ornl

NUREG/CR-4047
ORNL/TM-9444

OAK RIDGE
NATIONAL
LABORATORY

MARTIN MARIETTA

An Assessment of the Safety Implications of Control at the Oconee 1 Nuclear Plant Final Report

R. S. Stone
F. H. Clark
O. L. Smith
A. F. McBride
N. E. Clapp, Jr.
R. E. Battle

Prepared for the
Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Under Interagency Agreement 40-550-75

OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC
FOR THE UNITED STATES
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.

Available from

Superintendent of Documents
U.S. Government Printing Office
Post Office Box 37082
Washington, D.C. 20013-7982

and

National Technical Information Service
Springfield, VA 22161

NUREG/CR-4047
ORNL/TM-9444
Distribution Categories
R1, R4, R1G, 12

Instrumentation and Controls Division

AN ASSESSMENT OF THE SAFETY IMPLICATIONS OF CONTROL AT THE OCONEE 1 NUCLEAR PLANT

FINAL REPORT

Major Authors

R. S. Stone
F. H. Clark
A. F. McBride[1]
N. E. Clapp, Jr.
O. L. Smith
R. E. Battle

Contributors

P. N. Austin[1]
R. S. Booth
D. P. Bozarth[1]
R. Broadwater[2]
R. D. Dabbs[3]
F. C. Difilippo
E. W. Hagen
R. A. Hedrick[3]
L. L. Joyner[4]
J. Lewin
C. L. Mason[1]
J. P. Renier
A. Sozer

Manuscript Completed: September 3, 1985

Dated Issued: March 1986

[1] Science Applications, Inc., Oak Ridge, Tennessee.
[2] Tennessee Technological University, Cookeville, Tennessee.
[3] Technology for Energy Corporation, Knoxville, Tennessee.
[4] Joyner Engineers and Trainers, P.C., Forest, Virginia.

Prepared for the
Division of Engineering Technology
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Under Interagency Agreement 40-550-75
NRC Fin. Nos. B0467 and B0816

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831
operated by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U. S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-84OR21400

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES (continued

LIST OF TABLES

LIST OF TABLES (continued)

ACRONYMS

AFW	auxiliary feedwater
ATWS	anticipated transient without scram
B&W	Babcock and Wilcox
BWST	borated water storage tank
CCW	condenser circulating water
CE	Combustion Engineering
CRDCS	control rod drive control system
CRDM	control rod drive mechanism
EFW	emergency feedwater
EFIC	emergency feedwater initiation and control
ESFAS	engineered safety features actuation system
FMEA	failure mode and effects analysis
FSAR	final safety analysis report
FW	feedwater
GE	General Electric
HP	high pressure
HPI	high-pressure injection
IA	instrument air
ICS	integrated control system
LER	Licensee Event Report
LOCA	loss-of-coolant accident
LPI	low-pressure injection
LPSW	low-pressure service water
LST	letdown storage tank
MFW	main feedwater
MSLB	main steam line break
MU&P	makeup and purification system
NNI	nonnuclear instrumentation
NRC	Nuclear Regulatory Commission
NSAC	Nuclear Safety and Analysis Center
NSIC	Nuclear Safety Information Center
NSSS	nuclear steam supply system
ORNL	Oak Ridge National Laboratory
OTSG	once-through steam generator
PORV	pilot-operated relief valve
PRA	probabilistic risk assessment

PTS	pressurized thermal shock
PWR	pressurized water reactor
RCS	reactor coolant system
RCW	recirculated cooling water
RPS	reactor protective system
ry	reactor year
SG	steam generator
SICS	safety implications of control systems
SU	startup
TBS	turbine bypass system
TBV	turbine bypass valve
TCS	turbine control system
UCLA	University of California at Los Angeles
USI	unresolved safety issue

ABSTRACT

As part of the U.S. Nuclear Regulatory Commission's Unresolved Safety Issue on Safety Implications of Control Systems (USI A-47) Program, the Oak Ridge National Laboratory has completed an investigation of nonsafety-grade control system failures at Oconee 1 that could lead to rapid steam generator overfill, reactor overcooling, or reactor overheating (inadequate core cooling). Transients that result from loss of control system power and that threaten plant safety have also been investigated.

Detailed examinations of all Oconee 1 major plant systems were performed, followed by a logical evaluation of their influence in the transients of interest. Broad failure mode and effects analyses (FMEAs) were then conducted on each of the candidate plant systems to determine their safety consequences. In these analyses, the effects of common-cause failures upon the Oconee-1 control systems were examined. Sequence analyses using the results of the FMEAs were then performed to assess combinations of failures and the estimated frequencies of these accident sequences. Where simple cause-and-effect relationships could not be demonstrated (i.e., in cases where feedback was found to exist between the failure outcome and the initiating event), a hybrid computer model was used to augment the FMEAs. This model, which was developed with techniques similar to those currently used in other major systems class codes, combines thermal hydraulics, neutronics, and control system packages to produce a total-plant simulator with emphasis on control system dynamics.

Rapid steam generator overfill, reactor overcooling, and inadequate core cooling can be caused by failures in nonsafety-grade control systems. For example, failure of the steam generator high-level main feedwater pump trip, failure to open or to close the pressurizer pilot-operated relief valve, or loss of power to an integrated control system branch circuit resulting in loss of automatic control of the main feedwater flow can lead to transients in one of these respective classes. Proper operator intervention, however, can avert possible safety consequences resulting from such failures. Reevaluation of certain trip circuitry, more extensive utilization of the plant computer to process instrument signals, and rewriting of selected operator procedures are recommended to minimize the effect of control failures in nonsafety-grade control systems at Oconee 1. Generic extension of the Oconee 1 recommendations to all Babcock and Wilcox pressurized water reactors has also been addressed to the extent possible.

EXECUTIVE SUMMARY

An investigation of nonsafety-grade control system failures at Oconee 1 that could lead to rapid steam generator overfill, reactor overcooling, or reactor overheating (inadequate core cooling) has been completed. The safety implications of such control system failures were assessed by performing detailed plant-specific examinations of the interaction between control and safety systems, determining the relative importance of these interactions, and recommending plant design and operation guidelines based on their relative importance. The probabilities of certain events have been estimated to ensure the credibility of this study, and guidance has been provided to broaden the results of this plant-specific analysis to encompass all Babcock and Wilcox pressurized water reactors.

SELECTION OF PLANT SYSTEMS

All Oconee 1 major plant systems were evaluated logically to produce a candidate set of plant systems for analysis. Candidate systems are those that can potentially contribute to the initiation or exacerbation of rapid steam generator overfill, reactor overcooling, or inadequate core cooling. Subsystems and individual components that interface with the candidate set of plant systems were then identified to establish chains in which each link is significant to the transient event classes under study.

Two sets of systems were selected for failure mode and effects analyses (FMEA). The first system set can contribute to rapid steam generator overfilling or reactor overcooling (as these are directly coupled) and includes integrated control, nonnuclear instrumentation, pressurizer, steam generator, reactor coolant pumps, makeup and purification, chemical addition and sampling, coolant storage, coolant treatment, main steam and turbine bypass, turbine generator, main condenser, condensate and feedwater, reactor building component cooling water, recirculated cooling water, and instrument air. The second system set can contribute to rapid reactor overheating and is in general identical to the first set but operates under different scenarios.

BROAD FAILURE MODE AND EFFECTS ANALYSIS

Broad failure mode and effects analyses were conducted on each of the candidate plant systems by considering component failures and determining the safety consequences of such failures. To limit the effort involved in this task, a top-down methodology employing superposition was applied in generating first-order effects (i.e., those that can be defined a priori). Subsequently, system conditions necessary to bring about the projected failed state were determined, and then minimal failure chains required to produce these conditions were adduced. In this manner significant failed states were found, frequently with only one or two underlying failures (a failure chain stemming from a single failure is treated as one failure).

The broad failure mode and effects analyses included detailed examination of the Oconee 1 integrated control system. Plant events were selected based upon the integrated control system analysis and prioritized according to potential severity, need to determine the corresponding event sequence, and need to assess the time available to the operator for corrective action.

Common cause failures were investigated by examining loss of electrical power or pneumatic actuation capability. In general, the safety consequences of such failures could be avoided by appropriate operator intervention. Pneumatic actuation failures can be propagated across Oconee units because of the shared instrument air system. Moreover, substantial main feedwater upsets, abnormal operation of the emergency feedwater system, and abnormal operation of the turbine bypass valves can occur if instrument air availability is interrupted.

AUGMENTED FAILURE MODE AND EFFECTS ANALYSIS

Where feedback exists between the failure outcome and the initiating event, a hybrid computer model was used to augment the failure mode and effects analyses. The hybrid computer model emphasizes control system dynamics and was developed with techniques similar to those currently used in major systems class codes. It couples thermal hydraulics, neutronics, and control systems packages to produce a total-plant simulator. Characteristics of the hybrid model include (1) equilibrium (except in the pressurizer), one-velocity, two-phase thermal hydraulics; (2) various levels of treatment of core neutronics; and (3) representations of all primary controllers in the Babcock and Wilcox integrated control system. The hybrid computer model has been validated against Oconee 1 plant upset data and has been written to be adaptable to other plant configurations.

REACTOR OVERCOOLING

Rapid reactor overcooling transients fit into two classes: release of reactor coolant, and increased heat loss through the steam generators. In the first class, significant single failures include failure to the open position of the pressurizer pilot-operated relief valve, failure of a reactor coolant pump seal, and rupture of a steam generator (SG) tube. The second class comprises rapid steam generator overfills or failure open of a turbine bypass or main steam safety/relief valve. Failures of the integrated control system panelboard KI branch circuits HEX or HEY, as well as failure of branch circuits, can initiate some reactor overcooling transients.

STEAM GENERATOR OVERFILL

Steam generator overfill also can lead to two classes of problems that may compromise the system:

1. The primary system coolant may be overcooled directly by its thermal contact with an excessive amount of heat rejection on the secondary side. Using the hybrid computer program, this effect was studied in considerable detail for cases of no reactor trip. Low power levels produce more pronounced effects than high power levels, but the integrated control system appears capable of bringing the system to a new steady state whether the power is high or low.

2. A more serious event occurs when the overfill occurs in one SG, is rapid, and produces a reactor trip. The reactor trip can come as a result of cooling and power asymmetry in the core, or indirectly as a result of a turbine trip caused by excessive water present at the HP turbine outlet, water which had been introduced by excessive flow from a SG. Such an event can lead to water ingress to the steam line at rates and in amounts sufficient to cause damage to steam line instruments, associated components such as valves, and steam line supports. Such damage from SG overfills has occurred at Beznau, Switzerland (1969), and at Davis Besse (1985). If steam line supports are damaged, there is a reasonable probability that the steam line will deform or collapse and rupture, with some probability of consequent steam tube rupture. No event of this magnitude has occurred. Were such an event to occur, it would be a small-break loss-of-coolant accident (LOCA) vented directly to the atmosphere.

INADEQUATE CORE COOLING

Rapid inadequate core cooling can occur as a result of failure of the plant systems that replace lost reactor coolant. Three failure modes were found to require operator intervention to avoid possible rapid reactor overheating. Two failure modes involve failure of integrated control system power supply branch circuits (auto power and hand power), resulting in loss of automatic control of the main feedwater; the third consists of failure of a letdown cooler tube.

RECOMMENDATIONS AND FUTURE WORK

Proper operator intervention can, in general, avert the possible safety consequences resulting from the failures investigated in this study. The following actions are recommended:

1. redesign the steam generator high-level main feedwater pump trip circuitry from a series to a parallel configuration;

2. rearrange the gang selection switching algorithm to obtain compatible sets of pressure taps and other connecting equipment shared by the main and emergency feedwater systems;

3. use the plant computer more effectively to process instrument signals; and

4. rewrite certain operator procedures to minimize the impact of control failures in nonsafety-grade control systems at Oconee 1.

The Oconee 1 recommendations can be generically extended to all Babcock and Wilcox pressurized water reactors in a guarded fashion. Design differences compel caution in this regard, a matter treated to some degree in the body of this report. Unfinished work includes studies originally scheduled on (1) the effects of harsh environments in creating multiple failures of control systems, (2) operator response to multiple alarms and failures, and (3) the impact of frequent challenges to protection systems.

1. INTRODUCTION

1.1 PROGRAM SCOPE

The U.S. Nuclear Regulatory Commission (NRC) Unresolved Safety Issue (USI) on Safety Implications of Control Systems (USI A-47) Program is intended to generically assess the safety implication of nuclear power plant control systems by examining the consequences of control system failures and actions, both planned and unplanned.

These assessments are to be completed by performing thorough, plant-specific analyses of control/safety dynamics and interactions from a plant system perspective, developing criteria for establishing the relative importance of control/safety systems, and recommending design and operation guidelines for these systems based on their relative importance.

Specifically, the three interrelated goals addressed by the NRC USI A-47 Program are as follows:

1. assess the safety implications of control systems by examining the effects of control system malfunctions on plant dynamic behavior and by investigating the interactions of such malfunctioning controls with other plant systems;

2. formulate a method for assessing the failure mode and effects of control systems on the basis of common cause, common mode, and other multiple failures such as cascade failures; and,

3. develop criteria for establishing the relative importance of control systems important to safety, and recommend importance-to-safety classifications and any changes to regulatory requirements as may be indicated by the results of this work.

In performing these tasks, the NRC USI A-47 Program is governed by the following objectives of its Task Action Plan:[1]

". . . USI A-47 is to perform an in-depth evaluation of the control systems that are typically used during normal plant operation and to verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent non-safety grade control system failures,"

". . . During the licensing process, the staff performs an audit review of the non-safety grade control systems, on a case-by-case basis, to assure that an adequate degree of separation and independence is provided between these nonsafety-grade systems and the safety systems, and that effects of the operation or failure of these systems are bounded by the accident analysis in Chapter 15 of the plant's Safety Analysis Report,"

> ". . . On this basis it is generally believed that control system failures are not likely to result in loss of safety functions that could lead to serious events or result in conditions that the safety systems are not able to mitigate. In-depth studies for all the non-safety grade systems have not been performed however, and there exists some potential for accidents or transients being made more severe than previously analyzed, as a result of some of these control system failures or malfunctions,"
>
> and
>
> "Two potential concerns have already been identified in which a failure or malfunction of the non-safety grade control system can (1) potentially cause a steam generator or reactor vessel overfill, or (2) can lead to a transient (in PWRs) in which the vessel could be subjected to severe overcooling. In addition, there is the potential for an independent event like a single failure, (such as a loss of power supply, a short circuit, open circuit, control sensor failure) or a common mode event (such as a harsh environment caused by an accident or a seismic event) to cause a malfunction of one or several control systems which would lead to an undesirable control action, or provide misleading information to the plant operator. These concerns will be reviewed and evaluated. . . ."

1.2 OBJECTIVES

The objectives of this study, which represents one segment of the Oak Ridge National Laboratory (ORNL) contribution to the NRC USI A-47 Program, are to investigate, for a given set of pressurized water reactors (PWRs), the four principal foci of the NRC USI A-47 Program:

1. evaluate control system failures that could lead to steam generator (SG) overfill transients (reactor vessel overfill is also a USI A-47 concern but is a nonissue in the PWRs of the ORNL study),
2. evaluate control system failures that could lead to reactor overcooling transients,
3. evaluate other control system actions that have safety implications, and
4. evaluate the effect of loss of control system power sources (e.g., ac, dc, pneumatic, and hydraulic).

This plant-specific report documents the detailed examination of these four objectives for Oconee 1, which is an early generation Babcock and Wilcox (B&W) lower-loop pressurized water nuclear steam supply system (NSSS) located in Seneca, South Carolina and operated by the Duke Power

Company. An attempt will be made to broaden the results of this plant-specific analysis so that they may be generically applied to all B&W PWRs.

1.3 LIMITATIONS

This study embodies all of the objectives (as related to Oconee 1) of the NRC USI A-47 Program. It does not extend the NRC USI A-47 Program objectives to include multiple control system failure initiating events such as earthquakes, fires, and floods (both external and internal to the containment), nor does it look at the effects of sabotage. Because these initiating events are important, they should be addressed in another program or in a later extension of this one. Only the operator's first choice of the appropriate actions during a control system failure were identified; alternative operator actions were not studied.

Additional limitations of this study include

- Only single and two-at-a-time multiple failures were systematically considered in the initial broad FMEA. The follow-up computer augmented FMEAs considered single and two-or-more-at-a-time failures as dictated by program interests.

- The effects of control system failures during an accident or during normal plant operation will in some cases differ from plant to plant, thus making it difficult to develop complete generic solutions to the problems we find on a plant-specific basis.

1.4 METHODOLOGY

In completing detailed examinations of control-safety system failures for Oconee 1, certain systems were selected for analysis through a logical process which evaluated their relationship to the events to be examined in this study: steam generator overfill, reactor overcooling, and reactor overheating (inadequate core cooling). All major plant systems were screened to determine those whose failure could cause or exacerbate plant failure modes. Subsystems or components which interface with any of the selected major systems were then identified.

This system survey defines chains of interfacing components in which each member of the chain has some significance to the transient event classes under study.

Each component of each chain has been examined for modes of failure and for the effects of each such failure mode. The failures which define the minimum set leading to certain safety consequences are thus identified. Many of these failures lead to events that are clearly benign. These failures will be dropped from further consideration.

Other events not considered here are those found to be precursors of accident sequences that have been considered elsewhere [e.g., in the pressurized thermal shock (PTS) program, or in Chapter 15 studies for licensing reports].

A failure mode and effects analysis (FMEA) is the standard method implemented for a systematic, qualitative search for significant failures and their consequences. The standard FMEA[2] provides an orderly method for studying the possible failure modes of a single component in an important system and then treating all causes and consequences of each such failure mode. The FMEA process conceptually fails each of the systems that could potentially contribute to one of the three classes of safety consequences, and the results are determined (as far as possible) on an a priori basis. This process is a "broad FMEA."

Systems which have a capability to affect the chosen failure classes are systematically examined for failure modes and their resulting first-order effects. The term "First order" refers to those consequences that can be determined by logical inspection. For quantitative results, particularly those from scenarios in which the affected system feeds back altered input conditions to the initiating event, failure effects must be determined by computer analysis. These analyses are referred to as augmented FMEAs and consist of executing detailed total-plant thermal-hydraulic simulations of Oconee 1 using the ORNL-developed hybrid computer model. This model couples a digital simulation of plant fluid dynamics and neutronics to a simulation of the plant control systems. The results of these runs are fed back (augmented) to the FMEA process for final determination of the consequences of controls failures. Probabilities are then estimated for those failures of interest that can lead to steam generator overfill, reactor overcooling, or inadequate core cooling events.

Figure 1.1 is a flowchart illustrating the methodology used in this study.

Appendixes A, B, and C are structured to represent the detailed calculations supporting the following sections of this report as well as to provide generic information. Appendix D incorporates Duke Power Company's comments on the September 1984 draft report and ORNL's responses to those comments.

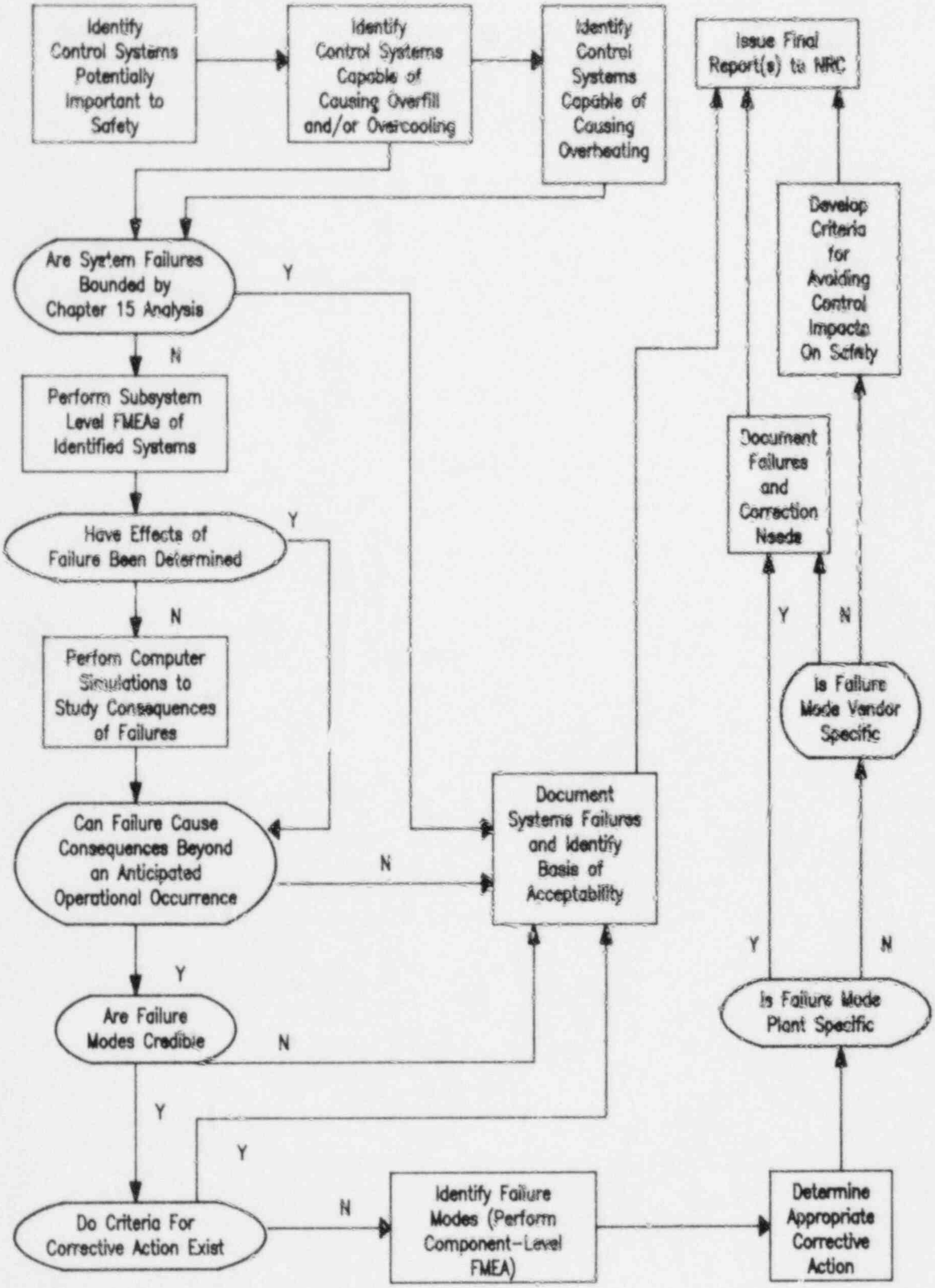

Identify Control Systems Potentially Important to Safety
Identify Control Systems Capable of Causing Overfill and/or Overcooling
Identify Control Systems Capable of Causing Overheating
Issue Final Report(s) to NRC
Are System Failures Bounded by Chapter 15 Analysis
Y
N
Perform Subsystem Level FMEAs of Identified Systems
Have Effects of Failure Been Determined
Y
N
Perform Computer Simulations to Study Consequences of Failures
Can Failure Cause Consequences Beyond an Anticipated Operational Occurrence
N
Y
Are Failure Modes Credible
N
Y
Y
Do Criteria For Corrective Action Exist
N
Identify Failure Modes (Perform Component-Level FMEA)
Determine Appropriate Corrective Action
Document Systems Failures and Identify Basis of Acceptability
Is Failure Mode Plant Specific
Y
N
Is Failure Mode Vendor Specific
Y
N
Document Failures and Correction Needs
Develop Criteria for Avoiding Control Impacts On Safety

Fig. 1.1. Flowchart for study of the safety implications of Oconee-1 plant control systems.

2. IDENTIFICATION AND SELECTION OF OCONEE PLANT SYSTEMS FOR SICS ANALYSIS

As discussed in Sect. 1, the objective of the Safety Implications of Control Systems (SICS) Program is to identify control system failures that can cause or contribute to severe nuclear power plant transients. In particular, severe overcooling or undercooling of the reactor coolant system (RCS), overfilling the steam generators, and adversely affecting recovery from design basis transients have been identified as severe plant transients of concern in the SICS Program.

Oconee Unit 1 was selected as the detailed design model for analysis of the B&W nuclear steam supply system (NSSS) plant design. The Oconee Nuclear Station, operated by Duke Power Company, has three similar PWR units, each rated at 866 MW(e). Unit 1 achieved initial criticality on April 19, 1973, Unit 2 on November 11, 1973, and Unit 3 on September 5, 1974. The Oconee units and B&W systems in general have several design features that make them unique among PWRs. These features include straight tube, counter flow, once-through steam generators (OTSG), highly automated and integrated plant control instrumentation, the integrated control system (ICS), and reactor vessel internals vent valves, which have been found to be useful in mitigating reactor vessel pressurized thermal shock.[3]

The first task in the SICS analysis is specific identification of the systems in Oconee Unit 1. This is discussed in Sect. 2.1. Due to the large number of systems and the scope of the SICS Program, a process for selecting those Oconee control systems pertinent to the SICS transient types discussed above was required prior to detailed systems failure analysis. The systems selection process for control systems contributing to RCS overcooling and undercooling transients is discussed in Sect. 2.3. The systems selection processes for SG overfill and impacts on design basis transients are discussed in Sects. 2.4 and 2.5 respectively. A summary and description of the systems selected for detailed analysis are provided in Sect. 2.5. Brief descriptions of the major operating systems are provided in Appendix A.

2.1 OCONEE UNIT 1 CONTROL SYSTEMS

Performing detailed analyses of the large number of systems in the Oconee Nuclear Power Station is not practical. Therefore, a method was required to (1) identify Oconee systems and (2) select systematically those control systems requiring detailed analysis. To ensure completeness, the methodology must also provide a means of tracking and reevaluating systems not selected for FMEA.

The first task, identification of Oconee systems, is basic to subsequent control systems analyses. Two principal sources of information were used to identify the plant systems: a generic PWR plant systems list[4] and the Oconee Final Safety Analysis Report (FSAR).[5] The method used to identify systems was based on the generic systems list. Specific Oconee systems with functions analogous to each of the generic systems were then identified, primarily from FSAR descriptions. In this way, all generic PWR system functions would have an identified Oconee system or the omission could be identified and resolved using supplementary information. In a similar manner, the identified generic systems were compared to the systems described in the FSAR to ensure that all generic systems and functions of importance were included.

A list of Oconee systems was developed using this method. This list, including numerical system designations, is provided in Appendix A, Tables A.1 through A.7.

Once the Oconee systems were identified, the functions of these systems were evaluated to narrow the number of plant systems to the specific scope of the SICS analysis. In this way, the analytic effort could be focused on plant control systems analyses, minimizing analyses that would be duplicated in other current programs. The systems not considered to be within the program scope included

1. Standby Safety Systems: Standby safety systems have been evaluated extensively in other programs, and the study of their failure modes in the control systems analysis would be redundant. However, safety qualification of a system alone is an insufficient basis on which to exclude the system from consideration. Safety-qualified systems performing a normal control function were included in the analysis. Furthermore, the response of safety systems to transients initiated by control system failure were considered because the identification of control system failures that degrade safety functions is an objective of the program.

2. Systems Isolated by Reactor Trip: During power operation, the plant systems are controlled within specified parameter limits. If these limits are exceeded, a reactor trip will be initiated. Failure to trip (failure of a standby safety system) is being studied as part of the Anticipated Transients Without Scram (ATWS) Program and will not be considered in this (control systems) analysis. Once the reactor is tripped, some plant systems are isolated and cannot affect the course of the post-trip transient [e.g., the control element drive (control) system]. Since a reactor trip transient itself is not of concern in this analysis, systems isolated following reactor trip were not evaluated in the control systems analysis.

3. Shutdown Systems: Certain plant systems such as the residual heat removal system (Oconee low pressure injection system) and reactor refueling equipment are placed in service manually following shutdown and depressurization of the reactor. The failure modes of these systems were not evaluated in this program because the residual heat removal systems are being evaluated in other analysis

programs, and shutdown systems would not be placed in service in response to control system-induced transients.

The above evaluation procedure has been used to categorize the Oconee systems into two groups: those to be excluded from the SICS analysis for the specific reasons outlined above, and those Oconee control systems within the specified scope of the SICS program. In addition to the systems listed in Appendix Table A.2, the Oconee plant electrical systems have been evaluated[6] and will be incorporated into the SICS results. The excluded systems, including the reason for their exclusion, are listed in Appendix Table A.11.

2.2 OPERATING EXPERIENCES

Plant operating experiences at Oconee and all other operating B&W plants were surveyed and analyzed. This type of study can be useful in two ways. First, it may uncover or suggest other sequences of interest not detected by the FMEA or simulator studies. Second, some rough estimate or corroboration may be obtained of the likelihood of development of events corresponding to the SICS sequences. One rather obvious observation indicates a significant limitation of the SICS study resulting from the methodology used and the ground rules that have been imposed. That is, events in which multiple independent control and safety system failures and operator errors are compounded, such as in the loss of all feedwater at Davis Besse on June 9, 1985, do not have, and would not be predicted to have, a significantly high probability of occurrence (see Sect. 2.2.2). This is because the probability of combinations of several "independent" failures, each with a relatively small likelihood, is diminishingly small. A suggested alternative approach for predicting these unlikely events is noted in Sect. 2.2.2.

Relevant operating experiences at the three Oconee plants are listed and analyzed in Sect. 2.2.1, and in Sect. 2.2.2, the same is done for the other operating B&W plants. In addition, the reader is referred to several recent NRC documents that contain extensive reviews and tabulations of B&W transients and operating records.[7-9]

2.2.1 Relevant Oconee Operating Experiences

Operating experiences extracted from Licensee Event Report (LER) reference files for Oconee Units 1, 2, and 3 were reviewed and analyzed, with particular attention to feedwater-related perturbations, both for SG overfeed events that could be considered overfill precursors and for undercooling events. The period covered is January 1975 through early 1985. In general, it was found that most of the events were of the single-failure type that would be covered by FMEA methodology. Only 14% of the events noted were attributed to operator error or maintenance problems, well below the industry norm. Four of the events involved the integrated control system (ICS) which, until placed in manual control mode, tended to further degrade the situations. The difficulty is that the ICS does not have the capability to distinguish a true from a false input signal. Although the B&W ICS is one of the most advanced control systems used in current U.S. commercial nuclear power plants, it is not the equal of today's "smart" controllers.

The events at the three Oconee units are listed and described in Table 2.1.

Of the five events listed that caused Unit 1 to trip, two were the result of ICS reactions. Another LER (84-002), involved multiple failures and is indicative of the complexity and unpredictability of some of the real-life transients noted above. The LER description indicates that the incident began during a check of pressurizer level instrumentation. When the level check switch was pushed, the relay for the reactor T-hot indication immediately dropped out, causing a low T-hot indication. The relay for the pressurizer level check was located in the same ICS cabinet as the T-hot relay; its actuation apparently caused the T-hot relay to open. The ICS began a feedwater (FW) runback on low T-hot indication that Btu limits were exceeded. The Btu limits were designed to prevent a steam temperature reduction if a unit tried to remove more energy from the steam generator than was available. In the case under consideration, FW flow demand was limited by T-hot because the Btu limit was in effect. The ICS was switched to manual to try to balance FW flow to reactor power output. The decreased FW flow resulted in decreased heat transfer from the RCS and caused RCS pressure to increase to the trip point. The T-hot relay failure was attributed to dirty contacts. Following the trip, two main steam relief valves did not reseat properly, and the pressure had to be reduced to 900 psi before they closed. The RCS temperature dropped to 545°F before the secondary response due to the unseated valves was stabilized. The RCS inventory was controlled by opening the RC loop A injection valve with the 1A high-pressure injection (HPI) pump in operation for normal makeup. Following the reactor trip, it was noted that the control rod drive position indication was showing 10% withdrawn (instead of 0%) due to a faulty power supply.

Five of the nine Unit 2 LER events were concerned with the turbine-driven EFW pump. The events were all trivial in nature and were rectified within 15 min.

At Oconee 3 there was a 1.5-y period of operation during which apparent problems with the preventive maintenance program may have been responsible for persistent valve failures. During that period, four LERs were issued on just two valves. The trouble ceased after the valves were repacked. Two other Unit 3 events could have produced a severe transient, resulting in equipment damage if they had occurred or gone to completion during plant operation. These were the SG overfill (LER 81-003) and the feedwater header design deficiency (LER 82-006). Overpressurization of the secondary side of OTSG B occurred during cold shutdown when the pressure was permitted to go to 550 psig. The SG overfilled, and water got into the main steam line. This incident

Table 2.1. Feedwater-related perturbations at Oconee Nuclear Plant

Event date	Event	Cause	Initiator	Duration of event	Power level	LER
Unit 1						
12/14/78	RSC T_{avg} erratic and indicating low	Short in power cord cord		NA	98%	78-027
	Reactor trip on high press/temp	ICS withdrew control rods				
	Both feedwater pumps trip	High discharge pressure	Emergency feedwater pumps started but stopped when normal feed pumps reset and restarted			
	OTSG B goes dry, OTSG A goes to 6" (normal ≥110")	Malfunctioning of valves				
	HPI system actuated	Low RCS pressure	Refill of OTSG B caused RCS pressure to drop below set point			
5/1/80	Turbine-driven emerg. feedwater pump isolated from SG 1B	Personnel error	Valve in discharge line to SG 1B was clogged instead of valve to SG 2B	16 h	73%	80-012
5/9/80	Turbine-driven emerg. feedwater pump declared inoperative	Bearing failure	Shaft packing leakage allowed water to contaminate bearing oil	53 h	75%	80-013
1/5/80	Reactor trip	Loss of excitation on generator field		NA	90%	81-001
	Large positive power tilt on restart	Large feedwater swing	Opening "A" feedwater block valve allowed a large flow due to excessive leakage thru main feedwater valve. Also, manual control of valves caused a large ΔT_C between loops			
6/2/81	Turbine-driven emerg. feedwater pump declared inoperative	Governor valve struck open	Fouled valve bushing	NA	100%	81-010
2/3/82	1B motor-driven emerg. feedwater pump inop.	Bearing vibration	Misalignment between pump and motor	NA	50%	82-001
7/6/82	Emergency feedwater pumps for Units 1 & 2 inoperative	Personnel error	Missed surveillance	43 d	70%	82-013
12/14/82	Turbine-driven & "A" motor-driven emerg. feedwater pumps inoperative	Defective procedures	Newly rewritten "Restoration to Service" procedures used for first time and breakers to oil pumps were deenergized	1 min	100%	82-020
5/12/84	Feedwater Btu limit runback	Dirty contacts	During test of pressurizer level switch, relay for reactor T_{hot} dropped out	14 s	100%	84-001
	T_{hot} relay drops out	Integrated control system began a feedwater runback				
	RCS press. increased	Decreased feedwater flow	ICS was switched to manual to balance feedwater flow to reactor output			
	Reactor trip	HI RCS pressure	Unit stabilized in hot shut-down			
	Main steam pressure reduced	2 MSIVs did not reset properly	RCS reduced to 900 psig and 585°F			
	Control rod drive relative position off 10%	Faulty power supply				

Table 2.1. (continued)

Event date	Event	Cause	Initiator	Duration of event	Power level	LER
12/3/84	Reactor trip on loss of main feedwater	Low oil pressure on shaft-driven oil pump for 1B feedwater pump	1A main feedwater pump out of service. Transferred oil supply for 1B MFWP from aux. oil pump to shaft-driven oil pump. SOP failed. Auto-transfer back to AOP failed	11 h	57%	84-007
	OTSG level increased 25 in.; slight over-cooling	Emerg. feedwater level control system fails				
	Main steam pressure reduced 200 psi	3 MSIVs did not reset properly	Unit stabilized in hot shut-down			
4/25/85	Loss of control room annunciators	KX inverter power supply lost	Transfer to alternate source prevented by a blown fuse	1 h	100%	Event No. 574
	Loss of one main feed pump	Oscillations in ICS	Manual swapping of oscillators			
	Reactor trip	Second main feed pump tripped			60-100%	
	RCS pressure reduced	MSRV stuck open	Pressure reduced to reset valve. Unit stabilized in hot shutdown			

Unit 2

Event date	Event	Cause	Initiator	Duration of event	Power level	LER
12/10/80	Turbine-driven emerg. feedwater pump inoperable	Start circuitry deenergized	Relay in start circuitry for TDEFWP aux. oil pump shorted and tripped the breaker	NA	100%	80-021
3/4/81	Motor-driven emerg. feedwater pump 1B inoperable	Motor arcing	Stator of motor shorted, then breaker was tagged out	64 h	74%	81-004
4/23/81	Turbine-driven emerg. feedwater pump inoperable	Loose trip level linkage	TDEFWP trip mechanism discovered tripped and discharge valve shut	NA	100%	81-010
5/6/81	Turbine-driven emerg. feedwater pump declared inoperable	Empty oil sump	Operator observation	NA	100%	81-012
5/6/81	Auto level control for OTSG B stuck in manual	Stuck solenoid valve	Operator observation	NA	100%	81-008
6/16/82	2B emerg. feedwater flowpath inoperable	Valve 2FDW-216 would not open fully	Found during functional testing; handwheeel was partially shut	NA	59%	82-009
9/16/82	Turbine-driven feed-water pump inoperable	Trip/throttle valve in tripped state	Alarm annunciated; trip probably due to vibration	10 min	100%	82-012
10/5/82	Turbine-driven feed-water pump inoperable	Personnel error	Maintenance bumped valve	13 min	100%	82-013
5/31/83	2A motor-driven emeg. feedwater pump inoperable	Loss of power	Power removed to facilitate repair of main feedwater disch. press. switch	18 h	100%	83-008

Table 2.1. (continued)

Event date	Event	Cause	Initiator	Duration of event	Power level	LER
Unit 3						
5/5/76	Lower-than-normal indicated RC flow	Feedwater & reactor reactor coolant incorrectly set	Plant computer flow constants inerror	NA	100%	76-006
7/13/76	Feedwater transient	Spurious control signal	30% decrease in feedwater water demand induced oscillations	2 s	81%	76-006
8/22/76	Feedwater penetration valve inoperable	Sampling valve failed to close	OTSG valve 3FDW-108 air operator failure	NA	100%	76-013
11/21/76	Feedwater penetration valve inoperable	Sampling valve failed to close	Fourth occurrence (74-4, 75-7, and 76-13)	NA	90%	76-020
3/22/76	Feedwater penetration valve inoperable	Sampling valve failed to close	OTSG valve 3FDW-106, repacked valve	NA	100%	77-004
11/29/80	Turbine-driven emerg. feedwater pump shut shutdown	Personnel error	Incorrect valve line permitted lube oil sump to empty	NA	50%	80-018
2/26/81	OTSG B over-pressurized & over filling	Startup control valve leakage	Overfilling permitted water to enter main steam line	NA	Cold Shutdown	81-003
5/17/81	3B motor-driven emerg. feedwater pump declared inoperable	Cooling water inlet valve failed	Airline, to valve 3LPSW-25 discovered broken	NA	100%	81-010
4/30/82	SG internal aux. feedwater heaters deformed	Inadequate design	Design could not accommodate the large pressure forces generated when cold aux. feedwater is injected into the header.	NA	Refueling Shutdown	82-006
5/13/83	Turbine-driven emerg. feedwater pump made inoperable	Personnel error	Loss of power to aux. oil pump when breaker was pulled	81 s	100%	83-006
10/13/83	3B motor-driven emerg. feedwater pump inoperable	No service water flow	Failed solenoid valve on motor cooler outlet	14 h	Hot Shutdown	83-011
10/18/83	3B motor-driven emerg. feedwater pump inoperable	Feedwater valve stuck partially open	Apparent component failure	40 min	100%	83-012
6/7/84	Reactor trip	Loss of both feedwater pumps	Erroneous indication to RPS, source unknown; unit runback from 100% (The same thing happened the day before without causing a trip.)	49 h	20%	84-003
8/14/84	Reactor trip	Main feedwater pumps trip	Air line to condensate outlet valve accidentially sheared. Condensate booster pumps tripped causing feedwater pumps to trip.	16 min	100%	84-005

apparently was caused by the startup control valve leaking through and filling OTSG B and the main steam line. Nothing was found wrong with the control valve, either electrically or mechanically. The cause of the incident was judged to be a procedural deficiency in that the block valves were not specified to be shut during that particular mode of operation. Inspection showed that no damage was done to the pipes or hangers; however, under different circumstances overfilling of the SG and pipes could have led to much more severe consequences.

The benefits derived from reviewing the experiences at other plants were demonstrated in the case of LER 82-006. Because of the discovery of damage to the OTSG internal auxiliary feedwater (AFW) headers at Davis Besse and Rancho Seco, Unit 3 was shut down to begin a refueling outage earlier than originally planned. Visual inspection revealed damage similar to that reported at the other plants. Some of the headers were deformed and showed extensive cracking and strong localized corrosion.

In conclusion, review of the Oconee LERs for the past 10 years indicated no abnormal occurrences led to potentially severe accidents or unsafe conditions, although under different circumstances a small number could be considered potential precursors to damaging accidents. In addition, an NRC survey of feedwater supply system failures showed Oconee 1 to have a much better record than other PWRs in the period 1981-1983.[9]

2.2.2 Relevant Operating Experiences at Other B&W Plants

The LER files at the ORNL Nuclear Operations and Analysis Center were searched for relevant occurrences at the other operating B&W reactors (Arkansas-1, Crystal River-3, Davis Besse, and Rancho Seco). Selected occurrences are listed by event date and LER number in Table 2.2. These experiences were reviewed to identify possible common traits or those irregular events that might be peculiar to B&W plants. Again, it was found that the integrated control systems (ICS) often made "events" caused by equipment problems more complex rather than keeping the situations under control. For example, the Control Element Assembly Calculator would at times generate penalty factors from extraneous signals, which caused a reactor trip when fed to the core protection calculators.

The following observations apply to the events listed in Table 2.2:

1. Errors made during construction activities and other inadvertent actions by operating personnel caused several violations of technical specifications, either by inadvertent actuation of equipment or by breach of containment integrity. This indicates a need for improved operator training and better orientation of maintenance personnel.

