (Oconee design) and 1.6E-6 (Davis-Besse design) with no credit for manual trip by the operator. These values are significantly lower than the 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-5 for CCF of two of four breakers (undervoltage coil and shunt trip failure, or mechanical failure). Both of the study results are lower than the 1983 document values. Therefore, the observed reactor trip breaker performance has improved since 1983.

In 1988, Babcock & Wilcox obtained approval to change RPS channel testing procedures.[15,20] 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 (Table 3-4), obtained with only two trip signals modeled, indicate that the channels contributed approximately 52 percent for Oconee and 25 percent for Davis-Besse designs to the overall RPS unavailability. With the low RPS unavailability for both designs, we do not see this relatively large contribution from the channels as a problem.

We generally expect the trip breaker segment to be the highest contributor to RPS unavailability. However, both Babcock & Wilcox designs have implemented an electronic diverse trip system. The addition of the electronic diverse trip system has the effect of reducing the importance of the trip breaker segment since the trip breakers and the diverse electronic trip relays must fail together. This can be seen by examining the cutsets in Appendix F. For a more detailed discussion of the sensitivity of the model to the electronic diverse trip, see Appendix G, Section G-3.

4. ENGINEERING ANALYSIS OF THE OPERATIONAL DATA

An analysis of trends is presented in this section based on overall system performance, total component performance, and CCF component performance. The methodology for evaluating the trends is presented in Section A-3.

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 ten failures in 1986 to a low of zero in 1995. In addition, a review of CCF counts in Table B-2 of Appendix B indicates two CCF events from 1984 to 1998. Detailed analyses of trends with time for component failure probabilities and CCFs, presented in Section 4.3, indicate no trends in events that dominate the RPS unavailability.

As indicated in Section 3.1, there were no RPS failures during the period 1984 through 1998. 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. Figure 4-1 shows that the rate of demands among Babcock & Wilcox plants has decreased since the middle 1980's. This trend is similar to the trend among Westinghouse, Combustion Engineering, and General Electric plants. When 1984, the year with the most reactor trips, is removed from the analysis, the decreasing trend is still statistically significant[2] (p-value[3] less than 0.00005). In this case, the trend line slopes from 4.9 scrams per reactor-operating year in 1985 to 0.8 in 1998, rather than the plotted 6.3 in 1985 to 0.7 in 1998.

4.2 Component Evaluation

Over 600 LER and NPRDS records were reviewed for the Babcock & Wilcox 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 NFS/CF and was added to the events already in the NFS/CF bin.) Babcock & Wilcox 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).

---

[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.

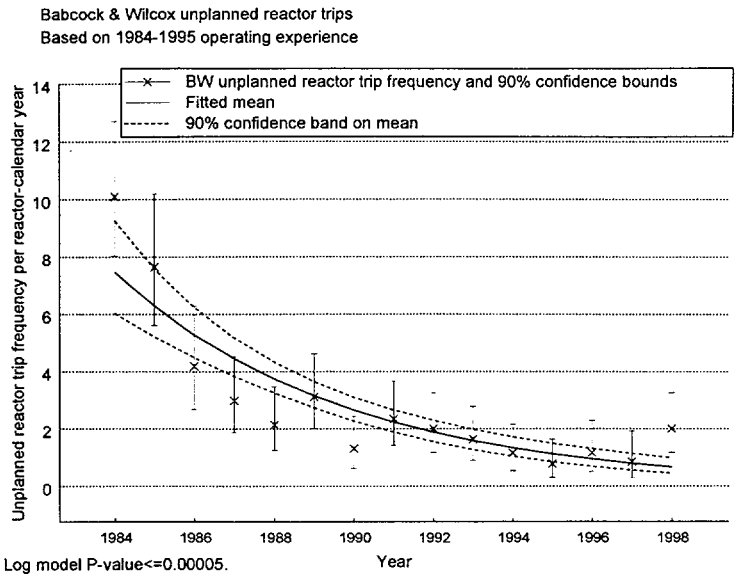


Figure 4-1. Trend analysis for Babcock & Wilcox unplanned reactor trips, per plant operating year.

Evaluations were performed for the overall rate 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 case used all complete losses of a component's RPS safety function. Another case included the upper bound 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, which 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, adequate new test data for 1996-1998 was not available for this study. The trend analysis for these Babcock & Wilcox components was therefore restricted to 1984-1995.

Figure 4-2 shows the total Babcock & Wilcox failure count for this period, normalized by the number of reactor-calendar years in the period. The trend is not statistically significant (p-value 0.017). The individual component failure frequencies, computed from the failure counts and the number of components in the Babcock & Wilcox plants in each year from 1984 to 1995, were also evaluated for trends. No trends were found among the sparse data for the individual components.

A final Babcock & Wilcox 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. In this data, the overall failure frequencies and the component-specific failure frequencies were much too sparse to observe trends. For the ten Babcock & Wilcox components evaluated for the unavailability analysis, just four complete losses of the components' safety-function and one uncertain failure were reported in the LERs.

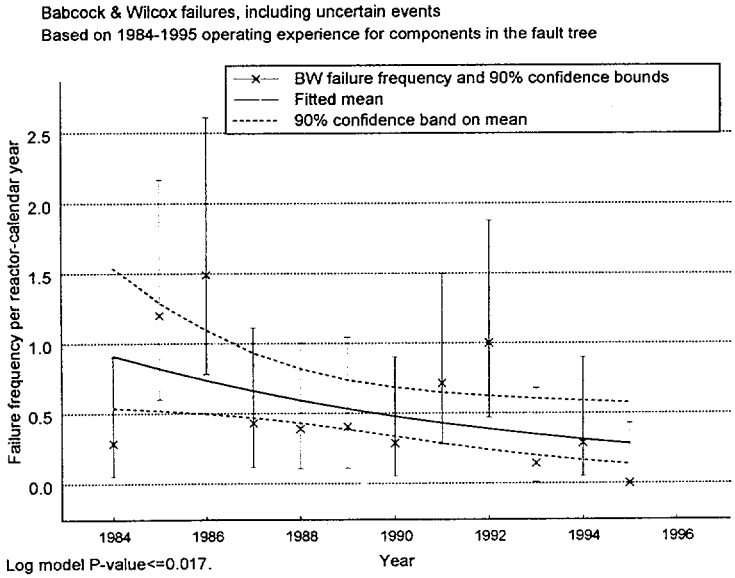


Figure 4-2. Trend analysis for Babcock & Wilcox failures of components in unavailability analysis, per plant year, including uncertain failures.

4.3 CCF Evaluation

The 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 less than 1.0.

Babcock & Wilcox 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. Two potential CCF events were identified for the period 1984 through 1998.

Since the set of data was sparse for the Babcock & Wilcox RPS CCFs, some comments on the general findings over all the RPS studies will be made here. 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 subtlest 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 which prevented a high containment pressure trip or a calibration procedure that gives an incorrect calibration parameter). While neither of these events occurred at a Babcock & Wilcox plant, the mechanisms are generic enough to apply to all vendors designs.

4.3.1 CCF Event Trends

Figure 4-3 shows the Babcock & Wilcox CCF events plotted based on when they occurred. No trend was seen among the two events (p-value 0.70). With so few Babcock & Wilcox CCF events, the CCF evaluation in this study used the pattern of CCF failures shown by the set of all PWR CCF events to form a starting point for assessing the Babcock & Wilcox operational data. Figure 4-4 shows the significant decreasing trend in the overall PWR CCF event frequency (p-value less than 0.00005).

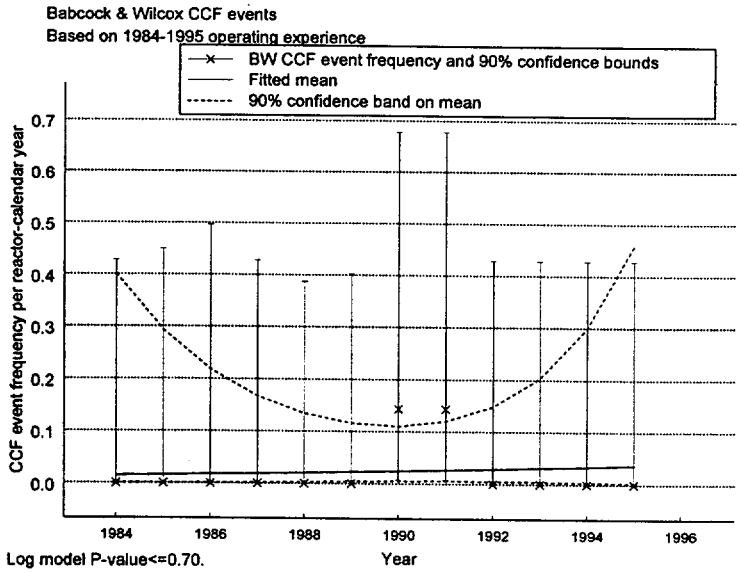


Figure 4-3. Trend analysis for Babcock & Wilcox CCF events per plant calendar year.

