NUREG/CR-3933
ANL-84-52

NUREG/CR-3933
ANL-84-52

# RISK RELATED RELIABILITY REQUIREMENTS FOR BWR SAFETY-IMPORTANT SYSTEMS WITH EMPHASIS ON THE RESIDUAL HEAT REMOVAL SYSTEM

by

C. P. Tzanos and W. A. Bezella

ARGONNE NATIONAL LABORATORY, ARGONNE, ILLINOIS
Operated by THE UNIVERSITY OF CHICAGO

Prepared for the Office of Nuclear Regulatory Research
U. S. NUCLEAR REGULATORY COMMISSION
under Interagency Agreement DOE 40-550-75

Argonne National Laboratory, with facilities in the states of Illinois and Idaho, is owned by the United States government, and operated by The University of Chicago under the provisions of a contract with the Department of Energy.

## NOTICE

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

## NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W., Washington, D.C. 20555.
2. The NRC/GPO Sales Program, U. S. Nuclear Regulatory Commission, Washington, D.C. 20555
3. The National Technical Information Service, Springfield, VA 22161.

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the NRC/GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U. S. Nuclear Regulatory Commission, Washington, D.C. 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG/CR-3933
ANL-84-52

Distribution
Code: RG

ARGONNE NATIONAL LABORATORY
9700 South Cass Avenue
Argonne, Illinois 60439

# RISK RELATED RELIABILITY REQUIREMENTS FOR BWR SAFETY-IMPORTANT SYSTEMS WITH EMPHASIS ON THE RESIDUAL HEAT REMOVAL SYSTEM

by

C. P. Tzanos and W. A. Bezella

Reactor Analysis and Safety Division

Manuscript Completed: April 1984

Date Published: August 1984

Prepared for the Division of Risk Analysis
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

NRC FIN No. A2242

# RISK RELATED RELIABILITY REQUIREMENTS
# FOR BWR SAFETY-IMPORTANT SYSTEMS
# WITH EMPHASIS ON THE
# RESIDUAL HEAT REMOVAL SYSTEM

by

C. P. Tzanos and W. A. Bezella

## ABSTRACT

The objective of this study was to identify and evaluate the major safety risk parameters of typical reactor safety systems for use in developing a reliability program. This effort was part of a larger research project aiming to evaluate the feasibility and effectiveness of introducing elements of proven reliability programs from other high technology industries into the nuclear industry. As a reference safety system, the Residual Heat Removal (RHR) system of a Boiling Water Reactor (BWR) was selected. A scoping evaluation was also made for a BWR reactor protection system (RPS). Plant information, existing PRA and other relevant analyses, as well as Licensee Event Reports were used as base material for this study. The results of this evaluation indicate that: (1) recovery of faults can have a very significant impact on the reliability requirements, (2) there exists an obvious need for an adequate reliability data base, (3) reliability analyses must be supported by detailed analyses of the plant's response to accident sequences, and (4) the development of effective emergency operating instructions and proper operator training must be one of the major elements of a Reliability Program.

| NRC FIN<br>No. | Title |
|---|---|
| A2242 | Reliability Assurance Program |

## Table of Contents

Table of Contents (cont'd)

## List of Figures

## List of Tables

## ACKNOWLEDGMENTS

The authors wish to thank a number of people who contributed to the preparation of this document. Walt Lipinski, John Marchaterre, Ira Charak, and Steve Halverson of Argonne National Laboratory (ANL) provided suggestions and recommendations relating to various aspects of this document. The guidance and ideas from Armand Lakner, Pat Baranowsky, Gary Burdick and Malcolm Ernst from the Office of Research within the NRC are also gratefully acknowledged. Special thanks are due to Chuck Mueller, the ANL principal investigator, who provided the technical guidance and helpful suggestions throughout this project. Finally, thanks also go to Marsha Mehaffey and Kathy Rank for their typing and assistance in preparing this document.

NOMENCLATURE ➡

## NOMENCLATURE

| | |
|---|---|
| AC | Alternating Current |
| ADS | Automatic Depressurization System |
| ATWS | Anticipated Transient Without Scram |
| BF1 | Browns Ferry Reactor Unit 1 |
| BWR | Boiling Water Reactor |
| CRD | Control Rod Drive |
| CS | Core Spray |
| CST | Condensate Storage Tank |
| DC | Direct Current |
| DFA | Defect Flow Analysis |
| DHR | Decay Heat Removal |
| ECCS | Emergency Core Cooling Water |
| EOI | Emergency Operating Instruction |
| EPRI | Electric Power Research Institute |
| GE | General Electric |
| HCU | Hydraulic Control Unit |
| HPCI | High Pressure Coolant Injection System |
| IREP | Interim Reliability Evaluation Program |
| IRM | Intermediate Range Monitor |
| LER | Licensee Event Report |
| LOCA | Loss of Coolant Accident |
| LOSP | Loss of Offsite Power |
| LPCI | Low Pressure Coolant Injection System |
| LWR | Light Water Reactor |
| MAAC | Mid-Atlantic Area Council |
| MOV | Motor Operated Valve |
| MSIV | Main Steam Isolation Valve |
| NASA | National Aeronautics and Space Agency |
| NRC | Nuclear Regulatory Commission |
| NSAC | Nuclear Safety Analysis Center |
| NSIC | Nuclear Safety Information Center |
| PCS | Power Conversion System |
| PRA | Probabilistic Risk Assessment |
| PWR | Pressurized Water Reactor |
| RCIC | Reactor Core Isolation Cooling |
| RCW | Raw Cooling Water |
| RHR | Residual Heat Removal System |
| RHRSW | Residual Heat Removal System Service Water |
| RPS | Reactor Protection System |
| RPV | Reactor Pressure Vessel |
| SASA | Severe Accident Sequence Analysis |
| SBCS | Standby Coolant Supply |
| SDV | Scram Discharge Volume |
| SERC | Southeastern Electric Reliability Council |
| SIL | Service Information Letters |
| SLC | Standby Liquid Control |
| SRV | Safety Relief Valves |
| TVA | Tennessee Valley Authority |

## Project Overview

The work described herein is part of the Reliability Program research project sponsored by the Division of Risk Analysis, Office of Research, NRC. The overall purpose of this research project is to develop and recommend a program of coordinated reliability engineering and management techniques (i.e., elements) that could interface with on-going industry and regulatory programs to help licensees achieve and maintain an acceptable level of nuclear power plant safety over the lifetime of the plant. The Reliability Program would complement a quality assurance program by establishing the needed reliability levels for structures, systems, components, and operations including procedural and personnel actions important to safety; the QA program would then assure that established procedures to attain these levels are followed.

Prompted by the TMI accident, NRC, DOE, and EPRI have all sponsored studies of aerospace, commercial aircraft, and military programs to understand their approach in optimizing the safety, reliability, and costs of key systems in these programs. NRC staff involved in the Indian Point Hearings, the Salem incident reviews, and ATWS rulemaking have all recommended Reliability Programs with varying descriptions as a potential means for cost-effectively maintaining LWR safety. Recent NRC-sponsored research has identified Reliability Program elements practiced in these other industries as having potential for use in the nuclear industry. Studies to date have made only rather broad generalizations on the benefits or costs of such programs or their activities. The Reliability Program research project discussed here will use these previous recommendations and study results to develop a viable Program and its associated activities, subject this program to detailed evaluation through regulatory analysis and in plant testing, and recommend a final Program that meets the objectives described above.

The research performed to date has been as follows:

(1) Benchmarking the existing regulations and their implementation relevant to reliability assurance and organizing them by life cycle phase, top level reliability assurance function, and material directly auditable by the NRC. This work, documented in a NUREG/CR to be released in mid-1984, allows a basis for comparison with reliability related regulations and their implementation from other safety-critical, high technology programs such as exist in the aerospace, military, and airline industries. It also provides an information base to facilitate future decision-making with respect to integrating reliability-related regulations with existing regulations. It has shown that within the current body of NRC rules, requirements and guidance, a framework already exists in which to integrate, not add, a reliability-based regulatory program. The most obvious missing ingredients are numerical performance standards tied to risk and reliability and standards outlining the degree of detail that reliability studies should have. Regulations on failure reporting and corrective actions are not currently tied to a Reliability Program framework.

(2) The work in this report, namely, determining the risk-dominant attributes of the residual heat removal and reactor trip systems for the Browns Ferry Unit-1 plant from a review of existing PRA informa-

tion for that plant, related LERs, and plant safety literature including emergency procedures. This allows focus on the parameters that govern the unavailabilities of specific, but representative, safety-related systems for nuclear plants so as to indicate the most important aspects of a reliability program. This work confirmed, not surprisingly except perhaps for degree, the dominance of dependent (common cause) failures on risk-important sequences involving complex nuclear systems and highlighted the importance of the operator(s) being able to recover safety functions during an accident.

(3) The development of a preliminary Reliability Program structure and associated activities for the operating phase of a nuclear power plant. This development provides a baseline for subsequent detailed evaluation and value-impact analysis. Previous recommendations of earlier industry and government groups and consultants were factored into this structure. Synopses of current licensee practices and regulatory requirements that address the same safety issues addressed by the Reliability Program were provided. Relevant new industry initiatives or regulatory activities were cited. Finally, preliminary qualitative judgements on potential value-impact were made. This work is documented in a NUREG/CR to be released in mid-1984. The key elements of the Reliability Program model developed for the operation phase are a systems reliability analysis program; a parallel plant/systems performance monitoring program; subprograms that perform the continuous integration of these with Operations and Maintenance requirements and activities; and a distinct subprogram to deal with accident recovery issues.

(4) Support work, as yet unpublished through NUREGs, surveying the most useful related activities in the aerospace, military, and airline industries. This was done by focusing on specific programs or practices, namely NASA's Space Shuttle Main Engine Program, the Navy's Trident Missile Guidance System Program, FAA certification of airframes, and FAA operation of ground control systems. This work was performed by Charles Stark Draper Laboratory (NASA, Navy, and FAA certification) and Reliability Technology Associates (FAA operations) under contract to ANL. The purpose was to identify the reliability activities that could best be integrated with existing plant practices and NRC regulations to enhance overall safety. Significant conclusions were centered on FAA certification and related that certain FAA practices have attractive features which might be applicable to the nuclear industry. These include the use of industry representatives who monitor and approve various production and manufacturing phases; the maintenance practices of the FAA in many aspects, e.g. certification of personnel, FAA/industry interactions, failure experience feedback, and reliability-centered-maintenance; and the anonymous reporting of the "Aviation Safety Reporting System".

On-going and future work will develop a Reliability Program structure and associated activities for the complete lifecycle of a power plant. Regulatory analysis and in-plant demonstration programs will be used to define the content of and tailor these elements so that they are responsive to what licensees feel is most warranted. Of course, the Reliability Program must also meet the NRC's purpose in helping to assure that operating safety is maintained at an adequate level through plant life. Regulatory value-impact analysis will also be used in conjunction with the demonstration program to identify the most cost-effective ways of implementing a Reliability Program, both from an industry and from a regulatory standpoint.

C. J. Mueller
ANL Principal Investigator

## Executive Summary

The Nuclear Regulatory Commission has sponsored a research project at Argonne National Laboratory to develop a pilot reliability program and evaluate the feasibility and effectiveness of its implementation in the nuclear industry. The development of this program will be based on relevant experience from the nuclear industry as well as from other high technology industries like civil aviation, and the industries involved in the NASA and defense department programs. A major objective of the reliability program is to assure by its implementation that reactor systems meet target reliability values allocated to them by a process based on quantitative safety requirements derived from risk considerations. For the purposes of this project the core melt probability was used as the quantitative measure of safety.

For the development of the pilot reliability program the Browns Ferry, Unit 1, Residual Heat Removal system (RHR) was chosen as a reference system. To assure that the information obtained from the analysis of the reference system in developing the reliability program is not strongly biased by this system, some analysis of scoping character was also performed for the BWR reactor protection system (RPS).

This report presents the work performed for Task 1.C of the reliability program research. The objective of this task was to identify from existing PRA and other relevant analyses the parameters that govern the contribution of the reference system to the risk of the reference BWR plant. These parameters will indicate what the major elements of the reliability program for the reference system should be, and what elements and methods of reliability programs from other high technology industries are relevant to important safety issues of the reference system.

The existing analyses that were used as base-material for the purposes of the work presented in this report are: (a) the study performed for Browns Ferry in the context of the Interim Reliability Evaluation Program (IREP), (b) WASH-1400, and (c) two studies performed by the Severe Accident Sequence Analysis (SASA) program for potential accident sequences involving loss of the decay heat removal capability at Browns Ferry. To identify the dominant causes of failure indicated by the operating experience of the BWR RHR system, an effort was undertaken to analyze the Licensee Event Reports (LERs) for this system. Some limited detailed information on plant operation, that was made available at this stage of the project, was also analyzed. This information includes a set of emergency operating instructions for the Browns Ferry station. The brief scoping analysis performed for the RPS of BWRs includes: (a) a review of generic information on the availability of the BWR RPS, on its contribution to the risk from BWRs and on RPS common-cause failures, (b) an analysis of the LERs for the BWR RPS. Finally, since the IREP study performed for Browns Ferry, which at this stage is the only PRA available for this plant, addresses only internal accident initiators, only these initiators are considered in this report.

The IREP study for Browns Ferry estimated a core melt frequency of $1.3 \times 10^{-4}$ for accidents sequences that involve failure of the RHR system. This constitutes about 70% of the estimate for the core melt frequency due to internal accident initiators. About 78% of this contribution was attributed to sequences initiated by events that did not involve loss of offsite power, and the remaining 22% to sequences initiated by loss of offsite power (LOSP). The above estimates were derived from RHR unavailability estimates of 5.7 x $10^{-5}$ and 9.4 x $10^{-4}$ for non-LOSP and LOSP initiating events, respectively. If the core melt frequency of 1.3 x $10^{-4}$, due to accident sequences involving RHR failure, is considered acceptable, the IREP unavailability estimates for RHR can be used as reliability goals. A reliability program for the RHR for the reference plant must demonstrate that throughout its lifetime its RHR system unavailabilities are maintained at levels smaller than or equal to these goals.

In the IREP study, failure of an RHR minimum-flow bypass valve to close was treated as an RHR loop failure. The same study showed that if a failure of an RHR minimum-flow bypass valve to close does not cause failure of its associated loop, the unavailability of decay heat removal is reduced by a factor of 22 for initiating events that do not render the offsite power unavailable. The contribution to the core melt frequency of accident sequences that involve failure of the RHR system and are initiated by non-LOSP events also becomes 22 times smaller. The evaluation of the impact that a bypass valve failure has on system success will affect significantly the required RHR reliability assurance program. If a bypass valve failure to close does not cause loop failure, the RHR reliability is significantly improved, and consequently the burden of proof imposed on the reliability program may be correspondingly relaxed or the RHR safety margin increased.

In the IREP study, no credit was taken for recovery of the Power Conversion System (PCS) in accident sequences initiated by transients that render it unavailable. If the WASH-1400 data for recovery of the PCS is valid for Browns Ferry, the frequency of accident sequences initiated by such transients is reduced by two orders of magnitude. This may relax very significantly the requirements on the unavailability of the RHR system, or improve the existing margin of safety which in turn may reduce the burden of proof on an RHR reliability program. If existing data from Browns Ferry cannot support the WASH-1400 data, but the potential of recovering the PCS with probabilities as the ones given in WASH-1400 is present, a trade-off may exist between RHR unavailability and PCS recovery, which a reliability program must consider.

From the RHR unavailability analysis presented in the IREP study for Browns Ferry, the following dominant contributors have been identified for non-LOSP initiating events. Failure of the shutdown cooling mode is dominated by faulty suction valve isolation signals (49%) and random failures of the same valves (45%). Operator failure to initiate shutdown cooling contributes 5% to the unavailability of this cooling mode. Failure of the torus cooling mode is dominated by: operator failure to initiate torus cooling (32%); double failures involving failure of one RHRSW header and either a RHR system valve failure or one RHR system loop in test or maintenance (25%); other combinations of random hardware failures. RHR valve failures are dominated by control valve circuit failures. Taking credit for recovery from RHR faults reduces the unavailability of decay heat removal by 25%.

In the IREP study, a time window of six to eight hours was considered for recovery of RHR failures. The time interval was based on the available water inventory in the Condensate Storage Tank (CST). The analysis performed in the SASA program shows that the available time interval is about 28 hours. This estimate is based on the expectation that the CST is nearly full of water, and on the capability of the CRD pump to provide the required coolant injection after four hours into the transient. Coolant injection by the CRD pump was ignored in the IREP study. Extending the available time window from eight hours to 28 hours, reduces greatly the probability considered in the IREP study for operator failure to initiate shutdown cooling or torus cooling. The same extension enhances the probability for recovery from RHR and PCS faults. Consequently, assuring that the CST remains always nearly full and a reasonable availability for the CRD pumps, may relieve further the reliability requirements or improve the reliability margin of RHR.

For accident sequences that are initiated by loss of offsite power, the dominant contributors to the unavailability of the RHR system are failure of three or more diesels to start due to common cause, and failure to recover offsite power. Both of these contributors are independent of the RHR system reliability. The core melt frequency due to such accident sequences is strongly dependent on the frequency of unit and site loss of offsite power, the rate for failure of three or more diesels to start, the availability of DC power, and the probabilities for failure to recover offsite power and failed diesel generators. The analysis performed in this work shows that if the probability to recover the PCS is substantial (as in WASH-1400), loss of offsite power events, including station blackout, are the initiators of the top dominant accident sequences that involve failure of the RHR system. The IREP study for Browns Ferry identified the non-LOSP events as the initiators of the top dominant accident sequences.

Recovery of faults can have a very significant impact on the reliability requirements of the RHR system. In the IREP study, no credit was taken for recovery of the PCS and diesel generators, and for the recovery probabilities of the RHR faults that were considered recoverable, no justification was given. A reliability program must develop a data base for and evaluate recovery probabilities.

The analysis performed in the SASA program shows very clearly that a reliability and a PRA analysis must be supported by detailed analyses of the plant's response to risk-significant accident sequences. These analyses identify the prevailing conditions during the accident, the response of all the systems and components involved in the sequence, the timing and sequence of events. From these analyses: the required operator actions can be defined; the probabilities of operator action can be assessed based on the time available, the adequacy of existing procedures, the training provided to the operators, the resources available to the operator. The same analyses determine the time available for system recoveries, and in conjunction with the probabilistic analysis of the accident provide the basis for reliability improvement recommendations.

The analysis of the Emergency Operating Instructions (EOIs) that were made available at this stage of the project, shows that these instructions have a very significant impact on the outcome of severe accident sequences. This impact is especially significant in accident sequences where the available response time for the operator is short, as the case is in the event the high pressure injection systems are unavailable, or offsite power is unavailable. A comparison of the required operator actions dictated by the analyses of the SASA program, with those indicated in the EOIs, shows that due to the lack of proper instructions, the probability of correct operator action becomes very strongly dependent on his training and experience. For the accident sequences that involve LOSP and failure of three or more diesel generators to start (which are among the dominant sequences), with the existing EOIs, the resulting core melt frequencies would be up to one order of magnitude greater than the values resulting from the operator actions indicated by the SASA analysis. The development of effective emergency operating instructions must be one of the major elements of a reliability program and must be based on detailed analyses of systems response to significant accident sequences. The same analyses must be used for proper operator training.

The analysis of operating experience, as presented in the LERs, shows that for RHR components about 54% and 61% of the events (other than instrument drift) reported from all BWRs and from the three Browns Ferry Units, respectively, were multiple failures or had the potential to be multiple failures. These failures were attributed to design, manufacturing, fabrication, installation and personnel errors, or procedural deficiencies. In the RHR reliability analysis performed in the Browns Ferry IREP study, from the different potential multiple failures only some personnel errors were accounted. The LER analysis of this report suffers from the limitations of the LER reporting system. A more complete analysis could be performed if the LER information was supplemented with information from plant records, and inputs from experts involved in the design, manufacturing, installation, operation and maintenance of the system considered. An adequate system of recording and analyzing operating experience, and using its results to assess system reliability, should be one of the major elements of a reliability program.

The brief scoping analysis performed for the RPS shows the following: The estimates of the unavailability of the BWR RPS presented in the literature vary greatly from $6.7 \times 10^{-7}$ to $1 \times 10^{-4}$ failures per demand (median values). The dominant contributors to this unavailability are: (a) failure of a sufficient number of control rods to insert, (b) common cause failures due to human error, and (c) failure of the scram discharge volume. The estimates of their contribution to the RPS unavailability vary significantly.

The estimates of the frequency of accident sequences that are characterized by failure to scram also vary greatly from $3 \times 10^{-7}$ to $2 \times 10^{-4}$. The estimates for their contribution to the BWR core melt probability cover the range from 2% to 91%.

The above wide variations are due to the lack of adequate experience data on RPS failures and transient frequencies during the lifetime of a BWR, and especially to inadequate data and analytic models for common-cause failures, including failures due to human error.

The scoping analysis of the RPS LERs shows that multiple failures, or potential multiple failures due to design, manufacturing, fabrication, installation and personnel errors, as well as procedural deficiencies were responsible for: ~ 50% of the instrumentation channel events (drift not counted), ~ 30% of the logic channel events, ~ 50% of the hydraulic control unit events, 100% of the scram discharge volume events, ~ 53% of the control rod drive mechanism events, and 100% of the control assembly events.

The above results stress further the need of an adequate data base derived from nuclear power plant operating experience. This need is more acute for common cause failures.

## 1.0 Introduction

The Nuclear Regulatory Commission in its efforts to improve current regulatory practices has proposed the adoption of qualitative safety goals supported by provisional numerical guidelines[1]. These goals and guidelines are based on the concept of measuring nuclear power plant safety under accident conditions with the risk resulting from such conditions. The risk from the operation of a nuclear power plant is a function of the reliability of its systems, the adequacy of the operational procedures used, and the reliability of the human factor involved in its operation. The Nuclear Regulatory Commission has sponsored a research project at Argonne National Laboratory to develop a pilot reliability assurance program and evaluate the feasibility and effectiveness of its implementation in the nuclear industry. The development of this program will be based on relevant experience from the nuclear industry, as well as from other high technology industries like the civil aviation, and the industries involved in NASA and Department of Defense programs. An objective of the reliability assurance program is to assure by its implementation, that reactor systems meet target reliability values allocated to them by a process based on quantitative safety requirements derived from risk considerations. For the purposes of this project, the core melt probability is used as the quantitative measure of safety.

For the development of the pilot reliability assurance program, the Browns Ferry, Unit 1, has been chosen as a reference plant. Probabilistic risk assessments that have been performed for BWR plants show that the risk from the operation of these plants is dominated by accident sequences involving either failure of the decay heat removal systems, or failure of the reactor protection system (failure to scram). The IREP study for Browns Ferry[2], Unit 1, concluded that "the RHR system is the most risk-critical system at BF1." In this work, the Browns Ferry, Unit 1, residual heat removal (RHR) system was chosen as a reference system. To assure that the pilot reliability assurance program will not be strongly biased by the reference system, some analysis of scoping character was also performed for the BWR reactor protection system (RPS).

This report presents the work performed for Task 1.C of the reliability assurance program research performed at Argonne National Laboratory. The objective of this task was to identify, using information from existing reactor probabilistic risk assessments (PRAs) and other relevant analyses, the parameters that govern the contribution of the reference system to the risk of the reference plant. These parameters will indicate what the major elements of the reliability assurance program for the reference system should be, and what elements and methods of reliability assurance programs from other high technology industries are relevant to important safety issues of the reference system.

The existing studies that were used as base-material for the objectives of Task 1.C are: (a) the IREP study performed for Browns Ferry, Unit 1, (b) the Reactor Safety Study (WASH-1400)[3], and (c) two studies performed by the Severe Accident Sequence Analysis (SASA) program[4,5] for potential accident sequences at Browns Ferry involving loss of the decay heat removal capability.

The PRA analysis of the IREP study for Browns Ferry did not consider extensively details of plant design and operation. Such details can have a very significant impact on risk and consequently should be scrutinized by a reliability assurance program. The detailed information on plant design and operation that was made available at this stage of the project is very limited. This information includes a set of emergency operating instructions for the Browns Ferry Station. These instructions were reviewed and an assessment has been made of their impact on the core melt probability.

Data from operating experience of nuclear power plants provides the raw material for the development of failure rate data bases, and for the identification of the dominant causes of component and system failures. Consequently, the analysis of operating experience data provides the basis of determining the reliability of systems, and where a reliability assurance program should concentrate its efforts in order to achieve its objectives. To identify the dominant causes of failure indicated by operating experience, an analysis of scoping character of the Licensee Event Reports (LERs) for the BWR RHR and RPS systems was performed.

This report is organized as follows. In Section 2, a brief description of the reference system and its functional testing and maintenance requirements is presented. The parameters that govern the risk significance of the reference system, as they evolve from analytic studies, are discussed in Section 3. The analysis of the Licensee Event Reports for the BWR RHR system is presented in Section 4.0. The risk related requirements imposed on a reliability assurance program for the reference system are discussed in Section 5.0. The analysis performed on the RPS system is presented in Appendix A. Finally, some RAP-important conclusions drawn from a NSAC study of emergency cooling systems are presented in Appendix B.

## 2.0 Reference Residual Heat Removal System

This section gives a brief description of the reference RHR system, of its functional, testing and maintenance requirements, based on information provided by the Browns Ferry Final Safety Analysis[6] report and by the IREP study for Browns Ferry.

The RHR system provides low pressure water to the reactor to insure coolability of the core during LOCAs and transient events, as well as after normal reactor shutdowns. It is the only system (other than the main condenser associated with the power conversion system (PCS)) which is designed to remove the reactor's residual heat directly to the river.

### 2.1 System Description

The RHR system consists of four pumps, four heat exchangers, associated piping, valves, controls and instrumentation. It is arranged into a two loop configuration. Each loop has suction lines, two sets of a pump and a heat exchanger combination, and discharge lines. The RHR loops take suction from the reactor recirculation loop A, or from the pressure suppression pool. A simplified drawing of one RHR loop is shown in Fig. 2.1.

The RHR system operates in four modes: (a) the low pressure coolant injection (LPCI) mode, the shutdown cooling mode, the pressure suppression pool cooling mode, and the standby coolant supply (SBCS) system mode. Depending on the mode of RHR system operation, the RHR loops discharge water to the reactor, the containment sprays, or to the pressure suppression pool cooling headers. In Fig. 2.1, the valves are shown in their normal position for operation in the LPCI mode with the pump suction aligned to the suppression pool.