2. Inverter malfunctions, although not frequent, always produced unanticipated results at unexpected times. The ensuing disturbances tended to bemuse the operators. When they correctly diagnosed the

Table 2.2. Operating experiences at other B&W reactors

Event date	Event	Cause	Initiator	Duration of event	Power level	LER
Arkansas 1 (50-313)						
4/7/80	Trip	Loss of offsite power	Tornado in area	25 min	100%	80-001
6/24/80	Trip	Partial loss of offsite power	Ground fault due to trees in the lines and subsequent overload	NA	100%	80-002
7/8/81	EFW pump tripped	Overspeed mechanism malfunction	4 events in 6-month period possibly due to vibration	NA	100%	81-005
7/27/81	Steam-driven EFW pump unavailable	Steam valve failed to open	6 other events - valve operator worn	NA	Hot shutdown	81-009
3/16/84	Trip	Anticipatory trip on loss of both MFW pumps	Perturbations in the control oil possibly due to clogged filters		17%	84-002
1/7/85	Steam-driven EFW pump tripped	Inadequate steam flow	Orifice and closed bypass valve found in line. These should have been removed during prior turbine replacement	24.5 h	Refueling	85-001
4/9/85	Trip	Feedwater transient	Apparent failure in ICS		100%	4/10/85
5/31/85	Trip	High primary pressure from loss of main feedwater pump	Main turbine intercept valves closed unexpectedly. Increased steam pressure caused a large crack in expansion joint of the feedwater heater	NA	100%	5/31/85
8/13/85	Trip	High RCS pressure	Loss of condenser vacuum due to fracture of one SG blowdown pump casting from water hammer	~12 h	100%	Daily rpt 8/14/85
Crystal River 3 (50-302)						
2/26/80	RCS transient	I&C electrical system malfunction	Malfunction opened PORV on pressurizer and held it open 5-7 min. Safety valve and possibly PORV discharged water during transient	2 h		80-010 EPRI NP-80-13-LD
10/28/82	Emergency feedwater train inoperable	Instrument failure	(15 events for this instrument) 23 total violations. Feedwater ultrasonic flow indicator inoperable. High ambient temperature		95%	82-067
8/30/83	Overfill of SG A	Control valve for feedwater pump stuck open during transient	Misaligned linkage arm on valve	7 min	75%	82-035
11/3/83	Inverter 3A inoperable	Blown fuse	Maintenance being performed shorted out a lamp base		97%	83-058
11/7/83	Containment radioactivity monitor inoperative	Isolation valve failed closed	Blown fuse caused by a defective light bulb; control circuit shorted		97%	83-052
3/12/84	Engineered safeguards actuated	Spurious noise	Testing on one train when other actuated. Borated water injected into RCS → power reduction	NA	98%	84-005
12/28/84	Improper response of control room annunciator	Grounds in electrical circuitry	Positive ground from case shorted wire, and preexisting intermittent negative ground disoriented the display system for 10 min	Several h	97%	84-010

Table 2.2. (continued)

Event date	Event	Cause	Initiator	Duration of event	Power level	LER
Davis Besse (50-346)						
4/19/82	Steam generator tube damage	Interaction with aux feedwater header	Discovered during SG eddy current inspection - subsequently found in other SGs	NA	0%	82-019
5/11/83	Steady state core quadrant power tilt		Inherent design of B&W NSSS coupled with a large negative temperature coefficient at the end of core life		25%	83-024
6/9/85	Loss of all feed-water	MFW pump trip	Reactor trip on high RCS pressure. SFRCS initiated on spurious low steam generator level signal. Both MSIVs closed. Operator error caused steam generator isolation. AFW pumps tripped on overspeed and would not restart automatically due to malfunction. PORV opened to relieve RCS pressure and stuck open. AFW restarted manually 17 min after trip	30 min	90%	IE note 85-50
Rancho Seco (50-312)						
6/9/80	Potential for SFAS unavailable	Inverter failure	If one inverter were out of service and the second one failed, automatic SFAS initiation would be prevented	NA	95%	80-028
4/19/81	4000-gal coolant transfer	Personnel error	Transfer from RCS to reactor building emergency sump. One DHR system in test, the other in service. Both have common suction header. Break-down in communications; procedures ok	NA	Refueling	81-024
7/7/81	Sample line isolation response slow	Foreign material in pneumatic line	Desiccant from instrument air dryers coated air passage fi.ters, slowing response	NA	100%	81-037
4/19/82	OTSG auxiliary feedwater header ring deformed	Generic B&W problem	Inspection revealed deforma-tions similar to those noted at Davis Besse	NA	0%	82-010
3/25/83	Cracked bolts - core barrel to support shield	Stress	19 out of 120 bolts showed cracks at head-to-shank transition	NA	Refueling	83-009
9/19/83	PORV failure	TMI modification	A visual indicating rod added to the operating lever caused valve to malfunction	NA		IE-83-78 (daily report)
2/29/84	Reactor trip on high pressure	Feedwater transient	ICS in auto mode for RCP shut-down. Plant response was unstable when a coincident grid frequency disturbance was experienced. The combination led to RPS actuation	NA	65%	84-007

situations, and when there were no other independent component or system failures, the event was usually terminated quickly. In other cases, however, more serious consequences--or at least significant precursors--would result.

3. Several other types of electrical problems led to reportable events. Low voltage readings on station batteries are indicative of inadequate maintenance practices or end of service life (see LER 313 82-028). There have also been recent incidents reminiscent of the Rancho Seco light bulb accident (see LER 302 83-058).

4. There are histories of unnecessary scrams that challenge the protection and shutdown cooling systems (see LER 313 82-020). Based on an NRC survey of 1984 scram data, B&W plants were found to have a better than average industry record for number of scrams, averaging about three per reactor year.[10] This was about half the rate for CE and GE plants and about one-third the rate for Westinghouse reactors, but still greater than the scram rates for Japanese and most European plants.

5. In the period since the TMI-2 accident, the most significant event at a B&W plant occurred at Davis Besse on June 9, 1985 (see Table 2.2). The incident involved multiple control and safety equipment and operator error problems, including at least 10 component failures classified as independent. Probably the most significant feature of the event is that in the preceding six months at Davis Besse, 10 interruptions of main feedwater (MFW) occurred. Problems with control of the AFW pumps were also experienced intermittently during that period. This suggests that the excessive number of challenges (MFW failures) to a safety system (AFW) that was already having reliability problems should be considered as a warning of an incipient incident. Operators and regulators perhaps should be more alert to patterns and frequencies of problems in order to prevent such incidents.

Events related to maintenance and testing are common to the entire reactor industry and in general deserve more attention. Improvements in man-machine interface areas would result in fewer challenges to the safety and plant protection systems as well as generally safer and more economic operation.

2.3 SELECTION OF CONTROL SYSTEMS POTENTIALLY AFFECTING RCS OVERCOOLING OR UNDERCOOLING

The control systems listed in Appendix Table A.8 have the potential to affect plant transients to varying degrees. These systems were further screened to assess their potential to affect RCS overcooling or undercooling.

Evaluating the specific undercooling or overcooling response of the RCS to system failures would require detailed analysis. However, for purposes of system selection, a method based on identification and characterization of system-to-system interfaces was used to select those control systems that potentially could affect RCS transient behavior.

Each control system listed in Appendix Table A.2 was evaluated based on the following criteria:

1. All systems having a direct (first-order) interface with the RCS (including the pressurizer and the steam generator) were listed and are tabulated in Appendix Table A.9.

2. Only those systems directly affecting RCS response were selected. Interfacing systems that may be affected by but do not themselves affect RCS response were eliminated, although it should be noted that some systems eliminated for this reason may be selected as an interfacing system (see Item 3 below).

3. For the remaining systems, all systems interfacing with the systems selected in Appendix Table A.9 were identified. These second-order interfacing systems, excluding those in Appendix Table A.9, are listed in Appendix Table A.10.

The list of systems initially selected for analysis includes all control systems that potentially affect RCS response during plant transients and all second-order systems that potentially affect the response of first-order systems. The specific impact of failures of these systems on RCS cooling are evaluated in this report.

In summary, the following 11 major control systems potentially affecting RCS overcooling or undercooling were selected for detailed failure modes and effects analysis (FMEA).

Principal Fluid Systems

1. Reactor Coolant System (N04)
2. Makeup and Purification System (N05)
3. Main Steam and Turbine Bypass System (P01)
4. Turbine Generator System (P02)
5. Main Condenser (P03)
6. Condensate and Feedwater System (P04)

Supporting Fluid Systems

7. Reactor Building Component Cooling Water System (W03)
8. Recirculated Cooling Water System (W04.D)
9. Instrument Air System (W07.B)

Control Instrumentation Systems

10. Integrated Control System (ICS) (N02.B)
11. Nonnuclear Instrumentation (NNI) (N02.C)

In addition to the above systems, local control instrumentation will be considered along with associated fluid system components (e.g., local pump and driver controls). Also, the plant electrical systems have been analyzed. The results of this analysis are described in ref. 6 and will be incorporated into the FMEA results presented in Sect. 3.

To ensure completeness and to verify the adequacy of the selection procedure, each of the systems not selected was briefly reevaluated to assess its potential impact on the SICS program. The results of this evaluation are provided in Appendix Table A.11.

2.4 SELECTION OF CONTROL SYSTEM POTENTIALLY AFFECTING SG OVERFILL

In contrast to RCS overheating or overcooling, SG overfill can be readily defined and contributing systems identified. SG overfill results directly from an uncontrolled injection of FW into either SG. Based on a review of the control systems listed in Appendix Table A.8, one principal fluid system and associated interfacing systems potentially affect SG overfill:

Principal Fluid Systems

1. Condensate and Feedwater System (P04)

Supporting Fluid Systems

2. Instrument Air System (W07.B)
3. Main Steam and Turbine Bypass System (P01)
4. Turbine Generator System (P02)
5. Main Condenser (P03)

Control Instrumentation Systems

6. Integrated Control System (ICS) (N02.B)
7. Nonnuclear Instrumentation (NNI) (N02.C)

Other systems that potentially affect SG overfill include electrical systems, local instrumentation, and physical interfaces with the NNI (e.g., the SGs). Although the auxiliary feedwater (AFW) system may initiate SG overfill, it is a safety system and will be considered only to the extent it responds to control system-initiated transients.

2.5 SELECTION OF CONTROL SYSTEMS POTENTIALLY AFFECTING RECOVERY FROM DESIGN BASIS TRANSIENTS

In evaluating the SICS, it is necessary to evaluate the effects of control system failures on noncontrol-system-initiated transients as well as those transients directly initiated by control system failures. The control systems of Appendix Table A.8 were reviewed with respect to the system responses described in the Oconee design basis accident analysis section of the Oconee FSAR.[5] Based on this evaluation, control systems potentially affecting recovery from design basis transients were identified.

Sixteen design basis accidents were evaluated in the Oconee FSAR. Of these, eight either did not affect the RCS (e.g., waste gas decay tank rupture) or were terminated by reactor trip (e.g., uncompensated operating reactivity changes). These accidents are listed in Appendix Tables A.12 and A.13. Accidents with significant post-trip RCS impact, including major events such as loss-of-coolant accidents (LOCAs), are listed in Appendix Table A.14.

The major accident analysis descriptions were reviewed with respect to the control systems listed in Appendix Table A.8. The principal fluid systems that could potentially affect recovery from the listed accidents were found to be those identified for RCS overcooling and undercooling transients (Sect. 2.3).

3. EVALUATION OF SICS TRANSIENTS

In Sect. 2, 11 Oconee control systems were identified that could contribute to the identified SICS transients of concern: RCS overcooling, RCS overheating, SG overfill, and recovery from design basis accidents. In Sect. 3, the specific failure modes of these systems are identified and evaluated to assess their relative importance to safety.

Evaluation of the safety implications of control system failures was accomplished in two steps: (1) a detailed evaluation of the specific failure modes of the systems and (2) subsequent evaluation of the combinations of failures that could result in significant adverse safety effects. Analyses of system failure modes using the FMEA technique is discussed in Sect. 3.1. Section 3.2 evaluates and discusses sequences of possible safety significance including evaluation of expected sequence frequencies. (The major analysis results are summarized in Appendix B.1.)

3.1 FAILURE MODE AND EFFECTS ANALYSES

Failure Mode and Effects Analyses (FMEA) have been performed on the Oconee control systems to identify failure modes of interest to the SICS Program. The choice of the FMEA technique over other techniques such as fault tree analysis was based on the relative lack of knowledge concerning specific failure modes of interest and the expected subtlety of the failures and their effects. A discussion of the methodology selection process is provided in Appendix B.1.

Detailed, component-level FMEAs have been performed on the major control systems selected (Sect. 2), and detailed tables of results are presented in the Appendices. Appendix B.2 contains the FMEA tables for the steam cycle systems: the main steam and turbine bypass system, the turbine generator, the main condenser, and the condensate and feedwater system. The makeup and purification system FMEA, including the letdown fluid processing equipment, is provided in Appendix B.3. Appendix B.4 provides the FMEA of the RCS pressurizer subsystem.

These appendices present the FMEA results based on fluid system components. They also address the effects of failures of control instrumentation and supporting fluid system components. The following subsections summarize and discuss the results of these analyses with respect to their significance to RCS undercooling, RCS overcooling, SG overfill, and recovery from design basis accidents.

3.1.1 Failures Contributing to RCS Undercooling

RCS undercooling occurs when heat generated in the reactor core (and to a lesser extent by the operating RC pumps) is not removed from the RCS. Safety implications of RCS undercooling, however, occur only when the combined actions of the plant control and safety systems fail to provide an adequate mechanism for heat transport from the reactor core itself.

Assuming that the reactor is tripped (a safety function), insufficient core cooling will occur in a PWR such as Oconee, only from an inadequate reactor coolant inventory. This condition can result from either a breach of the RCS (LOCA) or a total loss of steam generator cooling and loss of safety injection of reactor coolant.

Specific failures of the Oconee control systems that may contribute to or initiate a LOCA, a loss of steam generator cooling, or degradation of the safety injection functions are identified and discussed in this section. Insufficient core cooling effects resulting from failures in the RCS subsystems (pressurizer, RC pumps, and SGs) and associated control instrumentation and support systems are identified and discussed in Sect. 3.1.1.1. The insufficient core cooling effects of failures in power conversion and makeup and purification systems are discussed in Sects. 3.1.1.2 and 3.1.1.3, respectively.

3.1.1.1 Reactor Coolant Subsystems. Three RCS subsystems have been identified as potentially contributing to insufficient core cooling transients: pressurizer, RC pump, and SG subsystems. Table 3.1 lists the insufficient cooling failure modes and interfacing systems associated with the failure modes for each RCS subsystem, and component-level FMEAs of each of these subsystems are presented in Tables 3.2, 3.3, and 3.4. Following are discussions of the results of the pressurizer, RC pump, and SG subsystem FMEAs.

3.1.1.1.1 Pressurizer subsystem. Release of reactor coolant (a small LOCA) has been identified as an insufficient cooling initiator for the pressurizer subsystem. In Table 3.2 the specific component-level failures leading to or contributing to this failure mode are identified, and the potential causes of the failure, its effect on the RCS, and possible remedial actions are listed for each.

A release of reactor coolant will result initially from either the PORV or pressurizer code safety valve failing open. Code safety valves are passive devices that open when the fluid pressure on the valve's seat overcomes the spring force holding the valve closed. The valves are designed to close when the fluid pressure is no longer sufficient to hold the valve open (this trip point is typically lower than the opening pressure). Safety valves could fail to close due to improper valve maintenance or possibly severe operating conditions (e.g., liquid discharge), which could result from control system failures. If one of the safety valves does fail to close, the leak path cannot be isolated (see Table 3.2, Item 1).

The pilot-operated relief valve (PORV) opens and closes in response to external control signals. It is opened by applying power to the pilot valve solenoid. This results in the pilot valve opening and applying fluid pressure to the relief valve operator, which in turn opens the

Table 3.1. Summary of RCS subsystem failure modes

RCS Subsystem	Insufficient Cooling Failure Mode	Interfacing Systems and Components Affecting Failure Mode	Comments
1. Pressurizer	1.1 Release of Reactor Coolant	1.1.1 PORV	FMEA of Pressurizer System presented in Table 3.1.2.
		1.1.2 NNI	
2. RC Pumps	2.1 Release of Reactor Coolant	2.1.1 RC Pump Shaft Seals	FMEA of RC Pumps presented in Table 3.1.3.
		2.1.2 RB Component Cooling Water System	
		2.1.3 MU&P System	
3. Steam Generators	3.1 Release of Reactor Coolant	3.1.1 Steam Generator Tubes	FMEA of Steam Generators presented in Table 3.1.4.
		3.1.2 Main Steam and Turbine Bypass System (Excessive Cooldown Possibly Contributing Tube Failure)	
	3.2 Loss of Steam Generator Cooling	3.2.1 Feedwater and Condensate System	
4. Balance of RCS	4.1 Release of Reactor Coolant	4.1.1 MU&P System	FMEA of MU&P System presented in Table 3.1.6.

Table 3.2. Summary of pressurizer system FMEA: Failures leading to or affecting insufficient core cooling transients

	Failure	Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant				
1.	PORV RC-RV3 Fails Open	Mechanical failure of valve resulting in valve opening or failure to close once open.	Small LOCA. Pressurizer fills during RCS depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block valve, RC-4.
2.	Pressurizer Code Safety Valve Fails to Close	Mechanical failure of valve(s) to close after opening possibly due to control system failures.	Small LOCA or RCS leak. Pressurizer fills during depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA must be followed. Open valve may be identified by discharge pipe high temperature indication.
3.	Power to PORV Solenoid Fails On	o NNI Pressure Switch (RC3-PS8) or Controller (RC3-MIS2) Failure	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block valve, RC-4. PORV manual control may be operable.
		o NNI narrow range RCS pressure transmitter or signal conditioning modules produce spurious high RCS pressure signal.	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer spray valve RC-V1 opens and pressurizer heaters are deenergized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by manual closure of the PORV, RC-RV3 or its block valve RC-4. The pressurizer spray valve, RC-V1, may be manually closed and the pressurizer heaters manually controlled.
4.	Failure of Selected Pressurizer Level Transmitter Output Signal Low	Transmitter failure or a failure of the selected transmitter's power supply (ICS Panelboard KI branches HEX, HEY or Computer Panelboard KU)	A selected low pressurizer level signal results in the makeup valve opening and filling the pressurizer, deenergizing the pressurizer heaters and possibly initiating a steam generator overfill transient (see Table 3.1.3, FMEA of the Steam Generators). If the pressurizer is allowed to fill, the PORV or safety valves would be opened and the possible liquid discharge through the valve could contribute to their failure.	The operator can compare the three pressurizer level measurements through the computer and manually select an operable transmitter for control and indication. Manual control of the makeup valve (and feedwater control valves) is available. The loss of a transmitter power supply is alarmed in the control room.

Table 3.3. FMEA of RC pumps: failures leading to or affecting insufficient core cooling transients

Failure		Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant				
1. RC Pump Seal Failure	o	Simultaneous loss of pump seal injection and RB component cooling water.	Small LOCA. Seal failures can not be isolated.	Trip pump prior to seal failure and achieve cold shutdown. Emergency procedures for small LOCA's must be followed once seal failure occurs.
	o	Failure of seal injection following operation with excessive seal wear or damage.	Same as above.	Same as above.
	o	Undetected seal materials defects.	Same as above.	Same as above.
	o	Injection of particulates into seal-shaft surface.	Same as above.	Same as above.
	o	Excessive thermal cycling of seals.	Same as above.	Same as above.

Table 3.4. FMEA of Steam Generators: failiures leading to or affecting insufficient core cooling transients

Failure	Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant			
1. Steam Generator Tube Failure	o Material defects in tubes.	Steam generator tube rupture accident: a small break LOCA with the reactor coolant released to the main steam system and condenser.	Emergency procedures for steam generator tube rupture accident must be followed.
	o Long term operation with adverse feedwater chemistry.	Same as above.	Same as above.
	o Excessive magnitude/ frequency of compression and tension cycles on tubes with undetected defects in tube material.	Same as above.	Same as above.
	o Severe cooldown of RCS with undetected defects in tube material.	Same as above.	Same as above.
Insufficient Steam Generator Heat Transfer Rate			
2. Injection of Main Feedwater to Both Steam Generators Terminated	o Main feedwater pumps trip.	A trip of the feedwater pumps terminates main feedwater but automatically initiates Emergency Feedwater. Insufficient cooling will not occur unless the Emergency Feedwater System fails.	Confirm automatic initiation and control of Emergency Feedwater. If Emergency Feedwater fails, manually initiate HPI on low reactor coolant subcooling.
	o Main feedwater flow isolated (Main and Startup Valves Closed).	Steam generator dryout occurs with subsequent pressurization of the RCS and opening of the PORV and/or pressurizer safety valves.	Manually initiate Emergency Feedwater and confirm subsequent closure of PORV. If low reactor coolant subcooling occurs, manually initiate HPI.

relief valve. The relief valve is closed by deenergizing the pilot valve solenoid.

The PORV may fail open in response to mechanical failures of the relief valve or pilot valve (Item 1) or a control circuit failure, which energizes or fails to deenergize the pilot valve solenoid (Item 3). Certain circuit failures such as a failure of the valve control switch or pressure switch may occur with other pressurizer components operating normally. The decreasing pressurizer pressure will be detected, resulting in the spray valve closing and the pressurizer heaters being energized. Other failures, such as those generating a spurious high pressurizer pressure signal, will result in the PORV and spray valve opening and the pressurizer heaters being deenergized. In contrast to safety valve failures, a failed open PORV may be isolated by manually initiating PORV block valve closure, which will terminate the release of reactor coolant.

Failure of the pressurizer pressure transmitter or associated signal-conditioning modules producing a spurious high pressurizer pressure signal also will result in the opening of the spray valve. The effects of the spurious high pressure signal include opening the PORV (a small LOCA) and deenergizing the pressurizer heaters in addition to opening the spray valve.

Failure low of the selected pressurizer level transmitter has been included in this category because a pressurizer overfill transient could occur. Valve damage could occur if the overfill is allowed to result in liquid discharge through the PORV or the safety valves.

In addition to failures that result directly in a potential insufficient core cooling transient, other pressurizer system failures may exacerbate the effects of such a transient. These failures include instrumentation failures that could impede the detection of an open relief or safety valve and failure of the PORV isolation valve, which could prevent rapid termination of a transient resulting from a failed open PORV.

3.1.1.1.2 RC pump subsystem. One insufficient cooling initiator in the RC pump subsystem has been identified: release of reactor coolant due to failure of the RC pump shaft seals. RC pump seal failures may result from several causes (see Table 3.3). If degraded performance of the RC pump seals is recognized by the operator prior to complete failure of the seals, seal failure may be delayed by tripping the affected pump. Once seal failure occurs, however, the resulting small LOCA cannot be isolated.

3.1.1.1.3 Steam generator subsystem. Two potential insufficient cooling initiators have been identified for the SG subsystem: release of reactor coolant due to SG tube failure and insufficient heat transfer rate across the SG. The FMEA of the SG subsystem is presented in Table 3.4.

Steam generator tube leaks that occur during normal operation are typically due to a combination of causes (see Table 3.4). Although control system failures have not been identified as the sole cause of a tube leak or failure, control system failures may initiate a tube failure in combination with other existing conditions, or may increase the rate of tube degradation.

The impact of SG tube failure on insufficient cooling depends on the rate of release of reactor coolant. The more common small leaks may not result in a net loss of reactor coolant if the makeup system is capable of injecting coolant at the tube leak rate. However, the less frequent tube rupture transients which result in a leak rate of hundreds of gallons per minute are small LOCAs. In addition to the direct effects of the release of reactor coolant, SG tube rupture procedures typically require rapid cooldown and depressurization of the RCS.

Insufficient core cooling transients resulting from a loss of SG cooling have been identified in Table 3.4, Item 2. The FW pump trip and MFW isolation cases are considered in detail in the FMEAs of the main steam and turbine bypass system and the condensate and main feedwater system, which are discussed in Sect. 3.1.1.2.

3.1.1.2 Power Conversion Systems. As discussed earlier, the loss of SG heat transfer insufficient cooling mechanism can be initiated by failures in the MFW systems. Specific failures in these systems contributing to potential insufficient core cooling transients are discussed below.

3.1.1.2.1 Main Steam and Turbine Bypass System. The main steam and turbine bypass system transports the steam generated in the SG to the high-pressure turbines or diverts it directly to the atmosphere or condenser. In addition to piping, the system consists of 16 spring-loaded code safety valves, 4 pneumatic turbine bypass valves, the high-pressure turbine stop and governor valves, and high-pressure steam supply lines to the MFW and EFW pump turbines.

Following reactor and turbine trip, the steam generated by reactor core decay heat can be rejected to the condenser via the turbine bypass valves or to the atmosphere via any of the code safety valves. No credible failure modes could be identified that would significantly affect the capability to reject steam at decay heat levels.

Steam supply isolation valves MS-35 or MS-36, if closed during plant operation, would result in the inoperability of the associated MFW pump following main turbine trip. No single failure was found that would affect both pumps. Steam supply isolation valves MS-82 and MS-84, if closed during plant operation, would result in inoperability of EFW pump A. However, closure of both valves would be required to affect emergency pump operation, and even these failures do not affect operability of the two motor-driven EFW pumps.

3.1.1.2.2 Condensate and Main Feedwater System. Failures in the condensate and MFW systems have two principal effects of significance to inadequate core cooling: (1) a trip of both MFW pumps, and (2) isolation of the FW flow to both SGs. Component failures leading to these conditions are identified in Table 3.5 and discussed below.

Many single failures are expected to result in trip of both MFW pumps. These failures include loss of condenser vacuum, flow blockages upstream of the MFW pumps, or failures of the hotwell or condensate booster pumps. In addition, single failures in the FW control valves or the ICS FW control circuits that result in a high level in either SG will cause automatic trip of both FW pumps. Failures in the pump trip circuitry or selected ICS power supplies also result in FW pump trip. Trip of the MFW pumps results in automatic initiation and control of the EFW system.

Although failures can be identified that would isolate FW flow to one or the other SG, single-component failures that would isolate both SGs could not be identified. However, two ICS power supply failures, failures of the "auto power" (H1 or H circuits), of the "hand power" (H1X or HX circuits) and of one module in the FW pump speed control circuits may result in termination of MFW flow. These failures are of importance because automatic initiation of EFW would not be expected (EFW is automatically initiated by a trip of the FW pumps or very low discharge pressure).

Loss of hand power results in the speed of both MFW pumps decreasing to 2800 rpm (zero V speed signal in a ±10-V range) and the turbine bypass valves closing and remaining closed. In this condition, with the reduced shutoff head of the MFW pumps less than the lowest setpoint pressure of the main steam code safety valves, the flow to both SGs will stop (see Sect. 4).

In addition, low failure of a "sum" module in the speed control circuit of the ICS FW pumps may result in minimum pump speed. In contrast to the power failure, however, the turbine bypass valves would remain operable, which increases the likelihood of continued flow at lowered pump speed. In any case, this failure would not affect the ability of the operator to increase pump speed manually.

Failure of the auto power circuit may not result in an immediate transient. However, many plant controls would transfer to manual including the MFW flow control valves. Under this condition, the operator may close the main and startup control valves manually to prevent an initial SG overfill and the pump trip that would otherwise follow a reactor trip.

With either of the power supply failures, the FW flow to both SGs may be terminated without tripping the MFW pumps and consequently without an automatic initiation of EFW. Although the operator would be able to initiate and automatically control EFW manuallv, the spurious alarms and deenergized indicators may be confusing. Furthermore, the initial SG FW

Table 3.5. Summary of condensate and main feedwater FMEA: failures leading to or affecting insufficient core cooling transients

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Condenser Vacuum Breaker Valve V-186 (7)	Valve spuriously opens	Instrumentation or maintenance failure.	Turbine trip, trip of MFW pump turbines and interlock of turbine bypass valves closed.	Identify open valve and manually close. Reestablish condenser vacuum. Ensure automatic initiation of EFW if MFW pumps trip.
Hotwell Pump Isolation Valves C-1, 2, 4, 5	Valve spuriously closes	Instrumentation, maintenance failure.	Less than 50% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen valve or reopen failure. Ensure automatic initiation of EFW if MFW pumps trip.
Hotwell Pump B, C	One or both pumps tripped, inoperable	Electric power, motor failure, loss of Recirc. Cooling Water flow to bearing coolers.	Failure of both pumps and failure of one pump at higher power levels result in FW pump, reactor trip and automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue following loss of one pump.	Identify and repair failure. Ensure automatic initiation of EFW if MFW pumps trip.
Condensate Valve C-10	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Trip of FW pumps and reactor. Automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
Demineralizer Bypass Valves C-14, 15	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Less than 30% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen or repair.
Generator Water Cooler Bypass Valve C-61	Valve spuriously closes	Instrumentation or valve operator failure.	Trip of FW pumps and reactor. Automatic initiation and control of emergency feedwater.	Identify closed valve and repair failure.

Table 3.5. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Condensate Booster Pump Isolation Valves C-77, 80, 81, 84	Valve spuriously closes	Instrumentation, maintenance failure.	Less than 50% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen valve or reopen failure.
Condensate Booster Pumps A, B	One or both pumps tripped, inoperable	Electric power, motor failure, loss of Recirc. cooling water flow to bearing coolers.	Failure of both pumps and failure of one pump at higher power levels result in FW pump, reactor trip and automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue following loss of one pump.	Identify and repair failure.
"F" Low Pressure FW Heater Isolation Valves C-89, 90, 91	Valve spuriously closes	Instrumentation or maintenance failure.	Less than 33% reduction in condensate flowrate. Probable FW pump and reactor trip at higher power level with automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
Low Pressure FW Heater Isolation Valves C-103, C-104, C-110, C-111, C-117, C-118	Valve spuriously closes	Instrumentation or maintenance failure.	Less than 33% reduction in condensate flowrate. Probable FW pump and reactor trip at higher power levels with automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
FW Heater Drain System	Unspecified - Dwg. PO-123A not available	Unspecified - Dwg. PO-123A not available.	Effects bounded by a trip to the main FW pumps and automatic initiation and control of emergency feedwater.	Identify failure and repair.
FW Pumps A, B	Pump trip	Instrumentation failure, pump/turbine failure, high steam generator level, loss of Recirc. cooling water flow to oil coolers - see also FMEA of Condensate System and Main Steam System.	Trip of one pump will result in a plant runback and possible reactor trip at higher power levels (>50% power). Trip of both pumps results in reactor trip and automatic initiation and control of emergency feedwater.	Identify failure and repair.

Table 3.5. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
	Spurious speed decrease	Instrumentation or throttle valve operator failure.	Possible decrease in feedwater flowrate resulting in plant runback and possible reactor trip. A runback of both MFW pumps to minimum speed will not result in automatic initiation of EFW. Loss of steam generator cooling may occur if EFW not manually initiated.	Manually initiate EFW on low SG level. Identify failure and repair.
		Power to selected startup level transmitter fails (ICS Panelboard KI, branch HEX or HEY).	Depending on the manual selection of the HEX or HEY powered startup level transmitters, either or both main feedwater control valves open resulting in overfeeding of the associated steam generators and possible RCS overcooling. The transient is automatically terminated by high steam generator level trip of the main feedwater pumps and automatic initiation and control of emergency feedwater. In addition to effects on feedwater control, these power failures could result in opening the makeup control valve and closing the loop A and/or B turbine bypass valves depending on manual transmitter selection.	Manually close main feedwater control and startup valves and makeup control valves. Automatic control may be restored by manual selection of operable steam generator startup level and pressure transmitters and pressurizer level transmitters.
FW Pump Recirculation Control Valve FDW-53, 55	Valve fails to open on low FW flowrate	Instrumentation or valve operator failure.	Following substantial feedwater flowrate decrease transients (e.g., reactor trip), failure to maintain minimum pump flowrate will result in pump trip or possible pump damage.	Identify failure and repair.

Table 3.5. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Control Valve FDW-32, FDW-41	Valve(s) open or fail to close on demand	Loss of instrument air pressure, instrumentation, or valve operator failure.	Valve(s) opening or remaining in position after reactor trip may resuit in a steam generator overfeed condition. Transient will be terminated by automatic trip of main FW pumps and initiation and control of emergency feedwater unless manually controlled by the operator. If main and startup valves are manually closed by operator, the startup valves must be manually reopened and controlled to maintain SG level. Automatic initiation of EFW will not occur.	Identify closed valve and manually reopen or repair failure
FW Startup Valve FDW-35, FDW-44	Valve(s) open or fail to close on demand	Loss of instrument air pressure, instrumentation or valve operator failure.	Valve(s) remain in position following reactor trip which may result in a steam generator overfeed condition. Transient would be terminated by automatic trip of main FW pumps and initiation and control of emergency feedwater unless manually controlled by the operator.	Identify failure and manually close startup or startup isolation valves.

levels may be high. As a result, the time delay from initial loss of power supply to the time FW flow rate must be reestablished to prevent SG dryout could also impede the decision to initiate EFW manually.

If the SGs were allowed to dry out, the operator would be expected to initiate high-pressure injection (HPI) manually on low reactor coolant subcooling. However, the existing confusing conditions already have resulted in the operator failing to initiate EFW manually. A subsequent failure to initiate HPI manually under these same conditions would be significantly more likely than otherwise might be the case.

3.1.1.3 Makeup and Purification System. The makeup and purification (MU&P) system continuously processes reactor coolant and returns the purified coolant to the RCS. In addition to coolant purification, the MU&P system supplies RC pump seal injection flow.

A detailed FMEA of the MU&P system has been performed, and the effects of MU&P equipment failures have been identified. The MU&P failures potentially affecting insufficient core cooling are summarized in Table 3.6.

The failures listed result in or contribute to the release of reactor coolant and, potentially, to insufficient core cooling. An isolable small LOCA can result from a letdown cooler tube failure (Table 3.6, Item 1). Two failures (Items 2 and 3) have been identified that contribute to the potential for a small LOCA. If a drain path from the standby letdown cooler is left open following maintenance, the failure may remain undetected because the cooler is isolated from the RCS. Should the standby cooler subsequently be placed in operation (isolation valves manually opened), a small LOCA would result.

Failure of the operating reactor building component cooling water flow results in isolation of cooling water to the letdown coolers and RC pumps. This failure results in automatic isolation of letdown flow. If the letdown storage tank (LST) is allowed to drain, resulting in damage to the operating HPI pumps, or if the HPI pumps were manually tripped to protect them, a simultaneous loss of RC pump seal injection and cooling water flow occur. As identified in Table 3.3, this condition could lead to RC pump seal failure.

In the three MU&P failures listed in Table 3.6, the LST will be drained unless an alternate supply of water is provided to the HPI pumps. Following a small LOCA, this action may occur automatically if the 1500-psi engineered safety features actuation system (ESFAS) set point is reached prior to draining the LST. If the LST is allowed to drain, the operating HPI pump would be damaged, degrading the HPI safety function required for mitigation of small LOCAs.

This consequence of draining the LST has been recognized by Duke Power Company, and "A modification is currently under way which will address

Table 3.6. Summary of makeup and purification system FMEA: failures leading to or affecting insufficient core cooling transients.

	Failure	Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant				
1.	Letdown Cooler Tube Failure	Corrosion, stress on tubes.	Isolatable small LOCA or RC leak. Prior to ESFS actuation, operating HPI pumps will be depleting letdown storage tank (LST). If the LST is allowed to drain, the operating HPI pumps would be consequentially damaged.	Manually open a flowpath from the BWST to the HPI pumps prior to depleting the LST. Isolate the affected letdown cooler, and place alternate cooler in operation.
Contributing Failures				
2.	Open Letdown Cooler Drain Path	Undetected, improper maintanance resulting in open drain path from an isolated cooler and subsequently placing the cooler into operation.	Isolatable small LOCA or RC leak. Prior to ESFS actuation, operating HPI pumps will be depleting letdown storage tank (LST). If the LST is allowed to drain, the operating HPI pumps would be consequencially damaged.	Manually open a flowpath from the BWST to the HPI pumps prior to depleting the LST. Isolate the affected letdown cooler, and place alternate cooler in operation.
3.	Reactor Building Component Cooling Water Flow to Letdown Cooler and RC Pumps Terminated	Spurious containment isolation valve closure or trip of a component cooling water pump and failure to start spare pump.	Letdown path isolated resulting in the RC pump seal injection flow being pumped from the LST. If the LST is allowed to drain, the resulting pump damage could result in a simultaneous loss of component cooling water flow and RC pump seal injection flow.	Manually open a flowpath from the BWST to the HPI pumps prior to draining LST. If component cooling water flow cannot be restored, trip RC pumps to prevent damage to pump bearings.

the concerns of an alternate HPI pump suction supply and additional LDST level alarms."[11]

3.1.2 Failures Contributing to RCS Overcooling

RCS overcooling is a transient response which results in a continued decrease in reactor coolant temperature. In contrast to RCS undercooling transients, however, the specific safety implications of overcooling are more difficult to define. Loss of reactor coolant will result in a continued decrease in temperature due to decreasing RCS pressure (i.e., the coolant saturation temperature is reduced). As discussed in Sect. 3.1.1, loss of reactor coolant contributes to possible inadequate core cooling. More generally, significant RCS temperature reductions have been analyzed to assess their impact on reactor vessel integrity due to the pressurized thermal shock (PTS) phenomenon. (PTS analyses of the Oconee plant are discussed in ref. 5.)

Section 3.2 discusses component failures resulting in RCS overcooling due to excessive SG heat transfer from the RCS. Component failures contributing to a loss of reactor coolant were addressed in Sect. 3.1.1. Transients resulting in a decrease in RCS pressure can occur due to pressurizer spray valve malfunction in addition to loss of reactor coolant. Spray valve malfunctions, however, are self-limiting and, as such, are not considered RCS overcooling events.

Failures resulting in increased SG heat transfer were found to be limited to the power conversion systems, specifically the main steam and turbine bypass system and the condensate and feedwater system. These contributing failures are discussed in the following sections.

3.1.2.1 Main Steam and Turbine Bypass System. The principal RCS overcooling effect caused by failures in the main steam and turbine bypass system is the potential for depressurizing the SGs. Reducing SG pressure reduces the saturation temperature on the secondary side of the SGs and increases the heat transfer rate from the RCS. Table 3.7 lists failures in the main steam and turbine bypass system that cause depressurization of the main steam system and the resulting effects on the RCS.

Failures potentially resulting in depressurization of the main steam system include the failure of main steam safety valves or turbine bypass valves to close as designed, a diversion of steam to the startup steam header, and failure of the main turbine to trip following reactor trip.

The 16 main steam code safety valves (8 valves per SG) are spring-loaded valves that open upon high steam pressure on the valve seat. As the steam pressure decreases, the force of the springs on the valve seats closes the valves automatically. Some of the safety valves are expected to open following turbine trip. Improper valve maintenance could result

Table 3.7. Summary of main steam and turbine bypass FMEA: failures leading to or affecting RCS overcooling

	Failure	Possible Causes	Effects	Remedial Actions
Depressurization of Main Steam System				
1.	One or More Main Steam Safety Valves (MS-1 through MS-16) Fails to Close Following Turbine Trip	Mechanical failure of valve, improper maintenance, discharge of entrained liquid through valves.	Steam leakage to the atmosphere. Depending on the response of the turbine and reactor controls, automatic reactor and turbine trip and potentially overcooling of the RCS could occur.	Emergency procedures for a small steam line break must be followed. Isolation of feedwater to affected steam generator may be required to prevent exceeding 100°F/hr RCS cooldown rate.
2.	One or Both Steam Generator A Turbine Bypass Valves (MS-19, 22) Fail Open or Fail to Close Following Turbine Trip	Mechanical failure of valve(s) or transducers, improper maintenance.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-17 as required to control RCS cooldown rate.
3.	Both Steam Generator A Turbine Bypass Valves (MS-19, 22) Open in Response to a Spurious Control Signal	o Spurious output of manual control station SS15A-MC (aux. shutdown panel) signals valves to open.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-17 as required to control RCS cooldown rate.
		o Spurious high output from selected steam generator A outlet pressure transmitter (SS6A-PT1 or PT2) or train A control circuit modules.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor turbine trip and potentially overcooling of RCS could occur.	Identify open valves and manually control. Close isolation valve MS-17 if required to limit RCS cooldown rate.
4.	One or Both Steam Generator B Turbine Bypass Valves (MS-28, 31) Fail Open or Fail to Close Following Turbine Trip	Mechanical failure of valve(s) or transducers, improper maintenance.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-26 as required to control RCS cooldown rate.

Table 3.7. (continued)

	Failure	Possible Causes	Effects	Remedial Actions
5.	Both Steam Generator B Turbine Bypass Valves (MS-28, 31) Open in Response to a Spurious Control Signal	o Spurious output of manual control station SS15A-MC (aux. shutdown panel) signal valves to open.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-26 as required to control RCS cooldown rate.
		o Spurious high output from selected steam generator B outlet pressure transmitter (SS6A-PT1 or PT2) or train A control circuit modules.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-26 as required to control RCS cooldown rate.
6.	Steam Generator A and B Turbine Bypass Valves (MS-19, 22, 28, 31) Open in Response to a Spurious Control Signal	Common setpoint module generates a spurious low setpoint pressure.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-17 and MS-25 as required to control RCS cooldown rate.
7.	Steam Generator A and B Turbine Bypass Valves (MS-19, 22, 28, 31) Fail to Close Following Turbine Trip	An initiating transient causing turbine trip followed by a loss of ICS Panelboard K1 branch H or H1 (Auto Power).	Steam diverted to condenser coupled with a main feedwater overfeeding of the steam generators. Unless manually terminated, the potential for RCS overcooling is significant.	Manually control turbine bypass and main feedwater control valves. If required, trip main feedwater pumps and verify automatic initiation and control of emergency feedwater.
8.	Diversion of Steam to Startup Steam Header	Unknown - PU-284-1 not available.	Steam diverted from HP turbine - may cause turbine and reactor trip and potential overcooling of RCS.	Identify diversion of steam and close isolation valves MS-24 and 33.

Table 3.7. (continued)

	Failure	Possible Causes	Effects	Remedial Actions
9.	Main Turbines Fail to Trip Following Reactor Trip	o Contacts in CRDCS fail to open on reactor trip.	Following reactor trip, continued steam flow through the turbines would result in depressurization of the turbine header, throttling of the turbine governor valve and possible overcooling of the RCS. Feedwater flowrate to steam generators initially throttled until low steam generator level setpoint is reached. The extent of RCS overcooling following this transient is unknown.	Attempt to manually trip the high and/or low pressure turbines. Manually throttle main feedwater to control RCS depressurization if required.
		o Unspecified failures in turbine control system (details of turbine control instrumentation unavailable).	Same as above.	Same as above.

in one or more safety valves failing to close at their (closure) set point pressure, potentially leading to RCS overcooling.

In addition to the safety valves, four turbine bypass valves are installed to control the steam line pressure following turbine trip. Two turbine bypass valves are connected to the steam line from each SG and may be isolated from the steam line by a manually operated isolation valve. Each pair of valves is controlled by a separate control circuit based on the pressure of the associated steam line.

Failure modes of the turbine bypass valves include those affecting one of the valves, modes affecting both valves on either steam line and, potentially, modes affecting all four valves. Failure of a single valve open or its failure to close (Table 3.7, Items 2 and 4) could be caused by a mechanical failure of the valve, the pneumatic operator, or the associated E/P transducer. Failure of both valves on either steam line to open or to close (Items 3 and 5) would be caused by failures in the common control instrumentation strings.

Two failure modes were identified that potentially could cause all four valves to fail open. Failure of the pressure set-point module common to both instrument strings (Item 6) could result in both instrument strings signaling the four turbine bypass valves to open. The second failure mode results in the four transiently open turbine bypass valves failing to close (Item 7), and involves a sequenced loss of the ICS Panelboard KI branch H or H1 (auto power). The specific effect of a loss of auto power is transfer of the turbine bypass valve to manual control. The valves would then remain in their existing positions. If the power failure occurred immediately following turbine trip, the four turbine bypass valves would be open and would improperly remain open. In the case of this particular power supply failure, the MFW control valves also transfer to manual and remain open.

Although this failure mode sequence appears highly unlikely, similar events have occurred (Oconee Reactor Trip 3-35, 11/10/79). It is believed that the response of the control instrumentation to a transient (which may be caused by control instrumentation failure) increases the likelihood of subsequent isolation of the instrumentation power supplies. It should be noted that most power supply failures other than branch H or H1 will cause the turbine bypass valves to close and remain closed.

In any of the turbine bypass valve failure modes identified, the operator has the option of closing one or both isolation valves and terminating the depressurization.

