INEEL/EXT-95-00133

May 1998

High-Pressure Core Spray System Reliability, 1987–1993

J. P. Poloski
G. M. Grant
C. D. Gentillon
W. J. Galyean

INEEL/EXT-95-00133

High-Pressure Core Spray System Reliability, 1987–1993

J. P. Poloski
G. M. Grant
C. D. Gentillon
W. J. Galyean

Published May 1998

Idaho National Engineering and Environmental Laboratory
Nuclear Risk Management Technologies Department
Lockheed Martin Idaho Technologies Company
Idaho Falls, Idaho 83415

Prepared for the
Reliability and Risk Assessment Branch
Safety Programs Division
Office for Analysis and Evaluation of Operational Data
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Under DOE Idaho Operations Office
Contract DE-AC07-94ID13223
Job Code E8246

ABSTRACT

This report documents an analysis of the performance of the high-pressure core spray (HPCS) system at U.S. commercial boiling water reactor plants during the period 1987–1993. Both a reliability analysis and an engineering analysis of trends and patterns were performed on data from HPCS system operational events to obtain insights into the performance of the HPCS system throughout the industry and at a plant-specific level. Comparisons were made to probabilistic risk assessments and individual plant examinations for the eight plants to indicate where operational data either support or fail to support the assumptions, models, and data used to develop the HPCS system unreliability estimates.

Job Code E8246—Technical Assistance in Reliability and Risk Analysis

EXECUTIVE SUMMARY

This report presents a performance evaluation of the high-pressure core spray (HPCS) system at eight U.S. commercial boiling water reactors (BWRs) that have this system. The evaluation is based on the operating experience from 1987 through 1993, as reported in licensee event reports (LERs). The objectives of the study were (a) to estimate the system unreliability based on 1987–1993 experience and to compare these estimates with the assumptions, models, and data used in Probabilistic Risk Assessments and Individual Plant Examinations (PRA/IPEs) and (b) to review the operational data from an engineering perspective to determine trends and patterns in the data and obtain insights into the failures and failure mechanisms associated with the HPCS system.

The study used LERs identified using the Sequence Coding and Search System (SCSS). The SCSS database was only used to identify LERs for review and classification for the study. The reportability requirements of 10 CFR 50.73 (LER rule) were not used to define or classify any events used in the study. The full text of each LER was independently reviewed by a team of experienced U.S. commercial nuclear power plant engineers from a risk and reliability perspective. Each event was either excluded from the study or classified and subsequently used in the study based on this independent review of the full text of the LER.

The HPCS system unreliabilities were estimated using a fault tree model to associate event occurrences with broadly defined failure modes such as failure to start or failure to run. The probabilities for the individual failure modes were calculated by reviewing the failure information, categorizing each event by failure mode, and then estimating the corresponding number of demands (both successes and failures). Seven plant risk reports (i.e., PRAs, IPEs, and NUREGs) were used for comparison with the HPCS reliability results calculated in this study. The information extracted from the source documents contain data for the eight plants that have an HPCS system.

Since there are only eight U.S. BWR plants that have an HPCS system, the operating experience data, including demand counts, failure counts, and run times, for estimating HPCS system unreliability are limited. However, there is sufficient data to reasonably estimate the reliability of the system and its associated uncertainties, but information regarding dominant contributors and trends are less robust and could change as additional experience is obtained.

The notable observations and findings made from the limited data are as follows:

- The mean HPCS system operational unreliability (including recovery) estimate calculated from the 1987–1993 experience is 0.075. None of the actual HPCS demands to operate involved a loss of offsite power requiring the Division III emergency diesel-generator to energize the bus, nor did any last long enough to require pump suction transfer to the suppression pool. Only one demand failure was observed during 29 operational demands and accounted for 67 percent of the total system unreliability. This

failure occurred in the injection subsystem as a result of the system being in a maintenance-out-of-service condition when the system was demanded. The only other failure used in the operational unreliability estimate occurred during quarterly testing and had less impact on the estimate, accounting for only 7 percent of the total system unreliability.

- HPCS unreliability estimated from the 1987–1993 experience for comparison with PRA/IPE results and the HPCS unreliability calculated from the PRA/IPE data are plotted in Figure ES-1. For missions typical of those considered in PRAs and IPEs, the operational-data based unreliability is 0.23. This is higher than the equivalent unreliability estimated using the PRA/IPE data. The unreliability of the injection subsystem estimated from the operational experience is a factor of five higher than that estimated using the PRA/IPE data. The difference in the estimates is primarily attributed to a factor of 50 difference in the average hourly failure rates used in calculating the HPCS injection pump failure to run (FTR) probability.

  The PRA/IPE data appear to use generic FTR data for all pumps rather than plant-specific (or system-specific) data. The operating experience data for the HPCS showed no failures in a total of 316 hours of run time, primarily consisting of runs of one hour or less. The operational experience failure rate was estimated from this limited data and was assumed to remain constant for a typical PRA/IPE mission requirement of 24 hours. Thus, the operating experience estimate for FTR may be pessimistic. Additional data is necessary to ascertain whether the differences between the reliability estimates based on the operating experience data and the PRA/IPE data are real or an artifact of the limited available data.

- There was only one failure in 29 unplanned demands and one failure in a total of 299 test demands that were used in the estimation of the system operational reliability over the seven year period of this study. From this limited data, no trends over time for the reliability would be expected to be observed. None were observed in the statistical analyses of the unreliability versus calendar year, and none in the unreliability versus plant age (see Figures ES-2 and ES-3).

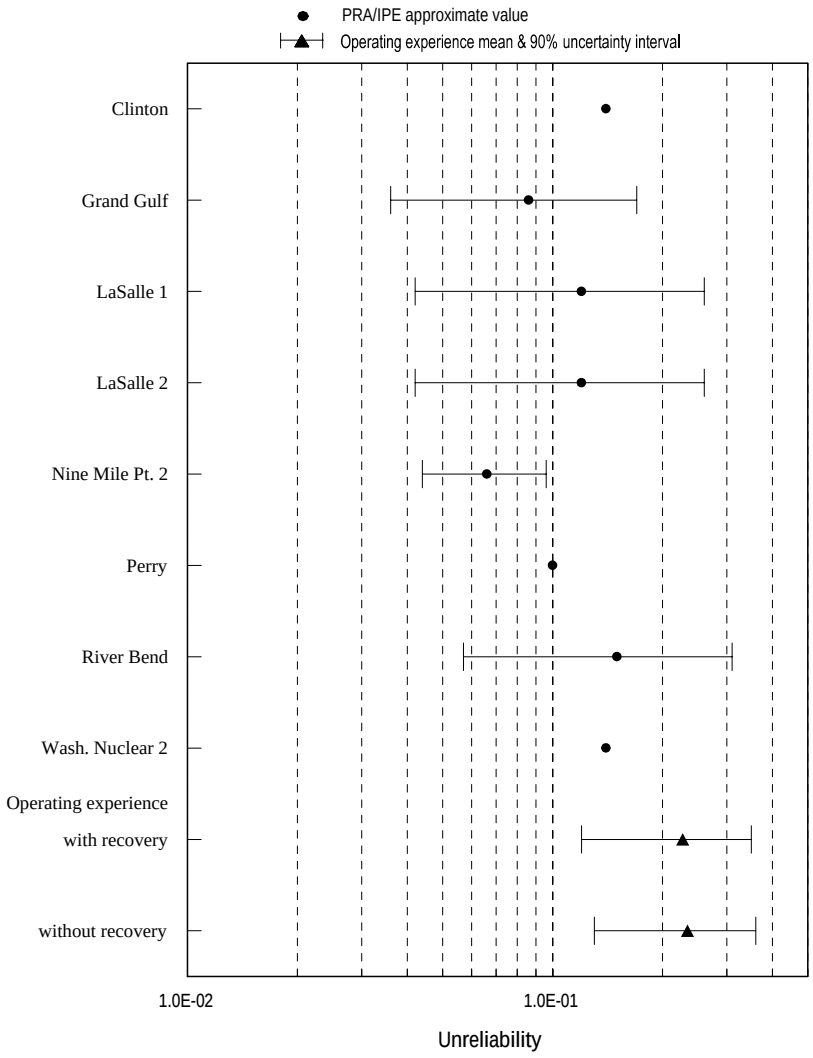


Figure ES-1. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience applies to all plants.)

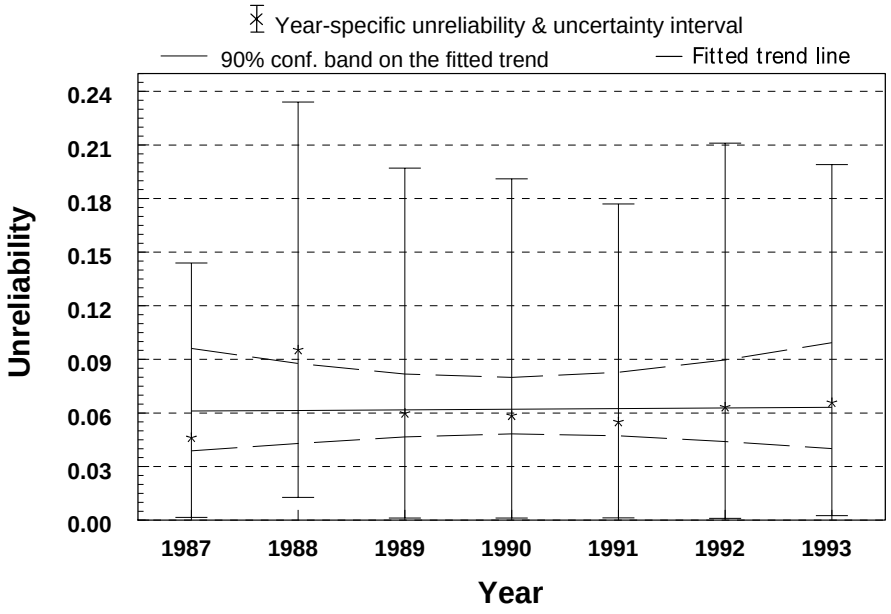


Figure ES-2. HPCS system unreliability by calendar year, which includes recovery actions. The plotted trend is not statistically significant (P-value = 0.91).

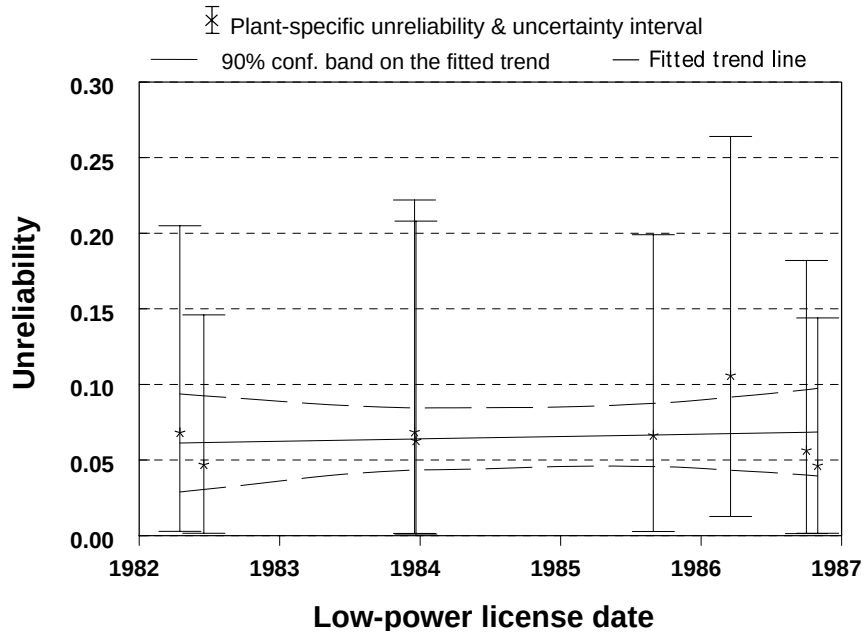


Figure ES-3. Plant-specific HPCS system operational unreliability plotted by low-power license dates. The plotted trend is not statistically significant (P-value = 0.71).

ACKNOWLEDGMENTS

This report benefited from the questions and comments of P. W. Baranowsky, S. E. Mays, and T. R. Wolf of the Nuclear Regulatory Commission.

Technical reviews by J. H. Bryce, T. J. Leahy, and C. L. Atwood of the INEEL; D. C. Bley of Buttonwood Consulting; G. W. Parry of the NUS Corp.; A. M. Kolaczkowski of SAIC; and F. H. Rowsome of FHR Associates contributed substantially to the final report.

Technical contributions by A. J. Luptak, W. S. Roesener, and D. A. Prawdzik of the INEEL contributed to the final report.

CONTENTS

ABSTRACT iii

EXECUTIVE SUMMARY v

ACKNOWLEDGMENTS ix

ACRONYMS xv

TERMINOLOGY xvii

1. INTRODUCTION 1

2. SCOPE OF STUDY 2

2.1 System Operation and Description 2

2.1.1 System Operation 2
2.1.2 System Description 3
2.1.3 System Boundaries 3

2.2 Operational Data Collection 5

2.2.1 Inoperability Characterization 5
2.2.2 Demand Collection and Characterization 7

2.3 Methodology for Operational Data Analysis 8

3. RISK-BASED ANALYSIS OF THE OPERATIONAL DATA 10

3.1 Estimates of HPCS Operational Unreliability 11

3.1.1 HPCS System Operational Unreliability 16
3.1.2 Investigation of Possible Trends 19

3.2 Comparison to PRAs 20

3.2.1 PRA Comparison Unreliability 23
3.2.2 Failure to Start 26
3.2.3 Failure to Run 29
3.2.4 Maintenance-Out-of-Service 31

4. ENGINEERING ANALYSIS OF THE OPERATIONAL DATA 34

4.1 Industry-wide Evaluation 35

4.1.1 Trends by Year 35
4.1.2 Factors Affecting HPCS Reliability 35

4.2 Plant-specific Evaluation 40

4.3 Evaluation of HPCS Failures Based on Low-power License Date 44

4.4 Accident Sequence Precursor Review 45

5. REFERENCES 47

Appendix A—HPCS Data Collection and Analysis Methods

Appendix B—HPCS Operational Data, 1987–1993

Appendix C—Basic Event Failure Probabilities and Unreliability Trends

Appendix D—Unreliability Model and Failure Probabilities Used for Comparison to PRAs

FIGURES

ES-1. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the1987–1993 experience applies to all plants.) vii

ES-2. HPCS system unreliability by calendar year, which includes recovery actions. The plotted trend is not statistically significant (P-value = 0.91) viii

ES-3. Plant-specific HPCS system operational unreliability plotted by low-power license dates. The plotted trend is not statistically significant (P-value = 0.71) viii

1. Simplified schematic of the HPCS system 4

2. Illustration of the relationship between the inoperability and failure data sets 9

3. System fault tree of HPCS for calculating operational unreliability 17

4. HPCS system operational unreliability plotted by calendar year. The plotted trend is not statistically significant (P-value = 0.91) 19

5. Plant-specific HPCS system operational unreliability plotted by low-power license dates. The plotted trend is not statistically significant (P-value = 0.71) 20

6. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience applies to all plants.) 23

7. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS injection subsystem unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987-1993 experience applies to all plants.)..... 25

8. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS emergency power (Division III) unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987-1993 experience applies to all plants.) 26

9. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS injection failure to start probability and uncertainties. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987-1993 experience applies to all plants.) 27

10. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS emergency power (Division III) failure to start probability and uncertainties. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience apply to all plants.) 28

11. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS injection subsystem failure to run probability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience apply to all plants.) 30

12. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS emergency power (Division III) diesel generator failure to run probability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience apply to all plants.) 31

13. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS injection and emergency power (Division III) diesel generator maintenance-out-of-service probability and uncertainties. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience applies to all plants.). 32

14. HPCS unplanned demand events per year, with 90% uncertainty intervals and confidence band on the fitted trend. Although a decreasing trend is visible, it is not statistically significant (P-value = 0.18) 36

15. HPCS failure events per year, with 90% uncertainty intervals and confidence band on the fitted trend. The trend is not statistically significant (P-value = 0.54) 36

16. Plant-specific unplanned demand frequencies with 90% uncertainty intervals 41

17. Plant-specific failure frequencies with 90% uncertainty intervals 42

18. Plant-specific unplanned demand frequency versus plant-specific failure frequency..... 43

19. Plant-specific HPCS system failures per operating year, plotted against low-power license date. Ninety-percent Bayesian intervals and a fitted trend are included. The trend is not statistically significant (P-value = 0.55)..... 45

TABLES

1. BWR plants with an HPCS system..... 2

2. Failure data sources and counts used for estimating HPCS injection failure mode probabilities..... 12

3. Failure data sources and counts used for estimating HPCS emergency power failure mode probabilities..... 14

4. HPCS system failure mode data and Bayesian probability information for estimating operational unreliability..... 18

5. Estimates of HPCS operational unreliability..... 18

6. PRA/IPE average subsystem failure probability contribution to HPCS system unreliability. Estimates were derived from the failure information obtained from the PRA/IPEs and assuming that the offsite power to the Division III bus is not available..... 24

7. Number of HPCS events by category for each year of the study 35

8. Subsystem contribution to HPCS system failures, by method of discovery 37

9. Component contribution to HPCS system failures, by method of discovery. 37

10. HPCS faults, failures, and demands differentiated by plant (excludes the MOOS events)..... 41

11. List of the ASP events that identified an HPCS unplanned demand..... 46

ACRONYMS

ADS	automatic depressurization system
AEOD	Analysis and Evaluation of Operational Data (NRC Office)
ASP	Accident Sequence Precursor (database)
BWR	boiling water reactor
CCDP	conditional core damage probability
CST	condensate storage tank
ECCS	emergency core cooling system
EDG	emergency diesel generator
ESF	engineered safety feature
FTR	failure to run
FTRD	failure to run of the emergency power subsystem
FTRI	failure to run of the injection subsystem
FTRT	failure to run of the suction path transfer capability
FTS	failure to start
FTSB	failure to start due to output breaker problems
FTSD	failure to start due to causes other than the output breaker for the emergency power subsystem
FTSI	failure to start due to causes other than injection valve for the injection subsystem
FTSV	failure to start because of injection valve problems
HPCS	high-pressure core spray
HVAC	heating, ventilating, and air conditioning
INEEL	Idaho National Engineering and Environmental Laboratory
IREP	Interim Reliability Evaluation Program
IPE	individual plant examination
LER	licensee event report

LOCA	loss-of-coolant accident
LPCS	low-pressure core spray
LPCI	low-pressure coolant injection
MOOS	maintenance-out-of-service
MOOSD	maintenance-out-of-service of the emergency power subsystem
MOOSI	maintenance-out-of-service of the injection subsystem
MOV	motor-operated valve
NPRDS	Nuclear Plant Reliability Data System
PRA	probabilistic risk assessment
RCIC	reactor core isolation cooling
RPV	reactor pressure vessel
SCSS	sequence coding and search system
SFL	safety function lost

TERMINOLOGY

Cyclic surveillance test—A test of the system typically performed once per operating cycle and required to be performed at least every 18 months.

Event frequency—The number of events of interest (failures, demands, etc.) divided by plant operating time.

Failure—An event in which the safety injection function is lost for the injection subsystem. For the emergency power subsystem, it is the loss of the ability to supply power to the Division III electrical bus.

Failure to run (FTR)—A failure of the HPCS injection subsystem after the subsystem starts injecting coolant to the reactor pressure vessel (RPV) or test return line, or a failure of the HPCS emergency power subsystem to continue to supply power to the Division III electrical bus.

Failure to start (FTS)—A failure of the HPCS injection subsystem prior to the subsystem reaching rated coolant flow or a failure of the HPCS emergency power subsystem up to and including the closing of the output breaker. The FTS for the HPCS injection subsystem is sometimes divided into failure to start because of injection valve problems (FTSV) and failure to start for other reasons (FTSI). For the HPCS emergency power subsystem, FTS is sometimes divided into a failure of the output breaker to shut (FTSB) and a failure to start for other reasons (FTSD).

Fault—The term *fault* is used in this study to refer to the subset of inoperabilities that were not classified as failures. Specifically, when considering all the data provided in the full text of the LER, the system is judged to have been able to complete a typical mission postulated in PRA/IPEs.

HPCS emergency power subsystem—The portion of the HPCS system consisting of the dedicated emergency diesel generator up to and including the output breaker to the dedicated Division III electrical bus.

HPCS injection subsystem—All the HPCS system except for the dedicated HPCS emergency power subsystem.

Inoperability—The term *inoperability* is used to describe any HPCS malfunction or situation, except an engineered safety feature actuation, in which a LER was submitted in accordance with the requirements identified in 10 CFR 50.73. Inoperabilities include both failures and faults.

Maintenance-out-of-service (MOOS)—A failure of the HPCS system caused by the HPCS system being out of service for maintenance when an unplanned demand of the system occurs.

P-value—The probability that the data set would be as extreme as it is, if the assumed model is correct. It is the significance level at which the assumed model would barely be rejected by a statistical test. A small P-value indicates strong evidence against the assumed model.

Recovery—The overcoming of a prior failure solely by operator actions without the need for any maintenance action or repair.

Reliability—Probability that the system/train/component/etc. will successfully complete its required mission (however that mission might be defined).

Safety function lost (SFL)—Same as failure.

Sequential loss of offsite power—A complete loss of offsite power that occurs over a period of time. An example would be a partial loss of offsite power (loss of one incoming line) followed by a complete loss of offsite power a few minutes later (second/remaining incoming line fails sometime after the first line failed).

Unplanned demand—An automatic or manual engineered safety feature actuation for the HPCS system to start.

Unreliability—Probability that the system will fail to complete its required mission when demanded. This includes the contributions of maintenance unavailability, failure to start, and failure to run identified in the operational data. Recovery may or may not be included, depending on the context.

High-Pressure Core Spray System Reliability, 1987–1993

1. INTRODUCTION

The U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data (AEOD), in cooperation with other NRC Offices, has undertaken an effort to ensure that the stated NRC policy to expand the use of probabilistic risk assessment (PRA) within the agency is implemented consistently and predictably. As part of this effort, the AEOD Safety Programs Division has undertaken to monitor and report on the functional reliability of risk-important systems in commercial nuclear power plants. The approach is to compare the estimates and associated assumptions as 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 was undertaken of the high-pressure core spray (HPCS) system in the U.S. commercial boiling water reactors (BWRs) that have an HPCS system.

The evaluation estimates HPCS system unreliability using actual operating experience. To perform this evaluation and make risk-based comparisons to the relevant information provided in the PRAs, unreliability estimates are presented in this study for two conditions. First, estimates are made of the reliability of the HPCS system in performing its routine mission resulting from unplanned actuations occurring in the operational experience. Second, the operational experience data are used to predict the reliability of the HPCS system in performing the risk-significant safety function postulated in probabilistic risk assessments and individual plant examinations (PRA/IPEs). The estimates of HPCS system unreliability were based on data from unplanned demands and system functional tests that best simulate system response to a low reactor vessel water level transient. The data from these sources are considered to best represent the plant conditions found during emergency conditions. Data from component malfunctions that did not result in a loss of safety function of the system were not used. The objectives of the study were to:

- Estimate unreliability based on operational experience data and compare the results with the assumptions, models, and data used in PRA/IPEs.

- Provide an engineering analysis of the factors affecting system unreliability and to determine if trends and patterns are present in HPCS system operational data.

2. SCOPE OF STUDY

This study documents an analysis of the operational experience of the eight BWRs listed in Table 1, all of which have an HPCS system. The analysis focused on the ability of the HPCS system to start and provide its associated emergency core cooling function for the required mission. The system boundaries, data collection, failure categorization, and limitations of the study are briefly described in this section.

Table 1 presents each plant's docket number, the report used to obtain the PRA/IPE estimates of plant specific system unreliability (used for comparison purposes) and other risk-related information, and the configuration of the cooling water system for HPCS. Also included in the table are the operating years used in the study for the eight plants. The operating years are the calendar time minus all periods when the main generator was off-line for more than two calendar days. Licensee event report (LER) data were not collected for a given calendar year if there was no operational time in that year. Appendix A details the calculation of operational time. Appendix B presents the plant data results discussed in Sections 3 and 4 of this report.

2.1 System Operation and Description

2.1.1 System Operation

The emergency core cooling system (ECCS) in the BWRs studied typically consists of the automatic depressurization system (ADS), the HPCS system, the low-pressure core spray (LPCS) system, and the low-pressure coolant injection (LPCI) mode of the residual heat removal system. The purpose of these systems is to reestablish adequate core cooling and maintain continuity of core cooling subsequent to the entire spectrum of postulated loss-of-coolant accidents (LOCAs).

If a LOCA should occur, a low reactor water level signal or high drywell pressure signal initiates the HPCS system and its support equipment. The system can also be placed in operation manually. If the leak rate is less than the HPCS system flow rate, the HPCS system automatically stops when a high reactor water level signal shuts the HPCS injection valve. The injection valve will automatically reopen upon a subsequent low water level signal. Should the leak rate exceed the HPCS system capacity and not

Table 1. BWR plants with an HPCS system.

Plant	Docket	Operating Years	Report	Dedicated Service Water System
Clinton	461	4.9	IPE	Yes
Grand Gulf	416	6.1	NUREG/CR-4550	Yes
LaSalle 1	343	5.4	NUREG/CR-4832	Yes
LaSalle 2	374	5.2	NUREG/CR-4832	Yes
Nine Mile Pt. 2	410	4.5	IPE	No
Perry	440	5.0	IPE	Yes
River Bend	458	5.3	IPE	No
Wash. Nuclear 2	397	5.0	IPE	Yes

result in rapid depressurization of the vessel, the ADS will actuate on a lower water level signal and depressurize the vessel for the LPCS and LPCI systems to provide adequate core cooling. Should the HPCS system fail to initiate during a LOCA, the ADS vessel depressurization and subsequent LPCS and LPCI system initiations will provide adequate core cooling as a backup for the HPCS system.

The HPCS system also serves as a backup to the reactor core isolation cooling (RCIC) system in the event the reactor becomes isolated from the main condenser during operation and feedwater flow is lost. Operational transients that may require HPCS are transients that include a reactor trip and a demand for coolant injection by high-pressure makeup systems (RCIC or HPCS). For example, a transient that results in a reactor trip without a loss of feedwater may require short-term operation of the HPCS and/or other high-pressure makeup system to restore reactor pressure vessel (RPV) water level. For a transient that includes a reactor trip and a loss of feedwater, with no immediate recovery of feedwater, high-pressure makeup is required to restore and maintain RPV water level. The latter type of transient would require longer operation of high-pressure makeup compared to the transients that do not lose feedwater.

2.1.2 System Description

The primary function of the HPCS system is to maintain reactor vessel inventory for line breaks up to 1-in. nominal size. The HPCS system also provides spray cooling heat transfer during breaks in which uncovering of the core is assumed. The HPCS system pumps water through a peripheral ring spray sparger mounted above the reactor core and can supply coolant over the entire range of system operation pressures.

The HPCS system consists of a single motor-driven centrifugal pump located outside primary containment, an independent spray sparger in the reactor vessel located above the core, and associated piping, valves, controls, and instrumentation. Figure 1 is a simplified schematic of the system. The system is designed to operate using normal offsite auxiliary power. Should a loss of offsite power occur, a dedicated backup source of power is available from a diesel generator. The backup source of power (diesel generator) only affects the unreliability of the HPCS system when a loss of offsite power occurs as an initiator or during an HPCS system demand.

The principal active HPCS equipment is located outside the primary containment. Suction piping for the HPCS pump is provided from the condensate storage tank (CST) and the suppression pool. Such an arrangement provides the capability to use reactor-grade water from the CST when the HPCS system functions to back up the RCIC system. In the event that the CST water supply becomes exhausted or is not available, automatic switch-over to the suppression pool water source ensures a cooling water supply for long-term operation of the system.

2.1.3 System Boundaries

The HPCS system consists of a motor-driven centrifugal pump located outside the primary containment, a spray header located in the RPV, and associated piping, valves, controls, and instrumentation. The HPCS system also includes a dedicated backup power source consisting of a diesel generator and its support systems, including lubricating oil, fuel oil and transfer, air start, control, and engine cooling water. In addition, all the power supply components from the dedicated Division III bus to the pumps, valves, controls, and instrumentation are also considered in this study. The normal power supply to the dedicated Division III bus is considered to be outside the scope of this study; however, a risk-based discussion of the effect of a loss of offsite power on the system is included. The HPCS system

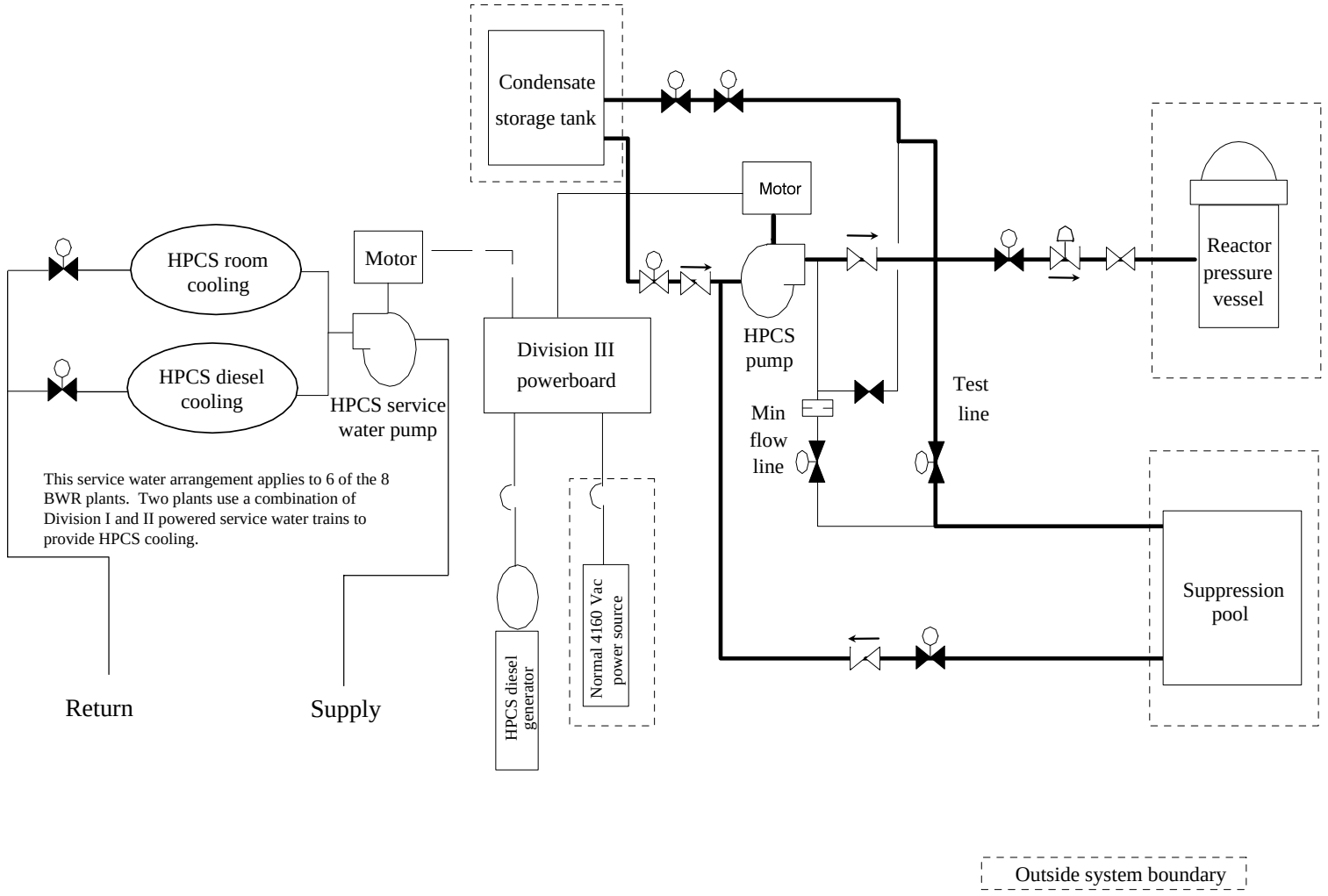


Figure 1. Simplified schematic of the HPCS system.

is supported by a dedicated[a] cooling system consisting of a cooling pump and associated valves and piping. Two plants, Nine Mile Pt. 2 and River Bend, do not have a dedicated HPCS cooling water system. These two plants use the standby service water system to supply HPCS cooling water needs. The dedicated portions of the piping and valves are included in this study; the remainder of the system and the ultimate heat sink are considered outside the scope of this study. The portion of the heating, ventilating, and air-conditioning (HVAC) system directly supporting the HPCS system is also included in this study.