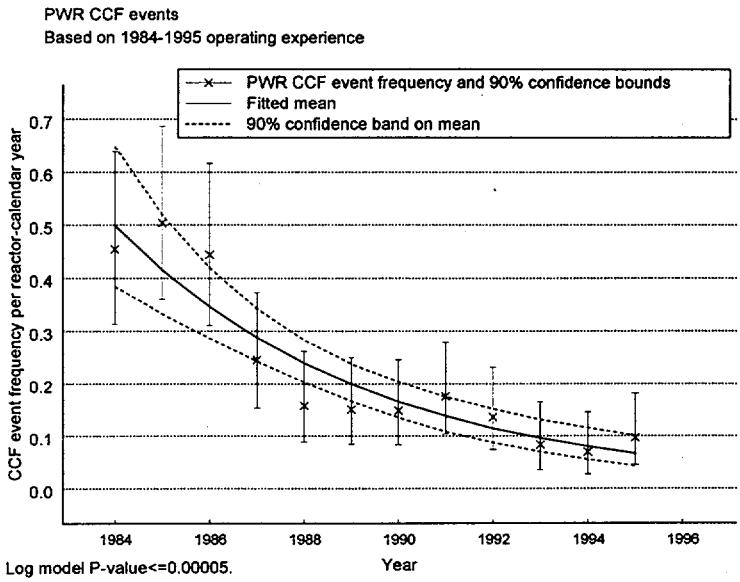


Figure 4-4. Trend analysis for PWR CCF events per reactor calendar year.

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 estimates. In some cases, these data included data from one or both other PWR vendors in addition to the Babcock & Wilcox data.

Three of the probability estimates showed decreasing trends. As shown in Figure 4-5, the logic relays show a decreasing trend in failure probability (p-value 0.0002). The trend in the Babcock & Wilcox and Westinghouse data with the plants operating was significant. Since other statistical tests showed a difference between the data for the 1980's and the 1990's, only the 1990-1995 data were used in the unavailability analysis.

Breaker undervoltage coil failure probability estimates also showed a somewhat significant trend (see Figure 4-6). The linear trend p-value was 0.031. More failures occurred in 1984 and 1985 than in the period since then. A decreasing trend was also observed for the pressure sensor/transmitter rates (see Figure 4-7). The linear trend p-value was 0.038.

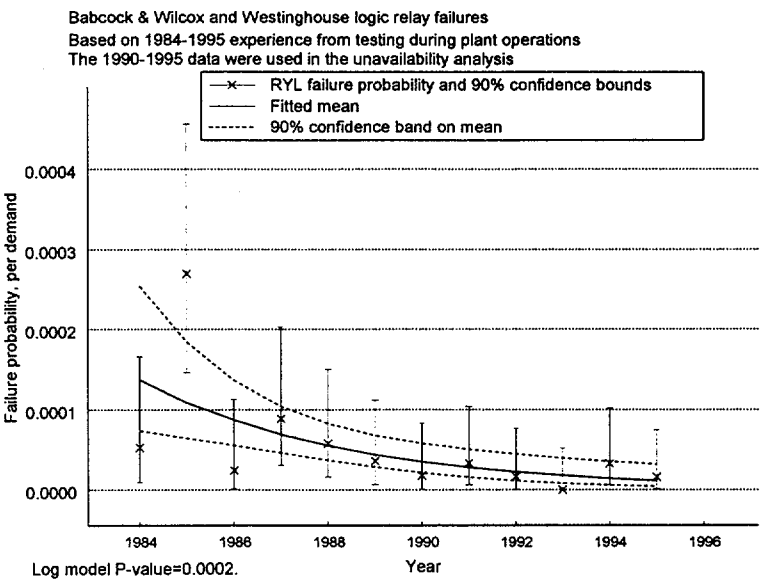


Figure 4-5. Trend analysis for logic relay total failure probability.

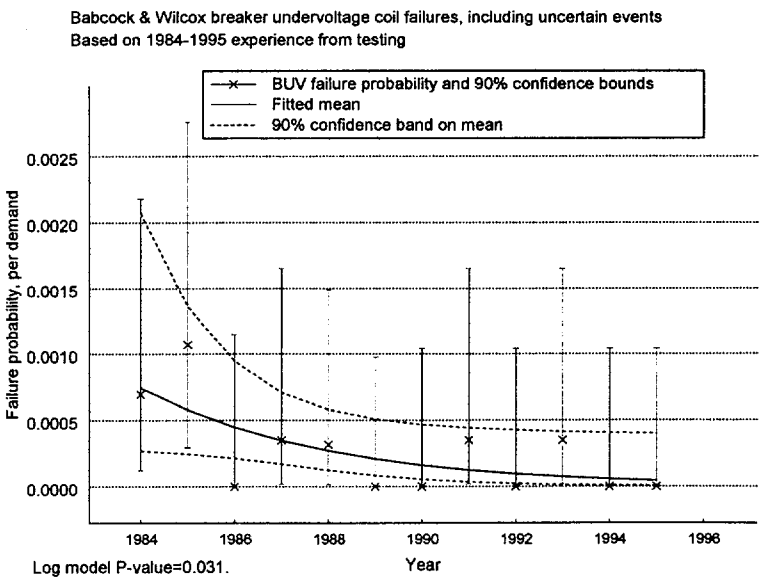


Figure 4-6. Trend analysis for breaker undervoltage coil total failure probability.

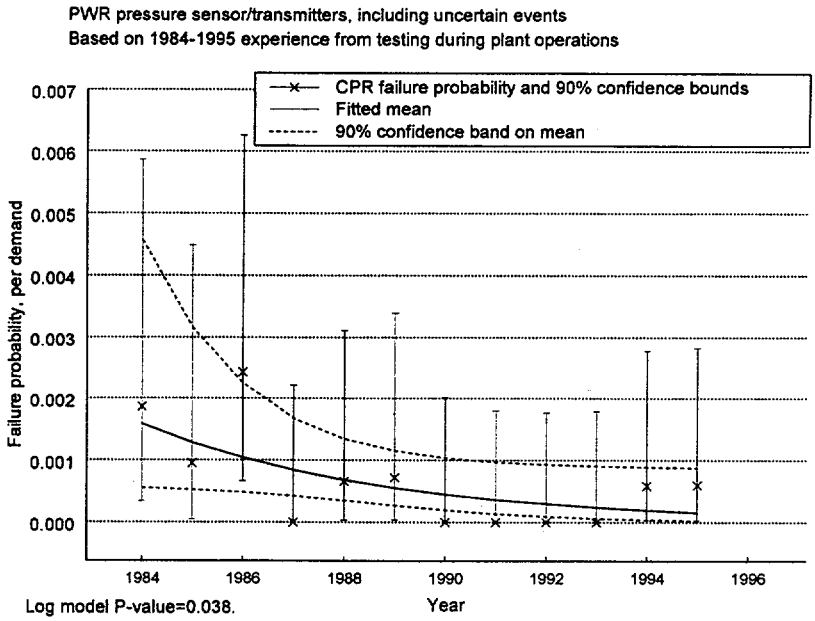


Figure 4-7. Trend analysis for PWR pressure sensor/transmitter total failure probability.

5. SUMMARY AND CONCLUSIONS

Fault trees for the two versions of the B&W RPS were developed and quantified using U.S. B&W commercial nuclear reactor data from the period 1984 through 1998. All B&W plants use a design similar to the Oconee RPS except the Davis-Besse plant. The Davis-Besse design is unique to Davis-Besse and was modeled separately. Table 5-1 summarizes the results of this study.