Diversion of steam to the startup steam header has been identified as a possible cause of steam line depressurization affecting both SGs. However, information concerning the distribution of steam to the startup steam piping has been unavailable. Should a control failure in the startup steam piping result in a significant diversion of steam from the steam lines, the operator has the option of terminating the depressurization by manually closing both startup header isolation valves.

Failure of the main turbine to trip following reactor trip has been identified as a possible cause of significant SG depressurization. However, while the potential for such a transient to occur is believed to be very unlikely, it remains unevaluated due to the unavailability of turbine control instrumentation design information. Following reactor trip, contacts in the control rod drive control system (CRDCS) open to signal the turbine controls to automatically trip the turbine. Should the CRDCS turbine trip contacts fail, the steam lines will begin to depressurize. The lower steam pressure would be sensed by ICS and a signal sent to the turbine controls to close the turbine throttle valves. It is unknown whether other parameters input to the turbine controls (e.g., turbine speed) would override the ICS signal and maintain the turbine throttle valves open. However, should the turbine trip and the throttle valves fail to close following a reactor trip, RCS overcooling potentially could occur. The consequences are bounded by those of the steam line break.

Two failures have been identified that would not result in an immediate steam line depressurization but could increase the severity of other subsequent failures. These are failures of the turbine bypass valve isolation valves and failure of a CRDCS turbine trip contact. It is believed that either failure could occur and remain undetected for a significant period of time.

3.1.2.2 Condensate and Main Feedwater System. The principal effect of failures in the condensate and main feedwater system on RCS overcooling is the potential for overfeeding the SGs. Following reactor trip, the potentially rapid increase in SG inventory is expected to result in RCS overcooling until it is terminated manually or automatically. Specific failures in the condensate and main feedwater system leading to overfeeding the SGs and the overall effects are identified in Table 3.8 and discussed below.

Steam generator overfeeding will occur if either MFW control valve fails open or fails to close following a reduction in FW demand such as a reactor trip. Typically, control valve failure open would be expected to have a greater impact on RCS overcooling at low reactor power levels; failure to close would be more severe at higher reactor power levels.

Failure open of one of the two control valves could occur due to a mechanical failure of the valve or its operator, failure of the E/P transducer, or failure of the associated ICS loop A or loop B FW control circuit (Table 3.8, Item 1). In the event one of the control valves fails open, the operator has the option of closing the main valve manually and controlling the startup valve, if possible, or tripping the MFW pumps. If the operator fails to control MFW flow, both MFW pumps will be tripped automatically on high level in either SG. Simulation was required for quantitative determination of the extent of RCS

Table 3.8. Summary of condensate and main feedwater FMEA: failures leading to or affecting RCS overcooling transients

Failure	Possible Causes	Effects	Remedial Actions
Excessive Addition of Feedwater to Steam Generators			
1. Main Feedwater Control Valve FDW-32 or FDW-41 Fails Open	o Unspecified failure in valve operator or associated valve control station.	Steam generator A or B level increases possibly resulting in reactor trip. Continued feedwater injection following reactor trip expected to result in RCS overcooling until terminated by high steam generator level trip of main feedwater pumps and subsequent automatic initiation and control of emergency feedwater. (Automatic closure of associated main feedwater block valve FDW-31 or FDW-40 is expected; however, this slowly closing valve is not expected to prevent the high level feedwater pump trip.)	Trip main feedwater pumps manually if required to control RCS overcooling. Confirm automatic initiation and control of emergency feedwater.
	o ICS Loop A or Loop B feedwater control circuit generates a spurious high demand signal due to a module failure.	Steam generator A or B level increases possibly resulting in reactor trip. Continued feedwater injection following reactor trip expected to result in RCS overcooling until terminated by high steam generator level control setpoint or high steam generator level trip of main feedwater pumps and subsequent automatic initiation and control of emergency feedwater.	Manually close main feedwater control valve and manually control startup control valve in the affected loop. Trip main feedwater pumps manually if required to control RCS overcooling. Confirm automatic initiating and control of emergency feedwater.
	o Failure of Steam Generator Startup Range Level Transmitter Sensing Tap.	Steam generator A or B level increases possibly resulting in reactor trip. Continued feedwater injection following reactor trip expected to result in RCS overcooling until terminated by high steam generator level control setpoint or high steam generator level trip of main feedwater pumps and subsequent automatic initiation of emergency feedwater. Emergency feedwater continues to overfill affected steam generator.	Manually close main feedwater control valve and manually control startup control valve in the affected loop. Trip main feedwater pumps manually if required to control RCS overcooling. Confirm automatic initiating and control of emergency feedwater. Manually control emergency feedwater based on steam generator operator range level signals.

Table 3.8. (continued)

Failure	Possible Causes	Effects	Remedial Actions
2. Main Feedwater Control Valves FDW-32 and/or FDW-41 Fails to Close Following Reactor Trip	o Loss of Instrument Air Pressure.	Following reactor trip, the supply of feedwater to the steam generators exceeds the RCS demand resulting in increasing steam generator levels and possible RCS overcooling. The transient is terminated by an automatic high steam generator level trip of the main feedwater pumps and automatic initiation and control of emergency feedwater using the backup nitrogen system. Loss of closure of the turbine bypass valves, the makeup control valve and RC pump seal return valve and opening the RC pump seal injection control valve.	Manually trip main feedwater pumps if required to control RCS overcooling. Follow emergency procedure for loss of instrument air.
	o Loss of ICS Panelboard KI Auto Power branch (H, H1) or manual transfer of main feedwater control valve to manual control.	Following reactor trip, the steam generators will be overfed resulting in possible RCS overcooling. The transient terminated automatically by a high steam generator level trip of the main feedwater pumps. Loss of auto power also results in the makeup, RC pump seal injection and turbine bypass valves transferring to manual and freezing in position. If the power failure occurred following turbine trip, the turbine bypass valves could fail in an open position resulting in a steam generator depressurization.	Manually close main feedwater control valves and manually control main feedwater startup turbine bypass and makeup control valves if required.
Contributing Failures			
3. Main Feedwater Pumps Fail to Trip Automatically on High Steam Generator Level	FPTX relay or associated steam generator operate range level transmitters or high level bistables fail to generate a main feedwater pump trip signal on demand.	Failure could occur and remain undetected during normal operation. The automatic main feedwater pump trip would not terminate a steam generator overfill transient if required.	If required, manually trip main feedwater, condensated booster or hotwell pumps to terminate overfill.

Table 3.8. (continued)

	Failure	Possible Causes	Effects	Remedial Actions
4.	RC Pumps Trip	Problems associated with pump seal or bearing cooling, electric power loss to RC pumps (and not affecting feedwater pumps), ESPS signal.	A trip of the RC pumps transfers control of the startup feedwater valves to the selected operate range level transmitters. If a selected transmitter was in an undetected failed low state, a steam generator overfill transient could occur with a simultaneous failure of the automatic high steam generator level feedwater pump trip.	Manually control the affected startup valve. Trip the main feedwater pumps if required to control steam generator overfill.
5.	Main Feedwater Block Valves FDW-31, 40 Fail Open	Failure of the valve, its motor operator or electric power supply.	Failure could occur and remain undetected during normal operation. Failure of the block valve eliminates one possible means of limiting steam generator feedwater injection.	If required, manually trip main feedwater, condensated booster or hotwell pumps to terminate overfill.

overcooling prior to automatic pump trip. Overcooling was minor, with results described in Sect. 4.

Single failures in the loop A and B common control circuitry are not expected to result in RCS overcooling due to downstream, loop-specific signal modification (ICS Btu limits or RCS T_{avg} controls). However, if the manually selected loop A and loop B startup level transmitters were powered from the same power source (ICS Panelboard KI branch HEX or HEY), a failure of this single power source would result in the loop A and loop B control valves failing open (Item 2). The operator has the option of controlling the main and startup FW control valves in each loop manually or tripping the FW pumps if required.

Loss of the instrument air system or failure of selected ICS Panelboard KI branch circuit H or H1 will result in the loop A and loop B MFW control valves failing in an "as is" position (Item 2). Loss of instrument air results in the FW control valves failing as is and the turbine bypass valves closing. If a SG overfeed transient results, it can be terminated by manual or automatic trip of the MFW pumps. Failure of Panelboard KI branch H, H1 (ICS auto power) results in many plant components, including the FW control valves, automatically transferring to manual control and remaining in position. If the plant was in steady state operation prior to the auto power, an automatic reactor trip may not occur in the short term. However, other effects of the loss of auto power such as the generation of many spurious control room alarms, may induce the operator to trip the reactor manually. Once the reactor is tripped, the SGs will be initially overfed. The operator has the option of manually controlling the FW control valves or tripping the FW pumps. Furthermore, a reactor trip from a high power level may result in an automatic trip of the MFW pumps on low suction pressure unless the operator rapidly throttles MFW. The FW pumps will be tripped automatically on high steam generator level if the level is not controlled manually. As noted in Tables 3.7 and 3.8, if the loss of auto power occurred following a turbine/reactor trip transient, the turbine bypass valves would be open. In such a case, the loss of auto power will transfer the turbine bypass valves to manual control while they are open, resulting initially in a combined SG depressurization and SG overfeed transient. The operator can manually control both the turbine bypass and the FW control valves. If required to control SG level, the operator may trip the MFW pumps and verify the automatic initiation and control of EFW.

In addition to condensate and feedwater system failures which directly result in overfeeding the SGs, a number of failures could combine with other failures to increase the severity of a transient.

Of the failures listed, possibly the most significant is the failure of the automatic high SG level MFW pump trip. This failure (Item 3), in combination with SG overfeed failures (Items 1 and 2), could result in the introduction of significant quantities of water into the steam lines unless the overfeed is manually terminated by the operator. The effects of SG overfill include, in addition to the potentially increased severity of RCS overcooling, possible damage to the main steam safety and turbine bypass valves, as well as significantly increased stresses on the main steam lines and their supports. Although the effects of increased stresses, possibly intensified by the opening and closing of turbine bypass or safety valves, have not been evaluated in detail, the conditional probability of consequential steam line failure would be increased.

Trip of the four RC pumps has been listed as a contributing failure (Item 4). Following a trip of the four pumps, control of the startup FW valves transfers to the operate range level transmitters at a 20-ft SG level set point. This action alone may produce some degree of RCS overcooling. However, the increased level is required to promote natural circulation in the RCS, and the rate of increase in SG level would be less rapid than following transients initiated by the MFW valves failing open or failing to close. If the selected operate range level transmitter on either SG were in a failed low state, the FW flow rate to the affected SG would continue beyond the 20-ft level set point and the automatic SG high level FW pump trip would be defeated.

Other contributing failures include failure of the MFW block valves (Item 5) and failures potentially resulting in exceeding FW chemistry specifications. Adverse FW chemistry could contribute to long-term degradation of SG tube integrity.

3.1.3 Failures Contributing to Steam Generator Overfill

Two classes of SG overfeed have been considered: (1) those which are associated with reactor and turbine trip and (2) those which are not. Any overfeed that causes liquid water to enter the steam line is considered an overfill. If water enters the steam line in sufficient quantity and is accelerated to sufficient velocity, the integrity of the steam line is threatened and additional serious hazards may arise.

Overfeeds not associated with reactor and turbine trip were studied in depth using hybrid computer simulation. Power levels from 20 to 100% and conditions corresponding to component failures in Classes D and E (as defined in Appendix D.9.1) were examined. These calculations are more fully described in Sect. 4 and Appendix C. The following summarizes the results sufficiently for the purposes of this section.

1. Some overfeeds led to low-quality steam that would carry moisture into the steam line. The quantities did not appear great enough to threaten the integrity of the steam line, although the levels might have been unacceptable for the turbine.

2. In each case the ICS brought the system to a new steady state or approached one. In no case was the primary side overcooled to the point that safety appeared threatened, although some of the

transient and new steady state conditions may have been unsatisfactory operating states.

3. Some of the cases probably would have induced reactor and turbine trips had there been additional trip logic enabled in the calculation. In particular, the conditions reached in some cases might have actuated a moisture separator turbine trip should such be provided in the reheater section, or could lead to a reactor trip on asymmetric power distribution. Such trips are not assumed in the SAR.

The second class of SG overfill, events associated with reactor and turbine trip, may in some events conceivably cause large quantities of water to flow into the steam line. These important events are described in Sects. 3.1.3.1 and 3.1.3.2.

A number of protective features are in the Oconee system to prevent the flow of water into the steam line:

1. ICS actions to adjust power level and secondary flow.

2. High level override signal, also in the ICS, which causes control to shift from demand to level control when the high level (85% of operate level range) has been reached.

3. Blocking valve which begins to close when the startup valve goes 50% closed (ICS actions).

4. High level MFW pump trip whose circuitry is considered external to the ICS and which is actuated when the operating level sensors register 90% of their range.

5. The operator may trip the MFW pumps to terminate the overfeed if he is aware of what is happening. However, the transients of concern are fast moving. We have therefore assumed no operator intervention.

We here consider failures that lead to overfill in a single SG, and which are much more likely to occur than failures affecting both SGs. Moreover, certain protective trips on the MFW pumps would affect only a single pump in a single SG overfill. In such cases the single SG overfill is the more dangerous.

Even with protective features 2, 3, and 4 defeated, the ICS appears to be able to maintain sufficient balance between power and secondary flow to limit water entry into the steam line to wet steam. However, as an overfeed caused by failures of features 2, 3, and 4 plus an initiating event develops, there will be accompanying upset conditions which can lead to reactor and turbine trips. Reactor trip causes turbine trip; turbine trip causes reactor trip; both will occur almost simultaneously.

We have found only one failure that defeats all protective features 1 through 4: the Class F failure described in Appendix B.5. Actually, this event does not defeat feature 4 (high level MFW pump trip). Instead, it causes the transient to continue under the head produced by the AFW after the MFW pump trip has occurred. As such, it is a somewhat more slowly developing transient, providing more time for operator intervention and less momentum into the steam line.

We will restrict consideration to the more dangerous case, in which the overfill occurs in a single SG driven by maximum allowed flow. As indicated, we have found no case where this might be brought on by a single failure. However, there are possible classes of failures such that one may occur and be present and undetected for an extended period of time; during that time the occurrence of a failure of one more component of an appropriate class can bring on overfill of one SG with water entering its steam line at maximum velocity.

The following two subsections deal with this scenario.

3.1.3.1 Water in the Steam Line. We have developed several ways of causing significant quantities of water to enter the steam line rapidly from a single SG. A Type A failure (one that disables both the MFW pump trip and the ICS high level signal limiting features) along with a Type D failure (an ICS failure that causes more FW demand than is necessary) will produce an overfill. The Type A failure can go undetected, but the operator should become aware of it fairly soon if it produces incorrect operation over the whole operating range. However, if the effects are confined to the high level end of the operating range, as they might be for certain kinds of pressure transducer or electronic logic module failures, the failed state could continue undetected for long periods of time.

Another compound failure mechanism combines a failure that places the high level MFW pump trip in an undetected failed state (Type B) and a subsequent failure that causes the low level sensing system to read low (Type C). Any one of several relays could fail in such a way as to leave the high level MFW pump trip disabled and undetected (see Sect. 3.2).

A single failure of the low SG pressure tap, its sense line, or the valve packing in its sense line can produce a condition that leads to SG overfill (Type F). Although the MFW pump trip remains operational in this case, the failure causes the EFW to continue to overfill following the pump trip (see Appendix B.5). This failure scenario is less threatening than the preceding two because it proceeds more slowly and imparts the momentum of the water to the steam line at a lower rate.

We next assume that an overfill has occurred in SG A as a result of one of the two preceding scenarios. Both MFW pumps increase to maximum speed because the pressure drop across control valve A is low. The overfeed of SG A then causes the secondary flow and inventory in SG A to increase while the outflowing steam temperature drops into the saturation region and the quality drops below one. The ICS, responding to the increased flow, calls for less flow, causing MFW B control valve to begin closing, but this closure has no effect on A because of the postulated failure. The net secondary flow increases, leading to a drop in core average temperature and a subsequent increase in power by the ICS in its attempt to compensate for this. These effects are demonstrated by calculations whose results are presented in Sect. 4 and Appendix C, showing the course of such an event without a turbine trip.

Steam from A and B mix in the turbine header, but since the mass flowing from A is much greater than the mass flowing from B, the net effect is a reduction in the quality of the total flow. With an assumed trip at .98 quality (main turbine manufacturer's specification), according to our calculations the turbine trips about 6.5 min into the transient. This causes closure of the turbine stop valves, reactor trip, and transfer of MFW pump turbine steam feed from the low-pressure turbine tap to the respective steam lines. (Trips could also arise from asymmetric cooling of the reactor core.)

Flow in the steam system is essentially stopped by the closure of the turbine stop valves. During this period of interrupted flow, which should continue until pressure builds to the point that a relief valve opens, phase separation should occur in the steam lines with the liquid draining into the lower regions of the SG.

Following reactor trip, the MFW pumps should initially slow down on a fast-acting, reduced-demand signal. However, the differential pressure across the SG A failed open MFW control valve will continue to generate an error signal whose integral soon dominates the demand signal and returns the MFW pump turbines to maximum speed. The diminished flow demand has no effect on the failed SG A control valve, but causes the SG B control valve to close further. The B control valve will remain open by ar. amount sufficient to satisfy the low-level set point constraint in SG B.

When the MFW pumps are operated at high speed with B control valve stopped down considerably, A control valve failed open, and the MFW high-level pump trip in an undetected failed state, the A steam line will be pressurized enough for one or more relief valves to open, thereby allowing significant flow and a relatively large amount of liquid to enter the line. As the steam quality deteriorates, MFW pump turbine A may trip. This can come about when excess liquid in the turbine intake causes excessive vibration or thrust, thus activating manufacturer-installed trips designed to protect the turbine against mechanical stress. In the absence of trips, the A pump turbine may fail as a result of excess liquid intake, or it may continue to function at normal or reduced efficiency. Regardless of which of these alternatives prevails at the A pump turbine, the B pump turbine and steam line should continue in good operating order. Ample pumping power is therefore available to continue the rapid overfeed of SG A.

This overfeed appears to require manual trip of the MFW pumps to avoid further damage. The Babcock & Wilcox "Abnormal Transient Operating Guidelines"[12] instruct the operator to trip the MFW pumps manually on suspicion of MFW overfeed. An alert operator following the existing procedures could therefore terminate this event. Note, however, that the event does develop quite rapidly.

Some of the hybrid computer calculations suggest that with a fully open control valve in the failed section, there would be a low suction pressure trip of the MFW pumps. The outcome of these calculations are critically dependent upon certain possibly unrealistic assumptions about control valve and MFW pump characteristics. The calculations in question introduce at most a borderline uncertainty for some of the cases.

The overfill scenario leads to very substantial water ingress to the steam line. If this water enters the steam line at a high flow rate, it will impart significant momentum to the steam line. Consideration was not limited to obvious high damage but perhaps relatively low probability events such as water hammer. Any significant transfer of momentum from the water to the steam line can produce a swaying or other motion of the steam line, which will stress its supports. If a sufficient number of supports fail, the steam line could deform or collapse with a prusumably high probability of rupture. Such an event occurred at the Beznau (Switzerland) PWR in July 1969.[13] Damage to equipment and line supports was extensive, although line rupture did not occur. Though steam lines differ in geometry, design, and materials, the Beznau event demonstrated that the postulated phenomenon can occur in a steam line with great force and cause great damage. Since steam lines are not qualified for this environment, prudence would suggest that line rupture should be assumed to be highly probable given a massive, continuing water ingress.

Steam line rupture without complications is analyzed in the FSAR, and the consequences are found to be acceptable. The next section will discuss why in the case just examined FSAR calculations do not seem to bound the possibilities of SG tube damage.

3.1.3.2 Possible Steam Generator Tube Rupture. Chapter 15.13 of the Oconee-1 FSAR considers a main steam line break and explores the possibility of resulting SG tube rupture. The mechanism for tube rupture would be increased tensile stress on the SG tubes as a result of severe differential contraction of the SG tubes and their massive shell-support structures in a SG blowdown. In such a situation there is a potential for multiple as well as single-tube rupture. The FSAR conclusion states that no significant expectation of SG tube rupture would result from a main steam line break.

We believe the FSAR conclusions are not applicable to the scenario described in the preceding subsection for the following reasons:

a. The FSAR tube rupture calculations are based on empirical data from experimental conditions less stringent than those proposed here.

b. In the proposed scenario, a maximum inventory of water is in the SG at the time of the line break. This extra water must be disposed of by flashing, causing additional cooling, or by expulsion from the SG by expanding steam, causing additional transverse stresses to the tubes--an effect apparently ignored in the FSAR.

c. The use in the FSAR of mean tube and shell temperatures to characterize thermal effects is not justified. The concern is not for the mean but rather for the tubes subject to extreme stress.

d. The preceding subsection proposes a scenario in which several RC circulatory cycles may have elapsed between the reactor trip and a steam line break. During that period of time the core power and the temperatures of the SG tubes would decrease considerably. The FSAR does not appear to have taken these effects into account.

e. The FSAR takes no account of the vibrational stresses induced in the tubes by blowdown.

f. The stress damage model used in the FSAR assumes the uniform application of stress to a tube whose original wall thickness has been uniformly reduced by 50% when, in fact, one would expect that the stresses (strains) would be concentrated heavily about isolated flaws. The FSAR provides no justification for the assumption that the uniform-thinning, uniform-stress model conservatively bounds the effects of concentrated stresses (strains) at isolated flaws.

The above facts indicate that there is insufficient information available to assess the effect of a steam line break on possible single or multiple SG tube rupture.

3.1.4 Failures Affecting Recovery from Design Basis Accidents

A brief evaluation has been made to assess the potential for control system failure to adversely affect recovery from design basis accidents. The evaluation was based on design information and transient analyses presented in the Oconee Nuclear Station FSAR.[12]

The evaluation demonstrated that continued normal operation of certain control systems was assumed in some of the accident analyses reported in Chapter 15 of the Oconee FSAR. These included post-accident MFW flow control, main steam isolation and pressure controls, and pressurizer spray and/or pilot-operated relief valve (PORV) controls. Failure modes of these control systems adverse to the transient would result in a more severe transient. However, simulation is required to assess the degree of acceptability of the resulting impact on the reactor core or RCS. A summary of potentially adverse control system failures is presented in Table 3.9. The accidents analyzed in FSAR Chapter 15 and the potential impact of control system failures are discussed below.

The Chapter 15 transients fell into three categories: miscellaneous nonreactor accidents, accidents terminated by reactor trip, and accidents exhibiting significant post-trip transient behavior. Accidents assigned to these categories are listed in Appendix Tables A.12, A.13, and A.14.

Waste gas decay tank rupture and fuel handling accidents (Appendix Table A.12) involve the release of radioactivity to the auxiliary building and then to the environment from the auxiliary building vents. Control system mitigation of these transients was not identified in the analyses described in the FSAR.

Six of the accidents listed involve a core reactivity excursion terminated by reactor trip. These accidents are listed in Appendix Table A.13. In each case, the accident is detected by the reactor protective system (RPS), which initiates reactor trip. Once trip occurs, a normal hot shutdown condition will result. Although control system failures could affect the hot shutdown, their impact would not be significantly different had the design basis accident not occurred.

Appendix Table A.14 lists the design basis accidents exhibiting significant post-trip transient behavior. These accidents and the potential impacts of control system failures are discussed below.

3.1.4.1 Loss-of-Coolant Accidents. Loss-of-coolant accidents (LOCAs) involve the uncontrolled release of reactor coolant from the RCS. This class of accident is discussed in FSAR Sects. 15.14, Loss of Coolant Accidents; 15.9, Steam Generator Tube Rupture Accident; 15.12, Rod Ejection Accident; 15.15, Maximum Hypothetical Accident; and 15.16, Post Accident Hydrogen Control.

Following the release of coolant, the core achieves a subcritical condition due to reactor trip, vaporization of the coolant in the core region, and injection of boric acid. Heat transfer from the subcritical core is maintained by pool boiling, with the coolant inventory in the reactor vessel maintained by high-pressure injection, low-pressure injection, and core flood safety systems.

Following large LOCAs, the RCS will depressurize rapidly and the accident will be mitigated solely by safety systems. Small-break LOCAs, however, may require SG heat transfer to aid RCS depressurization. In the Oconee design, following the LOCA-induced reactor trip the ICS regulates the flow of MFW to maintain a level of approximately 2 ft in each SG. This level will be maintained until the reactor coolant pumps (RCPs) are tripped manually following actuation of an engineered safety features actuation system (ESFAS). Upon RCS trip, the ICS modifies the level set point to maintain a 20-ft level in each SG.

Table 3.9. Summary of potentially adverse control system failures

FSAR Accident	Control System Failure	Potential Effect
Loss of Coolant Accident (Small Break/SG Tube Rupture)	o Main feedwater control valves fail to maintain SG level.	o Operator required to manually initiate emergency feedwater. Failure to provide feedwater has an adverse affect on RCS depressurization.
	o Turbine bypass valves fail to open.	o Increased duration of reactor coolant flow through a ruptured steam generator tube.
	o PORV fails to open.	o Increased duration of reactor coolant flow through a ruptured steam generator tube.
Steam Line Break	o Turbine fails to trip.	o Double SG blowdown until manually terminated.
	o Turbine bypass valves fail open or fail to close.	o Double SG blowdown until manually terminated.
	o Main feedwater control valves fail to close.	o More severe RCS cooldown and depressurization.
Loss of Coolant Flow	o Main feedwater control valves fail to maintain SG level.	o Operator required to manually initiate emergency feedwater. Failure to maintain adequate level adversely impacts natural circulation.
Loss of All AC Power	o Turbine bypass valves fail open or fail to close.	o Pressurizer may drain possibly impacting natural circulation.

Two ICS/MFW control valve failure modes may affect the mitigation of the small break LOCA: failure to initially maintain the 2-ft SG levels, and failure to transfer to the EFW nozzles and maintain 20-ft levels after the RC pumps are tripped. Manual initiation of EFW, a safety system, would ensure that SG levels are maintained.

The effects of the identified ICS failures, although adverse, are not expected to be large compared with the effects of other (additional) assumptions mandated for the LOCA evaluation model. Failure of a high-pressure injection train and conservative increases in core decay heat generation rates (currently being modified) would have greater impact.

The "Maximum Hypothetical Accident" and "Post-Accident Hydrogen Control" sections of the FSAR address post-LOCA containment conditions and do not involve control system interactions with the events described.

The rod ejection accident is failure of a control rod drive pressure boundary, which results in a control rod being rapidly removed from the core, increasing reactivity and creating a small-break LOCA. The core reactivity transient is terminated by reactor trip. Once the core is subcritical, the transient is similar to a small-break LOCA as discussed above.

The steam generator tube rupture accident is a small-break LOCA that results in release of reactor coolant to the environment via the SGs and main steam safety valves and/or main condenser. Mitigation of the tube rupture accident involves a manually initiated rapid cooldown and depressurization of the RCS to minimize the flow of reactor coolant from the RCS through the ruptured SG tube.

Cooldown and depressurization of the RCS requires the operation of control systems. The primary supply of FW to the SGs is provided by the MFW system. FW can be supplied by the EFW (safety) system through automatic actuation in most cases and manual actuation in all cases.

Isolation of the affected SG and regulation of main steam pressure requires turbine trip and control of the turbine bypass valves. Turbine trip is initiated by auxiliary relays and contacts located in the control rod drive control system (CRDCS). Although the turbine trip relays and contacts are redundant (a single failed relay or contact will not initiate or prevent a turbine trip signal), it is not known whether they are designed and tested as a safety system. Unless tested regularly, one or more of these devices may be in a failed state without detection following successful turbine trips.

Cooldown of the RCS requires the use of the nonsafety turbine bypass valves and the condenser and associated condenser support systems (principally the condenser circulating water system). Although steam may be released to the atmosphere via the manual steam dump valves, the use of these valves is expected to delay the cooldown significantly.

The required depressurization of the RCS following a tube rupture can be accomplished using the pressurizer spray valve (if the RC pumps are not tripped) or the pressurizer PORV. In the Oconee design, opening the PORV or the spray valve is considered a nonsafety function.

In summary, the normal operation of several control systems has been assumed in the mitigation of small LOCAs. Although failure of one or more of these control systems is not expected to have a significant effect on core integrity, it could affect the probability and extent of a consequent offsite radionuclide release following SG tube rupture. Quantification of such releases is beyond the scope of the simulation used in this study.

3.1.4.2 Steam Line Break Accident. The steam line break accident involves a postulated failure of a steam line that results in very rapid cooldown of the RCS. Of stated concern in the FSAR were the potentials for core criticality to impede continued core cooling and for a SG tube rupture to be caused by the steam line break.

Mitigation of the steam line break requires a reactor trip, a turbine trip to isolate one of the two SGs from the break, isolation of FW to the depressurized SG, and controlled injection of FW to the pressurized SG. The analyses of steam line breaks presented in the FSAR cover three postulated operating modes of the ICS and plant operator control of the MFW:

1. The ICS initially throttles MFW flow, and the operator prevents the ICS from automatically reopening the control valves.

2. The ICS initially throttles MFW, but the operator allows the ICS to reopen the control valves in order to maintain minimum SG level.

3. The ICS and the operator fail to throttle FW flow.

In all three cases considered, automatic turbine trip and proper ICS control of the TBV are assumed. Assumptions concerning EFW operation were not clearly specified. (Significant SG depressurization is expected to result in an automatic trip of the MFW pumps and automatic initiation of EFW. Main feedwater flow to the depressurized SG could continue due to the continued operation of the condensate and condensate booster pumps.)

Analysis results in the FSAR show that the core could return to 35% of rated power for case 2 (the worst case), and unacceptable fuel damage was not reported. Although adverse failure of control systems assumed to operate manually in these analyses could increase the severity of the reactivity insertion through RCS cooldown, the impact on core response would be mitigated by increased boric acid injection. Furthermore, each of the core responses presented assume the highest reactivity control rod failed to insert--a very conservative assumption.

Reactor building pressure responses to a steam line break as presented in the FSAR indicate that the building design pressure is not exceeded in any of the FW control failures considered. Additional adverse control system failures were not identified.

An analysis of the effect of the break on the SG tubes was presented in the FSAR. It is not clear that the analysis assumptions bound the worst-case RCS cooldown, since adverse control system failures could increase the potential for consequential damage of the SG tubes following a steam line break.

Although consequential tube rupture was not predicted, the FSAR presents the results of an analysis of the environmental consequences of 1, 3, and 10 SG tube ruptures coincident with a steam line break. The results were found to be acceptable. (The details of this analysis have been presented in cited FSAR references which have not been reviewed.)

3.1.4.3 Loss of Coolant Flow Accidents. Loss of coolant flow transients involve a reduction in the coolant flow rate through the core, resulting in inadequate heat transfer for the existing power level. These accidents are mitigated by reactor trip followed by control actions required to maintain post-trip core flow.

Loss of flow accidents such as a trip of less than four RC pumps, reduction in grid frequency, or a "locked rotor" are mitigated by reactor trip with otherwise normal post-trip conditions. Trip of four RC pumps requires that the ICS transfer the SG level to a 20-ft set point (assuming the MFW pumps are operating). This increased level is required to establish and maintain natural (convective) circulation of the reactor coolant.

Failure of the ICS to maintain the increased SG levels would require manual initiation of EFW.

3.1.4.4 Loss of Electrical Power Accidents. Two cases of loss of electric power are addressed in Chapter 15 of the FSAR, and additional results of loss of electric power analyses are addressed in Chapter 10.

One case addressed in Chapter 15 was separation of the unit generator from the grid with a successful turbine runback. Although this transient requires significant control system response, its categorization as an accident is questionable. The conditions in the RCS did not require reactor or turbine trip, and the case represents a limiting operational transient with plant power being supplied from the unit generator.

Failure of control systems during this transient could result in a reactor and turbine trip and could deenergize the ac electric power buses. This transient is mitigated by automatic reactor trip and automatic initiation of the EFW and emergency ac power systems. This transient was discussed briefly in Chapter 10 of the FSAR.

The limiting case of loss of ac power addressed in Chapter 15 consisted of separation from the grid, reactor and turbine trip, and a postulated failure of emergency ac power sources. This transient, as above, is mitigated by reactor trip and the EFW system.

The transients involving loss of MFW induced by ac power failure discussed above can be affected by failures in the turbine bypass and the letdown system. Following either transient, the steam line pressure is initially maintained by the ICS-controlled turbine bypass valves (TBV). If these valves fail to open, the pressure control function is provided by the main steam safety valves.

For the loss of power case with successful start of emergency ac power sources, failure of the TBV to properly close or to open results in an RCS cooldown transient. Depressurization to 1500 psi will result in automatic high-pressure safety injection. The open TBV can be isolated by the operator. (It should be noted that loss of coolant water to the condensers results in the TBV being interlocked closed. This is a control system action used to prevent overpressurizing the condensers.)

The case of limiting loss of all ac power results in establishing natural circulation in the RCS by automatically initiating and controlling EFW. As above, failure of the TBV in an open position will result in an RCS cooldown transient. For this case, the TBV isolation valves cannot be closed from the control room due to loss of ac power. However, the loss of power deenergizes the instrument air compressors, resulting in the TBV closing.

The normal makeup flow to the RCS will stop; however, letdown will continue initially. Letdown can be isolated manually or automatically by the loss of instrument air pressure or containment isolation signals if the RCS depressurizes to 1500 psi.

The possible initial RCS cooldown and/or loss of reactor coolant via the letdown line may result in the pressurizer draining. The effect of the pressurizer draining on natural circulation could be adverse but would be countered by the initiation of HPI.

3.2 ESTIMATED FREQUENCY OF SELECTED FAILURE SEQUENCES

In Sect. 3.1, several control system failures were identified that could cause or contribute to the following failure modes: SG overfill, RCS overcooling, inadequate core cooling, or recovery from design basis accident. Of these, those failures resulting in rapid SG overfill or total loss of SG cooling have been selected as failures with potentially high safety consequences. To evaluate the potential significance of these failures and failure sequences, their frequencies of occurrence at the three Oconee nuclear plants have been estimated.

3.2.1 Estimated Frequency of Steam Generator Overfill

The potential for overfilling a SG with FW has been identified as a transient of concern for the Oconee Nuclear Station. The estimated frequency of this transient has been estimated to be between 0.006 and 0.001 overfill transients per year. The methodology for this calculation is discussed in this section.

The sequences of events leading to SG overfill are depicted in event tree format in Fig. 3.1. Although not depicted in the figure, the significance of the SG overfill transient is expected to be the potential for contributing to subsequent failure of the steam lines and SG tubes. Other possible effects include consequential damage to the high-pressure main turbine and damage to the MFW or EFW pump turbine drivers. However, given SG overfill, the conditional probability of these cannot be estimated without significant analyses of the physical response of the steam lines and their supports to SG overfill. The conditional probabilities of subsequent damage would be required to evaluate the frequency of ultimate plant damage.

SG overfill is defined for purposes of this calculation as an uncontrolled addition of MFW to either SG, resulting in the addition of liquid to the steam lines. In the Oconee design, SG overfill resulting from failures in the MFW system requires a failure in the MFW control valves or instrumentation that results in overfeeding one of the two SGs (MFW overfeed), a concurrent failure of the MFW pump to trip on high SG ("operate range") level, and failure of the operator to detect and manually trip the MFW pumps or isolate the FW line. These three contributors to SG overfill are shown in fault tree format in Fig. 3.2.

3.2.1.1 Frequency of Main Feedwater Overfeed. The occurrence of MFW overfeed has been identified in Fig. 3.2 as a necessary condition for SG overfill. The component failure combinations leading to MFW overfeed are identified in Fig. 3.3. As shown, MFW overfeed may be caused by either startup (SU) feedwater flow path valve or either MFW flow path failing open. In either case it has been assumed that one of the control valves will fail to close following a reactor trip or fail open, resulting in a reactor trip, and that the block valves in each flow path are not closed. This condition results in the supply of FW exceeding demand and an increasing SG level.

Failure rates are calculated on the basis of a single SG overfeed. Although overfeeding both SGs is possible, the frequency is lower and the conditional probability is higher that the SG high level instrumentation will successfully trip the pumps.

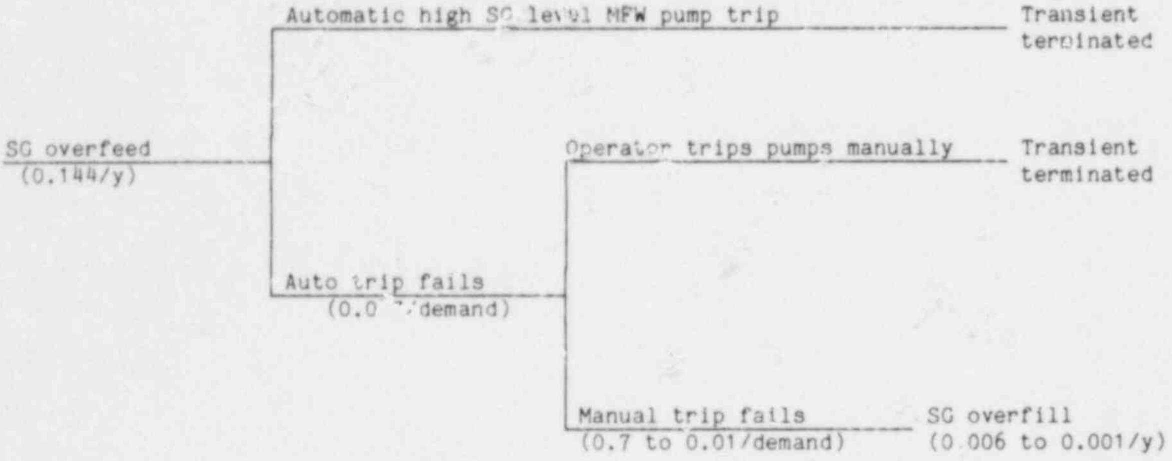


Fig. 3.1. Event tree of Oconee steam generator overfill sequences.

The probability that a 6-in. SU valve will fail in an open position and potentially result in SG overfeed must include consideration of the operator isolating the affected flow path. As shown in Fig. 3.3, given a failed open startup valve, the operator could terminate the flow to the affected SG by closing either of the two motor-operated isolation valves on the affected startup valve. Available information on operating experience indicates that operators will intervene manually to control MFW flow rate prior to reaching the high SG level MFW pump trip set point. Since 10 min or more (depending on the core residual heat generation rate) is available prior to reaching MFW pump trip, a probability of failure to isolate of 0.01 per demand has been assigned to this operator action based on the methodology described in Sect. 3.2.1.3. It should be noted that this operator action is separate from a manual trip of the MFW pumps.

As shown in Fig. 3.3, the failures resulting in a SU valve failing open and affecting the pump trip circuit are separated from other failures affecting only the valve position. The SU valve is controlled by the "operate range" level transmitters following a trip of the four RC pumps. Although an RC pump trip initiator, of itself, is expected to occur very infrequently without a loss of the external grid (which would result in trip of the feedwater pumps), the operator is required to trip the RC pumps manually following an ESFAS trip. Thus, failure of a SU valve resulting from a pre-existing operate range level transmitter failure is calculated based on the ESFAS trip frequency (3 trips per 18 reactor years[14]) and transmitter/ multiplier module failure rates. This yields a SU valve failure frequency of 0.004/y for this failure mode. However, since this failure also disables the automatic pump trip circuit, its contribution to SG overfeed is greater than that of other startup valve failure initiators.