The LPCI mode takes water from the pressure suppression pool and pumps it into the reactor recirculation discharge piping. The shutdown cooling mode takes water from the recirculation Loop A, cools it in the heat exchangers, and returns it to the reactor via the same discharge path as the LPCI mode. The pressure suppression pool cooling mode takes water from the pressure suppression pool, cools it in the heat exchangers, and returns the water to the

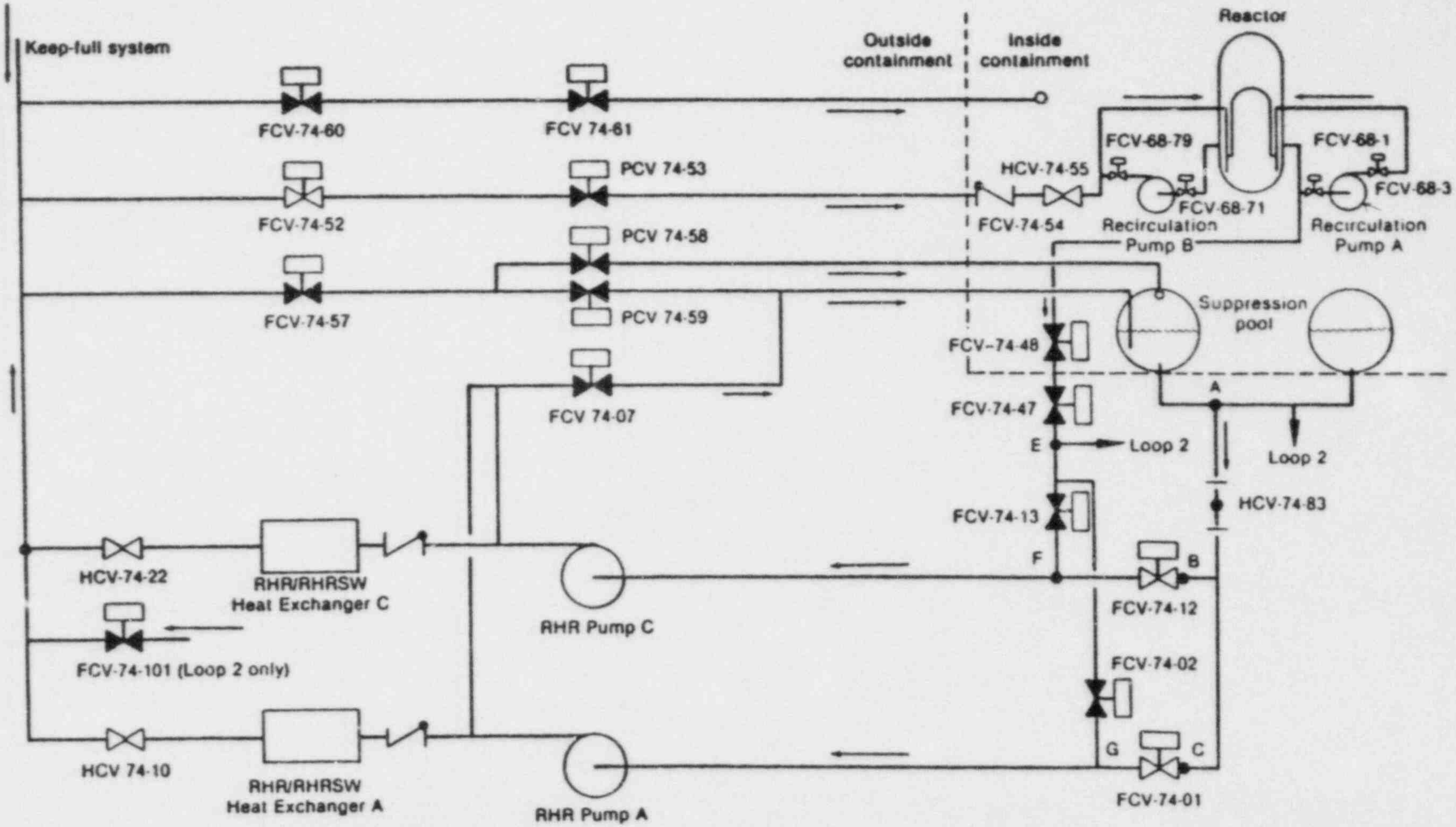


Figure 2.1 RHR System, Loop 1

pool either through the pressure suppression pool spray or through the pressure suppression pool recirculation lines. The SBCS mode is a "last resort" mode, which uses the residual heat removal service water (RHRSW) pumps to pump water from the river into the reactor via the LPCI discharge line of Loop 2.

The RHR system interfaces with: AC and DC power, the logic initiation circuitry, the keep-full system, the emergency equipment cooling water (EECW) system, the raw cooling water (RCW) system, and the residual heat removal service water system. The logic circuitry provides automatic initiation signals and protective interlocks to prevent overpressurization of the RHR system. It also provides automatic isolation signals to the containment cooling isolation valves and the shutdown cooling suction valves to prevent diversion of water from the reactor during operation of the LPCI mode. The RCW system and the EECW system provide room and pump seal cooling. To prevent damage from water hammer when the pumps start, the keep-full system insures that the discharge piping of the RHR loops are filled with water. Finally the RHRSW system provides cooling of the RHR heat exchangers.

## 2.2 Functional Requirements

The RHR system in its various modes of operation is designed to accomplish the following functions in the event of a LOCA or a transient:

a) restore and maintain the reactor vessel water level to prevent fuel damage,

b) remove the heat released to the suppression pool either through line breaks within the containment, or directly from the reactor vessel after safety/relief valve operation,

c) limit the long term pressure and temperature rise within the containment,

d) provide long-term shutdown cooling of the reactor and suppression pool.

The LPCI mode of operation provides restoration of reactor vessel water level after the vessel pressure has dropped below 450 psig. The shutdown cooling mode provides core cooling by circulating the reactor coolant through the RHR heat exchangers, after water level has been restored. The torus cooling mode provides pressure suppression pool and containment cooling. The SBCS mode, as previously mentioned, is a "last resort" mode, which uses the RHRSW pumps to pump water from the river into the reactor via the LPCI discharge line of loop 2.

The success criteria for the different RHR modes of operation, as defined in the IREP study for Browns Ferry, are shown in Table 2.1.

## 2.3 System Operation

Except from the LPCI mode which is initiated automatically, all the other modes are initiated manually by the operator. The RHR system is normally in a "ready" LPCI state with the valves aligned as in Fig. 2.1. The LPCI mode is initiated by either a low reactor vessel water level signal (378.0") or a high drywell pressure signal (+2 psig) both coincident with a low reactor vessel pressure signal. Each of these signals is generated from four separate sensors arranged in a one-out-of-two-taken-twice logic. The LPCI initiation signal causes closure of the containment cooling isolation valves (FCV-74-60, 61, 57 and 59) if open, and prevents their opening for 5 minutes after receipt of the signal. The initiation circuitry also isolates (if they were open at the time) the recirculation pump discharge valves (FCV-68-79 and 3) and the shutdown cooling suction valves (FCV-74-47 and 48). In the torus cooling mode, the operator must start the RHRSW pumps and the RHR pumps, and align the discharge valves to the desired flow path. In the shutdown cooling mode, the operator must start the RHRSW pumps, align the suction valves of the desired RHR loop to the recirculation loop A, start a RHR pump, and align the discharge valves (same as in the LPCI mode) to the desired recirculation loop discharge path.

Table 2.1. RHR System Operational Mode Success Criteria

| Mode of Operation | Success Criteria | Event |
|---|---|---|
| LPCI | Two RHR pumps deliver rated flow to the core | Large suction break |
| LPCI | Four RHR pumps deliver rated flow to the core | Large suction break<br>Large steam break |
| LPCI | One RHR pump delivers rated flow to the core | Large discharge break, large steam break, intermediate breaks, small breaks, transients |
| Shutdown Cooling | One pump-heat exchanger train is operable | All |
| Torus Cooling | Two pump-heat exchanger trains are operable | All |
| SBCS | One RHRSW pump delivers rated flow to the reactor through RHR Loop 2 | Transients |

## 2.4 Testing and Maintenance

Periodic testing of the RHR system and its control systems is required by the relevant technical specifications. Table 2.2 summarizes the RHR system tests, their frequency, the affected components, their expected outage time, and the resulting unavailabilities as determined by the IREP study for Browns Ferry. Scheduled maintenance (i.e., other than that initiated to restore already failed components) is performed periodically and can render portions of the RHR system unavailable. Table 2.3 summarizes such maintenance requirements, their frequency, their expected duration, and the resulting unavailabilities as determined in the IREP study for Browns Ferry.

## 2.5 Technical Specification Limits

The BF technical specifications require that the RHR system be operational prior to reactor startup. If one pump (LPCI mode) is inoperable, operation may continue for seven days provided that all other RHR pumps (LPCI mode), the core spray system, and the diesel generators are demonstrated to be operable. If two RHR pumps (LPCI mode) are inoperable, the reactor must be in the cold shutdown mode within 24 hours. If any containment cooling mode path is inoperable, the reactor may continue operation for seven days provided that at least one path for each mode (drywell spray, torus spray, and torus cooling) is operable. Otherwise, the reactor must be in the cold shutdown mode within 24 hours.

Table 2.2. RHR System Test Requirements Summary (from IREP study for Browns Ferry Unit 1)

| Component Undergoing Test | Type of Test | Expected Test Frequency | Expected Test Outage Time | Unavailability |
|---|---|---|---|---|
| RHR Loop 1 | Auto-initiation test (logic test) | Once every 6 months | 4 hr | $\bar{A} = \frac{4\text{ hr}}{(720)(6)} = 0.000913$ |
| RHR Loop 2 | Auto-initiation test (logic test) | Once every 6 months | 4 hr | Same as above; Technical Specifications require loops be tested at different times |
| Loop flow instrumentation (for minimum-flow bypass valve input) | Sensor calibration | Once every operating cycle | 2 hr per instrument | $\bar{A} = \frac{2\text{ hr}}{(8760)(1.5)} = 0.000152$ |
| Reactor low pressure sensor (for shutdown cooling interlock) | Sensor calibration | Once every month | 1.5 hr per instrument | $\bar{A} = \frac{1.5\text{ hr}}{720} = 0.0021$ |

Table 2.3 RHR System Maintenance Summary (from IREP study for Browns Ferry, Unit 1)

| Maintenance Requirement | Frequency | Duration | Unavailability |
|---|---|---|---|
| RHR pump oil Change A<br>B<br>C<br>D | Once every year | 4 hr | Only one pump at a time<br>$\bar{A} = \frac{4\text{ hr}}{8760} = 0.000456$ |
| RHR Pump seal heat exchanger clean-out | Once every operating cycle | 4 hr | Only one heat exchanger at a time<br>$\bar{A} = \frac{4\text{ hr}}{(8760)(1.5)} = 0.000304$ |

# 3.0 Residual Heat Removal System Risk Significance

## 3.1 Analysis of Information from WASH-1400 and the Browns Ferry IREP Study

To determine the parameters that dominate the risk contribution of accident sequences involving the RHR system of Browns Ferry, Unit 1, using information from existing reactor probabilistic risk assessments, the IREP study for Browns Ferry, Unit 1, and WASH-1400 were used as base-material. This section presents the results of the work performed using this base-material. More specifically, this section discusses: (a) the contribution of the RHR system to the core melt frequency, (b) transient initiator frequencies, (c) RHR unavailability, (d) recovery of the power conversion system, and (e) risk-significant issues in accident sequences that involve failure of the RHR system.

### 3.1.1 Residual Heat Removal System Contribution to the Core Melt Frequency

The Reactor Safety Study (WASH-1400), and the IREP study performed for the Browns Ferry, Unit 1, concluded that the dominant accident sequences, for the BWRs analyzed in these studies, are due to transients characterized either by reactor scram failure or by failure of the decay heat removal systems. The dominant accident sequences identified in the IREP study for Browns Ferry are presented in Table 3.1. They are initiated by transients which involve either failure of the power conversion system ($T_U$ transients), or do not render the power conversion system unavailable ($T_A$ transients), or by loss of offsite power ($T_p$ transients). The failures following the initiating event include: (a) failure of decay heat removal ($R_BR_A$), (b) failure to scram (B), (c) failure of the safety relief valves to close (K), and (d) failure of the recirculation pumps to trip (M). A brief description of these sequences is as follows.

Table 3.1. Dominant Accident Sequences (IREP)

| Sequence Initiator | Designator | Frequency |
|---|---|---|
| Transients without the PCS | $T_UR_BR_A$ | $9.7 \times 10^{-5}$ |
| Loss of offsite power | $T_PR_BR_A$ | $2.8 \times 10^{-5}$ |
| Transient-induced LOCAs | $T_AKR_BR_A$ | $3.7 \times 10^{-6}$ |
| Transients without the PCS-Failure to Scram | $T_UB$ | $5.1 \times 10^{-5}$ |
| Transients with the PCS-Failure to Scram | $T_ABM$ | $3.7 \times 10^{-6}$ |

Transients without the Power Conversion System (PCS) and with Decay Heat Removal (DHR) Failure ($T_U R_B R_A$). In this sequence, the initiating event renders the PCS unavailable as a heat sink. The reactor is successfully shut down. However, failure of the RHR system in the shutdown cooling mode ($R_A$) and in the torus cooling mode ($R_B$) leads to core cooling failure and core melt.

Loss of Offsite Power with DHR Failure ($T_p R_B R_A$). Loss of offsite power initiates a transient that renders the PCS inoperable. The reactor is successfully shut down. Failure of decay heat removal ($R_B R_A$) leads to core melt.

Transients with the PCS Available, Failure of the Safety Relief Valves and DHR ($T_A K R_B R_A$). In this sequence, the PCS is available. The reactor is successfully shut down. The relief valves open successfully for reactor vessel depressurization, however, one or more of them fail to reclose. This leads to loss of coolant through the open valve(s) to the torus. Failure of decay heat removal leads to core melt.

Transients with the PCS Unavailable and Failure to Scram ($T_U B$). In these transients, the PCS is unavailable as a heat sink. The reactor pressure rises until the relief valves open to pass steam from the reactor to the torus. Since scram has failed, the power generation and consequently the steam generation are high. The rate of coolant loss through the relief valves is higher than the makeup rate of the high pressure core cooling systems. The water level in the reactor vessel steadily decreases, and finally core melt occurs.

Transients with the PCS Available, Failure to Scram, and Failure of Recirculation Pump Trip ($T_A BM$). In this sequence, the PCS is available. However, due to scram failure and failure to trip the recirculation pumps, the power level remains above the bypass valve capacity of 30% full power. Thus, the condenser cannot provide adequate core cooling. The reactor pressure rises and the relief valves open to dump steam into the torus. Failure to provide core cooling at the prevailing high power level leads to core melt.

These accident sequences give a total core melt frequency for Browns Ferry, Unit 1, of $1.8 \times 10^{-4}$. WASH-1400 estimated a core melt frequency of $3.0 \times 10^{-5}$ for the Peach Bottom BWR power plant. As discussed earlier, core melt is due either to RHR system failures (failure to remove decay heat) or to reactor protection system failures. The contribution of these two failure categories to the core melt frequency as compared to WASH-1400 is:

| | | |
|---|---|---|
| RHR | Browns Ferry IREP | 70% |
| RPS | Browns Ferry IREP | 30% |
| RHR | WASH-1400 | 57% |
| RPS | WASH-1400 | 34% |

Both studies (IREP and WASH-1400) show that failure of decay heat removal provides the largest contribution to the core melt frequency. However, the core melt frequency estimated in the IREP study is six times higher than the estimate given in WASH-1400, and the contribution of decay heat removal failure to the core melt frequency is significantly higher than the contribution estimated in WASH-1400. The differences in the core melt frequencies estimated in the IREP study and in WASH-1400 are due to differences in: (a) the frequencies of the transient initiators, (b) the unavailabilities of decay heat removal systems, and (c) the recovery probabilities of the power conversion system.

### 3.1.2 Transient Initiator Frequencies

The transient initiator frequencies used in the IREP study are those estimated in EPRI NP-801[7] for Browns Ferry, Unit 1. These frequencies, as well as the frequencies estimated in EPRI NP-801 for all BWRs, and the frequencies used in WASH-1400 are given in Table 3.2. The transient frequencies in Browns Ferry, Unit 1, are smaller than those used in WASH-1400. Especially, the frequency for loss of offsite power is an order of magnitude smaller than the frequency used in WASH-1400.

In EPRI NP-801, one LOSP event is reported for Browns Ferry 1 and another one for Browns Ferry 2. The LOSP in Unit 1 occurred while the power level was below 25%. EPRI NP-2230[8], which is an update of EPRI NP-801, reports an additional LOSP event for Browns Ferry 1. This event occurred while the power level was over 25%. Thus, three LOSP events have been reported by EPRI for all Browns Ferry units. The data reported in EPRI NP-2301[9] shows that none of these events was a LOSP for all three units. Using the EPRI NP-801 methodology, the

Table 3.2. Transient Initiator Frequencies

| | Frequencies (events/year) | | |
|---|---|---|---|
| | Browns Ferry 1[a] | BWRs[a] | WASH-1400 |
| 1. Transients that render the PCS unavailable | | | |
| a. MSIV closure | 0.58 | 0.24 | |
| b. Loss of normal condenser vacuum | 0.56 | 0.41 | |
| c. Pressure regulator fails open | 0.00 | 0.25 | |
| d. Loss of feedwater flow | 0.51 | 0.17 | |
| e. Loss of offsite power[b] | 0.03 | 0.11 | |
| f. Loss of auxiliary power | 0.00 | 0.03 | |
| g. Increased feedwater flow at power | 0.05 | 0.18 | |
| Total | 1.73 | 1.39 | 3.0 |
| 2. Transients that do not render the PCS unavailable | | | |
| a. Electric load rejection | 1.02 | 0.74 | |
| b. Electric load rejection with bypass failure | 0.00 | 0.00 | |
| c. Turbine trip | 0.58 | 0.77 | |
| d. Turbine trip with bypass failure | 0.00 | 0.00 | |
| e. Inadvertent closure of one MSIV | 0.00 | 0.10 | |
| f. Pressure regulator fails closed | 0.00 | 0.11 | |
| g. Bypass/control valve fails causing pressure increase | 0.05 | 0.25 | |
| h. Recirculation control fails causing increased flow | 0.03 | 0.10 | |
| Total | 1.68 | 2.07 | 7.0 |

[a] from EPRI NP-801

[b] WASH-1400 estimate = 0.2 events/reactor-year

above three events give a LOSP frequency of 0.10 events per reactor year for LOSP events that affect only one unit. This frequency is three times higher than the frequency used in the IREP study. For LOSP events that affect all three units, a frequency of 0.131 per site year was derived in EPRI NP-2301 assuming that one event occurred immediately after the end of the data collection period analyzed in this report. The same report has estimated a frequency of 0.122 LOSP events per site year by pooling together the data from all reactor sites.

### 3.1.3 Residual Heat Removal System Unavailability

The RHR system unavailabilities estimated in the IREP study for Browns Ferry, Unit 1, and in WASH-1400 for the Peach Bottom BWR are given in Table 3.3. The IREP estimates refer to failure of the RHR in the shutdown and torus cooling modes. The WASH-1400 estimates refer to failure of either the low pressure coolant injection system or the high pressure service water system.

The shutdown ($R_A$) and the torus ($R_B$) cooling modes have some common components and support systems. In the IREP study, failure of both modes for transients with offsite power available and for "loss of offsite power" events was modeled as shown in the reduced fault trees of Figs. 3.1 and 3.2, respectively. In these trees no credit was taken for operator action to restore faults. The faults were divided into two categories. The independent faults are those that do not cause failure of both systems. The common faults cause failure of both systems. Close examination of the dominant minimum cut sets shows that some failures considered as independent in the reduced fault trees of Figs. 3.1 and 3.2, are not strictly independent. For example, operator failure to initiate the shutdown cooling mode is treated as independent of the operator failure to initiate the torus cooling mode. Dominant minimum cut sets that lead to shutdown cooling mode failure, have common components with dominant minimum cut sets that cause failure of the torus cooling mode. A quick examination of such commonalities indicates that their effect may not be significant.

Table 3.3. Residual Heat Removal System Unavailabilities

| | |
|---|---|
| Browns Ferry, Unit 1, IREP | |
| Offsite Power Available, No Recovery | $7.6 \times 10^{-5}$ |
| Offsite Power Available, Recovery | $5.7 \times 10^{-5}$ |
| Loss of Offsite Power, No Recovery | $4.9 \times 10^{-2}$ |
| Loss of Offsite Power, Recovery | $9.4 \times 10^{-4}$ |
| WASH-1400 | |
| Offsite Power Available | $2.3 \times 10^{-4}$ |
| Loss of Offsite Power | $2.3 \times 10^{-4}$ |

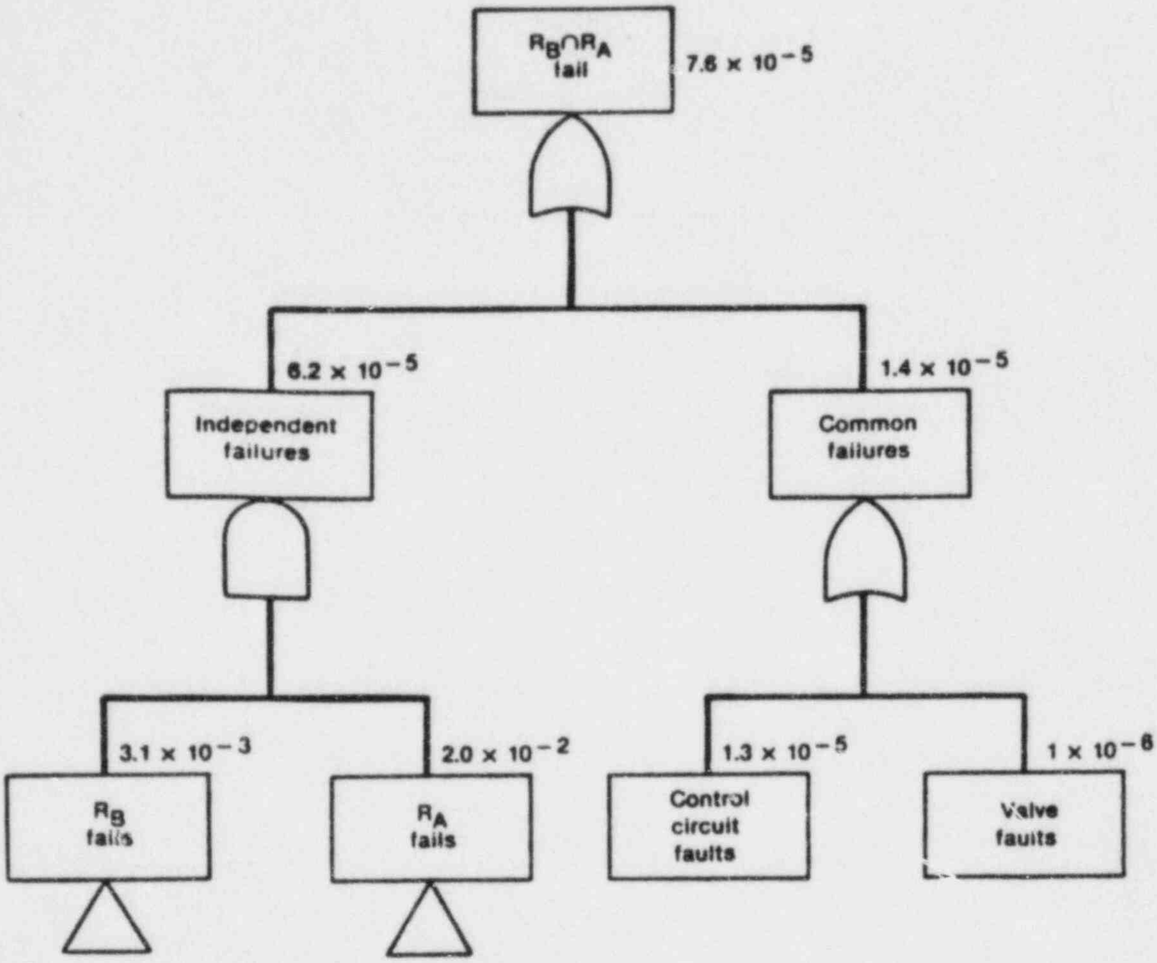


Figure 3.1 Reduced Fault Tree for RHR System Modes $R_A$ and $R_B$ - Normal Power is Available at Transient Initiation

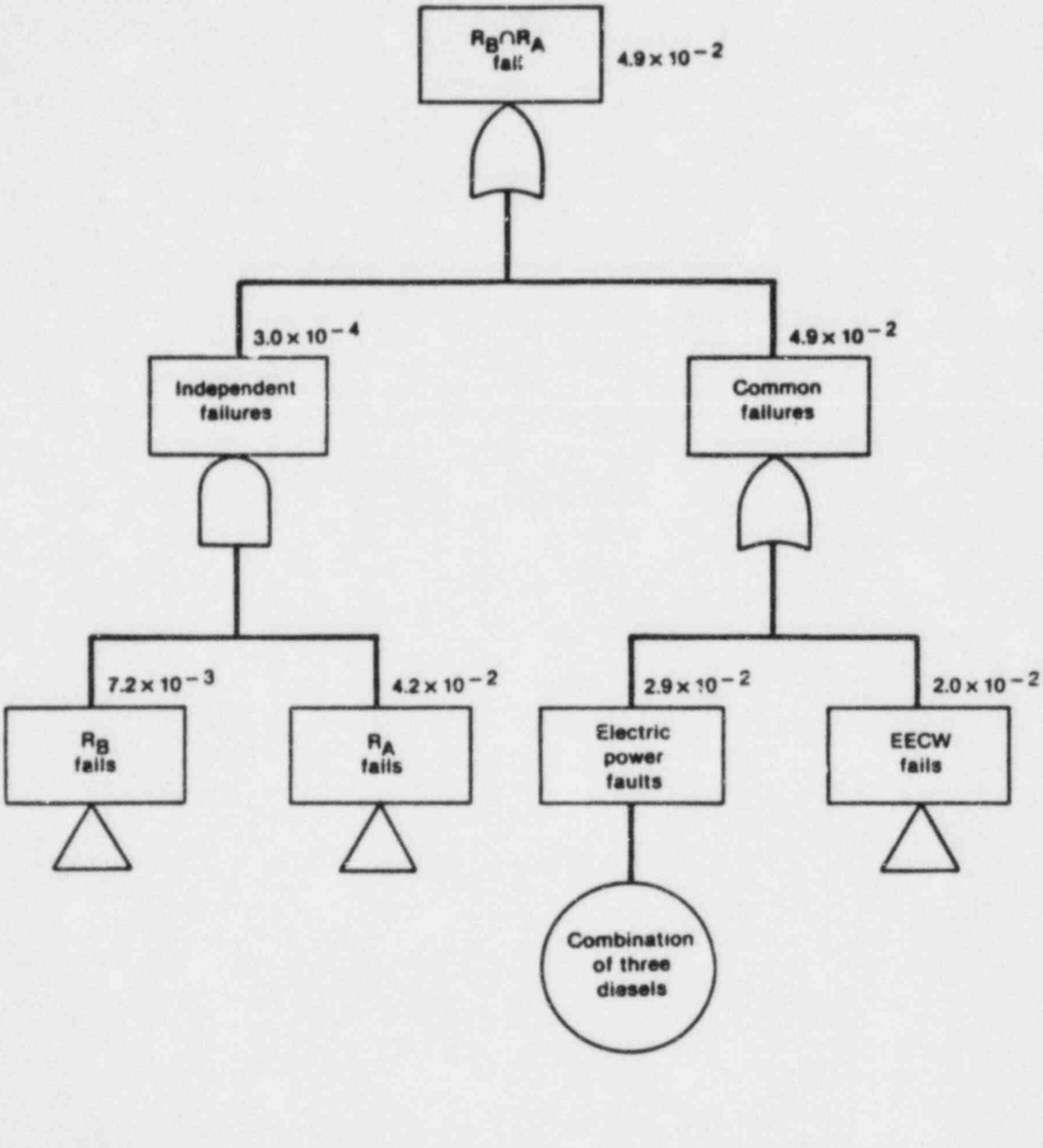


Figure 3.2 Reduced Fault Tree for RHR System Modes $R_A$ and $R_B$ - Loss of Offsite Power

The reduced fault trees of Figs. 3.1 and 3.2 show that if no credit is taken for operator action to recover from failures, the contributions to the unavailability of decay heat removal ($R_BR_A$) are:

| Offsite Power is Available at Transient Initiation | |
|---|---|
| Independent $R_BR_A$ Failures | 82% |
| Valve Control Circuit Faults (Bypass Valves FCV 74-07 and FCV 74-30) | 17% |
| Other Valve Faults (Bypass Valves FCV 74-07 and FCV 74-30) | 1% |

| Loss of Offsite Power | |
|---|---|
| Combination of Three Diesel Bus Failures | 59% |
| EECW Failures | 41% |

Thus, for transients with offsite power available at their initiation, the unavailability of decay heat removal is dominated by independent $R_BR_A$ failures and failure of the bypass valves FCV 74-07 and FCV 74-30. For loss of offsite power events, the dominant contributions to the decay heat removal unavailability are a combination of three diesel bus failures and failure of the EECW system.