The computed mean unavailability estimates were 7.8E-7 and 1.6E-6 (with no credit for manual trips). These are comparable to the values given in B&W IPEs, which ranged from 1.0E-6 to 5.0E-6, and other similar reports. Common-cause failures contribute greater than 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 allowing credit for manual scram by the operator (with a failure probability of 0.01). Operator action reduces the RPS unavailability by approximately 99 percent (8.7E-9, Oconee design) and 48 percent (8.4E-7, Davis-Besse design).

Table 5-1. Babcock & Wilcox fault tree model results with uncertainty.

	5%	Mean	95%
Oconee Model			
No credit for manual trip by operator	1.3E-7	7.8E-7	2.4E-6
Credit for manual trip by operator	1.8E-9	8.7E-9	2.5E-8
Davis-Besse Model			
No credit for manual trip by operator	2.6E-7	1.6E-6	4.8E-6
Credit for manual trip by operator	3.1E-8	8.4E-7	3.2E-6

Several general insights were obtained from this study:

- Neither design shows a significant contribution from the trip breakers/diverse trip segment.
- The Oconee design shows no contribution from the rods segment but the Davis-Besse design shows a significant contribution from this segment. This is because of the separation of the rods that are dropped by the diverse electronic trip. The Oconee design trips the safety rods with the trip breakers and the regulating rods with the diverse trip. This has the effect of having both a diverse means of tripping rods and a diverse group of rods that are tripped in the Oconee model. The Davis-Besse design trips all rods with both means.
- 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. Automatic actuation of the shunt trip mechanism within the reactor trip breakers and improved maintenance have resulted in improved performance of these components.
- Overall, trends in unplanned trips at B&W reactors decreased significantly over the time span of this study. Due to sparse data, trends in component failure probabilities and counts of CCF events are not significant in the B&W data. Trends for the pooled PWR overall CCF rate of occurrence used in this study showed a statistically significant decreasing trend. Relays, pressure sensor/transmitters, and undervoltage coils all showed significant decreasing trends.

- The causes of the Babcock & Wilcox CCF events are similar to those of the rest of the industry. That is, over all RPS designs for all vendors for all of the components 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 principal method of detection of failures of components in this study was either by testing or by observation during routine plant tours. No failures were detected by actual trip demands. No change over time in the overall distribution of the 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," *Code of Federal Regulations*, Office of the Federal Registrar, February 25, 1986.

8. The Institute of Nuclear Power Operations, *NPRDS Reportable System and Component Scope Manual, Babcock & Wilcox 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. A.F. McBride, et.al., *Babcock & Wilcox Anticipated Transients Without Scram Analysis*, Topical Report BAW-10099, Revision 1, Babcock & Wilcox, Lynchburg, Virginia, May 1977.

11. 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.

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

13. 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.

14. 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.

References

15. Enzinna, R.S., Levinson, S.H., and Swanson, E.W., *Justification for Increasing the Reactor Trip System On-line Test Intervals*, Prepared for the Babcock & Wilcox Owners Group Technical Specification Committee, BAW-10167 Topical Report, May 1986.

16. Arkansas Nuclear One, Unit 1 Probabilistic Risk Assessment, Individual Plant Examination Submittal for Arkansas Nuclear One, Unit 1, Entergy Operations, Inc. and Science Applications International Corporation and Erin Engineering and Research, Inc., April 1993.

17. Individual Plant Examination for the Davis-Besse Nuclear Power Station, The Toledo Edison Company, February 1993.

18. Oconee Nuclear Station Units 1, 2, and 3 Individual Plant Examination, Duke Power Company, December 1990.

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

20. Thadani, A.C., *NRC Evaluation of BWOG Topical Report BAW 10167 and Supplement 1, "Justification for Increasing the Reactor Trip System On-Line Test Interval"*, Included in latest issue of BAW-10167A Topical Report, August 1992.

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 eight Babcock and Wilcox (Babcock & Wilcox) pressurized water reactor (PWR) plants were considered. For these plants, reported inoperabilities and unplanned actuations were characterized and studied from the perspective of overall trends and the existence of patterns in the system performance. Unlike other operational data-based system studies sponsored by NRR at the 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 rather than viewing the RPS even at a train level.

Descriptions of the methods for the basic data characterization and the estimation of unavailability are provided below. In addition to a discussion of the methods, the descriptions provide summaries of the quality assurance measures used and the reasoning behind the choice of methods. Probabilities coming from the common-cause data analysis are explained in Appendix E.

A-1 DATA COLLECTION AND CHARACTERIZATION

In subsections below, methods for acquiring the basic operational data used in this study are described. 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 current 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 Equipment Performance Information Exchange (EPIX) has been underway. Because development for the EPIX data base 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 to 1998. Particularly, any inoperabilities discovered during unplanned reactor trips should be reported. The 1996-1998 LER data have been reviewed for Babcock & Wilcox plants and for Combustion Engineering (CE) plants, but not for Westinghouse (W) or General Electric (GE) plants.

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 to 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 ARTS circuitry, 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 non-failures and were not considered further.
- For events within the scope of RPS, the specific component affected by the event was indicated. For Babcock & Wilcox 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], power supplies (CPW); analog calculators [reactor flow (CFC) and overpower delta T (CPA)]; and bistables (BIS).

- Trains (logic cabinet): logic relays (RYL), silicon-controlled rectifiers (SCR), and the manual scram switch (MSW).
- Trip breakers: ac and tandem dc breakers (mechanical/electrical) (BME) and the associated reactor trip breaker (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 (UKN). 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 Appendix B and Appendix 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 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 data bases, 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 important 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. Thus, neither the NPRDS nor the LER data provide information on planned maintenance unavailabilities. Maintenance unavailabilities were included in the fault tree, with their associated impact on the RPS actuation logic. The fraction of time RPS channels, trains, and trip breakers are typically in maintenance was estimated directly from the operating procedures rather than from the failure data.

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 600 Babcock & Wilcox 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). 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 Babcock & Wilcox plants, this restriction removed Three Mile Island 1 from the start of the study through September of 1985, Davis-Besse 1 for the last half of 1985 and most of 1986.
- 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 walk-throughs by plant operators, and thus are not present during the monthly 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 non-testing 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. Estimates of component counts, demands, and operating times are discussed in the next three sections.

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 of differences in the component boundary definitions used for this study. Each channel processing module, for example, consists of a collection of NPRDS components.

Table A-2. Babcock & Wilcox RPS components used in the PRA.

Comp. code	Component	Testing Frequency [a]	Operating [b]	Used in each reactor trip	Count Basis
Channel					
CPR	Pressure sensor/transmitter	Cyclic [c]	Yes	No	1 per channel (4 total)
CTP	Temperature sensor/transmitter	Cyclic [c]	Yes	No	2 per loop per channel (16)
CBI	Bistable	Monthly	No	No	9 trips per channel (36 total)
Trains					
RYL	Logic relay	Monthly [d]	No	No	5 per channel (20)
SCR	Silicon-controlled rectifier	Monthly [e]	No	No	6*4 safety rod groups+12*4 reg. rod groups (72 total)
MSW	Manual scram switch	Monthly	No	Yes [f]	2
Trip breakers and rods					
BME	Breaker mechanical	Monthly [g]	No	Yes	6; 2 ac, 4 dc Oconee design
					4 ac Davis-Besse design
BSN	Breaker shunt device	Monthly	No	No [h]	1 per breaker, 6 total Oconee design, 4 total Davis-Besse design
BUV	Breaker undervoltage coil	Monthly [g]	No	No [h]	1 per breaker, 6 total Oconee design, 4 total Davis-Besse design
RMA	Control rod drive and rods	Cyclic	No	Yes	61 to 69, NPRDS failure data not collected after 3/15/1994

a. Information from BAW-10167A, V1 Section 2 (August 1992). This report justifies a switch from monthly to semiannual testing of channels. However, it is not known when (or if) particular plants switched to semiannual testing in 1993 or later, after release of this report. Therefore, this study assumes monthly channel 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.

c. In the monthly channel tests, responsiveness of the bistables is verified, but not the sensor/transmitters. Thus, testing frequency for the sensor/transmitters is cyclic.

d. Four relays (one in each trip module unit) each receive three demands in each monthly test. The fifth relay receives one demand in each monthly test.

e. Each monthly test includes 3 demands (from combinations of 2/4 channel test inputs).

f. Demanded in manual trips, not automatic trips.

g. Seven breaker demands/month: one from the shunt and six from the UV.

h. 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.