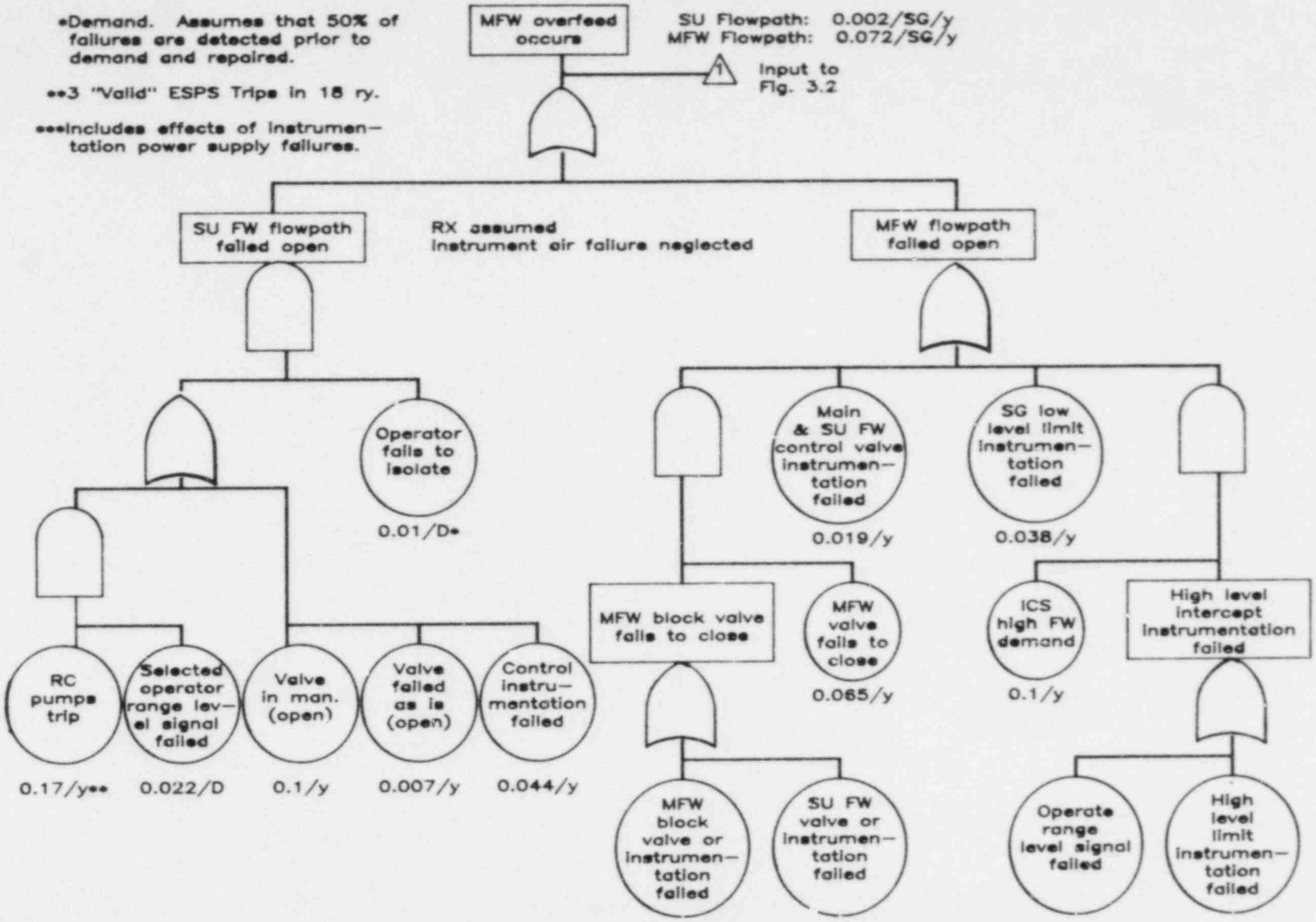
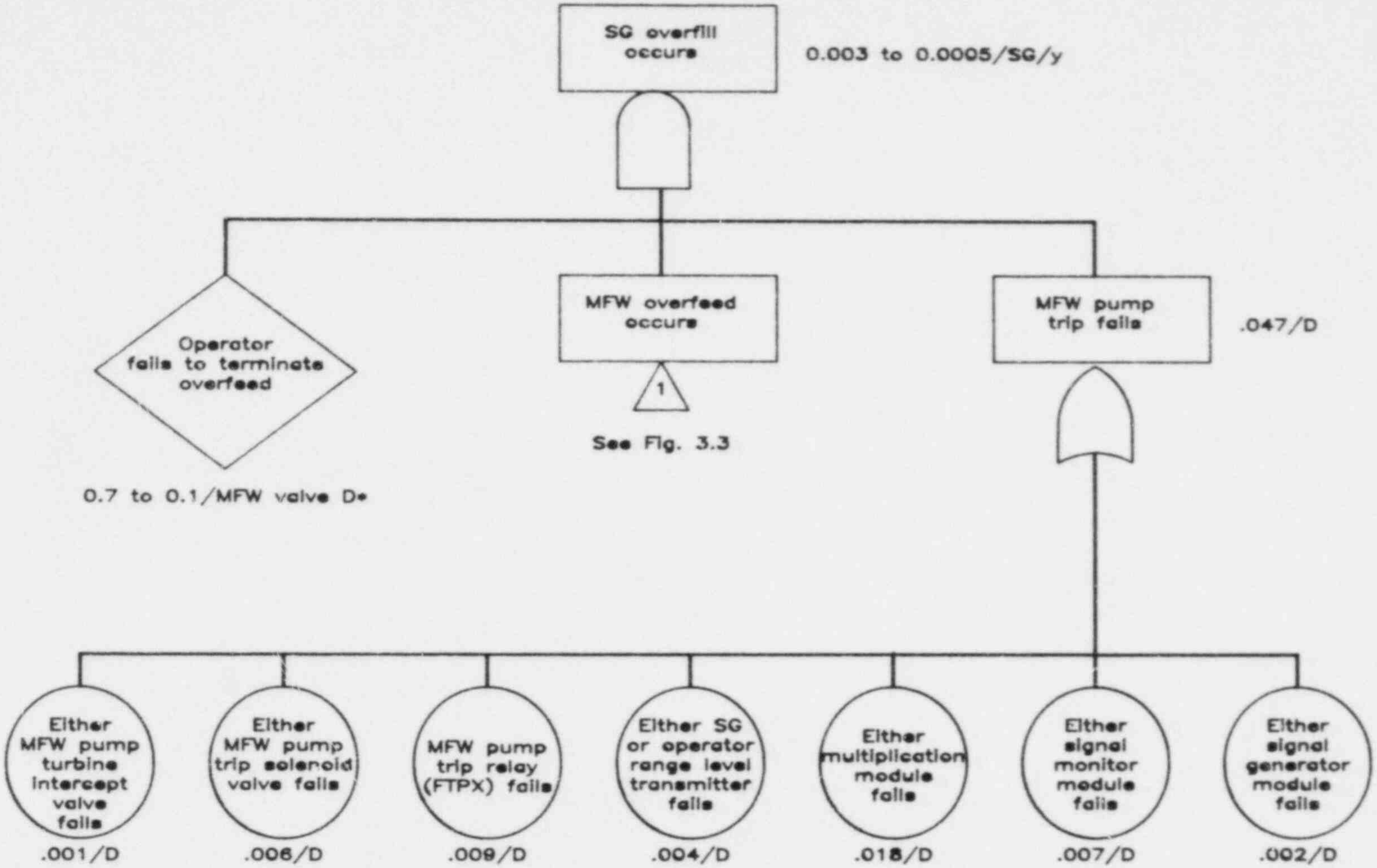

*Demand. Assumes that 50% of failures are detected prior to demand and repaired.
**3 "Valid" ESPS Trips in 18 ry.
***Includes effects of instrumentation power supply failures.
MFW overfeed occurs
SU Flowpath: 0.002/SG/y
MFW Flowpath: 0.072/SG/y
1
Input to Fig. 3.2
SU FW flowpath failed open
RX assumed
Instrument air failure neglected
MFW flowpath failed open
Operator fails to isolate
0.01/D*
RC pumps trip
0.17/y**
Selected operator range level signal failed
0.022/D
Valve in man. (open)
0.1/y
Valve failed as is (open)
0.007/y
Control instrumentation failed
0.044/y
Main & SU FW control valve instrumentation failed
0.019/y
SG low level limit instrumentation failed
0.038/y
MFW block valve fails to close
MFW valve fails to close
0.065/y
ICS high FW demand
0.1/y
High level intercept instrumentation failed
MFW block valve or instrumentation failed
SU FW valve or instrumentation failed
Operate range level signal failed
High level limit instrumentation failed

Fig. 3.2. Steam generator overfill fault tree.


SG overfill occurs
0.003 to 0.0005/SG/y
Operator fails to terminate overfeed
0.7 to 0.1/MFW valve D*
MFW overfeed occurs
1
See Fig. 3.3
MFW pump trip fails
.047/D
Either MFW pump turbine intercept valve fails
.001/D
Either MFW pump trip solenoid valve fails
.006/D
MFW pump trip relay (FTPX) fails
.009/D
Either SG or operator range level transmitter fails
.004/D
Either multiplication module fails
.018/D
Either signal monitor module fails
.007/D
Either signal generator module fails
.002/D

*Demand. Assumes that 50% of failures are detected and repaired prior to demand.

Fig. 3.3. MFW overfeed fault tree.

Other failures resulting in SU valve failure include control instrumentation module failures, failure of the valve, and transfer of the valve to manual control. Module failure rates were based on the number of operational amplifiers per module and the IEEE-500[15] operational amplifier failure rate. The operational amplifier count was based on 820 Series modules which, except for power supply, are believed to be similar in configuration to the Oconee 721 Series modules. This methodology produced reasonable estimates when compared to available observed ICS component failure data. The module count for an 820 Series ICS and the calculated module failure rates are shown in Table 3.10. The sum of these failure rates is 1.64 module failures/ICS/y. B&W topical report BAW-1564[16] lists 30 module failures per 19 calendar reactor years, which corroborates the estimate well.

The failure rate of the SU valve itself was based on historical nuclear plant pneumatic valve experience[17] and Oconee reactor trip frequency. The estimated frequency of the SU valve being placed in manual control (0.1/y) is based on engineering judgment and specifically considers the fact that transfer of the startup valve to manual cannot affect reactor performance until the reactor is tripped or shut down. A combined frequency of 0.15 SU valve failures per year was estimated for these failure modes.

As noted above, startup valve failure is considered an overfeed only if the high level trip circuit is challenged. The startup valve-induced overfeed rate is calculated as the product of the startup valve failure rate and the conditional probability that the operator will fail to isolate prior to high level trip challenge. This yields a frequency of 0.002 startup valve-induced overfeeds per year.

SG overfeeds due to failure open of the MFW flow path occur rapidly, in contrast to those induced by the SU valve. Since MFW valve overfeeds will challenge the high level trip in approximately 1 or 2 min, manual isolation prior to challenging the automatic high level pump trip has been ignored. However, a MFW block valve in the MFW flow path will be closed automatically once the SU control valve is 50% closed. It has been assumed that automatic closure of the block valve would prevent SG overfill, regardless of whether the MFW pumps are tripped.

As shown in Fig. 3.3, MFW overfeed can occur due to (1) independent failures of the MFW control valve and the MFW block valve to close, (2) instrument failures affecting both the MFW and SU control valves, and (3) failures affecting the MFW flow path and the MFW pump trip circuit. Failure of the block valve to close may occur due to failures of the valve itself or its control circuitry, or failure of the startup valve to close. Since these failures are of importance only following a MFW control valve failure, their failure probability has been reduced by half to account for an assumed yearly test interval. The frequency of the MFW control valve failing open or failing to close was based on failures only affecting MFW control valve position. Such failures include MFW valve failure, manually placing the MFW valve in manual, and ICS control circuit failures not affecting SU valve position.

Table 3.10. Calculated module type failure rates in 820 series ICS

Module Type	Module Failure Rate (Failures/ Module/Year)[1]	Number of Modules/Type in ICS	Calculated Failures/Module Type/Year[1]
Analog Memory	.002	14	.032
Summer	.003	53	.180
Signal Generator	.002	17	.038
Summer and Integral	.005	17	.077
Signal Limiter	.009	6	.054
Signal Log	.002	6	.014
Signal Monitor	.007	13	.088
Tri-stable	.007	16	.108
Function Generator	.016	19	.301
Aucticneer	.007	6	.041
Multiplier	.018	4	.072
Miscellaneous	.004	8	0.036
TOTAL		179	1.041

[1] Based on 2.26 x 10^{-3} Failures/Operational Amplifier/Year (IEEE-500).

A number of ICS module failures affect both the MFW and SU control valves. These module failures include portions of the ICS MFW demand circuit downstream of the maximum SG level circuit and the minimum SG level circuit.

The ICS control circuit failure probabilities were based on the module failure rates of Table 3.10 and IEEE-500,[15] and the valve failure probabilities were based on the data of NUREG/CR-3154.[17] The probability of the MFW and SU control valves being placed in manual control has been estimated to be 0.01 and 0.1/y respectively. These estimates were based on engineering judgment. One ICS power supply failure was found to contribute to failure of the minimum SG level circuit, selected branch circuit HEX or HEY. The failure rate of the branch circuit was estimated to be 0.009/y based on the failure of one of five ICS power supply branch circuits on a 23-ry experience base.[18]

The last main control valve failure mode considered affects the FW pump trip circuit in addition to the control valve. The ICS FW flow control circuits are designed to be limited (intercepted) by the maximum SG level signal based on operate range SG level transmitters. If the selected operate range level signal is failed when any of a number of ICS modules fail, thereby producing a high FW demand signal, an overfill transient not terminated by the automatic pump trip will occur. The frequency of the high level circuit failure has been separated into the failures that affect the pump trip and the balance of the module failures that do not. (These failures contribute to MFW overfeed but not to combined overfeed/pump trip failure). The ICS module failures (upstream of the high level auctioneer module) that could cause high FW demand are numerous, and no attempt has been made to individually quantify the individual module failure combinations. Based on engineering juċgment, these failures have been estimated to occur with a frequency of approximately 0.1/y, which is not inconsistent with ICS operating experience. Combining these failure probabilities yields 0.002 failures/SG/y that affect both the MFW flow path and high level pump trip circuit, and 0.07 failures/SG/y that affect only the MFW flow path.

The calculated frequency of significant overfeed transients for Oconee was 0.072 overfeeds/SG/y, which appears to be in excellent agreement with Oconee operations data. The Duke PTS evaluation report[19] describes 16 overcooling transients that occurred at the three Oconee units over a 23-ry span. Of these, five were found to be significant overfeed transients of the type of interest in this program (Events 5, 6, 7, 14, and 15). Two additional transients were considered marginal and were not selected (Events 11 and 13). None of these events could be identified as a startup valve-induced overfeed. From these data, a mean frequency of 0.22 overfeeds/ry or 0.11 overfeeds/SG/ry can be estimated assuming single SG overfeeds in the five events. The 5 to 95% chi-squared limits are 0.01 to 0.2 overfeeds/SG/ry.

In their PTS report, Duke Power Company estimated overfeed frequency (including overfeed initiators and failure to runback) at 0.29/ry or 0.15/SG/ry, again assuming single SG overfeeds.

It should be noted that the estimates, while valid for Oconee, may not apply to the general population of PWRs, as the generic PWR experience is not necessarily applicable to the unique Oconee design. However, in NUREG/CR-2789,[20] the "corrected" overfeed/cold FW transient was estimated to occur with a frequency of 0.161 events/ry for the general population of PWRs.

3.2.1.2 Automatic High Level Feedwater Pump Trip Failure. In the Oconee design, an indicated high SG level detected by both "operate range" level transmitters on either SG will initiate a trip of both MFW pumps. The pump trip circuitry modeled in the fault tree (Fig. 3.1) has been obtained from available Bailey Meter Co. ICS circuit diagrams[21] and Oconee circuit diagrams.[22] The circuitry for each steam generator consists of two level (ΔP) transmitters, each generating a signal proportional to the pressure difference between the SG operate range level taps. These two voltage signals are inverted in "function generator" modules and corrected for the SG downcomer temperature in "multiplication" modules, which generate temperature-corrected signals for transmission to "signal monitor" modules. Each signal monitor closes one set of contacts that activates an alarm and another set that forms part of the FW pump-trip logic on indicated high level. The four pump-trip contacts associated with the two SGs are arranged in a parallel series array to energize a pump-trip relay upon closure of both trip contacts associated with either SG. The trip relay activates trip contacts for each MFW pump to open a solenoid valve and initiate pump trip.

Assuming that an overfeed occurs and results in a high level in one of the two SGs, the conditional probability that the pump-trip circuitry will fail to initiate a pump trip has been estimated. As shown on Fig. 3.2, the pump-trip failure occurs if either of the two transmitters, function generator modules, multiplication modules, signal monitor modules, the pump-trip relay, or the pump-trip solenoid valves fail. In addition, the trip will fail if the mechanical equipment associated with either pump turbine inlet intercept valve fails to respond to the depressurized hydraulic reservoir.

Transmitter and solenoid valve failure rates were estimated based on IEEE-500 data. The module failure rates used are listed in Table 3.10. The failure rates of the trip circuit components have been reduced by 50% to account for failure detection and repairs prior to an overfeed transient. (The failure of the pump-trip circuit is of concern only if the circuit is failed when the overfeed transient occurs. Basing the conditional probability of failure on an assumed demand at one-half the yearly test interval produces reasonable estimates.) In addition to the failure probabilities listed for the trip circuitry, a failure probability of 0.001/demand has been included to account for failure of each of the intercept values for the MFW pump turbines.

Based on the model shown in Fig. 3.2 and described above, an estimate of 0.047 pump-trip circuit failures per demand has been obtained.

Oconee experience indicates that the trip circuit has been challenged six times without failing and has been tested, also without known failures. According to verbal information, the circuits on the three Oconee units have been tested yearly since 1974 without failure, thus an additional 30 challenges have occurred. Using the 50% chi-squared bound to estimate the mean failure rate would yield 0.02 failures per demand. The use of this estimating technique implies that if the actual failure rate were constant and equal to 0.02, there would be an equally likely chance of having zero failures or 1 or more failures in the 36 demands. The circuit failure rate calculated from estimated component failure rates, 0.047 failures per demand, is a factor of 2 higher than the "chi-squared" estimate.

Duke Power Company, in their PTS report, estimated the failure rate of the trip circuit to be 0.005/demand. Although this value is consistent with zero observed failures in 36 demands, it is lower than would be expected with the known ICS module failures. The 30 module failures in 19 ry and an assumed 179 modules/ICS yields an "average" module failure rate of 8.8×10^{-3} failures/module/y. With six ICS type modules/trip circuit and yearly testing, the module contribution to trip circuit failure would be 0.026/demand, which itself is higher than the Duke Power estimate of 0.005. (The module failure contribution, using the more detailed module failure rate estimates shown in Table 3.10, was 0.027/demand.)

Based on the above, the calculated trip circuit failure rate of 0.047/demand is considered reasonable, although it may be somewhat conservative compared with the test results.

3.2.1.3 Manual Feedwater Pump Trip Failure. Following an assumed overfeed and failure of the automatic trip circuit, the operator is expected to trip the MFW pumps manually or isolate FW.

Estimating the reliability of control room operators, especially in brief time frames, is uncertain. Some assessments suggest a "general error rate [of 0.2 to 0.3/demand] given very high stress levels (but not extremely high levels) where dangerous activities are occurring rapidly."[23,24] In the Oconee PRA,[25] Duke Power Company assumed that operator failures had a probability of 1.0 in the 0- to 1-min time frame. The probability of the operator failing to trip the FW pumps manually following an overfeed transient was estimated to be 0.05/demand in the Oconee PTS evaluation. For purposes of this analysis, a correlation relating the failure rate of a team of operators as a function of available time has been used.[25]

According to the calculations presented in the Duke PTS report, the SG MFW pump-trip level will be reached 36 s after a reactor trip from full power if one of the MFW control valves fail to close. If the high level trip fails, the steam generator will completely fill ("SG water solid") in an additional 79 s. These calculations provide a minimum time for operator action. Additional time is expected for operator action following less severe overfeed transients.

One of the transients listed in the Duke PTS report, Event 5, gave a time of 220 s to reach the SG high level pump trip. Extrapolating this time to an overfill condition based on the above calculation suggests that an additional 8 min would be required to fill the SG. This datum indicates that overfeed transients (failure to runback) do occur at rates considerably less than calculated maximum rates. The time to trip the FW pumps for the other listed transients was not given.

The Event 14 overfeed transient description also indicates two additional factors concerning operator response to overfeed transients. First, the overfeed transient was recognized prior to automatic MFW pump trip, and second, the operator attempted to throttle MFW flow until the automatic trip occurred. For the other listed overfeed transients, specific operator recognition or attempted throttling was not described. A manual MFW pump trip, however, did not occur for any of the listed transients. From this information, some credit for operator recognition of an overfeed transient prior to reaching the high level trip set point should be given. However, the operators appear to be reluctant to initiate MFW pump trip manually, at least prior to automatic trip failure.

Applying the operator failure/available time correlation to the maximum overfeed rate case yields a probability of approximately 0.7 that operators will fail to terminate the overfeed transient, assuming that the entire two min was available to the operators to perform this function. This value is the approximate midpoint of a range of failure probabilities from 0.3 to 0.95. For the time available in slower overfeed transients as represented by the Event 5 data, the probability of failure to trip the pumps manually on demand drops to approximately 0.1 (in a range of probabilities from 0.6 to 0.02). In both cases, the operators are assumed to be responding in a "cognitive mode" rather than the more reliable "rule-based mode." This assumption was based on the absence of manual MFW pump trips in the Oconee experience base.

The two operator failure probabilities calculated, 0.7 and 0.1, represent a credible range for the failure probability. However, without additional data on the expected time available for the operator to trip the pumps manually, a point estimate cannot be calculated.

3.2.1.4 Summary of Results. The MFW overfeed transient has been estimated to occur with a frequency of 0.072/SG/y (or 0.144/y). In addition, 0.002 transients/SG/y were estimated for those transients affecting both overfeed and the MFW pump trip.

As shown in Fig. 3.1, combining the estimated overfeed frequency with the MFW pump-trip failure frequency and the estimated frequency of the operator failing to trip the FW pumps manually yields a steam generator overfill frequency estimate of 0.005 to 0.001 events/SG/y for rapid SG overfill transients.

3.2.2 Estimated Frequency of RCS Overcooling Events

In addition to SG overfill, other RCS overcooling failures not involving SG overfill have been identified. The two events initially judged to be significant were a failed open PORV and failure to trip the main turbine following reactor trip.

A failed open PORV initially results in a LOCA; thus the initiating failures should be considered in terms of frequency and consequence. However, the FMEAs of the PORV and associated control circuitry did not identify failures leading to an open PORV and simultaneously affecting the systems and components required to mitigate the resulting transient. In particular, the failures that opened the PORV did not affect the ability to close the PORV isolation valve manually, maintain SG cooling, or automatically initiate HPI.

Oconee operating experience indicates that the PORV failed open twice in the 23-ry experience base[18] and resulted in HPI actuation. One of these failures resulted from a loss of instrumentation power. The PORV control design has since been modified to close the valve on loss of power, so this event is no longer applicable. The 0.04 failures/ry (1/23 ry) estimate, however, is conservative due to the substantially reduced number of PORV challenges following implementation of post-TMI design changes. This, in combination with the expected manual closure of the PORV isolation valve, would place the frequency of PORV failure-induced LOCAs well below the NRC's small LOCA screening estimate of 0.01/ry. Consequently, the failures resulting in an open PORV are no longer considered significant.

Failure to trip the turbine following reactor trip could result in a significant cooldown of the RCS similar to a steam line break. This transient was initially selected as significant due to the expected difficulty in testing the turbine trip contacts in the control rod drive control system (CRDCS).

The CRDCS contacts are arranged in a parallel-series configuration. Therefore, periodic tests of the array (as contrasted to tests of individual contacts) would not detect failures until the array is degraded to a completely failed state. The probability of such a failure would depend on the design life of these contacts relative to the 40-y plant life or to a preventative maintenance replacement interval.

However, even if the trip contact array fails, two additional features are expected to terminate the transient. First, the ICS will rapidly throttle the turbine in an attempt to maintain turbine header steam pressure, and second, the plant generator is expected to be separated from the grid. (Separating the generator from the grid would result in an overspeed trip of the turbine unless otherwise tripped or throttled.)

Although insufficient information is available to make an estimate of the frequency of turbine trip failure, the combined failure rate of the

CRDCS contacts, the ICS runback, and the generator separation trip is expected to be very low. The identified turbine trip failure is no longer believed to be significant.

3.2.3 Estimated Frequency of Insufficient Core Cooling Events

Two failure events were identified as potentially significant initiators of insufficient core cooling. Each was an ICS power supply branch circuit failure that could result in a loss of MFW. These initiators are of significance because MFW flow to the SGs can be lost without tripping the MFW pumps or depressurizing the pump discharge piping. Without these parameters, the EFW system in the Oconee design is not initiated automatically, and the operator is required to initiate the system manually. The insufficient core cooling sequences initiated by these branch circuit failures are discussed below.

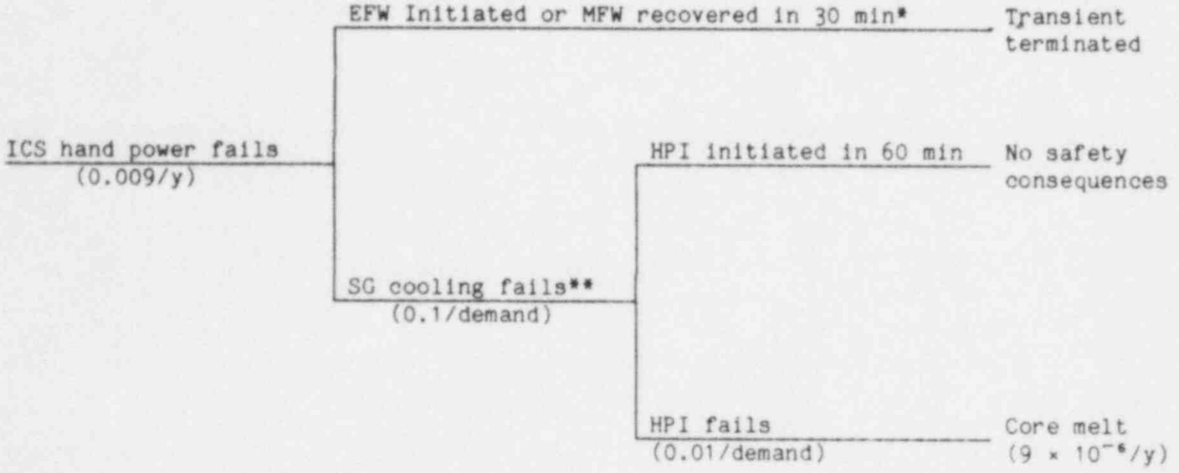
3.2.3.1 Loss of ICS Hand Power. A loss of ICS branch circuits HX or H1X, assuming that panelboard KI remains otherwise energized, will result in the MFW pump being runback to minimum speed and the turbine bypass steam dump valves being closed. The reactor and turbine are expected to trip on high RCS pressure. The sequences of interest following this initiating event are depicted in Fig. 3.4.

Given the initiating power supply failure, SG inventory will begin to be depleted. Due to the continued operation of the MFW pumps, neither the low MFW pump discharge pressure nor the MFW pump-trip EFW initiation signal is expected to start EFW operation. Thus, unless the operator manually initiates EFW or recovers MFW, the SG will boil dry and SG cooling will be lost. With the loss of reactor coolant subcooling margin, the operator is instructed to trip the RC pumps and initiate HPI.

With the loss of SG cooling and tripped RC pumps, core residual heat is expected to generate steam in the RCS which will cause filling of the pressurizer and discharge of liquid through the PORV and/or pressurizer safety valves. The depletion in reactor coolant inventory will affect the ability to restore SG cooling. Information in the Oconee PRA suggests that if the operator restores MFW or initiates EFW within the first 30 min, SG cooling can be restored. Initiating FW after 30 min is ineffective.

Even if SG cooling is lost, the initiation of HPI will provide long-term core cooling (i.e., hours). Based on the Oconee PRA, if the operator initiates HPI within the first 60 min, a stable core cooling condition will be established. If the operator fails to initiate HPI within this time period (assuming SG cooling during the first 30 min), a core melt sequence would be expected.

The frequency of the event sequence leading to core melt depends on the expected frequency of the loss of hand power and the conditional probability that the operator fails to restore SG cooling or initiate HPI. The frequency of a loss of hand power (branch HX or H1X) is



*Minimum MFW pump speed assumed insufficient for continuous FW flow at SG pressure of 1050 psig.
**EFW available: MFW can be recovered with difficulty, by operator action.

Fig. 3.4. Insufficient core cooling event tree: loss of ICS hand power (Branches HX, H1X).

estimated to be 0.009/ry based on one observed event of a loss of one of the five ICS power branch circuits (auto power) in 23 ry. Based on the circuit configuration, a loss of hand power (or another ICS power branch) is expected to be as likely as the loss of auto power (branch H). In the observed loss of auto power event, the power was restored in 30 to 45 s. The potential for recovery of the hand power and MFW is considered in the recovery of SG cooling.

Given the initiating event, the operator is capable of initiating EFW or restoring hand power manually. If hand power is restored, two conditions are possible: MFW may be restored and controlled, or the MFW pumps may trip during the power recovery transient, automatically initiating EFW. Either is considered a success path.

Although the restoration of SG cooling could be straightforward, several factors would tend to make the situation more difficult:

1. The hand power alarm may or may not indicate loss of the power supply. Although a loss of hand power (branch HX) alarm is indicated in the procedure for loss of panelboard KI, an alarm for the subsidiary circuit H1X is not specified.[26]

2. Several spurious alarms will actuate due to the power failure as well as other properly responding alarms.

3. Many RCS temperature indicators and recorders will fail low, midscale, or as is.

4. The procedure for loss of FW[27] as well as the ATOG[12] indicate that EFW will be initiated automatically.

5. Operators are required to perform other actions such as initiating HPI and tripping the RC pumps.

In the Oconee PRA, three probabilities for failing to recover SG cooling were given: 0.5, 0.3 and 0.1. These probabilities correspond to one, two, or three available secondary heat removal paths. Since it is possible to initiate EFW flow to either SG (two paths) or restore hand power (one path), this method suggests a failure probability of 0.1.

In addition to recovering SG cooling, the manual initiation of HPI will result in successful core cooling. As indicated in the Oconee PRA, the operator must initiate HPI within the first 60 min to be effective. (The specific action the operator is instructed to take is aligning the BWST to the HPI Pumps and throttling HPI flow with the pressurizer full.[27]) The Oconee PRA estimates the probability of failing to perform this action to be 0.01.

It should be noted that the estimated failure probabilities given in the Oconee PRA, although listed separately, considered interactions between SG cooling and HPI initiation actions. Thus, it may be more appropriate to consider a probability of 0.001 failures per demand to reestablish SG cooling within 30 min or initiate HPI within 60 min.

Applying the available time/operator failure correlation to the problem yields a comparable estimated failure rate. Operator failure within 30 min would have a probability of 0.01 and within 60 min a probability of 0.001. However, these estimates must be modified to account for coupling between operator action failures and impediments to appropriate operator actions (e.g., spurious low RCS temperature indications, a full pressurizer, etc.). If, as above, a single probability of not performing either required action within 60 min is estimated using the correlation, the 0.001 failure probability is obtained as indicated in the Oconee PRA.

Combining the power supply failure frequency, 0.009/ry, with the 0.001 conditional probability of the operator failing to restore SG cooling or initiate HPI yields a core melt sequence frequency of 9×10^{-6}/ry.

This sequence is considered to be significant. In particular, the fact that a control system failure could defeat automatic initiation of the required mitigating system should be investigated further. It also is noted that the 60-min operator action limit resulted from a procedurally required trip of the RC pumps. If the pumps were not tripped, ORNL calculations indicate that the time available for the operator to take the required actions would be extended significantly. The particular impact of this time extension on the sequence frequency has not been evaluated.

3.2.3.2 Loss of ICS Auto Power. A loss of ICS auto power, branch circuit H or H1, will result in many ICS control stations transferring to manual and the controlled components remaining in position. Failure event sequences that could occur following loss of auto power are depicted in Fig. 3.5.

Although a loss of ICS auto power would not result directly in a transient, automatic responses to perturbations in the plant operating state would be limited. A high probability has been assumed for an eventual reactor trip in response to such perturbations (e.g., a MFW control valve drifting due to air leakage from the valve operator).

Once the reactor trips, the SGs would begin to fill rapidly unless the operator throttled MFW flow by closing the main and startup control valves. These valves would be left closed until the existing high SG inventory boiled off to approximately the 30-in. level. The operator would then control the startup control valves to maintain this level.

As with the loss of ICS hand power, the operator has several alternate actions to control and terminate the transient. However, once the operator successfully throttles MFW, a second operator action will be required to prevent a loss of SG cooling.

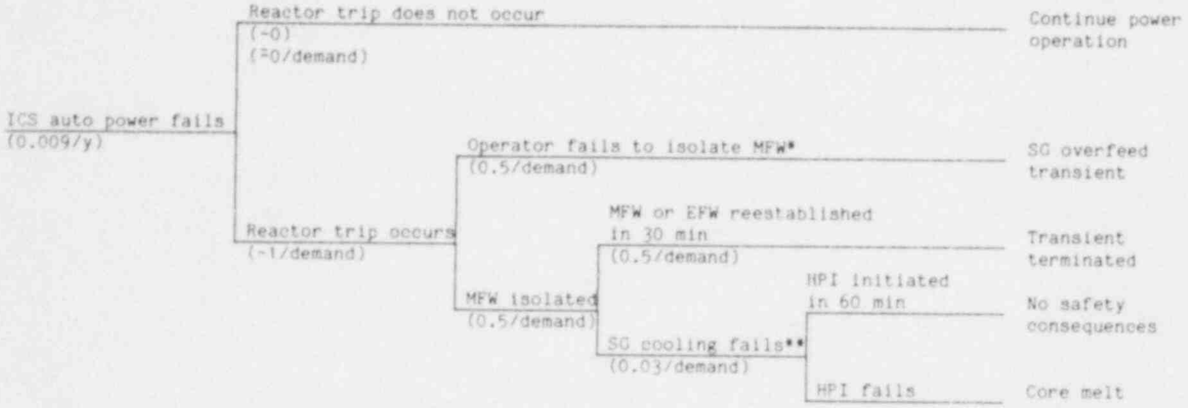
The frequency of the sequence leading to core melt has been estimated. This sequence frequency incorporates the frequency of the initial power supply failure and the conditional probabilities of the operator successfully throttling MFW, failing to reestablish SG cooling, and failing to initiate HPI.

The frequency of loss of ICS auto power is expected to be the same as for ICS hand power, 0.009/ry based on operating experience at Oconee. As indicated in Figure 3.5, the conditional probability that the reactor subsequently trips has been estimated to be 1.0.

Once reactor trip occurs, a rapid SG overfeed transient will begin. As discussed in Sect. 3.2.1, it is considered likely that the operator will attempt to throttle the MFW valve, although it is generally considered unlikely that he will succeed in preventing a SG high level trip challenge. For this particular transient, however, the operator may be alerted prior to the overfeed and may begin throttling prior to reactor trip. A 0.5 probability has been estimated for successfully throttling MFW prior to a MFW pump trip challenge.

Given the MFW isolation, a period of tens of minutes will elapse before MFW flow would be required. This period of time increases the opportun.ty for the operators to become occupied with other crises and to fail to reestablish SG cooling. With the MFW isolated, a plant condition similar to the condition following a loss of ICS hand power will occur. However, two factors are expected to increase the likelihood of successful recovery:

1. Manual MFW controls are available to the operator without recovering from the power supply failure.



*Closure of main and bypass FW control valves.
**MFW and EFW available by operator action.

Fig. 3.5. Insufficient core cooling event tree: loss of ICS auto power (Branches H, H1).

2. The operator has successfully used these controls to throttle MFW and is thus alerted to the subsequent requirement to reestablish flow.

For these reasons, a credit factor of three has been applied to the Oconee PRA 0.1 failure probability estimate. This yields a probability of 0.03 failures to reestablish SG cooling per demand.

The Oconee PRA estimate of 0.01 failures to initiate HPI given loss of SG cooling has been used. As indicated previously, failure to initiate HPI and failure to reestablish SG cooling are linked actions. The combined probability of 0.0003 failures to establish SG cooling or HPI is considered reasonable for the loss of ICS auto power sequence.

Combining the initiating failure frequency with probabilities of the other failure events in the sequence yields a sequence frequency of 1×10^{-6} for the loss of ICS auto power core melt sequence. Although this frequency is lower than that estimated for loss of ICS hand power, loss of ICS auto power remains a potentially significant transient.

4. AUGUMENTED FAILURE MODE AND EFFECTS ANALYSIS

4.1 HYBRID SIMULATION

The ORNL study of the safety-related aspects of control systems consists of two interrelated tasks: (1) a failure mode and effects analysis (FMEA) that, in part, identifies single- and multiple-component failures that may lead to significant plant upsets; and (2) a hybrid computer model that uses these failures as initial conditions and traces the dynamic impact on the control system and the remainder of the plant. The second task is treated in this section.

The initial step in model development was to define a suitable interface between the FMEA and computer simulation tasks. This involved identifying primary plant components that must be simulated in dynamic detail and secondary components that can be treated adequately by the FMEA alone. The FMEA in general explores broader spectra of initiating events that may collapse into a reduced number of computer runs. A separate task within the FMEA process included consideration of power supply failures. Consequences of the transients may feed back on the initiating causes, and there may be an interactive relationship between the FMEA and the computer simulation.

Since the thrust of this program is to investigate control system behavior, the controls are modeled in detail to accurately reproduce characteristic response under normal and off-normal conditions. The balance of the model, including neutronics, thermohydraulics, and component submodels, is developed in sufficient detail to provide a suitable support for the control system. The overall approach predominantly uses the existing state-of-the-art procedures available in production codes or in the literature. At the expense of generality, attempts were made to simplify and streamline programming, tailor it to a specific plant, and improve computational speed and maneuverability as compared with large production codes.

4.2 HYBRID MODEL OF OCONEE-1 PLANT

From a modeling point of view, all PWRs have many common elements. An obvious example is the reactor; with minor changes in parameters, a single structured simulation may be used for plants designed by B&W, Westinghouse, and Combustion Engineering. Other features such as pressurizer controls and high-pressure injection (HPI) systems may differ in detail but have the same generic features for modeling. The B&W (Oconee-1) model was developed as the prototype for a generic PWR system, and it incorporates modules that are broadly representative of the nuclear industry, thus minimizing the revisions needed should it become desirable to extend the model to accommodate other specific designs. Its principal components are shown in Fig. 4.1.

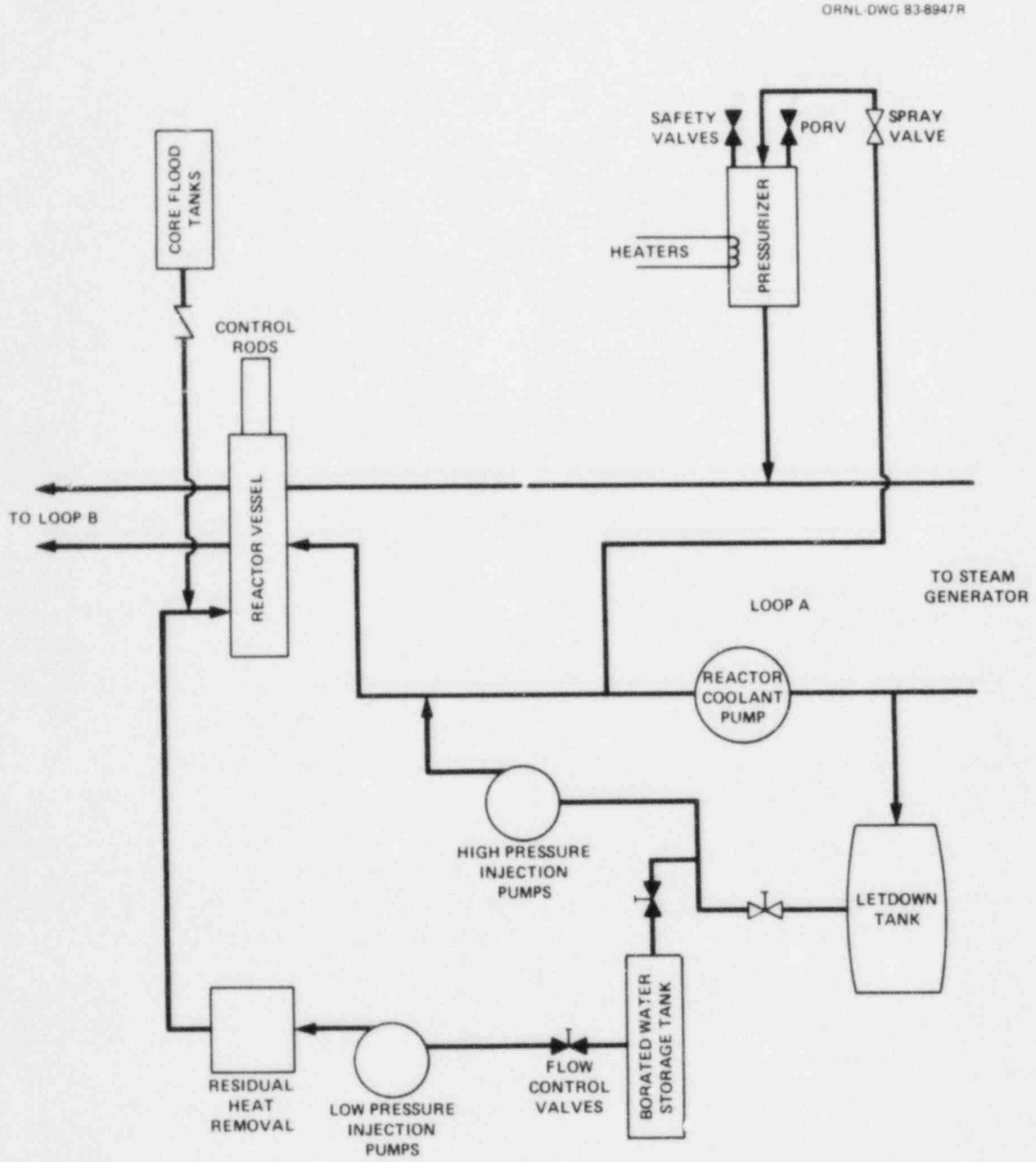


Fig. 4.1. ORNL hybrid computer model of Oconee Unit 1: (a) primary systems.

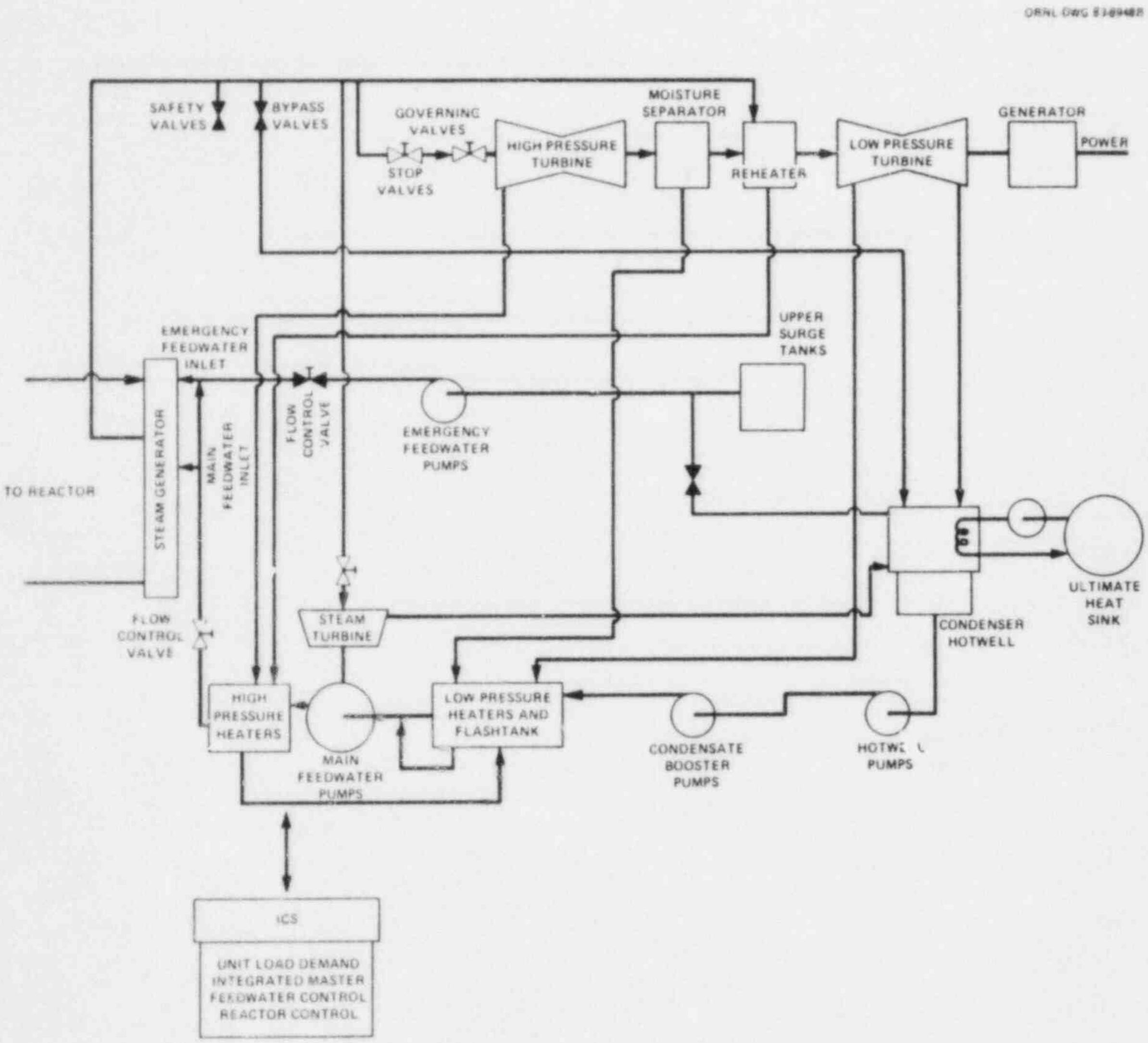


Fig. 4.1. ORNL hybrid computer model of Oconee Unit 1: (b) secondary systems.

The range of problems to be considered is extremely broad. For example, some specific control-related safety issues that have occurred in the past are as follows:

- steam generator and/or reactor overfill,
- reactor overcooling transients,
- misvalving that leads to direct loss of coolant,
- turbine trip-induced pressure surges,
- administratively mandated shutdown upon loss of one or more auxiliary power channels, creating immediate dependence upon the remaining auxiliary channels,
- misvalving that turns off oil to turbine bearings, with consequent loss of coolant pumps,
- switching errors that can discharge batteries and overload charges,
- startup procedures that may lead to short-period transients, and
- operating limits run outside technical specifications because of control sensor errors, and short circuiting of circuit components, leading to control system power supply failures.