The analysis of dominant minimum cut sets presented in the IREP study shows also the following. The main contributors to independent $R_BR_A$ failures are:

| Shutdown Cooling Mode ($R_A$) | No LOSP | LOSP |
|---|---|---|
| Faulty Signals that Isolate the Suction Valves FCV 74-47 and FCV 74-48 | 49% | 23% |
| Failure of Suction Valves FCV 74-47 and FCV 74-48 to Open | 45% | 20% |
| Operator Failure to Initiate $R_A$ | 5% | 2% |

Torus Cooling Mode ($R_B$)

| | | |
|---|---|---|
| Operator Failure to Initiate $R_B$ | 32% | 14% |
| Double Failures Involving Failure of one RHRSW Header and either a RHR System Valve Failure or one RHR System Loop in Test or Maintenance | 25% | 10% |
| Double Failures Involving Failure of a 4160 V Shutdown Board and a RHR System Valve Failure | - | 27% |
| Independent Failures of Three 4160 V Shutdown Boards | - | 10% |

In turn, the unavailability of one RHRSW header is dominated (92.5%) by failures of the motor operated valve that is located immediately after the RHR heat exchanger (valve FCV 23-34 for header A, etc.). The unavailability of one 4160 V shutdown board is dominated (83.6%) by the unavailability of its corresponding diesel generator (failure to start or diesel in test or maintenance).

The main contributor to the combination of three diesel bus failures in the event of LOSP, is failure of three diesels to start due to common cause. The failure of three diesel buses leads directly to failure of the torus cooling mode and of the EECW system. Failure of the EECW system causes the shutdown cooling mode to fail.

Finally, the dominant minimum cut sets in the unavailability of the EECW system, in the event of LOSP, are:

| | |
|---|---|
| Two Diesel Generators Fail to Start Due to Independent Faults | 34% |
| Double Failures Including Failure of One Diesel to Start and Failure of One Motor Operated Valve to Open | 8% |

In the IREP study for Browns Ferry, Unit 1, depending on the time available for operator action, system faults have been categorized as recoverable or nonrecoverable. In the analysis of accident sequences involving failure of decay heat removal, the following faults were considered as recoverable: loss of offsite power; failure of the control circuits of the motor operated valves FCV 54-07, and FCV 54-30; failure of some other control circuits, not specified, in the RHR system; EECW system failure in the event of

LOSP (by valving in spare pumps from the RHRSW system). For offsite power, a recovery probability of 0.97 was used, based on WASH-1400 data. To recoverable control circuit faults a recovery probability of 0.99 was assigned. The same probability was assigned to the recovery of the EECW system. With these assumptions, the unavailability of decay heat removal, $q(R_B R_A)$, for transients with normal power available was written:

$$q(R_B R_A) = rq(\text{recoverable}) + q(\text{nonrecoverable})$$

where

$q(\text{recoverable})$ = unavailability contribution of recoverable faults $= 1.9 \times 10^{-5}$

$q(\text{nonrecoverable})$ = unavailability contribution of nonrecoverable faults $= 5.7 \times 10^{-5}$

$r$ = nonrecovery probability of recoverable faults

For $r = 0.01$, the unavailability of decay heat removal, $q(R_B R_A)$, for transients with normal power available becomes

$$q(R_B R_A) = 0.01 \times (1.9 \times 10^{-5}) + 5.7 \times 10^{-5} = 5.7 \times 10^{-5}$$

In the event of loss of offsite power, the same unavailability was written

$$Q(R_B R_A) = 0.97\, q(R_B R_A) + 0.03\, q_{LOSP}$$

where

0.97 = probability of offsite power recovery

0.03 = probability for failure to recover offsite power

$q_{LOSP}$ = unavailability of decay heat removal with offsite power not recovered

The fault tree of Fig. 3.2 shows that $q_{LOSP}$ is mainly due to failure of three diesel buses and failure of the EECW. As mentioned earlier, in the IREP study, it was assumed that a failed EECW system can be recovered with a probability of 0.99. Thus,

$$\begin{aligned} Q(R_BR_A) &= 0.97\text{x}5.7\text{x}10^{-5}+0.03\ [2.9\text{x}10^{-2}+(2.0\text{x}10^{-2})\ (0.01)] \\ &= 5.53\text{x}10^{-5}+0.03\ (2.92\text{x}10^{-2})=5.53\text{x}10^{-5}+8.76\text{x}10^{-4} \\ &= 9.3\text{x}10^{-4} \end{aligned}$$

where

$5.7 \times 10^{-5}$ = $q(R_BR_A)$ = unavailability of decay heat removal with offsite power available

$2.9 \times 10^{-2}$ = unavailability of three diesel buses (see Fig. 3.2)

$2.0 \times 10^{-2}$ = EECW unavailability in the event of LOSP (see Fig. 3.2).

The above results show that if recovery of RHR faults and of offsite power, as defined in the IREP study, is taken into account, then:

a. For transients with offsite power available the unavailability of decay heat removal is reduced only by 25%.

b. If offsite power is lost, this unavailability is reduced by 98% (two orders of magnitude lower).

c. In the latter case, the dominant contributor to the unavailability of decay heat removal is common cause failure of three or more diesel generators.

In the event that all the RHR pumps and/or heat exchangers of Unit 1 are unavailable, a crosstie arrangement permits the use of the A or C RHR pumps and heat exchangers of Unit 2 to circulate and cool the Unit 1 pressure suppression pool water. The use of this option is included in the procedures and the training of the operators. In the IREP study for Browns Ferry, no credit was taken for this crosstie arrangement because its "components are tested less frequently than ECCS and operators must follow complicated, seldom-used procedures to bring them online." Since such an arrangement represents a potential resource for core cooling, its effectiveness must be assessed in a reliability assurance program for the RHR system.

### 3.1.4 Recovery of the Power Conversion System

In WASH-1400, the availability of the PCS was treated as follows. For initiating events involving the interruption of feedwater, "based on U.S. power reactor operating experience" a probability of $10^{-2}$ was estimated for failure to restore the feedwater system within one half hour. Loss of offsite power renders the PCS unavailable. For this event, a probability for PCS restoration was used that is the same as the probability of offsite power restoration. For transients that do not render the PCS unavailable, an unavailability of $7 \times 10^{-3}$ was estimated, "from operating experience in U.S. power reactors," for 27 hours of PCS operation. In the IREP study for Browns Ferry, Unit 1, no credit for PCS recovery was considered "since there is inadequate information available on which to base a probability of recovery."

If recovery of PCS is considered as in WASH-1400, the frequencies of the dominant accident sequences identified in the IREP study are modified as follows

$$T_U R_B R_A(PCS) = T_U\, q(R_B R_A)\, p(PCS) = (1.7) \times (5.7 \times 10^{-5}) \times 10^{-2}$$
$$= 9.7 \times 10^{-7}$$

$$T_p R_B R_A(PCS) = T_p\, [0.97\, q(R_B R_A)\, q(PCS) + 0.03 q_{LOSP}\, p(PCS)]$$
$$= 0.03\, [0.97 x 5.7 x 10^{-5} x 7 x 10^{-3} + 0.03 x 2.92 x 10^{-2} x 1.0]$$
$$= 2.6 x 10^{-5}$$

$$T_A R_B R_A(PCS) = 1.68 x 5.7 x 10^{-5} x 7 x 10^{-3} = 6.7 x 10^{-7}$$

where

$q(PCS)$ = unavailability of the PCS

$p(PCS)$ = probability for failure to recover the PCS

$T_A$ = 1.68 = frequency of transients that do not render the PCS unavailable

A comparison of these frequencies with the frequencies estimated in the IREP study (Table 3.1), shows the following. If the PCS can be recovered with the probabilities estimated in WASH-1400:

a. The frequency of the top dominant accident sequence, $T_U R_B R_A$, is reduced by two orders of magnitude.

b. Accident sequences initiated by transients that render the PCS unavailable ($T_U R_B R_A$) have a frequency that is comparable to that of sequences initiated by transients that do not render the PCS unavailable ($T_A R_B R_A$).

c. Loss of offsite power is the dominant initiator in sequences that involve loss of decay heat removal ($R_B R_A$).

d. The contribution of the residual heat removal system to the core melt frequency is reduced from 70% to 34%.

In WASH-1400, it was estimated that for the Peach Bottom BWR plant the decay heat removal systems must be operable within 27 hours after the transient initiation. In the same study, a mean time to repair a diesel of 20 hours, and a probability of diesel recovery within 27 hours of 0.9 were estimated. In the IREP study, it was estimated that the decay heat removal systems (RHR) must be operable within six to eight hours. If this time could be extended to 27 or more hours, and if a diesel could be recovered within this time with a probability of 0.9, the unavailability of $R_B R_A$, in the event of LOSP, would be reduced by one order of magnitude. In turn, the frequency of the dominant accident sequence $T_p R_B R_A$ (PCS) would be reduced by one order of magnitude (from $2.6 \times 10^{-5}$ to $2.6 \times 10^{-6}$) and the contribution of the residual heat removal system to the core melt frequency would be only 7%.

### 3.1.5 Conclusions

This analysis leads to the following conclusions. The most risk-significant issues in accident sequences that involve failure of the RHR system are:

a. The probability of recovering the PCS in sequences initiated by transients that render it unavailable.

b. The frequency of LOSP events and the probability of recovering offsite power.

c. Common cause failure of diesel generators.

d. The time, from transient initiation, that the RHR system must be operable.

e. Recovery of RHR faults by operator action.

f. Probability of recovering a failed diesel generator.

## 3.2 Analysis of Information from the Severe Accident Sequence Analysis Program

The Oak Ridge National Laboratory with the cooperation of the Tennessee Valley Authority (TVA) has conducted two studies of accident sequences at Browns Ferry, Unit 1, that involve loss of the decay heat removal capability[4,5]. These studies are titled "Station Blackout at Browns Ferry, Unit One - Accident Sequence Analysis," and "Loss of DHR Sequences at Browns Ferry Unit One - Accident Sequence Analysis". They were performed under the auspices of the Severe Accident Sequence Analysis (SASA) program, and were sponsored by the Division of Accident Evaluation of the Nuclear Regulatory Research arm of the Nuclear Regulatory Commission. The purpose of the SASA program was: (a) to pre-determine the probable course of a series of severe accident sequences so as to establish the timing and sequence of events, and (b) to produce recommendations for the implementation of better system design, as well as of better emergency operating instructions and operator training to further decrease the probability of such sequences. Both of these studies provide useful information for the analysis and identification of the dominant risk contributors in accident sequences involving the residual heat removal system.

Based on the information provided by the SASA studies, the frequency of the LOSP sequences in Browns Ferry was recalculated. In these calculations, the following data were utilized. For loss of offsite power at the Browns Ferry site, the frequency of 0.122 events per site-year was used. As discussed in Section 3.1.2, this frequency estimate was generated in EPRI NP-2301 by pooling together the data from all reactor sites. No loss of offsite power is reported in this report for the Browns Ferry site (LOSP in all Units). For recovery of offsite power, the log normal distribution derived in EPRI NP-2301 for the MAAC and SERC regional councils was used. These councils cover the Browns Ferry sit?. For comparis this distribution and the distribution derived in WASH-1400 are shown ir .e 3.4. Failure rates for diesel generators were obtained from EPRI NP-2433[10]. The same report has generated diesel repair times from the records of eight plants. The probabilities for failure of more than one diesel to start and the diesel repair data presented in this EPRI report, are shown in Tables 3.5 and 3.6, respectively.

### 3.2.1 Loss of Decay Heat Removal Sequences - Offsite Power is Available

The loss of DHR capability was defined as a prolonged loss of the power conversion system (PCS) and of the RHR system in the shutdown and torus cooling modes. Under these circumstances, the decay heat is transferred from the reactor vessel to the pressure suppression pool through the safety relief valves. In the SASA study, all the transient events that involved loss of DHR were grouped into three classes: (a) transients with uniform pool heatup, (b) transients with pool thermal stratification, and (c) transients involving a stuck-open relief valve.

In the first class, the suppression pool was treated as a well mixed volume of water undergoing a uniform pool heatup. This requires that at least one pump loop of the RHR system to be operable for circulation and mixing of the pool water, even though the heat removal function of the loop is not available.

In the second class of transients, no RHR pump loop is operable for pool water circulation and mixing. Pool thermal stratification can be avoided if the 13 relief valves are manually operated in an alternating scheme to distribute their discharge evenly around the circumference of the

Table 3.4. Cumulative Probability Function for Failure to Recover Offsite Power

| Time (t)<br>(hours) | Probability of non-recovery within t hours | |
|---|---|---|
| | WASH-1400 | EPRI NP-2433 |
| 1 | 0.24 | 0.59 |
| 2 | | 0.41 |
| 3 | 0.12 | 0.31 |
| 5 | | 0.20 |
| 7 | | 0.15 |
| 8 | | 0.13 |
| 10 | 0.035 | 0.10 |
| 12 | | 0.08 |
| 14 | | 0.07 |
| 16 | | 0.05 |
| 19 | | 0.04 |
| 23 | | 0.03 |
| 28 | | 0.02 |

Table 3.5. Failure Rates for Failure of More than One Diesel to Start

| | Number of Diesels Failed | Failure Rate |
|---|---|---|
| Plant Z | 2 | $1.5 \times 10^{-2}$ |
| | 3 | $8.4 \times 10^{-3}$ |
| | 4 | $3.9 \times 10^{-3}$ |
| Peach Bottom | 2 | $3.4 \times 10^{-3}$ |
| | 3 | $1.7 \times 10^{-3}$ |
| | 4 | $8.4 \times 10^{-4}$ |
| Trojan | 2 | $6.2 \times 10^{-3}$ |

Table 3.6. Diesel Repair Times from Plant Records of Eight Plants

| Length of Repair Time t (hours) | Number of Events | Relative Frequency |
|---|---|---|
| $t \leq 1$ | 12 | .23 |
| $1 < t \leq 4$ | 6 | .11 |
| $4 < t \leq 8$ | 12 | .23 |
| $8 < t \leq 12$ | 7 | .13 |
| $12 < t \leq 16$ | 1 | .02 |
| $16 < t \leq 20$ | 4 | .08 |
| $20 < t \leq 24$ | 3 | .06 |
| $t > 24$ | 8 | .15 |
| | 53 | 1.00 |

pressure suppression pool. However, manual relief valve operation is only possible when the drywell control air pressure is 25 psi or more over the drywell pressure. The maximum drywell control air presure is 100 psig. Consequently, the capability of manual relief valve operation will be lost after the drywell pressure reaches 75 psig. Subsequently, the reactor vessel will repressurize to the setpoint (1105 psig) for automatic actuation of the lowest-set relief valve which will repeatedly actuate thereafter. Significant thermal stratification will follow. The temperature of the upper pool water layer will rise significantly higher than the pool bulk average temperature, the containment pressurization rate will be higher than in the previous class of transients, and the drywell failure pressure will be reached earlier.

In the third class of transients, it was assumed that a single safety relief valve fails to close, either automatically or in response to operator manipulation of the remote-manual relief valve controls. The reactor vessel will depressurize more rapidly than if the operator had complete control of the safety relief valves.

Under normal operating conditions, the pump of the control rod drive (CRD) hydraulic system injects into the reactor vessel 60 gpm of water that is used for cooling of the CRD mechanisms. This water is pumped from the condensate storage tank. Following a scram, this injection flow increases to 170 gpm until the scram is reset. After scram reset, this flow is reduced to 60 gpm. In a loss of DHR sequence, a scram signal is continuously present after the drywell pressure reaches 2 psig. Thus, after this pressure is reached the CRD pump will provide a flow of 170 gpm. Four hours after reactor scram, the decay heat level is such that this flow is sufficient to maintain reactor vessel water level. In the IREP study for Browns Ferry, the supply of water to the reactor vessel through the CRD pump was neglected. The impact of this additional source of cooling water on the progression of an accident sequence characterized by loss of DHR, was considered in the SASA study.

Table 3.7. Chronology of Events in a Loss of DHR Accident Sequence with Uniform Pool Heatup

| Time (h) | Event |
|---|---|
| 0 | Reactor trip followed by MSIV closure and failure of both pool cooling and shutdown cooling modes of the RHR system. |
| 1 | High drywell pressure scram at 0.115 MPa (2 psig). Diesel generators and SGTS are automatically initiated. |
| 1 | Drywell control air suction is isolated. Operator valves-in the station control air. |
| 1 | Pool temperature exceeds 49°C (120°F) - operator begins controlled depressurization of reactor vessel. |
| 2 | Core spray initiation signal [reactor vessel pressure < 3.21 MPa (465 psia) and drywell pressure > 0.115 MPa (2 psig)] causes trip of drywell coolers. |
| 2 | Suppression pool temperature exceeds the 60°C (140°F) recommended maximum temperature for cooling of RCIC and HPCI lube oil. |
| 4 | Required reactor vessel injection rate falls below the flow provided by the CRD hydraulic system [0.011 $m^3/s$ (170 gpm)]. |
| 8.6 | Operator must begin to throttle CRD hydraulic system pump to avoid overfilling the reactor vessel. |
| 13 | HPCI and RCIC system steam line isolation caused by high [93°C (200°F)] torus room temperature. |
| 14 | RCIC turbine high exhaust pressure trip at containment pressure > 0.28 MPa (40 psia). |
| 21.5 | Drywell design pressure [0.49 MPa (70.7 psia)] exceeded. |
| 23.5 | SRVs become inoperative in remote-manual mode because drywell pressure exceeds 0.55 MPa (80 psia). |
| 35 | Drywell fails when internal pressure exceeds 0.91 MPa (132 psia). Suppression pool temperature has increased to 173°C (343°F). |

## Transients with Uniform Pool Heatup

The chronology of events during a transient that involves loss of DHR capability and uniform pool heatup, as determined in the SASA study, is shown in Table 3.7. As mentioned earlier, a basic assumption for this type of transient is that although decay heat can not be removed by the RHR system, at least one pump loop of this system is operable, and the operator will operate this loop to keep the suppression pool water well mixed. According to the emergency procedures, the operator must initiate a 56°C/h (100°F/h) depressurization, by manually controlling the safety relief valves, before the suppression pool temperature exceeds 49°C (120°F). As shown in Table 3.7, this temperature is reached in about one hour. The Browns Ferry emergency operating instructions also require that in the event of main steam isolation valve (MSIV) closure, the operators alternate their selection of relief valves to minimize local temperature buildup in the suppression pool. Thus, if the operators follow these instructions, uniform pool heatup is maintained as long as the relief valves can be manually controlled.

After about one hour the drywell control air suction would be isolated. This would compromise the long-term remote-manual operability of the safety relief valves. As discussed in the next section, the stored capacity of drywell air could last for seven hours. However, the operator would restore air supply to the relief valves by valving-in the station control air.

In about two hours, the suppression pool temperature exceeds the 60°C (140°F), which is the maximum recommended temperature for cooling of the RCIC and HPCI lube oil. Therefore, after two hours the RCIC and HPCI systems can be maintained operable only if their suction is connected with the condensate storage tank. After four hours, the flow supplied by the CRD pump is sufficient to maintain reactor water level. Consequently, after the first four hours of the transient, core cooling can be maintained by operating either the RCIC or the HPCI system, or the CRD pump. In 13 hours, the RCIC and HPCI systems become inoperable due to isolation of their steam lines caused by high (93°C, 200°F) torus room temperature. After this time, water can be supplied to the core by the CRD pump. In addition to the CRD pump, the RHR system and the core spray system can be used if the pump loops of these systems are operable, and the operator realigns their suction to the condensate storage tank. At the 14 h point, the RCIC turbine high exhaust pressure trip setpoint (40 psia) is also reached.

It must be pointed out that the HPCI system would be lost earlier, two and a half hours from transient initiation, if the operator does not take proper action. The HPCI booster pump is automatically (and irreversibly) shifted to the suppression pool after the pool level exceeds the +7-inches point. This point is reached in about 2.5 hours. At this time the water pool temperature exceeds the maximum recommended temperature for cooling of the HPCI lube oil (Table 3.7). To prevent this, the operator must take corrective action before the system is automatically shifted to the suppression pool. Also, for the RCIC system to remain operable, the operator must keep the vessel pressure above 65 psia. The RCIC turbine steam supply line automatically isolates when the reactcr vessel pressure drops below 65 psia.

In 23.5 hours the drywell pressure exceeds 80 psia and remote-manual control of the safety relief valves is lost. Thereafter the reactor vessel repressurizes to the setpoint (1105 psig) of automatic actuation of the lowest-set relief valve which will open and close repeatedly. To avoid thermal stratification in the suppression pool, at least one RHR pump loop must be operable for pool water circulation and mixing. In the SASA study, it is estimated that the containment failure pressure (131.7 psia) is reached in 35 hours after the transient initiation. Depending on how the containment fails, the systems providing water to the core may survive or fail with the containment. If they survive, water injection to the core could be maintained as long as these systems and water are available. For example, if the standby coolant system is available, river water could be used even after the condensate storage tank supply has been exhausted.

The solenoid valves, which are necessary for remote manual operation of the safety relief valves, have a long-term design temperature of 138°C (281°F) and a short-term design temperature of 163°C (325°F). Depending on the operability of the drywell coolers, the long-term design temperature is reached sometime between about 15 to 27 hours. Thus, remote manual control of the safety relief valves may be lost at about 15 hours from transient initiation.

From the above discussion is clear that the amount of water available in the condensate storage tank is a very important parameter. The Browns Ferry operating instruction require the operator to keep the condensate storage tank nearly full. The median volume for the allowable operating band is 362,000 gallons. In the SASA study, it is estimated that after 35 hours about 290,000 gallons have been injected into the core. This is well below the median volume of 362,000 gallons.

### Transients with Thermal Stratification in the Suppression Pool

If all the RHR pump loops are unavailable, suppression pool water circulation and mixing can not be provided. As discussed in the previous section, in about 23.5 hours remote manual control of the safety relief valves is lost. Subsequently, the reactor vessel will repressurize to the setpoint (1105 psig) of automatic actuation of the lowest-set relief valve, which will repeatedly actuate thereafter. Significant pool thermal stratification will follow. In the SASA study, it was estimated that at the worst case containment failure would occur after 28 hours.

### Loss of Decay Heat Removal with Stuck Open Relief Valve

This class of transients are characterized by loss of decay heat removal and failure of a single safety relief valve to reclose either automatically or in response to operator manipulation of the remote-manual safety relief valve controls in the main control room. The analysis performed in the SASA program shows that a stuck open safety relief valve does not have a great impact on the overall system behavior during a loss of DHR sequence. Due to the open safety relief valve, the reactor vessel depressurizes faster than if the operator was controlling all the safety relief valves. By about 6 hours, the vessel pressure falls below the 115 psia setpoint for isolation of the HPCI turbine steam line. After 6 hours, the CRD pumps provide all the required injection flow to the reactor vessel. If forced pool circulation is available, through at least an RHR pump, the drywell failure pressure is reached at 34 hours. If forced pool circulation is not available, this pressure is reached at 32 hours.

Summary

The SASA analysis shows that if DHR is unavailable, the containment failure pressure will be reached at:

a. 34 hours if uniform pool heatup is available.

b. 28 hours if uniform pool heatup is not available.

c. 32 hours if a relief valve is stuck open.

As mentioned earlier, the solenoid valves, which are necessary for remote manual operation of the safety relief valves, have a long-term design temperature of 138°C (281°F) and a short-term design temperature of 163°C (325°F). If uniform pool heatup is available, depending on the operability of the drywell coolers, the long and short term design temperatures would be reached sometime between 15 to 27 and 26 to 28 hours, respectively, from accident initiation. In Ref. 4 it is stated that "considerable operator ingenuity would be required to effect a normal recovery if the MSIV and SRV solenoid operators have failed". Therefore, if the drywell coolers are operable, the time available for normal recovery may be shorter than 28 hours. This time is significantly longer than the six to eight hours considered in the IREP study. The core melt frequency due to loss of DHR becomes strongly dependent on the probability of recovering the power conversion system within the above interval. However, for this time interval to be valid, it must be ascertained that the probability of the operator keeping a nearly full condensate storage tank is high.

### 3.2.2 Loss of Decay Heat Removal - Sequences Initiated by Loss of Offsite Power

If offsite power is lost and diesel power is available, the system response is similar as in the case where offsite power is available. The drywell coolers will be tripped automatically on high drywell pressure about two hours from accident initiation and logic exists which prevents their restart. The unavailability of the coolers will shorten the time that the long- and short-term design temperatures of the solenoid valves are reached from 27 to 15 hours and from 28 to 26 hours, respectively. In the event of LOSP, only the spare pump of the CRD hydraulic system is supplied power by a diesel bus. Thus, operator action is required to establish water supply to the reactor vessel by the CRD pump. Also, cooling to the CRD pumps is provided by the raw cooling water system which is inoperable in the event of LOSP. However, with proper operator actions, pump cooling can be provided by the emergency equipment cooling water system. Finally, if coolant injection by the CRD pump is available, the containment failure pressure will be reached about 2.5 hours earlier than in the case where offsite power is available. If coolant injection by the CRD pump is not available, as shown in Table 3.7 the RCIC and HPCI systems are isolated about 13 hours from transient initiation and coolant injection is lost. Core uncovery will follow soon after. Units 1 and 2 share the same spare CRD pump. Unit 3 has its own spare CRD pump. If offsite power is lost in Units 1 and 2, then even if operator action is taken to power the spare CRD pump from the diesels, only one of the two units can use the spare CRD pump.

As discussed in Section 3.1.3, the unavailability of decay heat removal in the event of LOSP is dominated by the common cause failure of three or more diesel generators. At Browns Ferry there are eight diesel generators, which are designed to automatically start and load whenever normal AC power is lost. With proper operator action, the operation of any six diesel generators would be sufficient for the safe shutdown and cooldown of the three Browns Ferry units. Without operator action, for adequate short term shutdown and cooldown response, the six operable diesel generators would have to be three of the four provided for the Unit 1/Unit 2 complex and three of the four provided for Unit 3.

If offsite power is lost in all units, even if proper operator action is taken to shift loads to operating diesels, failure of three diesels would lead to inadequate power supplies for safe cooldown of at least one unit. As mentioned earlier, the RCIC and HPCI systems would be isolated 13 hours from transient initiation. The probability of failure to recover offsite power within 13 hours is about 0.07 (EPRI NP-2301). From EPRI NP-2433, the probability for failure of three diesel generators to start is 8.4 $10^{-3}$/

demand (plant Z data) or 1.7 x $10^{-3}$/demand (Peach Bottom data). For a site LOSP frequency of 0.122 events per year, the frequency of such a sequence is

$$0.122 \times 0.07 \times 8.4 \times 10^{-3} = 7.2 \times 10^{-5} \text{ (Plant Z diesel data)}$$

or

$$0.122 \times 0.07 \times 1.7 \times 10^{-3} = 1.5 \times 10^{-5} \text{ (Peach Bottom diesel data).}$$

If more than three diesels are unavailable, depending on the number of the unavailable diesels and on the actions taken by the operator, one or more of the Units may experience station blackout.

### 3.2.3 Station Blackout

A station blackout is defined as a complete loss of AC power to the essential and nonessential switchgear buses in a nuclear power plant. At Browns Ferry, a station blackout would be caused by a loss of offsite power and subsequent failure of all onsite diesel generators to start and load. After such an event, the only remaining sources of electrical power would be the battery-supplied 250 V, 48 V and 24 V DC electrical distribution systems. AC power would be limited to the instrumentation and control circuits supplied by the feedwater inverter or the unit-preferred and plant-preferred motor-generator sets that are driven by the above DC systems.

During a prolonged station blackout, the coolant injection capability will be lost when the unit battery that supplies the 250 V DC logic and valve-control power to the RCIC and HPCI systems becomes exhausted. It has been estimated that under the conditions of station blackout, the necessary 250 V DC power for HPCI or RCIC system operation would remain available during the first four to six hours of the blackout. This estimate is based on the assumptions: (a) all unit batteries are available, and (b) prudent action is taken by a well-trained operator to conserve battery potential by minimizing the connected DC loads. Under the same conditions, a recent TVA calculation shows that it can be expected that the unit batteries would last as long as seven hours.