2.2 Operational Data Collection

The source of HPCS system operational data used in this report is LERs identified by the Sequence Coding and Search System (SCSS) database. The SCSS database was searched for all HPCS records for the years 1987 through 1993. To ensure as complete a data set as possible given the LER reporting requirements for HPCS, a search was conducted of all the immediate notification reports required by 10 CFR 50.72 for the same time period that identified the HPCS system. The immediate notification report search results identified fewer events than the SCSS LER search results, and all of the events identified in the immediate notification reports were captured in the LERs. Also, the immediate notification reports did not contain the necessary detail about the HPCS event to conduct a reliability analysis. As a result, only the LER data were used in this report.

2.2.1 Inoperability Characterization

Because the HPCS is an ECCS system required by technical specifications to be operable,[b] all occurrences that resulted in the system not being able to perform its safety function as defined by the respective plant technical specifications (for example, see References 1 and 2) are required by 10 CFR 50.73(a)(2)(v) to be reported in LERs. In addition, 10 CFR 50.73(a)(2)(vii) requires the licensee to report all common mode failures resulting in a loss of capability for safe shutdown. Therefore, the SCSS LER database should include all occurrences when the HPCS system was not operable.

In this report, the term *inoperability* is used to describe any HPCS malfunction or situation in which a LER was submitted in accordance with the requirements identified in 10 CFR 50.73(a)(2). The inoperabilities were subsequently classified as *faults* and *failures* for the purposes of this study. The classification of faults and failures was based on an independent review of the events and was not related to the reportability requirements identified in the LER. The term *failure* is used to identify the subset of the inoperabilities for which the coolant injection function of the HPCS system is lost. The term *fault* is used to describe the subset of inoperabilities that were not classified as failures.

Because the HPCS system includes a dedicated diesel generator, it is necessary to define the term *failure* for this portion of the system separately from the coolant injection portion of the system. For the HPCS diesel generator, a failure is defined as any inoperability for which the ability to supply emergency power to the Division III electrical bus is lost.

Failure Classification—Each of the LERs identified in the SCSS database search was reviewed by a team of U.S. commercial nuclear power plant experienced personnel. Care was taken to properly

a. The ultimate heat sink for the cooling system is not dedicated to the HPCS system.

b. Except where the reactor vessel head is removed, the cavity is flooded and the spent fuel gates are removed, and water level maintained with the limits defined by technical specifications.

classify each event and to ensure consistency of the classification for each event. Because the focus of this report is on risk and reliability, it was necessary to review the full text of each LER and classify or exclude events based on the available information reported in the LER. Specifically, the information necessary for determining reliability such as classification of HPCS failures and faults, failure modes, failure mechanisms, causes, etc. in this report was based on the independent review of the information provided in the LERs. The SCSS data search was only used to identify LERs for screening; no data characterization, evaluation, or reliability analysis was performed on the information encoded in the SCSS database.

Two engineers independently evaluated the full text of each LER from a risk and reliability perspective. At the conclusion of the independent review, the data were combined, and classification of each event was agreed upon by the engineers. The events identified as failures that could contribute to system unreliability were reviewed by the NRC technical monitor and technical consultants with extensive experience in reliability and risk analysis. The review was conducted to ensure consistent and correct classification of the failure event for the reliability estimation process.

Failure classification of the inoperability events was based on the ability of the HPCS system to function as designed for at least a 24-hour mission or until the system was no longer needed for actual missions longer than 24 hours. Each LER was reviewed to determine if the system would have been reasonably capable of performing its design function. Examples of the types of inoperabilities that are classified as failures include (a) malfunctions of the initiation circuit that prevent the system from starting automatically, (b) malfunction of the injection motor-operated valve (MOV) to open with the pump operating properly and RPV water level at or below the initiation setpoint and (c) RPV water level at or below the initiation setpoint and the system out of service for preplanned maintenance.

The HPCS events identified as failures in this study represent actual malfunctions, which prevented the successful operation of the system. When the HPCS injection subsystem receives an automatic start signal as a result of an actual low RPV water level condition or a manual start, the system functions successfully if the HPCS motor-pump starts and obtains rated pressure, the injection valve opens, and coolant flow is delivered to the RPV until the flow is no longer needed. Failure may occur at any point in this process. For the purposes of this study, the following injection subsystem failure modes were observed in the operational data:

- Maintenance-out-of-service (MOOS) occurs if, due to maintenance, the HPCS subsystem is prevented from starting during an unplanned demand.

- Failure to start (FTS) occurs if the subsystem is in service but fails to automatically or manually start, develop sufficient injection pressure, and flow to the reactor pressure vessel.

- Failure to run (FTR) occurs if, at any time after the subsystem is delivering sufficient coolant flow, the HPCS injection subsystem fails to maintain this flow to the RPV while it is needed.

Whenever the HPCS system receives an automatic start signal, the emergency diesel generator (EDG) is demanded to start. If the automatic start is the result of a low-voltage condition on the Division III electrical bus, or if an under-voltage condition occurs following a reactor coolant low-level or high-drywell pressure signal, then the EDG output breaker will shut. Emergency power subsystem failure modes include the following:

- Maintenance-out-of-service of emergency power subsystem (MOOSD) occurred if, because of maintenance, the HPCS emergency power subsystem was prevented from starting automatically during a demand

- FTS occurred if the subsystem was in service but failed to automatically start and, if demanded, the breaker failed to close and energize the Division III bus

- FTR occurred if, at any time after the EDG had started, it failed to power the Division III bus, or would have failed to do so had the output breaker been shut.

Recovery of failures is important and was considered when estimating system unreliability. To recover from a failure, operators have to recognize that the system is in a failed state, restart it without performing maintenance (for example, without replacing components), and restore coolant flow to the RPV. An example of such a recovery would be an operator (a) noticing that the injection MOV had not opened during an automatic start of the system and (b) manually operating the control switch for this valve, thereby causing the MOV to open fully and allow coolant flow to the RPV. Recovery for the other failure modes is defined in a similar manner. Each failure was evaluated to determine whether recovery by an operator occurred.

The analysis section of each LER was used to determine if the system would have been able to perform as required even though the system was declared not operable as defined by plant technical specifications. As an example, the LER may have been submitted for the late performance of a technical specification required surveillance test. This event would be classified a fault, not a failure. This classification is based on the judgment that given a demand, the system would still be capable of functioning as designed. Moreover, plant personnel typically would state in the LER that the system was available to respond and that the subsequent surveillance test was performed satisfactorily. If the system failed the subsequent surveillance test, the event would have been classified as a failure. In addition, administrative problems associated with HPCS were also classified as faults, given the system had successfully passed a recent surveillance test or remained capable of injecting water into the RPV. As an example, the discharge piping was found to not have the required number of seismic restraints. However, the results of an engineering analysis in the safety analysis section of the LER indicated that the existing system configuration would successfully complete the missions postulated in this report. As a result, the event was classified as a fault.

2.2.2 Demand Collection and Characterization

For the reliability estimation process, the total number of demands associated with a specific set of failures must be known. Two criteria are important in selecting data sets for reliability analysis. First, useful data must, of course, be *countable*. Reasonable assurance must exist that the number of failures and demands can be estimated, that all failures will be reported, and that sufficient detail will be present in the failure reports to match the failures to the applicable demand estimates.

The second criterion is that the demands must reasonably approximate the conditions being considered in the unreliability analysis. The unplanned demands or tests must be rigorous enough that successes as well as failures provide meaningful system performance information. The determination of whether each demand reasonably approximates conditions for required accident/transient response depends in turn on the missions being modeled by each failure probability estimate.

Unplanned Demands—LERs can be used to provide information on unplanned demands following plant transients that resulted in an actual low RPV water level condition, that is, an actual need

for the HPCS system. These unplanned demands were identified by searching the SCSS database for all LERs containing critical reactor scrams for plants having an HPCS system during the 1987—1993 study period. The critical reactor scram events are reportable under 10 CFR 50.73 (a)(2)(iv). Critical reactor scram events provide the basis for determining if the HPCS system was used to mitigate the consequences of a RPV water level control transient during the scram. In addition, unplanned HPCI and HPCS engineered safety feature (ESF) actuations are reportable under the same reporting requirements as reactor scrams.

The LERs that contained HPCS actuations were screened to determine the nature of the HPCS actuation. The HPCS actuations identified in the LERs and classified in this study as HPCS unplanned demands were events that resulted in coolant flow to the RPV. Some of the actuations were demands of only a part of the system. The partial demands did not exercise the system in response to an actual need for injection because RPV water level was restored using another source (typically feedwater) prior to the injection valve opening. Therefore, these records were excluded from the count of HPCS unplanned demands.

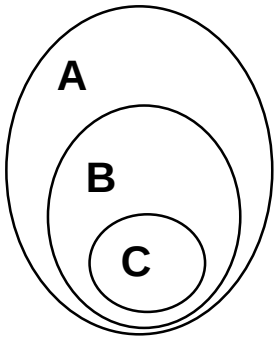
Surveillance Test Demands—A review of several plant technical specifications indicated that plants are required to simulate an actuation of the automatic start of the HPCS system with a periodicity of once a fuel cycle, or once every 18 months (referred to as cyclic tests). These tests typically simulate automatic actuation of the system throughout its emergency operating sequence and that each automatic valve actuate to the correct position. Because of the completeness of the cyclic surveillance test compared to other tests, the cyclic surveillance test data were included in the system unreliability calculation. However, because the injection valve is not tested under the conditions the valve would experience during an unplanned demand (flow to the vessel), data from cyclic tests were not used to estimate the failure probability for this valve.

In addition to the cyclic surveillance tests, quarterly surveillance tests of the injection pump that are required to be performed per ASME Section XI can also be utilized to estimate unreliability. Because of the completeness of the cyclic and quarterly (for the injection pump only) surveillance tests compared to other surveillance tests (weekly, monthly, etc.), only these surveillance tests were used to estimate unreliability. For more details on the counting of unplanned demands and surveillance test demands, see Section A-1.2 in Appendix A.

2.3 Methodology for Operational Data Analysis

The risk-based and engineering analyses of the operational data are based on two different data sets. The Venn diagram in Figure 2 illustrates the relationship between these data sets. Data set A represents all the LERs that identified an HPCS system inoperability from the previously mentioned SCSS database search. Data set B represents the inoperabilities that were classified as failures of the HPCS system. Data set C represents those actual failures identified from LERs for which the corresponding demands (both failures and successes) could be counted. It is data set C that provides the basis for estimating the unreliability of the HPCS system. Data set C contains all relevant failures that occurred during either an unplanned full demand, a cyclic surveillance test, or for the injection subsystem FTR failure mode, quarterly surveillance tests. The only criteria are the occurrence of a *real* failure and the ability to count all corresponding demands (that is, both failures and successes). Data set C represents the minimum requirements for the data used in the risk-based analysis of the operational experience.

To eliminate any bias in the analysis of the failure and demand data in data set C and to ensure a homogeneous population of data, three additional selection criteria on the data were imposed. These criteria were: (1) the data from the plants must be reported in accordance with the same reporting



A The HPCS system was inoperable as defined by applicable technical specifications.

B The injection function of the HPCS system was lost (failure).

C The injection function of the HPCS system was lost (failure), and the demand count could be determined or estimated.

Figure 2. Illustration of the relationship between the inoperability and failure data sets.

requirements, (2) the data from each plant must be statistically from the same population, and (3) the data must be consistent (that is, from the same population) from an engineering perspective. Each of these three criteria must be met, or the results of the analysis would be incorrectly influenced. As a result of these three criteria, the failure and demand data that constitute data set C were not analyzed strictly on the ability to count the number of failures and associated demands for a risk-based mission, but also to ensure each of the above three criteria was met.

The purpose of the engineering analysis was to provide qualitative insights into HPCS system performance, not to calculate quantitative estimates of unreliability. Therefore, the engineering analysis used all HPCS inoperabilities appearing in the operational data. That is, the engineering analysis focused on data set A, which includes data set C with an engineering analysis of the factors affecting HPCS system reliability. However, the MOOS events were excluded from the engineering analysis because, though they result in the inability of the HPCS system to supply coolant to the vessel, they do not always involve an actual failure of the system (that is, they could be preventative rather than corrective). An unplanned demand of the HPCS system while maintenance was being performed on that system during power operating conditions was considered in estimating unreliability but was not part of the engineering analysis.

3. RISK-BASED ANALYSIS OF THE OPERATIONAL DATA

The data pertaining to the capability of the HPCS system to inject water into the RPV (referred to as 1987–1993 operational experience data for the purposes of this section of the report) were assembled from LERs and analyzed in two ways. First, estimates of HPCS unreliability were calculated directly from the 1987–1993 experience. These unreliability estimates are based on the operational missions that HPCS encounters during transients that include a reactor trip and a demand for coolant injection by high-pressure makeup systems (RCIC or HPCS). For example, a transient that results in a reactor trip without a loss of feedwater may require short-term operation of the HPCS and/or another high-pressure makeup system to restore RPV water level. For a transient that includes a reactor trip and a loss of feedwater, with no immediate recovery of feedwater, high-pressure makeup is required to restore and maintain RPV water level. The latter type of transient would require longer operation of high-pressure makeup compared to the transients that have feedwater available. Estimates of HPCS operational unreliability were based on these operational missions (transients).

The estimates of HPCS system operational unreliability are further analyzed to uncover trends and patterns within HPCS systems in U.S. commercial nuclear power plants. Plant-specific and industry-wide trend and pattern analyses provide insights into the reliability performance of the HPCS system.

Next, comparisons were made between the HPCS unreliabilities based on 1987–1993 experience and those reported in selected PRAs, IPEs, and NUREGs. To provide an appropriate comparison, the conditions typically postulated in the PRA/IPEs were also assumed for quantifying the HPCS unreliability model. The comparisons provide an indication of the extent that unreliabilities based on 1987–1993 experience are consistent with those reported in the PRAs, IPEs, and NUREGs.

Data results from seven plant risk information reports (that is, PRAs, IPEs, and NUREGs) were compared with the HPCS reliability results calculated for this study. These risk reports document risk information for eight BWR plants. The data contained in these reports represent all of the operating BWR plants with an HPCS system. For the purposes of this study, the risk reports are referred to collectively as PRA/IPEs.

HPCS unreliabilities were estimated using fault tree logic to associate failure events with broadly defined failure modes such as failure to start and failure to run. The probabilities for the individual failure modes were calculated by reviewing the failure information (see Appendix C), categorizing each failure event by failure mode and subsystem, and then estimating the corresponding number of demands (both success and failures). HPCS system unreliability was also estimated from PRA/IPE information. Generally, the HPCS fault tree logic models were not available in the PRA/IPEs. However, the component failure probabilities used in calculating HPCS unavailability were available. In order to compare the PRA/IPE data and results to those calculated from the operational data, unreliabilities were approximated from the relevant information contained in the PRA/IPEs. The component failure probabilities were extracted and linked to the corresponding system failure modes identified in the fault tree developed for analysis of the 1987–1993 experience. The component failure probabilities extracted from the PRA/IPEs were generally those identified as the major contributors to HPCS unavailability. Therefore, the PRA/IPE estimates approximated for this study are likely to be different, but not significantly, from those used in PRA/IPE quantification.

The following is a summary of the major findings:

- The HPCS system operational unreliability (including recovery) estimate calculated from the 1987–1993 experience is 0.075. If recovery is ignored, the operational unreliability estimate

is unaffected, since no failures could be recovered. Maintenance-out-of-service is the leading contributor (67%) to HPCS operational unreliability followed by failure of the injection valve (27%).

- The HPCS unreliability estimate calculated for comparison with PRA/IPE results is 0.23. The potential for failure recovery exists; however, the HPCS unreliability estimate (0.23) essentially remains unchanged. The leading contributors to HPCS unreliability estimate used for comparison to PRA/IPE results are maintenance of the injection subsystem (22%), maintenance of the emergency power subsystem (21%), failure to run of the Division III diesel generator (19%), failure to run of the injection subsystem (16%), and failure of the suction transfer from the condensate storage tank to the suppression pool (15%).

- The HPCS unreliability estimated from the 1987–1993 experience for comparison with PRA/IPE results and the HPCS unreliability calculated from the PRA/IPE data are plotted in Section 3.2 (Figure 6). The HPCS system mean unreliability estimates approximated from the PRA/IPE data are lower than the mean estimates derived from the 1987–1993 experience. The contributors to HPCS system unreliability calculated from the PRA/IPE information are not consistent with those calculated from the 1987–1993 experience. The PRA/IPE estimates resulted in the HPCS emergency power subsystem being the leading contributor (75%), with the HPCS injection subsystem contributing 25% to overall HPCS unreliability. Based on the 1987–1993 experience, the HPCS injection subsystem accounted for roughly 60% of the HPCS system unreliability. The reasons for this difference appear to be the lower failure probabilities used in the PRA/IPEs for the maintenance out of service and failure to run of the HPCS injection subsystem. The PRA/IPEs average hourly failure rate for the HPCS motor-pump is 3E-5 per hour compared to the 1987–1993 experience mean of 1.6E-3 per hour. The pump train failure to run rate (1987–1993 experience) was based on sparse data, no failures in 316 hours. Further, the HPCS motor run times were short, therefore, lacking evidence to the contrary, the failure rate was assumed to be constant. The constant failure to run rate is typically assumed in PRA/IPEs as well as the system operational requirement of twenty-four hours. Based on no failure observations and the short run times in the 1987–1993 experience, the PRA/IPEs hourly failure rate for the HPCS injection pump may be optimistic. Additional data (i.e., operating experience) are needed before high confidence can be placed on either the PRA/IPE failure to run estimate or the estimate based on 1987–1993 experience.

- No trends were identified in the HPCS operational unreliability when plotted against low-power license date or when plotted with regard to calendar year.

3.1 Estimates of HPCS Operational Unreliability

Estimates of HPCS unreliability were calculated using the unplanned demands and the cyclic and quarterly (for injection subsystem FTR) tests data. The failure data were used to develop failure probabilities for the observed failure modes defined in Section 2. The contributions to the unreliability of the HPCS system from support systems outside the HPCS boundary defined in Section 2.1.3 are excluded from the failure counts.

The failures identified below fall into the following failure modes: MOOS, FTS, and FTR. The FTS and FTR modes were further broken down into more specific failure modes in order to use as much of the failure and demand data as possible. The maximum usage of the data was to obtain additional

insights into the HPCS reliability, minimize the effects of sparse data, and to reduce the uncertainty associated with the particular estimate of failure probability.

Additionally, the data associated with the MOOS failure mode were segregated with respect to plant operating mode. The maintenance events were categorized as to whether the plant was operating or was shut down at the time of the unplanned demand. For the unreliability estimates calculated, only the contribution of MOOS while the plant is operating was included.

HPCS Injection—For injection, the FTS mode was split into two components to incorporate both the cyclic and quarterly test data into the analysis. The cyclic and quarterly tests do not test the injection valve under the same conditions observed during an unplanned demand. Specifically, the injection valve is isolated from the rest of the system; therefore, the injection valve operates with no differential pressure applied across the valve. For unplanned demands, the valve is subjected to a differential pressure. For this reason, the FTS consists of failure to start attributed to the injection valve (FTSV) and failure to start of the injection subsystem due to causes other than injection valve problems (FTSI). The FTSI probability estimates are derived using the cyclic and quarterly test and unplanned demand data. However, the probability estimates for FTSV are calculated from only the unplanned demand data.

FTR events were also broken into two failure modes. FTR was split into those events pertaining to the suction path transfer capability (FTRT) and all other events related to the injection segment (FTRI). The FTRT probability estimate was based only on the cyclic test data (since this capability is tested). The FTRI failure probability was based on the cyclic test data and the unplanned demand data.

The types of data (that is, cyclic and quarterly test and unplanned demands), failure counts, and demand counts used for estimating probabilities for the HPCS injection subsystem failure modes are identified in Table 2.

Table 2. Failure data sources and counts used for estimating HPCS injection failure mode probabilities.

	Unplanned Demands		Cyclic Tests		Quarterly Tests	
Failure mode	f [a]	d [a]	f [a]	d [a]	f [a]	d [a]
Maintenance-out-of-service (MOOSI)[b] while shut down	0	4	—	—	—	—
Maintenance-out-of-service (MOOSI)[b] while not shut down	1	29	—	—	—	—
Failure to start other than injection valve (FTSI)	0	32	0	43	1	224
Failure to start, injection valve (FTSV)	0	24	—	—	—	—
Failure to run other than suction transfer (FTRI)	0	31	0	43	0	223
Failure to run, suction transfer (FTRT)	—	—	1	43	—	—

a. f denotes failures; d denotes demands.

b. In this report, the MOOS contribution to HPCS injection system unreliability was determined using those unplanned demand failures that resulted from the HPCS injection system being unavailable for preventive or corrective maintenance at the time of the demand.

The demand counts identified in Table 2 represent opportunities for HPCS injection subsystem success. Each failure observed in an HPCS operational phase that was not recovered takes away an opportunity from a following phase. With this in mind, the counts in Table 2 are based on the following logic:

- For the HPCS injection subsystem to have the opportunity to start the system, it could not be inoperable because of maintenance at the time of the demand. If so, there is no opportunity for HPCS to start. There were a total of 33 unplanned demands. Of the 33 events, 29 unplanned demands occurred while operating and four while shut down, with one failure caused by the system being out for maintenance.

- The opportunities to start consist of the number of initial unplanned demands minus any MOOSI failures observed. Hence, there were 32 opportunities for the system to start resulting from unplanned demands (33 demands minus one MOOSI failure). The failure to start of the HPCS injection subsystem was partitioned into FTSI and FTSV to gain further insight into the reliability for this operational phase and to use as much of the cyclic and quarterly test data as possible. The next event in the sequence of system response is the FTSI category. The FTSI unplanned demand and failure count is based on the 32 unplanned demands, 43 cyclic tests, and 224 quarterly tests for the injection system to succeed.

- The next operational event in an HPCS injection subsystem response deals with FTSV. The injection valve opens when a permissive signal based on pump discharge pressure is activated. Therefore, the opportunities for FTSV consist of 32 demands minus any failures that were not recovered from FTSI. The FTSV unplanned demand count was further reduced by eight unplanned demands that did not challenge the injection valve. The cyclic and quarterly tests of the injection subsystem do not challenge the injection valve under the same stresses as those present in an unplanned demand. Therefore, these test opportunities of the injection valve are not included in the FTSV failure mode calculation.

- Since no failures were observed during the failure to start phase, there are no opportunities to be recovered. Therefore, the recovery of failure to start is not included due to the absence of data. For failures detected during testing, the test is generally terminated, and no immediate (urgent) attempt is made to recover from the test failure.

- For the run phase of the HPCS injection subsystem operation, there were a total of 31 unplanned demands, 43 cyclic test, and 223 quarterly test (224 tests minus one FTSI failure) opportunities. The failure to run of the HPCS injection subsystem was partitioned into FTRI and FTRT to gain further insight into the reliability for this operational phase and to use as much of the data as possible. The FTRI counts are based on no failures in the 31 unplanned demands and 43 cyclic and 223 quarterly test opportunities. The FTRT counts are based only on the one failure detected during the 43 cyclic tests that challenged the suction path transfer function of the injection system. The unplanned demands were of short duration, thereby not requiring the suction path to be transferred. The quarterly tests also do not exercise this capability of the injection subsystem.

- The failures observed during the run phase have the opportunity to be recovered. However, for the unplanned demands, there were no failures to be recovered. Failures observed during

the run phase of the test generally result in the test being terminated, and no immediate effort to recover the failure is attempted.

HPCS Emergency Power—For the emergency power portion of the HPCS, a similar rationale that was used for the injection subsystem was applied to the failure mode breakdown. FTS was subdivided into failure to start due to the Division III EDG output breaker (FTSB) failure and failure to start due to reasons other than the output breaker (FTSD). The main reason for this breakdown was that many of the starts of the emergency power only resulted in the EDG starting with no closing of the output breaker. This is primarily caused by the EDG receiving a start signal in response to a safety injection demand but not with a coincident undervoltage condition on the Division III electrical bus. The FTSB probability estimate was calculated from the cyclic test data and only those unplanned demands challenging the output breaker. The probability estimate for FTSD was based on the cyclic test and unplanned demand data.

The demand counts identified in Table 3 represent opportunities for HPCS emergency power subsystem success. The counts in Table 3 are based on the following logic:

- For the HPCS emergency power subsystem to have the opportunity to start, the system could not be inoperable because of maintenance at the time of the demand. If so, there is no opportunity for HPCS EDG to start. There were a total of 46 unplanned demands for the emergency power. Of these, 30 unplanned demands occurred while operating and 16 while shut down.

- The opportunities to start consist of the number of initial unplanned demands minus any MOOSI failures observed. Therefore, 43 opportunities for the system to start were recorded as a result of the unplanned demands. The failure to start of the HPCS emergency power

Table 3. Failure data sources and counts used for estimating HPCS emergency power failure mode probabilities.

	Unplanned Demands		Cyclic Tests	
Failure Mode	*f* [a]	*d* [a]	*f* [a]	*d* [a]
Maintenance-out-of-service (MOOSD)[b] while shut down	2	16[c]	—	—
Maintenance-out-of-service (MOOSD)[b] while not shut down	1	30[c]	—	—
Failure to start other than output breaker (FTSD)	0	43	0	43
Failure to start due to output breaker (FTSB)	0	8	0	43
Failure to run (FTRD)	2	43	0	43
Failure to recover from FTRD (FRFTRD)	2	2	—	—

a. *f* denotes failures; *d* denotes demands

b. In this report, MOOS contribution to HPCS emergency power system unreliability was determined using those unplanned demand failures that resulted from the HPCS emergency power system being unavailable because it was in maintenance at the time of the demand.

c. The unplanned demand count for the emergency power subsystem is larger than that for the injection subsystem since an undervoltage condition on the Division III bus will result in an unplanned demand for the HPCS emergency power subsystem but not the HPCS injection subsystem.

subsystem was partitioned into FTSB and FTSD to gain further insight into the reliability for this operational phase. Therefore, the next event in the sequence of system response is the FTSD category. The FTSD unplanned demand count is based on the 43 unplanned demands. Also, there were 43 cyclic test opportunities for the emergency power to succeed. No failures were detected by either type of demand; hence, no recovery data are available for FTSD.

- Of the 43 unplanned demands for the start phase, only eight challenged the output breaker to close. Cyclic testing provided an additional 43 opportunities for the output breaker to function. No failures for FTSB were observed for either the unplanned demands or cyclic tests.

- Since no failures were observed during the failure to start phase, there are no opportunities to be recovered. Therefore, the recovery failure modes are not included.

- For the run phase of HPCS emergency power operation, there were a total of 43 unplanned demands for which the EDG reached rated speed and voltage and/or was loaded. Of these demands, two failures were counted. There were another 43 cyclic test opportunities for this operational phase with no failures.

- Of the failures observed during the run phase, there is a potential for these failures to be recovered. For the unplanned demands, the two failures to run were not recovered.

In calculating failure probabilities for the individual failure modes, the data were analyzed and tested (statistically) to determine if significant variability was present in the data. All data were initially analyzed by plant, by year, and by source (that is, unplanned, cyclic, and quarterly test demands). Each data set was modeled as a binomial distribution with confidence intervals based on sampling uncertainty. Various statistical tests (Fisher's exact test, Pearson chi-squared test, etc.) were then used to test the hypothesis that there is no difference between the types and sources of data.

Due to concerns about the appropriateness and power of the various statistical tests and the possibility that there are real physical differences between groups, an empirical Bayes method to model variation was attempted regardless of the results of the statistical testing for differences. The simple Bayes method was used only if no empirical Bayes could be fitted. [For more information on this aspect of the data analysis, see Appendixes A and C (Sections A-2.1 and C-1.1)]. In the simple Bayes case, the uncertainty in the calculated failure rate is dominated by random or statistical uncertainty (also referred to as *sampling* uncertainty). The simple Bayes essentially pools the data and treats it as a homogeneous population. On the other hand, if an empirical Bayes distribution was fitted, then the uncertainty was dominated by the *plant-to-plant* (or year-to-year) variability. That is, the data were not pooled, and individual plant or year-specific failure probabilities were calculated based on the factor that produced the variability.

For the maintenance failure mode, the unplanned demand data were not pooled with test data since plant personnel are unlikely to initiate an HPCS system test if the HPCS system is out of service for maintenance. Only maintenance events that resulted from an unplanned demand while the plant was not shut down are included in the unreliability estimates. No statistical plant-to-plant variability exists for the maintenance failure mode.

Also, it was assumed that the HPCS dedicated service water subsystem would be demanded every time the HPCS EDG received an actuation signal to start. There were no failures of the dedicated service

water subsystem upstream of the system boundaries [i.e., upstream of HPCS room and EDG coolers service water isolation valves (motor-operated)]. Further, it was postulated that the HPCS dedicated service water subsystem would be out of service anytime the maintenance was performed on the Division III EDG, and vice versa. The maintenance contribution of the dedicated service water subsystem was accounted for implicitly in the unreliability calculation (MOOSD) for the HPCS emergency power subsystem. No maintenance events were identified for the dedicated service water subsystem, thereby strengthening the belief that the service water maintenance can be included as part of the HPCS EDG maintenance calculation. Therefore, to minimize the potential for overcounting the maintenance contribution, the dedicated service water maintenance was implicitly included as part of the MOOSD probability.