The ORNL development approach was to model first the projected scenarios of greatest concern, and to allow sufficient flexibility in the simulation framework to expand into other areas with a minimum of retrofitting. A principal purpose of this study was to discover undesirable control actions that may arise from unanticipated interactions among system components. While model simplicity is desirable in many respects, particularly for grasping major characteristics, the dynamic detail needs to be sufficient to encompass the more complex and subtle interactions that can occur in a real plant.

Extensive modeling of nuclear components, some of which was done at ORNL, has been accomplished in the past and described in the literature. A literature search was made of the state-of-the-art modeling for each component. Although much of this was immediately applicable, some modifications and new model development were required.

Details of the model will be given in a separate topical report.[28] An overview is presented here.

4.2.1 Core

4.2.1.1 Neutronics. The treatment of core neutronics has available the following possible levels of detail.

1. Zero-order kinetics, the simplest level, is useful in afterheat and comparable fixed- or zero-flux studies.

2. Point kinetics, the next level of complexity, is useful in fixed flux-shape cases. Three to six neutron groups are appropriate.

3. One-dimensional (1-D) flux distribution is useful when axial spatial neutronics is important, such as when treating details of the interaction among rods and/or coolant temperature and/or boron poison in maintaining reactivity and axial offset. Here the computationally fastest appropriate 1-D code is used and the two-group diffusion approximation is employed. Control rod action can be simulated by suitably modifying neutron cross sections with a preprogrammed correlation between cross sections and rod location. This level of detail is based on the WIGL3 neutronics code and was used in all calculations reported.

4. Though not used up to this point, higher-order geometries (e.g., X-Y, R-θ, 3-D) ultimately could be included in the neutronics for a more complete mapping of core detail.

4.2.1.2 Thermal Hydraulics. In choosing a formalism for core thermal hydraulics, we reviewed the following theories and codes developed in the U.S. and abroad that treat single- and two-phase flow: RELAP4 and RELAP5 (EG&G), TRAC PD2 and PF1 (LASL), RAMONA-3B and THOR (BNL), THOR RETRAN2 and FAST (EPRI), FLASH-5 (Bettis), COBRA-3 (Battelle), MATTEO (European Atomic Energy Community), BRUNCH-DL (West Germany), HUBBLE-BUBBLE-1 (UKAEA), THIRST (Atomic Energy of Canada), SINOD (Yugoslavia), UTSG (West Germany), and STUDS 1,2 (Sweden). The methodology chosen most closely follows the formalism of RELAP4.

For the mild to moderate transients of this study, nonequilibrium conditions are generally significant only in the pressurizer. Further, interphase slip is not expected to contribute significantly to control system evaluation in most cases. Therefore, the homogeneous approximation is sufficient of the majority of calculations.

4.2.2 Steam Generator

The PWR SG varies from vendor to vendor in ways that do not invite a single generic representation. B&W design characteristics supplemented by Oconee-1 data were used for the model. Primary and secondary coolant were one-pass systems, and coolant regimes having suitable correlations include subcooling, nucleate boiling, transition boiling, film boiling, and superheating.

4.2.3 Pressurizer

Equilibrium models of pressurizers have been shown to substantially underpredict pressure under important conditions. In our programming a nonequilibrium formalism was used that includes subcooled, saturated, and superheated phases. This methodology is an expansion of the treatment used in the RETRAN codes.

4.2.4 Reactor Coolant Pumps

The RETRAN2, TRAC, and other codes include pump models; we have adapted this work to ours. Multiple pumps and loops are treated to allow studies of failures of fewer than all pumps; thus asymmetries in the loops can be studied.

4.2.5 Turbine Generator and Feedwater Heaters

The dynamics of the turbine generator are significant in some cases of interest. ORTURB, a production code for turbine-generator-condenser simulation, is the basis for balance-of-plant modeling. This code has been applied extensively in studies of Ft. St. Vrain and other plants. The feedtrain simulation permits detailed modeling of steaming and condensation in heaters and uses the formalism developed by J. G. Delene, which was extensively applied in the desalination program. Modifications have been made as needed to accommodate specific requirements of this program. The low voltage bus is the modeling boundary.

4.2.6 Feedwater Pumps

RETRAN21, TRAC, or other sources provide the formalism adapted to our model. Multiple pumps and loops were simulated and therefore failure of fewer than all pumps can be studied. The AFW system was included.

4.2.7 Condensate Pumps

The same sources used for the FW pumps provide the formalism. The cooling water inlet pipe is the model boundary.

4.2.8 Emergency Core Cooling System (ECCS)

While the functions of the ECCS are not the thrust of this study, certain components are activated in some of the transients investigated. For example, during overcooling incidents the system pressure may fall enough to trip the high-pressure injection system and possibly the low-pressure injection system. These components, including accumulators, are treated in the model at a suitable level of detail.

4.2.9 Control System

The control system (Fig. 4.2) includes a realistic representation of primary controllers that simulate basic operating requirements. The detailed actions of secondary controllers, such as those for bearing lubrication or power supply function, were considered in the failure analysis implicitly as causes under broader simulation categories such as FW pump failure or instrument malfunction.

The kernel of B&W's integrated control system (ICS) comprises three major loops coupling megawatt demand with turbine, feedwater, and

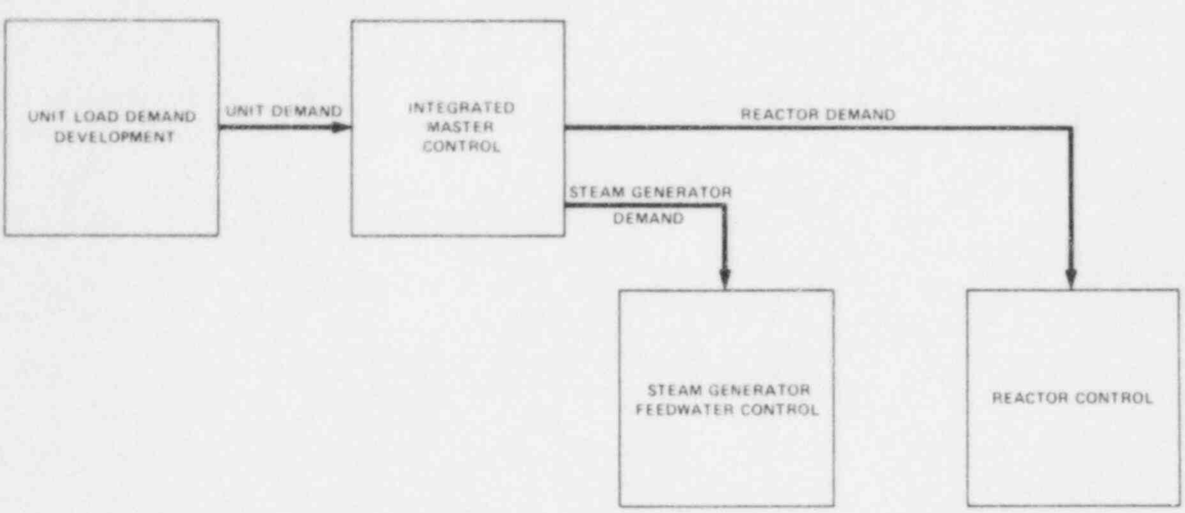

ORNL-DWG 83-8946
UNIT LOAD DEMAND DEVELOPMENT
UNIT DEMAND
INTEGRATED MASTER CONTROL
REACTOR DEMAND
STEAM GENERATOR DEMAND
STEAM GENERATOR FEEDWATER CONTROL
REACTOR CONTROL

Fig. 4.2. Model of the integrated control system.

reactor control plus pressurizer controllers. Simulation is complicated by feedforward signals, direct cross coupling of loops, and many rate and magnitude limiters that restrict loop functions or that reorganize portions of loops under prescribed conditions. These nonlinearities are typically excited during off-normal or upset conditions. Since it is the intent of this study to investigate such conditions, it was necessary to reproduce the ICS in considerable detail.

4.3 MODEL VALIDATION

The use of previously confirmed modeling techniques wherever possible provided a leg up on verification of the hybrid model of Oconee-1. Testing progressed along two fronts: (1) comparison with data from B&W plants including Oconee-1, and (2) comparison with the results of other codes such as TRAC and RELAP5. Details of both types of comparisons including numerous examples are given in Appendix C.

Comparisons to plant operating data and to steady state profiles from B&W design reports show good agreement. Detailed comparisons of the hybrid model predictions to data from Oconee 3 turbine trip (March 1980) were also in good agreement. The hybrid model shows the same degree of agreement with the data as do the TRAC and RELAP5 codes for cases run as part of the pressurized production codes (see Appendix C).

4.4 APPLICATION OF THE MODEL

The simulation was used primarily to address mild to moderate transients that can occur at least partially under action of the nonsafety control system. Severe transients simulated included steam line breaks. Attention initially focused on overfill events that assumed single or multiple failures of feed valves or the generator low and high level set points and the trips that regulate these valves. Cases were run at 20, 50, and 100% initial power levels, with failures occurring either in loop A or in both loop A and loop B. The classes of events listed below were considered. (In the first six sets, the initiating event was failure high of the low level set point.)

1. Intermediate overfeed failure insufficient to activate SG level protective features other than ICS interaction.

2. Overfeed failure when the high level control transfer is approached but not reached.

3. Slow MFW control valve action in combination with overfeed failure when the high level control transfer is approached but not reached.

4. Overfeed in which high level control transfer fails and high level pump trip is approached but not reached.

5. Overfeed with high level control transfer and high level pump trip failed.

6. Overfeed with high level control transfer and high level pump trip failed in combination with a steam leak in line A.

7. MFW blocking valve position indicator falsely indicated closed; flow reading taken from loop A startup meter.

8. Potential overfeed, which begins with main turbine trip and failure-in-place of main and startup feed value controllers, in some cases in combination with failure of bypass valve controllers.

9. Turbine trip during overfeed.

In general, these calculations showed that for single-SG overfeed, water inventory in the affected SG could increase to a level sufficiently high to saturate the SG fluid, quench superheat, and inject water into the steam line. In some cases of two-SG overfeed, the transient terminated on low suction trip of the main feed pumps. Overcooling of the primary side was usually modest.

Other events studied using the model include depressurization of the secondary side, overheating of the primary, and SG tube rupture:

1. Secondary side depressurization induced by steam line rupture or by steam valves failing open in loop A or in both loop A and loop B at low and high power levels.

2. Overheating induced by loss of all FW to SGs.

3. Partial or full rupture of one or more SG tubes following generator overfill, with or without main steam line break.

In the next sections the above groups of cases will be described in more detail. Transients were normally run for 10 min of plant time, although some were as short as 30 s and others extended to 1 h. (The model has restart capabilities for transient continuation.) Descriptions of lengthier event sequences are supplemented by tables. Although all available information on plant trips was included, it is possible that trips unknown to the authors would terminate some of the transients. Operator intervention was excluded.

In presenting the results of the hybrid simulations, only those figures that demonstrate the most important conclusions will be given here. For complete results, refer to Appendix C.

4.5 STEAM GENERATOR OVERFILL TRANSIENTS

As indicated above, nine classes of overfill sequences were considered:

Class 1: Intermediate overfeed failure insufficient to activate SG level protective features other than ICS interaction. In these cases the low level set point in SG A was assumed to fail high at 198 in. on the operating range. None of the high level set points was approached. At 100% power, the impact of this degree of overfill on the primary side was minor. At 50% power (and lower) overcooling remained minor, but as SG A filled to the set point the outlet quality* decreased below 1.0 and liquid was injected into the steam line (Fig. 4.3). Figure 4.3 is the time integral of liquid exiting the generator, indicating the total water passing into but not necessarily accumulating in the line. Phase separation and any attendant accumulation were not considered. Loss of superheat at lower power levels results from the larger incremental rise in generator water level necessary to reach the spurious set point.

Class 2: Overfeed failure when the high level control transfer is approached but not reached. In these cases the low level set point in SG A is failed to a higher value than previously: 240 in., which is near but below the high level set point. Because of the greater water loading in the SG, even at 100% power the steam quality at the generator outlet dropped below 1.0 at approximately 2.5 min. and water was injected into the steam line (Fig. 4.4). Runs at 20 and 50% power showed approximately half as much injection into line A in 10 min. As in Class 1 events, the impact on the primary side appeared to be minor.

The above runs were repeated with level failure occurring in both SG B and SG A. At power levels above approximately 50%, the results for both steam lines were comparable to those for line A discussed above. At lower initial powers, the MFW pumps tripped on low suction pressure and terminated the overfill before water was injected into the steam lines.

*Throughout this chapter the term quality refers to the thermodynamic quality.

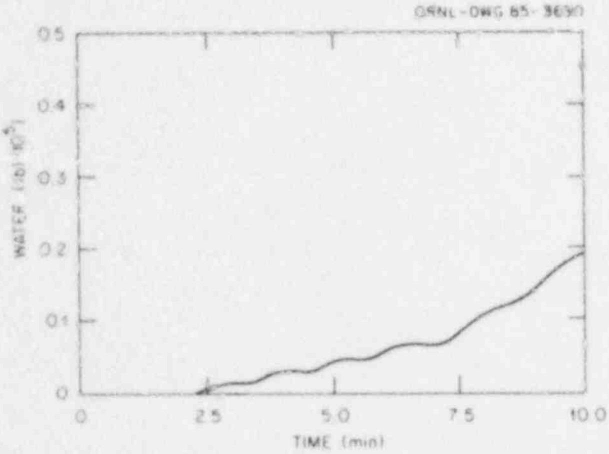


Fig. 4.3. Water injection into steam line A at 50% power (Class 1).

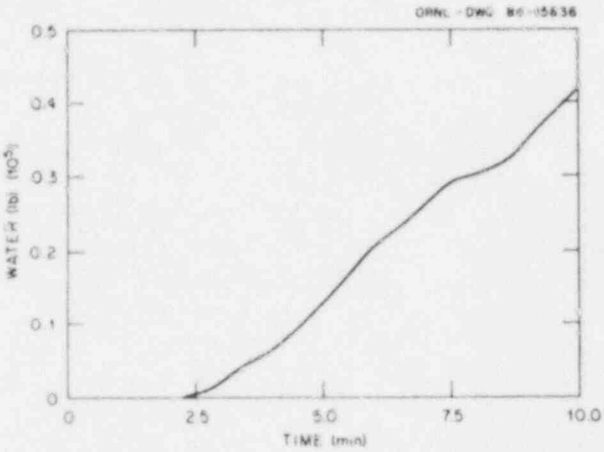


Fig. 4.4. Water injection into steam line A at 100% power (Class 2).

Class 3: Slow MFW valve action combined with overfeed in which the high level control was approached but not reached. These cases were a repeat of the Class 2 events but with an added FW control valve malfunction in which the stroke rate was significantly slower than normal. Full stroke time was assumed to be 60 s rather than the nominal 5 to 10 s. At full power, sluggish valve action reduced water injection by 50% compared with normal valve action; the ICS had more time to reduce flow to SG B and maintain system balance. Conditions on the primary side were largely unchanged. At lower power (20%), the ICS increased reactor output and FW to SG B in an attempt to match SG A overfeed. The net imbalance, combined with the longer time required to reach the failed level set point, was such that water injection doubled in comparison with normal valve action.

Class 4: Overfeed in which high level control transfer fails and the high level pump trip is approached but not reached. In these runs the low level set point was assumed to fail at 263 in., near but below the point at which pump trip would be initiated. Water injected into the steam lines in the first 10 min of the transient varied from 35,000 to 75,000 lb over the power range considered. Cooling of the primary remained minor. When set point failure in line B was combined with line A, water injection occurred in both lines at powers above 50%, while at lower power the system tripped on low FW pressure.

Class 5: Overfeed in which high level control transfer and high level pump trip failed. (See also Table 4.1.) In these cases, the low level set point in SG A was assumed to fail arbitrarily high; a value of 700 in. was used in the simulation. All high level control points in SG A were thus exceeded and assumed failed. Depending upon initial power level, the ICS took different courses of action to reestablish

Table 4.1. Class 5 overfeed: failure of high-level control transfer and high level pump trip of Steam Generator A

Event	Time (min)
20% Power	
Low level set point of SG A failed arbitrarily high (700 in.); high level control and trip failed	0
SG A feed valve opened; flow reached maximum rate	0.5
SG A superheat lost; water injection into steam line began	1.5
Reactor power matched increased flow	2.0
Loop A cold-leg coolant temperature stabilized 35°F below initial value	2.0
SG A outlet quality stabilized at 0.6	2.5
Primary pressure bottomed at 1985 psia	2.5
SG A water level stabilized at 350 in.	4
Pressure control system restored primary to set point	10
Gross water injection to line A was 380,000 lb	10
100% Power	
Low level set point of SG A failed arbitrarily high (700 in.); high level control and trip failed	0
SG A feed valve opened to 132% of normal flow; SG B valve closed to 79%	2
SG A superheat lost; water injection to steam line began	2
SG B superheat increased 12°F	2
Primary coolant temperatures restabilized; loop A cold-leg temperature 15°F below initial value	3.5
SG A level reached new steady state at 260 in.; SG B level at 130 in.	6.2
Gross water injection to line A was 68,000 lb	10

balance between reactor power and FW flow. At 20% power, the failed set point caused the SG A feed valve to run full open in a few seconds. Generator level increased to 350 in. and then stabilized because (1) the maximum pumping power in line A was reacned, and (2) balance between power and flow was reestablished at 60%, with most of the heat transferred to SG A. Superheat in SG A was lost in approximately 1.5 min. Total water injection was 380,000 lb after 10 min (Fig. 4.5). On the primary side, pressurizer pressure decreased 200 psi in 2.5 min and then recovered. Pressurizer level indication dropped 5 ft in the first 3 min and was beginning to rise after 10 min. The cold leg temperature of the affected loop decreased 35°F in 2 min (see Fig. 4.6).

At 100% initial power, the ICS was limited in its capacity to adjust power to match overfeed. In this case the control system reduced flow to SG B to compensate for the increase in tne flow to SG A. The level indication in SG A stabilized near 260 in. Water injected into line A was 68,000 lbs in 10 min (Fig. 4.7). Secondary and primary temperature variations are generally smaller than at 20% power because the overfeed at 100% is a smaller percentage change in flow.

In both of these transients, actions of the ICS to match power and feed flow resulted in a stabilized system. If the turbine does not trip on low quality, this configuration may be sustainable.

Class 6: Overfeed with high level control transfer and high level pump trip failed in combination with a steam leak in line A. The previous 100% power case was repeated with the addition of a steam leak in line A. The leak was sized to correspond to full-open bypass valves and began after the overfill was well established (5 min). In the affected line, steam flow redistributed between the leak and header in such a way that turbine flow decreased but total flow was nearly preserved. Conditions on the primary side did not differ markedly from the previous case. The configuration appeared to be controllable by nonemergency ICS action.

Class 7: The MFW blocking valve position indicator falsely indicated closed; flow reading taken from the startup meter in loop A. Initial power was 100%. The FW flow signal for SG A was 15% (see Table 4.2). The ICS reduced reactor power to 70% (Fig. 4.8). Total feed flow was reduced less rapidly, and some overcooling of the primary occurred.

Primary pressure decreased 230 psi, and pressurizer level fell from 18 ft to 9 ft in 1.5 min. Core average temperature, as calculated from the hot and cold legs of the affected loop, decreased 18°F in 1.5 min and then began a slow recovery. Water injection into steam line A was 20,000 lbs in 10 min.

Class 8: Potential overfeed that begins with main turbine trip and failure-in-place of main and startup feed valve controllers. Three subsets of events were considered, beginning at steady state with reactor and turbine trip: (a) main and startup valves frozen in place; (b) same as (a) except that in addition the condenser bypass valves were

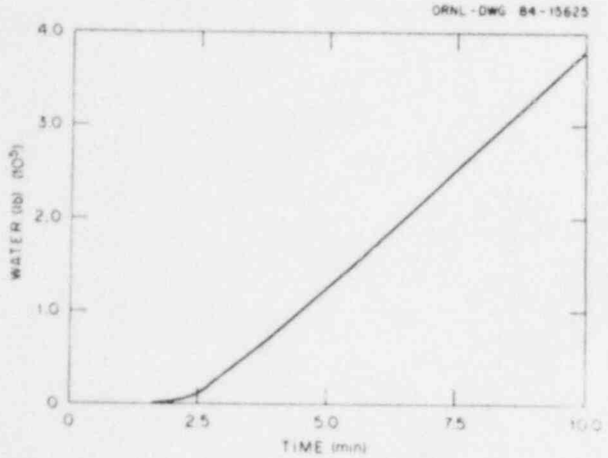


Fig. 4.5. Water injection into steam line A at 20% power (Class 5).

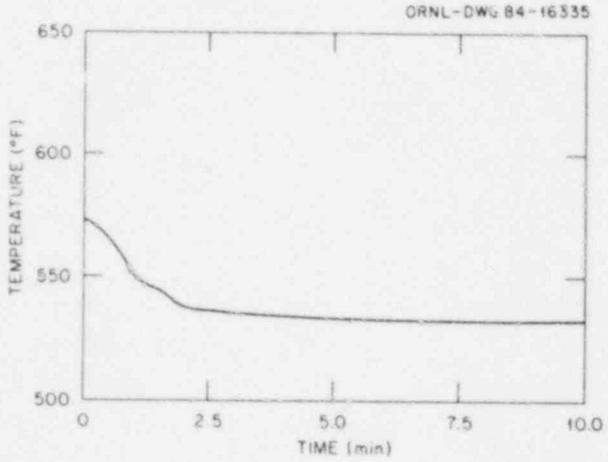


Fig. 4.6. Loop A cold-leg coolant temperature at 20% power (Class 5).

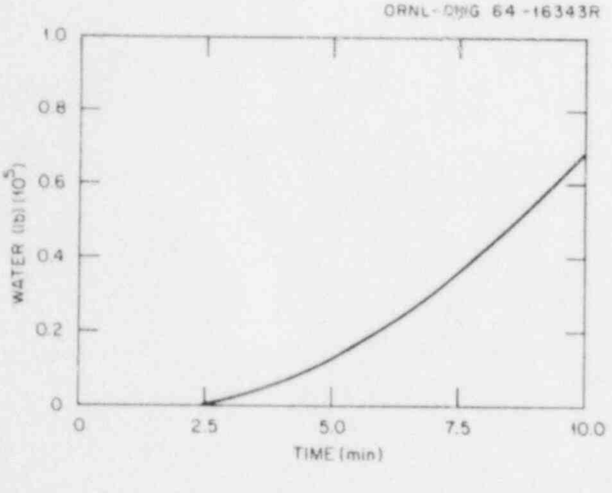


Fig. 4.7. Water injection into steam line A at 100% power (Class 5).

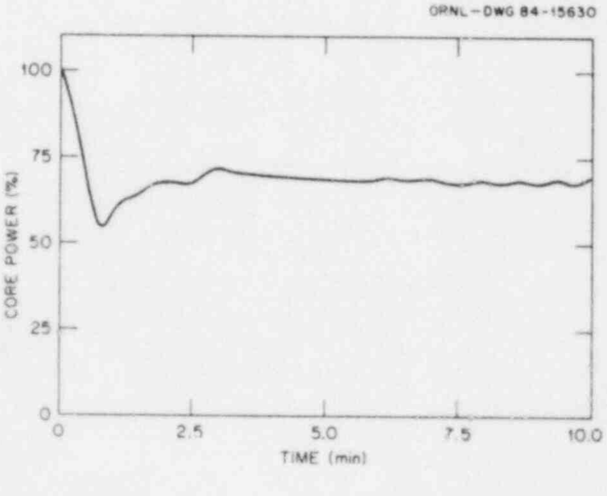


Fig. 4.8. Core power fraction (Class 7).

Table 4.2. Class 7 overfeed: main feedwater block valve position indicator falsely indicated closed
(Flow reading taken from startup meter in loop A; 100% power.)

Event	Time (min)
SG A MFW block valve indicator falsely indicated closed; flow reading taken from startup meter	0
ICS reduced reactor power to 55%	0.8
Primary pressure bottomed 230 psi below set point	1.5
Pressurizer level bottomed 9 ft below set point	1.5
Core average coolant temperature bottomed 18°F below set point	1.5
SG A superheat lost; water injection to line A began	1.5
ICS increased power from 55 to 70%	2.5
ICS ramped total feed flow back to 70%	5
Pressure control restored set point	10
Gross water injection to line A was 20,000 lb	10

locked shut, and (c) same as (b) except that the FW pumps were run back to minimum speed. Cases were run at 100% and 50% power. Overfeeding both generators resulted in tripping the FW pumps on low suction pressure approximately 20 s into the transient. Representative of these results is the Class 8a case at 100% power. The turbine tripped at time zero, the main and startup valves were frozen in place, and the turbine bypass valves were locked shut. Turbine bleed-steam valves closed in 5 s, shunting bleed flow (approximately one-third of the total) through the condenser. During this interval, high SG pressure reduced FW flow sufficiently to prevent feed pump trip. After a few more seconds, steam safety valve actuation limited pressure increase and the ICS increased main pump speed and flow to reestablish 35 psi across the main valves. At 20 s increasing flow caused suction pressure of the condensate booster pumps to drop below the 16-psig trip point. Loss of the booster pumps in turn tripped the main pumps on low suction, and feed flow ceased. Effects of the brief overfeed were negligible.

Allowing the bypass valves normal action somewhat reduced SG pressure buildup and slightly shortened the time taken for feed flow to build up to the pump-trip point; however, the overall results were not changed materially. In one simulation, the pump speed was manually run back to minimum (2800 rpm) to determine whether this action would reduce flow sufficiently to prevent a trip. When the speed fell below approximately 3200 rpm, the pump became effectively deadheaded (though recirculation to the condenser existed) and overfeed was thereby terminated. Thus, in these Class 8 cases, overfeed did not extend beyond the first 20 s of the transients. No water entered the steam lines, and cooling effects on the primary were minor.

The previous two-SG cases were repeated with only one SG affected. At 100% power, normal bleed flow shunted through the condenser and pumps caused sufficient incremental line loss to trip the booster pumps (and then the main pumps) on low suction pressure 55 s into the transient. However, at 50% power, low suction trip did not occur.

These results indicate that SG overfeed in coincidence with turbine trip may or may not be terminated by low pump suction pressure, depending on the initial power level. For two-SG overfeed, pump trip occurred at midrange power levels and higher. For single SG overfeed, pump trip occurred only at higher power levels.

It was noted, however, that the occurrence of predicted booster pump trips (followed by MFW pump trips) on low suction pressure is sensitive to the assumptions of line pressure drops, control valve losses, and details of the operational sequences. Only minor changes in these assumptions, within the bounds of the uncertainty ranges, could change the probability of pump trip.

Class 9: Turbine trip during overfeed. A series of runs was made to determine whether turbine trip during an overfeed event would exacerbate the amount of moisture injected into the steam line. It is unclear whether or how wet steam causes a turbine trip, either directly by active protection devices or indirectly by secondary disturbances. The study was done parametrically by initiating trip at time zero and at 3 min and 6.4 min after onset of overfeed. The overfeed initiator was failure high of the low level set point at 700 in., which caused the feed valves to open fully. At 100% power, the feed pumps tripped on low booster-pump suction following turbine trip. Although the failed low level set point actuated the EFW system, injection of water into the steam lines terminated on main pump trip (Fig. 4.9). With trip at onset of overfeed, superheat was not lost and no water was injected into the steam line. At power, injection commenced at 1.8 min. Trip at 3 min limited injection to 2.6×10^3 lb and trip at 6.4 min terminated injection at 4×10^4 lb. Principal thermal changes on the primary side were associated with reactor trip and were approximately the same magnitude for all three overfeed conditions (Fig. 4.10).

These runs suggested that excess main feed flow would have to be limited if consequential overfeed were to continue after turbine trip. The next case was started at 50% power (and flow). It was determined that failure of the SG A feed valve 80% open provided the maximum flow rate that could be sustained without pump trip following turbine trip.

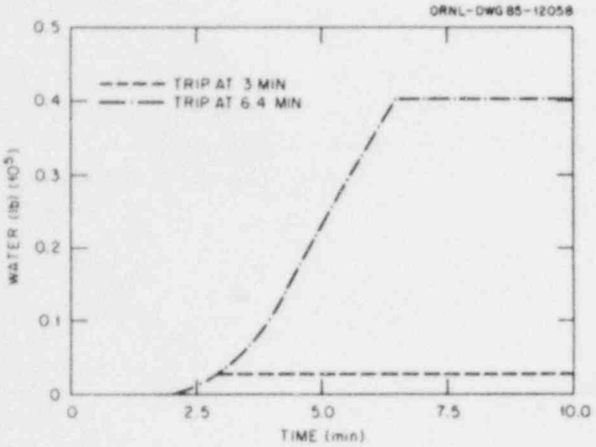


Fig. 4.9. Water injection into steam line A at 100% power (Class 9).

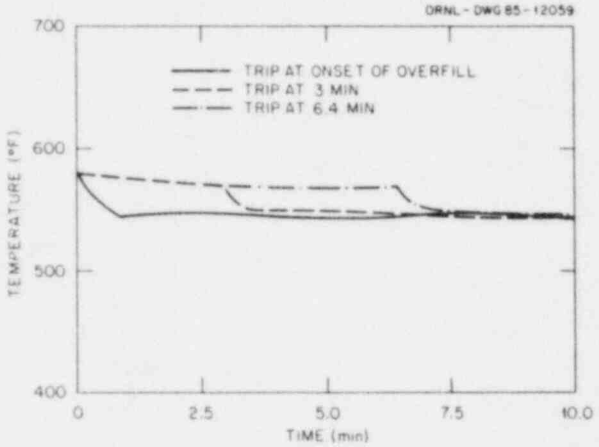


Fig. 4.10. Core average coolant temperature as measured by sensors in Loop A at 100% power (Class 9).

However, since the overfill rate was slower, the Btu-limit circuitry of the ICS was able to take corrective action and rebalance the system. Power increased and loop B SG feed flow increased to match that of loop A. The system restabilized near 80% power. Power increase was sufficiently rapid compared to the rate of overfill to prevent loss of SG superheat.

Thus, in this study turbine trip effectively terminated water injection into the steam line. When overfeed was restricted to a rate that would not cause pump trip, the Btu limits acted to prevent loss of superheat and hence injection of water into the steam line.

4.6 SECONDARY SIDE DEPRESSURIZATION TRANSIENTS

In these events, secondary side depressurization is induced by partial steam valve failure or steam line rupture in loop A or in both loop A and loop B and at low and high power levels. At 20% power, a fault in steam line A was sized to accommodate the line's total available flow. An initial modest pressure reduction in the SG resulted in a temporary increase in feed flow, and the ICS increased reactor output and reestablished equilibrium at 35% power. The ICS maintained header pressure by throttling turbine flow, forcing virtually all line A flow through the fault. Impact on the primary and secondary pressures and temperature was minor. Plant conditions appeared to remain manageable by the ICS. Without operator intervention, the system would be expected to trip on depleted FW inventory.

At 100% power, over the time interval considered, the ICS appeared to be capable of managing single-line faults that released up to 100% of one line's nominal flow. Perhaps the most noteworthy imbalance was the substantial downtrend in FW temperature that resulted from loss of one-half of the bleed steam to the heaters. Leaks of this magnitude or larger in both lines resulted in depressurization of the secondary side and system trip within 1 min on low steam flow to the turbine or a presumed disturbance resulting therefrom.

4.7 OVERHEATING TRANSIENTS

Overheating was induced by loss of all FW to SGs. Transients were initiated at steady state 100% power by tripping the reactor and turbine and closing the main and startup FW valves. The turbine bypass valves failed closed, and the EFW system did not actuate (see Table 4.3). In the first case considered, the primary coolant pumps were not tripped. The SGs dried out in 1.5 min; thereafter, decay heat was not removed at the SGs. The steam line safety valves cycled until SG dryout, whereupon the pressure stabilized. There was no further significant coupling to the balance of plant, and that part of the simulation was discontinued. Core average temperature dropped 25° during SG dryout and then began to rise from decay heating (Fig. 4.11). Six minutes into the transient, following the initial drop, pressurizer pressure reached the PORV set point and stabilized. At 14 min the pressurizer went solid (Fig. 4.12). Core fluid quality increased and reached saturation at 30 min. Core temperature stabilized while quality continued rising and the core began to void (Fig. 4.13). Shortly after the onset of voiding, primary pressure rose to the safety valve set point and then cycled between set points as the safety valves opened and reseated. At 1 h, when the transient was terminated, the core void fraction had reached 0.8 (Fig. 4.13); the core would have dried out in another 15 min.

The second overheating case was the same as above except that the reactor coolant pumps were tripped when the primary subcooling margin was less than 50°F, which occurred 12.5 min into the transient. This case explored whether reduced circulation would accelerate the rate at which the primary system overheated. It was found that, after the pumps tripped, the pipes and SG metal extracted enough heat from the coolant to establish natural circulation at approximately 2% of full flow. This provided sufficient effective mixing of the primary fluid to give a heat-up rate not materially different from the previous full-flow case.

4.8 STEAM GENERATOR TUBE RUPTURE TRANSIENTS

These cases investigated partial or full rupture of one or more SG tubes following SG overfill, with or without main steam line break (see Table 4.4). The principal interest here is based upon the following postulated scenario: Starting from failure high of the low level set point in one SG, the SG overfills, outlet quality falls below unity, water is injected into the steam lines (as occurred in Class 5 events),

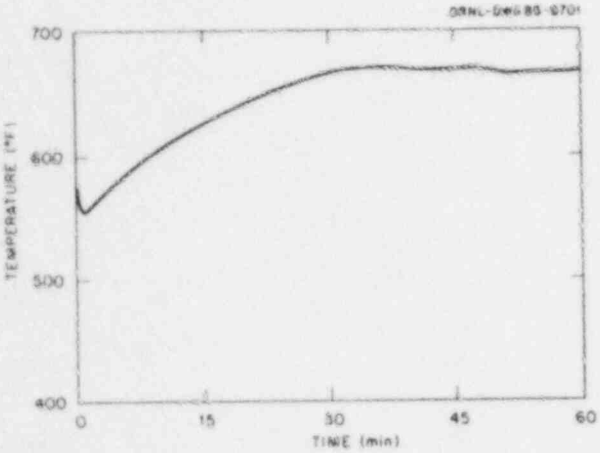


Fig. 4.11. Core average coolant temperature at 100% power.

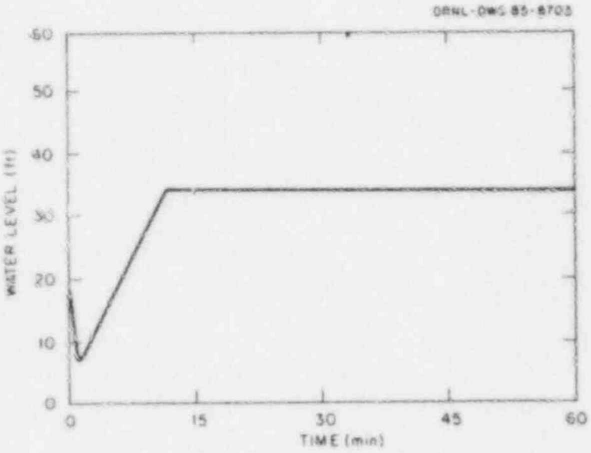


Fig. 4.12. Pressurizer water level at 100% power.

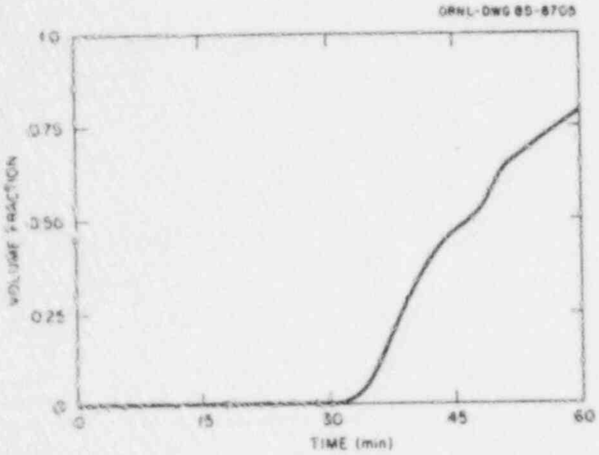


Fig. 4.13. Upper core vapor volume fraction at 100% power.

Table 4.3. Overheating induced by loss of all feedwater to steam generators
(Primary pumps not tripped; 100% power.)

Event	Time (min)
Loss of all FW, including emergency, to both SGs; turbine bypass valves failed shut; reactor and turbine trip assumed	0
SGs dried out; loss of decay heat removal	1.5
Core average coolant temperature bottomed 25°F below set point	1.5
PORV opened at set point	6
Pressurizer went solid	14
Primary fluid quality positive; voiding began	30
Primary pressure activated pressurizer safety valves	32
Core void fraction reached 0.8	60

and liquid-induced dynamic stresses in the pipes cause a full steam line break and a rupture of SG tubing. It is to be emphasized that while these cases predict liquid injection into the steam lines, they do not predict pipe break and/or tube rupture.

Three transients involving tube rupture were simulated. In all three the rupture was presumed to occur near the bottom tube sheet of the overfed SG. Each rupture event began 6.2 min after overfeed started, at which time the SG water level was 20 ft.

In the first and mildest case, one tube was partially ruptured with an average leak rate of 7.5 × 10^4 lb/h. No other failures were postulated. The plant was not tripped. The leak was of such size that the makeup systems compensated two-thirds of the loss, and primary inventory decreased slowly (Fig. 4.14). Primary pressure remained near set point until the pressurizer heaters tripped off on low level at 22 min. Core average temperature was controlled near set point. The contribution of the leak did not materially change the already overfilled SG level, the generator pressure or temperature, or injection into the steam line (Fig. 4.15).

In the second case, the leak rate was postulated to be substantially larger. Three tubes were presumed to have double-ended breaks with an

Table 4.4. Tube rupture transients
(100% power)

Event	Time (min)
Precursor to all tube rupture sequences	
Low level set point of SG A failed arbitrarily high (700 in.)	0
SG A feed valve opened to 132% flow; SG B valved closed to 79% flow	2
SG A superheat lost; water injection to steam line began	2
Primary pressure and pressurizer level bottomed; makeup and pressure control began to restore set points	3.5
SG A level increased to new steady state value of 240 in.; SG B level at 130 in.	6.2
One SG tube ruptured	
One tube in SG A experienced single-ended break; or equivalent leak of 7.5×10^4 lb/h	6.2
Primary inventory, partially compensated by makeup, slowly declined	6.2+
Pressurizer heaters operated to maintain set point	6.2+
Pressurizer level fell below heater trip point; pressure began to decrease; leak continued	22
Three SG tubes ruptured	
Three SG A tubes experienced double-ended breaks; total leak rate 6.2×10^5 lb/h	6.3
Low primary pressure tripped reactor	7.2
Pressurizer dried out; heaters tripped	7.9
HPI turned on at set point; pressure increased; inventory continued to decrease ~1%/min	8.3

Table 4.4 (continued)

Event	Time (min)
<u>One SG tube and steam line ruptured</u>	
Steam line A experienced full rupture; one tube of SG A had double-ended break with leak rate of 2 × 10^5 lb/h	6.2
False high-level signal in SG A tripped feed pumps, reactor, and main turbine	6.3
Pressurizer temporarily dried out; heaters tripped	6.5
Primary pressure fell to HPI set point	6.6
Core average coolant temperature as measured by loop A sensors dropped to ~505°F	6.6
Core average coolant temperature as measured by loop B sensors dropped to ~535°F and stabilized with slow downward trend	6.6
SG A coolant temperature dropped to ~495°F	6.6
SG A blew down to ~100 psia	6.7
Core average coolant temperature as measured by loop A sensors recovered to ~535°F and stabilized with slow downward trend	6.8
SG A coolant temperature recovered to ~535°F and stabilized with slow downward trend	7
SG A dried out	7
HPI rewetted pressurizer	7.5
HPI restored primary pressure to set point	13
HPI built pressurizer inventory to normal level; leak continued	30

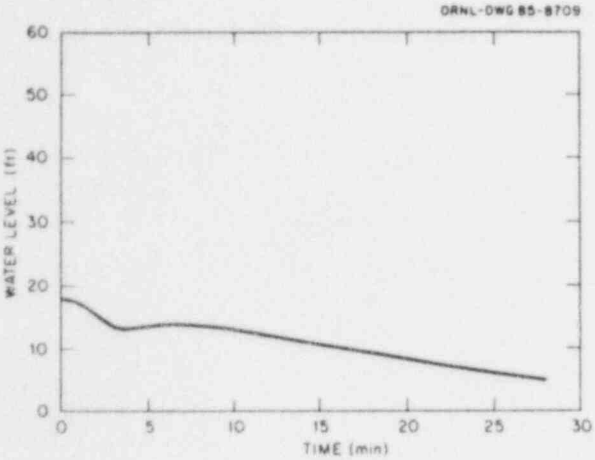


Fig. 4.14. Pressurizer water level. Overfill of steam generator A followed by partial rupture of one tube.

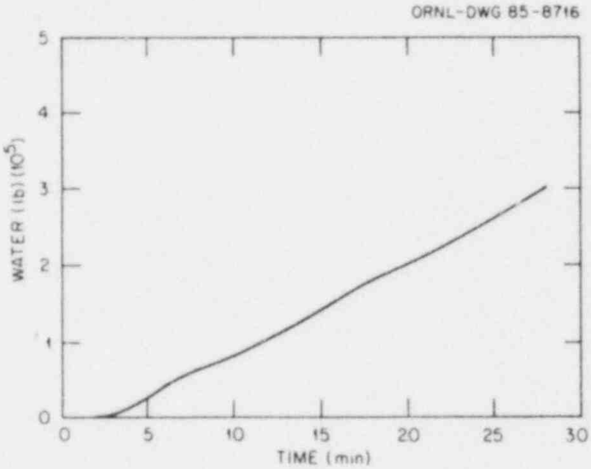


Fig. 4.15. Water injection into steam line A. Overfill of steam generator A followed by partial rupture of one tube.

average total leak of 6.2 × 10^5 lb/h. No other failures were postulated. In this case the leak was an order of magnitude larger than the normal makeup capacity. Primary pressure violated the protection system pressure-temperature constraint at 7.2 min and tripped the reactor.

At 8.3 min the HPI system actuated and reversed the pressure trend. Although the primary began to repressurize, the leak exceeded the capacity of the HPI, and net inventory loss continued (Fig. 4.16). The pressurizer dried out at 7.9 min. Primary inventory gross loss continued at the full leak rate, ~2.5%/min, and net loss was ~1%/min. In this case, throttling the HPI and depressurizing the primary would appear to be requisite operator actions not only to staunch release of coolant but also to prevent core exposure.