As long as DC power is available, the operator would maintain reactor vessel water level in the normal operating range by intermittent operation of the RCIC system. The HPCI system is available as a backup. The operator would also control reactor vessel pressure by remote-manual operation of the safety relief valves. Since during a station blackout the drywell coolers are inoperable, the SASA analysis shows that the operator must start reactor vessel depressurization down to about 100 psig within one hour from accident initiation.

In the SASA analysis, it was assumed that the unit battery is exhausted in four hours. After DC power is lost, the water injection capability is also lost. The SASA analysis shows that core uncovery starts about eight hours after accident initiation. The same analysis also shows that:

> "Although fuel damage is significantly delayed, the ability to avoid ultimate fuel damage is compromised because of the elevated drywell temperature experienced after loss of the 250 V DC batteries. As discussed in Sect. 3, a containment temperature of 149°C (300°F) would not prevent normal recovery. This temperature is reached about 40 min. after loss of the batteries. At about four hours after the battery loss, the fuel is beginning to be uncovered, and the drywell temperature is above 191°C (375°F). This elevated temperature may cause failure of the drywell electrical penetrations and may fail the solenoid operators necessary for operation of the SRVs, inner isolation valves, and containment cooler dampers (which fail closed on loss of AC power). Even if electrical power were fully restored at this point, considerable operator ingenuity would be required to effect a normal recovery if the MSIV and SRV solenoid operators have failed."

Therefore, although core uncovery starts about eight hours after accident initiation, the time available for restoration of power is less than eight hours.

In addition to the accident sequence described so far, six more sequences were analyzed in the SASA program. These sequences are:

1. Station Blackout -- HPCI and RCIC are operable. No operator action to provide manual reactor vessel depressurization (TB').

2. Same as above with a safety relief valve stuck open (TPB').

3. Station Blackout -- RCIC is operable - HPCI is inoperable - Operator takes proper actions for RCIC and manual safety relief valve operation ($T_vB'$).

4. Same as $T_vB'$ with a safety relief valve stuck open ($T_vPB'$).

5. Station Blackout -- HPCI and RCIC are unavailable (TUB').

6. Same as TUB' with a safety relief valve stuck open (TUPB').

The times of core uncovery and core melt initiation for these sequences are shown in Table 3.8. These results show that if both the RCIC and the HPCI systems are available and the operator does not take action, or if the operator takes action and at least the RCIC system is available, core uncovery starts five to six hours after accident initiation. However, if both the HPCI and the RCIC systems are unavailable, core uncovery starts within 0.3 to 0.5 hours. If DC power lasts up to seven hours, as TVA estimated, the SASA study concluded that if power were recovered within these seven hours a normal recovery from the accident would be possible.

Station blackout renders the RHR system as well as the CRD pumps unavailable as long as power is not recovered. The probability of power recovery depends on the time available before core melt initiation. The EPRI data shows that the probability of recovering offsite power within one hour is about 41% and within seven hours about 85%. Thus, if the HPCI and RCIC systems are operable as long as DC power is available, the core melt frequency due to station blackout will be equal to

$0.122 \times 3.9 \times 10^{-3} \times 0.15 = 7.1 \times 10^{-5}$ (Plant Z diesel data)
$0.122 \times 8.4 \times 10^{-4} \times 0.15 = 1.5 \times 10^{-5}$ (Peach Bottom diesel data)

Table 3.8. Timing of Core Uncovery and Core Melt Initiation - Station Blackout

| Accident Sequence | Time of Core Uncovery (hr) | Time of Core Melt Initiation (hr) |
|---|---|---|
| TB' | 5.0 | 5.9 |
| $T_vB'$ | 5.8[a] | 6.6 |
| TPB' | 5.3 | 6.5 |
| $T_vPB'$ | 5.6[b] | 6.6 |
| TUB' | 0.5 | 1.1 |
| TUPB' | 0.3 | 0.9 |

[a] Core uncovers first at 21 min. and is reflooded at 22 min.

[b] Core uncovers first at 11 min. and is reflooded at 12 min.

where

0.122 = LOSP frequency
$3.9 \times 10^{-3}$ = failure for four or more diesels to start (plant Z)
$8.4 \times 10^{-4}$ = failure for four or more diesels to start (Peach Bottom)
0.15 = failure to recover offsite power within seven hours.

If the HPCI and RCIC systems were both unavailable, the resulting core melt frequency would be

$0.122 \times 3.9 \times 10^{-3} \times 0.59 \times 1.8 \times 10^{-3} = 5.1 \times 10^{-7}$ (Plant Z diesel data)
$0.122 \times 8.4 \times 10^{-4} \times 0.59 \times 1.8 \times 10^{-3} = 1.1 \times 10^{-7}$ (Peach Bottom diesel data)

where 0.59 = failure to recover offsite power within one hour
$1.8 \times 10^{-3}$ = RCIC and HPCI unavailability.

From these two sequences (i.e., (a) station blackout - HPCI and RCIC operable, (b) station blackout - HPCI and RCIC unavailable), the first one is dominant. Its contribution to the core melt frequency is strongly dependent on the frequency of diesel generator failure to start due to common cause, and on the probability of recovering offsite power before core melt initiation.

A number of considerations that must be addressed while efforts would be made to restore AC power are pointed out in the SASA study. These considerations include the following.

Plant ventilation is lost during station blackout. The ambient temperature near the RCIC turbine may reach 93.3°C (200°F) causing automatic isolation of the RCIC system. If this would occur, operator action is required to override the isolation signal.

The condensate storage tank has a guaranteed minimum stored supply of 135,000 gallons. About 95,000 gallons would be used during the first five hours of the transient. For normal system recovery it must be assured that adequate water supply is available from the condensate storage tank.

If the local water temperature around the relief valve tailpipe terminus in the pool is excessive, condensation oscillations may occur causing gross unstable vibrations of the torus assembly. These oscillations are not expected to occur if the local temperature is limited to 93.3°C (200°F) or equivalent to 87.8°C (190°F) average pool temperature. To avoid such oscillations, the operator must actuate the relief valves in an alternate scheme to achieve an even energy addition to the pool.

The HPCI logic will automatically shift its suction from the condensate storage tank to the suppression pool after the pool level reaches +7 inches. This would occur after about three hours. Since the lubricating oil of the HPCI turbine is cooled by the water being pumped, this shift would threaten the viability of the HPCI system. To keep this system available, operator action is required to prevent shifting of the HPCI suction.

To keep the drywell temperature below the damage limit of the SRV and MSIV solenoid operators, the operator must depressurize the reactor vessel within one hour. There are no Emergency Operating Instructions for station blackout at Browns Ferry. Based on LOCA considerations, current operator training stresses concern for high suppression pool temperatures. Thus, the operator would be reluctant to proceed into fast depressurization. As mentioned earlier, even if electrical power is restored, considerable operator ingenuity would be required to effect a normal recovery if the MSIV and SRV solenoid operators have failed.

During station blackout the control air system is unavailable. For remote-manual control of the safety relief valves sufficient stored capacity of drywell control air must be available. The accumulators provided for the six relief valves of the ADS system are sized to permit five operations per valve, or a total of 30 actuations. The SASA study has concluded that the stored capacity of drywell air is sufficient for seven hours.

To retain the necessary DC power available up to four hours, or seven hours as estimated by TVA, the operator must take action to disconnect all the loads of the 250 V DC system that are not absolutely necessary. For such an action to be effective a procedure must be available that lists all the loads that have to be disconnected.

### 3.2.4 Conclusions

The analysis performed in the SASA program shows very clearly that a reliability and a PRA analysis must be supported by a detailed analysis of the plant's response to risk-significant accident sequences. This analysis determines:

a) the prevailing conditions during the accident

b) the response of all the systems and components involved in the sequence of events

c) the timing and sequence of the events.

From this analysis: the required operator actions can be defined; the existing emergency procedures can be evaluated; the probabilities of operator action can be assessed based on the time available, the adequacy of existing procedures, the training provided to the operators, the resources available to the operator. On the other hand, this analysis provides the basis for establishing emergency procedures and proper operator training. The same analysis determines the time available for system recoveries and in conjunction with the probabilistic analysis of the accident provides the basis for reliability improvement recommendations.

If the PCS can be recovered within 28 hours with the probability estimated in WASH-1400 (i.e., 0.99), then the accident sequences that involve failure of the RHR system are dominated by loss of offsite power events and failure of three or more diesel generators to start due to common cause. The estimated frequencies of these sequences (based on EPRI data and on the SASA analysis) are summarized in Table 3.9. The frequencies of these sequences must be reassessed after plant specific information becomes available.

Table 3.9. Frequency of Dominant Accident Sequences

| Sequence | | Frequency | |
|---|---|---|---|
| | | Without Diesel Recovery | With Diesel Recovery |
| LOSP - Plant Z data | | $7.2 \times 10^{-5}$ | $2.2 \times 10^{-5}$ |
| LOSP - Peach Bottom data | | $1.5 \times 10^{-5}$ | $4.5 \times 10^{-6}$ |
| Station Blackout - Plant Z data | | $7.1 \times 10^{-5}$ | $3.1 \times 10^{-5}$ |
| Station Blackout - Peach Bottom data | | $1.5 \times 10^{-5}$ | $6.5 \times 10^{-6}$ |
| $T_U$ $R_B$ $R_A$ (PCS)[a] | $9.7 \times 10^{-7}$ | | |
| $T_A$ $R_B$ $R_A$ (PCS)[a] | $6.7 \times 10^{-7}$ | | |

[a] Based on IREP and WASH-1400 data.

## 3.3 Risk Significance of Emergency Operating Instructions

The operator response during a transient event that has the potential to lead to core damage depends very strongly on the availability of proper emergency operating instructions (EOIs) and on relevant operator training. Both items must be among the most significant elements of a reliability assurance program. To assess the impact that the emergency operating instructions of the reference plant may have on accident sequences that involve the RHR system, a review of the relevant instructions was undertaken. A list of the EOIs that were made available by Browns Ferry, at this stage of the project, is given in Table 3.10.

There is no EOI that deals specifically with failure of the RHR system to provide decay heat removal. The actions of the operator must be synthesized from a number of EOIs which provide relevant instructions. The effectiveness of this synthesis will depend very strongly on operator training and experience, and must be carefully evaluated by a reliability assurance program. Since at this stage of the project all the plant EOIs were not available, it can not be assured that the EOIs listed in Table 3.10 comprise a complete set of the available instructions in the event of RHR failure. However, as the available instructions are scattered into a larger number of documents, it is expected that the operator effectiveness will depend more strongly on his training and experience. On the other hand, it must be taken into account that events like failure of the RHR system to provide decay heat removal are very rare. Consequently, such events are not part of the experience the operator acquires from every day plant operations. The conclusions derived in this section must be re-examined, if more information on EOIs is provided that warrants such a re-examination.

Further insights in evaluating the effectiveness of procedures, and operator training and experience can be obtained by analyzing the operator response during events like the fire at Browns Ferry, the TMI accident, and potential accident precursors that have occurred at operating nuclear power plants.

Table 3.10. Emergency Operating Instructions That Were Made Available to the Project

1. Emergency Operating Instruction No. 26 - Loss of Control Air, Units I, II, and III.

2. Emergency Operating Instruction No. 34 - Control Room Abandonment, Units I, II and III.

3. Emergency Operating Instruction No. 36 - Loss of Coolant Accident Inside Drywell, Units I, II, and III.

4. Emergency Operating Instruction No. 37 - Irradiated Fuel Damage While Refueling, Units I, II, and III.

5. Emergency Operating Instruction No. 40 - Loss of Shutdown Cooling (RHR), Units I, II, and III.

6. Emergency Operating Instruction No. 41 - Water Makeup Methods to Reactor Vessel, Unit I, II, or III.

7. Emergency Operating Instruction No. 46 - Loss of Feedwater in Conjunction with RPV Isolation.

To assess the impact of EOIs on the outcome of accident sequences involving the RHR system, a comparison was made between the operator actions indicated by the SASA analysis and those required by the EOIs.

### 3.3.1 Required Operator Actions Versus Emergency Operating Instructions

The EOIs stress avoidance to place controls on manual operation when automatic operation functions properly "unless unsafe plant conditions will result". The SASA analysis shows that HPCI and RCIC would be automatically initiated about 10.5 minutes from transient initiation. Thus, in the event that these systems are unavailable, unless there are indications of their failure available to the operator, he will not be aware of their unavailability earlier than the above time interval (10.5 min). EOI-46 (Loss of Feedwater in Conjunction with RPV Isolation) instructs the operator to verify RCIC and HPCI automatic initiation after "low" water level (476.5") has been reached. From the available information, it seems that there is no EOI for failure of HPCI and RCIC. In the event that the RCIC and HPCI systems fail to start, an instruction flow diagram in EOI-46 gives the following instructions: "start spare CRD pump, line-up demineralized water to SLC, start installing HPCI, RCIC spool pieces". EOI-41 states that approximately four hours are required to install a "spool piece". The CRD pump injection is not adequate for the first four hours of the transient, and the SLC flow is about one third of the CRD pump flow. The EOI-46 flow diagram continues as follows. If a relief valve is not stuck open, "manually open relief valves, panel 9-3, panel 25-32" and "depressurize to CS, LPCI permissive, condensate booster pump". If a relief valve is stuck open, "depressurize to CS, LPCI permissive, condensate booster pump". The instruction does not state how many relief valves should be manually opened. EOI-26 states that the depressurization rate should be 100°F/hr. At higher rates reactor vessel damage may occur. If the operator opens the relief valves such that the depressurization rate is 100°F/hr, from the information provided in Fig. EOI-34-1 of EOI-34 it is determined that: (a) the actuation pressure of the core spray system (500 psig) would be reached in 0.9 hours from initiation of manual depressurization, (b) the pressure at which the core spray delivers rated flow (350 psig) would be reached in 1.25 hours, (c) the LPCI actuation pressure (450 psig) would be reached in one hour, and (d) the pressure of 300 psig at which the LPCI pump discharge pressure overcomes the reactor pressure would be reached at 1.4 hours. The SASA analysis shows that if the HPCI and RCIC are unavailable, and no operator action is taken to depressurize the reactor, then: (a) if a relief valve is not stuck open core uncovery starts at 0.5 hours and core melt at 1.1 hours from transient initiation, (b) if a relief valve is stuck open, core uncovery and core melt start at 0.3 and 0.9 hours, respectively. This analysis shows that if the operator starts depressurization at 10 min from transient initiation (time at which RCIC and HPCI should start automatically) at a rate of 100°F/h some core damage may not be avoided. Since the operator knows that at rates higher than 100°F/h the vessel may be damaged, in the absence of specific instructions, it should not be expected that he would depressurize at higher rates to reach the core spray initiation pressure before core damage initiation.

The success criteria of the automatic depressurization system (ADS) state that the opening of four valves is required for mission success. In the event of a transient, the ADS is not initiated automatically early enough. EOI-46 instructs the operator to verify ADS initiation after manual depressurization has been initiated and after "low, low, low" vessel water level has been reached (384.5"). This indicates that the previous instructions "manually open relief valves" and "depressurize to CS, LPCI permissive..." do not mean manual actuation of the ADS system. Moreover, if the operator finds out that the ADS has not started, the instruction does not require manual ADS initiation. Instead, it states: "Take prompt operator (or maintenance) actions as severity of failure or transient warrant. Priority of safety equipment actuations must be considered in restoring failed equipment". These are not specific instructions. The actions that have to follow are left to operator judgement.

For transients that render the PCS unavailable (MSIV closure, loss of condenser vacuum, loss of feedwater) a probability of about $10^{-1}$ is used in recent PRAs for failure to recover the PCS in the short-term. The frequency of core damage due to accident sequences initiated by such events and involving failure of the RCIC and HPCI systems would be

$$1.7 \times 1.8 \times 10^{-3} \times 10^{-1} \times p_h = p_h \times 3.1 \times 10^{-4}$$

where

1.7 = frequency of transients that render the PCS unavailable.

$1.8 \times 10^{-3}$ = RCIC and HPCI unavailability.

$10^{-1}$ = probability for failure to recover the PCS in the short-term.

$p_h$ = probability for operator failure to depressurize at the proper rate.

This result shows that the frequency of core damage is strongly dependent on the probability of operator failure to depressurize at the proper rate. In turn, since EOI-46 (Loss of Feedwater in Conjunction with RPV Isolation) does not provide the required specific instructions, the above probability becomes very strongly dependent on relevant operator training and experience. However, in balancing EOI deficiencies with training and experience it must be taken into account that since such events are very rare, they are not part of the usual operator experience and frequency of relevant training becomes even more significant.

EOI-46 (Loss of Feedwater in Conjunction with RPV Isolation) states: "Maintain torus level. Transfer HPCI/RCIC suction to torus to prevent level increase in torus. Maintain CST invent ry (transfer water from hot well or demineralized water storage tank)." The instruction does not specify at what specific level the torus water must be maintained. The HPCI suction is automatically transferred to the suppression pool after the pool level exceeds the +7 inches point. The SASA analysis shows that this point is reached about two and a half hours from transient initiation. The same analysis shows that if torus cooling is unavailable, in about two hours the suppression pool temperature exceeds the 60°C (140°F), which is the maximum recommended temperature for cooling of the RCIC and HPCI lube oil. Thus, if the operator would transfer HPCI/RCIC suction to torus, to prevent increase of its water level, both systems would fail. The CRD pump does not provide adequate flow during the first four hours of the transient. In addition, in the event of LOSP only the spare CRD pump is powered by the diesels. This pump is common to both Unit 1 and Unit 2 and operator action is required to establish pump cooling through the EECW system. As discussed in Section 3.2.2, if offsite power is lost in all units, even if proper operator action is taken to shift loads to operating diesels, failure of three diesels would lead to inadequate power supplies for safe cooldown of at least one unit. In the event of station blackout, the core spray, the RHR system and the CRD pumps are unavailable.

In the event of LOSP, EOI-46 gives the following instructions: "verify diesel generators on", if diesels are not on "manually start and tie on diesels", if this action fails "crosstie to other unit's diesels". The same instruction also states: "Attempt to restore offsite power, use 4160 kV bus tie board to crosstie diesels between units if necessary. Transfer station loads and manually start available high pressure and low pressure systems. Re-establish plant systems as soon as practicable." There are no instructions for station blackout, which occurs if offsite power is lost and diesel power is unavailable.

From the above, the following are concluded for accident sequences initiated by transients that render the PCS unavailable and involve failure of the RHR system to remove decay heat. If the instruction EOI-46 is followed, HPCI and RCIC would be lost within about three hours. If offsite power is available the gap between loss of HPCI and RCIC and adequate injection by the CRD pump can be covered by the core spray system.

In the event of LOSP and failure of three or more diesel generators to start, failure of the HPCI and RCIC systems within three hours would lead to core damage with frequencies higher than those estimated in Section 3.2.2. The Section 3.2.2. estimates were based on the SASA analysis, which assumed that the RCIC and HPCI suctions are not transferred to the suppression pool, and consequently these systems are kept operational for thirteen hours. Reducing the available time for recovery from thirteen to three hours increases the non-recovery probabilities for offsite power and diesel generators by a factor of 4.4 and two, respectively (Tables 3.4 and 3.6).

In the event of station blackout, if the RCIC and HPCI systems are lost within three hours, the available recovery time of seven hours (SASA estimate) is reduced to about three hours. Consequently, the non-recovery probabilities for offsite power and for the diesel generators would increase by a factor of two and 1.6, respectively.

As discussed in Section 3.2.2, the SASA and TVA estimates of four and seven hours, respectively, for the availability of DC power under station blackout conditions, were based on the assumptions that: (a) all unit batteries are available, and (b) prudent action is taken by a well-trained operator to conserve battery potential by minimizing the connected DC loads. However, there is no EOI available that instructs the operator what loads to disconnect. Therefore, the time of DC power availability may be shorter than the above estimates.

As mentioned earlier, EOI-46 instructs the operator to cross-tie diesels between units in the event a LOSP is followed by failure of some diesels to start. As the SASA analysis shows, to maximize the available time for power recovery, the operator should try to keep at least the minimum required DC power available. If three of more diesels fail in the event of LOSP, it may be possible by proper switching to maintain at least DC power in all units. However, for this switching to be successful proper instructions must be available to the operator.

As the SASA analysis shows, during the course of an accident sequence some systems or components fail or are isolated as certain temperature and pressure limits are reached. For example, on high drywell pressure the drywell control air suction is isolated and the operator has to valve-in the station control air; the RCIC and HPCI systems would fail if their suction is shifted to the torus and the torus water temperature exceeds 60°C (140°F); the SRV's become inoperable in remote-manual mode when drywell pressure excees 80 psia, etc. The operator will be more effective if the procedures inform him what failures or isolations he should expect as different limiting conditions are reached.

### 3.3.2 Conclusions

The effect on the frequency of the dominant accident sequences of the EOI deficiencies discussed in the previous section is summarized in Table 3.11. It is clear that EOIs have a very significant impact on the outcome of severe accident sequences and there is a lot of room for their improvement. Their impact is more significant in accident sequences where the available response time for the operator is short, as the case is in the event the high pressure injection systems are unavailable or offsite power is unavailable. The development of effective procedures must be based on detailed analyses of the significant accident sequences, to determine the prevailing conditions during the accident, the response of all the risk significant systems and components, the timing and sequence of events. The form of the emergency instructions must be such that the proper actions can be identified very clearly and quickly. In formulating them, the stress, and the available response time and resources to the operator must be very seriously taken into account.

Table 3.11. Summary of Dominant Accident Sequences

| Sequence | | Frequency (per reactor-year) | |
|---|---|---|---|
| | | Without Diesel Recovery | With Diesel Recovery |
| | IREP Estimates | | |
| $T_U QDV$[a] | $5.5 \times 10^{-7}$ | | |
| LOSP | | $2.8 \times 10^{-5}$ | |
| $T_U\ R_B\ R_A$ | $9.7 \times 10^{-5}$ | | |
| $T_A\ R_B\ R_A$ (PCS) | $8.9 \times 10^{-7}$ | | |
| EPRI Data - Sequence of Events Based on SASA Analysis | | | |
| LOSP - Plant Z data | | $7.2 \times 10^{-5}$ | $2.2 \times 10^{-5}$ |
| LOSP - Peach Bottom data | | $1.5 \times 10^{-5}$ | $4.5 \times 10^{-6}$ |
| Station Blackout - Plant Z data | | $7.1 \times 10^{-5}$ | $3.1 \times 10^{-5}$ |
| Station Blackout - Peach Bottom data | | $1.5 \times 10^{-5}$ | $6.5 \times 10^{-6}$ |
| $T_U\ R_B\ R_A$ (PCS)[b] | $9.7 \times 10^{-7}$ | | |
| $T_A\ R_B\ R_A$ (PCS)[b] | $6.7 \times 10^{-7}$ | | |
| EPRI Data - Emergency Operating Instructions | | | |
| $T_U$ QDV (PCS) | $3.1 \times 10^{-4}\ P_h^c$ | | |
| LOSP - Plant Z data | | $3.2 \times 10^{-4}$ | $1.9 \times 10^{-4}$ |
| LOSP - Peach Bottom data | | $6.6 \times 10^{-5}$ | $4.0 \times 10^{-5}$ |
| Station Blackout - Plant Z data | | $1.4 \times 10^{-4}$ | $9.9 \times 10^{-5}$ |
| Station Blackout - Peach Bottom data | | $3.0 \times 10^{-5}$ | $2.1 \times 10^{-5}$ |
| $T_U\ R_B\ R_A$ (PCS)[b] | $9.7 \times 10^{-7}$ | | |
| $T_A\ R_B\ R_A$ (PCS)[b] | $6.7 \times 10^{-7}$ | | |

[a] QDV = RCIC, HPCI and Manual Depressurization Failure.
[b] Based on IREP and WASH-1400 data.
[c] Probability for Operator Failure to Depressurize Properly.

## 4.0 Analysis of Operating Experience with the RHR System of BWRs

The analysis of operating experience with nuclear power plant systems provides the basis to develop failure rate data banks for reliability and risk analyses, as well as to identify the dominant causes of component and system failures. A continuous evaluation of operating experience data should be one of the main elements of a reliability assurance program. It provides the indicators to measure the success of such a program, as well as to where the efforts of a reliability assurance program must focus in order to achieve its objectives.

In this work, an effort was undertaken to analyze the operating experience from the RHR system of BWRs with the objective of identifying the dominant causes of system failures. This information will indicate where a reliability assurance program for the RHR system should mainly concentrate its efforts to assure that a desired RHR reliability goal has been achieved and will be maintained throughout plant lifetime.

The only available source of system operating experience, at this stage of the project, was the Licensee Event Reports compiled by the Nuclear Safety Information Center (NSIC) at Oak Ridge National Laboratory. As discussed in the following sections, the information provided by the LERs in many instances is not adequate to identify the cause of failure. Moreover, the LER data may be incomplete, i.e., all the relevant failure events may have not been reported. A more complete analysis could be performed if the LER information was supplemented with information from plant records, and inputs from experts involved in the design, manufacturing, installation, operation and maintenance of the system considered. Thus, the analysis presented in this report suffers from the limitations of the LERs.

The analysis of the RHR related LERs is presented into two main parts. The first part presents an analysis of the LERs for all operating BWRs. The second part presents a more detailed analysis of the LERs reported for the Browns Ferry RHR system, which is used as a reference system in this study.

## 4.1 Operating Experience with the RHR System of All BWRs

From the LERs reported in the NSIC compilation those that refer to the LaCrosse and Humbolt Bay power plants, which were considered atypical, were excluded from the analysis. The analyzed LERs cover all those contained in the NSIC file from December 29, 1976 to December 8, 1982. From them, a total of 360 events wer( considered as applicable to the RHR system. They include events that refer ιither strictly to RHR system components, or to the RHRSW system and the RHR equipment cooling water systems, that support RHR system operation.

A tabulation of the reported events per operating BWR plant is presented in Table 4.1. The identification of the plant designations used in this Table is given in Table 4.2. The results of Table 4.1 show that a wide variation exists both in the number and the type of RHR problems reported by the operating BWR plants. Of the 23 plants, 6 plants (26% of the total number of plants) reported 5 or fewer events whereas 9 plants (39%) generated 20 or more LERs. The three Browns Ferry plants with a total of 71 RHR related events (average of 24 events/plant) were above the average of about 16 events/plant obtained from this data base.

The number of LERs seems to be strongly utility dependent as a comparison of the number of LERs generated at sister plants seems to indicate. The three Browns Ferry plants, BF-1, BF-2 and BF-3, had 21, 20 and 30 LERs respectively which would put them in the above average LER number category for the 23 BWR plants. The two Brunswick plants, BR-1 and BR-2, with 28 and 34 LERs and the two Hatch plants, HT-1 and HT-2, with 48 and 33 LERs had also an above average number of RHR related problems. The three Dresden plants, DR-1, DR-2 and DR-3, reported an abnormally low number of events with only one for each plant. The two-plant Peach Bottom facility, PB-2 and PB-3, also had a relatively low number of LERs (8 reported at each). The only plant complex which showed a rather large inconsistency (in the LER trend of sister plants) was the two reactor Quad Cities complex, QAC-1 and QAC-2, where 8 and 17 events were reported.