3.1.1 HPCS System Operational Unreliability

The operational unreliability of the HPCS system was calculated using the simple fault tree model shown in Figure 3. The model was constructed to reflect the failure modes identified in the unplanned demand and cyclic/quarterly test data. Furthermore, the fault tree model of the HPCS system consists of two subtrees for the two major HPCS subsystems: injection and emergency power. Estimates of HPCS unreliability were calculated using the 1987–1993 experience. These data were statistically analyzed to develop failure probabilities for each of the failure modes included in the fault tree model (see Appendices A and C for the details on the statistical applications and methods). The following failure modes were developed:

HPCS injection

Failure to start, other than the injection valve (FTSI)

Failure to start, injection valve (FTSV)

Failure to run, other than suction transfer (FTRI)

Maintenance-out-of-service of the injection subsystem (MOOSI).

For the operational model, the HPCS emergency power was treated as an undeveloped event. The primary reason for using an undeveloped event is that the failure information contained in the unplanned demand data identified only safety injection demands with no concurrent undervoltage condition on the Division III bus. The normal power to the Division III bus was available during all these events. The philosophy for calculating the HPCS operational unreliability is strongly predicated on the unplanned demand data (that is, no need for emergency power). Further, the suction transfer failure mode was left out since the unplanned demands did not identify any challenges of this function. Recovery failure modes with no failure data are also modeled as undeveloped events. The undeveloped events are depicted by a diamond shape in the fault tree.

Table 4 presents the probabilities and associated uncertainty intervals calculated from the 1987–1993 experience for each of the failure modes. Table 5 presents the estimated HPCS unreliability and associated uncertainty intervals resulting from quantifying the HPCS fault tree using the estimates in Table 4. For the purposes of quantifying the fault tree, the following conditions were assumed:

- A demand to provide core spray to the RPV is received by the HPCS system
- The FTR contribution to the unreliability is estimated on a per mission demand basis

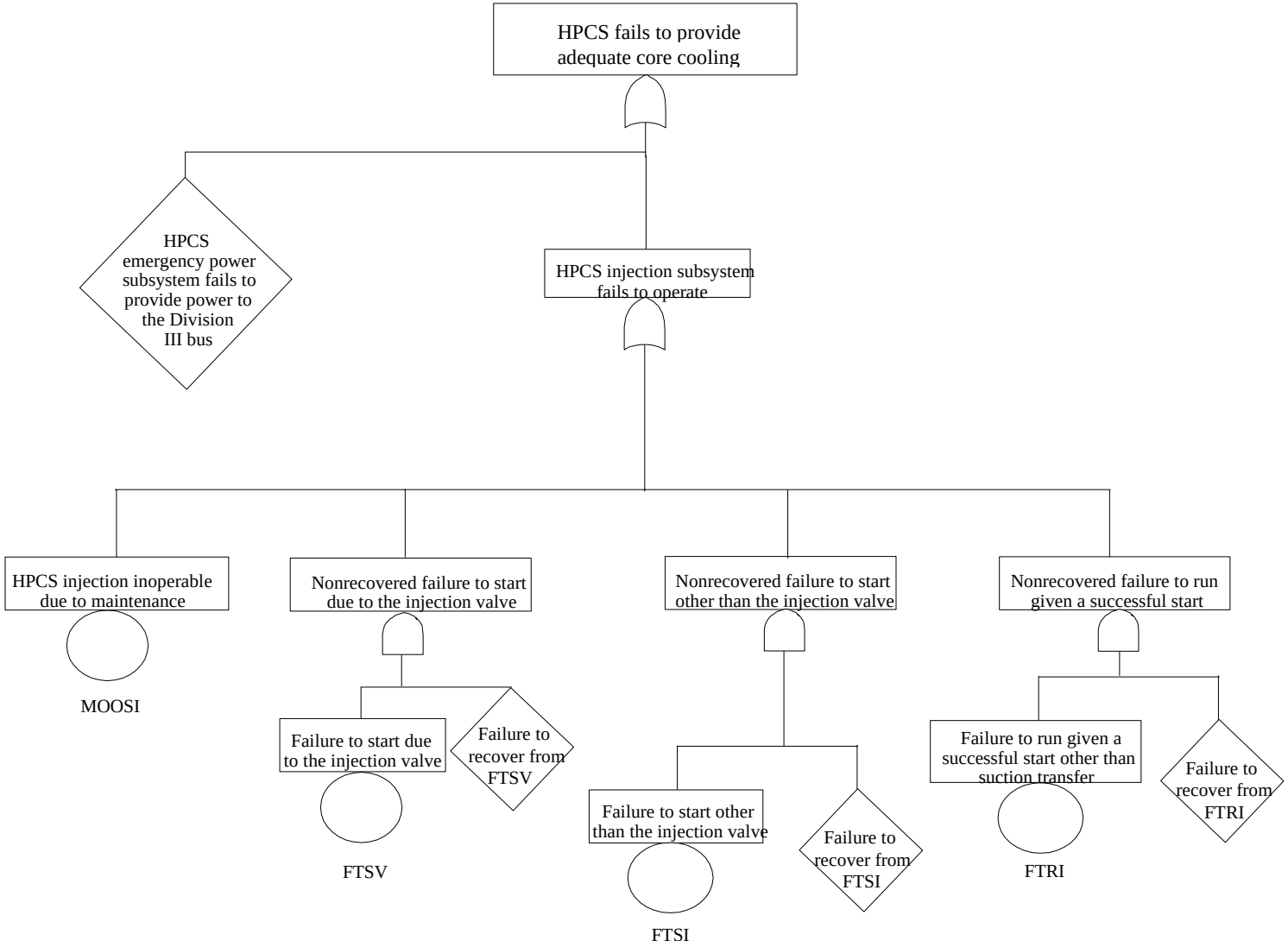


Figure 3. System fault tree of HPCS for calculating operational unreliability.

Table 4. HPCS system failure mode data and Bayesian probability information for estimating operational unreliability.

Failure Mode	f [a]	d [a]	Modeled Variation	Distribution	Bayes Mean and 90% Interval[b]
HPCS injection					
Maintenance-out-of-service while not shut down (MOOSI)	1	29	Sampling	Beta(1.5, 28.5)	(6.1E-3, 5.0E-2, 1.3E-1)
Failure to start other than injection valve (FTSI)	1	299	Sampling	Beta(1.5, 298.5)	(5.9E-4, 5.0E-3, 1.3E-2)
Failure to start due to injection valve (FTSV)	0	24	Sampling	Beta(0.5, 24.5)	(8.1E-5, 2.0E-2, 7.6E-2)
Failure to run other than suction transfer (FTRI)	0	297	Sampling	Beta(0.5, 297.5)	(6.6E-6, 1.7E-3, 6.4E-3)

a. *f* denotes failures; *d* denotes demands.

b. The values in parenthesis are the 5% uncertainty limit, the Bayes mean, and the 95% uncertainty limit.

Table 5. Estimates of HPCS operational unreliability.

Failure Mode	Failure Probability	Contribution (%)
HPCS injection		
MOOSI	0.05	67
FTSI	0.005	7
FTSV	0.02	27
FTRI	0.002	3
HPCS injection unreliability (mean)	0.075[a]	
90% uncertainty interval	(1.7E-2, 1.6E-1)	

a. Mean unreliability for the subsystem is calculated by combining individual failure probabilities. Note that this is not the simple sum of the individual failure probabilities.

- The normal offsite power is available to the Division III bus

- No suction transfer to the suppression pool is required.

Since empirical Bayes distributions were not found for any of the failure modes for the operational unreliability, no plots of plant-specific estimates of HPCS operational unreliability are provided. The plant-specific estimates of operational unreliability are simply those presented in Table 5 for the overall population.

3.1.2 Investigation of Possible Trends

Estimates of HPCS unreliability on a per year basis were calculated to identify any overall trends within the industry estimates. Figure 4 displays the unreliability trend of the HPCS system by calendar year. The unreliability for each calendar year was obtained using the "constrained noninformative prior" for each failure mode pooled across plants for each calendar year as described in Appendix C. The calculated unreliabilities are based on the operational model depicted in Figure 3. The slope of the trend line is not statistically significant (P-value = 0.91).

To give some indication of the effect of plant aging (that is, older plants versus newer plants) on HPCS performance, plant-specific estimates of HPCS unreliability were plotted against the plant low-power license date. The plot is shown in Figure 5 with 90% uncertainty bars plotted vertically. A trend line and a 90% confidence band for the fitted trend line are also shown in the figure. The slope of the trend line is not statistically significant (P-value = 0.71).

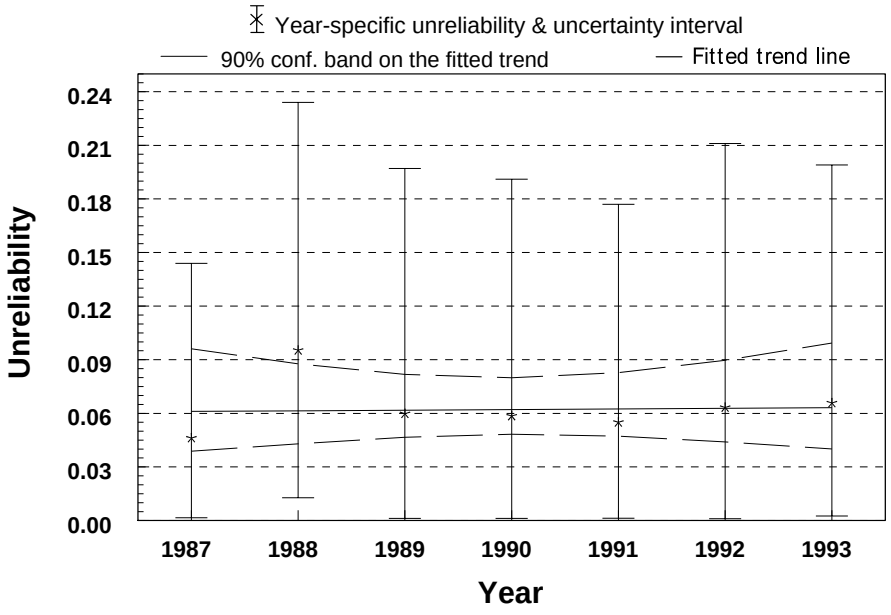


Figure 4. HPCS system operational unreliability plotted by calendar year. The plotted trend is not statistically significant (P-value = 0.91).

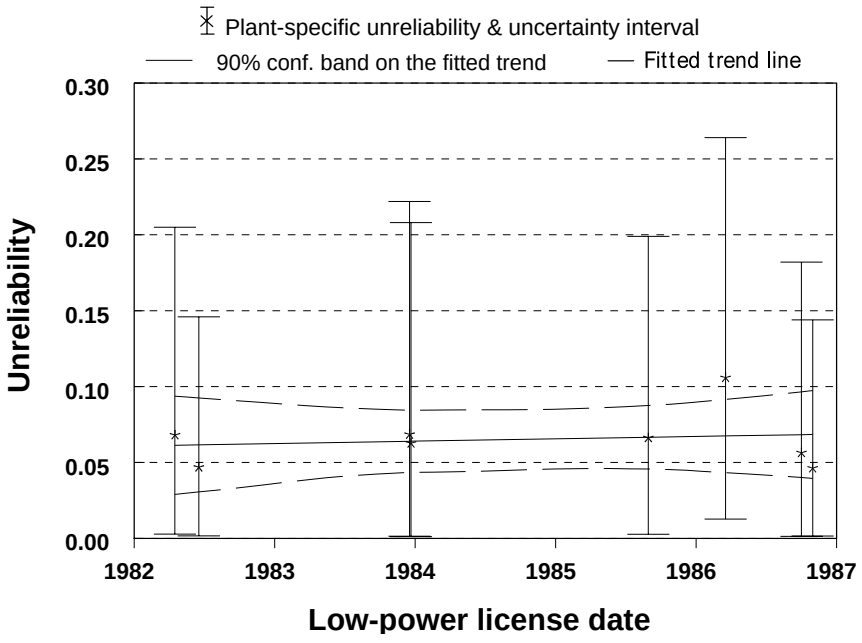


Figure 5. Plant-specific HPCS system operational unreliability plotted by low-power license dates. The plotted trend is not statistically significant (P-value = 0.71).

3.2 Comparison to PRAs

The fault tree models shown in Figures D-1 and D-2 of Appendix D present the logic for calculating HPCS system unreliability based on the postulated conditions stated in the PRA/IPEs. The logic model also provided the template for mapping relevant PRA/IPE component failure probabilities into an HPCS system model. The mapping provides a relational structure for comparing PRA/IPE results to the estimates derived from the 1987–1993 experience. The component failure probabilities were taken from seven PRA/IPEs (References 3 through 9), documenting all eight plants with HPCS systems.

For the purposes of quantifying the fault tree, the following conditions were assumed:

- A demand to provide core spray to the RPV is received by the HPCS system
- The HPCS system is required to be operable for 24 hours
- The FTR contribution to the unreliability assumes a mission time of 24 hours
- The normal offsite power to the Division III electrical bus is not available
- The HPCS system is assumed to require automatic transfer of suction from the CST to the suppression pool.

To provide consistency in comparisons of PRA/IPE results to corresponding results of analysis of the 1987–1993 experience, the contributions to the HPCS unreliability from support systems outside the HPCS boundary defined in Section 2.1.3 were excluded from the PRA/IPE models. The recovery event of failure to recover from FTRD is included in the unreliability analysis of the 1987–1993 experience.

The recovery failure modes identified in the data are defined such that actual diagnosis (beyond identifying the need to attempt re-starting the system) and repair of HPCS system is not required to make the system operational. Generally, the events listed in these categories require a simple restarting of the system if the automatic initiation circuitry did not start the system. Hence, the estimate of HPCS unreliability includes recovery. PRA/IPEs may model this type of event at the system level. However, because of the summary nature of the information presented in many of the PRA/IPEs (for example, the lack of information related to model/quantification assumptions) and the small contribution this type of recovery has on the final estimate (that is, failure to recover from an automatic initiation failure), these actions are not explicitly accounted for in the PRA/IPE results.

Other types of recovery modeled in PRA/IPEs involve actual diagnosis and repair of the components that experience a catastrophic failure. These types of recovery are generally modeled at the accident scenario level (that is, accident sequence cutset) since actual diagnosis and repair of the failed equipment is required. Evaluating the potential for recovery of the various system failures identified in the accident sequence cutset allows for the optimum recovery strategy to be considered. This type of recovery is significantly different from the recovery failure modes identified in the 1987–1993 experience (that is, no repair required). Only the recovery requiring no repair is used in the HPCS system calculations.

The failure mode estimates based on 1987–1993 experience used in the unreliability calculations are listed in Table D-1. No plant-specific estimates were calculated using an empirical Bayes method since no plant-to-plant variability was identified in the respective failure modes. Appendix C contains the results of the plant-specific analysis. Since no plant-to-plant variability could be quantified (or at least it is overwhelmed by the statistical data uncertainty), the industry average probabilities for the respective failure modes were applied to all plants.

The failure probability estimates associated with the FTRI mode of HPCS operation were not calculated on a per demand basis as was done for the operational mission analysis of the previous section. An hourly failure rate was used instead to quantify the overall probability of failure to run for the injection subsystem. For these calculations, the injection run times stated in the LERs for the unplanned demands were used. The cumulative run time based on the 31 unplanned demands is approximately 50 hours. One hour of running time was assumed for each cyclic and quarterly test for a cumulative test run time of 266 hours (43 run hours from cyclic tests and 223 hours from quarterly tests). The run time assumed for the tests was based on a survey of Idaho National Engineering and Environmental Laboratory (INEEL) personnel (former plant operators, examiners, maintenance personnel, etc.) who have experience in the operation and testing of the HPCS system. Further, the run times based on cyclic and quarterly tests were only used in estimating the FTRI probabilities. Since the run times are short and no failures were observed in the 316 hours of run time, postulating a time dependent failure rate was not possible. The failure rate based on the sparse data was assumed to be constant throughout the entire mission (twenty-four hours). (The constant failure rate assumption was made in all of the IPEs.) Additional data are needed in order to establish a higher confidence in the failure to run estimate. Details of the total run time calculations are presented in Appendix A.

The FTRD estimates were calculated from the pooled data from unplanned demands and cyclic tests even though the two FTRD data sets were statistically flagged as not poolable (P-value = 0.004). The unplanned demands accounted for two failures in 73 hours, while the cyclic tests resulted in no failures in 1,032 hours for the FTRD failure mode. One of the two failures in the unplanned demands data set is a sequential loss of offsite power at Nine Mile Pt. 2 that resulted in the Service Water system being isolated, thereby causing the HPCS EDG failure to run. Nine Mile Pt. 2 is one of only two HPCS plants that does not have a cooling water system dedicated to the HPCS diesel. In addition, the design of the Service Water was subsequently modified to account for the effect of a sequential loss of offsite

power on Service Water system availability. The inclusion of this failure, even though it is somewhat unique and was subsequently designed out, resulted in the nonpoolable data sets. However, the failure was included for completeness of the failure data and because the failure did affect HPCS system reliability.

In addition to the overall HPCS system unreliability comparisons, the component failure probabilities from the PRA/IPEs were grouped into the same system failure modes defined for analysis of the 1987–1993 experience. The component failure modes identified in the PRA/IPEs were grouped according to the following breakdown:

HPCS Injection

FTSI—HPCS pump failure to start, failure of the actuation circuit, valve failures (except for the injection valve and the valves in the suction transfer paths).

FTSV—Failure of the injection valve to open.

FTRT—Failure of the condensate storage tank suction MOV and check valve, suppression pool suction MOV and check valve, and associated level/actuation circuitry to realign suction sources from condensate storage tank to the suppression pool.

FTRI—HPCS pump failure to run and the failure of the associated room cooler/fan.

MOOSI—HPCS injection maintenance unavailability.

HPCS Emergency Power

FTSD—Failure to start of the emergency diesel generator and associated actuation circuitry.

FTSB—Failure of the Division III EDG output breaker to close.

FTRD—Failure of the Division III EDG to run and the HPCS dedicated service water cooling pump failure to start and run (River Bend and Nine Mile Pt. 2 service water failures were not included since they have no dedicated independent cooling water subsystem for HPCS).

MOOSD—HPCS emergency power (Division III) and dedicated service water cooling subsystem maintenance unavailability.

The majority of the PRA/IPEs stated that the failure of the minimum flow control valve to close would not affect rated flow to the reactor vessel either because of its small size and/or installed flow limiting orifices. Therefore, for these plants, the minimum flow valve failing to close was not included in the unreliability estimate.

While there are additional component failure modes in a given PRA/IPE for the HPCS system, the effect of not including these additional components in the system failure probability estimate is small.

River Bend and Nine Mile Pt. 2 have no independent HPCS dedicated service water system. The service water for cooling HPCS components at these plants is supplied by the main plant service water system. The HPCS unreliability estimates calculated from the PRA/IPEs do not include the contributions from the main service water system for River Bend and Nine Mile Pt. 2.

3.2.1 PRA Comparison Unreliability

The estimates of HPCS unreliability based on the 1987–1993 experience and the approximate PRA/IPE estimates are plotted in Figure 6 for comparison. The PRA/IPE estimates of HPCS unreliability range from about 0.07 to 0.15. The PRA/IPE estimates were calculated according to the mission times stated in the respective reports. The mission time for the HPCS system specified in all of the PRA/IPEs is 24 hours. The 1987–1993 experience estimates of unreliability were also based on this 24-hour mission time.

Based on the PRA/IPE data, the emergency power and injection subsystems contributed approximately 75% and 25%, respectively, to the overall HPCS system unreliability (industry average

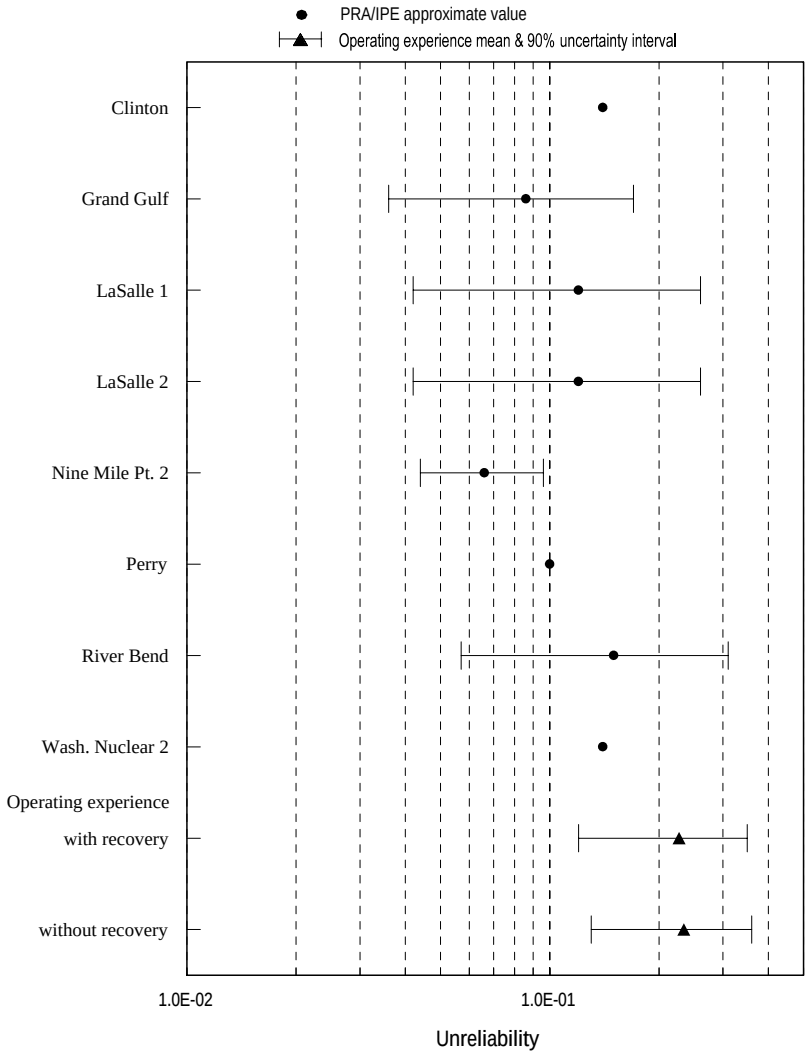


Figure 6. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience applies to all plants.)

estimates are presented in Table 6). These contributions are not consistent with the estimates computed from the 1987–1993 experience (see Table D-2 of Appendix D). The HPCS emergency power is the leading contributor to the HPCS system unreliability estimate based on the PRA/IPE estimates, while the injection subsystem is the leading contributor (roughly 60%) based on the 1987–1993 experience. While the unreliability estimates (PRA/IPE and 1987–1993 experience) for emergency power subsystem estimates tend to agree, the injection subsystem estimates differ by about a factor of five [0.03 (PRA/IPE) versus 0.14 (1987–1993 experience)].

The assumption of automatic transfer of HPCS suction from the CST to the suppression pool on low CST water level is based on the modeling information contained in the PRA/IPEs. However, recent information identifies the current operational alignment of HPCS suction for several plants to be different from what was initially modeled in the PRA/IPEs. HPCS suction was realigned (temporarily) from CST to suppression pool at Perry due to safety concerns over missiles resulting from tornadoes. At the LaSalle site, the HPCS suction was permanently (installed blank flange in CST suction to HPCS) shifted to the suppression pool due to biological concerns associated with the CST. The effect on HPCS unreliability of the realignment to the suppression pool at these plants is minimal. The fault models for the affected plants were quantified (using both IPE data and operational experience data) with suppression pool as the only suction source. The results of the requantification are: Perry—*initial value*: IPE 1.0E-01, 1987–1993 experience 2.3E-01; *suppression pool realignment*: IPE 9.7E-02, 1987–1993 experience 2.0E-01. LaSalle—*initial value*: IPE 1.2E-01, 1987–1993 experience 2.3E-01; *suppression pool realignment* IPE 1.0E-01, 1987–1993 experience 2.0E-01.

Figure 7 is a plot of the injection subsystem unreliability estimates computed from the PRA/IPEs and those calculated from the 1987–1993 experience. The difference in injection subsystem estimates is primarily attributed to the failure rates used in calculating the failure to run probability of the HPCS injection pump in the PRA/IPEs compared to the hourly rate calculated for this study (3E-5 versus 1.6E-3 per hour). Section 3.2.3 provides further insights on this failure mode.

Figure 8 is a similar plot of the emergency power subsystem of the HPCS with the exception of the recovery probability included for the EDG failure to run. The contribution of this subsystem to the overall HPCS unreliability is based on the offsite power to the Division III bus being unavailable (that is, a failure probability equal to one). The HPCS EDG (that is, Division III EDG) unreliability estimate (0.10) is a factor of two greater than the Division I and II EDG unreliability estimate (0.05) provided in an earlier system study report (Reference 10). Both estimates (Divisions I and II and Division III) are based on 1987–1993 experience and calculated for a 24-hour mission time. However, keep in mind that the HPCS EDG unreliability estimate is based on only three failures (one MOOS and two FTR), one of which (as discussed in Section 3.2) might not be totally applicable to most HPCS EDG designs in service today. The 90% uncertainty interval for the Division I and II EDG unreliability estimate is (0.016, 0.088).

Table 6. PRA/IPE average subsystem failure probability contribution to HPCS system unreliability. Estimates were derived from the failure information obtained from the PRA/IPEs and assuming that the offsite power to the Division III bus is not available.

	Failure Probability	Contribution (%)
HPCS injection	0.03	25
HPCS emergency power	0.09	75

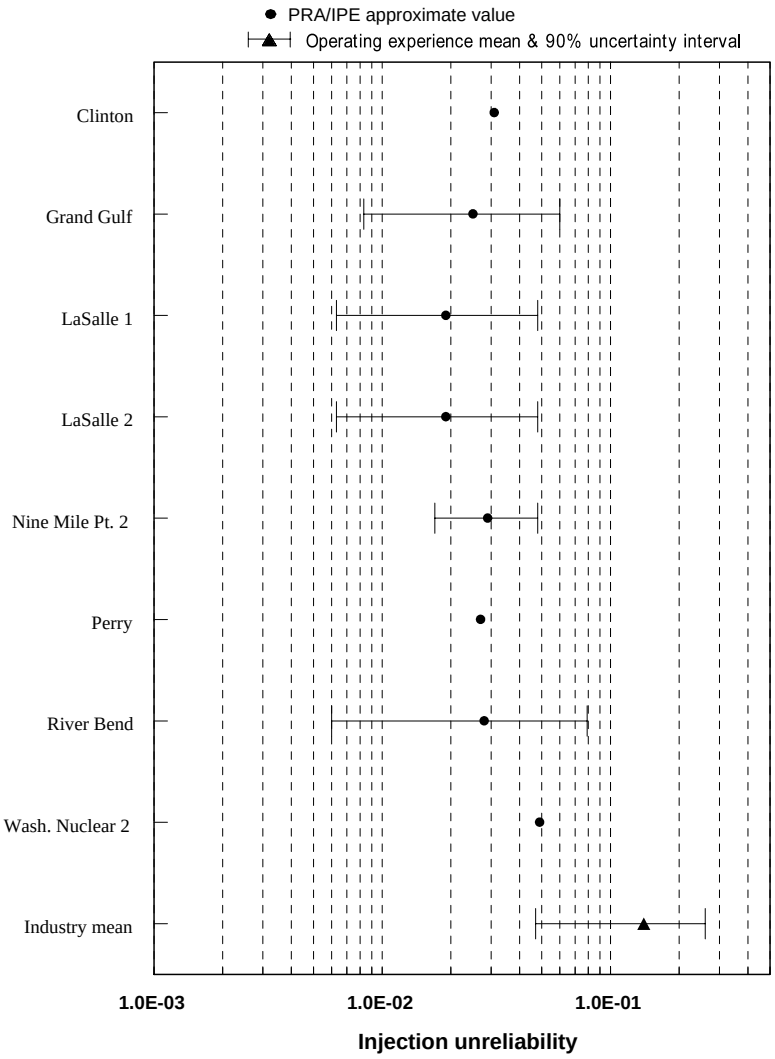


Figure 7. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS injection subsystem unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987-1993 experience applies to all plants.)

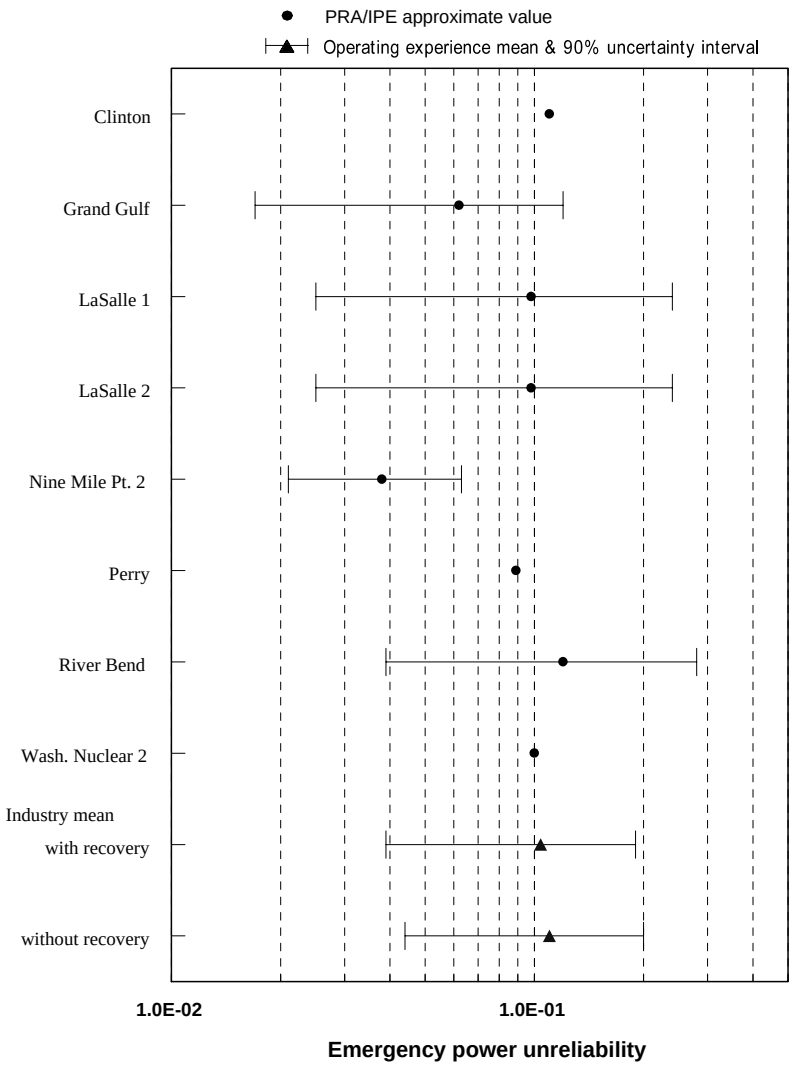


Figure 8. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS emergency power (Division III) unreliability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987-1993 experience applies to all plants.)