In the last tube rupture event studied, one SG tube was assumed to experience a double-ended break with an average leak rate of 2 × 10^5 lb/h in conjunction with a guillotine-type break in the main steam line of the overfilled SG. No operator actions were included. The massive disturbance was presumed to trip the main turbine and reactor, at least on false high-SG-level signal (noted below). Blowdown of the affected SG reduced the pressure to 100 psi within 30 s, at which time SG A dried out and thereafter the influx of primary coolant flashed to steam upon entering the secondary side. The dynamic head associated with the initial acceleration of fluid in the affected SG caused the level sensor to register higher than the high-level trip, and the feed pumps tripped. Steam temperature dropped during blowdown and, after dryout, tracked the temperature of the flashing primary fluid. Primary pressure fell rapidly during SG blowdown. HPI was initiated at set point in 20 s, and pressure was subsequently restored to the PORV set

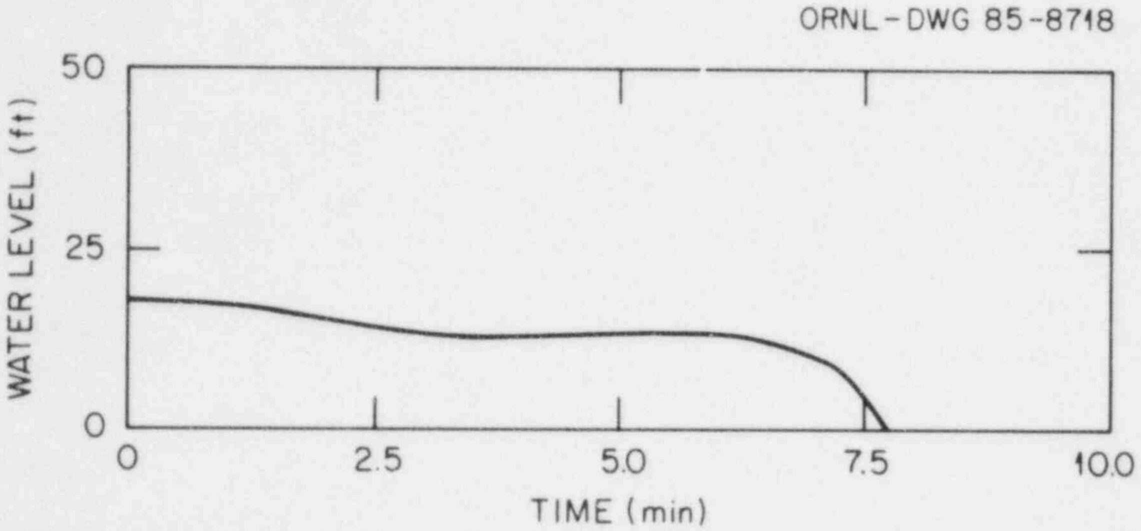


Fig. 4.16. Pressurizer water level. Overfill of steam generator A followed by full rupture of three tubes.

point. The pressurizer temporarily dried out until HPI was established. Core average temperature decreased rapidly during depressurization, then stabilized at ~535°F. At 30 min, when the calculation was terminated, the system inventory was increasing and the leak into the secondary system was continuing.

An additional case was run to help estimate the amount of radioactive primary coolant that might be released to the atmosphere in the event of steam tube rupture. The calculation began with the assumption that radiation alarms instigated a reactor trip. Total heat generation (Btu), total steam generation (lb), and total steam released to the atmosphere through the safety valves as a function of time after trip are shown in Fig. 4.17. Steam released through the safety valves, which opened only during the first half-minute of the transient, amounted to 1.1×10^4 lb. If the bypass valves are operative, that would also be the total steam released (27% of the total steam generated during the time the safety valves cycled). If the bypass valves failed closed, the total steam curve (Fig. 4.17) is a guide to the amou... that would be released through the safety valves during the early minutes of the transient. For longer times, extrapolation of the total heat generation curve provides a measure of the amount of steam that would be produced at ~700 Btu/lb. Initially a greater amount of steam is produced because the primary system experiences a temperature drop.

Assuming that one SG tube ruptured with an average leak rate of 2×10^5 lb/h, and that the bypass valves operated as designed,

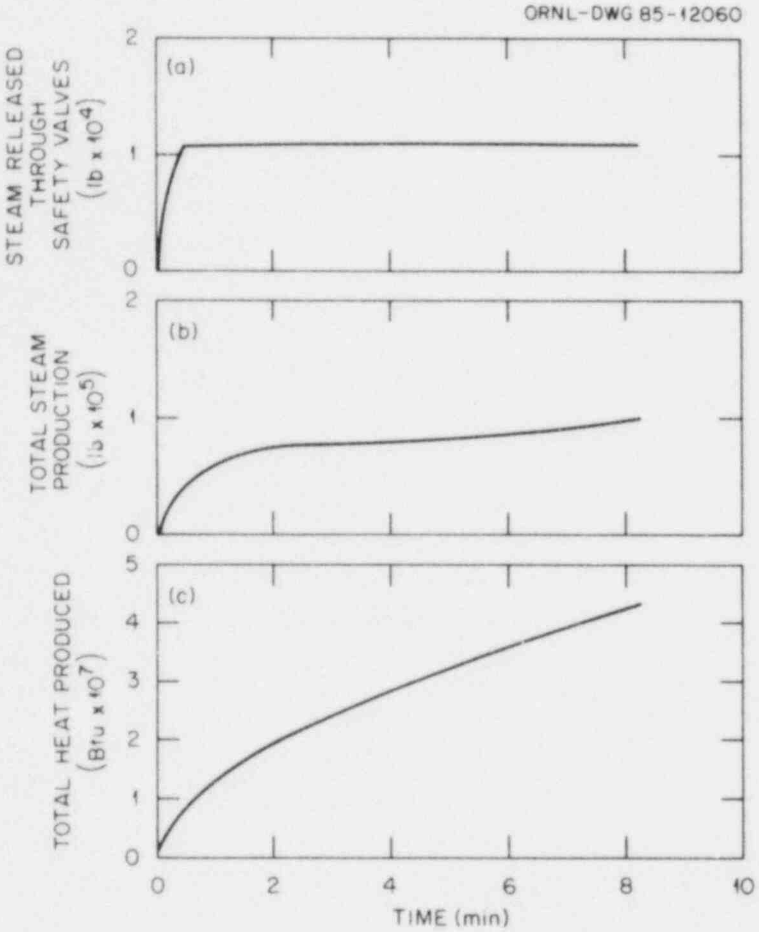


Fig. 4.17. Energy and steam production following a reactor trip.

~450 lb of the primary coolant would be discharged through the safety valves. If the bypass valves failed closed, the coolant should be discharged at approximately the leak rate.

4.9 REVISION OF THE HYBRID MODEL OF THE STEAM GENERATOR

Using data provided by NRC, the steam generator model was originally designed with an outlet steam temperature of 570°F, which yielded 38° of superheat. The superheat region started at 72% of the length of the tubes relative to the bottom tubesheet. The primary- and secondary-side temperature distributions calculated by the model agreed closely with design profiles included in the NRC-supplied data. In reviewing ORNL's draft report on Oconee 1, Duke Power Company stated that SG superheat ranges from 48 to 63°, that the outlet temperature is nearer to 595°F, and that the superheat region begins at 55% of the length of the tubes.

The hybrid model has been revised accordingly. Using the midpoint of the stated range of superheat, the SG outlet temperature was increased to 590°F to provide 55° of superheat. The model superheat region now begins at 55% of the length of the tubes.

Following revisions of the model, the Class 5 event overfill that occurred at 100% power was repeated to judge whether this higher level of superheat would qualitatively change the conclusions of previous overfill calculations in which water was injected into the steam line. Although the added superheat had the expected effect of retarding loss of superheat, the overall course of the transient was not changed. Results based on the two SG models are compared in Figs. 4.18 and 4.19. With the revised model, the overfilled generator lost superheat in 3.5 min (versus 2.5 min with the original model), and 3.2×10^4 lb (versus 6.8×10^4 lb) water was injected into the steam line in 10 min. The basic conclusions of the overfill studies appear to remain unaltered; for certain conditions, superheat can be lost and water injected into the steam line. It should be noted that ORNL studies have indicated that the ICS Btu limits will act to prevent loss of superheat if the rate of overfill is not too great. This was found in the Class 9 event in which the rate of overfill at 50% power was limited by failing the feed valve only 80% open.

4.10 PRELIMINARY CONCLUSIONS

A number of general conclusions may be drawn from these simulations. Safety implications are treated more fully in Sects. 3 and 5. The ICS shows considerable ability to deal appropriately with many of the off-normal conditions investigated. The feedforward and feedback control matrix, which matches FW and reactor power, has a versatility that tended to buffer the disturbances. This is seen particularly in the Class 5 overfeed events in which all high level control was inoperative. The ICS manipulated either the power level at low power or the distribution of feed flow between generators at high power to maintain Btu balance.

In a number of the simulations, superheat was lost, SG quality fell below 1.0, and water was injected into the steam lines. While these cases presume no quality trip, conditions could exist in which the quality hovered just above a trip set point and injected water into the lines for a sustained period. For example, in the Class 2 event in which the low level set point in SG A failed to 240 in., the quality was marginally below unity and water was injected into the line (Fig. 4.4).

Overfeed of both SGs tended to inject water into the lines at power above approximately 50%, whereas the calculations indicated that at lower powers the systems would trip on low FW suction pressure before water was injected. Safety implications of water injection are discussed elsewhere.

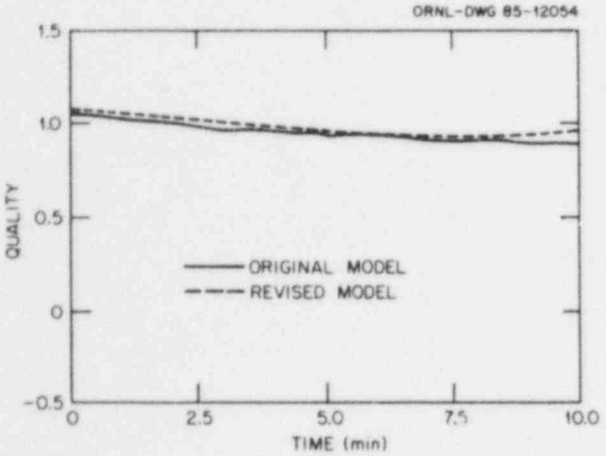


Fig. 4.18. Steam generator A outlet quality at 100% power: comparison of original and revised SG models. (Class 5: overfeed with level control transfer and high-level pump trip failed.)

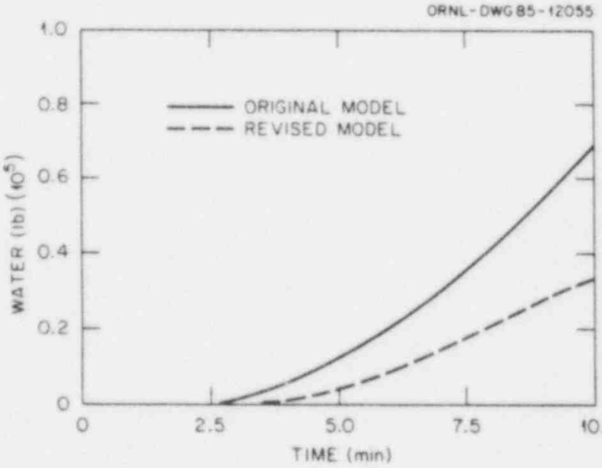


Fig. 4.19. Water injection into steam line A at 100% power: comparison of original and revised SG models. (Class 5: overfeed with level control transfer and high-level pump trip failed.)

In another type of overfeed event, the transient began with turbine trip and failure of the FW control valves in place. On turbine trip the bleed lines are sealed off and an additional one-third of flow is rerouted to the condenser and through the feed pump lines, with attendent increase in pressure loss at the pumps. The result indicated that the transient may or may not be terminated by low pump suction pressure, depending on initial power level (and flow) as well as on assumptions made about the operational sequences and the modeling of line and control valve pressure losses. For two-SG overfeed, the incremental flow on turbine trip was sufficient to cause pump trip if the initial power and flow were midrange or higher. For single-SG overfeed, trip occurred only at high power, and even then the trip condition appeared marginal (as noted).

Turbine trip at full power (and flow) effectively terminated water injection into the steam line. When overfeed was restricted to a rate that would not cause feed pump trip, the Btu limits acted to prevent loss of superheat and hence water injection into the line.

In the majority of cases studied, overfill of the SGs appeared to have only minor effects on the temperatures and pressures of the primary side. An exception was the Class 7 event in which the MFW blocking valve position indicator falsely indicated closed and the flow reading was taken from the startup meter in loop A. The ICS ran the power back more rapidly than feed flow, and primary pressures and temperatures dropped significantly. This case suggests that the automatic ramp rates for power and flow may lead to notable thermal imbalances under certain operating (nontrip) conditions.

The ICS demonstrated ability to manage single-line steam leaks up to the full normal flow in the line for the existing power level. In the simulations there was a tradeoff of flow between the leak anu the turbine, with consequent reduction in turbine power. Turbine trip may occur even though the leaks appeared otherwise controllable by the ICS in the short term.

Overheating of the primary on loss of all FW was dominated by the combined heat capacity of the primary fluid and metal, and was marginally affected by main pump operation. For the conditions studied, boiling began in the core in 30 min, and dryout would occur in an additional 45 min.

Steam generator tube ruptures varying in size from partial rupture of one tube up to double-ended breaks of three tubes were considered in conjunction with an overfill incident. Operator action was not addressed. In all cases the HPI operated to reestablish pressure at set point and perpetuate leakage into the secondary system and out the steam-line valves. In the case of a triple-tube rupture, rate of inventory loss exceeded HPI capacity, the pressurizer dried out in ~1.5 min and primary inventory net loss continued at the rate of ~1%/min, indicating that operator action was needed to prevent uncovering the core. Each additional simultaneous tube rupture would increase the net loss by ~1%/min and correspondingly reduce the time available for remedial action. When rupture of one tube was accompanied by a full steam-line break, the average core temperature decreased ~50°F during rapid steam generator blowdown, then stabilized as leaking primary fluid flashed in the dried-out generator.

5. SUMMARY AND CONCLUSIONS

A detailed analysis of the Oconee-1 nuclear power plant systems has been performed to evaluate possible safety implications of control system failures. Results of the control system failure analysis for the Oconee plant design have been discussed in detail in Sect. 3 and are summarized in Sect. 5.1. Section 5.2 identifies possible areas of investigation to assess mitigation of these control system failure transients, and Sect. 5.3 discusses generalization of these areas of investigation of the Oconee design to B&W NSSS plants as a category.

5.1 SUMMARY OF CONTROL SYSTEM FAILURES WITH SAFETY IMPLICATIONS

Two Oconee 1 control system failure-initiated transients have been identified with potentially significant safety implications: SG overfill and loss of SG cooling. These two transients are discussed below.

5.1.1 Control System Failures Leading to SG Overfill

SG overfill has been identified as a transient consequence of concern in the SICS Program. Although specific analysis of the consequences of SG overfill are beyond the scope of this program, possible areas of concern include consequential steam line failure and SG tube ruptures. As discussed in Sect. 3, such consequences of SG overfill may not occur; however, the conditional probability of steam line damage and tube rupture following SG overfill is expected to be significant. Further analysis of these consequences is recommended.

In the SICS Program, the analysis was directed toward identifying and analyzing failures that result in SG overfill. Control system failures were found that result in two types of liquid injection into the steam lines:

1. Certain failures resulted in increasing SG inventory without initiating reactor trip. These failures, while they may result in turbine blade damage, are not expected to cause a gross injection of liquid into the steam lines.

2. Similar failures which either follow reactor/turbine trip or cause such a trip have potentially more severe consequences. With the reactor tripped, the MFW system is capable of rapidly filling the SG secondary volume and injecting a significant quantity of liquid into the steam lines.

As described in Sect. 3.2, several control system failures could initiate such an event. In the Oconee design, existing instrumentation results in an automatic trip of the MFW pumps on high SG level in addition to possible operator actions that could terminate the overfeed. As described in Sect. 3.2, the combinations of control system failures and operator failures required to cause SG overfill were analyzed. Based on this analysis, the frequency of SG overfill due to all causes at Oconee has been estimated to be between 6×10^{-3} and 1×10^{-4} events/ry.

5.1.2 Control System Failures Leading to Loss of SG Cooling

Two failures were found that could result in loss of SG cooling. In either case, subsequent operator action would be required to prevent significant core damage.

The first failure involves a loss of ICS hand power. This failure reduces the MFW pump speed and terminates FW injection to the SGs without tripping the MFW pumps. Without a trip of the MFW pumps, the EFW will not be initiated automatically. In this case the operator must manually initiate EFW or the HPI to prevent core damage.

Another ICS power failure, loss of auto power, also may lead to loss of SG cooling. Loss of auto power transfers the MFW controls to manual, with the MFW control valve in an "as is" position. Should a reactor trip result from the transients, an overfeed transient would occur. If the operator manually throttles MFW flow, FW injection to the SG ceases and SG cooling will be lost unless the operator manually restores MFW or manually initiates EFW.

The sequences of these events leading to significant core damage have been evaluated to estimate core damage frequencies. Core damage sequence frequencies of 10^{-5}/ry and 10^{-6}/ry have been estimated for the loss of SG cooling sequences initiated by loss of ICS hand power and loss of ICS auto power respectively.

5.2 MITIGATION OF SIGNIFICANT CONTROL SYSTEM FAILURES

The potentially significant control system failures discussed above have been evaluated to identify possible areas of improved mitigation. These areas of possible improvement are discussed below.

5.2.1 Steam Generator Overfill

In the SG overfill case, there exists a circuit largely independent of identified initiating failures which will trip the MFW pumps on high SG level. However, due to the long test interval for circuit components (1 y) and the 2-out-of-2 logic used, the expected failure rate of this circuit was relatively high.

If the estimated frequency of SG overfill is found to be too high, several options are available to reduce it. These options include shorter trip circuit test intervals and circuit modifications. Although modification of the existing MFW pump trip circuitry is not recommended, parallel circuits that close the MFW block valve (in series with the MFW control valve) could significantly reduce SG overfill frequency.

5.2.2 Loss of Steam Generator Cooling

The two loss of SG cooling transients are significant due to the coupled loss of MFW and loss of automatically initiated EFW. In this case, automatic initiation of EFW based on low SG level is recommended. It is noted that 1E SG level transmitters are mounted on the SGs at Oconee but are not used for EFW initiation.

5.3 APPLICABILITY OF RESULTS TO OTHER B&W INSTALLATIONS

Results to date have been based on a model of Oconee-1 and are therefore, in the first analysis, plant-specific for the three very similar units at the Oconee Nuclear Station. Generic extensions of these results to other B&W installations will depend primarily upon balance-of-plant configurations at the other facilities, which in general will show more variation than will the primary systems. In the interest of generality of application, to the limited extent possible other B&W-designed plants have been examined for those features that have caused interest in certain transients at the Oconee installation.

One aspect of plant behavior developed in previous sections of this report involves the overfill of a single SG, with subsequent possibility of steam line flooding. In general, this scenario requires a failure that initiates a FW overfeed, plus another condition that avoids a high level MFW pump trip. In those cases where a failure of the high level trip mechanism itself must be assumed, there can be significant differences between B&W plants. For instance, in Oconee the high level trip is a nonsafety system whereas at Davis-Besse the same trip is safety grade, with the appropriate design and surveillance requirements imposed by that designation. This type of consideration will affect failure probability calculations, and therefore probabilities calculated for Oconee-1 should not be uncritically applied to another plant. The newly deployed emergency feedwater initiation and control (EFIC) system has already been installed in, or is planned for, Arkansas Nuclear One-1, Crystal River-3, SMUD, and Three Mile Island-1. Earlier versions of EFIC had high level trips, but most of these have been removed because of problems with noisy level transmitters. Because of these plant-specific variations in high level trips, the exact situation in a given plant must be assessed before an overfill probability can be addressed. We have found no significant differences between plants in their proneness to sensing line failures or in the amount or quality of information available to their operators during overfill sequences.

Another evaluation addressed potentialities for dryout. At Oconee, if both MFW pumps trip, the AFW starts automatically. AFW also starts in response to low pressure in the MFW header. In contrast to Oconee, plants using the EFIC add an AFW start on low SG level. In general, it appears a good idea to provide for such AFW actuation on low level, a direct measurement of the variable at risk.

Other B&W plants have more or less diversity in equipment than Oconee. (All of the AFW pumps presently at Davis-Besse, for example, are steam-turbine driven; all other U.S. PWRs have at least one motor-driven AFW pump.) Other plants also exhibit widely varying historical rates of MFW loss and AFW failures as a function of routine operation. The record of Oconee 1 FW problems was found to be much better than both the B&W and other PWR averages (see Sect. 2.2). The evaluation of Oconee thus provides a useful guide to safety implications of control in other B&W plants and even, to some extent, in the PWRs of other manufacturers. It obviously cannot be taken as a quantitative guide to such problems in any other system.

The further question arises as to whether certain control system problems precluded by Oconee's design and therefore not found in our study may nevertheless exist in other B&W plants of substantially different design. The broad FMEA described in this report examines the control systems that may affect safety in a truly broad generic sense. The historical record was also examined for failures in all B&W plants. There is thus a general basis for expecting that the broad systems and issues of concern have been identified for the class of B&W plants as a whole. Where potential problems were found in this broad approach, the Oconee system was examined in an augmented, very plant-specific fashion to verify and quantify the effects to be expected. While the results of this augmented, simulator-aided study can be expected to give useful insight for all B&W installations, it must be understood the design parameters used were from the Oconee 1 plant, and that the results of the augmented study can be applied to another plant only in the context of an informed consideration of design differences that may alter results.

REFERENCES

1. Task Plan for USI A-47.

2. IEEE FMEA definition (standard).

3. "Pressurized Thermal Shock Evaluation of the Oconee-1 Nuclear Power Plant," NUREG/CR-3770, April 15, 1984.

4. "A Ranking of Nuclear Plant Systems for Failure Modes and Effects Analysis," ORNL #62-13819C/62X-30, December 31, 1982.

5. "Final Safety Analysis Report - Oconee Nuclear Station," Duke Power Company.

6. "Failure Modes and Effects Analysis (FMEA) of the ICS/NNI Electric Power Distribution Circuitry at the Oconee 1 Nuclear Plant," NUREG/CR-3991, ORNL/TM-9383, August 1985.

7. U.S. Nuclear Regulatory Commission, "Transient Response of B&W Reactors." NUREG-0667.

8. U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of Nuclear Reactor Regulation of Preliminary Design for Safety-Grade Anticipatory Reactor Trip (ARTs) on Loss of Main Feedwater and/or Turbine Trip," Document 800111058.

9. Letter from H. L. Thompson, Jr., to H. R. Denton (NRC), "Preliminary Review of the Design and Performance of the Davis Besse Feedwater and Related Systems," July 2, 1985.

10. M. L. Ryan, "AEOD Finds Many Scrams That Occur at Power Are Due to Non-Safety Hardware," Inside NRC, McGraw-Hill, Vol. 7, No. 7, May 13, 1985.

11. "Letter from K. S. Canady (Duke Power Co.) to A. P. Malinauskas (ORNL)," March 13, 1985.

12. Babcock & Wilcox, Anticipated Transient Operating Guidelines

13. Nuclear Power Experience, Vol. PWR-2, VI Turb. Cycle Syst. E. Cond. & FW, p. 3).

14. Letter from W. Parker (Duke Power Co.) to H. Denton (NRC), Attachment 1, July 12, 1980.

15. IEEE Guide for the Collection and Presentation of Electrical and Electronic Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations, IEEE-500, 1984.

16. Integrated Control System Reliability Analyses, Report BAW 1564, August 1979.

17. In-Plant Reliability Data Program, NUREG-CR-3154, December 1983.

18. Letter from W. Parker to H. Denton, July 23, 1980.

19. "Reactor Vessel Pressurized Thermal Shock Evaluation," Duke Power Co., January 1982.

20. NUREG/CR-2789

21. Schematic Diagram DB032344, Revision D, Bailey Meter Co.

22. Elementary Design OEE-121-4, Revision 4, Duke Power Co.

23. An Assessment of the Impact of Human Factors on the Operations of the CRBR SCRS," R. R. Fullwood and K. J. Gilbert, SAI-010-76-PA, August 1976.

24. A Probabilistic Risk Assessment of Oconee Unit 3, NSAC 60, June 1984.

25. "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," NUREG/CR-3010, November 1983, Figure 6.1.

26. "Loss of 1, 2 KI Buses," EP/1&2/A/1800/31, November, 1979.

27. "Loss of Steam Generator Feedwater," EP/0/A/1800/14, January 1981.

28. O. L. Smith, "A PWR Hybrid Computer Model For Assessing the Safety Implications of Control Systems," NUREG/CR-4449, ORNL/TM-9868.

APPENDIX A

Detailed System Descriptions

APPENDIX A

Detailed System Descriptions

Brief system descriptions are provided for each of the major control systems identified in Sect. 2. Support systems (e.g., instrument air and control systems) are discussed with each major system. The Oconee final safety analysis report (FSAR) was the principal source of information used to develop these system descriptions. (See Tables A.1 through A.14 at the end of this appendix.)

A.1 NUCLEAR SYSTEMS DESCRIPTIONS

Nuclear systems include the reactor core and those systems and subsystems that monitor and control core reactivity, remove heat from the core, and otherwise support safe operation of the reactor. The major systems and subsystems identified in Sect. 2 are as follows:

- N01 - Reactor Core
- N04 - Reactor Coolant System
- N02 - Regulation Systems
- N05 - Makeup and Purification System

Brief descriptions of these systems are provided in this section.

A.1.1 Reactor Core

The reactor core consists of 177 fuel assemblies supported within the reactor vessel by internal grid plates. Fission of the slightly enriched uranium in the core fuel assemblies produces thermal power, which is ultimately used in the unit's main generator to produce electric power.

The reactor core produces heat at a rate consistent with exterior factors such as the density of the moderator (reactor coolant), the concentration of boric acid in the coolant, and the position of control rods in the core. Heat is removed from the core by pumping the reactor coolant upward through the fuel assemblies. The rate of heat transfer depends on the fuel temperatures, the reactor coolant temperatures, and the coolant velocity.

Although the response of the core to external parameters is important to a study of reactor coolant system overcooling or undercooling, a detailed analysis of core failure mechanisms initiating a transient is considered beyond the scope of this study. For purposes of this analysis, the reactor core is assumed to be operating within technical specification limits at the onset of externally initiated transients, and to respond to external factors as designed.

A.1.2 Reactor Coolant System

Together with the reactor core, the Oconee reactor coolant system (RCS) constitutes a Babcock and Wilcox (B&W) designed nuclear steam supply system (NSSS). The RCS consists of or is impacted by the following major components of the reactor pressure boundary:

1. A reactor vessel to house and support the reactor core.

2. Four reactor coolant pumps to circulate reactor coolant through the reactor core and the steam generators (SGs).

3. A pressurizer to control RCS pressure and maintain the reactor coolant in a subcooled state.

4. Two SGs to transfer heat from the reactor coolant and produce steam to drive the plant turbines.

5. Sixty-nine control rod drive mechanisms to position the individual control rods.

Reactor coolant is pumped from the SGs into the reactor vessel through the four "cold-leg" inlet pipes. As the coolant flows upward through the pipes, heat is transferred from the fuel elements to the coolant, raising its temperature. The heated coolant flows from the reactor vessel to each of the two SGs through one of two "hot-leg" outlet pipes. Heat is transferred from the high temperature reactor coolant as it flows downward through the tubes of the two SGs. The heat flowing across the SG tube walls vaporizes and slightly superheats the feedwater (FW) pumped into the shell side of the SGs to produce steam. The reduced temperature reactor coolant then flows through two pipes leading from each SG, one to each of the four reactor coolant pumps.

The reactor vessel and connecting piping are safety-qualified passive-pressure boundaries. Consideration of the failure of these pressure boundaries is beyond the scope of this study. The functions of the reactor coolant pumps, pressurizer, SGs, and associated equipment are discussed below.

A.1.2.1 Reactor Coolant Pumps. Each reactor coolant loop contains two vertical single-stage centrifugal type pumps having a controlled leakage seal assembly. Reactor coolant is pumped by the impeller attached to the bottom of the rotor shaft. The coolant is drawn up through the bottom of the impeller, is discharged through passages in the guide vanes, and exits through a discharge in the side of the casing. The impeller can be removed from the casing for maintenance or inspection without removing the casing from the piping. All parts of the pumps in contact with the reactor coolant are constructed of austenitic stainless steel or equivalent corrosion-resistant materials.

The pump employs a primary, high-pressure-controlled leakage seal assembly to restrict leakage along the pump shaft, as well as a secondary high pressure seal to direct the controlled leakage out of the pump. A low pressure vapor seal minimizes the leakage of vapor from the pump to the containment atmosphere.

A portion of the high pressure water flow from the high pressure injection (HPI) pumps is injected into the reactor coolant pump between the impeller and the controlled leakage seal. Part of the flow enters the RCS through a labyrinth seal in the lower pump shaft to serve as a buffer to keep reactor coolant from entering the upper portion of the pump. The remainder of the injection water flows along the drive shaft, through the controlled leakage seal, and finally out of the pump. The small amount that leaks through the secondary seal is also collected and removed from the pump.

Component cooling water is supplied to the thermal barrier cooling coil. In the event seal injection from the HPI pumps stops, reactor coolant will flow from the coolant system and through the thermal barrier labyrinth seal. The temperature of the reactor coolant is reduced in the labyrinth seal (thermal barrier cooling coil) prior to passing through the controlled leakage seals.

The reactor coolant pump seals are designed to operate with either high pressure seal injection flow, component cooling water flow, or both.

The reactor coolant pump motors are large, vertical, squirrel cage induction motors. They have flywheels to increase their rotational inertia, thus prolonging pump coastdown and assuring a more gradual loss of main coolant flow to the core in the event pump power is lost. The flywheel is mounted on the upper end of the rotor, below the upper radial bearing and inside the motor frame. An anti-reverse device is included in the flywheel assembly to prevent reverse rotation in the event of back flow. Prevention of back rotation also reduces motor starting time.

The motors are enclosed with water-to-air heat exchangers to provide a closed-circuit air flow through the motor. Radial bearings are of the floating pad type, and the thrust bearing is a double-acting Kingsbury type designed to carry the full thrust of the pump. A high pressure oil system with separate pumps is provided with each motor to jack and float the rotating assembly before starting. Once started, the motor provides its own oil circulation.

The bearing oil flows through a heat exchanger from which its heat is rejected to the component cooling water flow. Loss of the component cooling water flow will result in excessive oil temperature and possible bearing failure in the long term (hours).

Instrumentation is provided to monitor motor cooling, bearing temperature, winding temperature, winding differential current, and speed.

A.1.2.2 Pressurizer. The pressurizer in a pressurized water reactor (PWR) coolant system (RCS) is a large tank containing saturated water and steam. The pressurizer water space is connected to one of the reactor outlet pipes (hot legs) by the surge line, which allows a flow of water from or to the RCS during changes of reactor coolant specific volume.

In addition to providing a surge volume, the pressurizer is used to control RCS pressure and provide a rough indication of the reactor coolant inventory. The pressure in the pressurizer (and in the RCS) is controlled at a set point to maintain the reactor coolant in the RCS in a subcooled state.

During transient reductions in the reactor coolant volume, both the liquid level in the pressurizer and the RCS pressure tend to decrease. The liquid level in the pressurizer is monitored, and a decrease below the set point results in a control circuit automatically increasing the net flow rate to the RCS from the makeup and purification system (MU&P) to restore the level to its set point. The RCS pressure is also monitored, and a decrease results in a control circuit automatically energizing the pressurizer electric resistance heaters (located in the pressurizer water space). The heaters increase the temperature of the saturated water in the pressurizer, which increases the RCS pressure.

During transient increases in reactor coolant volume, set-point values will be reestablished by processes inverse to those in the paragraph above. An increased pressurizer liquid level results in a decrease in the net flow rate from the MU&P system, and increased RCS pressure results in an increase in the flow rate from the reactor inlet (cold leg) pipe to the pressurizer steam space through the spray line. The subcooled water sprayed into the steam volume condenses some of the steam, resulting in a decreased saturation temperature in the pressurizer and decreased pressure in the RCS.

Transients causing a pressure increase beyond the control capacity of pressurizer spray will result in the actuation of one or more of the three relief valves mounted on the top of the pressurizer (steam space). The pilot-operated relief valve (PORV) is opened by a control circuit if the RCS pressure set point is exceeded. If the PORV does not limit the pressure, the two spring-loaded code safety valves will open through direct action of the steam pressure on the valve seats (no control circuit is required).

A.1.2.3 Control Rod Drive Mechanisms. The function of the control rod drive mechanisms (CRDM) is to position the control rods in the core during power operation and release the control rods in response to reactor trip signals from the reactor protection system (RPS). The

69 CRDMs are divided into 4 safety banks and 4 control banks. The safety banks are held completely out of the core during power operation and are released to fall into the core on a reactor trip signal or are fully inserted into the core to achieve a controlled shutdown. The control (regulating) banks are inserted or withdrawn sequentially to decrease or increase reactor core power by the control rod drive control system (CRDCS) acting on Integrated Control System (ICS) insert or withdraw signals. Upon an RPS trip signal, the control bank control rods are released to fall into the core regardless of CRDCS or ICS control signals.

Control rods are inserted or withdrawn from the core by rotating an engaged "roller nut" around the threaded control rod lead screw. The roller nuts are both engaged and rotated in the desired direction by the application of electric power to external coils. The sequenced application of power is performed by the CRDCS in response to ICS signals, and reactor trip is accomplished by deenergizing the CRDCS in response to RPS signals. This deenergizes each of the CRDM coils, disengaging the roller nuts and allowing the control rods to fall into the core.

Three failure modes can be postulated for the CRDM and associated CRDCS: mispositioning the control rods in the core, failing to release the control rods on demand, or spuriously releasing the control rods. Of these, only the last is of interest to overcooling transients (i.e., decreasing RCS temperature, pressure, or inventory following reactor trip). Mispositioning the control rods may, at most, result in a reactor trip (release of all control rods). Failure to release one control rod following a reactor trip signal is a design basis condition analyzed in the Oconee FSAR accident analysis.[1] Failure to release more than one control rod has been analyzed in the NRC "Anticipated Transients Without Scram" Program and is beyond the scope of this study. A spurious release of one or more control rods may, at most, result in a reactor trip signal and release of all control rods.

Reactor trip is an expected condition in the context of the transients considered in this study. Although malfunctions of the CRDM or CRDCS can produce a reactor trip transient, reactor trip itself is not a transient of concern. This being so, detailed analysis of CRDM or CRDCS malfunctions is not required in the study of overcooling transients.

A.1.3 Regulation Systems

The operation of the RCS and key interfacing systems is controlled by three major instrumentation systems: CRDCS, Nonnuclear Instrumentation (NNI) and ICS. The functions of these regulating systems are described below.

A.1.3.1 Control Rod Drive Control System. The CRDCS applies power to the CRDM motors to insert or withdraw the control rods in response to commands from the control room manual control station or to automatic signals from the ICS during power operation. Additional CRDCS design information is provided in ref. 2.

Upon reactor trip, which occurs during any major reactivity transient, the CRDCS and CRDMs are deenergized and cannot influence the course of the subsequent transient. Therefore, CRDCS failure modes associated with reactor trip are not analyzed in this program. However, failure of the turbine trip auxiliary contacts located in the CRDCS cabinets is considered in the evaluation of the turbine controls.

A.1.3.2 Nonnuclear Instrumentation. The NNI is a collection of process instrument circuits used to measure, display, and alarm process variables and provide process signals to the ICS. In addition, NNI includes control circuits used to control process variables such as RCS inventory (makeup flow rate control), RCS pressure (pressurizer spray, heater, and relief valve control), and RC pump seal injection flow rate control. The NNI is described in detail in refs. 1 and 2, and the NNI control and measurement circuits are analyzed in detail as part of the analysis of fluid system-controlled components.

A.1.3.3 Integrated Control System. The principal function of the ICS is to develop coordinated control signals to regulate main feedwater (MFW) flow rate, reactor power, and steam pressure during power operation. Based on process parameter signals developed in the NNI, the ICS develops signals to modulate the MFW control valves, turbine throttle and turbine bypass valves, and control rod position to meet existing electric power demand and RCS operating limits.

Following reactor and turbine trip, the ICS continues to modulate the FW control valves to maintain the SG water level and the turbine bypass valves to maintain steam line pressure. Either of these functions can have significant influence on RCS overcooling, and for this reason the ICS control circuits are analyzed in detail as part of the analysis of fluid system-controlled components. The ICS functions and circuitry are described in detail in refs. 1 and 2.

A.1.4 Makeup and Purification System

The functions performed by the Oconee HPI, coolant storage, coolant treatment, and chemical addition systems are sequential and complementary. The equipment in these systems has been grouped into a general MU&P system.

The MU&P system consists of the piping and process equipment required to remove, process, and replace reactor coolant at the flow rates required to maintain constant RCS coolant volume. The major functions performed by the MU&P system are as follows:

1. Letdown control: Controlled removal of reactor coolant from the RCS and reduction of coolant temperature and pressure at a preset flow rate.

2. Purification: Removal of impurities from the reactor coolant using boric acid-saturated ion exchange resins.

3. Coolant processing and chemical addition: Recovery of concentrated boric acid and demineralized water from letdown reactor coolant; supply of demineralized (boric acid-free) water and concentrated boric acid to adjust reactor coolant boric acid concentrations; and supply of lithium hydroxide to control reactor coolant pH.

4. RC pump seal return: Collection, filtering, and cooling of coolant flowing past the RC pump shaft face seals.

5. RC pump seal injection: Injection and filtering of processed letdown coolant to the RC pump shaft seals at a constant flow rate.

6. RC makeup: Injection of processed letdown coolant to the RCS at a flow rate controlled to maintain constant reactor coolant volume (coolant pressurizer level).

In addition to the normal functions performed by the MU&P system, portions of the system are used to provide emergency injection of coolant following design basis plant accidents.

A.2 POWER CONVERSION SYSTEMS DESCRIPTIONS

The power conversion systems are designed to convert heat produced in the reactor to electrical energy.

The superheated steam produced by the SGs is expanded through the high pressure turbine and then reheated in the moisture separator reheaters. The moisture separator section removes the moisture from the steam, and the two-stage reheaters superheat the steam before it enters the low pressure turbines. The steam then expands through the low pressure turbines and is exhausted into the main condenser, where it is condensed and returned to the cycle as condensate. The heat rejected in the main condenser is removed by the condenser circulating water system.

The first-stage reheaters are supplied with steam from the A bleed steam line, and the condensed steam is cascaded to the B FW heaters. The second-stage reheaters are supplied with main steam, and the condensed steam cascades to the A FW heaters. Heat for the FW heating cycle is supplied by the moisture separator reheater drains and by steam from the turbine extraction points.

The hotwell pumps take suction from the condenser hotwell and pump the condensate through the condensate polishing demineralizers. Downstream of the polishers, the condensate flows through the condensate coolers, generator water coolers, hydrogen coolers, condenser steam air ejectors, and the S.P.E. steam seal condenser to the suction of the condensate booster pumps. The condensate booster pumps in turn pump the condensate through three stages of intermediate pressure FW heaters (F, E, and D). The flow combines with the D heater drain pump discharge before entering the C FW heaters and then divides to provide input flow to the suction of each of the SG FW pumps. The steam turbine-driven MFW pumps deliver FW through two stages of high pressure FW heaters (B and A) to a single FW distribution header, from which the FW flow is divided into two lines to the SGs.

Brief descriptions of the power conversion systems are provided in the following sections.

A.2.1 Steam Generator

The SG is a vertical, straight tube, tube and shell heat exchanger that produces superheated steam at constant pressure over the power range. Reactor coolant flows downward through the tubes and transfers heat to generate steam on the shell side. The high pressure (reactor coolant pressure) parts of the unit are the hemispherical heads, the tube sheets, and the tubes between the tube sheets. Tube support plates maintain the tubes in a uniform pattern along their length. The unit is supported by a skirt attached to the bottom head.

The shell, the exterior surface of the tubes, and the tube sheets form the boundaries of the steam-producing section of the vessel. Within the shell, the tube bundle is surrounded by a cylindrical baffle. Openings in the baffle at the FW inlet nozzle elevation provide a path for steam to afford contact FW heating. The upper part of the annulus formed by the baffle plate and the shell is the superheat steam outlet, while the lower part is the FW inlet heating zone.

FW is heated to saturation temperature by direct contact heat exchange. During normal power operation, FW is sprayed into the downcomer annulus formed by the shell and the cylindrical baffle around the tube bundle. Steam is drawn by aspiration into the downcomer and heats the FW to saturation temperature.

The saturated water level in the downcomer provides a static head to balance the static head in the boiling section of the SG. The downcomer water level varies with steam flow from 15 to 100% load. A constant minimum level is held below 15% load.

The saturated water enters the tube bundle just above the lower tube sheet, and the steam-water mixture flows upward on the outside of the tubes countercurrent to reactor coolant flow. The vapor content of the mixture increases almost linearly along the tubes to produce saturated steam.

Saturated steam is raised to final temperature in the superheater region. The amount of surface available for superheat varies inversely with load; as load decreases, the superheat region gains surface from the nucleate and film boiling regions. Mass inventory in the SG increases with load as the lengths of the heat transfer regions vary. Changes in temperature, pressure, and load conditions cause an adjustment in the length of the individual heat transfer regions and result in a change in inventory requirements. If the inventory is greater than required, the pressure increases. Inventory is controlled automatically as a function of load by the FW controls in the ICS.

In the event of MFW pump trip, the emergency feedwater (EFW) system injects FW into the EFW spray header located near the top of the SG. MFW flow also may be injected through the EFW header by valve realignment. This action enhances natural circulation of reactor coolant when the reactor coolant pumps are tripped or deenergized.

Figure A.1 is an outline sketch of the thermohydraulic aspects of the PWR system of the Oconee plant, much of which would apply to any B&W PWR system. Generally, the lower half of the diagram along with the secondary sides of the SGs is the FW system. Feed comes from the condensate, through the FW pumps, into a common header. It is then split into loop A and loop B flow. Each loop contains a startup valve and a MFW valve in parallel. A flowmeter in the startup leg is sensitive to low flows, and downstream beyond where the two legs come together is a flowmeter receiving the combined flow through both valves. This meter may be relatively inaccurate at low flows.