Table 4.1 Reported Events by Each BWR Plant

| Fault/Failure Area | BF-1 | BF-2 | BF-3 | BR-1 | BR-2 | COOP | DR-1 | DR-2 | DR-3 | ARLD | HT-1 | HT-2 | FIZP | ML-1 | MONT | NM-1 | OYCK | PB-2 | PB-3 | PL-1 | QAC-1 | QAC-2 | VERY | TOTALS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RHR Valves | 7 | 3 | 9 | 5 | 6 | 10 | - | - | 1 | 4 | 23 | 8 | 6 | 2 | 7 | 1 | - | 1 | 1 | 7 | - | 8 | - | 109 |
| RHR Pumps | - | 1 | 4 | 5 | 3 | 2 | - | - | - | 2 | 3 | 2 | 1 | - | - | - | - | 3 | 1 | - | - | 2 | - | 29 |
| RHR Related Instrumentation | 9 | 8 | 10 | 7 | 5 | - | - | - | - | 4 | 4 | 7 | 6 | 1 | - | 1 | - | - | 2 | 3 | 1 | 5 | - | 73 |
| RHR Heat Exchanger | 3 | 4 | - | 1 | - | - | 1 | - | - | - | 1 | - | - | - | - | - | 2 | - | - | - | 2 | 1 | 1 | 16 |
| RHR Piping and Fittings | - | 1 | - | 5 | 16 | 3 | - | 1 | - | 11 | 10 | 3 | 6 | - | 2 | - | 3 | 2 | 2 | 4 | 1 | - | - | 70 |
| RHR Standby Coolant Supply | - | - | 1 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 1 |
| Total System Human Errors | - | 1 | - | - | - | - | - | - | - | - | - | 3 | - | - | - | - | - | - | - | - | - | - | - | 4 |
| Equipment Cooling System | 1 | 2 | 6 | - | 2 | - | - | - | - | - | 1 | - | - | - | - | - | - | 2 | - | - | - | - | - | 14 |
| RHR Service Water System | 1 | - | - | 5 | 2 | 2 | - | - | - | 4 | 6 | 10 | 1 | - | 1 | - | - | - | 2 | - | 4 | 1 | 5 | 44 |
| TOTAL | 21 | 20 | 30 | 28 | 34 | 17 | 1 | 1 | 1 | 25 | 48 | 33 | 20 | 3 | 10 | 2 | 5 | 8 | 8 | 14 | 8 | 17 | 6 | 360 |

Table 4.2. BWR Plants Used in RHR System LER Study.

| Plant Designation | Plant Name | MWe Ultimate | Architect Engineer | Criticality Date |
|---|---|---|---|---|
| BF-1 | Browns Ferry 1 | 1065 | TVA | 08/17/73 |
| BF-2 | Browns Ferry 2 | 1065 | TVA | 07/20/74 |
| BF-3 | Browns Ferry 3 | 1065 | TVA | 08/08/76 |
| BR-1 | Brunswick 1 | 821 | United Eng. | 10/08/76 |
| BR-2 | Brunswick 2 | 821 | United Eng. | 03/20/75 |
| COOP | Cooper | 778 | Burns & Roe | 02/21/74 |
| DR-1 | Dresden 1 | 200 | Bechtel | 10/15/59 |
| DR-2 | Dresden 2 | 794 | Sargent/Lundy | 01/07/70 |
| DR-3 | Dresden 3 | 794 | Sargent/Lundy | 01/31/71 |
| ARLO | Duane Arnold | 538 | Bechtel | 03/23/74 |
| HT-1 | Hatch 1 | 786 | SSI | 09/12/74 |
| HT-2 | Hatch 2 | 786 | SSI | 07/01/78 |
| FIZP | Fitzpatrick | 821 | Stone & Webster | 11/17/74 |
| ML-1 | Millstone 1 | 660 | Ebasco | 10/26/70 |
| MONT | Monticello | 545 | Bechtel | 12/10/70 |
| NM-1 | Nine Mile Point 1 | 610 | Utility | 09/05/69 |
| OYCK | Oyster Creek | 650 | Burns & Roe | 05/03/69 |
| PB-2 | Peach Bottom 2 | 1065 | Bechtel | 09/16/73 |
| PB-3 | Peach Bottom 3 | 1065 | Bechtel | 08/07/74 |
| PIL-1 | Pilgrim 1 | 655 | Bechtel | 06/16/72 |
| QAC-1 | Quad Cities 1 | 789 | Sargent/Lundy | 10/18/71 |
| QAC-2 | Quad Cities 2 | 789 | Sargent/Lundy | 04/26/72 |
| VERY | Vermont Yankee | 514 | Ebasco | 03/24/72 |

There are probably several reasons for the above rather good agreement on consistency between sister plants in the number of LERs reported. It may be due to uniformity in design, construction, operation, testing and maintenance procedures (either good, bad or average) employed at a given utility complex. Another reason for the consistency may be due to the uniformity in LER reporting practices that a single organization provides. LER report variations among different utilities may arise from differences in interpretation of the rules for submitting incident reports, and the degree of importance assigned to the LER reports by their management. Moreover, LER reporting differences can arise from variations in the reporting requirements derived from the Technical Specifications of individual plants. The Technical Specifications for plants licensed prior to January 1, 1976 were independently written by each specific plant without any planned uniformity between plants. All plants that were licensed after this date use standardized technical specifications.

To determine the dominant causes of failure for the events reported in the LERs, it was attempted to classify them in one of the following categories: (a) design error, (b) manufacturing or fabrication error, (c) installation error, (d) plant operating personnel error, (e) procedural deficiency, and (f) random failure. The majority of the LERS that refer to RHR related instrumentation failures state that the cause of these failures was instrument drift. Reference 11 reports that "The single most prevalent reason for the drift of a setpoint out of compliance with a technical specification has been the selection of a setpoint that does not allow a sufficient margin between the setpoint and the technical specification limit to account for instrument accuracy, the expected environment and minor calibration variations.... Other causes for drift of a setpoint out of conformity with the technical specification have been instrumentation design inadequacies and questionable calibration procedures." However, from the information provided by the LERs the cause of drift cannot be identified. Consequently, no further analysis of the instrumentation drift LERs was performed. A number of LERs state that the cause of the failure was unknown. If from the information provided by the LER the cause of failure could not be identified, the event was classified as random or as of unknown cause. Finally, it must be pointed out that from the limited information contained in the LERs the distinction between the different causes of failure in many instances is not clear. It is more clear that the potential of multiple failures was present than if the cause was a design or personnel error or procedural deficiency.

A categorization of the analyzed LERs by component or system and cause of failure is presented in Table 4.3. For the RHR supporting systems (RHRSW system and RHR equipment cooling system) the reported events have not been categorized by components (i.e., valves, pumps, etc.) as for the RHR system. Six LERs discussed events that involved multiple valve failures but from the information provided by them the cause of failure could not be identified. These events are included in the category "other" of Table 4.3. Seven LERs discussed failures due to water hammer. Again, from the information provided in these LERs it cannot be determined if the water hammer occurred because of design deficiencies or because the system was operated outside the range of the Technical Specifications, or because of some other reason. These events were also included in the category "other" of Table 4.3.

For 13 events (seven for valves, one for pumps, one for piping, one for instrumentation, and three for the RHRSW system) the cause of failure given in the LERs is "loose" component, for example "loose screw in valve operator", "loose valve seat", "loose screw holding a wire", etc. It is not clear if these failures were random or they were due to a systematic error that occurred when these components were assembled, installed, or maintained. These events were included in the category "cause unknown". For four events (two for valves and two for pumps) the cause of failure reported is accumulation of dirt. Again, from the LER information it is not clear if these events were random or their cause had the potential to lead to multiple failures. They were also included in the category "cause unknown". Finally, for ten events (five for valves, one for piping, one for pumps, and three for the RHRSW system) the cause of failure reported was "normal wear" or "worn" component. If components in a standby system are left in operation although they are in the wearout phase of their lifetime, multiple failures can occur when a demand for the system arises. For example, one of these LERs states: "while performing RHR service water pump operability test, RHR service water pumps were found incapable of delivering a rated flow from each pump.... The pumps and failure dates are: E11-C001B and E11-C001D on August 12, 1979, E11-C001A on August 16, and E11-C001C on August 20. Pumps failed due to normal wear on

Table 4.3. Categorization of RHR Related LERs Reported by BWR Plants

| | | Distribution by Cause of Failure | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Component or System | Number of Events | Design | Manufacturing or Fabrication | Installation | Personnel | Procedures | Random or Unknown | Drift | Other |
| RHR Valves | 110 | 14 | 3 | 1 | 16 | 3 | 67 | | 6[a] |
| RHR Pumps | 29 | 4 | | 3 | 9 | 3 | 10 | | |
| RHR Related Instrumentation | 73 | 3 | | 1 | 6 | 1 | 15 | 47 | |
| RHR Heat Exchangers | 16 | 10 | | 1 | | | 5 | | |
| RHR Piping and Fittings | 70 | 23 | 1 | 12 | 5 | 5 | 17 | | 7[b] |
| RHR Standby Coolant Supply | 1 | | | | | 1 | | | |
| RHR Testing[c] | 4 | | | | 3 | 1 | | | |
| Equipment Cooling System | 14 | 5 | | | 1 | 2 | 6 | | |
| RHR Service Water System | 43 | 7 | 1 | 3 | 5 | 4 | 23 | | |
| Total | 360 | 66(18.3%) | 5(1.4%) | 21(5.8%) | 45(12.5%) | 20(5.6%) | 143(39.7%) | 47(13.1%) | 13(3.6%) |

[a] Multiple failures, cause unknown.

[b] Failure due to water hammer.

[c] Inadequate testing due to personnel errors or to inadequate procedures.

the impeller wear rings and the bushings." These events were also included in the category "cause unknown".

About 84% of the reported events refer to strictly RHR components. Failure causes that led to multiple failures, or had the potential to lead to such failures, contributed a significant part of the reported events. More specifically, Table 4.3 shows that these causes (design, manufacturing, fabrication, installation, personnel and procedural errors, other) contributed:

| | |
|---|---|
| RHR Valves | 39% |
| RHR Pumps | 66% |
| RHR Related Instrumentation | 15% |
| RHR Heat Exchangers | 69% |
| RHR Piping and Fittings | 76% |
| RHR Standby Coolant Supply | 100% |
| RHR Testing | 100% |
| Equipment Cooling System | 57% |
| RHR Service Water System | 47% |

These results show that a reliablity assurance program must pay special attention to causes that have the potential to lead to multiple failures. Such failures not only can have a very significant impact on system reliability, but it is also very difficult to account for them in reliability analyses.

Finally, it must be pointed out that in the IREP study performed for Browns Ferry, the multiple failures considered for RHR components were only: (a) combinations of random failures, (b) multiple instrumentation failures due to miscalibration errors, and (c) operator failure to manually initiate or isolate a system, or initiate a transfer.

## 4.2 Operating Experience with the Browns Ferry RHR System

From the NSIC data base 61 events were identified that refer to failures in components of the RHR systems, and 10 events that refer to components of the equipment cooling water systems or the RHR service water systems of the three Browns Ferry Units. A categorization of the analyzed

LERs by system or subsystem and cause of failure is presented in Table 4.4. Instrumentation drift dominates the RHR related events (38%), the RHR valve failures follow with a contribution of 27%. About 38% of the reported events were attributed to design, installation and personnel errors or procedural deficiencies which are potential sources of common-cause failures. If the instrumentation failures, due to drift, are not counted, the contribution of the above events is raised to 61%.

A brief description of the reported LERs is given in Table 4.5. This description shows that 58% of the RHR valve events and all the RHR pump events are due to failures of electrical components. A number of the events described in Table 4.5 are worthy of special mentioning. Three LPCI MG set failures due to loss of lubricant were reported within one year. Seven RHR heat exchanger gasket leaks were reported all due to loose flange nuts. The standby coolant supply to Unit 3 was isolated due to defective procedures. A seal failure in the air vacuum valve of the A2 RHRSW pump, flooded the A RHRSW pump room, and rendered three, A1, A2 and A3, RHRSW/EECW pumps inoperable. Due to administrative deficiency three RHRSW system pumps were rendered unavailable. The RHR pump seal heat exchanger water flow was found inadequate, due to piping restrictions caused by accumulation of mud and shells. The core spray room cooler was found inoperable due to flow restrictions caused by biofouling, silt accumulation and corrosion. All these events caused multiple failures or had a strong potential to cause multiple failures. Such multiple failures were not considered in the IREP study for Browns Ferry, Unit 1.

Table 4.4. Categorization of RHR Related LERs Reported by Browns Ferry

| Component or System | Number of Faults | Design | Installation | Personnel | Procedures | Drift | Unknown or Random |
|---|---|---|---|---|---|---|---|
| RHR Valves | 19 | 3 | 1 | 3 | 1 | | 11 |
| RHR Pumps | 5 | | | 2 | 2 | | 1 |
| RHR Related Instrumentation | 27 | | | | | 27 | |
| RHR Heat Exchangers | 7 | 7 | | | | | |
| RHR Piping and Fittings | 1 | | | | | | 1 |
| RHR Standby Coolant Supply | 1 | | | | 1 | | |
| RHR Testing | 1 | | | | 1 | | |
| Equipment Cooling System | 9 | | | 1 | 4 | | 4 |
| RHR Service Water System | 1[a] | 1 | | | | | |
| Total | 71 | 11(15.5%) | 1(1.4%) | 6(8.5%) | 9(12.7%) | 27(38%) | 17(23.9%) |

[a] Two additional faults were common with the EECW system and have been included in the equipment cooling system faults.

Table 4.5. Brief Description of RHR Related LERs Reported by Browns Ferry

RHR Valves

1. Relay Coil Overheat.
2. Maintenance Personnel Failure to Replace Damaged Worm Shaft.
3. Loss of Lubricant in RMOV MG Set (11/18/81).
4. Loss of Lubricant in RMOV MG Set (11/24/81).
5. Loss of Lubricant in RMOV MG Set (10/9/82).
6. Valve Fails to Open - Relay did not Make Contact.
7. Broken Valve Operator Switch - Vibration Problem.
8. Valve Motor Bolts Broke.
9. Motor Braker Tripped.
10. Grounded Motor Caused Braker Trip.
11. Check Valve Leak (Four Previous Events).
12. Failure of a Gear Tooth in the Limit Switch.
13. Hardened Valve Stem Lubricant Caused Motor Trip.
14. Bearing Locknut Stripped - Caused by Motor Brake Being Out of Adjustment.
15. Bearing Locknut Stripped.

RHR Pumps

1. Pump 3C Motor Failed on Ground Overcurrent.
2. Loose Locking Nuts on Overcurrent Relay Caused Pump Trip.
3. Breaker Control Relay Dropped Due to Open Wire in Cable.
4. Pump Inoperable Due to Loose Breaker Trip Nut.
5. Motor Tripped on Instantaneous Overcurrent - Relay Settings Were Revised.

RHR Related Instrumentation

Twenty Seven LERs - Cause: Instrument Drift.

RHR Heat Exchangers

Seven LERs - Cause: Leaky Gasket Due to Loose Flange Nuts.

Table 4.5. Brief Description of RHR Related LERs Reported by Browns Ferry (Cont'd).

RHR Piping and Fittings

1. RHR Snubber Failed After a Locking Key Vibrated.

RHR Standby Coolant Supply

1. Cue to Defective Procedures the Standby Coolant Supply to Unit 3 was Isolated.

RHR Testing

1. Due to Defective Procedures, RHR was not Properly Tested.

Equipment Cooling System

1. Air Vacuum Valve of A2 RHRSW Pump Failed to Seal - RHRSW Pump Room A Flooded - A1, A2 and A3 RHRSW/EECW Pumps Rendered Inoperable.
2. Due to Administrative Deficiency Three Pumps were Rendered Unavailable.
3. RHR Pump Seal Heat Exchanger Water Flow was Inadequate - Piping Restriction Due to Mud and Shells in Piping (5/12/80, Browns Ferry 3).
4. Same as Previous LER (8/9/80, Browns Ferry 3).
5. Core Spray Room Cooler Inoperable - Biofouling Silt Accumulation, and Corrosion Caused Flow Restrictions (11/8/80, BF3, One Previous Event).
6. RHR Pump Room Cooler Leak - Crack at Vent Nipple of Cooler Coil.
7. Core Spray Area Cooler Fans Inoperable-Overload Relays Tripped (One Previous Event).

RHR Service Water System

1. RHRSW System Pipe Hangers Found to be Nonfunctional.

## 5.0 Risk Related Reliability Requirements

The concept of risk, which is a function of both the frequency of accident sequences and their potential consequences to health and property, can be used as a quantitative measure of safety. For risk considerations, only accidents that lead to core degradation are significant. From an investment risk viewpoint, accident sequences that lead to core damage are also extremely undesirable. Thus, the probability of a core melt can be used as a measure of risk for safety as well as for economic considerations. The Nuclear Regulatory Commission staff has also proposed to use the likelihood of a large-scale core melt as a provisional guideline in evaluating probabilistic risk assessments of nuclear power plants. For the purposes of this study the core melt probability can be used as the quantitative measure of safety.

The core melt probability is a function of the frequencies of the initiating events that have the potential to lead to core melt and of the unavailabilities of the plant systems that must be operable to prevent core damage. After an upper limit on the core melt probability has been established, reliability goals can be set for the different plant systems that are consistent with the safety limit on the core melt probability. The reliability goals can be expressed in terms of system unavailabilities for the different risk-significant accident sequences that involve the system under consideration. These unavailabilities are requirements imposed on a reliability assurance program by plant safety which is measured by the plant risk.

In setting reliability goals for a specific plant system all the significant accident sequences that involve this system must be considered. Its reliability goals will be functions of the frequencies of the events initiating the accident sequences and of the reliabilities of the other reactor systems involved in these sequences. If the frequency of one or more of the initiating events is a controllable parameter, i.e., it depends on the reliability of plant systems or the reliability of controllable human actions, then in setting a reliability goal for a specific plant system a trade-off is available between reliabilities of systems and human actions involved in the initiating events, as well as of systems involved in the sequences under consideration after accident initiation. Performing the proper trade-offs in selecting system reliability goals can have a crucial impact on the feasibility and economic cost of achieving these reliabilities. After a reliability goal has been set for a system, a reliability assurance program must ascertain that all the activities during the system's life-cycle, starting from design and proceeding to manufacturing, installation, preoperational testing, and operation, are consistent with this goal.

As discussed in Section 3.1.1, the IREP study for Browns Ferry estimated a core melt frequency of $1.3 \times 10^{-4}$ for accidents sequences that involve failure of the RHR system. This constitutes about 70% of the estimate for the core melt frequency due to internal accident initiators. About 78% of this contribution was attributed to sequences initiated by events that did not involve loss of offsite power, and the remaining 22% to sequences initiated by LOSP. The above estimates were derived from RHR unavailability estimates of $5.7 \times 10^{-5}$, and $9.4 \times 10^{-4}$ for non-LOSP and LOSP initiating events, respectively. If the core melt frequency of $1.3 \times 10^{-4}$, due to accident sequences involving RHR failure, is considered acceptable, the IREP unavailability estimates for RHR can be used as reliability goals. An RHR reliability assurance program for the reference plant must provide convincing evidence, that throughout its lifetime its RHR system unavailabilities are smaller or equal than these goals. The analysis presented in the previous sections shows that in setting reliability goals for the RHR system and in developing a reliability assurance program for the same system, the following must be considered.

Failure of an RHR minimum-flow bypass valve to close would divert about 10% of the flow from its associated loop. In the IREP study such a failure was treated as a loop failure. The same study showed that if a failure of an RHR minimum-flow bypass valve to close does not cause failure of its associated loop, the unavailability of decay heat removal ($R_B R_A$) is reduced to $2.6 \times 10^{-6}$. This value is 22 times lower than the unavailability of decay heat removal presented in Table 3.3 for initiatinq events that do not render the offsite power unavailable (credit for recovery from RHR faults is considered). The contribution to the core melt frequency of accident sequences that involve failure of the RHR system and are initiated by non-LOSP events becomes also 22 times smaller.

Even if 90% of the loop flow is not adequate for successful operation of the torus cooling mode, this flow will significantly extend the time before the suppression pool water temperature reaches its limiting value. This in turn will extend the time available for corrective actions. The evaluation of the impact that a bypass valve failure has on system success, will affect significantly the required RHR reliability assurance program. If a bypass valve failure to close does not cause loop failure, the RHR reliability is significantly improved, and consequently the burden of proof imposed on the reliability assurance program may be correspondingly relaxed or the RHR safety margin increased. The same result may be obtained by relocating the bypass flow branching point after the RHR/RHRSW heat exchanger (see Fig. 2.1).

In the IREP study, no credit was taken for recovery of the power conversion system (PCS) in accident sequences initiated by transients that render it unavailable. As discussed in Section 3.1.4, if the WASH-1400 data for recovery of the PCS is valid for Browns Ferry, the frequency of accident sequences initiated by such transients is reduced by two orders of magnitude. This may relax very significantly the requirements on the unavailability of the RHR system, or improve the existing margin of safety which in turn may reduce the burden of proof on the RHR reliability assurance program. If existing data from Browns Ferry can not support the WASH-1400 data, but the potential of recovering the PCS with probabilities as the ones given in WASH-1400 is present, a trade-off may exist between RHR unavailability and PCS recovery, which a reliability assurance program should consider.

A reliability assurance program must identify the dominant contributors to the unavailability of the system under consideration and ascertain that their contributions are consisent with the system reliability goal. If reliability goal changes have to be made, the dominant contributors show how such changes can be affected more effectively. Certain trade-offs may also exist between the dominant contributors, that reduce the burden of proof on the reliability assurance program or have cost advantages. Finally, the dominant contributors will dictate which the major elements of a reliability assurance program should be for the system under consideration. For example, if human errors is one of the dominant contributors, assurance of human reliability should be one of the major elements of the reliability assurance program.

Moreover, since the purpose of this study is to ultimately develop a reliability assurance program utilizing also the experience of other non-nuclear high technology industries, the dominant contributors will indicate what elements and methods of reliability assurance programs from these industries are most suitable for adoption in the nuclear industry.

As discussed in Section 3.1.3, from the RHR unavailability analysis presented in the IREP study for Browns Ferry the following dominant contributors have been identified for non-LOSP initiating events. Failure of the shutdown cooling mode ($R_A$) is dominated by faulty suction valve isolation signals (49%) and random failures of the same valves (45%). Operator failure to initiate shutdown cooling contributes 5% to the unavailability of this cooling mode. Failure of the torus cooling mode is dominated by: operator failure to initiate torus cooling (32%); double failures involving failure of one RHRSW header and either a RHR system valve failure, or one RHR system loop in test or maintenance (25%); other combinations of random hardware failures. RHR valve failures are dominated by control valve circuit failures. Taking credit for recovery from RHR faults reduces the unavailability of decay heat removal ($R_B$ $R_A$) by 25%. The core melt frequencies calculated in the IREP study have included this credit.

In the IREP study, a time window of six to eight hours was considered for recovery of RHR failures. This time interval was based on the available water inventory in the Condensate Storage Tank (CST). As discussed in Section 3.2, the analysis performed in the SASA program shows that the available time interval is about 28 hours. This estimate is based on the expectation that the CST is nearly full of water, and on the capability of the CRD pump to provide the required coolant injection after four hours into the transient. Cooling injection by the CRD pump was ignored in the IREP study. Extending the available time window from eight hours to 28 hours, reduces greatly the probability considered in the IREP study for operator failure to initiate shutdown cooling or torus cooling. The same extension enhances the probability for recovery from RHR faults. Consequently, assuring that the CST remains always nearly full and a reasonable availability for the CRD pumps, may relieve further the reliability requirements or improve the reliability margin of RHR.

For accident sequences that are initiated by loss of offsite power, as the analysis presented in Section 3.1.3 shows, the dominant contributors to the unavailability of the RHR system are failure of three or more diesels to start due to common cause, and failure to recover offsite power. Both of these contributors are independent of the RHR system reliability. The core melt frequency due to such accident sequences is strongly dependent on the frequency of loss of offsite power, the rate for failure of three or more diesels to start, the availability of DC power, and the probabilities for failure to recover offsite power and failed diesel generators. The available data for the frequency of LOSP events, the rate of failure of more than one diesels, and for recovery of LOSP and failed diesels shows wide variations. The analysis presented in this report shows that if the probability to recover the PCS is substantial (as many PRAs, including WASH-1400, indicate), loss of offsite power events, including station blackout, are the initiators of the top dominant accident sequences that involve failure of the RHR system. In the IREP study for Browns Ferry, non-LOSP events were identified as the initiators of the top dominant accident sequences. Since the dominant accident sequences will indicate where a reliability assurance program should concentrate its resources, the need to identify these sequences with confidence is obvious.

The above discussion also makes obvious the need of an adequate reliability data base including frequencies of initiating events, failure rates, and probabilities of recovery from failures.

The analyses performed in the SASA program for the loss of decay heat removal sequences at Browns Ferry, show very clearly that reliability and PRA analyses must be supported by detailed analyses of the plant's response to risk-significant accident sequences. Such analyses provide the information required to determine systems operability under the prevailing accident conditions, to define the required operator actions, and determine the available time for recovery of failed systems. Thus, the analysis of system response to risk significant accident sequences must be one of the major inputs of a reliability assurance program.

The analysis of the emergency operating instructions, presented in Section 3.3, shows that these instructions are one of the major parameters that determine the effectiveness of human action under accident conditions. Their impact is especially significant in accident sequences where the available time for operator action is short, as the case is in the event the high pressure injection systems are unavailable, or offsite power has been lost. In accident sequences that involve LOSP and failure of three or more diesel generators to start, with the EOIs analyzed in Section 3.3, the resulting core melt frequencies would be up to one order of magnitude greater than the frequencies resulting from the operator actions indicated by the SASA analysis. This conclusion has special significance since these sequences are among the dominant ones. The development of effective emergency operating instructions for the risk-significant accident sequences must be one of the major elements of a reliability assurance program.

A continuous evaluation of operating experience data must also be one of the basic elements of a reliability assurance program. It provides the required input data to assess system and human factor reliability performance, to measure the success of a reliability assurance program, and determine where its efforts should be concentrated in order to achieve its objectives. The analysis of the LERs presented in Section 4.0 shows that for RHR components about 54% and 61% of the events (other than instrument drift) reported from all BWRs and from the three Browns Ferry Units, respectively, were multiple failures or had the potential to be multiple failures. These failures were attributed to design, manufacturing, fabrication, installation and personnel errors, or procedural deficiencies. These results indicate that a reliability assurance program for the RHR system must pay special attention to the above potential causes of multiple failures. In the RHR reliability analysis performed in the IREP study for Browns Ferry, from the different multiple failures or potential multiple failures indicated by the LER analysis only some personnel errors were accounted. Consequently, the contribution of multiple failures to the unavailability of the reference system must be re-evaluated. The information that can be extracted from the LERs is limited by the shortcomings of the LER reporting system. This information can be utilized more effectively if it is supplemented with information from plant records, and inputs from experts involved in the design, manufacturing, installation, operation and maintenance of the system considered.

The brief scoping analysis for the BWR RPS presented in Appendix A shows the following. The unavailability estimates presented in the literature for the BWR RPS system vary from $6.7 \times 10^{-7}$ to $1 \times 10^{-4}$ failures per demand (median values). The dominant contributions to this unavailability are: (a) failure of a sufficient number of control rods to insert, (b) common-cause failures due to human error, and (c) failure of the scram discharge volume. The estimates of their contribution to the RPS unavailability vary significantly.

The estimates of the frequency of accident sequences that are characterized by failure to scram also vary greatly from $3 \times 10^{-7}$ to $2 \times 10^{-4}$. The esimates for their contribution to the BWR core melt probability cover the range from 2% to 91%.

The above wide variations are due to the lack of adequate experience data on RPS failures and transient frequencies during the lifetime of a BWR, and especially to inadequate data and analytic models for common-cause failures, including failures due to human error.

The scoping analysis of the RPS LERs shows that multiple failures, or potential multiple failures due to design, manufacturing, fabrication, installation and personnel errors, as well as procedural deficiencies were responsible for: ~50% of the instrumentation channel events (drift not counted), ~33% of the scram discharge volume events, ~50% of the hydraulic control unit events, 100% of the scram discharge volume events, ~53% of the control rod drive mechanism events, and 100% of the control assembly events.

The results of the RPS analysis stress further the need of an adequate data base derived from nuclear power plant operating experience. This need is more acute for common cause failures including human errors. Experience data from other high technology industries, that face similar high reliability requirements as the nuclear industry, can provide useful inputs in developing interim data bases and models to supplement the scarce data available.

## 6.0 References

1. "Safety Goals for Nuclear Power Plants: A Discussion Paper," U. S. Nuclear Regulatory Commission, NUREG-0880 (February 1982).

2. S. E. Mays, et al., "Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant," NUREG/CR-2802, EGG-2199 (July 1982).

3. "Reactor Safety Study: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/104) (October 1975).

4. D. H. Cook, et al., "Station Blackout at Browns Ferry Unit One - Accident Sequence Analysis," NUREG/CR-2182 (November 1981).