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 start-up or shut-down 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. Unplanned reactor trip demands are not used for the RTB shunt trip and undervoltage coils because these events demand both of these components, but a failure of one would not be detected if the other succeeded.

Most of the estimates in this report are therefore based on test data. For Babcock & Wilcox plants, monthly tests apply for trip module components and breakers, and channel components. In addition, the channel instruments are tested and calibrated during refueling outages and cyclic 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 percent, based on a comparison of 1990 NPRDS failure data and component failures that were reported in LERs. As mentioned previously, 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 post-maintenance 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, although the monthly testing occurs only twelve 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 periods. The failure probability in some cases is observed to be higher during the shutdown periods. This phenomenon is attributed to the additional complications introduced by the maintenance being done during shutdowns, rather than to an inadequacy in the monthly testing that occurs at power.

In the remaining subsections of this section, additional details of the methods for estimating the various types of demand counts are outlined.

A-1.2.2.1 Unplanned Demands. The NRC Performance Indicator (PI) data bases 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 data bases have been maintained since 1985 and are a reliable source of LER reactor trip data. The data bases include manual as well as automatic reactor trips.

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 vs. spurious reactor trips, automatic vs. manual reactor trips, and during operation vs. 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, and 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. Monthly test counts were estimated at a plant-year level by assuming twelve 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 various NRC programs. 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 pro-rated between plant operation time and plant shut-down time. For each plant and year, the outage time represented in the OUTINFO data base, including the days on which outages started and ended, was summed. The down time was summed separately and excluded for regulatory-imposed outages (as observed above, Three Mile Island 1, Davis-Besse 1, and Rancho Seco for selected periods in the early years 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 shut-down fraction.

For the current study, the time period covers 1984-1998. Outage data for the period prior to 1986, however, are not readily available. The OUTINFO data base has gaps for periods prior to 1986. For periods in 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 shut-down 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 time 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 shut-down periods for each component type. As needed, these times were converted to hours.

A-2. ESTIMATION OF UNAVAILABILITY

In the subsections below, statistical analysis for each separate component is described, then the combining of failure modes to characterize the total system unavailability and its uncertainty is addressed.

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 three percent error in overall result.

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, ten failure modes were identified, one for each of the ten component types listed in Table A-2. Each is based on the non-fail-safe failures of a particular type of component. Component failure data from the NPRDS and LERs was not available for just one component, namely the 125Vdc power supply to the shunt trip coils (PWR). The power supply failures that were in the data bases were fail safe, tending to cause rather than prevent RPS actuation. Generic data were used for PWR 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.

In subsections below, the processes of selecting particular data sets and estimating probability distributions that reflect uncertainty and variation in the data are described. Finally, a simulation method is described for quantifying the uncertainty in whether certain 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 twelve-year time frame of the study was separated into two periods, from 1984-1989 and from 1990 to 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 time periods. This topic is discussed further in the 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 period 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 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 Babcock & Wilcox analysis.

The pooling across vendor was considered only under the following three conditions. First, there had to be less than three failures in the Babcock & Wilcox data for the an 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 fairly 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 was 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 monthly testing of Table A-2 was used for the Babcock & Wilcox trip breaker data, but bimonthly testing was used for the W breakers and quarterly testing was used for CE 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 notice 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 the 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 to 1989 were compared with the more recent data and the more recent data was used to estimate the failure probability or rate when significant differences were seen. In this evaluation, the added set of data from 1996-1998 was included in the new period if applicable. However, it was rarely applicable. The newest data applies only to the unplanned demands, not to the testing data nor the occurrences in time since no NPRDS data were assessed for this period. The Westinghouse unplanned demand data for 1996-1998 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 there were no significant differences between vendors and less than three Babcock & Wilcox 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 time periods. 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, although 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 towards 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, Babcock and Wilcox generic distributions were sought rather than distributions updated with plant-specific data. Plant-specific evaluations are not in 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 recently become established 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 provided in 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 Babcock and Wilcox 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 non-informative 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 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 two fault trees.

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

$$\text{Prob}(kA) = k\,\text{Prob}(A) \quad \text{for the subsetting operation,}$$

$$\text{Prob}(A*B) = \text{Prob}(A \text{ and } B) = \text{Prob}(A)*\text{Prob}(B), \quad \text{and}$$

$$\text{Prob}(A+B) = \text{Prob}(A \text{ or } B) = 1 - \text{Prob}(\text{not } A)*\text{Prob}(\textit{not } B) = 1 - [1 - \text{Prob}(A)]*[1 - \text{Prob}(B)],$$

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, because 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*, INEL-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*, INEL-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, INEL-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, INEL-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), INEL/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. 52–516

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 is a summary of the data evaluated in the common-cause failure (CCF) data collection effort in support of the Babcock & Wilcox RPS study. Table B-1 lists Babcock & Wilcox independent failure counts by type of component from the source data files and is summarized on a yearly basis. Table B-2 lists the Babcock & Wilcox CCF failure event counts by type of component from the CCF file and is again summarized on a yearly basis. Table B-3 gives a detailed summary of the Babcock & Wilcox CCF events. The tables only show records for those components that are 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 Babcock & Wilcox plants. The second screening separated out the components of interest for the RPS study. The following list shows the components that are included in this summary and a short description of each:

Component	Component Description
BME	Trip breaker mechanical
BSN	Trip breaker shunt trip coil
BUV	Trip breaker undervoltage coil
CBI	Channel bistable (trip unit)
CPR	Channel pressure sensor/transmitter
CTP	Channel temperature sensor/transmitter
CRD	Control rod drive
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; non-fail-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), no failures (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. Babcock & Wilcox RPS independent failure yearly summary, 1984 to 1998.

SYSTEM ROD

Component	Safety Function	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	Total
CRD	UKN									1							1
Summary for 'SYSTEM' = ROD																	
Sum										1							1

SYSTEM RPS

Component	Safety Function	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	Total
BSN	NFS		1	1					1								3
BUV	NFS	2	3		1	1			1	1	1						10
CBI	NFS		1	2				1	2	3							9
CBI	UKN		1	2			1										4
CPR	NFS											2					2
CPR	UKN			2						1							3
CTP	NFS		2	2	1	1	1			1							8
CTP	UKN				1	1	1										3
MSW	NFS							1									1
RYL	NFS			1					1								2
Summary for 'SYSTEM' = RPS																	
Sum		2	8	10	3	3	3	2	5	6	1	2					45
Study Total		2	8	10	3	3	3	2	5	7	1	2					46

Table B-2. Babcock & Wilcox RPS common-cause failure yearly summary, 1984 to 1998.

SYSTEM RPS

Component	**Safety Function**	**1984**	**1985**	**1986**	**1987**	**1988**	**1989**	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**	**1998**	**Total**
CBI	NFS							1									1
CPR	NFS								1								1
Summary for 'SYSTEM' = RPS																	
Sum								1	1								2
Study Total								1	1								2

Table B-3. Babcock & Wilcox 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
CBI	IS	L-XXX-90-1176-IS	1990	PROCEDURES ALLOW THE BISTABLES TO BE CALIBRATED TO TRIP OOS	NFS	1.00	1.00	4	NL	11/27/90	4	0.10
CPR	IS	N-XXX-91-1155-IS	1991	PRESSURE TRANSMITTER OUT OF TOLERANCE	NFS	1.00	0.50	12	NL	11/11/91	1	0.10
										11/11/91	1	0.10
										11/10/91	1	0.10

Notes:

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 Babcock and Wilcox plants during the period 1984 through 1998. However, since relatively few B&W 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 was applicable and the B&W 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, then the channel bistables, then the logic relays, breakers, and rods. For each quantity that is to be estimated, the B&W 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, B&W and CE data combined, and B&W 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 is that pooling for B&W data will be done for pressure sensor/transmitter failures detected in testing, for pressure sensor/transmitter failures in time, for temperature sensor/transmitter failures in time, for logic relay failures, for manual switch failures, for breaker mechanical failures, and for control rods/drives. The pooling is over all three PWR vendors, unless the statistical tests show one vendor to be different from B&W 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, although pooling is recommended for temperature sensor/transmitter failures in time, it is not recommended for pressure sensor/transmitter failures on demand. Failures in time are failures that are detected during visual checks or are annunciated when an sensor for one channel behaves differently from the sensors monitoring the same parameter for other channels. These failures thus represent a different failure mode from failures on demand. B&W and CE have similar data for the failures in time, but the B&W data for the failures on demand show a significantly lower failure probability for B&W plants than for either of the other two PWR vendors. Therefore, because the failure mode behaves differently, a different estimation is used for the two aspects of the temperature sensor/transmitter performance. Similarly, pooling is considered for the mechanical