3.2.2 Failure to Start

HPCS Injection—As stated, failure to start was subdivided into two failure modes to use as much of the unplanned demand and test data as possible and to provide additional insight into the reliability of this phase of HPCS system operation. Figure 9 is a plot of the probability estimates of failure to start due to equipment failure other than the injection valve (FTSI) and failure to start due to injection valve failure (FTSV) calculated from the 1987–1993 experience and those based on the PRA/IPEs. The plant-specific probability of FTSI and FTSV estimated from the PRA/IPEs lie within the uncertainty bounds calculated from the 1987–1993 experience. The PRA/IPE estimates of FTSI have a tendency to be slightly larger than the mean probability based on the 1987–1993 experience, while the FTSV tend to be slightly smaller. The average FTSI probability for the PRA/IPEs is 8.6E-3 per demand, whereas the operational mean is 5.0E-3 per demand. Based on PRA/IPE estimates, FTSI is one of the largest contributors to

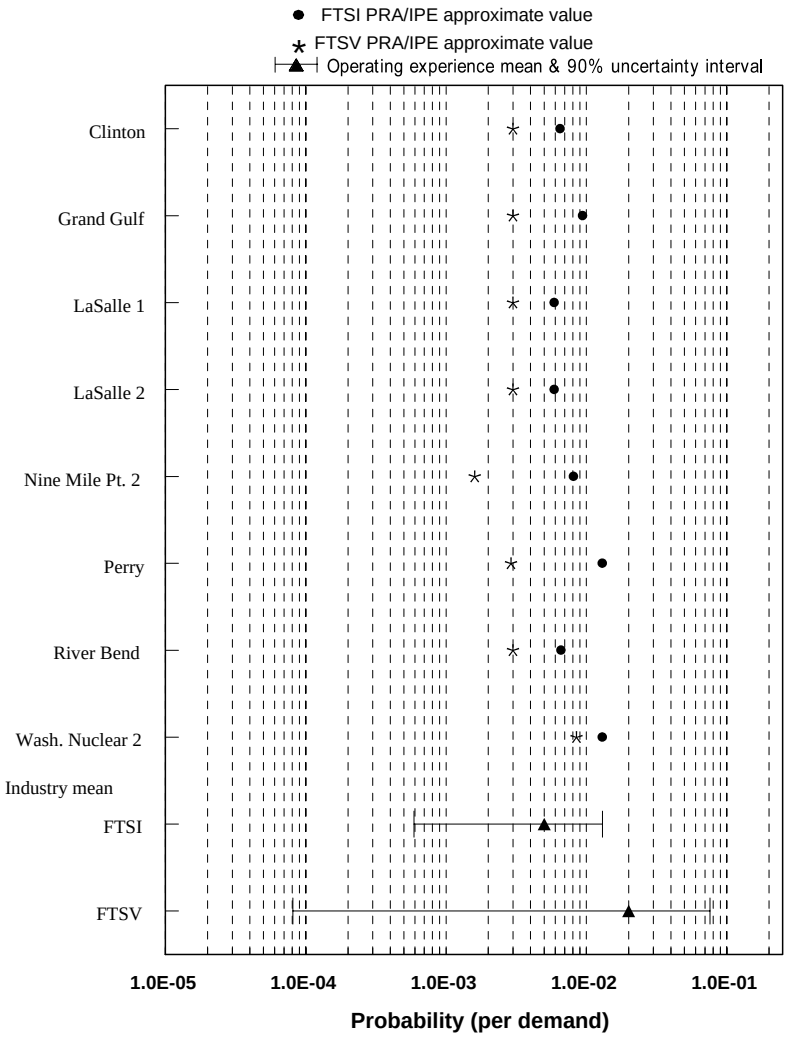
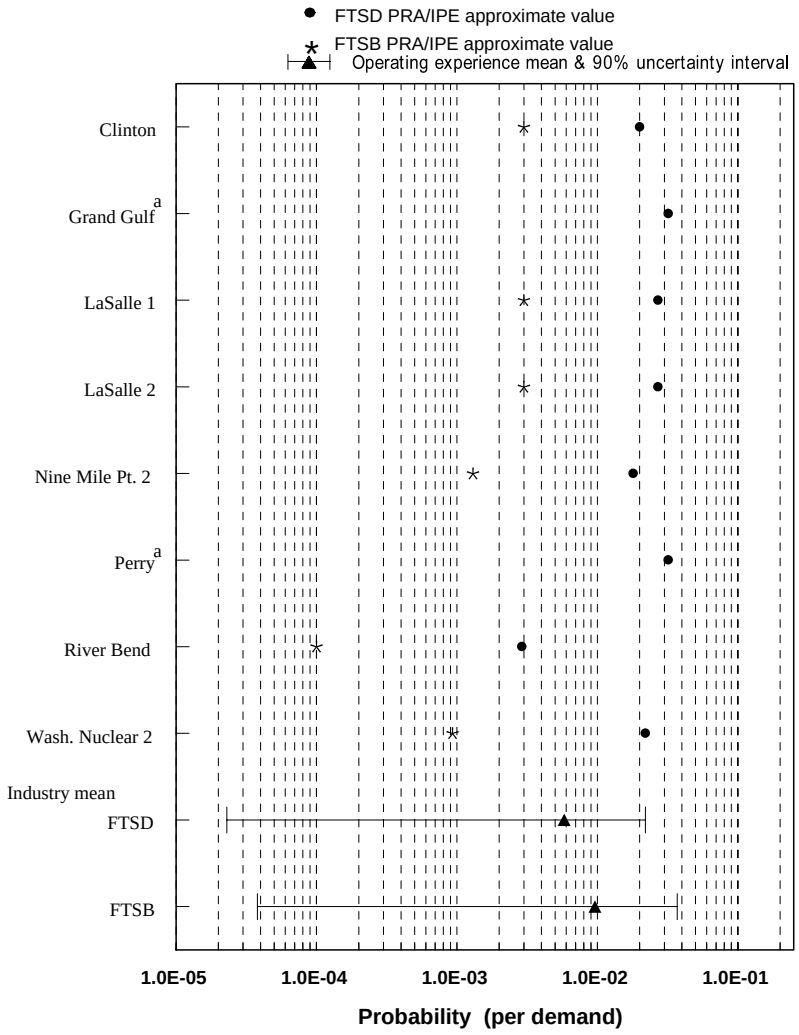


Figure 9. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS injection failure to start probability and uncertainties. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987-1993 experience applies to all plants.)

HPCS injection unreliability (approximately 30%). The range of the PRA/IPE values for FTSI is 5.9E-3 to 1.3E-2.

For the FTSV failure mode, the average of the PRA/IPE values is 3.5E-3 per demand (about 12% contribution to injection unreliability) compared to the mean estimate of 2.0E-2 per demand (14% contribution to injection unreliability) calculated from the 1987–1993 experience. The range of the PRA/IPE estimates for FTSV is 1.6E-3 to 8.5E-3 per demand.

HPCS Emergency Power—Failure to start of the HPCS emergency power subsystem was subdivided into two failure modes using similar reasoning as was applied to the HPCS injection model. Figure 10 is a plot of the probability estimates of failure to start of the emergency (Division III) diesel generator (FTSD) calculated from the 1987–1993 experience and those based on the PRA/IPEs. The



Note a. The FTSB value was not reported in the PRA/IPE.

Figure 10. Plot of the PRA/IPE and industry-wide (derived from the 1987-1993 experience) estimates of HPCS emergency power (Division III) failure to start probability and uncertainties. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience apply to all plants.)

average probability computed for FTSD based on the PRA/IPE estimates is 2.3E-2 per demand with a range of 2.9E-3 to 3.2E-2. Four of the eight plant-specific probabilities of FTSD estimated from the PRA/IPEs lie outside the upper 95th percentile of the distribution calculated from the 1987–1993 experience. The mean estimate calculated from the 1987–1993 experience is 5.8E-3.

The probability estimates of failure to start of the HPCS emergency power caused by the diesel generator output breaker faults (FTSB) are also shown in Figure 10. This component failure was not explicitly modeled/identified in the Grand Gulf or Perry IPE. Breaker failure may have been implicitly included in overall FTS probability for these plants. For the FTSB failure mode, the average of the PRA/IPE values is 1.9E-3 per demand compared to the mean estimate of 9.6E-3 per demand calculated from the 1987–1993 experience. The effect of FTSB on HPCS emergency power unreliability, based on the PRA/IPE estimates and 1987–1993 experience, is small (about 2% and 10%, respectively).

3.2.3 Failure to Run

HPCS Injection—As stated, failure to run was subdivided into two failure modes to use as much of the unplanned demand and test data as possible and to provide additional insight into the reliability of this operating phase of the HPCS system. Figure 11 presents a plot of these two failure modes for the 1987–1993 experience estimate and the PRA/IPE values. Overall, failure to run is one of the largest contributors (approximately 30%) to HPCS injection unreliability based on the PRA/IPE estimates. FTRI and FTRT contribute about 4% and 25%, respectively, to the HPCS injection unreliability based on PRA/IPE estimates. Based on the 1987–1993 experience, FTRI and FTRT contribute about 26% and 24%, respectively, to HPCS injection unreliability.

The PRA/IPE FTRI estimates are based on the HPCS motor-pump hourly failure rate for the individual plants. However, all but two of the plants used the Interim Reliability Evaluation Program (IREP) database for calculating the HPCS motor-pump failure probability. The mean failure rate specified in the IREP procedures guide is 3E-5 per hour. Nine Mile Pt. 2 and Washington Nuclear 2 specified that the Institute of Nuclear Power Operations' Nuclear Plant Reliability Data System (NPRDS) was the source of failure data used in estimating the component failure rates. The plant-specific estimates for the HPCS motor-pump failure rate at these two plants, based on NPRDS, are 5E-5 and 1.2E-5 per hour, respectively. However, the NPRDS results are generic (not HPCS system-specific) and for standby centrifugal pumps. The resultant average of the eight IPE estimates for HPCS motor-pump failure rate is 3E-5 per hour. The average of the PRA/IPE values differ by about a factor of 50, with the mean estimate calculated from the 1987–1993 experience, 3E-5 versus 1.6E-3 per hour, respectively. When comparing these values, be reminded that the 1987–1993 experience result of 1.6E-3 per hour is based on no failures in 316 operating hours. The limitations of the sparse data and short run times extracted from the 1987–1995 experience may be the reason for the discrepancy. The difference in results due to the FTR rates requires additional data to resolve the discrepancy. Given enough operating experience, the 1987–1993 experience based rate might be much closer to the PRA/IPE value. This is demonstrated by the wide uncertainty bands on the FTRI estimate shown in Figure 11, which encompass all of the PRA/IPE-based rates.

The average PRA/IPE estimate for the suction transfer failure mode (FTRT) is about 7.1E-3 per demand compared to the mean estimate of 3.4E-2 calculated from the 1987–1993 experience. While the plant-specific PRA/IPE estimates are smaller than the mean 1987–1993 experience estimate, all but one fall within the associated 1987–1993 experience uncertainty.

The other component failure accounted for in the FTRI mode was the HPCS room cooler fan. The failure rates identified in the PRA/IPEs for this component showed a little more variability than the HPCS motor-pump, though not enough to warrant explicit plotting of this estimate. The average hourly failure rate for the room cooler fan based on the PRA/IPE estimates is about 1.7E-5. Although this component was not explicitly modeled, the calculations include the contribution of the room cooler fan.

HPCS Emergency Power—Failure to run is the main contributor to HPCS emergency power unreliability, based on the PRA/IPE estimates, approximately 60%. For the 1987–1993 experience, this failure mode contributes only 43% of the HPCS emergency power unreliability.

The FTRD probability calculated from the PRA/IPEs include the HPCS-dedicated service water failure to start and run contribution to HPCS emergency power unreliability. The average hourly failure rate for FTRD based on PRA/IPE information is 2.3E-3 per hour, which is effectively identical to the 2.3E-3 calculated from the 1987–1993 experience. Figure 12 presents a plot of the FTRD estimates based on the PRA/IPEs and those calculated from the 1987–1993 experience.

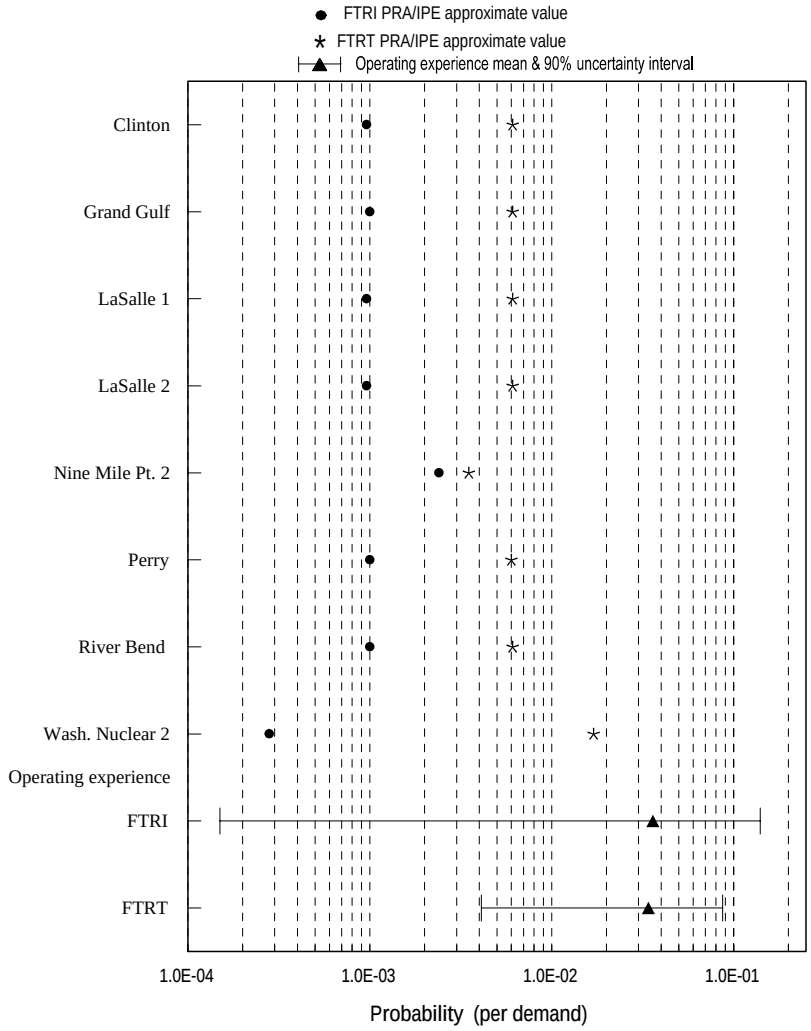


Figure 11. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS injection subsystem failure to run probability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience apply to all plants.)

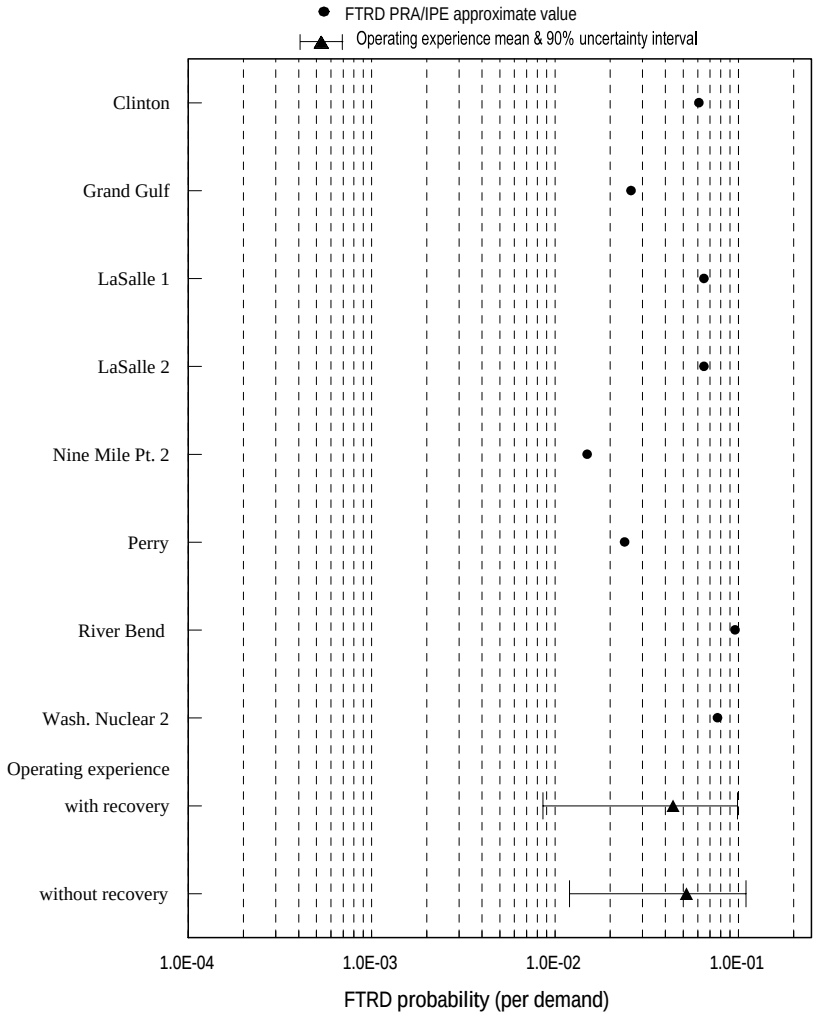


Figure 12. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS emergency power (Division III) diesel generator failure to run probability and uncertainties based on system operation for 24 hours. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience apply to all plants.)

3.2.4 Maintenance-Out-of-Service

In this study, maintenance unavailability is estimated using the failures and demands when the HPCS system was required to inject water into the reactor (that is, a reliability parameter). Risk analyses generally account for the MOOS probability as an unavailability estimate (that is, fraction of HPCS downtime compared to total plant operating time). In theory (that is, infinitely large sample), these two estimates should be equivalent. Since different calculation methods are used for computing maintenance unavailability, be cautious about making absolute comparisons of the PRA/IPE estimates and the 1987–1993 experience based estimates of MOOS unreliability.

HPCS Injection—The MOOSI contribution to HPCS injection unreliability is approximately 36% based on 1987–1993 experience compared to the 30% average contribution estimated from the PRA/IPEs. Figure 13 displays and compares the PRA/IPE estimates for maintenance-out-of-service for the injection

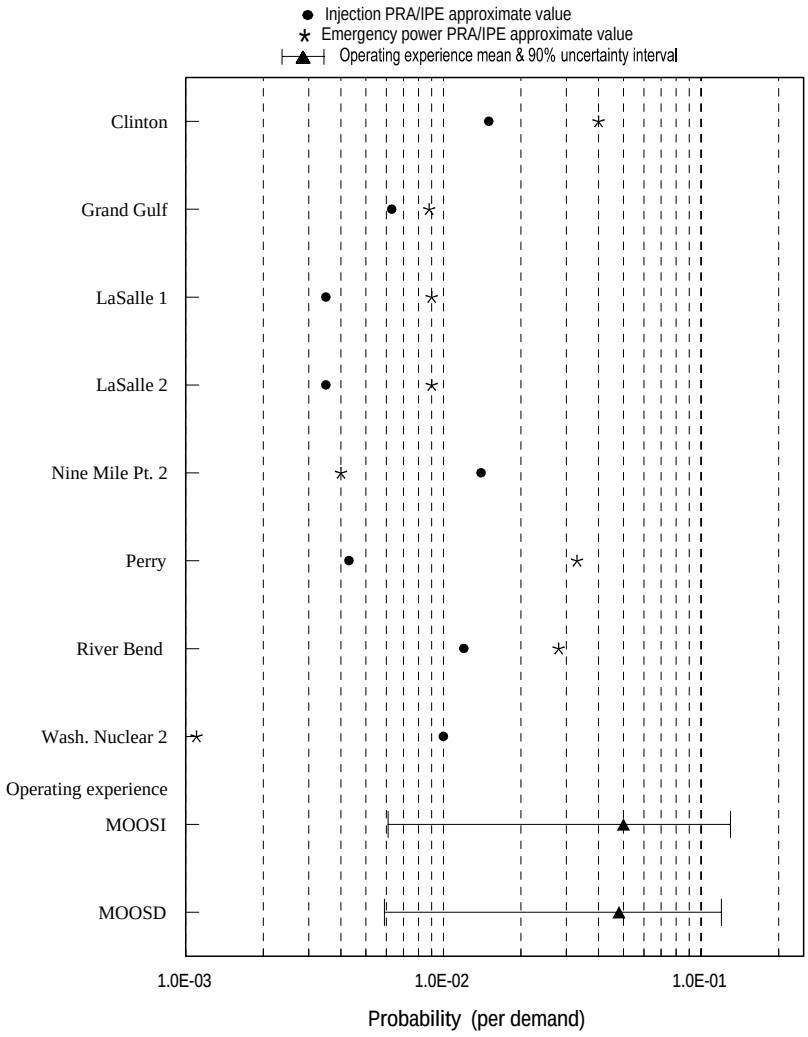


Figure 13. Plot of the PRA/IPE and industry-wide (derived from the 1987–1993 experience) estimates of HPCS injection and emergency power (Division III) diesel generator maintenance-out-of-service probability and uncertainties. (No plant-to-plant variation was observed in the 1987–1993 experience; therefore, the industry mean and uncertainty derived from the 1987–1993 experience applies to all plants.).

subsystem to the mean estimate and associated uncertainty calculated from the 1987–1993 experience. The range of maintenance estimates found in the PRA/IPEs is approximately 3.5E-3 to 1.5E-2 per demand with an average value of 8.6E-3. Comparing this range of values to the uncertainty interval for the MOOSI failure probability reveals three plants below the lower 5% uncertainty bound.

HPCS Emergency Power—The average of the PRA/IPE estimates for MOOSD is about 1.7E-2 per demand (approximately 19% contribution to the overall HPCS EDG unreliability) with a corresponding range of estimates of 1.1E-3 to 4.0E-2. The 1987–1993 experience estimate (4.8E-2 per demand) is about a factor of three greater than the PRA/IPE average value.

For reasons stated earlier in Section 3.1, the maintenance contribution of HPCS-dedicated service water subsystem is modeled implicitly as part of the HPCS emergency power maintenance-out-of-service

calculation. Even though the maintenance unavailability estimates for the HPCS-dedicated service water were available in the PRA/IPEs, these were included in the MOOSD estimates. Based on the PRA/IPE estimates for service water maintenance, the average of these estimates is about 4.7E-3. The range of the PRA/IPE plant-specific estimates is 2.3E-4 to 9.6E-3. Maintenance contributes about 47% to the HPCS-dedicated service water subsystem unreliability based on the PRA/IPE estimates. The HPCS-dedicated service water maintenance contribution calculated from the PRA/IPE information is approximately 5% of the HPCS emergency power unreliability.

The estimate of maintenance-out-of-service unreliability for the Division I and II EDG is 3.1E-2 per demand with an associated 90% uncertainty interval of 9.7E-3 to 6.2E-2 (see Reference 10). The maintenance-out-of-service unreliability for the Division III EDG is about 50% larger than the estimate for the Division I and II EDGs. Reference 10 further identifies the average value for maintenance-out-of-service unreliability based on PRA/IPE information for the Division I and II EDG as 2.1E-2 per demand.

4. ENGINEERING ANALYSIS OF THE OPERATIONAL DATA

This section documents the results of an engineering evaluation of the HPCS operational data derived from LERs and the Accident Sequence Precursor (ASP) database. The objective of this analysis was to analyze the data and obtain insight into the performance of the HPCS system throughout the industry and at a plant-specific level. Unlike the PRA analysis presented in Section 3, all LERs submitted during the evaluation period and the ASP events that mentioned the HPCS system were considered as part of this analysis; no data were excluded. The results of the operational data review are as follows:

- There were no statistically significant trends in the frequency of failures or the frequency of unplanned demands of the HPCS system over the study period.

- There were only two failures of the system to respond as designed during unplanned demands. Both were classified as failures to run of the emergency power subsystem. One failure was the result of a vibration-induced leak in the fuel oil line for the diesel; the other was a loss of cooling water to the diesel during a sequential loss of offsite power.

- The injection subsystem accounted for 63% (10 of 16) of the total number of failures, with the emergency power subsystem accounting for 25% (4 of 16) and the service water subsystem accounting for 12% (2 of 16).

    - Malfunctions associated with motor-operated valves accounted for half of the injection subsystem failures, which is approximately one-third of all failures. Because of the limited data, no other component was considered a significant contributor to the total number of failures.

    - The cause of the failures observed in the operational data was approximately evenly distributed between hardware-related malfunctions and personnel error.

    - The classification of the failures was approximately evenly distributed between failures to start and failures to run.

    - There were 14 of 16 failures observed other than during an unplanned demand, half of which were discovered during routine surveillance testing.

- There was no correlation observed between the plant-specific frequency of failures and low-power license date. The average frequency of failures was 0.29 failures per plant operating year. The frequency was based on an average of two failures per plant over the study period and varied from a low of one to a high of three failures per plant over the study period.

The following subsections present a comprehensive summary of the industry data supporting the above results and additional insights derived from (a) an assessment of the operational data for trends and patterns in system performance across the industry and at specific plants, (b) identification of the subsystems and causes that contribute to the system failures, (c) evaluation of the relationship between system failures and low-power license date, and (d) Accident Sequence Precursor events involving the HPCS system.

4.1 Industry-wide Evaluation

4.1.1 Trends by Year

Table 7 presents the HPCS system inoperabilities, faults, failures, and unplanned demands that occurred in the industry for each year of the study period. The number of unplanned demand events shown in Table 7 is the number of events in which the HPCS diesel generator, injection pump, and discharge valve were demanded, specifically events that required HPCS spray flow to the RPV. Figures 14 and 15 are illustrations of unplanned demand and failure frequencies for each year of the study with 90% uncertainty intervals. The figures include fitted trend lines and 90% confidence bands for the fitted trends. The frequency is the number of events (unplanned demands or failures) that occurred in the specific year divided by the total number of plant operational years for the specific year. (Total plant operational years was eight for each year of the study.)

Analysis of the unplanned demand and failure frequencies for trends showed no statistically significant trends over the past 7 years. The P-values of the fitted trend lines are 0.18 and 0.54 respectively.

Although, unplanned demands appear to be decreasing; the data are sparse enough that confidence in this trend is not high. More data (that is, years of operating experience) are needed before this trend can be verified or disproved.

4.1.2 Factors Affecting HPCS Reliability

The HPCS system failures and faults were reviewed to determine the factors affecting overall system reliability. The faults that were observed in the HPCS system generally are not risk-significant; therefore, this section focuses only on the failures. To direct the review, the system failures were partitioned by method of discovery for each subsystem and component within each subsystem. The methods of discovery are unplanned demands, surveillance tests (all types and frequencies), and other. The other category includes failures found from design reviews, walkdowns, control room annunicators and indications, plant tours, etc. The results of this data partition are presented in Tables 8 and 9.

Table 7. Number of HPCS events by category for each year[a] of the study.

Classification	1987	1988	1989	1990	1991	1992	1993	Total
Inoperabilities	3	8	14	12	6	8	6	57
Faults	3	6	11	9	5	5	2	41
Failures[b]	0	2	3	3	1	3	4	16
Unplanned demands	5	7	1	3	4	1	2	23

a. Each entry consists of the number of events that occurred in that calendar year.

b. Excludes the four MOOS events observed during unplanned demands.

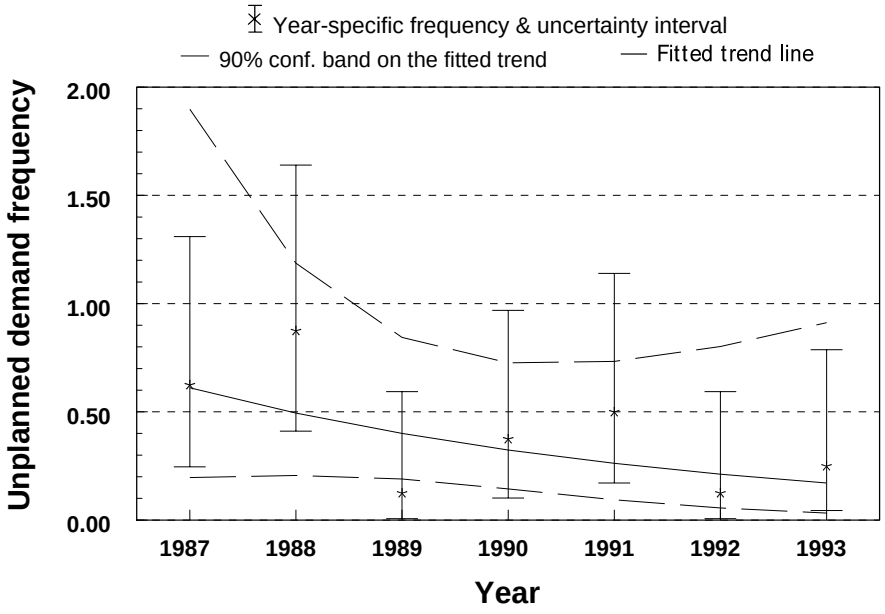


Figure 14. HPCS unplanned demand events per year, with 90% uncertainty intervals and confidence band on the fitted trend. Although a decreasing trend is visible, it is not statistically significant (P-value = 0.18)

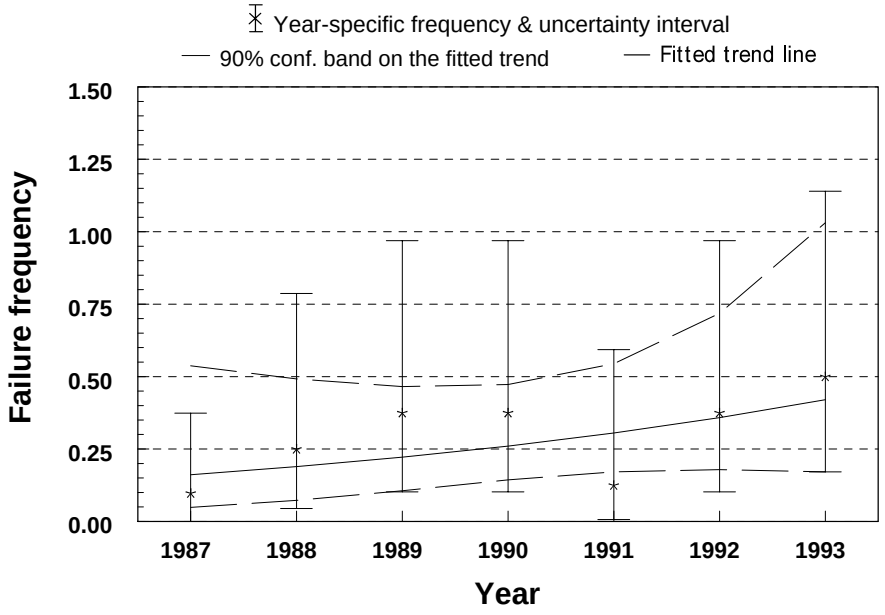


Figure 15. HPCS failure events per year, with 90% uncertainty intervals and confidence band on the fitted trend. The trend is not statistically significant (P-value = 0.54)

Table 8. Subsystem contribution to HPCS system failures, by method of discovery.