5. D. H. Cook, et al., "Loss of DHR Sequences at Browns Ferry Unit One - Accident Sequence Analysis," NUREG/CR-2973, Preliminary Draft.

6. Browns Ferry Final Safety Analysis Report.

7. F. L. Leverenz, et al., "ATWS: A Reappraisal Part III: Frequency of Anticipated Transients," EPRI NP-801 (July 1978).

8. A. S. McClymont and B. W. Poehlman, "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients," EPRI NP-2230 (January 1982).

9. A. S. McClymont, and B. W. Poehlman, "Loss of Off-Site Power at Nuclear Power Plants: Data and Analysis," EPRI NP-2301, Interim Report (March 1982).

10. A. McClymont and G. McLagan, "Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis," EPRI NP-2433, Interim Report (June 1982).

11. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants," Instrument Society of America, 1982.

## Appendix A

### Risk Related Reliability Considerations for the BWR Reactor Protection System

Probabilistic risk assessments that have been performed for BWR plants show that the risk from the operation of these plants is dominated by accident sequences involving either failure of the decay heat removal systems, or failure of the reactor protection system. As discussed in the main report, the residual heat removal system of the Browns Ferry, Unit 1, was chosen as a reference system in this study. To assure that the information obtained from the analysis of the reference system, on the parameters that are expected to be of main importance in a reliability assurance program, are not strongly biased by the reference system, a similar scoping analysis was performed using as a basis the BWR reactor protection system (RPS). In this brief scoping study, the following tasks have been undertaken: (a) a review of generic information on the availability of the BWR reactor protection system, on the contribution of reactor protection system failures to the risk from BWRs, and on reactor protection system common-cause failures, (b) a scoping analysis of the operating experience with the BWR reactor protection system.

This Appendix is organized as follows. The first section gives a brief description of the Browns Ferry RPS. In Section A.2, generic information on the unavailability of the BWR RPS, on its contribution to the risk from BWRs, and on RPS common cause failures is reviewed. From this review conclusions are derived on the parameters that dominate the risk contribution of the BWR RPS. In Section A.3, a scoping analysis of the Licensee Event Reports for the BWR reactor protection system is presented.

### A.1 Browns Ferry Reactor Protection System

This section gives a brief description of the Browns Ferry RPS based on the information provided in the Browns Ferry Final Safety Analysis Report[1].

The RPS can be divided into two subsystems; the electrical subsystem and the mechanical subsystem. The electrical subsystem monitors the state of the plant and generates a scram signal whenever a trip variable exceeds its set limit. The mechanical subsystem inserts the control rods into the core upon receipt of a scram signal.

### A.1.1 Electrical Subsystem

The electrical subsystem, shown in Fig. A.1, consists of instrument channels and logic channels. An instrument channel is an arrangement of one or more sensors and associated components or modules. The sensors monitor the operating variables that are used for reactor protection. If one of these variables exceeds its set limit, the instrument channel generates a trip signal, i.e., its electric contact opens and the corresponding relay is deenergized. In Browns Ferry, 11 operating variables are used for reactor protection. These variables are listed in Table A.1.

Table A.1. Operating Variables Used in Browns Ferry for Reactor Protection

1. Neutron Flux
2. Reactor Vessel Pressure
3. Drywell Pressure
4. Reactor Vessel Water Level
5. Main Condenser Vacuum
6. Main Steam Line Radiation
7. Main Steam Line Isolation Valve Closure
8. Turbine Control Valve Fast Closure
9. Turbine Stop Valve Closure
10. Scram Discharge Volume Water Level
11. Low Instrument Air Pressure

The logic channels are arranged into two independent trip systems, A and B. Each trip system consists of two automatic 1/11 (one out of 11) logic channels, one manual scram channel, and four actuator logic channels. The automatic 1/11 logic channels are identified as A1, A2, B1, B2 (see Fig. A.1). The manual channels are identified as A3 and B3. Each actuator logic receives input from the two automatic 1/11 logic channels and

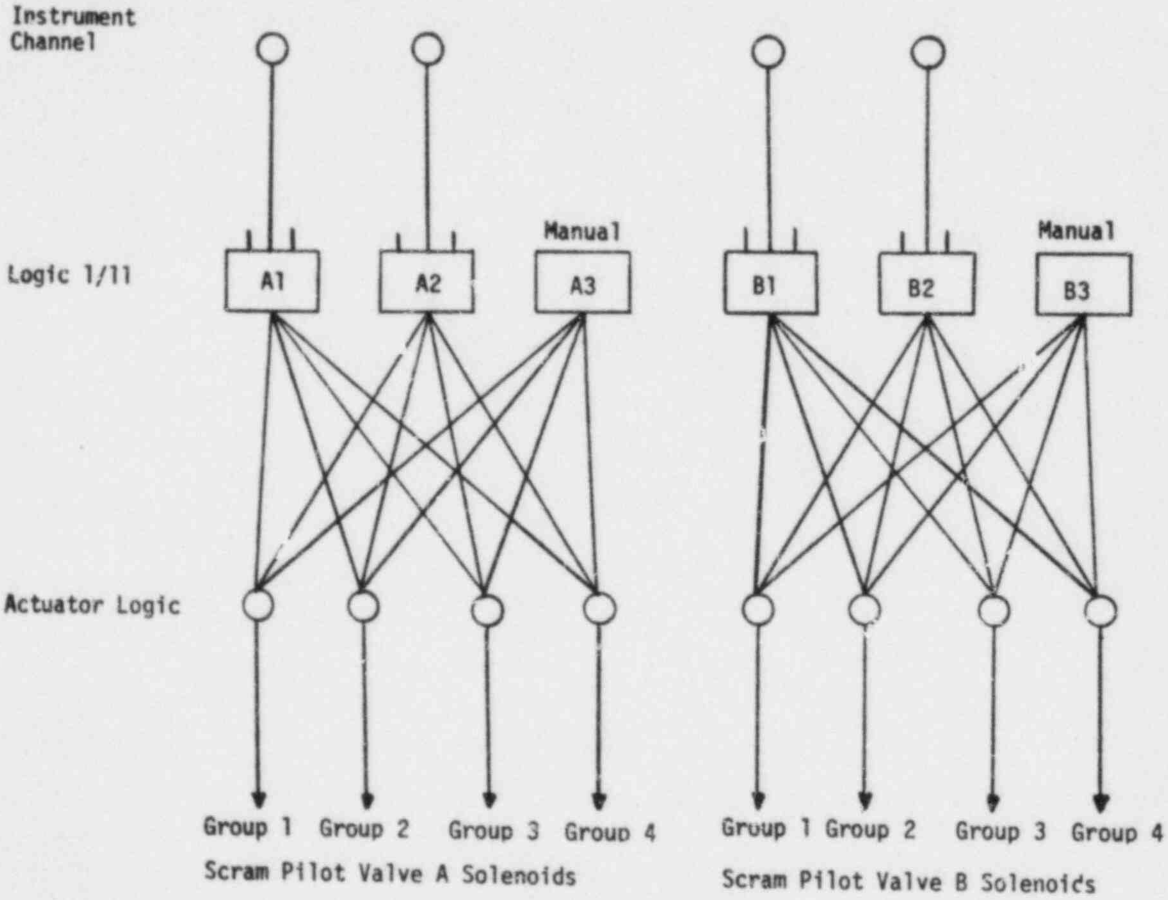


Fig. A.1. Schematic of the RPS Electrical Subsystem

the manual scram channel of its trip system, and feeds one group of trip pilot valve solenoids of the mechanical subsystem. The actuator logics are 1/3 logics (1/2 in the automatic mode).

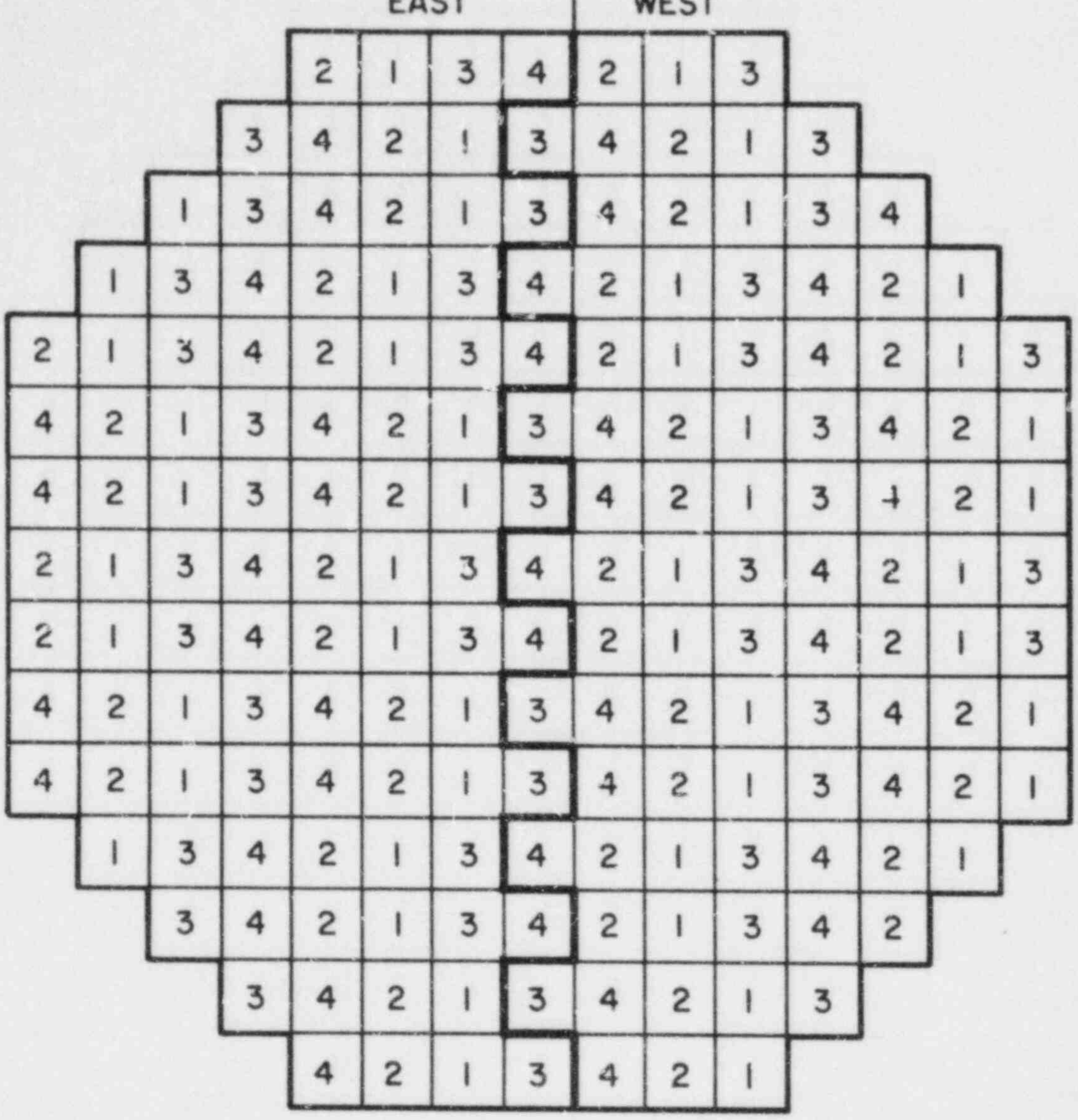
Each 1/11 logic channel receives input from at least one instrument channel for each monitored variable. Whenever an instrument channel generates a trip signal, its relay is deenergized and its corresponding contacts in the 1/11 logic channel open. In turn, the relays of the 1/11 logic channel are deenergized and their contacts in the actuator logic channels open. Each trip system (A,B) generates an automatic trip whenever one of its two 1/11 logic channels generates a trip signal. As discussed in the next section, to generate a reactor scram signal both trip systems must be tripped. Thus, the overall logic of the RPS can be characterized as one out of two taken twice.

### A.1.2 Mechanical Subsystem

The mechanical subsystem consists of the control rods and their associated drive and hydraulic control units, and of two scram discharge volumes. Each control rod has its own drive unit and hydraulic control rod unit. There are 185 control rods arranged into two sections and four groups as shown in Fig. A.2. All the control rods that belong to the same section are connected to the same scram discharge volume header.

The control rod drive mechanism, shown in Fig. A.3, is a double-acting, mechanically latched, hydraulic cylinder that uses water from the condensate storage tank as its operating fluid. The individual drives are mounted on the bottom head of the reactor pressure vessel.

The main moving assembly of the drive is made up by the drive piston and the index tube (Fig. A.3). The drive piston is mounted at the lower end of the index tube, it operates in the annular space between the fixed piston tube and the drive cylinder, and has both inside and outside seal rings. The index tube is a long hollow shaft having circumferential locking grooves spaced every six inches along the outer surface. These grooves transmit the weight of the control rod to the fingers of the collet assembly which positions the rod.

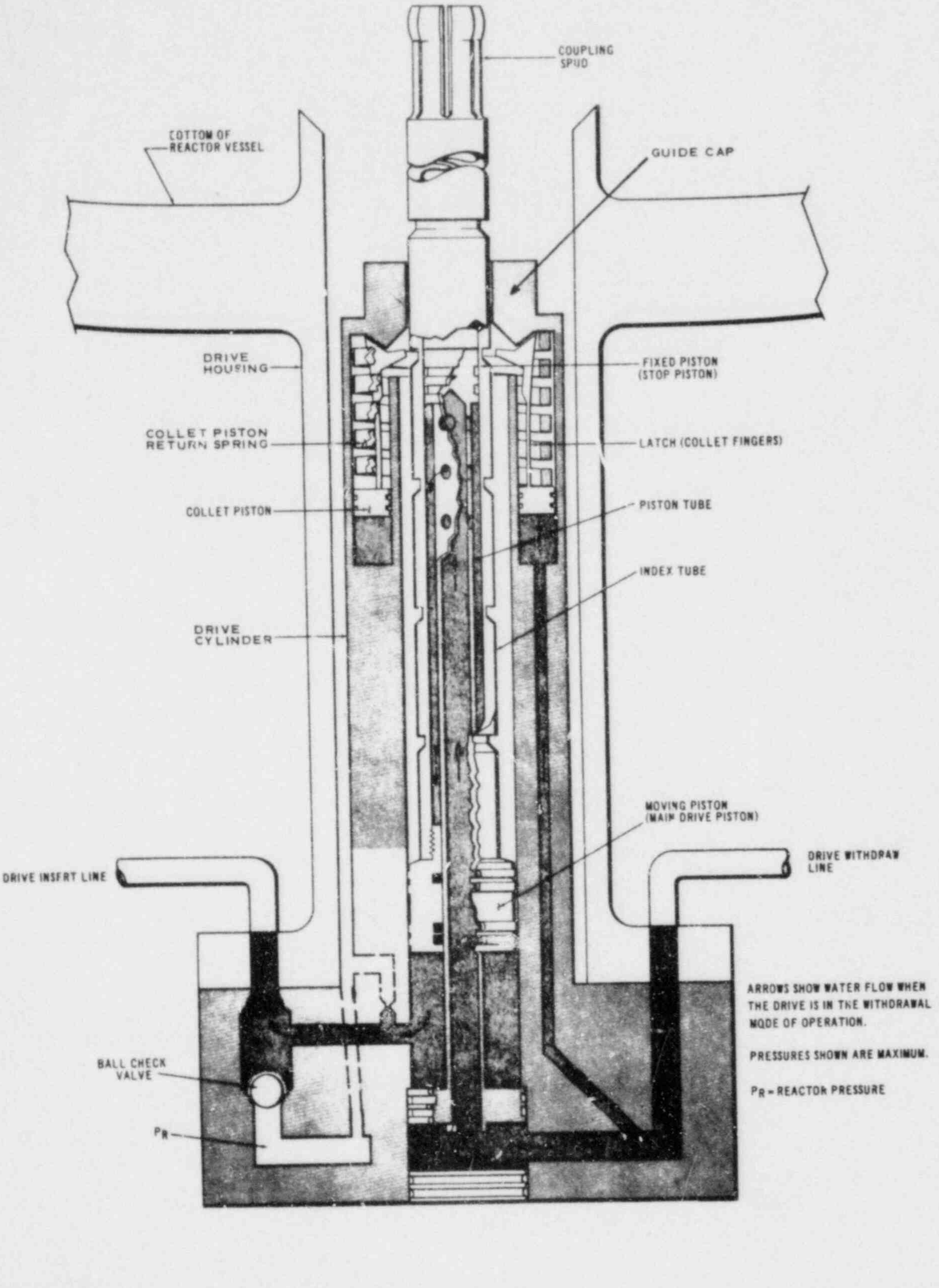


EAST WEST

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2 | 1 | 3 | 4 | 2 | 1 | 3 | | | | |
| | | | 3 | 4 | 2 | ! | 3 | 4 | 2 | 1 | 3 | | | |
| | | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | | |
| | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | |
| 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 |
| 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 |
| 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 |
| 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 |
| 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 |
| 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 |
| 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 |
| | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | |
| | | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | 4 | 2 | | |
| | | | 3 | 4 | 2 | 1 | 3 | 4 | 2 | 1 | 3 | | | |
| | | | | 4 | 2 | 1 | 3 | 4 | 2 | 1 | | | | |

NOTE: EACH SQUARE IN THE FIGURE REPRESENTS A CONTROL ROD

Fig. A.2. Arrangement of Control Rods into Groups



ARROWS SHOW WATER FLOW WHEN THE DRIVE IS IN THE WITHDRAWAL MODE OF OPERATION.

PRESSURES SHOWN ARE MAXIMUM.

$P_R$ = REACTOR PRESSURE

Fig. A.3. Control Rod Drive

The collet assembly positions the control rod and prevents accidental downward movement of the index tube. It consists of the collet fingers, a return spring, a guide cap, a collet housing, and the collet piston seals. The collet piston is normally held in the latched position by the force of the return spring. It is properly unlatched during control rod withdrawal.

Each hydraulic control unit (Fig. A.4) consists of manual, pneumatic, and electrically operated valves, an accumulator, filters, related piping, and electrical connections. During normal reactor operation, the scram pilot valves are energized. In this state, they apply pressurized air to the pneumatic actuators of the scram inlet valve and the scram exhaust valve to hold them closed. The scram accumulator is charged with water to approximately 1500 psi. The power of one of the scram pilot valves is controlled by trip system A and the power of the other by trip system B. The scram pilot valves are connected in series. Thus, both must be deenergized to open the scram valves. Upon receipt of a scram signal from both trip systems, the scram pilot valves are deenergized, the air pressure to the pneumatic actuators of the scram valves is relieved, and both valves open. High pressure water from the accumulators is admitted under the drive piston, the area over the drive piston is vented through the scram exhaust valve to the scram discharge volume, and the control rods are inserted into the core.

The accumulator of each control rod has adequate water capacity to complete a scram in the required time at low reactor vessel pressures. At higher reactor vessel pressures, as the accumulator pressure falls below the vessel pressure, a ball check valve (Fig. A.3) opens and reactor water is admitted under the drive piston to complete the scram stroke.

The air pressure in the trip pilot valve air header is controlled by two solenoid-operated backup scram valves. These two valves provide a second means of controlling the air supply to the scram valves of all the control rods. The solenoids of the backup scram valves are normally deenergized. When both trip systems A and B are tripped, the solenoids are energized and the backup valves vent the air supply of the scram valves. Thus, the backup scram valves will override any trip pilot valve which will fail to exhaust the air supply of its scram valve.

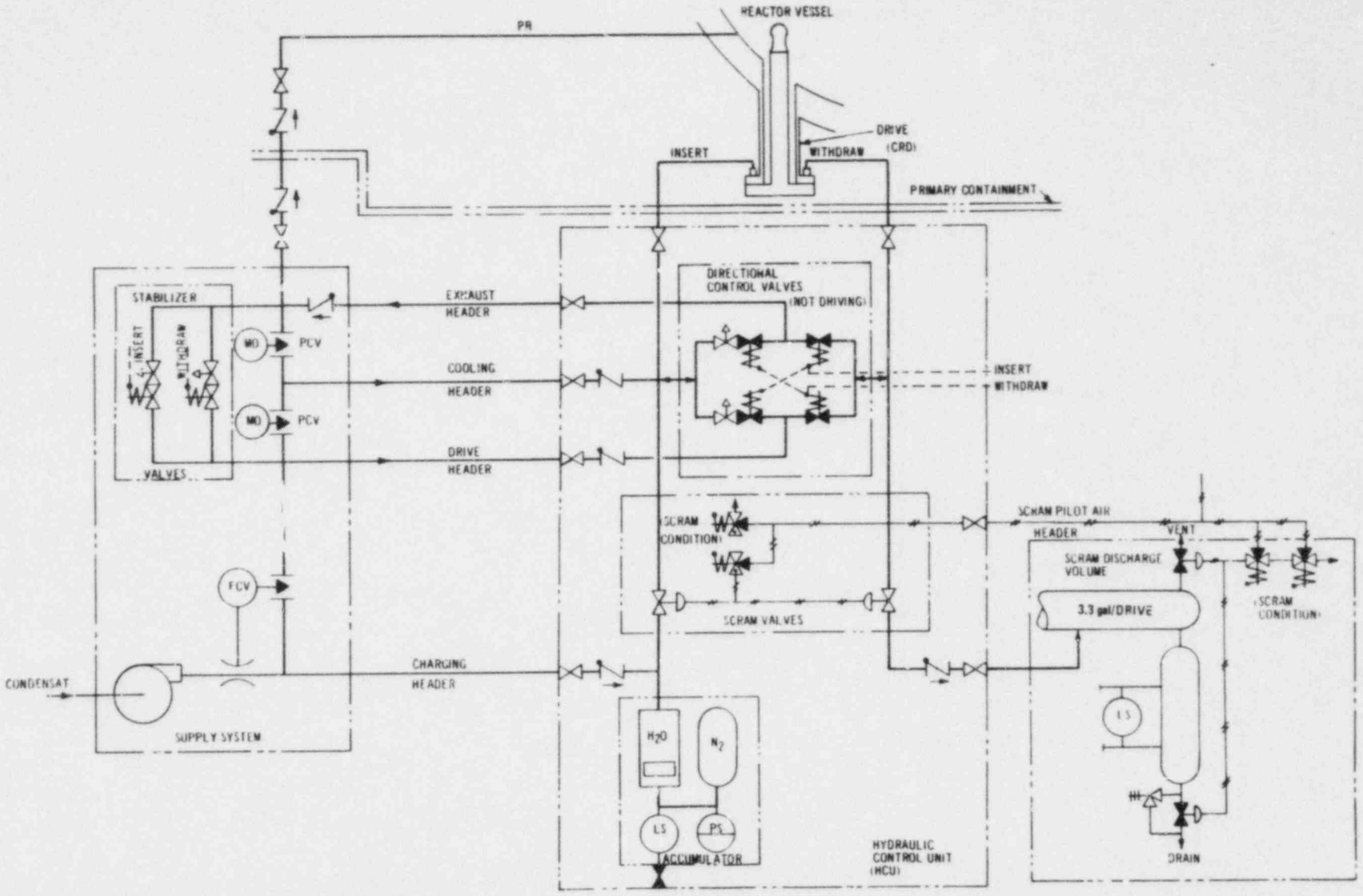


Fig. A.4. Control Rod Drive Hydraulic and Pneumatic System Schematic

During normal plant operation, the scram discharge volume header is empty with both its drain and two vent valves open. Upon receipt of a scram signal, to prevent loss of water from the reactor, the drain and vent valves close. Position indicator switches on the drain and vent valves indicate valve position by lights in the control room.

During a scram, the scram discharge volume header partly fills with water which is discharged from above the drive pistons. While the reactor is scrammed, the control rod drive seal leakage continues to flow to the discharge volume until the discharge volume pressure equals reactor vessel pressure. There is a check valve in each HCU which prevents reverse flow from the scram discharge header volume to the drive. When the initial scram signal is cleared from the reactor protection system, the scram discharge volume scram signal is overridden with the override switch and the scram discharge volume is drained. A control system interlock will not allow the drives to be withdrawn until the discharge volume is emptied to a safe level.

Six level switches on the scram discharge volume, set at three different water levels, guard against operation of the reactor without sufficient free volume present in the scram discharge volume to receive the scram discharge water in the event of a scram. At the first (lowest) level, one level switch initiates an alarm for operator action. At the second level, one level switch initiates a rod withdrawal block to prevent further withdrawal of any control rod. At the third (highest) level, the four level switches (two for each reactor protection system trip system) initiate a scram to shut down the reactor while sufficient free volume is still present to receive the scram discharge. After a scram, these same level switches must be cleared by draining the scram discharge volume before reactor operation can be resumed.

Since the partial scram failure event at Browns Ferry 3 on June 28, 1980, several modifications have been or will be made to the scram discharge system to prevent a similar event. A sonic instrumentation system has been mounted on each scram discharge volume header to back up the level switches in the instrument volume. This system generates an alarm in the main control room. Also, the two scram discharge volume headers will be decoupled so that each one of them will have its own instrument volume. Each instrument volume will have two float and two differential pressure level sensing instruments feeding the reactor protection system.

## A.2 Risk Related Reliability Considerations

### A.2.1 Unavailability of BWR Reactor Protection System

In WASH-1400,[2] the Peach Bottom Unit 2 was used as a reference BWR. A median estimate of $1.3 \times 10^{-5}$ per demand was obtained for the unavailability of the RPS of this BWR. The dominant contributions to this unavailability were due to the following events: (a) failure of three adjacent control rods to insert on reactor trip signal, (b) common-cause failure of the electrical subsystem of the RPS due to miscalibration of sensing switches, (c) plugging of the drain line that connects the header of a scram discharge volume (SDV) with the trip discharge instrument volume. The contributions (point estimates) of these events to the RPS unavailability were:

Failure of three adjacent rods = 73%,<br>
Common-cause failure due to human error = 24%,<br>
Plugging of the SDV drain line = 3%.

The failure rate of three adjacent control rods is dominated by common-cause failures. It must be pointed out that the unavailability analysis of the BWR RPS presented in WASH-1400 was based on the assumption that a loss-of-coolant accident had taken place. This assumption is important in the calculation of the contribution to the RPS unavailability of the common-cause failure due to miscalibration of sensing switches. The quantification of the RPS failure rate due to this cause of failure was based on the trip parameters that generate a trip in the event of a LOCA.

In the context of the ATWS studies performed by EPRI, the unavailability analysis of the BWR RPS presented in WASH-1400 was reexamined. In WASH-1400, a lognormal distribution was used for the failure of three adjacent control rods and a failure rate of $1 \times 10^{-4}$ per demand for a single control rod. In the EPRI analysis,[3] a normal distribution for the failure of three adjacent control rods was considered a better representation of this event, and a control rod failure rate of 8.9 x $10^{-6}$ per demand was used, based on a reevaluation of the BWR control rod failure data base. Due to these differences, a median estimate of 2.3 x $10^{-6}$ and a mean of 5.2 x $10^{-6}$ was obtained in the EPRI analysis for the unavailability of the BWR RPS. In this new unavailability estimate, the dominant contributions were: (a) common-cause failure due to miscalibration or damage (human error) of the sensing switches ~83.8%, (b) plugging of the SDV drain line ~14.8%, and (c) failure to insert three adjacent control rods ~1.4%.

Attempts have been made to estimate the unavailability of LWR protection systems utilizing the accumulated experience from the operation of these reactors. Three events have occurred in operating BWRs that had the potential to cause a scram failure due to a common-cause malfunction in the RPS. These events are: (a) the Kahl relay failure, (b) the RPS relay problem at Monticello, and (c) the partial failure to scram at Browns Ferry Unit 3.

At the Kahl BWR, the original scram relays were replaced by a complete new set. Testing of the new set before the reactor returned to operation did not reveal any problems. However, due to inadequate heat curing of a protective coating during manufacturing of the relays, heat generated in the coils during reactor operation hardened the coating and caused the contact points of the relays to stick closed. Thus, interruption of power would not open the stuck contacts and scram would not be initiated. The malfunction was discovered during a periodic surveillance test.