Table C-1. Vendor differences applicable to B&W 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
CPR	Pressure sensor/ transmitter	Cyclic and monthly testing failures and demands	B	1 to 2	4269 d	—	Pool BCW data
			BCW	14 to 36	23157 d	0.12 (all f.)	
			BC	9 to 21	15457 d	0.05 (all f.)	
			BW	6 to 17	11969 d	0.04 (all f.)	
		Occurrences in time	B	1 to 3	335.3 y	—	Pool B and C data
			BCW	37 to 96	4,327.3 y	<=1.E-5	
			BC	12 to 18	2,696.2 y	>=0.72	
			BW	26 to 81	1,966.4 y	0.002 (all f.)	
CTP	Temperature sensor/ transmitter	Cyclic and monthly testing failures and demands	B	0 to 3	17,070 d	—	Use B data alone (lower failure probability than other vendors)
			BCW	34 to 63	48,647 d	<=1.E-5	
			BC	9 to 24	29,600 d	<=1.E-5	
			BW	25 to 42	36,117 d	<=1.E-5	
		Occurrences in time	B	5 to 8	1,341.2 y	—	No need to pool. Use B data alone.
CBI	Bistable	Monthly testing failures and demands	B	8 to 12	36,214 d	—	No need to pool. Use B data alone.
RYL	Logic relay	Monthly testing failures and demands	B	1	58,343 d	—	Pool B and W data
			BCW	45 to 58	849,025 d	<1.E-5 (all f.)	
			BC	3 to 9	74,503 d	<=0.01	
			BW	43 to 50	832,865 d	>=0.085	
SCR	Silicon-controlled rectifier	Monthly testing failures and demands	B	0	217,280 d	—	Used just in B RPS. Not applicable for other vendors.
MSW	Manual scram switch	Automatic trips and monthly testing failures and demands	B	0	2,112 d	—	Pool data from all three PWR vendors
			BCW	2	19,790 d	0.23	
			BC	1	5,538 d	1.0 [d]	
			BW	1	16,364 d	1.0 [d]	

Table C-1. Vendor differences applicable to B&W 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
BME	Breaker mechanical	Trips and monthly testing failures and demands	B	0	41,800 d	—	Pool B and C data
			BCW	4 to 6	113,585 d	0.006 (all f)	
			BC	1	83,813 d	1.0	
			BW	3 to 5	71,572 d	0.01 (all f)	
BSN	Breaker shunt device	Monthly testing failures and demands	B	3	5,786 d	—	Use B data alone (no need to pool data)
BUV	Breaker undervoltage coil	Monthly testing failures and demands	B	6 to 9	34,708 d	—	Use B data alone (no need to pool data)
RMA	Control rod drive and rods	Trips and cyclic testing failures and demands	B	0	19,086 d	—	Pool B, C, and W data.
			BCW	1 to 5	189,536 d	>0.10	
			BC	1 to 3	77,092 d	>0.58	
			BW	0 to 2	131,530 d	1.0	

Notes:

a. B, Babcock and Wilcox; C, Combustion Engineering, and 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.

breaker failures but not for the associated shut or UV trips. In this case, the greater number of failures for the trip devices makes pooling for their data unnecessary.

Table C-2 provides a breakdown of 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 B&W and CE 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 was used for the analysis. The analysis also considered whether the test data and data from unplanned trips 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 provide information on how the subsets were selected using these two sets of data. Figure C-1 is an overview of 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 column 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 provided 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 in every case are subdivided according to the method of discovery, if applicable. In the table, finding empirical Bayes distributions 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 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 0.008 p-value for logic relay differences in

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 B&W 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)	PWR cyclic and monthly tests	14	12	3	7	36	24.2
	—(op)	1	6	0	3	10	2.3
	—(s/d)	13	6	3	4	26	20.5
	(1984-1989)	6	9	2	4	21	13.2
	—(1984-1989 op)	1	4	0	3	8	2.8
	—(1984-1989 s/d)	5	5	2	1	13	9.9
	(1990-1995)	8	3	1	3	15	10.8
	—(1990-1995 op)	0	2	0	0	2	0.2
	—(1990-1995 s/d)	8	1	1	3	13	10.3
	BC occurrences in time	12	3	1	2	18	13.9
	—(op)	6	3	0	2	11	6.9
	—(s/d)	6	0	1	0	7	6.5
	(1984-1989)	8	2	1	2	13	9.6
	—(1984-1989 op)	4	2	0	2	8	4.7
	—(1984-1989 s/d)	4	0	1	0	5	4.5
	(1990-1995)	4	1	0	0	5	4.4
	—(1990-1995 op)	2	1	0	0	3	2.3
	—(1990-1995 s/d)	2	0	0	0	2	2.0
Temperature sensor/transmitter (CTP)	B cyc. and monthly tests (all during op. in the 1984-1989 period)	0	3	0	0	3	1.5

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 B&W 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		
Temperature sensor/transmitter (CTP) (continued)	B occurrences in time	5	0	3	0	8	6.5
	—(op)	3	0	2	0	5	4.0
	—(s/d)	2	0	1	0	3	2.5
	(1984-1989)	4	0	3	0	7	5.5
	—(1984-1989 op)	2	0	2	0	4	3.0
	—(1984-1989 s/d)	2	0	1	0	3	2.5
	(1990-1995) (all are op.)	1	0	0	0	1	1.0
Bistable (CBI)	B mon. tests	8	4	0	0	12	11.4
	—(op)	4	3	0	0	7	6.3
	—(s/d)	4	1	0	0	5	4.9
	(1984-1989)	2	4	0	0	6	4.5
	—(1984-1989 op)	0	3	0	0	3	0.8
	—(1984-1989 s/d)	2	1	0	0	3	2.8
	(1990-1995)	6	0	0	0	6	6.0
	—(1990-1995 op)	4	0	0	0	4	4.0
	—(1990-1995 s/d)	2	0	0	0	2	2.0

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 B&W 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		
Trains (trip logic)							
Logic relay (RYL)	BW mon. tests	43	5	2	0	50	45.0
	—(op)	29	1	2	0	32	30.2
	—(s/d)	14	4	0	0	18	14.7
	(1984-1989)	28	2	2	0	32	29.4
	—(1984-1989 op)	22	0	2	0	24	23.0
	—(1984-1989 s/d)	6	2	0	0	8	6.3
	(1990-1995)	15	3	0	0	18	15.7
	—(1990-1995 op)	7	1	0	0	8	7.2
	—(1990-1995 s/d)	8	2	0	0	10	8.5
	—BW trips (op) (not used)[c]	1	0	0	0	1	1.0
Silicon-controlled rectifier (SCR)	B mon. tests (no failures). SCR used only in the B&W RPS evaluation	0	0	0	0	0	0.0
Manual scram switch (MSW)	PWR mon. tests	2	0	0	0	2	2.0
	(1990-1995) (all in this period)	2	0	0	0	2	2.0
	—(1990-1995 op)	1	0	0	0	1	1.0
	—(1990-1995 s/d)	1	0	0	0	1	1.0
	—PWR unplanned manual trips	0	0	0	0	0	0.0

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 B&W 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		
Reactor trip breakers							
Breaker mechanical (BME)	Unplanned reactor trips	0	0	0	0	0	0.0
	BC mon. tests (1990 – 1995 op)	1	0	0	0	1	1.0
Breaker shunt device (BSN)	B mon. tests	3	0	0	0	3	3.0
	—(op)	2	0	0	0	2	2.0
	—(s/d)	1	0	0	0	1	1.0
	(1984-1989)	2	0	0	0	2	2.0
	—(1984-1989 op)	2	0	0	0	2	2.0
	(1990-1995)	1	0	0	0	1	1.0
	—(1990-1995 s/d)	1	0	0	0	1	1.0
Breaker undervoltage coil (BUV)	B mon. tests	6	0	3	0	9	7.5
	—(op)	4	0	3	0	7	5.5
	—(s/d)	2	0	0	0	2	2.0
	(1984-1989)	3	0	3	0	6	4.5
	—(1984-1989 op)	2	0	3	0	5	3.5
	—(1984-1989 s/d)	2	0	0	0	2	2.0
	(1990-1995) (all op)	2	0	0	0	2	2.0
Control rod drive and rod							
Control rod drive & rods (RMA)	Unplanned reactor trips (both in 1990-1998 period)[d]	0	0	2	0	2	1.0