A.2.2 Feedwater System

A.2.2.1 Operating Controls. Control of the FW system is provided through MFW and startup valves and FW pump speed. The following sensed signals are sent to the ICS and there processed to produce control signals for the FW system:

1. FW flow measures, both loops
2. Level indicators (startup and operating), both SGs
3. FW temperature, both SGs
4. Temperature difference between cold legs in the primary system
5. Turbine header pressure signal
6. Neutron error signal
7. RC hot-leg temperature
8. RC flow
9. SG outlet pressure
10. RC average temperature error
11. Pressure drops across FW valves

In maintaining total FW flow equal to total FW demand, the FW control subsystem manipulates two startup valves, two main valves, and two pumps. The FW control includes the following considerations, each of which will be discussed in detail (all references to points and blocks are on Fig. A.2):

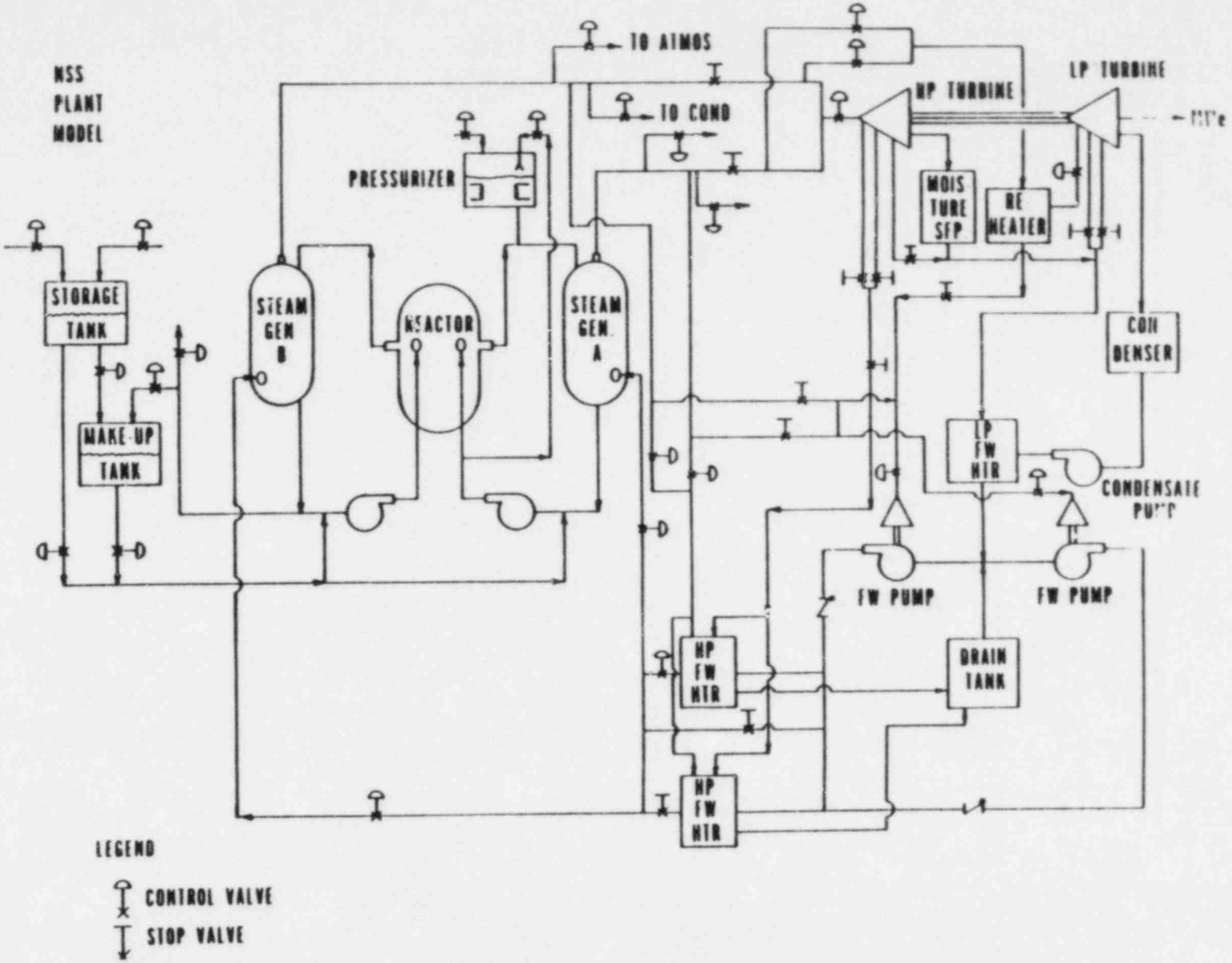
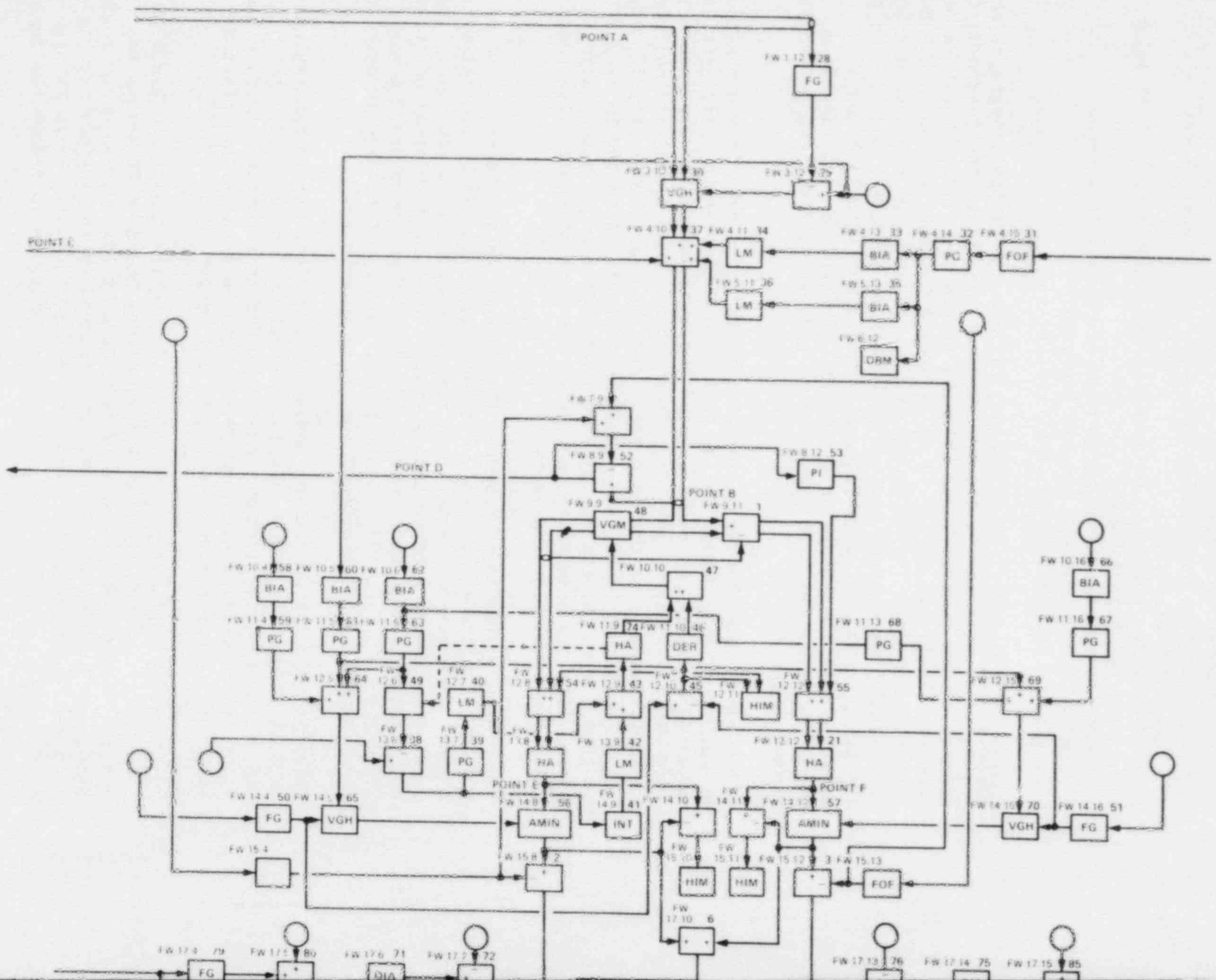
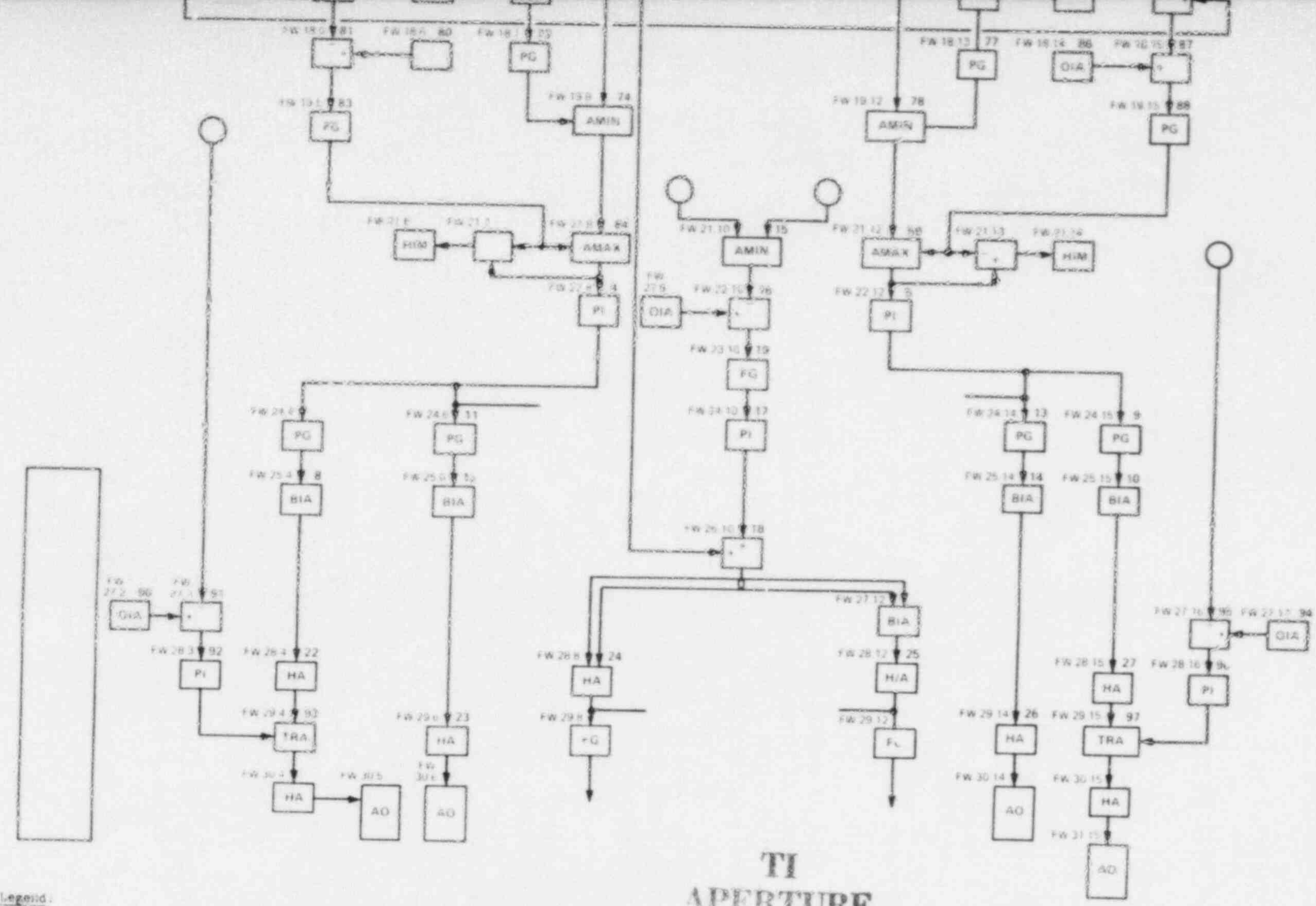


Fig. A.1. Simplified schematic diagram of a nuclear power plant.

ORNL DWG 84 7839





Legend:

AMAX - select maximum	HIM - high signal monitor
AMIN - select minimum	INT - integrator
AO - analog out	LM - low signal monitor
BIA - bias	OIA - operator input analog
DBM - deadband monitor	PG - proportional gain
DER - derivative	PI - proportional integral controller
FG - function generator	TRA - transfer
FOF - first-order filter	VGM - variable gain multiplier
FW - feedwater	
HA - hand/auto station	

Fig. A.2. Schematic diagram of the Oconee-1 steam generator control system.

normal control mode
FW temperature compensation
high and low cross limits with the reactor power level
T_{avg} control to FW
correct FW flow ratio between the two SGs for control of inlet reactor temperatures
total flow control on large reactor coolant flow error
minimum SG superheat limits (degrees)
minimum and maximum SG level limits

Normal control mode: In this mode, FW demand from the integrated master (Point A) is used for feedback control of the valves and feedforward control of the pumps. Under balanced system conditions, total FW demand from the integrated master is split evenly between FW loops A and B (Point B and Block 1). Measured FW flow to each SG is compared with individual loop demand; individual FW errors (Blocks 2 and 3) then pass through proportional plus integral controllers (Blocks 4 and 5) to establish the control valve positions. Individual loop demands are summed together (Block 6) and used to generate a feedforward pump speed demand signal.

Operation of the startup valve and main valve in each loop are sequenced. Normally, as loop demand varies from 0 to 15%, startup valve gain is adjusted to cause the startup valve position demand to vary from 0 to 100% (Blocks 7, 8, 9, and 10). Then, as the loop demand varies from 15 to 100%, the gain on the main valve and the bias (Blocks 11, 12, 13, and 14) are adjusted to cause the main valve position demand to vary from 0 to 100%. When the startup valve becomes 80% open, a block valve in series with the main valve is opened; when the start-up valve becomes 50% closed, the blocking valve is closed.

The minimum pressure drop across the control valves is selected (Block 15) and used to form a feedback signal to the FW pump speed demand. The minimum pressure drop is compared with a set point, the resulting error passed through a proportional plus integral controller, and the feedback demand added to the feedforward pump speed demand (Blocks 16, 17, and 18). The feedback gain for the valve pressure drop error varies with the size of the error (Block 19).

FW demands for each loop are passed through loop master hand/automatic (H/A) stations (Blocks 20 and 21) so that the operator has the capability of establishing a manual FW demand for either or both loops. Valve position and pump speed demands can be manually specified for all actuators from H/A stations (Blocks 22 through 27).

Feedwater temperature compensation: A function generator (Block 28) is used to compute the desired FW temperature based on FW demand and exit conditions required on the secondary side of the SG. An error signal based on the difference between the desired FW temperature and the measured FW temperature (Block 29) is used to modify total FW demand (Block 30). The purpose of this modification is to reduce the demand on the primary side of the once-through steam generator (OTSG) while maintaining the desired exit conditions. Thus, when FW temperature varies from that demanded by the function generator, a correction to the total FW flow demand is applied. The correction to the total FW demand is applied in such a direction as to maintain the outlet SG temperatures at the values desired, modifying flow demand as a function of FW temperature.

Cross limits with reactor: Cross limits are used to maintain FW flow percentage within a certain ratio of reactor power percentage (Blocks 31 through 36). Whenever measured neutron power differs more than 5% from neutron power demand, a correction is made to increase or decrease FW flow demand accordingly. For instance, if the neutron power error is -7%, the cross limits will cause FW flow demand to be decreased by 2% (Blocks 23 and 34); if the neutron power error is 6%, the cross limits will cause FW flow demand to be increased by 1% (Blocks 35 through 36).

T_{avg} control to feedwater: Under certain conditions, the reactor control subsystem cannot control reactor coolant average temperature (T_{avg}). One such condition is when the reactor H/A station is in manual. When the reactor control subsystem cannot control T_{avg}, T_{avg} control is transferred to the FW control subsystem. When this occurs, the T_{avg} error is operated on by a proportional plus integral controller (Point C), and the resulting feedback demand is summed with the feedforward total FW demand (Block 37).

Plant conditions that would prevent FW control from accepting the T_{avg} control are (1) both SGs meeting level limits, (2) either SG on a Btu limit, or (3) both FW H/A master stations in manual.

Delta-T_C control: To ensure uniform reactor inlet temperature distribution, the FW control ratios the two FW loop flows to maintain the temperature of the reactor coolant in cold leg A equal to the temperature of the reactor coolant in cold leg B. This may be expressed as $T_{CA} = T_{CB}$, or $\Delta T_C = T_{CA} - T_{CB} = 0$. Rationing FW flow between the two SGs to control reactor inlet temperature is referred to as ΔT_C control. Both reactor coolant cold-leg temperature measurements and reactor coolant flow measurements are used in implementing feedback control of ΔT_C. A variable gain is modified by the ΔT_C feedback control signals and applied to loop A FW demand (Block 48). The loop A demand is then subtracted from the total demand (Block 1) to create the loop B demand modified by ΔT_C feedback.

The ΔT_C set point is normally entered as zero (Block 49). A proportional gain, a calibrating integral, and high/low limiters operate on the cold-leg temperature difference ΔT_C error (Blocks 38 through 43). Both the proportional and calibrating integral actions are blocked if either FW loop H/A station is in manual or if either SG is on level limit. The calibrating integral action only, and not the proportional action, will be blocked if the megawatt electric demand is changing faster than a specified rate or if a reactor coolant flow transient exists. A ΔT_C H/A station (Block 44) may be used to replace the demand created by ΔT_C feedback error with manual ratioing of FW flow demands.

There are four reactor coolant pumps, two operating in parallel in each loop. If an imbalance in primary flows through the SGs exists, as when the number of reactor coolant pumps running in each of the two primary loops is not equal, ΔT_C will deviate from zero unless the FW flows are ratioed properly. To aid in maintaining ΔT_C equal to zero in this situation, derivative and proportional control actions are used to operate on the difference between reactor coolant flows (Blocks 45 and 46, 50, and 51). Feedbacks due to ΔT_C error and primary loop flow imbalance are summed (Block 47) to create the variable gain applied to loop A FW demand (Block 48).

Total flow control: If reactor coolant flow error becomes greater than 10% (Point D), the total FW flow error passed through a proportional plus integral controller is used to modify each of the individual loop demands (Blocks 52 through 55). The effect of this controller is modified by conditions in the following manner: If both reactor coolant pumps on one loop are tripped, the controller output is bled to 0% with a 60-s time constant. If SG A is on low level control and SG B is on manual control, the output of the total flow controller due to integral action is held constant. The same output will occur if the roles of A and B are reversed as well as when both SGs are on low level control.

Btu limits: To ensure steam with a minimum specified number of degrees superheat [usually 19.4°C (35°F)], Btu limit calculations are implemented. Btu limits are the maximum allowable FW flow demands for each loop. A low auctioneer is used in implementing the Btu limits in each loop (Blocks 56 through 57). FW flow demands higher than the Btu limit would result in the degrees superheat at the outlet of the SG falling below the minimum specified.

Btu limit calculations are based on measurements of reactor coolant flow, primary coolant temperature at the reactor outlet, FW temperature, and SG outlet pressure (Blocks 58 through 70). These variables are used to determine the amount of energy available from the SG at the desired steam temperature. If the normal FW demands (Points E and F) are calling for the removal of more energy from the SGs than is available for the desired steam temperature, the Btu limits override the normal FW demands.

A.2.2.2 Level Limits and Sensors: Low and high level limits are imposed on the operation of the SGs. In high level limit control, a low auctioneer is used to compare FW flow error against an appropriately gained operate level error signal, and the minimum error signal is passed on to the valve control (Blocks 71 through 78). In low level limit control, a high auctioneer is used to compare FW flow error against an appropriately gained startup level error signal, and the maximum error signal is passed on to the valve control (Blocks 79 through 89).

Note that this is not level control, that no attempt is made to maintain a set level; the limits simply give assurance that the level remains between preselected high and low points. Note further that a low level error signal, if present, will dominate.

Figure A.3 shows a schematic diagram of the Oconee 1 SG, water level sensing pressure taps (labeled A-A', B-B', D-D', and E), the MFW and auxiliary feedwater (AFW) ΔP cells associated with the A, B, and D taps, and the valves and pipes that connect the taps to the cells. An identical set of valves, cells, and pipes is associated with taps A', B', and D'. Referenced from the bottom tube sheet as 0, the tap heights are A-A', 6 in.; B-B', 102 in.; D-D', 394 in.; and E, 606 in.

The operator selects one group of taps, A-B-D or A'-B'-D', which will have its sensed signals sent to the ICS and the control room display. Tnis is called the "selected" set.

The path from each pressure tap to the (normally open) blocking valves is open as shown (Fig. A.3), clear of obstructions or other valves. When the water level is above a tap it flows into the connecting pipe. When the water level is below tap D or D' (as it is normally), the pipe from that tap is filled to tap level by evaporation from the SG and condensation in the pipe. D (D') is the reference tap, and the water in it is maintained in this manner at height D-D'.

The failure possibilities are noted below for this arrangement of sensing equipment. Each of these failures, in addition to sending misinformation to the control system, would send misinformation to the control room display. This misinformation would be inconsistent with other information available in the control room display, and the failure would be undetected until the operator observes the inconsistency and deduces its cause.

1. A sufficient leak in the selected A-A' tap or the connecting pipe, or in the packing of the blocking valves between the tap and the corresponding AFW or MFW ΔP cell, can cause an apparent drop in the sensed low level of the SG and bring on an overriding requirement to increase FW flow. This misinformation would go to both AFW and MFW controls.

2. A sufficient leak in the selected B-B' level tap or connecting pipe, or packing if the terminating blocking valves will similarly cause the operating level (or high level) sensing equipment to sense a lower level than is actually present. This failure can defeat both high level protection systems--the high level MFW pump trip and the high level control valve closure.

3. Failure of the selected B-D (B'-D') MFW ΔP cell so that it reads low when the level is high will also defeat both high level protection systems.

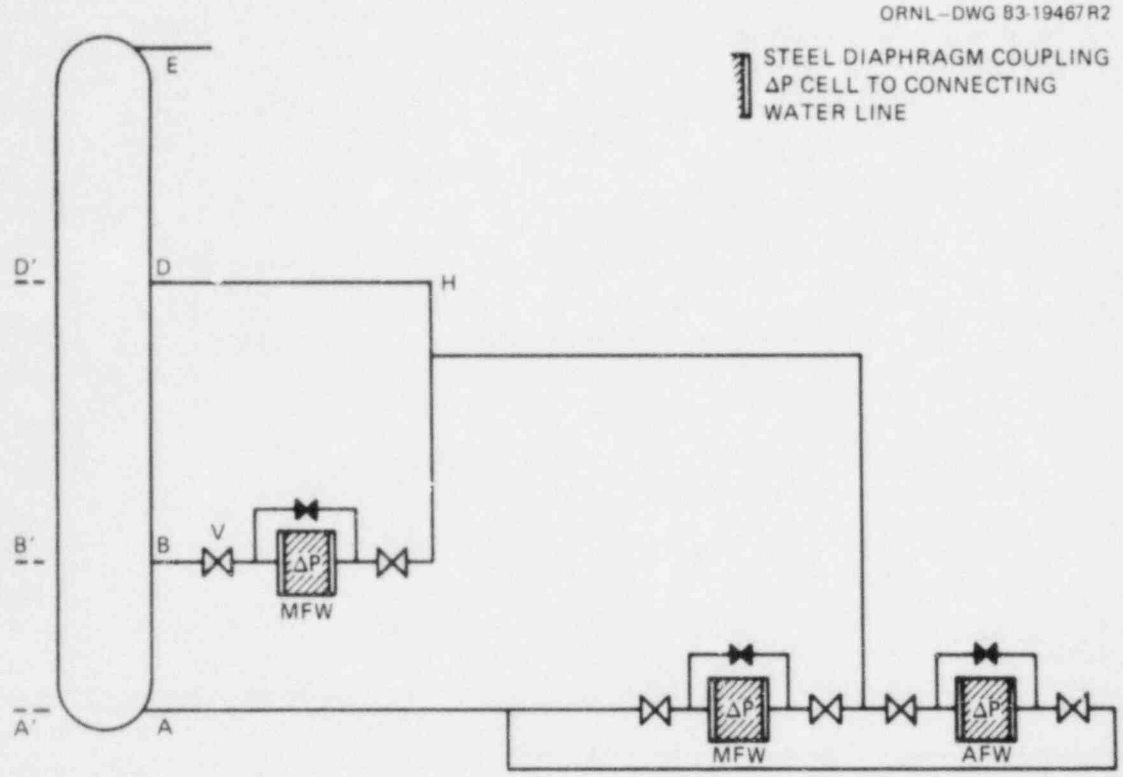


Fig. A.3. Schematic diagram of steam generator pressure taps and Δp cells.

4. The blocking valve in the selected set (marked V in Fig. A.3), if failed into a closed position during operation, will isolate the B-D MFW ΔP cell from sensing any further pressure changes at the B-level tap. The other side of the cell "sees" the water column from the D level. This should remain essentially invariant until the water level exceeds the D level. At that point the cell should "see" a relative increase in the D over the B level, or, equivalently, a decrease in the B under the D level. This should be interpreted as a falling water level. Hence, this failure also defeats the two high-level protection systems.[3]

A.2.2.3 High Level Main Feedwater Pump Trip Circuitry. Figure A.4 is a schematic diagram of the circuit transmitting SG high level sensed signals to the high level MFW pump trip and alarm. The following failures can place this system in an undetected failed state.

1. For purposes of high level MFW pump trip and high level alarm, the signals from both B-D and B'-D' are used. The signals B-D and B'-D' from SG A (Fig. A.3) go respectively to contacts 2A and 3A (Fig. A.4); similarly, B-D and B'-D' from SG B go to 2B and 3B. Note that if either 2A or 3A is in a failed open condition, SG A cannot cause a high level MFW pump trip. Trips from SG B are similarly blocked if either 2B or 3B is failed open.

ORNL-DWG 84 8479

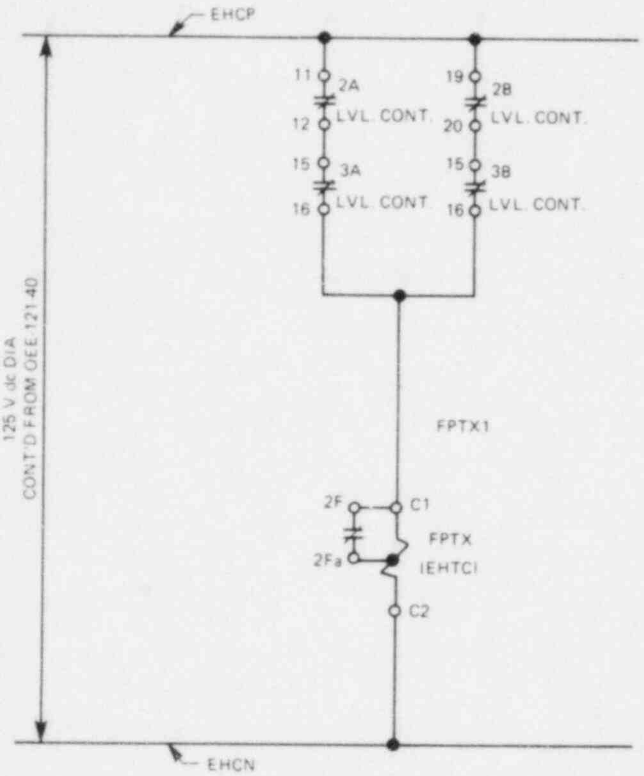


Fig. A.4. Main feedwater pump high-level trip circuit.

2. If the relay FPTX is failed open, all high level MFW pump trips from whatever source are blocked.

The circuitry shown in Fig. A.4 is not part of the ICS. Hence, failures within this circuitry will not fail protective features such as the high level MFW control valve closure, which are operated from the ICS.

This circuitry is routinely tested during refueling.

A.2.2.4 Further Details of System Description. In order to follow the scenario descriptions presented, some further understanding of system detail is necessary.

1. The detectors on the SGs are considered to be level detectors but, in fact, are not; they are detectors of differential pressure. The confusion is somewhat compounded because the low-level instrumentation, at least, is calibrated to read differential pressure in units of inches of water. The use of differential pressure as a level indicator is straightforward when the gravitational term is dominant. In an active flow region like the SGs, which are two-phase flow devices, the flow terms are not only

important--they dominate. The relation between level (if, indeed, a level can be defined) and differential pressure is heavily flow dependent. Hence, even if a differential pressure detector were calibrated to some arbitrarily defined equivalent level during normal operations, the strong flow variations that accompany many transients would cause the calibration to be of no value during the transient or other off-normal condition.

2. Discharge from the high-pressure turbine goes to a moisture separator. When the liquid level indication in the moisture separator exceeds a set point, the turbine trips automatically. This is an approximate trip on low steam quality, although the set point-quality relationship is probably power dependent.

3. Turbines of the kind that drive the MFW pumps are customarily supplied by the manufacturer with built-in trips as protection against excessive thrust or excessive vibration. These undesirable mechanical conditions can be expected to be brought on by, among other things, an excessively low steam quality. Hence, they may be regarded roughly as steam-quality trips.

The kernel of B&W's ICS has three major loops coupling megawatt demand with turbine, FW, and reactor control plus pressurizer controllers. Simulation is complicated by feedforward signals, direct cross coupling of loops, and many rate and magnitude limiters that restrict loop functions or that reorganize portions of loops under prescribed conditions. These nonlinearities are typically excited during off-nominal or upset conditions. Since it is the intent of this study to investigate such conditions, it was necessary to reproduce the ICS in considerable detail.

A.2.3 Main Steam and Turbine Bypass System

Main steam is generated in the two SGs by FW absorbing heat from the RCS. Main steam is conveyed to the turbine inlet valves by two lines, one from each SG. A pressure equalization and steam distribution header is connected to each main steam line upstream of the turbine inlet valves.

Eight spring-loaded safety valves are located on each main steam line (a total of sixteen) to prevent overpressurization of the main steam system under transient conditions. The valves, designated MS-1 through MS-16, are designed to pass 105% of the design steam flow at a pressure not exceeding 110% of the system design pressure (1050 psig).

The turbine bypass system (TBS) is designed to reduce steam line pressure following large turbine load reductions by dumping main steam directly to the main condenser. Two turbine bypass valves, MS-19 and MS-22, release steam from the A steam line; valves MS-28 and MS-31 release steam from the B steam line to the main condenser shells. Steam supply piping from each turbine bypass header feeds the startup steam header. Check valves are installed to prevent cross flow between the main steam lines.

High pressure steam supply piping provides steam for each MFW pump turbine following main turbine trip. In addition to an isolation valve in each line, the steam flow to each turbine is controlled by a governor and stop valve separate from the governor and stop valves controlling low pressure bleed steam flow. The high pressure governor and stop valves are designated MS-41 and 40 and MS-44 and 43 for FW pump turbines A and B respectively. In addition to the steam supply to FW pump turbine B, the steam header from main steam line B supplies the three condenser steam air ejectors.

Separate lines are installed to supply high pressure steam from the two main steam lines to the two reheaters. The two main steam lines supply the EFW pump turbine. Check valves are installed to prevent cross flow between the main steam lines through the EFW pump turbine header.

Each of the supply headers off the main steam lines can be isolated by motor-driven isolation valves. Although not described, the branch steam piping has numerous steam traps in operation to remove condensate and normally isolated drain lines.

A.2.4 Turbine Generator System

The turbine generator system converts the thermal energy of steam produced in the SGs into mechanical shaft power and then into electrical energy. The Oconee turbine generator system normally is operated with an electrical power output of 866 MW, but may be operated with reduced power output when required. Each unit's turbine generator consists of a tandem (single-shaft) arrangement of a double-flow high-pressure turbine and three identical double-flow low pressure turbines driving a direct-coupled generator at 1800 rpm.

Main steam from the SGs is directed to the high pressure turbine through four parallel stop valves and four parallel control valves. After expanding through the high pressure turbine, the exhaust steam passes through external moisture separators and two-stage steam-to-steam shell and tube type reheaters. Extraction steam from the high pressure turbine is supplied to the first reheater stage tube bundle in each reheater, and main steam is supplied to the second reheater stage tube bundle in each reheater. Reheated steam is admitted to the three low pressure turbines and expands through the low pressure turbines to the main condensers.

Part of the steam expanding through the turbines is extracted at selected points (pressures) to heat the FW pumped to the SGs. The A (highest pressure), B, and C FW heaters are supplied from the high pressure turbine (or its exhaust). The A bleed line also supplies the first-stage reheater. The D, E, and F FW heaters are supplied from the low pressure turbines. The D bleed lines also supply the MFW pump turbines during power operation.

Turbine generator functions are monitored and controlled automatically by the turbine control system (TCS). The TCS regulates the electric power production rate of the turbine generator based on power demand signals from the ICS. The TCS also includes redundant mechanical and electrical trip devices to prevent excessive overspeed of the turbine generator. Additional external trips are provided to ensure operation within conditions that preclude damage to the turbine generator. A standby manual control system is also provided for use if the automatic control system is not available.

Based on turbine, generator, or condenser parameters exceeding limits, or on loss of power to the turbine trip circuits or reactor trip auxiliary contacts in the CRDCS, the TCS develops trip signals to deenergize trip solencid valves. These valves depressurize turbine hydraulic controls and result in closing the four high pressure turbine stop valves, the four high pressure turbine governor valves, and the six low pressure turbine intercept valves. In addition, low hydraulic system pressure signals are sent to the RPS to trip the reactor upon turbine trip.

A.2.5 Condenser

The condenser is designed to condense turbine exhaust steam for reuse in the steam cycle. The condenser also serves as a collecting point for various steam cycle vents and drains to conserve condensate from a number of sources, all of which is stored in the condenser hotwell. The condenser also serves as a heat sink for the TBS and is capable of handling 25% of rated main steam flow. Rejected heat is removed from the main conden by the condenser circulating water system.

The condenser consists of three surface type deaerating condenser shells, with each shell condensing the exhaust steam from one of the three low pressure turbines. The condenser shells are conventional shell and tube design, with steam on the shell side and circulating water in the tubes. A low pressure FW heater is mounted in the neck of each of the three condenser shells. The combined hotwells of the three condenser shells have a water storage capability equivalent to approximately 10 min of full load operation (nominally 142,000 gallons). The condenser provides for condensing steam, scavenging and removing noncondensible gases, and deaerating the condensate. Impingement baffles are provided to protect the tubes from incoming drains and steam dumps.

The condenser can accept a bypass steam flow of ~18% of rated main steam flow without exceeding the turbine high backpressure trip point with design inlet circulating water temperature. This bypass steam dump to the condenser is in addition to the normal duty expected.

The condenser evacuation subsystem is designed to remove noncondensible gases and air inleakage from the steam space of the three shells of the main condenser. It consists of the condenser steam air ejector subsystem and the main vacuum subsystem.

The condenser steam air ejector (CSAE) subsystem consists of three CSAEs per unit. Normally, each CSAE draws the noncondensible gases and water vapor mixture from one of the three main condenser shells to the first air ejector stage. The mixture then flows to the intercondenser, where it is cooled to condense the water vapor and motive steam. The second air ejector stage draws the uncondensed portion of the cooled mixture from the intercondenser and compresses it further. The compressed mixture then passes through the aftercondenser, where it is cooled and more water vapor and motive steam are condensed. The intercondenser drains back to the main condenser, and the aftercondenser drains to the condensate storage tank.

The main vacuum subsystem consists of three main vacuum pumps connected to the condenser crossties on the CSAE subsystem to allow the main vacuum pumps to evacuate the main condenser, the main turbine casing, and the upper surge tanks during startup. These pumps are used only during startup; normal operation requires the use of only the CSAE.

A.2.6 Condensate and Feedwater System

The condensate and feedwater system purifies, heats and pumps the condensate from the condenser hotwells to the two SGs to complete the steam-FW cycle.

Three hotwell pumps normally are in operation to pump the condensate from the three condenser shell hotwells to the condensate booster pumps. From the hotwell pumps, a portion of the condensate normally flows through four of the five polishing demineralizers. The flow is controlled by automatically regulating the pressure drop across the demineralizer bypass valve (C-14). Ammonia and hydrazine are added to the condensate downstream of the demineralizers to control pH and reduce oxygen concentration.

The condensate flows through the hydrogen coolers and generator water coolers in parallel. Flow through the generator water and hydrogen coolers is controlled automatically by bypass valve C-81 to regulate the pressure drop across the coolers. The flow through the hydrogen coolers is controlled independently by control valve C-58 to regulate hydrogen temperature. The condensate flows through the three condenser steam air ejector coolers to the suction of the condensate booster pumps.

Two of the three condensate booster pumps normally operate to pump the condensate through the low pressure FW heaters to the MFW pumps. The condensate is heated in four stages of low pressure FW heaters: F, E, D, and C. Three parallel F heaters heat the condensate by condensing steam from the three low pressure turbines. The E, D, and C heaters are arranged in two parallel flow paths; the E and D heaters condense extraction steam from the low pressure turbine, and the C heaters condense extraction steam from the high pressure turbine.

From the low-pressure heaters the condensate flows to the two MFW pumps. The flow rate through the two FW pumps is controlled by the two MFW control valves based on reactor/turbine demand. To increase the efficiency of the pumps, the pressure drop across the FW control valves is limited to 35 psi by regulating the speed of the FW pumps. Under conditions of low flow demand with the control valves closing, the increasing pressure drop is measured and the pump spced demand signal from the ICS is reduced. The resulting lower pump speed results in a decreased pressure drop across the valves. In addition to the pump speed and FW flow rate controls, the minimum flow through each pump is limited to ~2500 gpm to protect the pumps. Lower flow rates measured in the pump suction lines result in automatic opening of the bypass valves that divert FW from the pump discharge lines to the upper surge tank.

From the FW pumps, the water (which may at this point be termed FW) flows through the two parallel B high pressure FW heaters and two parallel A high pressure FW heaters. The FW is heated to its final temperature in the FW heaters, which condense extraction steam from the high pressure turbine. Downstream of the common line from the AFW heaters, the flow divides into two lines that individually feed the two SGs.

The equipment described above makes up the main flow path from the condensers to the two MFW lines. However, the main flow rate pumped from the condenser hotwells (normal flow rate: 6.6×10^6 lbm/h) is approximately one-half that delivered to the two SGs (normal flow rate: 11.3×10^6 lbm/h). The balance of the flow is pumped into the condensate and FW lines by the heater drain system. The extraction steam condensed in the steam reheaters and the high and low pressure FW heaters is collected and pumped into the condensate lines at points of comparable temperature.

The heated FW flows to the two main SGs through the two MFW lines. The flow rate in each normally is controlled by the FW control valves, FDW-32 and FDW-41, which are positioned based on FW demand signals developed in the ICS. At low flow conditions, the MFW control valves and the MFW block valves, FDW-31 and FDW-40, located in series with the control valves, are closed on automatic control signals from the ICS. Under these conditions, the FW sources fcr the two SGs bypass the main control and block valves, and are controlled by the two startup FW control valves, FDW-35 and FDW-44, which are positioned based on automatic control signals from the ICS. Downstream of the FW control valves, the two FW lines penetrate the reactor building and inject the FW into the SGs through the MFW ring headers.

As described above, the FW flow rate is controlled by ICS control signals to the main and startup FW control valves. During power operation, the FW flow rates to the two SGs are controlled principally to maintain constant and equal average reactor coolant temperatures in the two reactor coolant loops over the range of power production rates from ~15 to 100% full power. The control signals are modified as functions of SG heat balances (Btu limits), the status of key plant equipment (e.g., turbine trip, RC pump trip) and SG level limits. The FW control valve demand signals are limited based on high SG level as measured by pressure drops in the SG. Exceeding the high level control limit in either SG will result in ICS-generated signals tripping the MFW pumps.

As reactor pcwer decreases below ~15% full power, the FW demand required to maintain reactor coolant average temperature results in a SG level less than the minimum level control limit. As a result, FW demand is controlled to maintain the minimum SG level (~30 in.), allowing the reactor coolant average temperature to decrease over the reactor power range from 15 to 0% full power.

As FW demand decreases, the main control valves and then the startup control valves will be closing. As the startup valves close to a position more than 50% closed (based on measured valve positions), signals will be generated to close the MFW block valves. These valves are closed to prevent possible leakage through the main control valves from interfering with control of the startup valves. The block valves are opened automatically when the startup valves are positioned more than 80% open.

Following reactor trip, the FW flow rate is controlled to maintain SG levels of ~30 in. with one or more RC pumps in ^peration. If all four RC pumps are tripped, the ICS automatically increases the minimum level set point to ~20 ft to maintain the desired rate of natural (convective) circulation of reactor coolant through the core.

A.3 PROCESS AUXILIARY SYSTEMS

Process auxiliary systems include those systems and subsystems that support the operation of the nuclear system and the power conversion systems. The major control systems are:

W03 - Reactor building component cooling water
W04.A - Condenser circulating water
W04.D - Recirculated cooling water

Brief descriptions of these systems are provided in the remainder of this section.

A.3.1 Reactor Building Component Cooling Water

This system is designed to provide cooling water for various components in the reactor building including the letdown coolers, reactor coolant pump cooling jacket and seal coolers, quench tank cooler, and control rod drive cooling coils. The design cooling requirement for the system is based on the maximum heat loads from these sources. The system provides an additional barrier between high pressure reactor coolant and service water to prevent an inadvertent release of activity.

Following is a brief functional description of the three major components of the system.

1. Component Cooler. Each component cooler is designed for the total system heat load for one reactor unit. Oconee 1 and 2 each have a single component cooler with a shared common spare; Oconee 3 has two coolers. The coolers reject the heat load to the low pressure service water (LPSW) system.

2. Component Cooling Pumps. Each component cooling pump is designed to deliver the necessary flows to the letdown coolers, reactor coolant pump cooling jackets and seal coolers, quench tank cooler, and rod drive cooling coils. Each unit has one operating pump and one spare.

3. Component Cooling Surge Tank. This tank allows for thermal expansion and contraction of the water in the closed-loop system. It also provides the required suction head for the component cooling pumps.

During operation, one component cooling pump and one component cooler recirculate and cool water to accommodate the system heat loads for each reactor unit. The component cooling surge tank accommodates expansion, contraction, and leakage of coolant into or out of the system. The surge tank also would provide a reservoir of component cooling water until a leaking cooling line was isolated. Makeup water and corrosion-inhibiting chemicals are added to the system in the surge tank.

A.3.2 Condenser Circulating Water (CCW)

The Little River arm of Lake Keowee is the source of water for the CCW systems. Each unit has four CCW pumps supplying water via two 11-ft conduits into a common condenser intake header beneath the turbine building floor. The discharge from the condenser is returned to the Keowee River arm of Lake Keowee.

The intake of the condenser circulating pumps extends below the maximum drawdown of the lake. The intake structure is provided with screens that can be removed manually for periodic cleaning.

The CCW systems are designed to take advantage of the siphon effect so that the pumps are required only to overcome pipe and condenser friction loss. The siphon is initiated at startup by plant vacuum pumps and sustained during operation by continuous-priming vacuum pumps.

The CCW system has a 48-in. emergency discharge line to the Keowee hydro tailrace. This discharge is connected to each of the three condensers of each unit. Under a loss-of-power situation, the emergency discharge line will open automatically and the CCW system will continue to operate as an unassisted siphon system supplying sufficient water to the condenser for decay heat removal and emergency cooling requirements. The vacuum is sustained by steam air ejectors.

A.3.3 Recirculated Cooling Water (RCW)

This system provides inhibited closed-cycle cooling water to various components outside the reactor building including the following:

RC pump seal return coolers
Spent fuel cooling
Sample coolers
Evaporator systems
Various pumps and coolers in the turbine building
Instrument air compressors.

The RCW system consists of four motor-driven pumps and four RCW heat exchangers to supply cooling water service to the three Oconee units. A 25,000-gallon surge tank accommodates temperature changes and leakage. Condenser circulating water is used to cool the RCW heat exchangers.

RCW effluent from the auxiliary building is monitored for radioactivity. The monitors will detect leakage of radioactive fluids from any of the coolers in the auxiliary building. Separate monitors are provided on the return lines from the Oconee 1 and 2 auxiliary building and the Oconee 3 auxiliary building.

During normal operation of the three Oconee units, three RCW pumps and three RCW heat exchangers will be in service. One pump and one heat exchanger are installed as spares common to the three units.

A.4 DESCRIPTION OF THE OCONEE-1 PNEUMATIC SYSTEM

A.4.1 System Purpose and Design Basis

The purpose of the compressed air system is to provide dry, oil-free air as needed throughout the plant to pneumatic valves and instruments (instrument air), and to various outlets for tools and miscellaneous uses (service air).

The air compressors provide air at a pressure of 100 psig, with pressure reduced as necessary for the various service requirements.

A.4.2 System Description

The compressed air system at the Oconee Nuclear Station is one large, integrated system that supplies instrument and service air to all three units.

The compressed air system can be divided into four components: instrument air supply, service air supply (which also serves as the backup system for supplying instrument air), the instrument air distribution network, and the service air distribution network. The service air distribution network is of no interest to this study and will not be considered further.