The same common-cause failure occurred at the Monticello BWR. In this case, the long period of preoperational testing produced the necessary conditions for failure before initiation of reactor operation and the failure was discovered during preoperational testing. In addition, the failure observed at Monticello was partial, i.e., it did not cause a complete RPS failure.

On June 28, 1980, at Browns Ferry 3, manual scram from ~36% power failed to insert about 40% of the control rods (out of 185)[4,5]. Scram was finally achieved in about 15 minutes after two additional manual scram attempts and one automatic scram. The failure was caused by an accumulation of water in the header of the east-side scram discharge volume which had not been detected by the instrumentation of the instrument volume. Although the detailed reasons of the failure are not known, it seems that it was caused by poor hydraulic coupling between the scram discharge volume and the instrument volume.

Since there is not enough data to estimate the BWR RPS unavailability from BWR experience alone, in scram failure estimates based on operational experience, BWRs and PWRs are treated as parts of the same population. Further, the operating experience data suffers from unresolved questions which include: (a) the number of scram failures that have occurred, (b) the applicability of the data from the naval reactors to commercial LWRs, and (c) the appropriate testing frequency. EPRI[6] and Ref. 7 consider the navy data as applicable to commercial LWRs. The NRC staff, in NUREG-0460[8], excludes the navy data. EPRI and Ref. 7 consider the Kahl event as rectified and do not count it as a scram failure in the estimation of the RPS unavailability. The NRC staff rejected the EPRI argument of "rectifiability" and counted the Kahl event as a scram failure. The Monticello event, since it was discovered in a preoperational test, is not counted as a scram failure in all the above studies. The Browns Ferry partial failure to scram occurred after the publication of the above studies.

There are also significant differences in the RPS testing frequency utilized in these studies. In the EPRI document[6], EPRI NP-251, testing frequencies of 26 and 60 tests per reactor-year were assumed for the commercial and the navy reactors, respectively. In Ref. 7, testing frequencies of 200, 23, and 60 tests per reactor-year were used for the BWRs, PWRs, and navy reactors, respectively. Finally, the NRC staff in NUREG-0460 used a testing frequency of 12 tests per year (one per month).

Different estimates for the unavailability of the BWR RPS, as summarized in NUREG-0460, are given in Fig. A.5. The median values presented in this figure vary from $6.7 \times 10^{-7}$ to $1 \times 10^{-4}$ failures per demand. The NRC staff argues in NUREG-0460, that with the existing reactor-years of experience it cannot be assured that all the common-cause failures, that have a signifi-

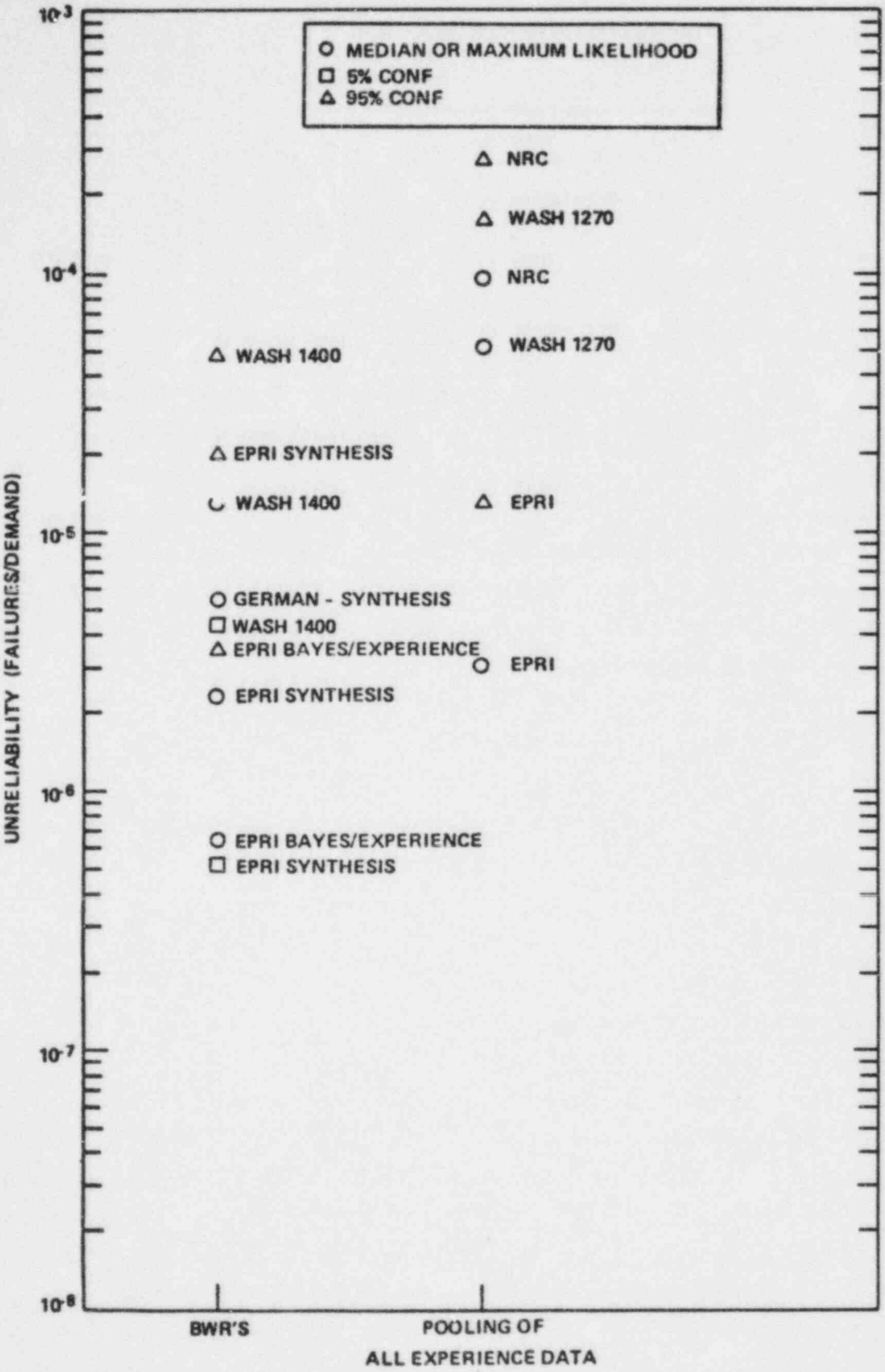


Fig. A.5. Unavailability Estimates for the BWR RPS

cant impact on the reliability of the reactor protection system, have been identified. For this reason, the NRC staff "does not weigh synthesis calculations very heavily in arriving at estimates of scram reliability in current systems." Finally, in NUREG-0460 the NRC staff uses the value of 3 x $10^{-5}$ per demand for the probability of scram failure in LWRs. This value "includes some allowance for the improvement in future reactor protection systems compared with the systems used to derive the estimate."

In conclusion, the existing experience data is not sufficient to provide a conclusive estimate for the unavailability of the LWR reactor protection systems. The unavailability of such highly reliable systems tends to be dominated by common-cause failures of very low frequency. The existing experience data base also cannot support conclusive estimates for the frequencies of such failures. Thus, in analytic models like fault trees, judgment must be used in estimating common-cause failures. Consequently, neither analytic models can provide an indisputable estimate for the unavailability of the LWR protection systems.

### A.2.2 Contribution of RPS Failure to the Risk from BWRs

The contribution of the RPS to the risk from the operation of a nuclear power plant arises from the possibility of scram failure in the event of an anticipated transient. An anticipated transient is defined as a transient that is expected to occur one or more times during the service life of a plant and requires reactor scram. The contribution of Anticipated Transients Without Scram (ATWS) to the risk from a BWR is a function of the frequency of anticipated transients, of the unavailability of the RPS, and of the unavailability of mitigating features such as recirculation pump trip and standby liquid control system (liquid poison injection). This contribution can be expressed either in terms of the ultimate consequences to health and property of ATWS sequences or in terms of the contribution of these sequences to the core melt probability. The calculation of the latter contribution is simpler and does not involve the additional uncertainties of the phenomena that follow core melting.

Differences in the RPS unavailabilit·· estimates, in the frequency of the anticipated transients, and in the ..rectiveness of the liquid poison injection system used in different ATWS related studies, have led to different estimates for the significance of the ATWS events to the risk from BWRs. In WASH-1400, a frequency of ten anticipated transients per reactor-year was used. EPRI[9], based on data from operating experience in BWRs, has assessed the frequency of anticipated transients, that is applicable to the ATWS events, as 3.52 and 1.22 events per reactor-year for plants with a steam bypass of < 25% and > 25%, respectively. Based on the same data, the NRC staff (NUREG-0460) estimated a frequency of eight events per BWR reactor-year. In WASH-1400, a probability estimate of $10^{-1}$ was used for operator failure to shut the reactor down either by liquid poison injection or by manual insertion of the control rods. In NUREG-0460, no credit was allowed for recirculation pump trip and liquid poison ejection "because in many BWRs successful actuation of the pump trip and manual boron injection do not shut the reactor down and reduce the pressure fast enough to allow many of the systems to maintain the coolant inventory and remove the energy." The above differences lead to the following estimates for the core melt frequency due to ATWS.

| Source | RPS Unavailability | Transient Frequency | ATWS Frequency |
|---|---|---|---|
| WASH-1400 | $1.3 \times 10^{-5}$ | 10 | $1 \times 10^{-5}$ |
| EPRI (<25% bypass) | $2.3 \times 10^{-6}$ | 3.52 | $8 \times 10^{-7}$ |
| EPRI (>25% bypass) | $2.3 \times 10^{-6}$ | 1.22 | $3 \times 10^{-7}$ |
| NUREG-0460 | $3 \times 10^{-5}$ | 8 | $2 \times 10^{-4}$ |

The EPRI estimate is based on the WASH-1400 probability value ($10^{-1}$) for operator failure to shut the reactor down either by liquid poison injection or manual insertion of the control rods. Finally, if the same frequency as in WASH-1400 is used for the other, non-ATWS, accident sequences that lead to core melt in BWRs, then the contribution of ATWS sequences to core melt is: (a) WASH-1400 estimate: ~ 34%, (b) EPRI estimates: ~ 4% (< 25% bypass), ~ 2% (> 25% bypass), (c) NUREG-0460 estimate: ~ 91%.

The above results show that there are significant variations in the estimates presented in the literature for the contribution of ATWS sequences to the core melt probability. They also show that at the present state of the art ATWS sequences remain to be among the significant accident sequences in BWRs.

### A.2.3 Common-Cause Failures

The analytical evaluations of the unavailability of the BWR reactor protection system performed in WASH-1400 and in the EPRI ATWS studies show that this unavailability is dominated by common-cause failures. The three events (Kahl, Monticello, Browns Ferry) that have occurred in operating BWRs, and had the potential to cause a scram failure, were common-cause failures. Concerns over common-cause failures were also the deciding factor in the NRC staff assessment that a 3 x $10^{-5}$ value is more appropriate for the unavailability of LWR reactor protection systems. In a reliability assurance program, both the frequency as well as the sources of common-cause failures are clearly very important. Identification of the sources of such failures allows the enactment of measures for the control or the elimination of these failures.

Attempts have been made to utilize data from operating experience to classify common-cause failures into categories that provide useful information to the designer, the operator, and the reliability analyst. A literature survey on the classification of common-cause failures is presented in Ref. 10, published in July 1979. Based on this survey, on a review of operating experience data for reactor protection systems, and on the needs that a classification system of common-cause failures must satisfy, Ref. 10 has proposed the system shown in Fig. A.6. In the same reference, a review was performed of LERs for the electrical subsystem of the RPS of LWRs in the United States from 1971 to 1976. Based on this review, it was concluded that human errors in design and maintenance are the main sources of common-cause failures.

In Refs. 11 and 12, LERs involving LWR control rods and control rod drive mechanisms published between Jan 1, 1975 and Jan. 30, 1973

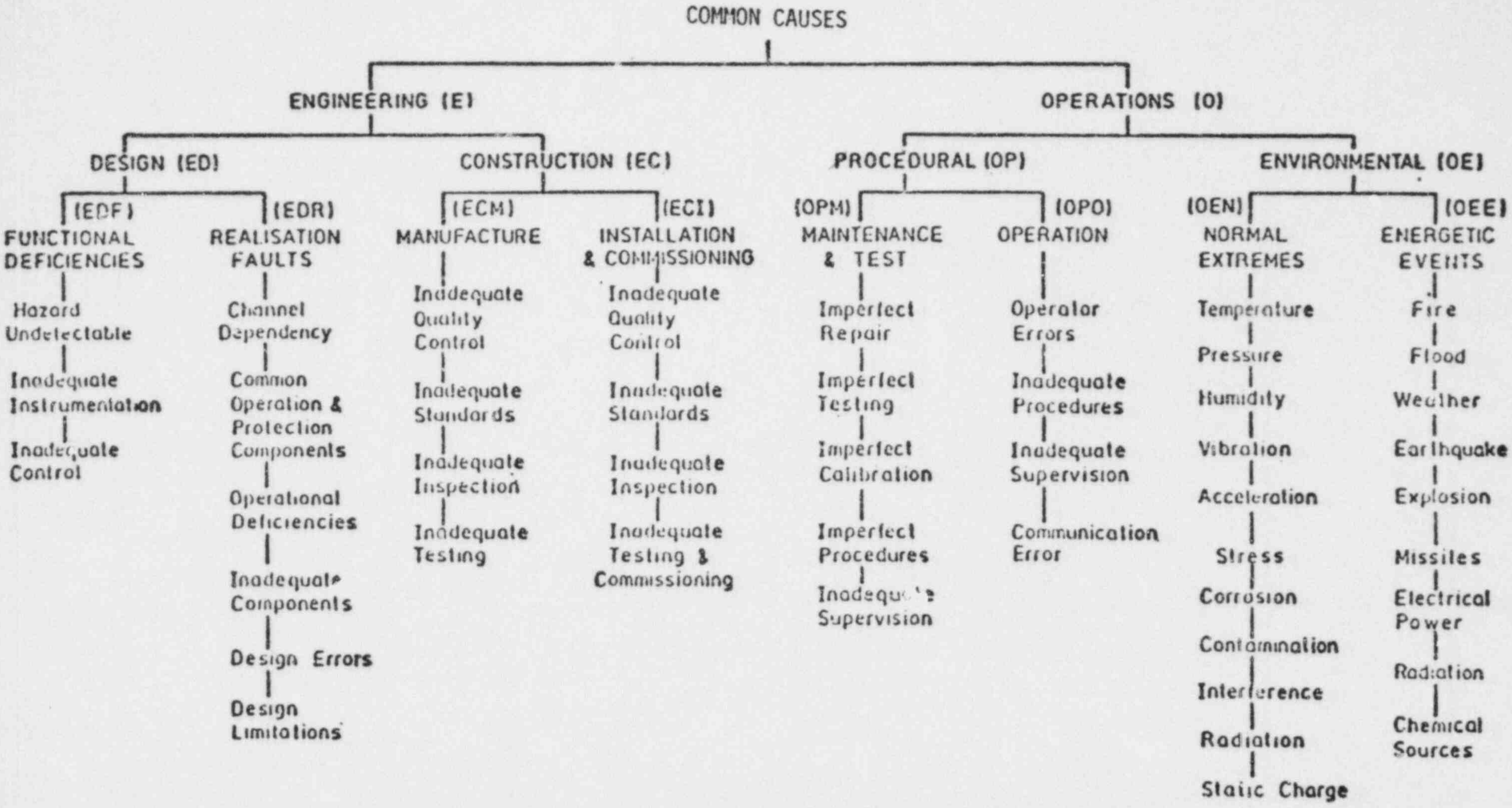


Fig. A.6. Classification System for Common-Cause Failures

were reviewed with the purpose of extracting the lessons to be learned from operating reactor experience. It was concluded that: (1) a relatively large number of defects are systematic, (2) the leading direct causes of defects are inadequate design and inadequate operator training, and (3) defects that result in system failure are rare.

Preliminary estimates of common-cause failure rates for some instrumentation and control assemblies of LWR protection systems, based on LER data and the Binomial Failure Rate Common-Cause Model, have been reported in an informal interim EG&G report.[13] These estimates suffer from input data imperfections such as: not all faults in a plant are reported in the LERs; the strictness of the reporting policy may vary from plant to plant; the component populations were not well known; in many instances the number of components that failed is not specified in the LERs. Moreover, these estimates refer to assemblies of redundant elements, e.g., the instrumentation channels that monitor coolant temperature. No estimates are provided for functionally diverse assemblies that both can generate a trip in the event of a transient, e.g., temperature and pressure instrumentation channels.

In the same report, as well as in other EG&G reports[14,15] that deal with LER data referring to the RPS, a categorization of events has been made according to the cause of failure. However, many of the causes of failure used in this categorization do not provide all the information that is required by a reliability assurance program. For example, causes like "seal failure," "weld failure," "instrument drift," etc. do not give the original cause of failure. Seal failures can be due to bad design, installation, or maintenance errors, etc. Similarly, weld failures may be due to a bad welding process or to the employment of welders that were not well qualified, etc. In Ref. 14 (EG&G), out of 233 faults reported for the instrumentation and control components, 120 of them have been attributed to instrument drift. Since this represents over 50% of these faults, it is important to identify the original source or sources of drift. In Ref. 13 (EG&G), it is indicated that defective procedures and maintenance errors dominate the common cause failures of instrumentation and control assemblies in BWRs. Finally, in Ref. 15 (EG&G), none of the observed failures in BWR control rod and control rod drive mechanisms has been attributed to design errors. This is in disagreement with the conclusion of Refs. 11 and 12 that design errors is one of the leading direct causes of defects in LWR control rods and control rod drive mechanisms.

From this discussion it is clear that there is a need for a thorough evaluation of LER data for the BWR RPS to properly classify common-cause failures, determine the dominant sources of these failures, and provide estimates for the frequency of such failures.

### A.2.4 Conclusions

From the review of the generic information on the BWR RPS that is relevant to this work, the following conclusions can be derived.

The estimates of the unavailability of the BWR RPS vary greatly - from 6.7 x $10^{-7}$ to 1 x $10^{-4}$ failures per demand (median values). The dominant contributors to this unavailability are: (a) failure of a sufficient number of control rods to insert, (b) common cause failures due to human error, and (c) failure of the scram discharge volume. The estimates of the contribution of these dominant contributors to the RPS unavailability that have been presented in the literature vary significantly.

The estimates of the frequency of accident sequences that are characterized by failure to scram also vary greatly - from 3 x $10^{-7}$ to 2 x $10^{-4}$. The estimates for the contribution of these sequences to the BWR core melt probability vary from 2% to 91%.

The above wide variations are due to the lack of adequate experience data on RPS failures and transient frequencies during the lifetime of a BWR, and especially to inadequate data and analytic models for common-cause failures, including failures due to human error.

The analyses of the operating experience data that have been performed so far, indicate that human errors in design and maintenance are dominant sources of common-cause failures in the BWR RPS.

The generic analyses of the RPS presented in the literature do not have the depth and detail that a reliability assurance program requires. The same observation is valid for the analyses of the operating experience data. However, these analyses give a very good picture of the existing uncertainties and a reliability assurance program must take them into account.

### A.3 Operating Experience with the BWR Reactor Protection System

To obtain information on the sources of failure that have the potential to lead to RPS failure, the experience from the operation of the RPS in the BWR power plants operating in the United States has been analyzed. This information can be utilized in assessing the reliability of the RPS as well as in devising means to reduce or eliminate observed sources of failure. In this analysis, the Licensee Event Reports (LERs) compiled by the NRC Office of Analysis and Evaluation of Operational Data was used as a data base. This NRC data covers the period from 1969 up to October 1981 when the further development of the data base was terminated.

Section A.3.1 of this Appendix presents an analysis of the RPS LERs for all BWRs. Section A.3.2 presents a similar analysis for the RPS of the Browns Ferry Units. Both analyses are of a scoping character.

#### A.3.1 Operating Experience with the RPS of All BWRs

From the LERs reported in the compilation generated by NRC, those that refer to the LaCrosse and Humbolt Bay power plants, which were considered atypical, were excluded from the analysis. Events that refer to control rod uncouplings that did not inhibit reactor scram were not counted. Some of the reports discuss scheduled tests that were not performed in the scheduled time due mainly to personnel error. However, the oversight was discovered soon and the tests were performed. These events were also not counted in the analysis. Finally, from the list compiled by NRC 751 events were considered as pertinent.

These events were grouped into the following categories.

a. Instrumentation Channel Events
b. Logic Channel Events
d. Scram Discharge Volume Events
e. Control Rod Drive Mechanism Events
f. Control Assembly Events

The category "instrumentation channel" includes all the instrumentation channels that are used for reactor scram. The control assembly failures refer to failures that could lead to a lower control assembly reactivity worth than designed.

The contribution of each category to the total population of LERs reported is as follows.

| | Fraction of Total |
|---|---|
| Instrumentation Channels | 0.818 |
| Logic Channels | 0.004 |
| Hydraulic Control Units | 0.096 |
| Scram Discharge Volume | 0.008 |
| Control Rod Drive Mechanisms | 0.068 |
| Control Assemblies | 0.007 |

The instrumentation channel failures dominate the events reported. They constitute 82% of the LERs. Failures in the hydraulic control units and in the control rod drive mechanisms comprise 10% and 7%, respectively, of the analyzed LERs. The instrumentation channel failures are dominated by instrument drift. In assessing the significance of instrumentation drift, the observed drift must be compared with the margin between instrument setpoint and l[illegible] parameter. Many of the observed drifts are sm[illegible] the margin between the setpoint and the [illegible] meter is significant, these drifts [illegible] Reference 16 states that:

> "The single most prevalent reason for the drift of a setpoint out of compliance with a technical specification has been the selection of a setpoint that does not allow a sufficient margin between the setpoint and the technical specification limit to account for instrument accuracy, the expected environment and minor calibration variations. In some cases the setpoint selected was numerically equal to the technical specification limit and stated as an absolute value, thus leaving no apparent margin for uncertainties. In other cases the setpoint was so close to the upper or lower limit of the instrument's range that instrument drift placed the setpoint beyond the instrument's range, thus nullifying the trip function. Other causes for drift of a setpoint out of conformity with the technical specification have been instrumentation design inadequacies and questionable calibration procedures.
>
> The Instrument Society of America sponsored a review of the setpoint drift problem in April 1975 by establishing the SP67.4 committee. (Now renumbered SP67.04).
>
> The committee's review indicated that a more thorough consideration of setpoint drift was necessary in the design, test, purchase, installation and maintenance of nuclear safety-related instrumentation."

The instrument Society of America has developed a standard titled, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants," aiming to establish a basis for setpoint setting that acccounts for instrument errors and drift in the instrument channel from the sensor through the bistable trip device.

If instrument drifts were rectified, the contribution of each event category to the total population of LERs reported would be:

| | Fraction of Total |
|---|---|
| Instrumentation Channel Events | 0.664 |
| Logic Events | 0.007 |
| Hydraulic Control Unit Events | 0.176 |
| Scram Discharge Vol'ıme Events | 0.015 |
| Control Rod Drive Mechanism Events | 0.125 |
| Control Assembly Events | 0.012 |

Instrumentation channel failures remain the dominant contributor providing about 66% of the analyzed events. The contributions of hydraulic control unit events and control rod drive mechanism events are raised to 18% and 13%, respectively.

Each of the above event-categories was further analyzed to identify the dominant causes of failure. In this identification process the following causal categories were used: (a) design error, (b) manufacturing or fabrication error, (c) installation error, (d) plant operating personnel error, (e) procedural deficiencies, and (f) random errors. However, in many instances the LERs do not provide any information about the cause of failure, or the information provided is not adequate to identify the original cause of failure. For example, in many instances the reported cause of failure is: accumulation of foreign material, excessive seal leakage, filter plugging, corrosion, etc. It is clear from the information provided that these failures were not random, and that they were due either to design, installation, personnel, or procedural error, or to other potential causes of multiple failures. However, the LER information is not adequate to identify the specific cause of failure. In these cases, the identifications "accumulation of foreign material," "seal leakage," etc. have been retained.

## Instrumentation Channel Failures

The events reported as failures of instrument channel components were categorized as follows.

| | Fraction of Total | |
|---|---|---|
| | With Drift | Without Drift |
| Instrument Drift | 0.559 | - |
| Personnel Errors and Defective Procedures | 0.182 | 0.423 |
| Design Error | 0.025 | 0.057 |
| Fabrication, Manufacturing Error | 0.003 | 0.007 |
| Installation Error | 0.005 | 0.011 |
| Foreign Material | 0.020 | 0.045 |
| Corrosion | 0.005 | 0.011 |
| Others | 0.193 | 0.445 |

Instrument drift dominates the reported events. The next dominant group is "personnel errors and defective procedures". The information provided by the LERs is not adequate to always distinguish between failures due to personnel errors and those due to defective procedures. For this reason both causes of failure were placed in the same group. If instrument drift is considered as rectified, personnel errors and defective procedures constitute 42% of the analyzed events. Personnel errors include miscalibration, damage of instruments during calibration, testing or maintenance. Failures due to defective procedures include those caused by instructions that could be misinterpreted, by wrong instructions, or by complete lack of proper instructions. Design errors include failure to design a component for the proper environment, wrong analysis, use of wrong components. The group "foreign material" includes failures due to dirty contacts, to crud accumulation, to the presence of construction material and other foreign material. The group "others" includes failures characterized in the LERs as "component failure", "cause unknown", or failures due to loss of power. It must be noted that loss of power causes failure of more than one instrument channels. Finally, for the events other than instrument drift, personnel error, defective procedures, design, fabrication, manufacturing and installation errors, which have the potential to cause common-cause failures, account for about 50% of them.

## Logic Failures

Only 0.4% of the reported events were identified as failures of components in the logic channels. However, the actual fraction may be higher. From the information provided in the LERs it is not clear if some of the relay failures refer to relays in an instrumentation channel or to relays in a logic channel. From the information provided in the LERs, about 33% of the logic component failures were attributed to personnel error, and the remaining 67% to random failures.

## Hydraulic Control Unit Failures

The failures reported for components of the hydraulic control units have been distributed as follows.

| | Fraction of Total |
|---|---|
| Personnel Error and Defective Procedures | 0.264 |
| Design Error | 0.153 |
| Foreign Material in Accumulator Switches | 0.056 |
| Corrosion | 0.014 |
| Instrument Drift | 0.014 |
| Random or Unknown | 0.507 |

Failures due to personnel error and defective procedures constitute 26% of the reported events and design errors about 15%. All the failures of accumulator switches due to accumulation of foreign material were multiple failures reported by Browns Ferry. The instrument drift failure was also a multiple failure. Sixty-one out of 137 pressure switches were found out of the technical specification limit. In summary, about 50% of the events were due to causes that led to multiple failures or had the potential to lead to such failures.

## Scram Discharge Volume Failures

As discussed earlier, these failures do not include failures of the scram discharge volume instrumentation used for reactor scram (they were included in the category "instrumentation channel failures"). About 83% of the scram discharge volume failures have been attributed to design error. They include no compliance with the seismic design requirements and the partial failure to scram event at Browns Ferry. The remaining events have been attributed to maintenance personnel errors.

## Control Rod Drive Mechanism Failures

The reported failures for components of the control rod drive mechanisms have been distributed as follows.

| | Fraction of Total |
|---|---|
| Design Error | 0.039 |
| Excessive Leakage Past Piston Seals | 0.255 |
| Foreign Material Obstructed Rod Movement | 0.255 |
| Personnel Error or Defective Procedures | 0.118 |
| Inner Filter Plugged | 0.059 |
| Manufacturing Error | 0.039 |
| Leakage of "O-ring" Seals | 0.059 |
| Cause Unknown | 0.176 |

About 26% of the reported failures were due to excessive leakage past the piston seals. About 77% of these events involved two or more control rod drives. In one event 93 drives were involved. In another one 46 drives were involved. Four events involved 15, 11, 8, and 6 drives, respectively. The potential of common cause failure in these events is clear. About 31% of these events were reported at Dresden 2 and 3 and about 23% at Oyster Creek. From the information provided in the LERs it can not be determined if these failures were due to design, installation, maintenance or other error.