	Method of Discovery		
Subsystem	Unplanned Demand	Surveillance Test	Other
Injection	—[a]	4	6
Emergency power	2[b]	1	1
HPCS service water	—	2	—
Total	2	7	7

a. Excludes the one MOOS event associated with the injection pump during power operations.

b. Excludes the two MOOS events associated with the diesel generator when the plant was shut down, and one MOOS event during power operations.

Table 9. Component contribution to HPCS system failures, by method of discovery.

	Method of Discovery		
Subsystem Component	Unplanned Demand	Surveillance Test	Other
Injection			
Motor-pump	—	2	1
MOV	—	2	3
Other	—	—	2
Emergency power			
Governor/Fuel	1	1	—
Stator	—	—	1
Engine cooling	1	—	—
HPCS service water			
Pump	—	1	—
Other	—	1	—

As indicated in Tables 8 and 9, the failures that occurred in the HPCS system were distributed throughout the three subsystems. There were only two unplanned demand failures, and the remaining 14 failures were observed equally during surveillance tests and the other category. Considering that there were only 16 failures observed throughout the study period, it is not unusual to have the failures distributed in this manner. The injection subsystem accounted for 63% (10 of 16) of the total number of failures, with the emergency power subsystem accounting for 25% (4 of 16), and the service water subsystem accounting for 12% (2 of 16). Malfunctions associated with motor-operated valves accounted for half of the injection subsystem failures, which is approximately one-third of all failures. Because of

the limited data, no other component can be considered a significant contributor to the total number of failures.

Factors Affecting Unplanned Demand Reliability—There were four failures observed during unplanned demands that directly contributed to HPCS unreliability; two were classified as MOOS events and two as failure to run. The MOOS events were associated with the emergency power and injection subsystems. The FTR events occurred in the emergency power subsystem and were associated with the diesel generator. In addition, two other emergency power subsystem MOOS events were observed in the operational data; however, they were excluded from the unreliability estimates presented in Section 3 because they occurred during shutdown conditions.

The injection subsystem MOOS event was observed during an automatic reactor scram that resulted from a reactor vessel low water level condition caused by a loss of all operating feedwater pumps. The reactor core isolation cooling system automatically started to restore RPV level. The HPCS system was not available because it had been previously removed from service for preplanned maintenance. The emergency power subsystem MOOS event occurred when the HPCS diesel was out of service for maintenance and the fire deluge system for the system auxiliary transformer inadvertently actuated. The transformer was automatically isolated as a result of a subsequent fault. The fault on the transformer resulted in a loss of power to Division III electrical buses and a need for the diesel generator to provide power. The LERs did not specify the type of preplanned maintenance being performed on the system (that is, surveillance test or other).

The two diesel generator failures to run involved a fuel system leak and a loss of cooling water flow to the engine. The fuel oil leak occurred when the HPCS diesel was started to power the Division III electrical bus following a loss of power to the bus because of a failed transformer. Repairs to the transformer required that the transformer remain de-energized for over two days. The HPCS diesel provided power to the bus for approximately 48 hours when a fuel oil leak developed on two fuel oil instrument lines as a result of vibration. The diesel was shut down and the instrument lines plugged by maintenance personnel. The diesel was returned to service after the repairs.

The second diesel generator FTR event was the result of a loss of cooling water flow during a sequential loss of offsite power. The diesel was not recovered during the event. The cooling water failure was caused by a design error. As originally designed, the cooling water supply isolation valve closed as a result of low flow in the supply header. Closure of the valve on low flow was a design function to mitigate service water loss on a postulated service water header leak. The low flow was a result of the loss of one division of offsite power (and corresponding shutdown of that division's service water pumps). Because power was not restored within the time delay associated with the closure circuitry, the valve closed and remained closed. The second service water supply valve to the diesel remained open as a result of power available to the other division's service water pumps. When the second offsite power line was lost a few minutes later, the remaining division's service water pumps tripped and the other cooling water supply valve closed on low flow. This second supply valve closure resulted in the HPCS diesel supplying power to the Division III bus with no cooling water flow. The diesel overheated and tripped several minutes later. Because the loss of Division I and II power occurred sequentially, the cooling water supply valves to the Division III diesel would not automatically reopen. The design was changed to allow multiple automatic recoveries during sequential loss of offsite power events. This failure mechanism is unique to the plant (that is, not representative of the eight BWR plant designs), and the design was changed to preclude this type of failure in the future.

Factors Affecting Reliability During Surveillance Tests—During the performance of surveillance tests, there were two failures that contributed to the unreliability estimates presented in

Section 3. Both failures were observed in the injection subsystem; one failure was a failure of the injection pump to start; the other was a failure of the suction source to transfer function.

The failure to start of the injection pump that contributed to the system unreliability estimate was the result of a failed over-frequency relay. During the performance of a surveillance test, the coolant injection pump would not start as required. Investigation by plant personnel revealed that the over-frequency relay would consistently trip at a lower frequency value than its design setpoint, indicating relay failure as the root cause of the failure to start. The relay was replaced, and the injection pump was successfully started and operability verified.

The failure of the suction source transfer function that contributed to the unreliability estimate was the result of the HPCS suction valve from the suppression pool failing to open during the performance of a cyclic surveillance test. Upon investigation by plant personnel, the motor was found running; however, the valve was not moving. Plant personnel also heard a gear-grinding noise coming from the motor-operator gear box. The motor operator was replaced. The cause identified in the LER was a failure of the manufacturer to build the operator per design.

Other Surveillance Test Failures—Five other failures were observed during surveillance tests; however, these were not used to estimate system reliability because the periodicity of the surveillance test was unknown or the number of tests could not be reasonably estimated from the data available for the study. These five surveillance test failures were observed in each of the three HPCS subsystems; two were observed in the injection subsystem, two in the HPCS service water subsystem, and one in the emergency power subsystem. Three of the failures were classified as failures to start, the other two as failures to run.

Of the two failures observed in the injection subsystem, one was classified as a failure to start and the other as a failure to run. The failure to start event was the result of a motor-operated valve failing to open. The valve failed to open because the valve disc and disc nut had separated from the stem. This caused an over-thrust condition that subsequently caused the cast carbon steel yoke to crack 360 degrees circumferentially in the necked transition region of the yoke's bonnet flange and the yoke body. The failure to run event was a result of a personnel error associated with the injection pump motor. The personnel error was the result of poor maintenance practices that caused the weakening of an air deflector inside the motor stator. The air deflector subsequently broke and became lodged in the motor stator.

There were two surveillance test failures observed in the HPCS service water subsystem; one was classified as a failure to start and the other as a failure to run. The failure to start event was the result of personnel error. The operator when starting the diesel generator inadvertently lowered engine speed below the setpoint for the automatic shutdown of the service water pump, resulting in the pump tripping. When the operator subsequently raised engine speed, the service water pump received a second start signal. However, because the pump was still coasting down, excessive starting current caused the breaker for the cooling water pump to trip on magnetic overload. The operator, realizing the diesel was running without cooling water, shut down the engine. The second event, a failure to run event, was the result of a hardware-related failure associated with the pump motor. The motor failed as a result of a phase-to-phase ground caused by stator end winding movement during motor startups.

The emergency power subsystem failure to start event was the result of a failed droop switch in the governor. The failed droop switch caused the generator output breaker to trip on reverse power while trying to load the diesel during a surveillance test. The faulty droop switch caused an electrical load instability while the unit was synchronized with the grid. While this type of failure mechanism would be bypassed during a loss of offsite power start of the diesel, subsequent restoration of Division III power

using offsite power would be disrupted by this failure mechanism. In this situation, the ability of the diesel to run would be affected.

Other Factors Affecting Reliability—There were seven failures discovered by methods other than surveillance testing or unplanned demands. Six were associated with the injection subsystem and the other with the emergency power subsystem. Of the six injection subsystem failures, three affected the ability of the system to run, two were related to the suction source transfer function, and one affected the ability of the system to start. The single emergency power subsystem failure affected the ability of the diesel to start.

Two of the failures to run of the injection substem were the result of personnel error; the other failure to run was a hardware-related failure. One of the personnel error-related failures was the result of plant operators inadvertently disabling the auto-start function of the dedicated HPCS room cooling fan (HVAC). The failure of HVAC does not affect the auto-start of the HPCS injection function; however, analysis of the event by the plant personnel indicated that the injection pump would not run for a prolonged period of time. The other personnel error-related failure was the result of operators over-torquing a motor-operated valve; such that the valve would not function properly. The hardware-related failure to run event was the result of an injection pump motor bearing oil plug thread failure as a result of normal operation, allowing oil to leak out of the bearing. The design was changed so that the plug would not be operated as frequently.

The two failures of the suction source transfer function were associated with the suppression pool suction motor-operated valve. In one case, the suppression pool suction valve failed to open during a routine plant evolution. The cause was a torque switch setting that was too sensitive to jarring during initial valve operation. The torque switch was adjusted to fix the problem. The other suppression suction pool valve failure was the result of plant operators inadvertently disabling the operation of the valve.

The event classified as an injection subsystem failure to start was the result of an operator inadvertently isolating one channel of the low-level instrumentation while a second channel had a leaking equalizing valve. With both channels of the low level instrumentation inoperable, the auto-start of the system on low RPV level was rendered inoperable.

The failure of the emergency power subsystem to start was the result of the spurious out-of-phase closure of the auxiliary transformer feed breaker while attempting to parallel the diesel to the Division III electrical bus. The closure of the feed breaker caused winding damage to the generator. The entire generator was replaced because the effects of the winding damage could not be fully determined.

4.2 Plant-specific Evaluation

Table 10 presents the following information for each plant: operating years during the study period, number of faults, the number of failures, the number of unplanned demands, and the frequency of faults, failures, and unplanned demands. As used here, a *frequency* is simply an event count divided by the number of operating years.

The unplanned demand and failure frequencies are plotted in Figures 16 and 17, respectively. To account for plants with no failures or unplanned demands, Bayes statistical techniques were used to estimate the failure and unplanned demand frequencies shown in the figures. In each plot, the plant-specific point estimate is shown with the 90% uncertainty interval.

Table 10. HPCS faults, failures, and demands differentiated by plant (excludes the MOOS events).

Plant Name	Operating Years	Number of Faults	Fault Frequency	Number of Failures	Failure Frequency	Number of Unplanned Demands	Unplanned Demand Frequency
Clinton	7	5	0.71	1	0.14	1	0.14
Grand Gulf	7	3	0.43	3	0.43	7	1.00
LaSalle 1	7	5	0.71	1	0.14	0	0.00
LaSalle 2	7	5	0.71	2	0.29	0	0.00
Nine Mile Pt. 2	7	3	0.43	1	0.14	5	0.71
Perry	7	7	1.00	3	0.43	6	0.86
River Bend	7	1	0.14	2	0.29	2	0.29
Wash. Nuclear 2	7	12	1.71	3	0.43	2	0.29
Industry	56	41	0.73	16	0.29	23	0.41

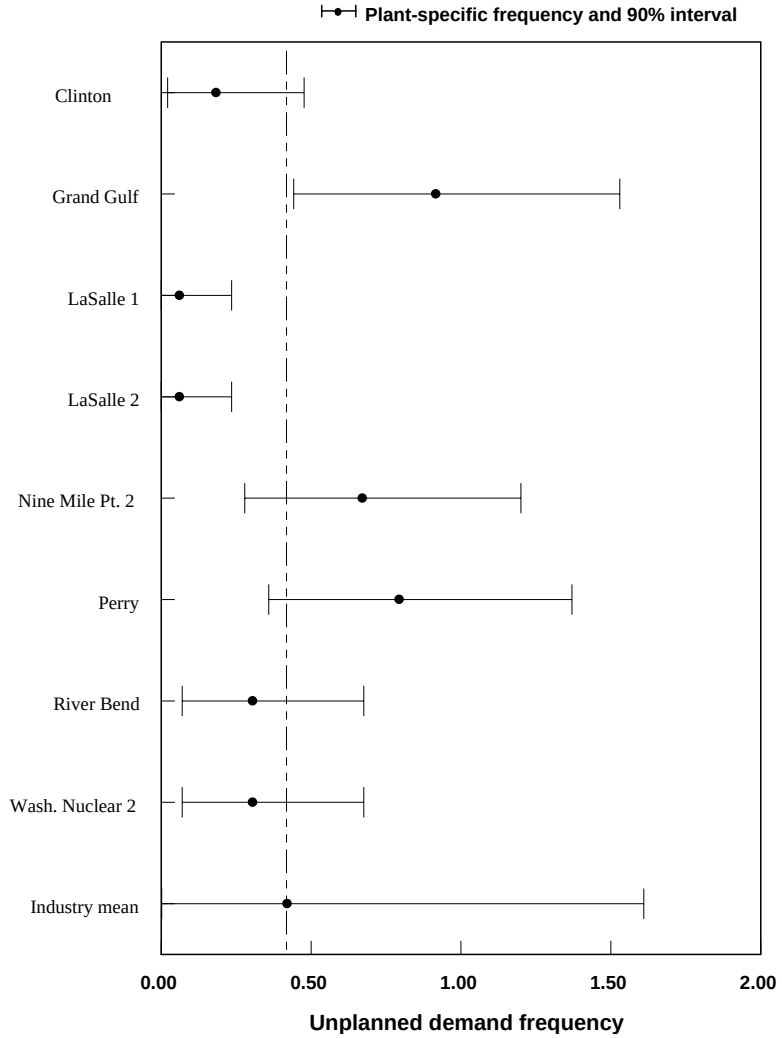


Figure 16. Plant-specific unplanned demand frequencies with 90% uncertainty intervals.

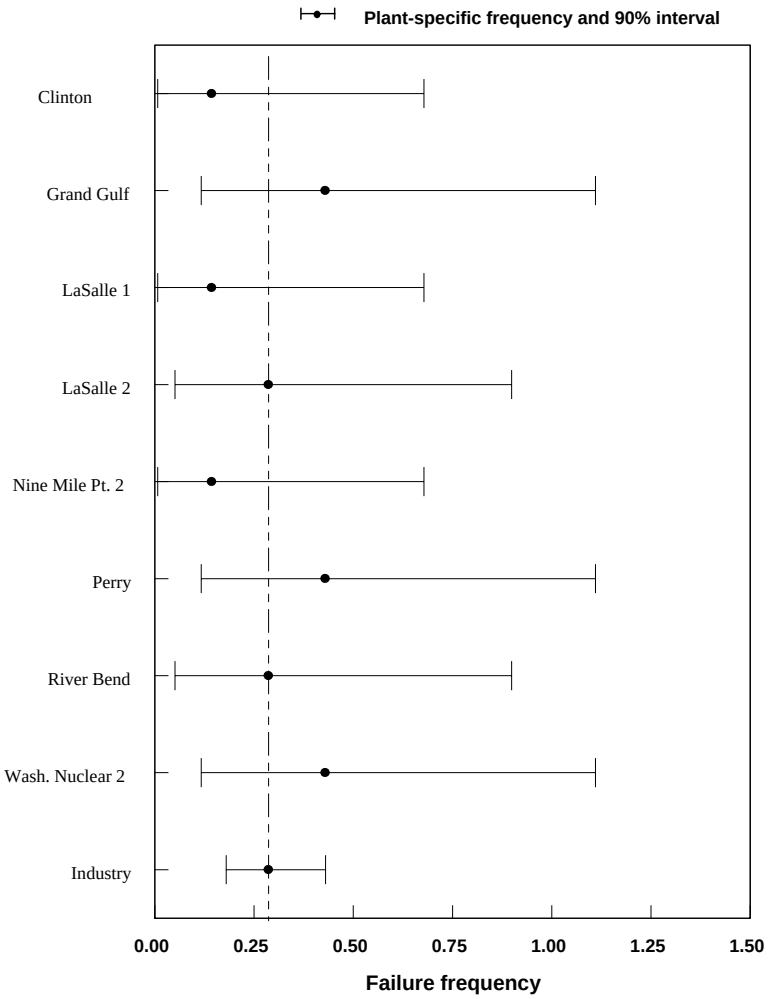


Figure 17. Plant-specific failure frequencies with 90% uncertainty intervals.

Because the plants with high failure frequencies do not necessarily have high unplanned demand frequencies, Figure 18 shows the two frequencies used in Figures 16 and 17 plotted on the two axes of one graph. The points are labeled with the plant name. Any point in the upper right of the graph corresponds to a plant with both a high failure frequency and a high frequency of unplanned demands. Based on the data displayed in Figure 17, four plants were selected for detailed review of their failure and unplanned demand data: Grand Gulf, Nine Mile Pt. 2, Perry, and Washington Nuclear 2.

Compare the individual plant data with the reliability estimates provided in Section 3 with caution. Plant-specific estimates derived solely from the failure and demand data at a particular plant may produce results that differ from those presented in Section 3. There are several reasons for this, two of which are the sparse number of data associated with HPCS system performance at individual plants and the ability to recover from HPCS system failures. However, sparse data alone do not create differences between the best estimates of unreliability presented in Section 3 (which are calculated using Bayesian statistics) and what can be calculated if only the individual plant data were used (that is, using classical statistics). Sparse data provide the opportunity for rare or atypical performance to overly influence any unreliability estimate that is based solely on the plant-specific data. (Note that in the long run, the atypically high reliability performance will be balanced out by atypical low reliability. *Sparse data* is

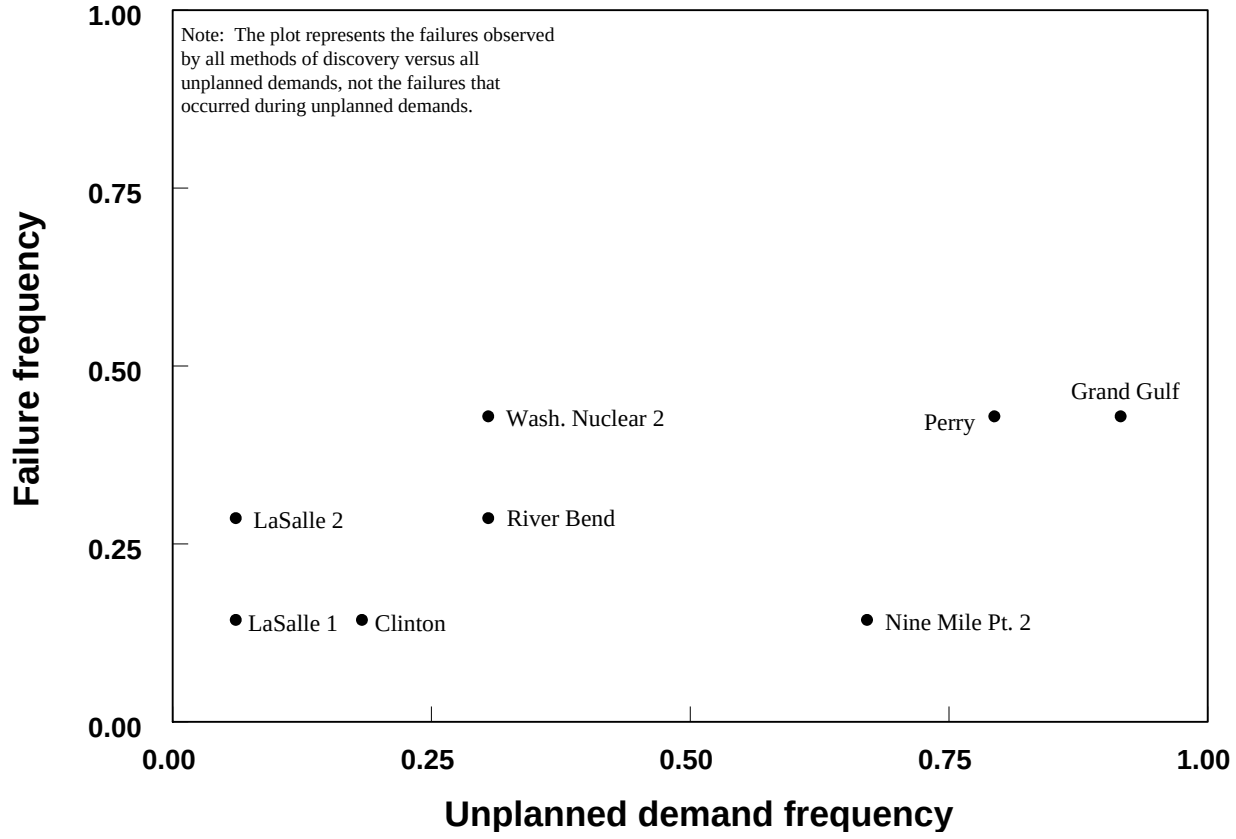


Figure 18. Plant-specific unplanned demand frequency versus plant-specific failure frequency.

defined such that the HPCS system experience is not sufficient to allow the data to converge on the true unreliability.) These atypical data can result in the unreliability estimate either overpredicting or underpredicting the true unreliability of the HPCS system. Of course, it is impossible to determine absolutely whether or not the sparse data are atypical of the true system performance; maybe the system really is as reliable or as unreliable as the data suggest. Nevertheless, to minimize the chance of producing nonrepresentative estimates based on sparse data, the best estimates presented in Section 3 are calculated using Bayesian statistics that use all knowledge of HPCS performance across the industry.

The second issue to consider when reviewing the individual plant experience is the possibility of recovering from an HPCS system failure. Industry-wide, there were two opportunities in which plant personnel, due to circumstances of the particular events, made an effort to recover the HPCS system from the failure. In neither instance was the recovery successful. The unreliability estimates presented in Section 3 include the likelihood that the failure events will be successfully recovered, whereas the results of individual plant-specific comparisons presented in Section 4 do not necessarily include consideration of recovery.

Grand Gulf—Grand Gulf experienced three failures and seven unplanned demands during the study period. The failures were all unrelated and did not contribute to the unreliability estimates presented previously in Section 3. Two of the failures were the result of hardware-related problems that occurred in 1993, and the other was the result of a personnel error that occurred in 1988. Two of the failures were observed in the injection subsystem and the other in the HPCS service water subsystem. The seven

unplanned demands occurred following critical reactor scrams and were distributed throughout the study period.

Nine Mile Pt. 2—Nine Mile Pt. 2 experienced one failure and five unplanned demands during the study period. The failure was a diesel generator FTR event that was the result of a loss of cooling water flow during a sequential loss of offsite power. The diesel was not recovered during the event. The cooling water failure was caused by a design error in the operation of the two cooling water supply valves from Division I and II service water headers. The design was changed to allow multiple automatic recoveries during sequential loss of offsite power events. Three of the five unplanned demands occurred in 1988, the other two in 1989 and 1991, respectively. The demands were following critical reactor scrams.

Perry—Perry experienced four failures (includes one MOOS event not counted in Table 10) and six unplanned demands during the study period. The MOOS event was attributed to injection subsystem pre-planned maintenance. The three other failures were discovered other than during a surveillance test or unplanned demand. One failure was a hardware-related failure to run event that was the result of an injection pump motor bearing oil plug thread failure resulting from normal operation and allowing oil to leak out of the bearing. The design was changed so that the plug would not be operated as frequently, hopefully reducing the likelihood of a reoccurrence of this failure. The second failure was associated with the suction source transfer function. The suppression pool suction valve failed to open during a routine plant evolution. The cause was a torque switch setting that was too sensitive to jarring during initial valve operation. The third failure was the result of an operator inadvertently isolating one channel of the low-level instrumentation while a second channel had a leaking equalizing valve. All of the failures observed at Perry were distributed throughout the study period. The unplanned demands observed at Perry were also distributed throughout the study period.

Washington Nuclear 2—Washington Nuclear 2 experienced five failures (includes two MOOS events during shutdown operations not counted in Table 10) and two unplanned demands during the study period. The two shutdown MOOS events were associated with emergency power subsystem preplanned maintenance. The three other failures were discovered during surveillance testing and were all unrelated. Two failures were associated with the injection subsystem, the other with the emergency power subsystem. One failure occurred during a cyclic surveillance test and was the result of the suppression pool suction valve failing to open. Plant personnel found the motor turning, yet the valve stem was not. They also heard a gear-grinding noise coming from the motor-operator gear box. The motor-operator was replaced. The cause identified in the LER was a failure of the manufacturer to build the operator per design. The other injection subsystem failure was a result of the air deflector failing and becoming lodged in the pump motor stator. The cause identified in the LER was improper work practices. The emergency power subsystem failure was the result of a failed droop switch for the diesel governor. The two unplanned demands occurred in 1988 and 1991 and followed critical reactor scrams caused by feedwater and RPV level control problems.

4.3 Evaluation of HPCS Failures Based on Low-power License Date

To determine if the age of the plant affects HPCS performance, a trend of plant-specific failures per operational year were plotted against the plant low-power license date. The failure frequency for a plant was estimated as the number of failures divided by the number of plant operational years, with plant operational years estimated as described in Section A-1.3 of Appendix A. The frequencies and 90% Bayesian intervals are plotted in Figure 19. A fitted trend line and 90% confidence band on the fitted line are also shown in the figure. The trend is not statistically significant (P-value = 0.55).

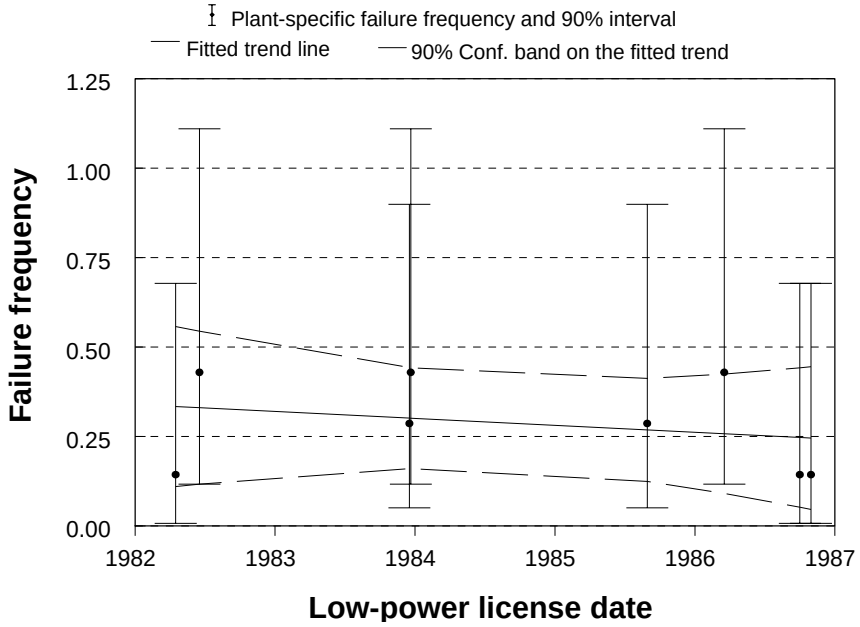


Figure 19. Plant-specific HPCS system failures per operating year, plotted against low-power license date. Ninety-percent Bayesian intervals and a fitted trend are included. The trend is not statistically significant (P-value = 0.55).

A similar plot was made previously using unreliability (Figure 5). The conclusion is the same for both plots. The trends are not statistically significant.

4.4 Accident Sequence Precursor Review

The events identified by the ASP Program (NUREG/CR-4674) were reviewed. The purpose of this review was to relate the operational data to the types of events that resulted in a conditional core damage probability (CCDP) of greater than 1.0E-6. The search for ASP events was limited to the 1987–1993 study period and included all ASP events in which the HPCS system was identified in the ASP database.

The search resulted in the identification of 12 events related to the HPCS system. Of these 12 events, only five involved an HPCS system actuation, two were partial demands, and the other three demands resulted in coolant injection to the reactor vessel. There were no HPCS failures identified in the ASP events. The ASP events that identified an HPCS unplanned demand are listed in Table 11. The seven remaining ASP events only mention that the HPCS system was available if required. Four of these seven events involved the unavailability of both the Division 1 and 2 emergency diesel generators but included a statement that the HPCS diesel was available. The other three events were not related to the HPCS system.

The ASP events that identified an HPCS demand had a CCDP that ranged from 1.2E-6 to 6.6E-6. Three of the ASP events indicated that the HPCS system was demanded to restore RPV level as a result of a loss of normal feedwater flow.

Table 11. List of the ASP events that identified an HPCS unplanned demand.

Plant Name	LER Number	Event Date	CCDP	Description
Grand Gulf	41689016	12/06/89	1.2E-6	A partial demand occurred on a momentary low-level spike, but the system did not inject coolant to the RPV.
LaSalle 1	37393015	09/14/93	1.3E-4	The HPCS EDG started on a loss of power, but the HPCS injection function was not demanded.
Perry	44087012	03/02/87	6.6E-6	The HPCS system started on a low RPV water condition as a result of a loss of feedwater. The RCIC system failed to start as required.
Perry	44090001	01/07/90	1.4E-6	The HPCS system started on a low RPV water level condition as a result of a loss of feedwater. The RCIC system failed after 37 minutes of operation.
Wash. Nuclear 2	39787002	03/22/87	6.5E-6	The HPCS system started on a low RPV water level condition as a result of a loss of feedwater. The RCIC system was also used to restore normal RPV level.

5. REFERENCES

1. LaSalle Unit 1 Plant Technical Specifications.

2. Grand Gulf Plant Technical Specifications.

3. Illinois Power, *Clinton Power Station Individual Plant Examination Final Report*, September 1992.

4. Sandia National Laboratories, *Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events*, NUREG/CR-4550, SAND86-2084, September 1989.

5. Sandia National Laboratories, *Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP)*, NUREG/CR-4832, SAND92-0537, 1990.

6. Niagara Mohawk Power Corporation, *Nine Mile Point Nuclear Station-Unit 2, Individual Plant Examination (IPE)*, July 1992.

7. Cleveland Electric Illuminating Company, *Individual Plant Examination of the Perry Nuclear Power Plant*, July 1992.

8. Gulf States Utility Company, *Individual Plant Examination, River Bend Station*, 1993.

9. Washington Public Power Supply System, *Individual Plant Examination, Washington Nuclear Plant 2*, Rev. 1, July 1994.

10. G. M. Grant, J. P. Poloski, et al., *Emergency Diesel Generator Power System Reliability 1987—1993*, INEL-95/0035, February 1996.