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 B&W 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		
	PWR cyc. tests (all in 1984-1989 period, classified as s/d)	1	0	2	0	3	2.0

a. NSSS vendor abbreviations: B, B&W (only); BC, B&W and CE pooled; BW, B&W 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 B&W components. Other vendors have different testing schedules for some of the components.

b. Suppose there are NFS = 14 complete failures for a component (CPR, for example) with the safety function lost, and FS = 13 complete faults that are 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) = 0.52. A similar ratio, (pucNFS), is estimated using the faults with unknown completeness and either known or unknown safety impact. For example for CPR with 3 safety function lost events with unknown completeness, and 1 fail safe reported event with unknown completeness, (pucNFS) is (3+0.5)/(3+1+1) =0.70. 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" (14 complete and with known safety impact) plus pcNFS times the number (12) of complete failures that might have had a safety impact, plus 0.5 times the number (3) 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 24.2 = 14 + 12 * 0.52 + 3 * 0.5 + 7 * 0.70 *0.5.

c. Not used in the RPS fault tree unavailability analysis.

d. The 1996-1998 period only considers B&W and CE 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 SCR, 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).

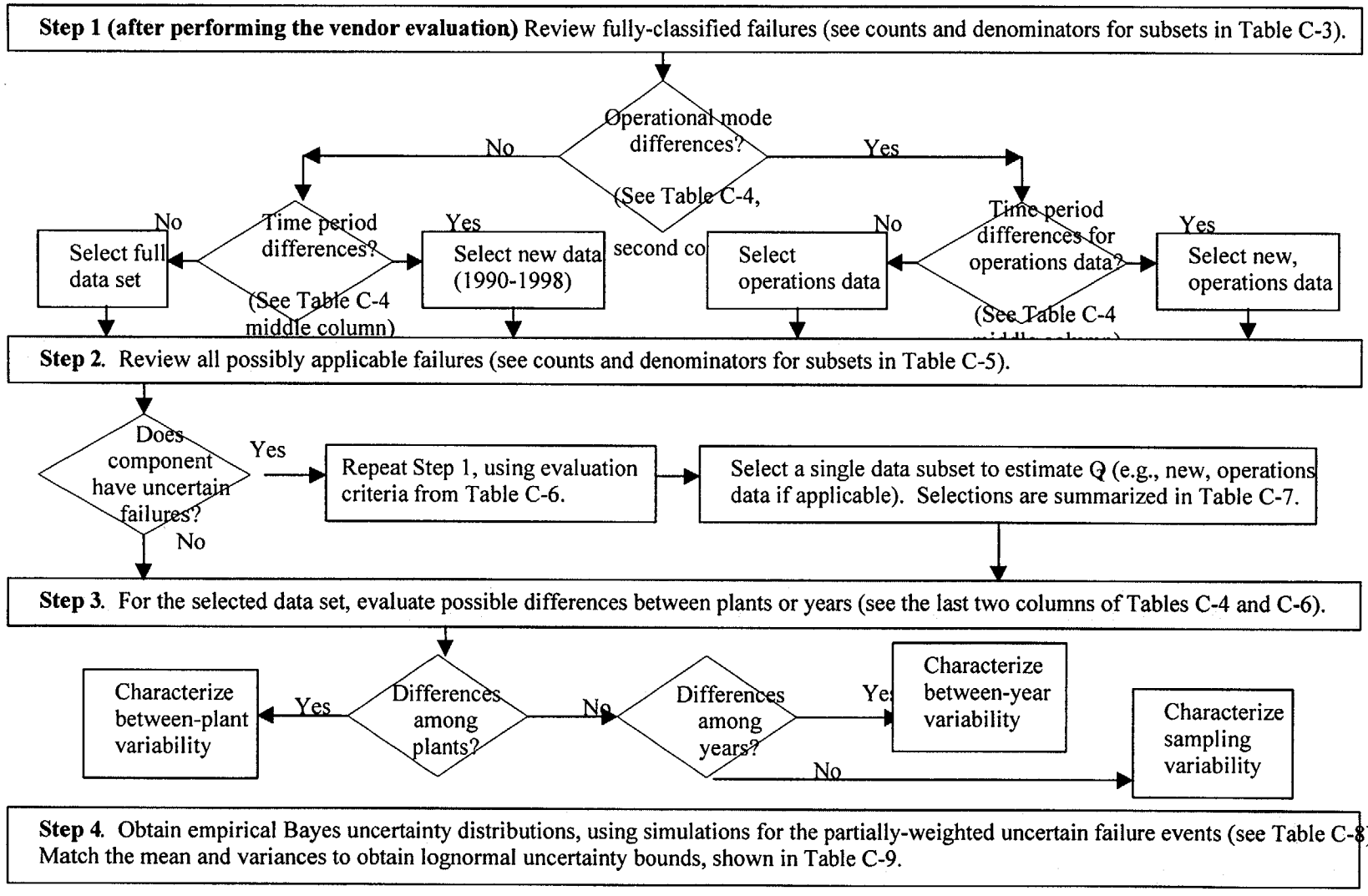


Figure C-1 . Decision algorithm for uncertainty distribution selection (applied for each component).

Table C-3. Point estimates and confidence bounds for component groups used in the assessment of B&W 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)	PWR cyclic and monthly tests	14	23157	(3.7E-04, 6.0E-04, 9.4E-04)
	PWR cyclic & monthly tests (op)	**1**	**17536**	**(2.9E-06, 5.7E-05, 2.7E-04)**
	PWR cyclic and monthly tests (s/d)	13	5621	(1.4E-03, 2.3E-03, 3.7E-03)
	BC occurrences in time	**12**	**2696.2** [c]	**(2.6E-03, 4.5E-03, 7.2E-03)**
	BC occurrences in time (op)	6	2008.0 [c]	(1.3E-03, 3.0E-03, 5.9E-03)
	BC occurrences in time (s/d)	6	688.2 [c]	(3.8E-03, 8.7E-03, 1.7E-02)
Temperature sensor/transmitter (CTP)	**B cyclic and monthly tests**	**0**	**17070**	**(0.0E+00, 0.0E+00, 1.8E-04)**
	B occurrences in time	**5**	**1341.2** [c]	**(1.5E-03, 3.7E-03, 7.8E-03)**
Bistable (CBI)	B monthly tests	8	36214	(1.1E-04, 2.2E-04, 4.0E-04)
	B monthly tests (op)	4	28912	(4.7E-05, 1.4E-04, 3.2E-04)
	B mon. tests, 1984-1989 (op)	0	13341	(0.0E+00, 0.0E+00, 2.2E-04)
	B mon. tests, 1990-1995 (op)	**4**	**15571**	**(8.8E-05, 2.6E-04, 5.9E-04)**
	B monthly tests (s/d)	4	7302	(1.9E-04, 5.5E-04, 1.3E-03)
Trains (trip logic)				
Logic relay (RYL)	BW monthly tests	43	832865	(3.9E-05, 5.2E-05, 6.7E-05)
	BW monthly tests, 1984-1989	28	368937	(5.4E-05, 7.6E-05, 1.0E-04)
	BW monthly tests, 1990-1995	**15**	**463928**	**(2.0E-05, 3.2E-05, 5.0E-05)**
Silicon-controlled rectifier (SCR)	**B monthly tests**	**0**	**217280**	**(0.0E+00, 0.0E+00, 1.4E-05)**
Manual scram switch (MSW)	PWR unplanned trips	0	2222	(0.0E+00, 0.0E+00, 1.3E-03)
	PWR monthly 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 mechanical (BME)	BC unplanned trips	0	5416	(0.0E+00, 0.0E+00, 5.5E-04)
	BC monthly 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)	**B monthly tests**	**3**	**5786**	**(1.4E-04, 5.2E-04, 1.3E-03)**
Breaker UV coil (BUV)	**B monthly tests**	**6**	**34708**	**(7.5E-05, 1.7E-04, 3.4E-04)**

Table C-3. Point estimates and confidence bounds for component groups used in the assessment of B&W 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
Control rod drive and rod				
Control rod drive & rods (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.

monthly tests by time periods shows that, when the more recent failures and demands are pooled and compared with the corresponding total failures and demands during the 1980 period, the likelihood of the observed difference or a more extreme difference if the groups did have the same failure probability is 0.8 percent. Either a "rare" (probability 0.008) situation occurred, or the two pooled sets of failures and demands have different failure probabilities. 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.