About 50% of the events "foreign material obstructed rod movement" were reported by the Big Rock Point plant. One of these events involved two drives.

The events "inner filter plugged" involved two or more drives. One of them involved 12 drives and another one 8 drives.

The reported failures of the "O-ring" seals were all multiple. One event involved two drives. The LER of another event states that "several recent failures of these "O-rings" have occurred and the problem is under review with the vendor". Another LER states "investigation following cooldown revealed leakage at several "O-ring" seals....seal design is being reviewed with the NSSS."

The above analysis shows that about 53% of the reported events were due to causes that either led to multiple failures or had the potential to lead to such failures.

Control Assembly Failures

This category refers to events that may had affected the reactivity worth of the control assemblies. In sixty percent of these events it is reported that absorber tubes were found inverted due to fabrication error. In one occasion 33 out of the 185 control rods contained inverted absorber tubes. One LER reports loss of $B_4C$ due to tube cracking and another one reports small errors in the calculation of control rod worths.

Conclusions

None of the events reported in the LERs have caused a scram failure. However, errors due to personnel, defective procedures, design, fabrication, manufacturing and installation have the potential of common-cause failures. Also, many of the failures reported in the LERs as component failures without information about the failure cause, involved more than one component. In some cases "normal wear" or "aging" are given as failure cause. Multiple failures can occur by aged components in standby systems, especially if the testing interval is long.

An extensive analysis of LERs supported by experts in the design, manufacturing, installation, operation and maintenance of the system considered can provide valuable feedback information. This information can be used to reduce or eliminate many sources of error that have the potential to cause multiple failures by improving the design, manufacturing and installation processes, operating and maintenance procedures, and pers..nel training. The analysis presented in the previous sections indicates that such sources of failure were responsible for: ~ 50% of the instrumentation channel events (drift not counted), ~ 33% of the logic channel events, ~ 50% of the hydraulic control unit events, 100% of the scram discharge volume events, ~ 53% of the control rod drive mechanism events, and 100% of the control assembly events.

### A.3.2 Operating Experience with the Browns Ferry RPS

The NRC data base includes 78 events for the Reactor Protection Systems of the three Browns Ferry Units. These events are distributed as follows:

| | |
|---|---|
| Trip Instrumentation | 59 |
| Hydraulic Control Units | 12 |
| Scram Discharge Volume | 3 |
| Control Rods and Drives | 4 |

The above tables shows that 76% of the reported events refer to the instrumentation used to monitor the trip parameters, including the Scram Discharge Volume (SDV) trip instrumentation. The events that refer to the Hydraulic Control Units (HCUs) account for 15% of all the reported events.

From the 59 instrumentation failures 40 of them (68%) were due to setpoint drift. These drift events are distributed as follows:

| | |
|---|---|
| Turbine First Stage<br>Pressure Permissive Switches | 13 |
| Reactor Water Level | 9 |
| Reactor High Pressure | 5 |
| Drywell Pressure | 4 |
| Condenser Low Vacuum | 3 |
| Flux Monitoring | 3 |
| SDV Water Level | 1 |
| Unclarified | 2 |

There were many events where more than one instruments were found drifted. In 11 of the 13 events reported as "turbine first stage pressure permissive switch" drift, more than one switch were found drifted. In 10 of these events, enough switches had drifted to prevent scram if the drift was over the limiting pressure.

The causes of instrumentation failure, other than drift, reported in the Browns Ferry LERs include:

-- Personnel error

- "seven out of eight high voltage cables to the detectors were not connected"
- calibration error
- "switch was rewired incorrectly during maintenance as a result of the failure to follow administrative controls"
- pressure switch was plugged with teflon tape
- error in reactor water level scram switches probably due to "inadvertent operation of equalizer or drain valves"
- "reactor water level instrumentation indicated full upscale... equalizing valve was partially open".

-- Inadequate procedures

-- Impact of other activities: "reactor water level switches...drifted due to air impact drilling next to the panel on which they were mounted"

-- Environment

- buildup of foreign material
- crud accumulation
- corrosion
- dirty switch contacts

-- Design errors

- instruments were not qualified for conditions under which they should be operable
- other design errors

-- Design or installation errors

"IRM F signal cable was sheared by the CRD repair platform"

Although none of the failures caused by the above sources led to a scram failure, all of them are potential sources of common-cause failures.

The 12 events reported for the HCUs are distributed as follows:

| | |
|---|---|
| Scram Accumulators | 9 |
| Piping Systems for Control Rod Drives | 1 |
| Manual Valves | 2 |

From the nine events reported for the scram accumulators eight referred to accumulator water level switch failures, and the other one to leakage from accumulator pistons. From the eight accumulator water level switch failures five of them were multiple. In one occasion "a number of them" are reported as found failed in unit 1. Subsequent inspection in unit 2 discovered two switches failed. In another occasion eight were found failed and in two other occasions seventeen were found failed in each occasion. All the multiple failures were due to accumulation of foreign material. More specifically the LERs report:

- "thread lubricant on switch float and float guide spool prevented level switches from operating"
- "excessive amounts of some substance found on switch float and guide stem which caused the float to stick"
- "crud from system accumulated on floats" prevented operation

- "some gummy substance was observed...might have caused floats to stick".

Two single failures have been attributed to broken reed switches.

The LER that refers to leakage from accumulator pistons, reports three failures that occurred within two weeks. They were attributed to normal wear of the O-rings. If this is the case, it means that these rings had been left in operation while they were in the wearout phase of their lifetime.

The one LER that refers to the piping system for control rod drives states: "review of documentation... revealed that seismic criteria were not included in design and that additional pipe supports were required. QA oversight."

The two LERs on manual valves state that valves were found closed or open while they should be open or closed, respectively. Both events are attributed to personnel error.

None of the above events led to a scram failure. However, all the reported sources of multiple failures are potential sources of common-cause failures.

The two reported events on the Scram Discharge Volume involved: (a) the one-inch vent line on the SDV of Unit 1 was not seismically qualified, and (b) the partial failure to scram in Unit 3 where 76 of 185 control rods failed to fully insert. The failures of the instrumentation that monitors the SDV level and initiates a trip, have been included in the trip instrumentation events. In two of these events the failure was due to buildup of foreign material, which is a potential source of common-cause failures.

For the Control Rod Drives and Control Assemblies four events have been reported.

a. One rod was founa valved out and another one could not be moved because of a dirty strainer.

b. Rod uncoupled from drive, reason unknown.

c. 33 out of 185 control rods were found with inverted absorber tubes. Error in control assembly operations.

d. Reactor pressure during scram timing tests was 950 psia than the required 950 psig. Personnel failed to properly implement procedural requirements.

Valving out of control rods due to personnel error as well as personnel failure tu properly implement procedures are potential sources of common-cause failures. Accumulation of dirt in strainers is also a potential source of common-cause failure.

References

1. Browns Ferry Final Safety Analysis Report.

2. "Reactor Safety Study: An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014) (October 1975).

3. R. C. Erdman, et al., "ATWS: A Reappraisal, Part II, Evaluation of Societal Risks Due to Reactor Protection System Failure, Vol. 2 BWR Fault Tree Evaluation," EPRI NP-265 (August 1976).

4. "Generic Safety Evaluation Report: BWR Scram Discharge System," NRC unnumbered report (December 1, 1980).

5. W. R. Casto, "Partial Failure to Scram at Browns Ferry 3," Nucl. Safety, 22, 226 (1981).

6. ATWS: A Reappraisal:

   Part I. "An Examination and Analysis of WASH-1270, Technical Report on ATWS for Water-Cooled Power Reactors," EPRI NP-251 (August 1976).

   Part II. "Evaluation of Societal Risks Due to Reactor Protection System Failure," EPRI NP-265, Vols. 1, 2, 3 (August 1976), Vol. 4 (January 1977).

7. G. S. Lellouche, "Anticipated Transients Without Scram," Nucl. Safety, 21, 469 (1980).

8. "Anticipated Transients Without Scram for Light Water Reactors," NUREG-0460, Vols. 1, 2, 3 (1978), Vol. 4 (1980).

9. F. L.Leverenz, et al., "ATWS: A Reappraisal, Part III, Frequency of Anticipated Transients," EPRI NP-801 (July 1978).

10. G. T. Edwards and I. A. Watson, "A Study of Common-Mode Failures," UKAEA, SRD R 146 (July 1979).

11. H. L. Thaggert, et al., "Defect Flow Analysis of Control-Rod-Drive Operational Events," Nucl. Safety, 22, 466 (1981).

12. I. M. Jacobs, et al., "Defect Flow Analysis of Licensee Event Reports on Control Rods and Control Rod Drive Mechanisms," GEFR-00513 (January 1981).

13. C. L. Atwood, "Common Cause and Individual Fault Rates for Licensee Event Reports of Instrumentation and Control Assemblies at U. S. Commercial Nuclear Power Plants," Draft Interim Report EGG-EA-5623, EG&G Idaho, Inc. (December 1981).

14. C. F. Miller, et al., "Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U. S. Commercial Nuclear Power Plants," NUREG/CR-1740 (1981).

References (cont'd)

15. W. H. Hubble and C. F. Miller, "Data Summaries of Licensee Event Reports of Control Rods and Drive Mechanisms at U. S. Commercial Nuclear Power Plants," NUREG/CR-1331 (1980).

16. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants," Instrument Society of America, 1982.

## Appendix B

## Reliability of High Pressure Core Cooling Systems

In addition to the low-pressure RHR system other coolant injection systems are provided in BWRs for coping with transients and loss-of-coolant accidents. A NSAC reliabil:ty study has recently been completed on two of these systems; the high-pressure coolant injection system (HPCI), and the reactor core isolation cooling system (RCIC) [B-1]. As these two systems are somewhat comparable to the RHR system in safety significance, importance and operating characteristics the results of this NSAC study are pertinent to this RAP study and a comparison of the major findings are in order. In addition, the reliability analysis techniques and methods identified in this NSAC study are somewhat unique and of interest for potential application to this present RAP study. Therefore, a brief summary of the NSAC analysis methods and significant reliability findings on the high-pressure HPCI and RCIC systems are provided along with a brief comparison of these results with the RAP reliability results for the RHR system.

### B.1 HPCI and RCIC System Descriptions

Both of these high-pressure coolant injection systems are steam turbine-driven systems that can inject water into the BWR at full operating pressure. The HPCI is part of the emergency core cooling system (ECCS). Its purpose is to reflood the reactor core with water in the event of a small LOCA which does not depressurize the reactor vessel. In the case of Browns Ferry, the HPCI provides protection for all liquid breaks less than 0.12 $ft^2$ in area and all steam breaks that are less than 1.4 $ft^2$. The HPCI system is also available to provide makeup water to the reactor at near operating pressure when normal makeup sources are unavailable.

The RCIC system is also designed to provide a source of high-pressure water coolant makeup water to the reactor vessel when feedwater flow to the reactor is lost. Its flow capacity is smaller than the HPCI system - providing only about 10% as much coolant as the HPCI system. For events other than pipe breaks or transient induced loss-of-coolant accidents, this flow rate is sufficient to prevent core uncovery. Both the HPCI and the RCIC are designed to provide full water flow in less than 30 seconds from the time of initiation.

## B.2 Reliability Analysis Approach

The HPCI and RCIC systems were studied by NSAC [B.1] in an effort to identify ways in which the reliability of these systems could be improved. The study approach centered on a detailed evaluation of the licensee event reports (LERs). Trends, insights, and projections were obtained from this analysis of the HPCI and RCIC system LERs to provide a basis for specific reliability improvement recommendations. In addition, surveys and discussions with personnel at BWR plants having HPCI and RCIC systems were held in an attempt to correlate the LER results with successful reliability programs. These plant-by-plant surveys considered the degree of implementation of the numerous General Electric (GE) Service Information Letters (SILs) on operations and maintenance matters. The SILs are provided by GE to the industry in an attempt to improve reliability by recommending component and procedural changes.

The reliability analysis of the HPCI and RCIC systems included several interesting techniques which appear to be useful in evaluating reliability improvement trends. Use was made of Duane plots with the LERs as data points [B-2]. The Duane method of evaluating failure trends of a system or component involves calculating the failure rate, $\lambda\Sigma$, defined as:

$$\lambda\Sigma = \frac{F}{H} K\ H^{-\alpha}$$

where

$\lambda\Sigma$ = cumulative failure rate

$H$ = total test time

$F$ = failures during the period $H$

$K$ = a constant

$\alpha$ = failure growth rate

Plotting $\lambda\Sigma$ versus H on log-log paper results in a trend line. If the shape is negative, the cumulative failure rate is decreasing, whereas if the slope is positive, the failure rate is increasing. This technique was originally applied to aerospace components and appears to have merit in inferring system reliability of plants from the trend of their LERs. In applying the method to LERs, F was taken to be the cumulative number of LERs with H (the unit operating time in months) taken as the LER generation period which was evaluated (January 1978 through April 1981).

Another method called Defect Flow Analysis (DFA) was applied to the LER data by Engineering Decision Analysis Company, Inc. This technique systematically evaluates recorded product failures (i.e., known defects) to determine the defect population characteristics or dimensions. The DFA consists of two processes, Dimensional Analysis and Screen Analysis. The Dimensional Analysis phase consists essentially in posing a series of questions which, when answered, reveal properties (i.e., dimensions) about the defect population. Examples of properties include questions about failure cause and levels of criticality. These properties or dimensions are indicative of both the product peculiarities and the uniqueness of the organization which produced or operated the product.

In the Screen Analysis, the various screens (e.g., design review, qualification test) are reviewed to see what they reveal in the way of defect detection. From a comparison of the "most eligible screen" to detect a failure and the "actual screen" that detected the failure, reliability weakness can be identified. Shortcomings in, for example, operation/maintenance can then be corrected from a study of the failure-related causes and failure to detect them.

## B.3 Results of Reliability Analysis of HPCI and RCIC Systems

The reference B-1 study evaluated the 169 licensee event reports (LERs) that were filed between January 1978 and May 1981 where the HPCI or RCIC system was inoperable or declared inoperable. The major conclusion of this investigation was that at least 40% of the HPCI/RCIC problems might be averted by a high-quality preventative maintenance program. Other important findings and conclusions were:

1. On the average the RCIC and HPCI systems performance has fallen short of expected levels. The causes, however, did not appear to be attributable to inadequate design. Important differences were found between individual plants, and the number of problems varied markedly among the plants. It was determined, for example, that 61% of the 117 HPCI LERs were issued by 33% of the plants, and 70% of the 32 RCIC LERs were issued by 31% of the plants.

2. The largest percentage of the HPCI and RCIC inoperability problems involved turbine-governor control valves and motor-operated valves. A large percentage of these problems occurred at a small number of plants with the major causes (e.g., dirty contacts, instrument calibration loss) indicative of a need to improve the preventative maintenance program.

3. The frequency of HPCI and RCIC inoperability problems appeared to be constant or decreasing for plants with low to moderate numbers of LERs. For some plants, the number of HPCI and RCIC inoperability LERs is increasing with time, showing an adverse trend. Use of just the inoperable or declared inoperable LERs was felt to eliminate differences between plants which would occur in dealing with non-operability LERs (e.g., technical specification violations).

4. Three cases of concurrent loss of HPCI and RCIC, when auto-initiated by low reactor water level, were identified. There was one case of sequential failure of RCIC and HPCI during surveillance testing. Plants with only steam-driven reactor feedwater pumps were found to be especially susceptible to concurrent failures due to the occurrence of main steam line isolation when the reactor trips. This condition can be prevented by a simple reactor mode switch change from "run" to "shutdown" immediately following scram appears to bypass the low steam line pressure isolation signal to prevent this condition from occurring.

5. Only about one-half of the plants perform a cold, quick-start surveillance test of the HPCI and RCIC systems. Other plants conduct startup tests with the equipment preheated, which does not simulate the abrupt emergency startup from the cold conditions. Although this procedure meets the technical specifications, the only way to assure that all components are functioning correctly for automatic safety initiation is to perform cold, quick-start testing.

6. It was determined that plants with only turbine-driven feedwater pumps have a less reliable feedwater system than do plants with at least one electric motor driven feedwater pump. More HPCI and RCIC problems were reported for these plants with only turbine-driven feedwater pumps, presumably because the HPCI and RCIC are not challenged as often in plants with motor-driven feedwater pumps.

7. The number of spurious trips and isolations of the HPCI and RCIC can be reduced if certain trip and isolation functions are bypassed in the event that there is an auto-initiation signal and the need to maintain water in the vessel is real and takes priority over protection of the HPCI and RCIC systems. In addition, by adding trip and isolation signal redundancy and some further time delay in the DP signal (which isolates the RCIC/HPCI steam lines), the reliability of the systems should improve.

8. Discussions with personnel at plants with low HPCI/RCIC LER rates indicated that they have an aggressive and well-defined preventative maintenance program. In place was a quality assurance program requiring scheduled preventative maintenance, records of maintenance performed on safety related components, review by others of critical component maintenance, and testing before the component is returned to service.

## B.4 Comparison with RHR System Reliability Results

A detailed and direct comparison of the HPCI/RCIC system reliability results obtained in the NSAC study with the RHR system reliability results from the ANL/RAP study is not possible because of the different study objectives and approaches. In spite of the differences in the two studies, and the basic differences in the systems, there are some trends in the results which are similar and will be discussed below.

The NSAC study focused primarily on the system reliability aspects from the standpoint of potential operational maintenance and testing improvements. This study tabulated the HPCI/RCIC LERs into the following four categories:

A. Active Components and Functions

B. Non-active Valve Lineup Required for Operation

C. HPCI/RCIC Turbine Trip Functions

D. HPCI/RCIC System Isolation Functions

Eliminated from consideration in this NSAC study were LERs reporting violations of Tech Specs which included most instrumentation drift events and reports of seismic deficiencies. Only events where the safety systems were inoperable or declared inoperable were considered. For the HPCI system these considerations reduced the original 247 LER population to 117 and for the RCIC system the original 153 LER population was reduced to 52.

The ANL/RAP study of the RHR system on the other hand had a more general and broader objective; namely to study the systems reliability problems from a quantitative risk standpoint. The LERs for the RHR were therefore evaluated and categorized by major subsystem according to cause of failure.

From an overall system problem standpoint the number of problems reported for each plant varied markedly from plant to plant in both the NSAC and RAP studies. In the NSAC investigation it was found that 61% of the 117 HPCI LERs were issued by 33% of the plants. The RCIC system LERs had a similar distribution with 70% of the LERs issued by 31% of the BWR plants. This overall distribution of problems was surprisingly similar to that found in the RHR LER population as determined in this RAP study where 60.8% of the LERs were issued by 30.4% of the plants. It should be noted that the same plants were not all involved in the large number of problems for the HPCI and RCIC systems or the RHR system. In the case of the NSAC study, 2 out of the 6 plants that were the major HPCI LER issuants were also in the 5 plant group which issued the majority of the RCIC LERs. Without an identification of the specific plants in the HPCI/RCIC study (only a letter key was provided) it is impossible to determine if the same plants were included in the group of plants issuing the majority of the RHR LERs.

In the case of the HPIC/RCIC system a large percentage of the inoperability problems involved turbine governor control valve and motor operated valves. Approximately one-third of the LERs for the HPIC/RCIC systems were valve related. It was found that five plants (28% of the unit population) represented 64% of the valve LERs. There were four units (24%) that had no MOV LERs causing HPCI and RCIC inoperability. All units used the same valve operators and the fact that the reported failure were concentrated in five plants suggests that the failure causes were not generic, but rather were highly dependent on local site installation, maintenance and operating practices. There appeared to be, based on a survey of BWR plants, a correlation between preventative maintenance practice and low MOV LER rates.

The fault pattern and distribution found for the RHR system in this RAP study tended to agree with the NSAC valve experience observed in the HPCI/RCIC systems. Of the 360 total faults or failures 109 (30%) were associated with valve related problems. These RHR system valve problems were also distributed similarly to the HPCI/RCIC systems with six plants (26% of the unit population) representing 58% of the valve faults. It was also found that five units (22%) had no MOV LERs. This clustering of valve faults among only a relatively few number of units suggests that the RHR system valve problems were also plant dependent (i.e., a function of installation, maintenance and operating practices). As over 60% of the valve related problems were in the random or unknown category, a strong preventative maintenance program should yield beneficial results for the RHR system comparable to those seen in the HPCI/RCIC system.

One of the major findings of the NSAC investigation was the relatively high frequency of serious failures of the HPCI/RCIC systems. There were four cases of concurrent or sequential failure of the RCIC and HPCI to auto-initiate and maintain water level. One case was an actual demand for HPCI/RCIC caused by low reactor water level and resulted in the loss of all high pressure injection and feedwater for approximately 5 minutes. A second event suffered concurrent failure of mechanical components in both the RCIC and HPCI systems when auto-initiated by a low reactor water level after a scram. The third event involved an isolation of both the HPCI and RCIC by a high steam line pressure drop during auto-initiation. The fourth event happened when the HPCI system failed during surveillance testing. The RCIC system was then tested (as required by the Tech. Spec.) and also failed to start. Manual operator intervention was required to place the system into operation in the case of the first and third events. Repairs were required in the second situation before the RCIC/HPCI systems were operational. In the case of the forth event the feedwater system remained operable to maintain reactor water level.

There were also several multiple failures reported for the RHR system. However, from the information provided by the LERs, it could not be concluded if these failures resulted in complete loss of the RHR system.

Finally the contention and conclusion in the NSAC study that at least 40% of the HPCI/RCIC problems might be averted by a high quality preventative maintenance program appears to apply to the RHR system as well. In the RAP study, considering only those LERs related to operational problems (e.g., the unknown/random fault category) a total of 143 LERs were identified out of the 360 LER population (see Table 4.3). Therefore, a preventative maintenance program has the potential to correct about 40% of the RHR problems which is the corrective level that was also seen in the NSAC study of the HPIC/RCIC systems.

## B.5 Conclusions

The NSAC sponsored investigation of the reliability of the HPCI and RCIC systems operating at 18 BWR plants resulted in a comprehensive list of 13 recommendations for improving availability and reliability. These specific recommendations were, in general, based upon procedures or practices employed by plants which had favorable HPCI and RCIC experience. Of the 13 recommendations, 12 addressed ways of improving maintenance or testing procedures or practices. (The only exception was a design change recommendation to revise the HPCI and RCIC trip and isolation logic to prevent the inadvertent trips and isolations of the systems.) These maintenance recommendations varied from being very general (e.g., carrying out a documented, comprehensive preventative maintenance program) to very specific (e.g., having a second person confirm the proper reconnection of any wires that one disconnected for maintenance or tests). While all thirteen recommendations were of safety importance, the most significant appear to be the call for the performance of surveillance tests of the HPCI and RCIC with a cold quick start. As emergency startups are abrupt and from the cold conditions, this was felt to be the only way to assure that all components, control systems, and instruments are functioning correctly for automatic safety initiation.

In this NSAC study, extensive use was made of the HPCI and RCIC system LERs generated at the operating BWR plants. Variations have been noted in the quality and quantity of LERs received by the NRC (e.g., see Ref. B-3). The use of LERs generated only from January 1978 through April 1981 has helped to alleviate this concern somewhat as individual plants licensed after January 1, 1976 have been required to use standardized technical specifications. This, along with other changes made since 1976 in the rules that govern LER reporting, suggested a more consistent and uniform LER reporting for events occurring in plants licensed after January 1, 1976. In addition, by selecting only those LERs (169 out of a total of 400) in which either the HPCI or RCIC system was inoperable or declared inoperable, eliminates the question of whether an event was of safety significance or not. Excluded from consideration were LERs reporting such events as violations of Tech Specs that did not result in inoperability of HPCI/RCIC (e.g., most instrument drifts) and reports of seismic deficiencies.

The major conclusion and relevancy to the RAP study of this NSAC study of HPCI and RCIC reliability was the finding that at least 40% of the safety-related problems might be averted by the implementation of a high-quality preventative maintenance program. There appeared to be direct evidence, based upon visits and discussions with personnel at plants with low

LER rates, that system reliability improvement could be correlated with an aggressive and well-defined preventative maintenance and testing program. A method of evaluating the improvement of the HPCI/RCIC systems was to use Duane plots with LERs as data points. This technique, when used in conjunction with a consistent set of LERs, appears to have promise as an auditable indicator of the adequacy of a system's reliability programs and practices.

## References

B-1. F. S. Mollerus, "Reliability of BWR High Pressure Core Cooling," NSAC-53, August 1982.

B-2. J. T. Duane, "Technical Information Series Report DF62MD300," General Electric Co., DCM-G Department, Erie, PA, February 1, 1962.

B-3. C. F. Miller, et al., "Data Summaries of Licensee Event Reports of Valves at U. S. Commercial Nuclear Power Plants, January 1, 1976 to December 31, 1980," NUREG/CR-1363, Rev. 1, p. 111, April 1982.

Distribution for NUREG/CR-3933 (ANL-84-52)

Internal:

R. Avery
W. A. Bezella (5)
I. Charak
L. W. Deitrich
S. Halverson
J. B. Heineman
J. M. Kramer
L. G. LeSage
W. C. Lipinski
P. A. Lottes
C. J. Mueller (10)
R. J. Page
W. A. Ragland
A. B. Rothman
J. H. Tessier
C. E. Till
C. P. Tzanos (5)
R. A. Valentin
D. P. Weber
R. S. Zeno
ANL Patent Dept.
ANL Contract File
ANL Libraries
TIS Files (6)

External:

NRC, for distribution per RG (250)
DOE-TIC (2)
Manager, Chicago Operations Office, DOE
Reactor Analysis and Safety Division Review Committee:
W. P. Chernock, Combustion Engineering, Inc., Windsor, Conn. 06095
L. C. Hebel, Xerox Corp., 3333 Coyote Hill Rd., Palo Alto, Calif. 94304
S. Levine, NUS Corp., 910 Clopper, Gaithersburg, Md. 20878
W. F. Miller, Jr., Los Alamos National Lab., Los Alamos, NM 87545
M. J. Ohanian, U. Florida, Gainesville, Fla. 32611
T. H. Pigford, U. California, Berkeley, Calif. 94720
J. J. Taylor, Electric Power Research Inst., Palo Alto, Calif. 94303

NRC FORM 335
(2 84)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

# BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)

NUREG/CR-3933
ANL-84-52

2. TITLE AND SUBTITLE

Risk Related Reliability Requirements for BWR Safety-Important Systems with Emphasis on the Residual Heat Removal System

3. LEAVE BLANK

4. DATE REPORT COMPLETED

| MONTH | YEAR |
|---|---|
| April | 1984 |

5. AUTHOR(S)

C. P. Tzanos and W. A. Bezella

6. DATE REPORT ISSUED

| MONTH | YEAR |
|---|---|
| August | 1984 |

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Argonne National 'aboratory
9700 S. Cass Avenue
Argonne, Illinois 60439

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER

A2242

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)

Division of Risk Analysis
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

11a. TYPE OF REPORT

Technical

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

The objective of this study was to identify and evaluate the major safety risk parameters of typical reactor safety systems for use in developing a reliability program. This effort was part of a larger research project aiming to evaluate the feasibility and effectiveness of introducing elements of proven reliability programs from other high technology industries into the nuclear industry. As a reference safety system, the Residual Heat Removal (RHR) system of a Boiling Water Reactor (BWR) was selected. A scoping evaluation was also made for a BWR reactor protection system (RPS). Plant information, existing PRA and other relevant analyses, as well as Licensee Event Reports were used a base material for this study. The results of this evaluation indicate that: (1) recovery of faults can have a very significant impact on the reliability requirements, (2) there exists an obvious need for an adequate reliability data base, (3) reliability analyses must be supported by detailed analyses of the plant's response to accident sequences, and (4) the development of effective emergency operating instructions and proper operator training must be one of the major elements of a Reliability Program.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT

Unlimited

16. SECURITY CLASSIFICATION

(This page)
Unclassified

(This report)
Unclassified

17. NUMBER OF PAGES

138

18. PRICE