Appendix A

HPCS Data Collection and Analysis Methods

Appendix A

HPCS Data Collection and Analysis Methods

To characterize high-pressure core spray (HPCS) system performance, operational data pertaining to the HPCS system from the eight U.S. commercial nuclear boiling water reactor plants having HPCS systems were collected and reviewed. This appendix provides descriptions for the operational data collection and the subsequent operational data characterization for the estimation of HPCS system unreliability. The descriptions give details of the methodology, summaries of the quality assurance measures used, and discussions of the reasoning behind the choice of methods.

A-1. DATA COLLECTION AND CHARACTERIZATION

The source of HPCS system operational data utilized in this report was LERs found using the Sequence Coding and Search System (SCSS) database. The SCSS database was searched for all HPCS records for the years 1987 through 1993. Because HPCS is a part of the emergency core cooling system (ECCS) required by technical specifications to be operable except when the reactor vessel head is removed, the cavity is flooded and the spent fuel pool gates are removed, and water level maintained within the limits defined by technical specification limits, all occurrences that resulted in the system not being operable as defined by the respective plant technical specifications are required by 10 CFR 50.73 to be reported in LERs.[A-1] In addition, LERs associated with the HPCS system can be submitted by the licensee for other reasons. As an example, the plant is in an unanalyzed condition or outside design basis are required to be reported by 10 CFR 50.73(a)(2)(ii), or events that alone could have prevented the fulfillment of a safety function are required to be reported by 10 CFR 50.73(a)(2)(v), or common mode failures resulting in at least one inoperable train or channel are required to be reported by 10 CFR 50.73(a)(2)(vii). Based on the reportability requirements in 10 CFR 50.73, the LERs encoded in the SCSS database should include all occurrences when the HPCS system was not operable defined by the above requirements.

In the subsections below, methods for acquiring the basic operational data used in this study are described.

A-1.1 Inoperability Identification and Classification

The SCSS database was searched for all HPCS records for the years 1987–1993. The search included all HPCS events reported under any 10 CFR 50.73 reporting requirement. The SCSS data search included all the failure timing codes as defined in SCSS: actual immediate; actual pre-existing, both previously detected and not previously detected; and potential. The preexisting detected category in SCSS includes cases where the HPCS system is out of service for maintenance when an actual need for HPCS occurred (e.g., low reactor vessel water level condition). The SCSS data search was only used to identify LERs for screening for this study; no data characterization, evaluation, or reliability analysis were performed on the information encoded in the SCSS data base.

For the purposes of this report, the term *inoperability* is used to describe any HPCS malfunction or situation, [except an engineered safety feature (ESF) actuation] in which a LER was submitted in accordance with the requirements identified in 10 CRF 50.73. It is distinguished from the term *failure*, which is a subset of the inoperabilities for which the ECCS core spray function of the system is lost. Because the HPCS system consists of a dedicated emergency power subsystem with a diesel generator, it

is necessary to define the term failure for this portion of the system separately from the ECCS core spray portion of the system. For the HPCS emergency power subsystem, a failure is defined as any inoperability for which the ability to supply emergency power to the Division III electrical bus is lost. The term *fault* is used in this study to refer to the remaining subset of inoperabilities that was not classified as failures.

A-1.1.1 Failure Classification

Each of the LERs identified in the SCSS database search was reviewed by a team of U.S. commercial nuclear power plant experienced personnel, with care taken to properly classify each event and to ensure consistency of the classification for each event. Because the focus of this report is on risk and reliability, it was necessary to review the full text of each LER and classify or exclude events based on the available information reported in the LER. Specifically, the information necessary in this report for determining reliability, such as classification of HPCS failures and faults, failure modes, failure mechanisms, causes, etc. were based on the independent review of the information provided in the LERs.

Two engineers independently evaluated the full text of each LER from a risk and reliability perspective. At the conclusion of the independent review, the data from each independent LER review were combined, and classification of each event was agreed upon by the engineers. The events that were identified as failures that could contribute to system unreliability were peer reviewed by the NRC technical monitor and technical consultants that have extensive experience in reliability and risk analysis. The peer review was conducted to ensure consistent and correct classification of the failure event for the reliability estimation process.

Failure classification of the inoperability events was based on the ability of the respective subsystem to function as designed for at least a 24-hour mission or until the system was no long needed for actual missions longer than 24 hours. For the HPCS injection subsystem, when an automatic start signal is received, the subsystem functions successfully if the pump starts, the pump discharge valve opens, and spray flow is delivered to the RPV until the flow is no longer needed. For the HPCS emergency power subsystem, when an automatic start signal is received, the subsystem functions successfully if the diesel generator starts, the output breaker closes and the diesel generator carries the loads on the Division III bus until no longer needed. Failure can occur at any time during the mission for either subsystem.

Based on the detailed review and evaluation of the HPCS operational data, the following failure modes were identified and used to estimate unreliability:

- For the HPCS injection subsystem, the possibility of the system being out of service for maintenance (MOOSI), failing to start (FTS), failing to run (FTRI), and failing to transfer the suction source from the condensate storage tank to the suppression pool (FTRT) were considered. For failure to start of the injection subsystem, whether the failure was the result of the injection valve (FTSV) or some other part of the subsystem (FTSI) was considered.

- For the HPCS emergency power subsystem, the possible failure modes are: being out of service for maintenance (MOOSD), failing to start, and failing to run (FTRD). For the emergency power subsystem starting probabilities, failures to start as a result of the output breaker (FTSB) were distinguished from other emergency power subsystem failures to start (FTSD). (These distinctions are discussed further below.)

Recovery from failures is also important in estimating subsystem reliability. For each failure that was identified during an unplanned demand, a determination was made as to whether recovery from the failure was successful. Recovery was defined as operators restoring normal system operation without repairing and/or replacing components. An example of such a recovery would be an operator (a) noticing that a motor-operated valve (MOV) in the spray path had not opened during an automatic start of the subsystem, and (b) manually operating the control switch for this valve, thereby causing the MOV to open fully and allow rated coolant flow to the RPV. Recovery from a failure that contributed to the other failure modes is defined in a similar manner.

In addition to the failure mode data, other information concerning the event were collected from the detailed review of the full text of the LER:

- The plant conditions at the time of the event (e.g., power operations, hot/cold shutdown, or refueling)
- For events classified as failures to run, the run time prior to failure
- The immediate cause of the event (e.g., hardware, personnel, or procedures)
- The subsystem and component involved
- The method of discovery of the event (unplanned demand, surveillance test, other routine plant operations), and for surveillance tests, the test frequency.

As a result of the review and evaluation of the full text of the LER, the number of events classified and used in this study to estimate HPCS unreliability will differ from the number of events and classification that would be identified in a simple SCSS database search. Differences between the data used in this study and a tally of events from a SCSS search would stem primarily from the reportability requirements identified for the LER and the exclusion of events for which the failure mechanism is outside the HPCS system boundary defined for this study.

Each LER usually has the reportability requirements identified in Block 11 of page 1. As an example, an event is reported based on the requirements identified in 10 CFR 50.73(a)(2)(i), technical specification prohibited operation or condition. The LER may be submitted specifically for the late performance of a technical specification required surveillance test. This event would be classified as a failure in the SCSS coding methodology. However, for this study, late performance of a surveillance test was classified as a fault. This classification was based on the judgment that given a demand for the system, the system was still capable of functioning as designed. Moreover, plant personnel typically stated in the LER that the system was available to respond and that the subsequent surveillance test was performed satisfactorily. If the system failed the subsequent surveillance test, the event would have been classified as a failure.

Other differences in classifications could exist for situations reported under the requirements of 10 CFR 50.73(a)(2)(ii), operating the plant in a degraded or unanalyzed condition. The LER in the SCSS database may identify HPCS being in a degraded condition. However, a risk-based review of the data provided in the LER may indicate that the system would not be able to operate as required for the 24-hour mission assumed in a PRA. As a result, the event would be classified as a failure even though the LER was submitted for a degraded condition. As an example, a lubrication oil leak was found during an unplanned demand of the system. The lubrication oil leak was such that the system operated as required for the few minutes necessary to restore reactor vessel water level and was shut down. However, the

information provided by plant engineers in the LER may identify that the oil leak was sufficient to allow operation of the pump for only 30 minutes. Because the system would be required to operate for a 24-hour mission as assumed in the plant's Individual Plant Evaluation (IPE), the event would be classified as a failure for this study. Conversely, a LER may be submitted per the requirements of 10 CFR 50.73(a)(2)(v), a condition that alone could prevent the mitigation of the consequences of an accident. This event would be classified as a failure in the SCSS database. However, a risk-based review of all the data in the LER may indicate that the system would be able to function as assumed for a 24-hour mission. As an example, a failed open minimum flow line isolation valve would not prevent the system from injecting coolant to the reactor vessel. In addition, an engineering analysis provided by the plant in the safety analysis section of the LER may state that the system would have been able to meet the requirements identified in the FSAR for adequate core cooling even considering the failed open minimum flow line isolation valve. Therefore, the event would not be classified as a failure for this study.

Other events reported per the requirements of 10 CFR 50.73(a)(2)(v) may be excluded from the study because the failure mechanism is outside the system boundary. As an example, the offsite power relays are found to be set below the technical specification minimum setpoints. The offsite power system is outside the system boundary. As a result, this event is not included in an HPCS study, even though it is a potential failure mechanism of the HPCS system.

Additional differences would be observed because of the definition of failure used in this study and that used in the SCSS database. Specifically, a system that is out of service for maintenance at the time of an unplanned demand would not be classified as a failure in the SCSS database, however, it would be classified as a failure for this study in an effort to estimate a maintenance-out-of-service unreliability. Also, the SCSS database would identify a system as failed if the system is out of service for pre-planned maintenance and another system subsequently fails. As an example, the HPCS system is out of service for maintenance when a relief valve that is part of the automatic depressurization system fails a surveillance test. The SCSS database would identify both systems as failed; however, pre-planned maintenance of the HPCS system without a corresponding demand is not considered a failure in this study.

Because of these differences, the reader and/or analyst is cautioned from making comparisons of the data used in this study with a simple tally of events from SCSS without first making a detailed evaluation of the data provided in the LERs from a reliability and risk perspective. The results of the LER review and evaluation are provided in Appendix B, Section B-1.

A-1.2 Demands

For the reliability estimation process, demand counts must be associated with failure counts. The identification of a set of particular system demands determines the set of failures to be considered in the reliability estimation (namely, the failures occurring during those demands). Two criteria are important in selecting event sets for reliability analysis. First, useful event sets must, of course, be *countable*. Reasonable assurance must exist that the number of demands can be estimated, that all failures associated with these demands will be reported, and that sufficient detail will be present in the failure reports to match the failures to the applicable failure events included in the fault tree model.

The second criterion is that the demands must reasonably approximate the conditions being considered in the unreliability analysis. The unplanned demands or tests must be rigorous enough that successes as well as failures provide meaningful system performance information. The determination of whether each demand reasonably approximates conditions for required accident/transient response depends in turn on the specific failure mode quantified by each failure probability estimate.

For the HPCS system, two estimates of unreliability were calculated. The first estimate pertains to *operational unreliability*; i.e., where HPCS is typically required to meet as observed in the operational data. Estimates of this type shows the strengths and weaknesses of the HPCS system during the conditions encountered most often. The operational events are typically events in which HPCS received a reactor low water level signal that was not caused by spurious signals as a result of inadvertently shorting test leads, tripping relays, etc. Based on the LER data the HPCS operational events consists of a pump start, the injection valve opening and spray flow delivered to the reactor vessel for a short period of time. The run times were generally 1 to 3 minutes. The short run time was the result of either normal feedwater or the reactor core isolation cooling system being available to maintain reactor vessel water level. This event also included a diesel generator start. During these events, the diesel generator was not required to power the Division III bus to support the core spray function. Therefore, the diesel generator ran unloaded (output breaker open) for a short period of time and was shut down. Because these events are of a short duration and did not require diesel generator operation, losses of room cooling or dedicated service water failures would not affect the success of the system in restoring reactor vessel level.

HPCS system unreliability was also estimated for comparison to PRAs. For this estimate, the assumptions postulated require the core spray pump to start and run for 24 hours, the injection valve to open, and the diesel generator to start and power the Division III electrical bus. These assumptions also require the system to provide adequate core cooling for 24 hours. The diesel generator is assumed to be needed to power the Division III bus for the full 24 hours. Any unavailability from the dedicated service water system is included in the emergency power subsystem, since the diesel generator will fail to run within a few minutes without adequate cooling water flow. A further requirement, implied by the 24-hour core cooling requirement, is that the core spray pump suction source must be able to switch from the condensate water storage tank to the suppression pool.

A-1.2.1 Unplanned Demands

To estimate unreliability, information on the frequency and nature of HPCS demands is needed. LERs provide information on unplanned demands. These demands were identified by searching the SCSS database for all LERs containing HPCS engineered safety feature (ESF) actuations that occurred from 1987 through 1993. In addition to the search for ESF actuations, a search was conducted for events in which the system was out of service for pre-planned maintenance when a demand of the system occurred (i.e., reactor vessel low water level condition). The identified LERs were screened to determine the nature of the HPCS ESF actuation.

The LERs that identified an HPCS ESF actuation were screened to determine the extent of the actuation and the portion of the system involved. Unplanned ESF actuations that required the ECCS function of the system were, of course, included in the study. ESF actuations that exercised only a small portion of the HPCS system were excluded if they were caused by maintenance (e.g., removing fuses or shorting test leads) since system response might be affected by the maintenance itself. Other demands were included to estimate the unreliability of a portion of the system, such as whether the system would start, for example, the manual start of the core spray pump as a precautionary measure or to provide load for the diesel generator. This partial nature of some of the injection subsystem demands is accommodated by splitting failure to start of the injection subsystem into failure of the core spray pump to start and failure of the injection MOV to open. Failure to start thus led to two basic events for the injection subsystem fault trees.

Another consideration for the unplanned demands is that some demands applied to the emergency power subsystem only. For example, a low-voltage condition on the Division III electrical bus would demand the diesel generator to start and the output breaker to close; however, the core spray pump would not be demanded to start. Also, a low water level condition associated with the reactor vessel would

require the diesel generator to start as a precautionary measure. However, the output breaker would not close because power would still be available to the Division III electrical bus from the normal source. Therefore, the emergency power subsystem demands were listed in two groups: demands that resulted in an attempt to start the diesel generator and demands that attempted to close the output breaker. This partial nature of some of the emergency power subsystem demands is accommodated by splitting failure to start of the subsystem into failure of the diesel generator start and failure of the output breaker to close. Failure to start thus led to two basic events for the emergency power subsystem fault trees.

In addition for each demand, the associated running time was obtained if it was stated or could be reasonably determined from the sequence of events stated in the LER. This determination was particularly important for quantifying the failure to run events for comparison to PRAs, as explained in Section A-2.

A-1.2.2 Surveillance Tests

Data from surveillance tests that are performed on a periodic basis may be used to estimate selected aspects of HPCS system unreliability. For reasons described below, quarterly surveillance tests and surveillance tests that are conducted on a cyclic interval (approximately 18 month) were used to estimate unreliability for the HPCS injection subsystem, while just the cyclic surveillance tests were used to estimate unreliability for the HPCS emergency power subsystem.

Routine surveillance tests of the HPCS system are performed as required by plant technical specifications and ASME Section XI for motor-driven pumps. HPCS failures during these tests are a 10 CFR 50.73 reportability requirement. Therefore, the failure count from routine surveillance tests is believed to be as complete as possible. To ensure accuracy and applicability of the data for use in this study, the completeness of each of these tests was evaluated based on a detailed review of several available technical specifications and, for the HPCS emergency power subsystem, on a review of Regulatory Guide 1.108.[A-2] The conclusions of the technical specifications and regulatory guide review are listed below.

For the HPCS injection subsystem:

- The cyclic surveillance tests require the system to be functionally tested. This testing includes simulated automatic actuation of the system throughout its emergency operating sequence and verification that each automatic valve in the flow path actuates to its correct position. The ability of the HPCS system to sustain flow in a recirculation mode over a period of time, and the ability to transfer the suction source, is also verified. However, the cyclic surveillance tests do not challenge the injection valve at the pressures, flow rates, and temperatures that the system would experience during a demand for emergency operation. Therefore, the cyclic surveillance tests were regarded as demands on the system except for the injection valve. Test failures reported in LERs can be identified as occurring on cyclic tests by supplementing the LER narrative with the event date and the dates of the plant's refueling outages; cyclic tests are typically performed during refueling outages.

- The quarterly tests of the core spray pump as required by ASME Section XI demand the pump to start. Also, the testing performed during the quarterly test (pump vibration, etc.) was assumed would require the pump to run for approximately 1.5 hours to complete the ASME Section XI requirements. This test provided data for both the failure to start and failure to run of the core spray pump. However, the injection valve and the suction source transfer valves are not challenged at the pressures, flow rates, and temperatures that the

system would experience during a demand for emergency operation. Therefore, the quarterly surveillance tests were regarded as demands for the core spray pump only. Lack of ability to determine the type of surveillance being performed when a failure occurs, so that failures can be properly associated with countable demands, sometimes prevents the use of quarterly test data. However, just three failures were seen on non-cyclic tests and the particular LERs were clear about the type of testing being performed. Therefore, quarterly surveillance test data were used for applicable failure modes in the reliability analysis for the HPCS injection subsystem.

For the HPCS emergency power subsystem:

- The cyclic surveillance tests as a group mimic unplanned demands to start and run. The cyclic 24-hour load test is performed while the diesel generator is in parallel with the grid rather than as an independent unit; however, the results are considered applicable to the FTR failure mode.

- The monthly diesel generator test does not mimic an unplanned demand well. It is simply a manual start (sometimes by partial simulation of an automatic start signal) with manual synchronization to the grid and controlled loading to full rated load for 1 hour. This surveillance test does not represent an unplanned demand for emergency operation except for achieving proper voltage or speed. Like the 24-hour cyclic load test, it tests parallel operation rather than independent operation. Furthermore, the system may be prepped prior to the test. Therefore, successes in these tests do not necessarily imply success is applicable to the models developed for this study. Other difficulties precluding the use of monthly test data include the fact that the total number of EDG demands for monthly EDG testing is unknown and likely to be more than 12 per year since Regulatory Guide 1.108 requires increased monthly EDG testing depending upon the failure history of each EDG.

Demand counts for cyclic surveillance tests for both the HPCS injection and emergency power subsystems were estimated as follows. The plants are required to perform the test at least every 18 months. The tests are typically scheduled to coincide with refueling outages. These refueling outage start dates were found in the monthly operating reports submitted by the licensees to the NRC. For this study, a plant was assumed to perform the cyclic surveillance test as part of starting up after each refueling outage. If the time period until the start of the next refueling outage was more than 550 days (18 months), the necessary number of intermediate tests was assumed. Quarterly test demands were estimated as four per year.

A-1.3 Estimating Run Times

The reported system inoperabilities, failures, and unplanned demands were characterized and studied from the perspective of overall trends and the existence of patterns in the performance of particular plant units. These assessments were based on frequencies of occurrence per year. Since the HPCS system is a required safety system for the plant whenever irradiated fuel is in the core, i.e., both when a plant is operational and most of the time when it is shut down, there was no need to derive the operational time for each plant. Instead, trends were studied based on straight calendar time for the plant from low-power license date. It was also assumed that the age of the HPCS system is the same as the total calendar time of the plant from the low-power license date.

For the PRA comparison, rates were also used to quantify probabilities for the injection subsystem failing to run from causes other than failure of the suction source transfer, and for the diesel failing to run. For these calculations, the run times stated in the LERs were used for the unplanned demands.

For one event among the unplanned demands, no run times could be inferred from the LER. In this event, the diesel supplied power to the bus for a period of time without failure. HPCS injection also occurred during the event, but the injection was initiated spuriously from an instrumentation inoperability (with no loss of safety function) and was very brief. The event was judged not to provide useful information about the injection pump running. The emergency power subsystem run time for this event was estimated as the average of the run times for four of the remaining seven events with loaded diesel run times. Among the seven events, three were excluded because their run times were known to be atypical of the run time being estimated. One event's run time was just 5 minutes, and a second event's run time was cut short (at 7 minutes) by a diesel failure. These run times were known to be shorter than the run time being sought. In the last excluded event, the run time (48 hours) was known to be much longer than the run time being estimated. The average of the remaining four run times is 4.6 hours.

In testing, each cyclic and quarterly test for the injection and service water pumps includes at least an hour of run time unless a failure occurs. Tests of the HPCS injection system do not require simultaneous operation of the HPCS emergency power subsystem. For the emergency power subsystem, the cyclic test run times are typically 24 hours. These times were used in the failure rate estimates.

A-2. ESTIMATION OF UNRELIABILITY

Five failure modes were identified for estimating HPCS injection subsystem unreliability: maintenance-out-of-service at the time of a demand (MOOS), failure to start from injection valve problems (FTSV), failure to start from other problems (FTSI), failure to run for the required duration of HPCS mission due to failures of the switching logic or valves that transfer suction from the CST to the suppression pool (FTRT), and other failures to run for the required duration (FTRI). Each of these five HPCS injection subsystem failure modes corresponds to a basic event. The HPCS injection subsystem fault tree is discussed in Section 3.1. No failures to recover from these events were modeled because no injection subsystem failures other than maintenance unavailability occurred among the unplanned demands. With no failures, neither failure counts nor demands were available to estimate the nonrecovery probabilities. The recovery events for modes for which recovery is a possibility were therefore left undeveloped.

The HPCS unreliability model used for comparison to PRAs requires success of the HPCS injection subsystem, as well as successful operation of the HPCS emergency power subsystem. For the HPCS emergency power subsystem, similar failure modes are defined: out of service for maintenance at the time of a demand (MOOSD), failure to start from output breaker problems (FTSB), failure to start from other problems (FTSD), and failure to run (FTRD). As with the HPCS injection subsystem, estimates for the probabilities of failure to recover from these events (other than MOOS) were developed only for failure modes for which unplanned demand failures occurred. One the emergency power subsystem recovery probability could be estimated: failure to recover from FTRD.

The operational mission for HPCS is less rigorous. The emergency power subsystem is not required, and the injection subsystem required time is much shorter. The shorter operation time results in two additional differences in the details of the injection subsystem unreliability model. First, the failure to transfer event (FTRT) is not included. Second, since each operational mission is an example of success or failure of the operational mission, the failure to run probability was estimated simply as the number of failures divided by the number of demands. In the calculations, this estimate is labeled FTRI-OP to

distinguish it from the longer running time included in the PRA model injection system failure to run estimate (FTRI).

Because the operational mission run times for injection were much shorter than the mission time postulated in the PRA/IPEs, each operational mission was not taken to show a success in running for the PRA comparison. Instead, the associated run times were pooled across events to estimate a failure rate. Performance for 24 hours with the estimated rate was then assessed. The sparse data provide no evidence for a non-constant failure rate.

For comparison to PRAs, the same approach was used for the failure to run estimate for the emergency power subsystem as for the injection subsystem.

The failure probabilities identified for the operational mission were combined to estimate the total unreliability, or probability of failure to start and run as required given a demand, for the operational mission. Similarly, the individual failure probabilities, failure rates, and mission times were combined to estimate the total unreliability for the comparison to PRAs. Estimating each unreliability and its associated uncertainty involves two major steps: (a) estimating probabilities and uncertainties for the different failure modes or fault tree basic events and (b) combining these estimates. These two steps are described below.

A-2.1 Estimates for Each Failure Mode

Estimating the probability for a failure mode requires decisions about which data sets (unplanned demands, cyclic surveillance tests, and/or quarterly surveillance tests) to use, a determination of the failure and demand counts (or operating times) in each data set, and a method for estimating the failure probability and assessing the uncertainty of the estimate.

A-2.1.1 A Priori Choice of Data Sets

Maintenance unavailability for the HPCS system does not occur on surveillance tests; therefore, the MOOSI and MOOSD failure modes were found only in the unplanned demands. The same applies to the failure to recover from FTRD mode, because responses to failures during tests focus on diagnosing the problem rather than prompt recovery of the system. HPCS injection subsystem cyclic tests do not test the injection valve under the stresses present during unplanned demands; therefore, the failure mode FTSV can be found only during the unplanned demands, not in the cyclic surveillance tests. Tests do provide useful data for the FTSI, FTRT, and FTRI/FTRI-OP failure modes of the HPCS injection subsystem and the FTSD, FTSB, and FTRD failure mode of the HPCS emergency power subsystem. For the FTRT failure to transfer failure mode, cyclic tests provide the only useful data. Further restrictions on the application of cyclic tests and unplanned demands to specific failure modes, which were revealed after examination of the data, are discussed below.

A-2.1.2 Demand and Failure Counts

Unplanned Demands. The unplanned demands were counted by failure mode as follows. The total demand data set was obtained as described in Section A-1. The number of MOOSI demands is simply the number of unplanned HPCS injection subsystem demands obtained from the LERs. The number of MOOSD demands is the number of unplanned HPCS emergency power subsystem demands. In the analysis of each of these demands and associated failures, separate estimates were computed for operational and shutdown periods.

For both the HPCS injection and emergency power subsystems, events in which the maintenance unavailability mode did not occur provide demands for the respective failure to start (other) modes (FTSI and FTSD). Demands for tests of the FTSV mode and the FTSB mode, respectively, consist of the subset of these events that were full demands without unrecovered other failures to start.

Opening of the injection valve for the injection subsystem is not required to observe the injection subsystem running, since the system can operate in a recirculation mode. Similarly, operation of the emergency diesel can be observed even in those operational missions for which the diesel output breaker was not closed and the diesel was not loaded. Thus, the failure to run modes for both subsystems were estimated starting with the same data sets as for the failures to start from other modes. Unrecovered failures from these modes would be excluded as demands for running. The event with negligible injection time was excluded for the injection subsystem failure to run analyses.

As described above, injection subsystem failure to run estimates were evaluated on a per demand basis for the operational mission and on a per hour basis for comparison to PRAs. Failure rates for the HPCS emergency power subsystem were developed for comparison to PRAs. In each failure rate analysis, the total observed running time was combined with the number of failures to estimate an occurrence rate that could be extrapolated to estimate the probability of failure to run during the 24-hour mission time.

No unplanned demands adequately tested the FTRT failure mode. Although unplanned spurious signals activated a portion of this capability, these events were not associated with any other aspect of the HPCS system and were judged not applicable to the HPCS for comparison to PRAs. As stated earlier, none of the unplanned demands that required the HPCS injection subsystem resulted in a demand for a transfer.

Where non-maintenance failures were found among the unplanned demands, estimates of failure to recover probabilities were based on the total number of failures and the number of associated unrecovered failures.

Surveillance Tests. The above discussion has considered only unplanned demands. Surveillance tests are described in Section A-1.2.2. The number of cyclic and/or quarterly surveillance test demands for each applicable failure mode was estimated as follows.

For the HPCS injection subsystem, the estimated number of test demands was applied for the FTSI, and FTRI/FTRI-OP failure modes. Cyclic test data (but not quarterly test data) were considered for the FTRT failure mode. For the FTRI failure mode, an estimated running time of 1 hour was applied for each applicable test. The modeling assumes that failures of the suction source transfer function (FTRT) can occur after success of FTRI, and conversely. As mentioned previously in Section A-2.1.1, surveillance tests are not applicable to FTSV.

For the HPCS emergency power subsystem, cyclic test demands were applied for the FTSD, FTSB, and FTRD failure modes. The run time for FTRD was 24 hours per test.

A-2.1.3 Data-Based Choice of Data Sets

At this point, failures and demands or operating time had been counted or estimated for selected failure modes for as many as three sets of data: unplanned demands, quarterly surveillance tests, and cyclic surveillance tests. To determine which data to use in particular cases, each mode failure probability and the associated 90% confidence interval was 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. A comparison of the plotted confidence intervals gave a visual indication of whether the data sets could be pooled.

For each failure mode, the hypothesis that the underlying probabilities and/or rates as applicable were the same in each data set was tested. When two groups of data with failures and demands were compared, as for the diesel FTSD failure probability, Fisher's exact test (described in many statistics references) was used, based on a contingency table with two rows corresponding to failures and successes and two columns corresponding to unplanned demands and cyclic surveillance tests. In other cases, chi-square tests were used to evaluate the null hypothesis of equal rates or probabilities for a failure mode across data sets from different types of testing or from unplanned events.

Two sets of data were also considered for the maintenance-out-of-service events (MOOSI and MOOSD). As already stated, only unplanned demand data apply to maintenance unavailability; however, occurrence probabilities a priori are expected to differ based on plant mode (operating versus shutdown). The duration of HPCS system maintenance outages during plant operations is limited by plant technical specifications. During plant outages, the technical specifications are much less restrictive. For most plants, having two emergency core cooling systems available during shutdown suffices. Thus, maintenance outages are expected to occur more often during shutdown. Statistical tests for differences between operational and shutdown maintenance probabilities were performed in the same manner as the tests just described for differences between unplanned demand data and cyclic or quarterly tests.

Other types of failures were not analyzed with regard to plant mode. Differences based on plant mode are not expected, the failure data are sparse, and mode information is not available for the successes that occur during cyclic tests.

To further characterize the failure probability estimates and their uncertainties, probabilities and confidence bounds were computed in each data set for each year and 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. They are useful for screening, however.

As with Fisher's exact test, a premise for these 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 short, 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 years, plant units, or data sources, rather than to mask existing differences in these attributes.

A-2.1.4 Estimation of Failure Probability Distributions using Demands

Three methods of modeling the failure/demand data for the unreliability calculations were employed. They all use Bayesian tools, with the unknown probability 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 unreliability.

In all three methods, Bayes Theorem provides the mechanics for this process. 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-3] 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-4] 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-5] 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-4] 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. Occasionally, the unreliability was modeled by group (such as by plant or by year) to see if trends existed, such as trends due to time or age. 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. Even when no differences can be seen between groups for any one failure mode, so that the above methods would pool the data for each failure mode, the failures of various modes could all be occurring in a few years or at a few plants. They could thus have a cumulative effect and show a clearly larger unreliability for those few years or plants. Therefore, it is useful to calculate the unreliability for each group (each year or plant) in a way that is very sensitive to the data from that one group.

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 unreliability 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-6 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-7] 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-6.

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-8] was made in the posterior beta distribution parameters for particular plants and 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. Two probabilities were computed, the probability that, given the resulting beta posterior distribution and binomial sampling, as many or more than the observed number of failures for the group would be observed, and the probability that as many or fewer failures would be observed. If either of these probabilities 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. No strong evidence against the model was seen in this study. See Atwood[A-4] for more details about this test.

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

A-2.1.5 Assessments and Estimation of Failure Probability Distributions using Rates

As stated above, the HPCS injection subsystem FTRI and FTRD probabilities were derived from a rate of occurrence rather than from failures and demands. Bayesian methods similar to those described above were used. 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 shape parameter $1/T$, where T is the total pooled running time. An *empirical Bayes* method also exists, but the data were too sparse to find a non-degenerate distribution. 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-6 and A-9.