In each of the first three 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 first column, where applicable, the testing versus reactor trip data were compared. This evaluation is for information only; both sets of data were pooled for the unavailability analysis.

The second and third evaluations in Table C-4 also reflect the comparison of pairs of attributes. "Step 1" in Figure C-1 shows how the plant operating mode and time period 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 several of the components. In the overall analysis described below, subsets were used if either of the bounding analyses showed a need for them. This point is explained in the last Step 2 box in Figure C-1. In both Tables C-3 and C-5, lines are

Table C-4. Evaluation of differences between groups for B&W 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)	PWR cyclic and monthly tests	—	**<5.0E-4 (E)**	1.000	**0.005 (E)**	0.146 (E)
	PWR cyclic & monthly tests (op)	—	—	0.435	1.000	0.167
	PWR cyclic & monthly tests (s/d)	—	—	0.409	**<5.0E-4 (E)**	**0.022 (E)**
	BC occurrences in time	—	0.052 (E)	0.163	0.199 (E)	0.377
	BC occurrences in time (op)	—	—	0.277	0.311 (E)	0.458
	BC occurrences in time (s/d)	—	—	0.486	0.715 (E)	**0.018 (E)**
Temperature sensor/transmitter (CTP)	B cyclic and monthly tests	—	0 F	0 F	0 F	0 F
	B occurrences in time	—	0.269	0.178	0.158 (E)	0.266
Bistable (CBI)	B monthly tests	—	0.058 (E)	0.289	0.126 (E)	0.131 (E)
	B monthly tests (op)	—	—	0.129 (E)	0.359	0.289 (E)
	B mon. tests, 1984-1989 (op)	—	—	—	0 F	0 F
	B mon. tests, 1990-1995 (op)	—	—	—	0.388	0.393
	B monthly tests (s/d)	—	—	0.617	0.510	0.677
Trains (trip logic)						
Logic relay (RYL)	BW monthly tests	—	0.211	**0.008 (E)**	**<5.0E-4 (E)**	**<5.0E-4 (E)**
	BW monthly tests, 1984-1989	—		—	**<5.0E-4 (E)**	**0.016 (E)**
	BW monthly tests, 1990-1995	—		—	**0.005 (E)**	0.099 (E)
Silicon-controlled rectifier (SCR)	B monthly tests	—	0 F	0 F	0 F	0 F
Manual scram switch (MSW)	PWR unplanned trips	—	0 F	0 F	0 F	0 F
	PWR monthly 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	1.000	1.000	0.495	**<5.0E-4[d]**	0.673
Breaker shunt device (BSN)	B monthly tests	—	0.490	1.000	0.770	0.569
Breaker undervoltage coil (BUV)	B monthly tests	—	0.347	0.688	0.246	0.880

Table C-4. Evaluation of differences between groups for B&W 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
Control rod drive and rod						
Control rod drive and rods (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: B, B&W (only); BC, B&W and CE pooled; BW, B&W and W pooled; and PWR, B&W, CE, and W all pooled.

c. —, not applicable; 0 F, no failures (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.

highlighted corresponding to the subsets selected. Table C-7 provides a concise summary of 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 just discussed, the rod and control rod drive component shows 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.

Table C-5. Point estimates and confidence bounds for component groups used in the assessment of B&W 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)	PWR cyclic and monthly tests	36	23157	(1.2E-03, 1.6E-03, 2.1E-03)
	PWR cyclic and monthly tests (op) [b]	**10**	**17536**	**(3.1E-04, 5.7E-04, 9.7E-04)**
	PWR cyc. and mon. tests, 1984-1985 (op)	8	7632	(5.2E-04, 1.0E-03, 1.9E-03)
	PWR cyc. and mon. tests, 1990-1995 (op)	2	9904	(3.6E-05, 2.0E-04, 6.4E-04)
	PWR cyclic tests (s/d)	26	5621	(3.2E-03, 4.6E-03, 6.4E-03)
	BC occurrences in time	**18**	**2696.2** [c]	**(4.3E-03, 6.7E-03, 9.9E-03)**
	BC occurrences in time, 1984-1989	13	1256.2 [c]	(6.1E-03, 1.0E-02, 1.6E-02)
	BC occurrences in time, 1990-1995	5	1440.0 [c]	(1.4E-03, 3.5E-03, 7.3E-03)
Temperature sensor/transmitter (CTP)	**B cyclic tests**	**3**	**17070**	**(4.8E-05, 1.8E-04, 4.5E-04)**
	B cyclic tests, 1984-1989	3	8462	(9.7E-05, 3.5E-04, 9.2E-04)
	B cyclic tests, 1990-1995	0	8608	(0.0E+00, 0.0E+00, 3.5E-04)
	B occurrences in time	8	1341.2 [c]	(3.0E-03, 6.0E-03, 1.1E-02)
	B occurrences in time, 1984-1989	7	669.2 [c]	(4.9E-03, 1.0E-02, 2.0E-02)
	B occurrences in time, 1990-1995	**1**	**672.0** [c]	**(7.6E-05, 1.5E-03, 7.0E-03)**
Bistable (CBI)	**B monthly tests**	**12**	**36214**	**(1.9E-04, 3.3E-04, 5.4E-04)**
Trains (trip logic)				
Logic relay (RYL)	BW monthly tests	50	832865	(4.7E-05, 6.0E-05, 7.6E-05)
	BW monthly tests (op)	32	632310	(3.7E-05, 5.1E-05, 6.8E-05)
	BW mon. tests, 1984-1989 (op)	24	269890	(6.1E-05, 8.9E-05, 1.3E-04)
	BW mon. tests, 1990-1995 (op)	**8**	**362420**	**(1.1E-05, 2.2E-05, 4.0E-05)**
	BW monthly tests (s/d)	18	200555	(5.8E-05, 9.0E-05, 1.3E-04)
Reactor trip breakers				
Breaker undervoltage coil (BUV)	**B monthly tests**	**9**	**34708**	**(1.4E-04, 2.6E-04, 4.5E-04)**
Control rod drive and rod				
Control rod drive and rods (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, 1990-1995	0	14019	(0.0E+00, 0.0E+00, 2.1E-04)

Table C-5. Point estimates and confidence bounds for component groups used in the assessment of B&W 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
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, 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. Note also that manual switches, silicon-controlled rectifiers, breaker mechanical, and breaker shunt trip devices 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-3).

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.

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-6. Evaluation of differences between groups for B&W 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)	PWR cyclic and monthly tests	—	**<5.0E-4 (E)**	0.134	**0.001 (E)**	0.049 (E)
	PWR cyclic and monthly tests (op)	—	—	**0.025 (E)**	**0.001 (E)**	0.163 (E)
	PWR cyc.and mon. tests, 1984-1989 (op)	—	—	—	**0.001 (E)**	0.451
	PWR cyc.and mon. tests, 1990-1995 (op)	—	—	—	**0.001**	0.573
	PWR cyclic tests (s/d)	—	—	0.847	**0.001 (E)**	0.179 (E)
	BC occurrences in time	—	0.193	**0.029 (E)**	**0.004 (E)**	0.215 (E)
	BC occurrences in time, 1984-1989	—		—	0.287 (E)	0.411
	BC occurrences in time, 1990-1995	—		—	**0.010 (E)**	0.639
Temperature sensor/transmitter (CTP)	B cyclic and monthly tests	—	1.000	0.122 (E)	**0.003 (E)**	0.677
	B cyclic & monthly tests, 1984-1989	—		—	**0.001 (E)**	0.754
	B cyclic & monthly tests, 1990-1995	—	0 F	—	0 F	0 F
	B occurrences in time	—	0.222	**0.033 (E)**	0.346	0.442
	B occurrences in time, 1984-1989	—		—	0.309	0.701
	B occurrences in time, 1990-1995	—		—	0.423	0.416
Bistable (CBI)	B monthly tests	—	0.075	1.000	0.178 (E)	0.093 (E)
Trains (trip logic)						
Logic relay (RYL)	BW monthly tests	—	0.067 (E)	**0.006 (E)**	**<5.0E-4 (E)**	**0.001 (E)**
	BW monthly tests (op)	—	—	**<5.0E-4 (E)**	**<5.0E-4 (E)**	**<5.0E-4(E)**
	BW mon. tests, 1984-1989 (op)	—	—	—	**<5.0E-4 (E)**	**0.002 (E)**
	BW mon. tests, 1990-1995 (op)	—	—	—	**0.027 (E)**	0.770
	BW monthly tests (s/d)	—	—	0.815	**0.010 (E)**	**0.030 (E)**
Reactor trip breakers						
Breaker undervoltage coil (BUV)	B monthly tests	—	1.000	0.180	0.622	0.237 (E)
Control rod drive and rod						
Control rod drive	PWR unplanned trips	—	—	0.077	0.666	0.209

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

Failure mode (component) and rods (RMA)	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
	PWR cyclic tests	—	**0.015 (E)** [d]	0.125 (E)	**<5.0E-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	—		—	**<5.0E-4 (E)**	0.262
	PWR cyclic tests, 1990-1995	—	0 F	—	0 F	0 F
	PWR pooled trips & tests	**0.026** [d]	**<5.0E-4 (E)**[d]	0.648	**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, breaker mechanical, and breaker shunt trip devices 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: B, B&W (only); BC, B&W and CE pooled; BW, B&W and W pooled; and PWR, B&W, CE, and W all pooled.

c. —, not applicable; 0 F, no failures (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 & 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.

Table C-7. Point estimates of failure probabilities and rates for B&W 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)	PWR cyc. & mon. tests (op)	1	10	0.150	0.250	2.3	17536.	1.3E-04	1.6E-04
	BC occurrences in time	12	18	0.379	0.300	13.9	23618887.	5.9E-07	6.1E-07
Temperature sensor/transmitter (CTP	B cyc. & mon. tests	0	3	0.500	—	1.5	17070.	8.8E-05	1.2E-04
	B occurrences in time, 1990-1995	1	1	—	—	1.0	5886720.	1.7E-07	2.5E-07
Bistable (CBI)	B mon. tests, 1990-1995 (op)	4	4	—	—	4.0	15571.	2.6E-04	2.9E-04
Trains (trip logic)									
Logic relay (RYL)	BW mon. tests, 1990-1995 (op)	7	8	0.234	—	7.2	362420.	2.0E-05	2.1E-05
Silicon-controlled rectifier (SCR)	B mon. tests	0	0	—	—	0.0	217280.	0.0E+00	2.3E-06
Manual scram switch (MSW)	PWR unpl. trips & mon. tests	2	2	—	—	2.0	19789.	1.0E-04	1.3E-04
Reactor trip breakers									
Breaker mechanical (BME)	BC unpl. trips & mon. tests	1	1	—	—	1.0	83813.	1.2E-05	1.8E-05
Breaker shunt device (BSN)	B mon. tests	3	3	—	—	3.0	5786.	5.2E-04	6.0E-04

Table C-7. Point estimates of failure probabilities and rates for B&W 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				
Breaker UV coil (BUV)	B mon. tests	6	9	—	—	7.5	34708.	2.2E-04	2.3E-04
Control rod drive and rod									
Control rod drive & rods (RMA)	PWR unplanned trips & cyc. tests	1	5	—	—	3.0	189536.	1.6E-05	1.8E-05

a. Vendor groups are given as follows: B, B&W (only); BC, B&W and CE pooled; BW, B&W and W pooled; and PWR, B&W, CE, 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 applied for uncertainty in completeness is 0.5.
c. (Failures + 0.5)/(Denominator+1) for probabilities; (Failures + 0.5)/Denominator for rates.

Table C-8 gives 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-3and 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.

Failure Mode (Component)	Failures[a]	Denominator[b]	Modeled variation[c]	Distribution[d]	Bayes mean and interval[e]
Channel components					
Pressure sensor/ transmitter (CPR)	2.3	17536	Between plant	Beta(0.1,691.5)	(1.00E-09,1.57E-04,9.04E-04)
	13.9	2696.2[f,g]	Between plant	Gamma(0.7,136.5)	(8.85E-05,5.12E-03,1.74E-02)
Temperature sensor/ transmitter (CTP)	1.5	17070	Between plant	Beta(0.2,2157.0)	(1.84E-09,1.15E-04,5.59E-04)
	1	672.0[f,g]	Sampling (only)[h]	Gamma(1.5,672.0)	(2.62E-04,2.23E-03,5.81E-03)
Bistable (CBI)	4	15571	Sampling (only)[h]	Beta(4.5,15568)	(1.07E-04,2.89E-04,5.43E-04)
Trains (trip logic)					
Logic relay (RYL)	7.2	362420	Between plant	Beta(2.5,116750)	(4.74E-06,2.11E-05,4.69E-05)
Silicon-controlled rectifier (SCR)	0	217280	Sampling (only)[h]	Beta(0.5,217281)	(9.05E-09,2.30E-06,8.84E-06)
Manual scram switch (MSW)	2	19789	Sampling (only)[h]	Beta(2.5,19788)	(2.89E-05,1.26E-04,2.80E-04)
Reactor trip breakers					
Breaker mechanical (BME)	1	83813	Sampling (only)[h]	Beta(1.5,83813)	(2.10E-06,1.79E-05,4.66E-05)
Breaker shunt device (BSN)	3	5786	Sampling (only)[h]	Beta(3.5,5783.5)	(1.87E-04,6.05E-04,1.22E-03)
Breaker undervoltage coil (BUV)	7.5	34708	Between Year	Beta(6.1,26532)	(1.00E-04,2.29E-04,4.00E-04)
Control rod drive and rod					
Control rod drive and rods (RMA)	2.9	189536	Between plant	Beta(0.1,5223.8)	(1.39E-19,1.67E-05,9.73E-05)

a. Number of failures, averaged over 1000 simulation iterations, each of which had an integral number of failures.
b. Estimated number of demands or exposure time, based on the selected data sets or subsets shown in Table C-7.
c. In addition to variation from unknown completeness and/or from unknown loss of safety function.
d. 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.
e. 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, 20% of the time; CTP probability, 11%; and RMA, 50% of the time. Sampling variation (from the simple Bayes method) entered the simulation mixture when EB distributions were not found.
f. Component years rather than demands. Also, the rates in the Bayes mean column are per year.
g. Rate not used in fault tree assessment, because the unavailability associated with the failure rate was much lower than the unavailability estimated from the testing data.
h. Simple Bayes distribution not based on the simulations. No uncertain events were in the selected subsets.

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

Failure Mode (Component)	Median	Error factor [a]	Lognormal distribution mean and interval [b]
Channel components			
Pressure sensor/transmitter	4.9E-05	12.3	(4.0E-06, 1.6E-04, 6.0E-04)
Temperature sensor/transmitter	5.1E-05	8.1	(6.3E-06, 1.2E-04, 4.1E-04)
Bistable	2.6E-04	2.1	(1.3E-04, 2.9E-04, 5.5E-04)
Trains (trip logic)			
Logic relay	1.8E-05	2.6	(6.8E-06, 2.1E-05, 4.6E-05)
Silicon-controlled rectifier	1.3E-06	5.6	(2.4E-07, 2.3E-06, 7.4E-06)
Manual scram switch	1.1E-04	2.6	(4.1E-05, 1.3E-04, 2.8E-04)
Reactor trip breakers			
Breaker mechanical	1.4E-05	3.2	(4.3E-06, 1.8E-05, 4.5E-05)
Breaker shunt device	5.3E-04	2.3	(2.3E-04, 6.1E-04, 1.2E-03)
Breaker undervoltage coil	2.1E-04	1.9	(1.1E-04, 2.3E-04, 4.0E-04)
Control rod drive and rod			
Control rod drive and rods	4.7E-06	13.6	(3.5E-07, 1.7E-05, 6.4E-05)

a. Lognormal error factor corresponding to 5% and 95% bounds.

b. Mean and lognormal distribution 5th and 95th percentiles. Obtained by matching the mean and variance of the distributions from Table C-8 that are used in the unreliability analysis.