The resulting gamma distributions for uncertainty in FTRI and FTRD were converted to beta distributions describing the probability of failure during a specified mission time. Given an occurrence rate, say *r*, the probability of failure in mission time *T* (assuming a Poisson distribution for the occurrence of failures) is:

$p(r) = 1-\exp(-rT)$.

If E(*r*) is the mean of the rate and V(*r*) is its variance, and r has a gamma distribution with parameters (a,b), then is can be shown that the mean of p(*r*) is

$1- (1 + T/b)^{-a}$

and the variance of p(*r*) is

$(1 + 2T/b)^{-a} - (1 + T/b)^{-2a}$.

These equations were applied using the gamma distribution means and variances for the rates for the two failure modes. Beta distributions having the resulting means and variances were computed by matching moments. This evaluation was performed for the mission time, namely T=24 hours.

A-2.2 The Combination of Failure Modes

The failure mode probabilities are combined to obtain the unreliability. The following algebraic approximation was used. The method is presented in more generality by Martz and Waller,[A-5] but is summarized for the present application here. According to the logic models, the mission unreliabilities are given by the following expressions:

Operational mission unreliability = Prob[MOOSI or FTSI or FTSV or FTRI-OP].

Unreliability for comparison to PRAs = Prob[(MOOSI or FTSI or FTSV or FTRI or FTRT) or (MOOSD or FTSD or FTSB or (FTRD and FR FTRD)].

Each of these expressions can be rewritten by repeatedly using the facts that

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

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

In practice, estimates are obtained by the following process:

- Compute the mean and variance of each beta distribution

- Compute the mean and variance of the unreliability for each case using simple equations for expected values of sums for "or" operations and of products for "and" operations

- Compute parameters for the beta distribution with the same mean and variance

- Report the mean of the unreliability and the 5th and 95th percentiles of the fitted beta distribution.

The means and variances calculated from this process are exact. The 5th and 95th percentiles are only approximate, however, because they assume that the final distribution is a beta 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 a beta distribution. Nevertheless, the approximation seems to be close in cases where comparisons were made, and therefore the beta approximation was used in this study.

A-3. ESTIMATION OF FREQUENCY DISTRIBUTIONS FOR TREND ANALYSIS

In addition to the analyses used to estimate system unreliability, the overall frequencies of inoperabilities, failures, and unplanned demands were analyzed by plant and by year to identify possible trends and patterns. Two specific analyses were performed for the three occurrence frequencies. First, the frequencies were compared to determine whether significant differences exist among the plants or among the calendar years. Frequencies and confidence bounds were computed for each type of frequency for each year and plant unit. The hypotheses of simple Poisson distributions for the occurrences with no differences across the year and plant groupings were tested, using the Pearson chi-square test. The computed p-values are approximate since the expected cell counts were often small; however, they are useful for screening.

Regardless of whether particular years or plants were identified as having different occurrence frequencies, the occurrence frequencies were also modeled by plant and by year to see if trends exists. For plants, trends with regard to plant age are assessed, as measured from the plant low-power license date. For years, calendar trends are assessed. Least-squares regression analyses are used to assess the trends. The paragraphs below describe certain analysis details associated with the frequency trend analyses.

With sparse data, estimated event frequencies (event counts divided by time) are often zero, and regression trend lines through such data often produce negative frequency estimates for certain groups (years or ages). Since occurrence frequencies cannot be negative, log models are considered. Thus, the analysis determines whether log (frequency) is linear with regard to calendar time or age. An adjustment is needed in order to include frequencies that are zero in this model.

Using $0.5/t$ as a frequency estimate in such cases is not ideal. Such a method penalizes groups that have no failures, increasing only their estimated frequency. Furthermore, industry performance may show that certain events are very rare, so that $0.5/t$ is an unrealistically high estimate for a frequency. A method that adjusts the frequencies uniformly for all the grouping levels (plants or years) and that uses the overall frequency information contained in the industry mean is needed for sparse data and rare events.

As stated in Section A-2.1.5, constrained noninformative priors can be formed for frequencies. This method meets the requirements identified above. Because it also produces occurrence frequencies

for each group (each year or plant) in a way that is very sensitive to the data from that one group, it preserves trends that are present in the unadjusted frequency data. The method, described in Reference A-6, involves updating a prior gamma distribution using data from a single group. The prior distribution is a diffuse (somewhat noninformative) prior with a constrained mean. Keeping the prior diffuse is achieved by basing the modeling on a maximum entropy distribution, as explained in the references. The mean is constrained to be the estimated pooled industry mean [(0.5+N)/*T*, where *N* is the total number of events across the industry and *T* is the total exposure time]. The mean of the resulting updated posterior distribution is used in the regression trending. This process effectively adds 0.5 uniformly to each event count and *T/(2N+1)* to each group exposure time.

In practice, an additional refinement in the application of the constrained noninformative prior method adjusts the posterior gamma distribution parameters for particular plants and years to account for the fact that the prior distribution gamma scale parameter is only estimated, not known. This adjustment[A–8] increases the group-specific posterior variances somewhat.

A-4. REFERENCES

A-1. 10 CFR 50.73, “Licensee Event Report System,” Code of Federal Regulations, Office of the Federal Register, October 1994.

A-2. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.108, “Emergency Diesel Generator Testing and Reporting Requirements.”

A-3. G. E. P. Box and G. C. Tiao, *Bayesian Inference in Statistical Analysis*, Reading, MA: Addison Wesley, 1973, Sections 1.3.4–1.3.5.

A-4. C. L. Atwood, *Hits per Trial: Basic Analysis of Binomial Data*, EGG-RAAM-11041, September 1994.

A-5. H. F. Martz and R. A. Waller, *Bayesian Reliability Analysis*, Malabar, FL: Krieger, 1991, Section 7.6.

A-6. C. L. Atwood, *Constrained Noninformative Priors*, INEL-94/0074, October 1994.

A-7. B. Harris, "Entropy," *Encyclopedia of Statistical Sciences, Vol. 5*, S. Kotz and N. L Johnson, editors, 1982, pp. 512–516.

A-8. R. E. Kass and D. 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-9. M. E. Engelhardt, *Events in Time: Basic Analysis of Poisson Data*, EGG-RAAM-11088, September 1994.

Appendix B

HPCS Operational Data, 1987–1993

Appendix B

HPCS Operational Data, 1987–1993

In this appendix, listings of the data used for the high-pressure core spray (HPCS) system reliability study are provided. First, the results of the Sequence Coding and Search System (SCSS) data search and classification are listed. Then the inoperabilities are listed. Unplanned demands are then listed, followed by a listing of the estimated number of cyclic surveillance test demands. Finally, a tabular summary of the failures used to estimate unreliability are provided.

B-1. HPCS INOPERABILITIES

The source of HPCS operational data utilized in this report was based on LERs encoded in the SCSS database. The SCSS database was searched for all HPCS records for the years 1987–1993. The information encoded in the SCSS database includes actual and potential HPCS failures reported for various reasons in accordance with the 10 CFR 50.73 reportability requirements. The information encoded in the SCSS database was only used to identify LERs for the review and classification. The full text of each LER was independently reviewed and evaluated by a team of U.S. commercial nuclear power plant experienced personnel, with care taken to properly classify each event and to ensure consistency of the classification for each event. Because of the focus of this report is on risk and reliability, it was necessary to review the full text of each LER and classify or exclude events based on the review of all the available data reported in the LER. Specifically, the information necessary in this report for determination of reliability, such as classification of HPCS failures, demands, failure mode, failure mechanism, cause, etc., was based on the independent review of the information provided in the LERs. Table B-1 provides a breakdown of the results of the event screening and classification for the inoperabilities. The breakdown also identifies the failure mode for the inoperabilities that were classified as failures, and the method of discovery.

As a result of the review and evaluation of the SCSS LER data, the number of events classified and used in this study to estimate HPCS unreliability will differ from the number of events and classification that would be identified in a simple SCSS database search. Differences between the data used in this study and a tally of events from an SCSS search would stem primarily from the reportability requirements identified for the LER and the exclusion of events that the failure mechanism is outside the system boundary. Details of the event classification methodology were discussed previously in Appendix A.

Table B-2 provides the column headings and associated definitions of the information tabulated in Table B-3. Table B-3 is a listing of all the inoperability events that were classified for inclusion in the HPCS study. These events were used to provide the data summary listed in Table B-1. The events that were classified as failures include the applicable failure mode. For the unreliability estimation process, only the failures that occurred during an unplanned demand or that were found during the performance of cyclic and quarterly surveillance tests (quarterly tests were used only for the injection subsystem) were used to estimate unreliability.

Table B-1. The results of the data search and classification of HPCS inoperability events.

	Method of Discovery				
	Unplanned Demands	Cyclic Surveillance Tests	Other Surveillance Tests	Other[a]	Total
Failures					
Maintenance-out-of-service (MOOS)					
Injection subsystem (MOOSI)	1	NA	NA	NA	1
Emergency power subsystem (MOOSD)	3[b]	NA	NA	NA	3[b]
Failure to start (FTS)					
FTS of the injection subsystem (FTSI)	0	0	1	2	3
Failure of the injection valve to open (FTSV)	0	0	0	0	0
FTS of the emergency power subsystem (FTSD)	0	0	0	2	2
FTS of the diesel output breaker (FTSB)	0	0	0	0	0
FTS of the service water subsystem (FTSW)	0	0	0	1	1
Failure to run (FTR)					
FTR of the injection subsystem (FTRI)	0	0	1	3	4
Failure of the suction source transfer (FTRT)	0	1	0	2	3
FTR of the emergency power subsystem (FTRD)	2	0	0	0	2
FTR of the service water subsystem (FTRW)	0	0	0	1	1
Total Failures	6[c]	1	2	11	20
Total Faults	0	1	6	30	37
Grand Total	6	2	8	42	57

a. Observation, design review, etc.

b. Two of the three events occurred when the plant was shut down, and therefore were not used to estimate unreliability.

c. Only four of the six events were used to estimate unreliability. Refer to note b.

Table B-2. Column heading definitions and abbreviations used in Table B-3.

Column Heading	Definition
Plant name	Self-explanatory.
LER number	Self-explanatory. However, in some cases, the LER number listed is for the unplanned demand in which a failure was observed. It is not unusual for a plant to report the unplanned demand in one LER and mention that the system did not respond as designed. LER number XXX89001 and a followup LER (i.e., LER number XXX89003) provide the details of the failure and subsequent corrective actions. Also, the LER number may not match the docket number for a dual unit site. The LER may be under a Unit 1 number because the event affected both units; however, a failure may also be identified at Unit 2.
Event date	The event date is typically the date identified in Block 5 of the LER. In some cases, the Block 5 date may be different than the failure date, because the system may have run for a period of time prior to the failure. In all cases, the event date is the date of the actual failure.
SFL	Safety function lost: T, true— the deficiency identified in reviewing the full text of the LER was such that the system would **not** have been able to respond as designed for a risk-based mission. F, false— the deficiency identified in reviewing the full text of the LER was such that the system would have been able to respond as designed for a risk-based mission. These events (SFL=F) are referred to as faults. These classifications are not based on the reportability requirements identified in Block 11 of the LER.
Failure mode	The failure mode is risk-related information that is only provided for the events that are classified as failures (i.e., SFL=T). FTS, failure to start; FTR failure to run; FTRT, failure to run transfer (failure of the suction path to transfer from the condensate storage tank to the suppression pool); MOOS, maintenance-out-of-service.
Method of discovery	The method of discovery identifies how the inoperability was found. O, operational occurrence, is discovered through the normal course of routine plant operations. This category includes operator walkdowns, control room annunicators or alarms, etc. S, periodic surveillance test (other than cyclic or quarterly), [S(C)] identifies a cyclic surveillance test; [S(Q)] identifies a quarterly surveillance test; A, unplanned demand.
Subsystem	Subsystem: I, injection; D, dedicated diesel and associated emergency power; S, dedicated service water system; H, dedicated heating, ventilation or room cooling.

Table B-3. Events found in the SCSS database search that were classified as faults or failures.

Plant Name	LER Number	Event Date	SFL	Failure Mode	Method of Discovery	Subsystem
Clinton	46187069	12/03/87	F	—	S	I
Clinton	46188018	07/07/88	T	FTR	O	I
Clinton	46188027	11/10/88	F	—	O	D
Clinton	46189017	02/28/89	F	—	O	D
Clinton	46189039	12/03/89	F	—	O	I
Clinton	46189041	12/18/89	F	—	S	H
Grand Gulf	41688020	12/06/88	T	FTR	S	I
Grand Gulf	41690003	02/15/90	F	—	O	S
Grand Gulf	41690010	07/06/90	F	—	O	H
Grand Gulf	41690012	07/24/90	F	—	O	S
Grand Gulf	41693003	03/24/93	T	FTS	S	S
Grand Gulf	41693019	11/22/93	T	FTS	S	I
LaSalle 1	37387011	03/07/87	F	—	S	I
LaSalle 1	37387027	07/14/87	F	—	O	I
LaSalle 1	37388019	08/29/88	F	—	S	D
LaSalle 1	37391016	10/24/91	F	—	O	D
LaSalle 1	37392006	04/27/92	F	—	O	H
LaSalle 1	37393010	04/14/93	F	—	S	S
LaSalle 2	37488005	04/12/88	F	—	S	I
LaSalle 2	37489007	06/12/89	T[a]	MOOS	A	D
LaSalle 2	37489008	06/14/89	T	FTS	O	D
LaSalle 2	37489010	07/15/89	F	—	O	D
LaSalle 2	37389011[b]	03/04/89	T[a]	FTR	A	D
LaSalle 2	37489017	11/17/89	F	—	S	I
LaSalle 2	37491001	01/10/91	F	—	O	I
Nine Mile Point 2	41088053	09/28/88	F	—	O	D
Nine Mile Point 2	41091020	09/29/91	F	—	S	I
Nine Mile Point 2	41092006	03/27/92	T[a]	FTR	A	D
Nine Mile Point 2	41093010	11/08/93	F	—	O	I
Perry	44088012	04/27/88	T[a]	MOOS	A	I

Table B-3. (continued)

Plant Name	LER Number	Event Date	SFL	Failure Mode	Method of Discovery	Subsystem
Perry	44088027	06/29/88	F	—	O	I
Perry	44089032	12/22/89	F	—	S	D
Perry	44090002	01/07/90	F	—	O	D
Perry	44090005	04/05/90	F	—	O	D
Perry	44090041	12/12/90	T	FTS	O	I
Perry	44091017	10/02/91	T	FTR	O	I
Perry	44091025	12/12/91	F	—	S	I
Perry	44092015	07/01/92	T	FTRT	O	I
Perry	44093012	06/07/93	F	—	O	D
River Bend	45890022	05/18/90	F	—	S	I
River Bend	45890029	10/06/90	T	FTRT	O	I
River Bend	45893013	06/29/93	T[a]	FTS	S(Q)	I
Wash. Nuclear 2	39789015	05/12/89	F	—	S(C)	I
Wash. Nuclear 2	39789016	05/14/89	T	MOOS	A	D
Wash. Nuclear 2	39789030	02/10/89	T[a]	FTRT	S(C)	I
Wash. Nuclear 2	39789043	11/21/89	F	—	S	I
Wash. Nuclear 2	39789044	11/28/89	F	—	O	I
Wash. Nuclear 2	39790004	02/08/90	T	FTS	S	D
Wash. Nuclear 2	39790017	08/30/90	F	—	S	D
Wash. Nuclear 2	39790025	10/23/90	F	—	S	I
Wash. Nuclear 2	39790028	10/31/90	F	—	S	I
Wash. Nuclear 2	39791017	07/08/90	T	MOOS	A	D
Wash. Nuclear 2	39792001	01/02/92	F	—	S	D
Wash. Nuclear 2	39792014	03/26/92	F	—	O	I
Wash. Nuclear 2	39792025	05/22/92	T	FTR	S	I
Wash. Nuclear 2	39792034	07/13/92	F	—	O	I
Wash. Nuclear 2	39793015	03/31/93	F	—	O	H

a. This event was used in the estimation of unreliability.

b. The failure was reported for Unit 2 on a Unit 1 LER number because the event affected both units. In addition, the demand occurred on 03/02/89; however, the diesel failed on 03/04/89.

B-2. HPCS UNPLANNED DEMANDS

To estimate unreliability, information on the frequency and nature of HPCS demands was needed. LERs provide information on unplanned demands. These demands were identified by searching the SCSS database for all LERs containing HPCS engineered safety feature (ESF) actuations that occurred from 1987 through 1993. In addition to the search for ESF actuations, a search was conducted for events in which the system was out of service for pre-planned maintenance when a demand of the system occurred. The identified LERs were screened to determine the nature of the HPCS ESF actuation.

Specific aspects of the LER review were included for the emergency power subsystem: whether the HPCS diesel generator was demanded to start and run, and whether the HPCS diesel generator output breaker was required to close on an undervoltage signal on the Division III bus, and for the HPCS injection subsystem: whether the pump was demanded to start and run, and if the injection valve was demanded to open. The demands identified in Table B-4 may or may not have been in response to a reactor pressure vessel water level transient. The portion of the system demanded is identified in Table B-4 with a "T" in the appropriate column. For the events that resulted in the running of the diesel or the injection pump, the run time is recorded, if known. The run time is shown in Table B-4 in an HHMM format (e.g., 0105 corresponds to a run time of 1 hour and 5 minutes).

Table B-4. HPCS unplanned ESF actuations.

Plant	LER Number	Event Date	EDG Demand	BKR[a] Closed	Pump Demand	Injection Demand[b]	Run Time[c]
Clinton	46187014	03/15/87	T	F	T	F	0002
Clinton	46187022	04/07/87	T	F	T	T	0001
Clinton	46187026	05/11/87	T	F	T	F	0003
Clinton	46188022	09/01/88	F	F	T	T	0001
Clinton	46191003	02/20/91	T	T	F	F	1057
Grand Gulf	41688006	01/20/88	T	F	T	T	0004
Grand Gulf	41688019	10/10/88	T	F	T	T	0001
Grand Gulf	41690017	09/16/90	T	F	T	T	0003
Grand Gulf	41690028	12/09/90	T	F	T	T	0003
Grand Gulf	41691005	06/17/91	T	T	T	T	0005
Grand Gulf	41691007	07/28/91	T	F	T	T	0005
Grand Gulf	41693008	09/13/93	T	F	T	T	0001
LaSalle 2	37389009	03/02/89	T	T	T	F	4802
LaSalle 2	37489002	01/25/89	T	F	F	F	0002
LaSalle 2	37489007	06/12/89	T	F	F	F	N/A[d]
LaSalle 2	37492003	03/23/92	T	F	F	F	0002
Nine Mile Point 2	41087010	02/02/87	T	F	F	F	0005
Nine Mile Point 2	41088001	01/20/88	T	F	T	T	0005
Nine Mile Point 2	41088012	03/05/88	T	F	T	T	0011
Nine Mile Point 2	41088014	03/13/88	T	F	T	T	0003

Table B-4. (continued)

Plant	LER Number	Event Date	EDG Demand	BKR[a] Closed	Pump Demand	Injection Demand[b]	Run Time[c]
Nine Mile Point 2	41088043	10/08/88	T	F	T	F	0002
Nine Mile Point 2	41089006	02/19/89	T	F	T	F	0002
Nine Mile Point 2	41089014	04/13/89	T	F	T	T	0005
Nine Mile Point 2	41090016	12/02/90	T	F	F	F	0001
Nine Mile Point 2	41091023	12/12/91	T	F	T	T	0001
Nine Mile Point 2	41092006	03/23/92	T	T	F	F	0007
Nine Mile Point 2	41092008	03/27/92	T	F	T	F	0001
Nine Mile Point 2	41092020	09/25/92	T	T	F	F	0307
Nine Mile Point 2	41092023	09/25/92	T	T	F	F	0212
Perry	44087012	03/02/87	T	F	T	T	0003
Perry	44087014	03/05/87	F	F	T	F	0001
Perry	44087064	09/09/87	T	F	T	T	0003
Perry	44087072	10/27/87	T	F	T	T	0003
Perry	44088012	04/27/88	T	F	T	F	0001
Perry	44089014	04/25/89	T	F	F	F	0001
Perry	44090001	01/07/90	T	F	T	T	0026
Perry	44092017	09/10/92	T	F	T	T	0001
Perry	44093012	06/07/93	T	F	T	T	0001
River Bend	45888018	08/25/88	T	T	T	T	UNKN[e]
River Bend	45888021	09/06/88	T	F	T	T	0001
River Bend	45889027	05/28/89	T	F	F	F	0005
River Bend	45893016	07/27/93	T	F	T	F	0003
Wash. Nuclear 2	39787002	03/22/87	T	F	T	T	0015
Wash. Nuclear 2	39789016	05/14/89	T	F	F	F	N/A[d]
Wash. Nuclear 2	39789025	06/17/89	T	F	F	F	0002
Wash. Nuclear 2	39791017	07/08/91	T	F	F	F	N/A[d]
Wash. Nuclear 2	39791032	11/19/91	T	F	T	T	0005
Wash. Nuclear 2	39793019	05/19/93	T	T	F	F	0200

a. The diesel generator breaker received a demand to close.

b. The injection valve received a demand to open.

c. The number listed corresponds to HHMM (e.g., 0105 corresponds to a run time of 1 hour and 5 minutes).

d. A demand was required; however, that portion of the system was out of service for maintenance.

e. The run time of the diesel generator was not specifically stated in the LER. The injection pump ran for less than 1 minute.

B-3. HPCS CYCLIC SURVEILLANCE TESTING DEMANDS

The estimated number of HPCS cyclic surveillance testing demands is summarized by plant in Table B-5. The total number is 42 cyclic surveillance tests. The method used to estimate the number of cyclic tests was discussed previously in Appendix A, Section A-1.2.

Table B-5. Estimated number of cyclic surveillance tests.

Plant Name	Total	Plant Name	Total
Clinton	5	Nine Mile Point 2	5
Grand Gulf	6	Perry	5
LaSalle 1	4	River Bend	4
LaSalle 2	6	Washington Nuclear 2	7
		Total	42

B-4. DATA USED FOR STATISTICAL ESTIMATION OF UNRELIABILITY

The six failures identified in Table B-3 for which a demand count could be determined or estimated were used to estimate unreliability. Table B-6 provides a summary description of the events used to determine system unreliability. The table lists the events alphabetically by plant name.

Table B-6. Summary of the six events used to estimate HPCS unreliability.

Plant Name	LER Number	Date	Failure Mode	Description
LaSalle 2	37389011	03/04/89	FTRD	The Unit 2 system auxiliary transformer tripped as a result of a ground. The transformer is the only offsite power source for ESF bus 243 (Division III). The HPCS diesel was started to power the bus, and the injection pump was started to provide additional load for the diesel. Repairs to the transformer required that the transformer remain de-energized for over two days. The HPCS diesel had provided power to bus 243 for approximately 48 hours when a fuel oil leak developed on two instrument lines as a result of vibration. The diesel was shut down and the instrument lines plugged by mechanical maintenance personnel. The diesel returned to service after the repairs.

Table B-6. (continued)

Plant Name	LER Number	Date	Failure Mode	Description
LaSalle 2	37489007	06/02/89	MOOSD	The Unit 2 HPCS diesel was out of service for maintenance when the fire deluge system for the system auxiliary transformer inadvertently actuated. The transformer was automatically isolated as a result of a subsequent fault. The fault on the transformer resulted in a loss of power to bus 243 (Division III).
Nine Mile Pt. 2	41092006	03/27/92	FTRD	The HPCS diesel generator failed to run during a sequential loss of offsite power event as a result of a loss of service water cooling to the engine. The loss of cooling water was the result of both cooling water supply valves tripping closed on low header pressure. The low header pressure closure of the supply valves was a design feature to project against a header rupture. However, the way in which power was lost caused the system to respond as if both service water supply lines to the HPCS diesel had failed. The loss of service water to the HPCS diesel from a sequential loss of offsite power was not considered in the plant's design bases.
Perry	44088012	04/27/88	MOOSI	An automatic reactor scram occurred as a result of a reactor vessel low water level condition caused by a loss of all operating feedwater pumps. The reactor core isolation cooling system automatically started to restore level. The HPCS system was not available because it had been previously removed from service for pre-planned maintenance.
River Bend	45893013	06/29/93	FTSI	During the performance of a routine surveillance test, the HPCS pump failed to start as a result of a failed over-frequency relay. The relay, which is part of the HPCS pump circuit breaker, tripped the circuit breaker at normal bus frequency when the control switch was placed in the start position. The relay was replaced, and the pump tested satisfactorily.

Table B-6. (continued)

Plant Name	LER Number	Date	Failure Mode	Description
Washington Nuclear 2	39789030	02/10/89	FTRT	The HPCS suction valve from the suppression pool failed to open during the performance of a cyclic surveillance test. Upon investigation by plant personnel, the motor was found running; however, the valve was not moving. They also heard a gear-grinding noise coming from the motor-operator gear box. The motor-operator was replaced. The cause identified in the LER was a failure of the manufacturer to build the operator per design.

Appendix C

Basic Event Failure Probabilities and Unreliability Trends

Appendix C

Basic Event Failure Probabilities and Unreliability Trends

This appendix displays relevant HPCS system counts and the estimated probability of each failure mode, including distributions that characterize any variation observed between portions of the data. It then evaluates whether trends exist in the HPCS system data. Three types of detailed analyses are given: a plant-specific analysis for probability of individual failure modes; an investigation of the possible relation between plant low-power license date and HPCS performance as measured by unreliability, by the frequency of unplanned demands, and by the frequency of failures; and an investigation of whether overall performance as measured by these attributes changed during the seven years of the study.

C1. FAILURE MODE PROBABILITIES

C-1.1 Analysis of Individual Failure Modes

Table C-1 contains results from the initial assessment of data for the five HPCS injection subsystem failure modes and the four HPCS emergency power subsystem failure modes, including point estimates and confidence bounds for each probability of failure. The tables also include the failure to recover probability for the single mode for which potentially recoverable failures occurred. Each entry in the table corresponds to a failure mode in one of the HPCS fault trees. Note that the point estimate and bounds do not consider any special sources of variation (e.g., year or plant). The purpose of Table C-1 is to assist the analyst in understanding the relationships between the different data groupings. Patterns such as trends or outliers become more apparent, if they exist. For example, comparison of the plotted confidence intervals provides a visual indication of the whether the data sets can be pooled.

Table C-2 summarizes the results from testing the hypothesis of constant probabilities or rates across groupings for each failure mode based on data source, plant mode for MOOS, calendar years, and plants. No statistical evidence of differences across these groupings was found in the sparse data. Even MOOS probabilities during operation for the two HPCS subsystems were not significantly lower than the corresponding probabilities during shutdown periods from a statistical point of view. The data were too sparse to show such distinctions.

Sections C-1.1.1 and C-1.1.2 below describe the particular data that were used to estimate the failure probability for each failure mode and the rationale for choosing that data for the HPCS injection and emergency power subsystems. The type of modeling selected to calculate the distributions that characterize sampling and/or between-group variation is also discussed. The resulting distributions are used to compute uncertainty bounds for the unreliability estimates.

Table C-1. Point estimates and confidence bounds for HPCS failure modes.

Failure Mode	Demand Source	Failures *f*	Demands *d*[a]	Probability[b]
Injection subsystem				
Maintenance-out-of-service (MOOSI)	Unplanned, operating	1	29	(0.002, 0.034, 0.153)
	Unplanned, shutdown	0	4	(0.000, 0.000, 0.527)
	Pooled	1	33	(0.002, 0.030, 0.136)
Failure to start, injection valve (FTSV)	Unplanned	0	24	(0.000, 0.000, 0.117)
Failure to start, other than	Unplanned	0	32	(0.000, 0.000, 0.089)
injection valve (FTSI)	Cyclic test	0	43	(0.000, 0.000, 0.067)
	Quarterly	1	224	(0.000, 0.004, 0.021)
	Pooled	1	299	(0.000, 0.003, 0.016)
Failure to run (operational	Unplanned	0	31	(0.000, 0.000, 0.092)
mission) (FTRI-OP)	Cyclic test	0	43	(0.000, 0.000, 0.067)
	Quarterly	0	223	(0.000, 0.000, 0.013)
	Pooled	0	297	(0.000, 0.000, 0.010)
Failure to run (PRA comparison)	Unplanned	0	50.1 h	(0.000, 0.000, 0.06)[c]
(FTRI)	Cyclic test	0	43.0 h	(0.000, 0.000, 0.07)[c]
(Rate)	Quarterly	0	223.0 h	(0.000, 0.000, 0.013)[c]
	Pooled	0	316.1 h	(0.000, 0.000, 0.009)[c]
Failure of automatic transfer function (FTRT)	Cyclic test	1	43	(0.0001, 0.023, 0.106)
Emergency power subsystem				
Maintenance-out-of-service (MOOSD)	Unplanned, operating	1	30	(0.002, 0.033, 0.149)
	Unplanned, shutdown	2	16	(0.023, 0.125, 0.344)
	Pooled	3	46	(0.018, 0.065, 0.160)
Failure to start, output	Unplanned	0	8	(0.000, 0.000, 0.312)
breaker (FTSB)	Cyclic test	0	43	(0.000, 0.000, 0.067)
	Pooled	0	51	(0.000, 0.000, 0.057)
Failure to start, other than	Unplanned	0	43	(0.000, 0.000, 0.067)
output breaker (FTSD)	Cyclic test	0	43	(0.000, 0.000, 0.067)
	Pooled	0	86	(0.000, 0.000, 0.034)
Failure to run (FTRD)	Unplanned	1	73.3 h	(0.001, 0.014, 0.065)[c]
(Rate)	Cyclic test	0	1032.0 h	(0.000, 0.000, 0.003)[c]
	Pooled	1	1105.3 h	(0.00005, 0.001, 0.004)[c]
Failure to recover from failure to run (FRFTRD)	Unplanned	1	1	(0.050, 1.000, 1.000)

a. Except for FTRI and FTRD, for which running time is given.

b. The middle number is the point estimate, *f/d*, and the two end numbers form a 90% confidence interval.

c. A 90% confidence interval for the failure rate was derived based on a Poisson distribution for the occurrence of failures. This rate was used with a total system mission time of 24 hours to derive the upper confidence limits for the probability of FTRI and of FTRD [probability=1-exp(rate*mission time)].

Table C-2. Evaluation of differences between groups for HPCS failure modes.

Failure Mode	Demand Source	P-values for test of variation[a] In Data Sources	In Plant Modes	In Years	In Plant Units	Entities with High Chi-Square Statistics[b]
Injection subsystem						
Maintenance-out-of-service (MOOSI)	Unplanned, operating	—	—	1F	1F	—
	Unplanned, shutdown	—	—	0F	0F	—
	Pooled	—	IF	1F	1F	—
Failure to start, injection valve (FTSV)	Unplanned	—	—	0F	0F	—
Failure to start, other than injection valve (FTSI)	Unplanned	—	—	0F	0F	—
	Cyclic test	—	—	0F	0F	—
	Quarterly	—	—	1F	1F	—
	Pooled	1F	—	1F	1F	—
Failure to run (operational mission) (FTRI-OP)	Unplanned	—	—	0F	0F	—
	Cyclic test	—	—	0F	0F	—
	Quarterly	—	—	0F	0F	—
	Pooled	0F	—	0F	0F	—
Failure to run (PRA comparison) (FTRI) (Rate)	Unplanned	—	—	0F	0F	—
	Cyclic test	—	—	0F	0F	—
	Quarterly	—	—	0F	0F	—
	Pooled	0F	—	0F	0F	—
Failure of automatic transfer function (FTRT)	Cyclic test	—	—	1F	1F	—
Emergency power subsystem						
Maintenance-out-of-service (MOOSD)	Unplanned, operating	—	—	1F	1F	None
	Unplanned, shutdown	—	—	NS	NS	None
	Pooled	—	NS	NS	NS	None
Failure to start, output breaker (FTSB)	Unplanned	—	—	0F	0F	—
	Cyclic test	—	—	0F	0F	—
	Pooled	0F	—	0F	0F	—
Failure to start, other than output breaker (FTSD)	Unplanned	—	—	0F	0F	—
	Cyclic test	—	—	0F	0F	—
	Pooled	0F	—	0F	0F	—
Failure to run (FTRD) (Rate)	Unplanned	—	—	1F	1F	—
	Cyclic test	—	—	0F	0F	—
	Pooled	1F	—	1F	1F	—
Failure to recover from failure to run (FRFTRD)	Unplanned	—	—	All F	All F	—

a. —, not applicable; NS, not significant (P-value >0.05); 0F, no failures (thus, no test); 1F, only one failure (thus, generally too sparse to observe significant differences in failures); All F, no successes (thus, no test).

b. Years and plants with an unusual failure probability (compared to others in the group) are flagged. Unusual means statistically significant at the 10% level, and unless noted otherwise, it was unusually high (versus low).

C-1.1.1 HPCS Injection Subsystem Failure Modes

Maintenance or Testing Out-of-Service. A single MOOSI event occurred among the 29 unplanned HPCS injection subsystem demands during plant operation during the study period. No maintenance unavailabilities were found among four HPCS injection subsystem unplanned demands while the plant was shut down. Although the data show no significant differences between the two plant modes, the MOOSI probability estimate obtained from the operating plant data, excluding the shutdown plant data, was used in this study. The data were not pooled across modes since an engineering/plant operations perspective shows that maintenance generally occurs at a higher rate during shutdown periods. Operating periods are more applicable for the estimates considered in this study. Therefore, the HPCS injection subsystem MOOS data were differentiated by plant mode throughout the reliability analysis.

The operating data were too sparse to identify empirical Bayes distributions describing differences in plants or years. Therefore, the simple Bayes beta distribution describing approximately the same variation as the confidence interval was derived. This distribution was used in the variance propagation to quantify the HPCS injection subsystem MOOS probability.

Failure to Start Injection Valve. Since no failures to start occurred, no empirical Bayes distributions were fitted for the failure to start due to injection valve failure (FTSV). For the reliability assessments, unplanned demand data applicable for FTSV (24 of the 32 events for which the injection subsystem was not in a maintenance outage) were used to form a simple Bayes beta distribution.

The mean of the resulting beta distribution is 0.020, and the 95th percentile is 0.076, which is relatively high. Another approach that was considered but not used in this study was to base the prior distribution for the pooled data on results of the high-pressure core injection (HPCI) system study.[C-1] In the HPCI study, one injection valve failure was observed in 59 demands. The resulting simple Bayes distribution mean was 0.025; whereas the simple Bayes method applied directly to the HPCS data starts with a noninformative prior distribution with a much higher mean— 0.50 (see Section A-2.1.4). The HPCI constrained noninformative prior-based distribution was considered, since just updating the HPCI simple Bayes beta distribution corresponds to treating the HPCI data as though it were 100% applicable HPCS data. That is, the results of updating the HPCI simple Bayes distribution with HPCS data are identical to what would be calculated if one failure were observed in (24+59) demands. Using the wider HPCI distribution for which only the mean is constrained allows the HPCS data a greater influence on the results.

The HPCI injection valve data were not used in this study because the results, with a mean of 0.018 and an upper bound of 0.069, were not significantly different than the results obtained using solely the sparse HPCS data.

Failure to Start, Other Than Injection Valve. As with FTSV, no failures to start from causes other than injection valve failure occurred, and thus no empirical Bayes distribution was fitted. However, the cyclic and quarterly surveillance data are applicable to the FTSI failure mode. The sparse statistical data showed no FTSI performance differences between events from the two types of tests and the 32 unplanned demands. Therefore, the data were pooled to form a simple Bayes distribution for use in the reliability analysis.

Failure to Run, Operational Mission. Each injection subsystem demand for which the injection pump started is potentially an opportunity to assess the success or failure of the system in running for the operational model. One event was excluded, since it was terminated immediately after the pump started. Long run times are not required in this model, nor is the performance of the automatic transfer function for the suction source required. The quarterly and cyclic test data were applicable, since the test run times

are an hour which is much longer than all but one of the operational demands. With no failures, no empirical Bayes distribution estimates apply to the FTRI-OP data. A simple Bayes distribution was calculated for the operational mission using the number of missions among the applicable unplanned demands and quarterly and cyclic testing demands.

Failure to Run, (hourly rate for comparison to PRA). Since short run times precluded the application of the operational data directly to unreliability for the length of mission (24 hours) typically assumed in a risk assessment, an analysis based on failure rates was performed. With no failures, no empirical Bayes distribution estimates apply to the FTRI data. For the assessment, the injection system run times from unplanned demands and from cyclic and quarterly surveillance tests were pooled to form a simple Bayes distribution describing the system rate of failure to run. This was a gamma distribution, since the analysis describes rates. Conversion of the rate to a beta distribution for the probability of failure in a 24-hour mission was completed as described in Section A-2.1.5. The resulting probability had a mean of 0.036, with 0.00015 and 0.14 as the 5th and 95th percentiles of the fitted beta distribution.

Failure of the Automatic Transfer Function. The single cyclic surveillance test failure in the operational data was a failure of the automatic suction source transfer function (FTRT). No unplanned injection subsystem demands lasted long enough to test this function, and it is not tested in the quarterly tests. The 43 cyclic tests and one failure were pooled to estimate a simple Bayes beta distribution to describe the probability of this failure for comparison to the PRA/IPE results.

Failure to Recover Failure Modes. None of the potential failure to recover probabilities for the HPCS injection subsystem (corresponding to all the above failure modes except for MOOSI) were analyzed since there were no demands for this recovery. Since the FTRT failure occurred on a test, problem diagnosis and repair were the focus of the event response, not recovery. The recovery events are left undeveloped in the HPCS fault trees for both the operational unreliability and for comparison to PRAs.

C-1.1.2 HPCS Emergency Power Subsystem Failure Modes

Maintenance Out-of-Service. Three MOOSD events were found among the 46 unplanned demands during the study period that activated the HPCS emergency power subsystem. The events were in the subset of spurious demands for which the HPCS injection subsystem was not demanded. Just one occurred during the total of 30 unplanned demands during plant operations; the other two occurred during the 16 shutdown period unplanned demands. The difference in estimated occurrence probabilities was not statistically significant (P-value=0.23). However, the HPCS emergency subsystem MOOS data were differentiated by plant mode throughout the reliability analysis for the same reason as for this distinction with the injection subsystem. Thus, only the plant operating data for maintenance-out-of-service were used for the unreliability analysis.

Although empirical Bayes distributions for differences in plants and in years were fitted for the overall pooled MOOSD data, no such differences were found for either the plant operating data or the plant shutdown data in the separate data sets. No statistically significant differences were found in any of the MOOSD data sets between plants or between years. Therefore, for the operating data, a simple Bayes distribution was fit to describe the sampling variation.

Failure to Start, Output Breaker. Since no failures to start occurred, no empirical Bayes distribution was fitted for the fail to start, breaker (FTSB) failure mode. The unreliability analysis used the simple Bayes distribution formed from the cyclic test data and the subset of the unplanned demand data for which the diesel output breaker was tested.

Failure to Start, Other Than Output Breaker. As with other failure modes, no empirical Bayes distribution was found for FTSD. For the unreliability analysis, the unplanned demands and cyclic test data were pooled and the simple Bayes beta distribution was used.

In the HPCS diesel analysis, the possibility of using operational data from the system study of emergency diesel generators that parallels this study was considered.[C-2] Updating an informative prior distribution derived from these data might be more realistic and useful than using the Jeffreys non-informative prior distribution. However, this approach was not taken because the startup sequence for the station diesel generators are much more complicated than for the HPCS diesel.

Failure to Run. The single failure to run occurred among the unplanned demands. With only one failure, differences in results from unplanned and cyclic surveillance test demands were not seen, nor were tests for differences between plants or between years significant. As with the injection subsystem, a failure rate analysis was performed in order to apply the data to the 24-hour mission time. This approach allows the results to depend most on the events that accrued the most running time. Among unplanned demands, these were six events for which the diesel output breaker was closed and the diesel was loaded. Even these events, however, contributed little time compared with the 24-hour test cyclic surveillance data. The cyclic surveillances provided 93% of the HPCS diesel running time experience. The cyclic surveillance data were pooled with the unplanned demand data to form the simple Bayes gamma distribution used for the unreliability estimates. Conversion of the rate to a beta distribution for the probability of failure in a 24-hour mission was completed as described in Section A-2.1.5. The resulting probability had a mean of 0.032 with 0.0038 and 0.08 as the 5th and 95th percentiles of the fitted beta distribution.

Failure to Recover from Failure to Run. The emergency power subsystem failure to run occurred among the unplanned demands. It was not recovered. The simple Bayes distribution for one failure in one demand was used for the unreliability estimates.

Other Failure to Recover Failure Modes. The other two failure to recover probabilities, namely, for recovery from FTSD and from FTSB, were not developed because no demands for these recoveries occurred in the very sparse data.

C-1.1.3 Summary of Beta Distributions for Individual Failure Modes

Tables 2 and 3 in the body of the report describe the Bayes distributions selected to describe the statistical variability in the data used to model HPCS injection and emergency power subsystem unreliabilities. Tables 2 and 3 in the body of the report differ from Table C-1 because they give 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 unreliability.

In all cases, the modeled variation is simply sampling variation derived from simple Bayes distributions. Two of the beta distributions were computed from gamma distributions on rates using the methods of Section A-2.1.5. The overall unreliability estimates given in Tables 4 and 5 in the body of the report are the recommended estimates and bounds from the operational data; no plant-specific estimates are given for comparison with PRAs.

C-1.2 Plant-Specific Failure Probabilities

This section exists to provide plant-specific basic event failure probabilities for the failure modes where such variation could be modeled. However, for all HPCS failure modes and data groupings

considered for reliability analysis in this study, the data were too sparse to estimate nondegenerate empirical Bayes distributions. The single instance of fitting empirical Bayes distributions occurred for total emergency power subsystem maintenance unavailabilities (MOOSD). Usage of this data, with both operating and shutdown plant data included, was not deemed reasonable from a systems engineering perspective. Therefore, these empirical Bayes results are not presented. The data were pooled across plants and years to form generic simple Bayes distributions for each failure mode.

C-2. INVESTIGATION OF RELATION TO PLANT LOW-POWER LICENSE DATE

The possibility of a trend in HPCS performance with plant age as measured by a plant's low-power license date was investigated. This evaluation was performed for a plant-specific estimate of the unreliability, for the annual frequency of unplanned demands, and for the annual frequency of failures.

Tables C-3 and C-4 show HPCS unreliabilities by plant, along with the plant low-power license date. Table C-3 shows just the injection subsystem, with relatively short run times and no need for automatic transfer to draw from the suppression pool. Table C-4 includes the contribution from longer operating times (24 hours), and the availability of the emergency power subsystem and the automatic transfer function. To yield unreliabilities that were very sensitive to the plant data, plant-specific failure mode failure probabilities were constructed from the sparse data using constrained non-informative priors as described in Section A-2.1.4 and, for the mission injection and emergency power system run probabilities (FTRI and FTRD), Section A-2.1.5. The resulting updated distributions were combined for each plant as described in Section A-2.2.

Table C-3. HPCS unreliability for the operational mission, by plant, based on diffuse prior distributions and annual data (short run times).[a]

Plant	Low-power License Date	Lower Bound	Mean	Upper Bound
Clinton 1	9/29/86	1.32E-03	5.65E-02	1.82E-01
Grand Gulf	6/16/82	1.59E-03	4.70E-02	1.46E-01
LaSalle 1	4/17/82	2.79E-03	6.82E-02	2.05E-01
LaSalle 2	12/16/83	1.44E-03	6.86E-02	2.22E-01
Nine Mile Pt. 2	10/31/86	1.57E-03	4.64E-02	1.44E-01
Perry	3/18/86	1.27E-02	1.06E-01	2.64E-01
River Bend	8/29/85	2.74E-03	6.64E-02	1.99E-01
Wash. Nuclear 2	12/30/83	1.08E-03	6.28E-02	2.08E-01

a. The upper and lower bounds form a 90% interval. The calculations use a diffuse prior, updated by plant-specific data, for each failure mode. Therefore, the intervals are wide, and the means vary greatly between plants.

Table C-4. HPCS unreliability for the operational mission, by plant, based on diffuse prior distributions and annual data (long run times).[a]

Plant	Low-power License Date	Lower Bound	Mean	Upper Bound
Clinton 1	9/29/86	4.33E-02	1.65E-01	3.35E-01
Grand Gulf	6/16/82	4.14E-02	1.49E-01	2.99E-01
LaSalle 1	4/17/82	4.91E-02	2.13E-01	4.42E-01
LaSalle 2	12/16/83	8.90E-02	2.65E-01	4.87E-01
Nine Mile Pt. 2	10/31/86	3.98E-02	1.43E-01	2.89E-01
Perry	3/18/86	6.72E-02	2.02E-01	3.79E-01
River Bend	8/29/85	4.84E-02	1.74E-01	3.47E-01
Wash. Nuclear 2	12/30/83	1.17E-01	3.17E-01	5.55E-01

a. The upper and lower bounds form a 90% interval. The calculations use a diffuse prior, updated by plant-specific data, for each failure mode. Therefore, the intervals are wide, and the means vary greatly between plants.

As shown on Figure 5 in the main report, a straight line was fitted to the unreliability (shown as dots in the plot), and a straight line was also fitted to log(unreliability). The fit selected was the one that accounted for more of the variation, as measured by R^2, provided that it also produced a plot with regression confidence limits greater than zero. The regression-based confidence band shown as dashed lines on the plots applies to every point of the fitted line simultaneously; it is the band due to Working, Hotelling, and Scheffé, described in statistics books that treat linear regression.

No significant trends were observed in the unreliabilities for the operational estimate or the estimate for comparison to PRAs (the P-values were, respectively, 0.71 and 0.41).

For the unplanned demand and failure frequency analyses, plant-specific event counts for the study period were normalized by the number of years during the study period for each plant. Each of the eight plants had seven plant years of experience. The resulting frequencies were trended against plant low-power license date using basically the same linear regression method as for the unreliabilities. The unplanned demands that were trended were the 23 actual injection events for which the diesel was also demanded (these demands are not spurious actuations of the system). The maintenance events were excluded from the failures.

A detail of the methodology for trending frequencies deserves mention. The log model cannot be used directly when a frequency is zero. Rather than simply use an (arbitrary) fraction of a failure or demand divided by exposure time to estimate a non-zero frequency for these cases, all the data for a particular frequency were adjusted uniformly. The constrained non-informative prior distribution described in Section A-3 was updated with plant-specific data, and the resulting plant-specific mean was used for the frequency. It was strictly positive, and therefore its logarithm was defined. For the HPCS system frequencies, this adjustment effectively added approximately 0.5 to each failure count and, depending on the frequency under consideration, from 0.5 to 1.7 years to each exposure time. (As explained in Section A-3, the exposure time increment is relatively large when industry event counts for a frequency are few.) This process results also in the calculation of 90% Bayesian uncertainty bounds for each frequency.

The results of the failure frequency analysis are shown in Figure 21 in the body of the report. No trends with plant age were found, nor were any significant differences in failure frequencies between plants found for the HPCS system failures.

The analysis of the frequency of unplanned demands for the HPCS system showed significant differences between plants (P-value=0.01). However, the differences did not show a trend with plant age. The linear model with the best fit was a log model; the data were adjusted away from zero with the Bayesian technique described above and in Section A-3. The resulting slope had a p-value of 0.37.

C-3. ANALYSIS BY YEAR, 1987–1993

The analyses of Section C-2 were modified to see if there was a time trend during the period of the study. As in Section C-2, the analyses apply to unreliability and to two frequencies (unplanned demand events per plant year and failures per year).

Table C-5 shows the unreliability by year for the operational model; Table C-6 provides these results for the PRA model that includes the emergency power subsystem. The estimates are obtained in the same manner as in Section C-2, except that the data used to update the constrained non-informative prior for each failure mode are pooled across plants for each calendar year instead of across calendar year for each plant. Each of the seven calendar years had eight plant years of experience. The linear model method to test for a trend was the same as described in Section C-2, except that the time variable was calendar year instead of low-power license date. The slope of the trend was not statistically significant for either HPCS subsystem.

Rates for each calendar year were also analyzed by pooling the data from all the plants during each calendar year. For the unplanned demands, the adjustment described in Sections C-2 and A-3 was used to account for zero frequencies, and logarithmic models were selected to ensure positive trend lines. No trends or significant between-year differences were found for the unplanned demands or for the failure frequency.

Table C-5. HPCS unreliability for the operational mission, by year, based on diffuse prior distributions and annual data.[a]

Year	Lower Bound	Mean	Upper Bound
87	1.56E-03	4.63E-02	1.44E-01
88	1.28E-02	9.54E-02	2.34E-01
89	1.18E-03	5.99E-02	1.97E-01
90	1.22E-03	5.86E-02	1.91E-01
91	1.34E-03	5.51E-02	1.77E-01
92	1.06E-03	6.34E-02	2.11E-01
93	2.61E-03	6.59E-02	1.99E-01

a. The upper and lower bounds form a 90% interval. The calculations use a diffuse prior, updated by year-specific data, for each failure mode.

Table C-6. HPCS unreliability for comparison to PRAs, by year, based on diffuse prior distributions and annual data.[a]

Year	Lower Bound	Mean	Upper Bound
87	4.19E-02	1.51E-01	3.04E-01
88	6.47E-02	1.89E-01	3.52E-01
89	1.38E-01	3.13E-01	5.17E-01
90	4.25E-02	1.65E-01	3.37E-01
91	6.83E-02	2.18E-01	4.15E-01
92	4.06E-02	1.63E-01	3.36E-01
93	4.58E-02	1.67E-01	3.37E-01

a. The upper and lower bounds form a 90% interval. The calculations use a diffuse prior, updated by year-specific data, for each failure mode.

C-4. REFERENCES

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

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

Appendix D

Unreliability Model and Failure Probabilities used for Comparison to PRAs

Appendix D

Unreliability Model and Failure Probabilities used for Comparison to PRAs

The logic model for estimating HPCS unreliability for comparison to PRA/IPEs is shown in Figures D-1 and D-2. Table D-1 provides the failure mode estimates used in the fault tree quantification of the logic model depicted in Figures D-1 and D-2. Table D-2 presents the estimated HPCS unreliability and associated uncertainty intervals resulting from quantifying the HPCS fault tree using the estimates presented in Table D-2. The subsystem unreliabilities are included as well as individual failure mode contributions. The percentages do not add to 100% due to the algebraic approximation for combining the failure modes (see Section A-2.2 for further details of the approximation.

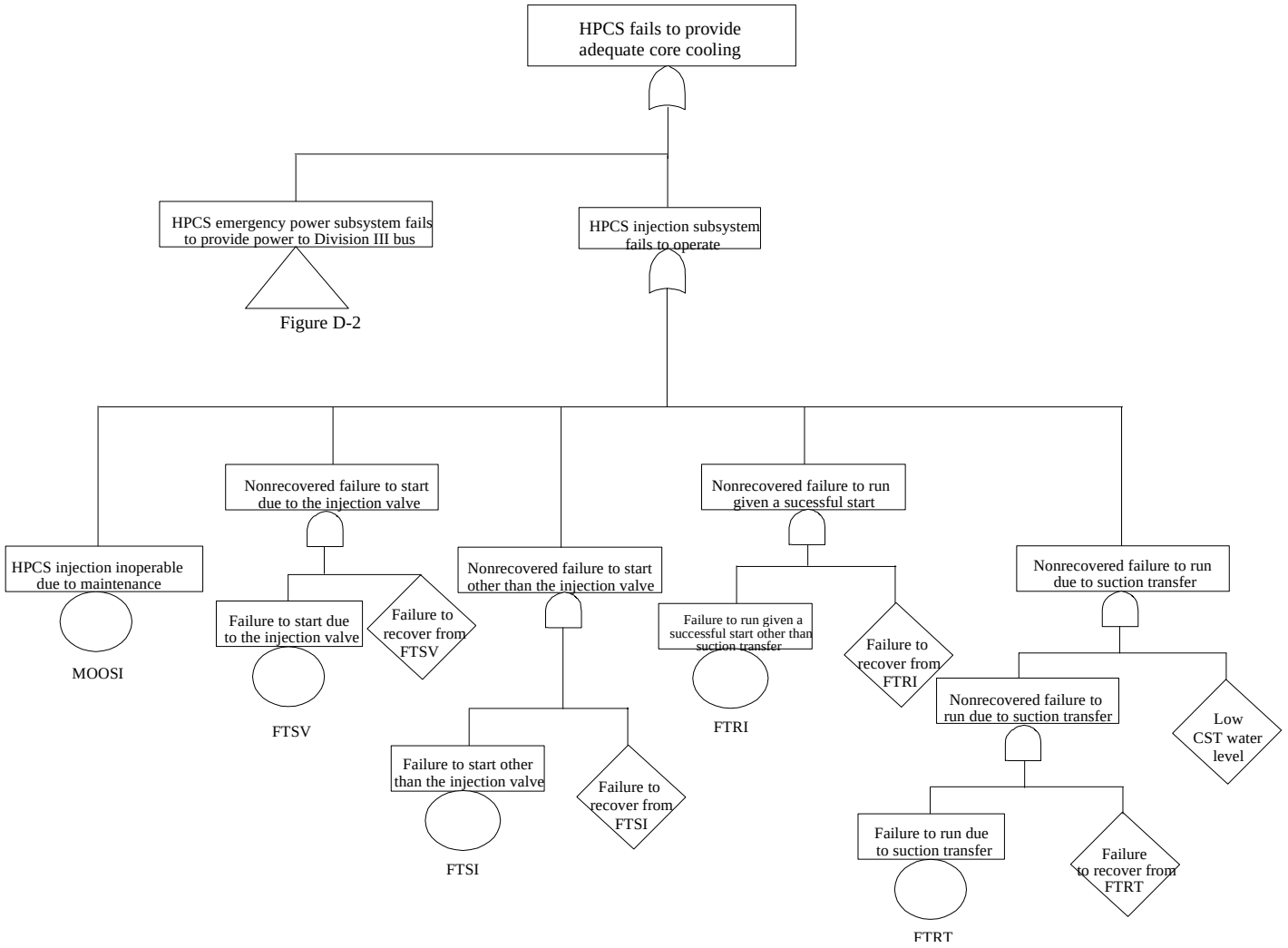


Figure D-1. System fault tree of HPCS injection for calculating HPCS unreliability for comparison with PRA/IPE results.

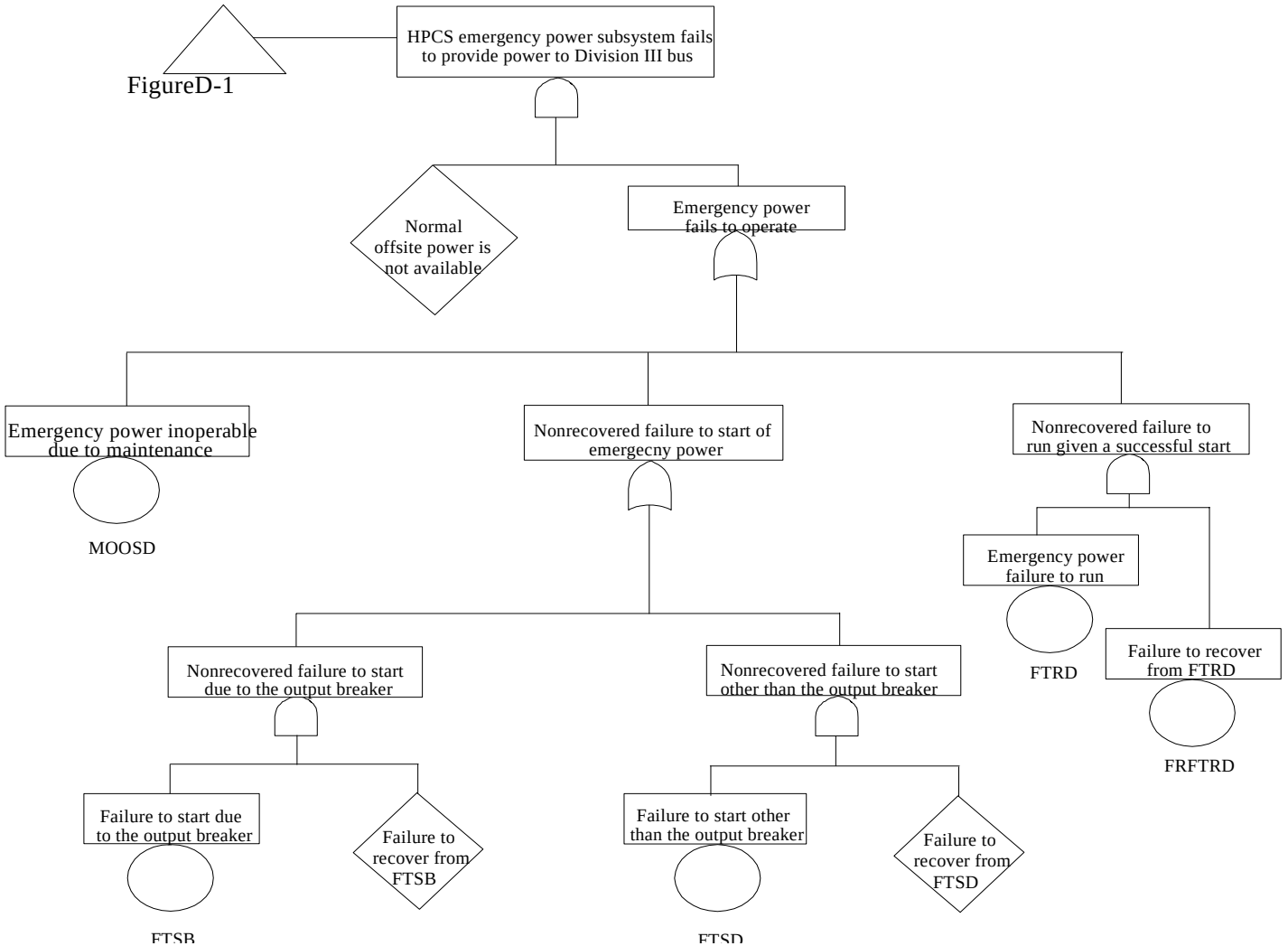


Figure D-2. System fault tree of HPCS emergency power for calculating HPCS unreliability for comparison with PRA/IPE results.

Table D-1. HPCS system failure mode data and Bayesian probability information normalized for comparison to PRA/IPE information.

Failure Mode	f [a]	d [a]	Modeled Variation	Distribution	Bayes Mean and 90% Interval[b]
HPCS injection					
Maintenance-out-of-service while not shut down (MOOSI)	1	29	Sampling	Beta(1.5, 28.5)	(6.1E-3, 5.0E-2, 1.3E-1)
Failure to start other than injection valve (FTSI)	1	299	Sampling	Beta(1.5, 298.5)	(5.9E-4, 5.0E-3, 1.3E-2)
Failure to start, injection valve (FTSV)	0	24	Sampling	Beta(0.5, 24.5)	(8.1E-5, 2.0E-2, 7.6E-2)
Failure to run, suction transfer (FTRT)	1	43	Sampling	Beta(1.5, 42.5)	(4.1E-3, 3.4E-2, 8.7E-2)
Failure to run other than suction transfer (FTRI)	0	316[c]	Sampling	Gamma(0.5, 316) Beta(0.5, 13.4)[d]	(6.2E-6, 1.6E-3, 6.1E-3) (1.5E-4, 3.6E-2, 1.4E-1)[d]
HPCS emergency power					
Maintenance-out-of-service while not shut down (MOOSD)	1	30	Sampling	Beta(1.5, 29.5)	(5.9E-3, 4.8E-2, 1.2E-1)
Failure to start other than output breaker (FTSD)	0	86	Sampling	Beta(0.5, 86.5)	(2.3E-5, 5.8E-3, 2.2E-2)
Failure to start, output breaker (FTSB)	0	51	Sampling	Beta(0.5, 51.5)	(3.8E-5, 9.6E-3, 3.7E-2)
Failure to run (FTRD)	2	1105[c]	Sampling	Gamma(2.5, 1105) Beta(2.5, 45.8)[d]	(5.2E-4, 2.3E-3, 5.0E-3) (1.2E-2, 5.2E-2, 1.1E-1)[d]
Failure to recover from FTRD (FRFTRD)	2	2	Sampling	Beta(2.5, 0.5)	(4.3E-1, 8.3E-1, 1.0E+0)

a. *f* denotes failures; *d* denotes demands.

b. The values in parenthesis are the 5% uncertainty limit, the Bayes mean, and the 95% uncertainty limit.

c. This entry corresponds to the estimated hours of operation.

d. Distributions and estimates for the failure probabilities assuming a 24-hour mission.

Table D-2. Estimates of HPCS unreliability (with recovery and a 24-hour mission time) based on the 1987-1993 experience for PRA/IPE comparisons.

		Contribution (%)	
	Failure Probability	Subsystem	Overall
HPCS injection			
MOOSI	5.0E-2	36	22
FTSI	5.0E-3	4	2
FTSV	2.0E-2	14	9
FTRI	3.6E-2	26	16
FTRT	3.4E-2	24	15
Injection unreliability (mean)	1.4E-1		
90% uncertainty interval	(4.7E-2, 2.6E-1)		
HPCS emergency power			
MOOSD	4.8E-2	48	21
FTSB	9.6E-3	10	4
FTSD	5.8E-3	6	3
FTRD * FRFTRD	4.3E-2	43	19
Emergency power unreliability (mean)	1.0E-1		
90% uncertainty interval	(3.9E-2, 1.9E-1)		
HPCS unreliability (mean)	2.3E-1		
90% uncertainty interval	(1.2E-1, 3.5E-1)		