A.4.2.1 Instrument Air Supply. Figure A.5 shows schematically the major components of the instrument air (IA) supply. Three Worthington electric motor-driven compressors provide the normal source of IA through three air intakes and silencers. Each compressor is powered from a different 600-V ac motor control center. Compressors A and B receive electric power from a Unit 1 motor control center, and compressor C receives power from a Unit 2 motor control center. Each compressor is rated at 489 scfm at 100 psig.

Each compressor can be placed in BASE, STANDBY No. 1, or STANDBY No. 2 operating mode. In the BASE mode, when pressure decreases to 95 psig a compressor will turn on; when the pressure reaches 100 psig, the compressor will turn off. In the STANDBY No. 1 mode, the compressor starts at 90 psig, again turning off at 100 psig. In STANDBY No. 2, the set points are 85 and 100 psig. Depending on the amount of air leakage and the system load, it may be necessary to run two or even all three compressors in BASE to maintain 100 psig. All three compressors are cross connected at their discharges and connected by 8-in. lines to aftercoolers. Each compressor can be isolated by manual valves.

The IA system has two air compressor aftercoolers that cool the compressed air leaving the station air compressors. The aftercoolers receive cooling water from the LPSW system.

From the aftercoolers, air passes to three 302-ft^3 air receivers that serve as air storage tanks to dampen system pressure variations. Each receiver is equipped with a safety relief valve that can arrest excessive pressure increases in the system. The three receivers can be cross connected or isolated at both their inlets and outlets by manual valves. Three-inch lines pass from the receivers to the turbine maintenance area.

After leaving the air receivers, air enters four interconnected air dryers that dry the air by means of electrically powered chillers. Both inlet and outlet lines are 3 in., and each dryer can be isolated by means of manual valves.

The compressors, aftercoolers, air receivers, and dryers described above constitute the IA supply train. All of these components are located in the basement of the turbine building between Units 1 and 2.

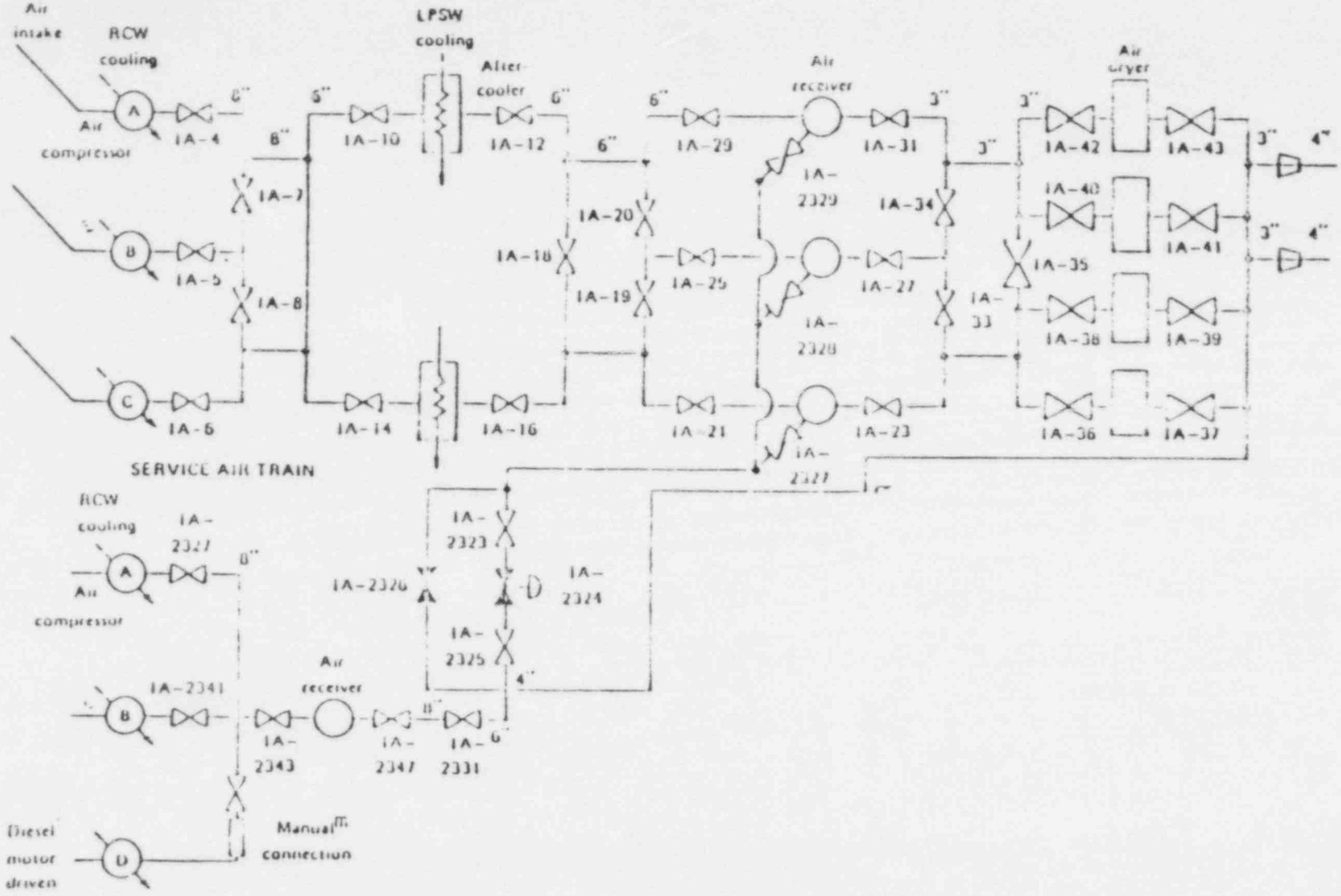


Fig. A.5. Instrument and Service Air Supply Systems at Oconee Nuclear Station.

A.4.2.2 Service Air Supply. The service air system provides compressed air for miscellaneous uses at the station (i.e., tools, cleaning). The service air supply subsystem also serves as a backup for I/A supply. An air-operated valve (No. 1A-2324 in Fig. A.5) automatically connects the service air system to the air receivers in the IA supply subsystem whenever the IA pressure drops below 87 psig. Service air is supplied by two Sullair electric motor-operated compressors, each with a capacity of ~730 scfm at 100 psig. Power for each service air compressor and its controller is supplied by a different Unit 3 600-V motor control center. Both Sullair compressors are located in the Unit 3 turbine building.

A third Sullair compressor is available to the service air system. This portable diesel-driven compressor is located outside in the vicinity of the service air electric compressors. It is battery started and connects to the service air outlet lines by a flexible hose and manual valve. It has the same capacity as the other Sullair compressors, ~730 scfm at 100 psig. This compressor must be started, operated, and connected locally.

A.4.2.3 Instrument Air Distribution Network. After exiting the air dryers, IA passes through one of two 4-in. lines that supply air to the three units. Figure A.6 shows schematically the major interconnections and block valves in the distribution network. This drawing is greatly simplified, and all dead-end feeder lines have been eliminated since its purpose here is solely to illustrate the interconnections of IA between units. This drawing is from the Oconee "Plant Compressed Air Procedure."*

A.4.2.4 Alarms and Gauges. Each unit has an alarm for low IA pressure at the auxiliary building header. The alarms are set at 90 psig decreasing, and they print out on the alarm typer in addition to the control room annunciator panel. In addition, Unit 1 has an alarm for low IA pressure in the turbine building. This alarm prints on the alarm typer and is displayed as "IA System Trouble" on the Unit 1 annunciator panel. This pressure switch is located on Column L-32 in the turbine building. The alarm is tapped off the outlet of the air receivers at the same location as the compressor pressure switches and is set at 80 psig decreasing.

Furthermore, there is a turbine bypass control air failure alarm on the control room annunciator panel. This signal comes from the pressure switch that closes the turbine bypass valves on loss of air. This pressure switch is set at 70 psig decreasing. In addition to the alarm described above, each unit has a control room gauge to monitor auxiliary building instrument air pressure. This gauge taps off the IA header at the same location as the IA auxiliary building low air pressure alarm. Also, Unit 1 has a gauge that measures air pressure at the compressor air receiver outlet. It shares the tap with the compressor control pressure switches and the turbine building low air pressure alarm.

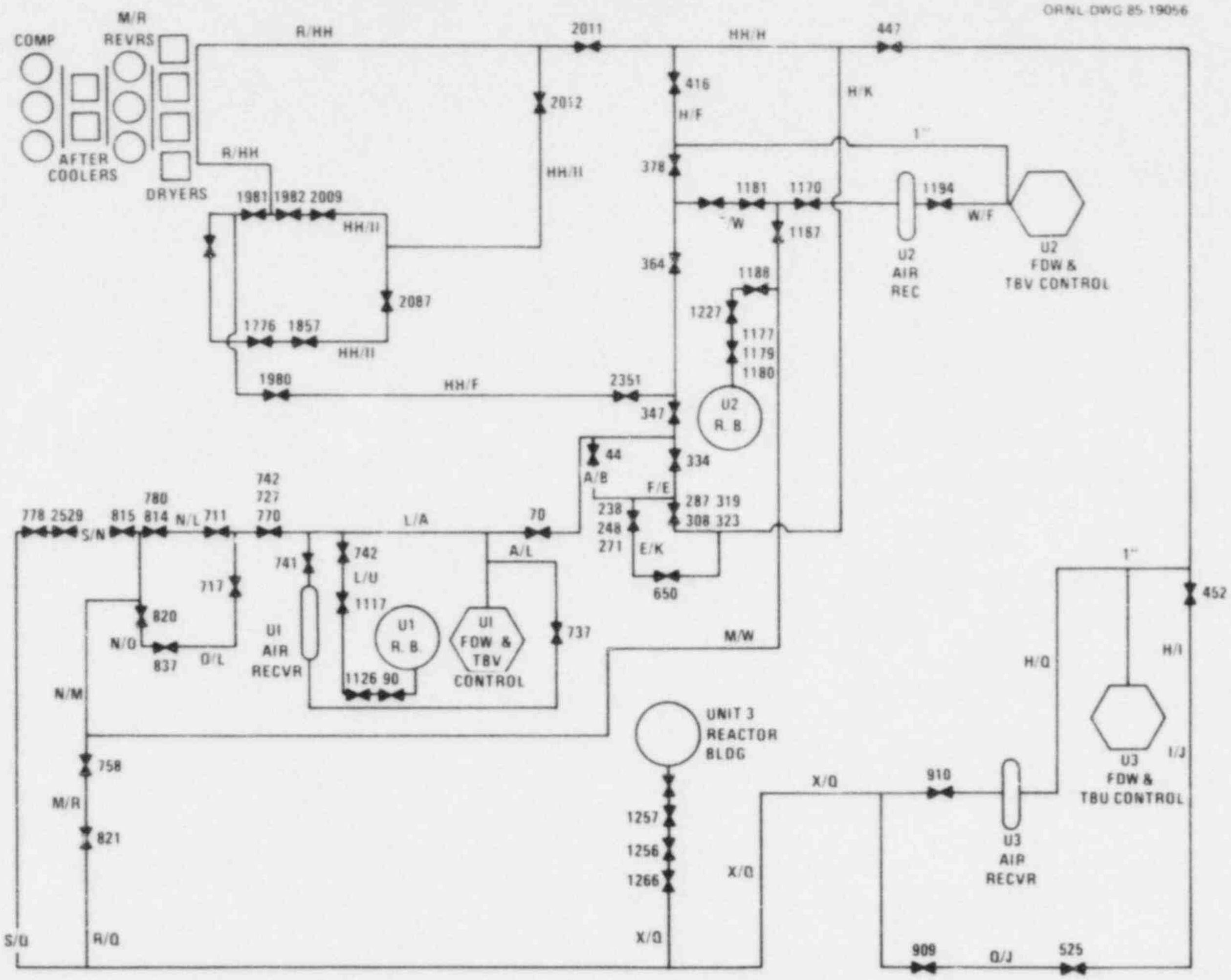


Fig. A.6. Instrument air distribution network.

A.4.3 Loads That Use Instrument Air

The IA distribution network provides air for operating valves and instruments throughout the three Oconee units. The loads using IA include the following (compiled from ref. 5 drawings):

primary coolant letdown system
RC pump seal injection flow
RC pump seal No. 1 leakoff and bypass RB isolation valve
pressurizer makeup
letdown storage tank
coolant treatment
coolant storage
gaseous waste disposal
demineralizer water
liquid waste disposal
reactor building purge system
component cooling
main feedwate
emergency feedwater
main steam
condensate
recirculating cooling water
low-pressure service water
high-pressure service water
auxiliary steam
chemical addition and sampling
air-conditioning system
high-pressure injection
high-pressure extraction (main turbine)
steam dump
heater drain
vacuum (main turbine condenser)
low-pressure extraction (main turbine)

While all of the above loads use IA for normal, routine plant operation, most of the systems can be operated satisfactorily in a manual mode should valves and instruments malfunction as a result of IA failures. Further, not all of the above systems have a direct input to plant response and are therefore not necessary for control or mitigation of plant transients.

A.4.4 Effects of Air System Failures

A.4.4.1 Systems and Instrumentation Required for Transient Mitigation. The abnormal transient operating guidelines (ATOG) for the Oconee Nuclear Station[6] were studied in an attempt to evaluate the effects of loss of IA on the NSS. The ATOGs were prepared to assist in procedure preparation and in training Oconee operators to cope with abnormal transients (i.e., those that might jeopardize plant safety). This review of ATOG has identified the following components and systems believed to be of prime importance in dealing with abnormal transients:

1. Main feedwater system
2. Emergency feedwater system
3. Steam line components
    - main steam safety valves
    - atmospheric exhaust valves
    - turbine bypass valves
4. Emergency core cooling system
    - makeup
    - HPI
    - LPI

5. Containment cooling system
    - building spray
    - building coolers
6. Containment isolation
7. Components for RC pressure control
    - pressurizer heaters
    - pressurizer spray

The ATOG were also studied to determine the instrumentation required to permit proper operation of the systems listed above. This study identified the following minimum required control instrumentation:

1. cold-leg primary temperatures,
2. in-core thermocouples,
3. RC pressure,
4. pressurizer level,
5. SG levels,
6. MFW flow rates,
7. EFW flow rates,
8. HPI flow rates,
9. LPI flow rates,
10. borated water storage tank level, and
11. condensate tank level.

A.4.4.2 Effects of Air System Failures on Required Systems. The systems, components, and instrumentation listed above were surveyed to determine the extent of their dependence on IA. Following is a discussion of the findings of this survey.

A.4.4.2.1. Main feedwater system (PO121A-1,121B-1[7]). The MFW, condensates, and heater drain systems are heavily dependent upon proper operation of a number of pneumatic valves, instruments, and controllers. Substantial pressure upsets or loss of adequate IA pressure to all or any subset of these valves and controllers during power operation can result in significant condensate and MFW upsets. Depending upon the IA failure assumed different transients can result. Following is a brief discussion of two kinds of failures.

1. Total loss of air compressors or failure of the IA supply line so that IA pressure decreases throughout the entire IA distribution network: When low instrument air pressure occurs, interactions among the turbine extraction, FW heater drain, condensate, and MFW systems are extremely difficult to predict. A low IA pressure transient occurred at the Oconee Nuclear Station on October 13, 1983. A brief description of the resulting nuclear steam supply (NSS) transient was included in the Duke Power Company information submittal of May 7, 1984.[8] Units 1 and 3 were operating at power when the IA pressure transient began. IA pressure dropped to below 54 psig, and both Units 1 and 3 condensate and FW systems experienced perturbations. The Unit 3 reactor tripped after the condensate booster pumps and MFW pumps tripped. Unit 1 avoided reactor trip, although MFW upsets occurred.

2. Loss of air to MFW control valves FW-32, 35, 41, and 44: These four valves are fed from a common IA supply line (PO149-A) and could lose air pressure due to a common failure. If these valves lose air, they lock up and hold their position. This probably occurs at 70 psig. When the MFW control valves lock up, and if an NSS trip occurs, an MFW overfeed transient is possible. If MFW pump trip occurs in conjunction with low IA pressure to these valves, no overfeed will occur; in fact, a loss of MFW will result.

From the possibilities described, we can make two observations about the relationship between the IA system and the MFW system:

1. The MFW system cannot be depended upon for a reliable, controlled source of SG FW should an IA malfunction occur. This is due to the complexity of the MFW system and the large number of valves in the MFW system that depend upon IA. Also, the performance of the MFW system is very closely coupled with the performance of the condensate and heater drain systems, both of which depend heavily upon IA.

2. Performance of the MFW system following IA malfunctions is difficult to predict because it is quite dependent upon the particular malfunction assumed, NSS operating conditions, flow rates in the secondary plant, operator response, and a host of other variables. This was clearly demonstrated by the IA transient at Oconee on October 13, 1983.

A.4.4.2.2. Emergency feedwater system (PO121A-1, 122A-1[7]). The EFW system depends upon IA primarily through the two pneumatic valves used to modulate EFW flow rates to the two SGs. These two valves, EFW-315 and EFW-316, have an automatic backup supply of nitrogen for control purposes should a loss of IA pressure occur (see enclosure one to EP/O/A/1800/29.[9] If modulation of the EFW valves cannot be accomplished following loss of IA pressure in spite of the nitrogen supply backup, SG level control can still be accomplished by varying EFW pump speed or by locally throttling EFW 315 and 316. Steam flow to the EFW pump turbine is controlled by pneumatic valves MS-93 and MS-87, which fail open on loss of IA, admitting steam to the EFW pump turbine stop and governor valves.

Normal EFW operation depends on a continuous supply of air for the EFW control valves. To ensure that air is always available, Duke Power Company has provided a backup source of control air using bottled nitrogen. If both the IA and backup supply fails for any reason, control of SG level can still be accomplished by varying EFW pump turbine speed or by locally throttling control valves FDW-315 and 316.

A.4.4.2.3. Steam line components (PO122A-1[6]). After turbine trip, SG pressure is controlled by the combined operation of main steam safety valves, atmospheric exhaust valves, and turbine bypass valves.

Main steam safety valves are mechanically operated and are independent of the IA system. The atmospheric exhaust valves have manual actuators and must be locally opened and closed by an operator if they are needed for pressure control. There are two atmospheric exhaust valves and accompanying block valves, one set for each SG.

The turbine bypass system is composed of four air-operated steam valves, two for each steam line (MS-19, 22, 28, and 31). These four valves bypass main steam around the turbine to the condenser. The turbine bypass valves are equipped with an automatic control loop that can be used by the operator to set bypass valve position from the control room or to set a specific steam pressure. When the operator chooses to specify steam pressure, the automatic control loop modulates valve position to attain the desired set point.

Low IA pressure has no effect upon either main steam safety valves or atmospheric exhaust valves; however, turbine bypass valves fail closed on low IA pressure (~70 psig). If IA pressure is low and the turbine bypass valves fail closed, steam pressure cannot be controlled from the control room; it must be controlled by an operator physically located at the atmospheric exhaust valves. Of course, the main steam safety valves will open in a staged fashion when steam pressure exceeds ~1050 psig.

A.4.4.2.4. Emergency core cooling (P0101A-1, 101B-1).

A.4.4.2.4.1. Makeup and letdown system. Loss of IA pressure isolates the normal RCS letdown and makeup paths because a number of valves in these paths fail closed (HP-5, 6, 7, 8, 9, and 13 in the letdown path and HP 120 in the makeup path are most important). Also, RC pump seal injection flow increases from 32 gal/min to 60 gal/min due to the fail open action of HP-31, the seal injection control valve.

Upon misoperation of these valves, the operator must manually control RCS inventory by throttling letdown, makeup, and seal injection flows if IA pressure drops below ~70 psig. From this brief discussion, note that normal RCS inventory control depends upon IA availability, and although backup manual actions are possible, they are demanding on the operator.

A.4.4.2.4.2. High pressure injection (P0101A-1, 101B-1) The HPI system does not appear to have a direct dependence upon IA; however, HPI pumps do require cooling water for the pump lubricating oil coolers, and service water is also required for the pump's water-lubricated mechanical seals. In addition, the makeup pump speed increasers require cooling water for the heat exchangers that cool the oil used to lubricate the speed increaser bearings. HPI pump motors are air cooled.

Thus, the HPI pumps require a continuous source of both high-pressure and low-pressure service water for proper operation. The service water systems were surveyed to determine their dependence on the IA system, and results indicate that they should be able to operate satisfactorily following loss of IA.

A.4.4.2.4.3. Low pressure injection (LPI) (PO101B-1). The LPI system does not appear to have a direct dependence upon IA; however, as was true for the HPI pumps, service water is required for oil cooling and seal injection flow. The LPI pump motors are identical to HPI motors and are air cooled.

A.4.5 Containment Cooling Systems

A.4.5.1 Reactor Building Spray (Drawing Nos. PO103A-1, PO102A-1). The reactor building spray system is designed to provide reactor building atmosphere cooling by spraying borated water inside the reactor building. The system consists of two pumps, two spray headers, isolation valves, and the necessary piping, instrumentation, and controls. Upon initial actuation of the building spray system, due to either high building pressure or operator initiation, the building spray pumps start and take suction from the borated water storage tank (BWST) through the interconnection with the LPI system. If the BWST level drops to a low limit, spray pump suction can be transferred to the reactor building sump.

The building spray system appears to be capable of normal operation without IA. Components and systems required for building spray include the BWST, the reactor building sump, LPSW for the various coolers associated with the system, and numerous ac and dc electrical buses.

A.4.5.2 Building Coolers (PO 1240). The reactor building cooling systems are designed to remove heat from the containment atmosphere following an accident that releases energy inside containment. Each of the three cooling units consists of a fan, a tube cooler, and ductwork. The fan circulates containment air past the cooling tubes where heat is removed, thus keeping the reactor building cool and preventing containment pressure from exceeding the design limit.

The building cooling units are dependent upon (1) the LPSW system to provide water for the tube cooler and (2) several ac and dc electric buses. The coolers appear to be capable of automatic start upon receipt of an actuation signal from the engineered safety features actuation system (ESFAS) and of successful operation without dependence upon the instrument air system.

A.4.6 Pneumatic System Dependence of Containment Isolation

To prevent leakage of radioactive materials to the environment in the event of high containment radiation, the reactor building isolation system (Chap. 5 of the Oconee FSAR[1]) closes all fluid penetrations not required for operation of the ESFAS. Building isolation is accomplished by a large number (~82) of valves of different types (globes, gates, tilting disk checks, swing checks, stopchecks, butterflies, piston checks, turbine stops). Each reactor building penetration has one or more isolation valves, which are fitted with electric motor, pneumatic, manual, or hydraulic operators or, in the case of check valves, no operators. It should be noted that only electric motor-operated or check valves are used inside the reactor building.

In Chap. 5 of the Oconee FSAR,[1] Table 5, "Reactor Building Isolation Valve Information," lists the penetrations, valves, and actuators for the building isolation system. In all cases, when a pneumatically actuated valve is used by the ESFAS to affect building isolation, the valve fails closed on loss of air. Also, for all pneumatic valves actuated by the building isolation system, the closed position is the post-accident position, and each valve is equipped with position indication to assist the operator in malfunction diagnosis.

A.4.7 Pneumatic System Dependence of Components for RC Pressure Control (PO 100A-1)

A.4.7.1 Pressurizer Heaters. Pressurizer heaters are used to add heat to the RCS inventory, thus causing an increase in the volume of a given mass of inventory. The increased volume causes compression of the steam bubble in the pressurizer, thereby increasing primary pressure.

Proper operation of the pressurizer heater banks depends only upon the 600-V MCC buses and RC pressure instrumentation; the pressurizer heaters do not depend directly on the instrument air system.

A.4.7.2 Pressurizer Spray. Pressurizer spray at Oconee 1 is accomplished by opening two electrically operated valves in the spray line that connects RC pump IBI with the pressurizer spray nozzle. Proper operation of pressurize spray depends only upon operation of RC pump IBI, opening of the spray valve and the spray block valve, and operation of RC pressure instrumentation.

A.4.7.3 Pilot-Operated Relief Valve (PORV). The PORV can be used to relieve excess RC pressure during certain abnormal transients that result in insufficient primary-to-secondary heat transfer. The PORV is electrically actuated and is independent of IA.

A.4.7.4 Reactor Coolant Pumps. The RC pumps (Chap. 4, Oconee FSAR[1]) are mounted in the cold-leg RCS piping and circulate water to remove heat from the reactor core. Proper operation of the RC pumps requires 13,800 V ac power, LPSW for motor and pump cooling and for oil cooling, HPI for seal injection, and various instrumentation and control circuits as necessary to monitor pump performance; however, the RC pumps do not appear to depend directly on the IA system.

A.4.8 Conclusions

Based upon the survey of the IA system described above, the following conclusions were reached:

- The Oconee Nuclear Station has one large, integrated IA system for all three units. This interconnection makes it quite possible that simultaneous, quite involved transients could be induced in more than one Oconee unit by IA malfunctions.

- Because of heavy dependence of the MFW, condensate, and heater drain systems on pneumatic valves and instrumentation, IA malfunctions are expected to cause substantial MFW upsets, perhaps culminating in loss of MFW. Also, malfunction in the IA system conceivably can result in MFW overfeed. Further, IA malfunctions in the MFW system can render the system inoperable without substantial operator manual actions.

- Normal operation of the EFW system is dependent upon a continuous supply of IA. A backup supply has been provided to allow continuous air in the event of loss of IA; however, the reliability of the backup scheme is questionable.

- Normal operation of the turbine bypass valves to control SG pressure after reactor trip is quite dependent upon IA availability. Without adequate IA pressure, SG pressure must be controlled by an operator locally throttling the atmospheric exhaust valves.

- The drawings associated with the IA system are difficult to follow.

- Study of the information and drawings on the IA system provided by Duke Power Company did not reveal any design features in the system that act to isolate nonessential IA lines on low system pressure. This implies that a fault anywhere in the IA system could affect pressure in the entire system.

Table A.1. Oconee nuclear systems (Nxx)

System ID	System Name
N01	Reactor Core
N02	Regulation Systems
N02.A	Control Rod Drive Control System
N02.B	Integrated Control System
N02.C	Non-Nuclear Instrumentation System
N03	Incore Monitoring System
N04	Reactor Coolant System (including reactor vessel and internals)
N04.A	Pressurizer
N04.B	Steam Generator
N04.C	Reactor Coolant Pumps
N04.D	Control Rod Drive System
N05	Makeup and Purification Systr ıs
N05.A	Chemical Addition and Sampling System
N05.B	Coolant Storage System
N05.C	Coolant Treatment System
N05.D	Post-Accident Sampling System
N05.E	High Pressure Injection System
N06	Low Pressure Injection System
N07	Reactor Protective System
N08	Nuclear Instrumentation System

Table A.2. Oconee engineered safeguards systems (Sxx)

System ID	System Name
S01	Engineered Safeguards Protective System
S02	High Pressure Safety Injection System
S03	Low Pressure Safety Injection System
S04	Core Flood System
S05	Reactor Building Spray System
S06	Reactor Building Emergency Cooling System
S07	Reactor Building Penetration Room Ventilation System
S08	Reactor Building Isolation System
S09	Control Room Habitability System
S10	Emergency Feedwater System
S11	Emergency Feedwater Control System

Table A.3. Oconee reactor building/containment systems (Cxx)

System ID	System Name
C01	Reactor Building/Containment and Penetrations
C02	Reactor Building Hydrogen Purge System
C03	Reactor Building Ventilation System

Table A.4. Oconee electrical systems (Exx)

System ID	System Name
E01	Main Power System
E02	Plant AC Distribution System
E02.A	Essential Power System
E02.B	Nonessential Power System
E03	Instrumentation and Control Power Systems
E03.A	DC Power System o Vital DC Power Subsystem o Plant DC Power Subsystem
E03.B	Instrument AC Power System o Vital Instrument AC Power Subsystem o Plant Instrument AC Power Subsystem
E04	Emergency Diesel Generator Power System
E05	Plant Lightning System
E06	Plant Computer
E07	Switchyard

Table A.5. Oconee power conversion systems (Pxx)

System ID	System Name
P01	Main Steam and Turbine Bypass System
P02	Turbine Generator System
P02.A	Turbine Gland Seal Subsystem
P03	Main Condenser System
P03.A	Main Condenser Evacuation System
P04	Condensate and Feedwater System
P04.A	Condensate Cleanup System
P05	Auxiliary Steam System

Table A.6. Oconee process auxiliary systems (Wxx)

System ID	System Name
W01	Radioactive Waste System
W02	Radiation Monitoring System
W03	Reactor Building Component Cooling Water System
W04	Cooling Water Systems
W04.A	Condenser Circulating Water (CCW) System
W04.B	High Pressure Service Water (HPSW) System
W04.C	Low Pressure Service Water (LPSW) System
W04.D	Recirculated Cooling Water (RCW) System
W05	Fuel Storage and Handling System
W05.A	New Fuel Storage System
W05.B	Spent Fuel Storage System
W05.C	Spent Fuel Pool Cooling System
W05.D	Fuel Handling System
W06	Auxiliary Service Water System
W07	Compressed Air System
W07.A	Service Air System
W07.B	Instrument Air System
W08	Plant Gas System

Table A.7. Oconee plant auxiliary systems (Xxx)

System ID	System Name
X01	Potable and Sanitary Water System
X02	Fire Protection System
X03	Communications System
X04	Security System
X05	Heating, Ventilating, and Air Conditioning Systems
X05.A	Turbine Building Ventilation System
X05.B	Reactor Building Purge System
X05.C	Auxiliary Building Ventilation System
X05.D	Spent Fuel Ventilation System
X05.E	Reactor Building Cooling System
X06	Non-Radioactive Waste System

Table A.8. Oconee SICS systems list

System ID	System Name
N02.B	Integrated Control System
N02.C	Non-Nuclear Instrumentation System
N03	Incore Monitoring System
N04	Reactor Coolant System (including reactor vessel and internals)
N04.A	Pressurizer
N04.B	Steam Generator
N04.C	Reactor Coolant Pumps
N05	Makeup and Purification Systems
N05.A	Chemical Addition and Sampling System
N05.B	Coolant Storage System
N05.C	Coolant Treatment System
C03	Reactor Building Ventilation System
P01	Main Steam and Turbine Bypass System
P02	Turbine Generator System
P03	Main Condenser System
P04	Condensate and Feedwater System
P05	Auxiliary Steam System
W0[illegible]	Radioactive Waste System
[illegible]	Radiation Monitoring System
W03	Reactor Building Component Cooling Water System
W04.A	Condenser Circulating Water (CCW) System
W04.D	Recirculated Cooling Water (RCW) System
W05	Fuel Storage and Handling System

Table A.8. (continued)

System ID	System Name
W06	Auxiliary Service Water System
W07	Compressed Air System
W08	Plant Gas System
X01	Potable and Sanitary Water System
X02	Fire Protection System
X03	Communications System
X04	Security System
X05	Heating, Ventilating, and Air Conditioning Systems
X06	Non-Radioactive Waste System

Table A.9. First order reactor coolant system interfaces

System ID	Oconee System Name	Criteria for Elimination
N02.C	Non-Nuclear Instrumentation	Selected for analysis
N03	Incore Monitoring	Signals not used for plant control
N04	Reactor Coolant System	Selected for analysis
N05	Makeup and Purification	Selected for analysis
P01	Main Steam and Turbine Bypass	Selected for analysis
P04	Condensate and Feedwater	Selected for analysis
W01	Radioactive Waste System	Waste systems isolated from RCS during plant operation
W03	Reactor Building Component Cooling Water	Selected for analysis

Table A.10. Second order reactor coolant system interfaces

First Order System ID	Second Order System ID	System Name	Criteria for Elimination
NO2.C	NO2.B	Integrated Control System (ICS)	Selected for analysis
	W01	Radioactive Waste System	System to be analyzed to the extent failures can impact the non-nuclear instrumentation functions
NO5	W01	Radioactive Waste System	System to be analyzed to the extent failures can impact the makeup and purification system functions
	W07.B	Instrument Air System	Selected for analysis
P01	NO2.B	Integrated Control System	Selected for analysis
	P02	Turbine-Generator System	Selected for analysis
	P06	Auxiliary Steam System	Operates during shutdown only. Interface with main steam system considered
	W07.B	Instrument Air System	Selected for analysis
P04	NO2.B	Integrated Control System	Selected for analysis
	P03	Main Condenser	Selected for analysis
	P04.A	Condensate Cleanup System	Selected for analysis
	W07.B	Instrument Air System	Selected for analysis
W03	W04.A	Condenser Circulating Water	To the extent the condenser circulating water system interfaces with the reactor building component cooling function, it is a passive safety system. System to be analyzed to the extent failures can impact the reactor building cooling water system function

Table A.11. Oconee 1 systems not selected for analysis

System ID	System Name	Potential Impact on RCS
N03	Incore Monitoring System	Provided for operator information only. However, high core temperature may induce operator to trip the reactor and initiate High Pressure Safety Injection (S02), a safety system. No other impact on RCS overcooling is apparent.
N05.C	Coolant Treatment System	Processes coolant stored in the Coolant Storage System producing demineralized water and boric acid solution which also is stored in the Coolant Storage System (N05.B). No impact on RCS apparent.
N05.D	Post-Accident Sampling System	System only operates in the post-accident, RCS shutdown mode. No impact on RCS apparent.
N05.F	Low Pressure Injection System	This system is a safety system used only to remove core decay heat in an RCS shutdown mode below 300°F and 300 psi.
N06	Reactor Protective System	System is a safety system used to initiate reactor trip and has no impact on post trip response.
N07	Nuclear Instrumentation System	System provides signals to regulate plant power generation. Although the system may induce spurious reactor trip, it has no impact on post-trip response.
N09	Emergency Feedwater Control System	System potentially may have a significant impact on RCS but it is a safety system and beyond the scope of this study.
S01	Engineered Safeguards Protective System	Engineered safeguards systems may have significant impacts on RCS but are safety systems and beyond the scope of this study.
S02	High Pressure Safety Injection System	

Table A.11. (continued)

System ID	System Name	Potential Impact on RCS
S03	Low Pressure Safety Injection System	
S04	Core Flood System	
S05	Reactor Building Spray System	
S06	Reactor Building Emergency Cooling System	
S07	Reactor Building Penetration Room Ventilation System	
S08	Reactor Building Isolation System	
S09	Control Room Habitability System	
C01	Reactor Building/Containment and Penetrations	The function of the containment is to prevent release of radioactivity to the environment following accidents. The effects of containment pressure boundary valves on RCS are considered in the analysis for the systems selected for analysis.
C02	Reactor Building Hydrogen Purge System	The function of the hydrogen purge system is to prevent hydrogen concentrations in the containment from reaching explosive levels. The effects of hydrogen explosives are beyond the scope of the study. No other impacts on RCS apparent.
C03	Reactor Building Ventilation System	Failure of this system could result in high reactor building temperatures. Adverse environmental conditions could contribute to components in the reactor building. However, the specific impacts of adverse operating environments are beyond the scope of this study.

Table A.11. (continued)

System ID	System Name	Potential Impact on RCS
P02.A	Turbine Gland Seal Subsystem	The gland seal system is designed to prevent air in-leakage to the turbines and condenser. During power operation, failure of the system may result in turbine trip. Following turbine trip, the system requires steam from the main steam system via the startup steam header (see Auxiliary Steam System, P06). No other potential impacts on RCS are apparent.
P03.A	Main Condenser Evacuation System	The function of the evacuation system is to remove non-condensible gases from the condenser. Failure of the system may result in turbine trip; however, no major impacts on RCS are apparent.
P05	Emergency Feedwater System	The emergency feedwater system may have significant impact on RCS. However, this system is a safety system and beyond the scope of this program.
P06	Auxiliary Steam System	During startup and shutdown operations, the Auxiliary Steam System provides steam to selected components from the startup steam header or the auxiliary boiler. Failure to provide steam to required components is addressed in the analyses of the selected systems. The interface with the main steam system (P01) is addressed in the analysis of the main steam system. No other potential impacts on RCS are apparent.
W01	Radioactive Waste System	The radioactive waste system collects and processes radioactive materials prior to reuse or disposal. Interfaces with the RCS are isolated during operation. No impacts on RCS are apparent.

Table A.11. (continued)

System ID	System Name	Potential Impact on RCS
W02	Radiation Monitoring System	The radiative monitoring system detects the release of radioactivity. No impacts on RCS are apparent.
W04.B	High Pressure Service Water (HPSW) System	The HPSW is a safety system designed to supress plant fires and serve as a backup to the LPSW. No impacts on RCS are apparent.
W04.C	Low Pressure Service Water (LPSW) System	The LPSW is required to support the operation of safety systems. As a safety system, its analysis is beyond the scope of this program.
W05	Fuel Storage and Handling System	The fuel storage and handling system have no interface with the RCS or RCS support systems except during refueling shutdown operations. As such, no impact on RCS is possible.
W05.A	New Fuel Storage System	
W05.B	Spent Fuel Storage System	
W05.C	Spent Fuel Pool Cooling System	
W05.D	Fuel Handling System	
W06	Auxiliary Service Water System	The auxiliary service water system is manually placed in operation following a postulated concurrent failure of the main and emergency feedwater systems and the decay heat removal system. No impacts on RCS are apparent.
W07.A	Service Air System	
W08	Plant Gas System	

Table A.11. (continued)

System ID	System Name	Potential Impact on RCS
X01	Potable and Sanitary Water System	These plant auxiliary systems have no interface with the RCS or RCS support systems. Potential effects of severe operating environment on the operation of plant equipments are beyond the scope of this study.
X02	Fire Protection System	
X03	Communications System	
X04	Security System	
X05	Heating, Ventilating, and Air Conditioning Systems	
X05.A	Turbine Building Ventilation System	
X05.B	Reactor Building Purge System	
X05.C	Auxiliary Building Ventilation System	
X05.D	Spent Fuel Ventilation System	
X06	Non-Radioactive Waste System	

Table A.12. Miscellaneous non-reactor accidents

FSAR Section	Transient
15.10	Waste Gas Tank Rupture Accident
15.11	Fuel Handling Accidents

Tabie A.13. Accidents terminated by reactor trip

FSAR Section	Transient
15.1	Uncompensated Operating Reactivity Changes
15.2	Startup Accidents
15.3	Rod Withdrawal Accidents at Rated Power
15.4	Moderator Dilution Accidents
15.5	Cold Water Accidents
15.6	Control Rod Misalignment Accidents

Table A.14. Accidents exhibiting significant post trip transient behavior

FSAR Section	Transient
15.6	Loss of Coolant Flow Accidents
15.8	Loss of Electric Power Accidents
15.9	Steam Generator Tube Rupture Accidents
15.12	Rod Ejection Accident
15.13	Steam Line Break Accident
15.14	Loss of Coolant Accidents
15.15	Maximum Hypothetical Accident
15.16	Post Accident Hydrogen Control

APPENDIX A REFERENCES

1. "Oconee Nuclear Station Final Safety Analysis Report," Duke Power Company,

2. "Instruction Book" for Integrated Control and Nonnuclear Instrumentation Systems (for the Oconee Nuclear Plant, Unit 1), Vol. 4, Bailey Meter Company, March 15, 1977.

3. Delta P Transmitter for Nuclear Service, Product Instruction, E21-20, Bailey Meter Company,

4. Oconee Nuclear Station, "Plant Compressed Air Procedures," OP/O/A/1106/27 - change 6.

5. Oconee Nuclear Station Drawings, "Diagramic Layout of Instrument Air Stations" PO-149-A, PO-149-B, PO-149-C, PO-149-D, PO-149-L, PO-149-U, PO-149-Z, PO-149-AA, PO-149-BB, PO-149-DD, PO-149-GG, PO-149-JJ.

6. "Oconee Nuclear Station Abnormal Transient Operating Guidelines," B&W 74-1123297-00, March 1982.

7. Oconee Nuclear Station Process and Instrumentation Drawings

PO 100A-1	Reactor Coolant System
PO 100A-1	High Pressure Injection System
PO 101B-1	High Pressure Injection System
PO 102A-1	Low Pressure Injection and Core Flooding System
PO 103A-1	Reactor Building Spray System
PO 107A-1	Coolant Storage System
PO 115B	High Pressure Service Water
PO 115B	HPI Pump Motor Cooling
PO 115B	EFW Pump Cooling Water
PO 115B	LP & HPSW & Jockey Pump Packing
PO 121A-1	Condensate System
PO 121B-1	Feedwater System
PO 122A-1	Main Steam & Auxiliary Steam System
PO-122B-1	HP & LP Turbine Exhaust & Steam Seal System
PO 122C-1	Moisture Separator & Reheater Heater & Drain System
PO 124A	Service Water System - Turbine Room
PO 124B,C,D	Service Water System - Auxiliary & Reactor Buildings
PO 144A	Component Cooling System

8. Duke Power Company information submittal to A. P. Malinauskas May 7, 1984: Brief description of an instrument air system transient at the Oconee Station, October 13, 1983, and "Compressed Air System Description."

9. Oconee Nuclear Station, "Loss of Instrument Air Procedures," EP/O/A/1800/29 - change 4.

APPENDIX B

Failure Modes and Effects Analyses (FMEA)

APPENDIX B

Failure Modes and Effects Analyses (FMEA)

B.1 FMEA OBJECTIVES AND METHODOLOGY

B.1.1 Objectives

The objective of performing FMEAs on the control systems selected in Sect. 2 is to identify failure modes whose effects have potential safety implications for Oconee Unit 1. The basis for choosing a FMEA methodology and the application of this methodology to the Safety Implications of Control System (SICS) Program is discussed in Sect. B.1.2.

Once a system's failure modes and their effects are tabulated, the effects that may contribute to accident sequences of concern can be identified. These failure modes can then be combined with other initiating events or other equipment failures to assess their safety implication in the context of accident sequences. The sequence development methodology is discussed in Sect. B.1.3.

B.1.2 Selection and Application of Methodology

In general, two systems failure analysis methodologies are available to analyze the relationship of failures and their effects: "top-down" methods such as fault trees, and "bottom-up" methods such as FMEA. Each method has its advantages, depending on the analysis objective, and the reasons for selecting the FMEA methodology are discussed below. It should be noted that these two analysis methods offer different insights into system failures and often are used together.

Top-down methods typically are used when a system failure state is known and the combinations of failed components producing this failed state are desired (e.g., define the combinations of failed components of a fluid system resulting in a system flow rate of less tnan 500 gpm). Since the method yields a complete listing of failures resulting in a particular failed state, it is particularly useful in assessing the probability of that failed state.

The FMEA method, in contrast, proceeds from the opposite direction: given a set of equipment, define the failure modes and evaluate the effects of each. FMEAs typically are used to find undesirable failure modes of systems in which the particular failure modes are not known on some other basis. FMEAs are useful in a analyzing a limited scope of equipment in detail, but they will not necessarily identify all combinations of failures leading to any of the effects identified and, as such, cannot be used directly to assess the probabilities of effects unless other methods such as fault trees are used in conjunction with them.

The SICS Program is characterized by an equipment scope limited to control systems and, beyond being adverse to plant safety, a lack of specified control system failure modes. As such, the FMEA was chosen as the principal systems failure analysis method. Fault trees are used in the SICS Program to evaluate the probabilites of selected system failure modes of significance once they are identified (see Sect. 3). In addition, it is recognized that due to federal design requirements for nuclear power plants and extensive regulatory design review, control system failure modes with safety significance are expected to be subtle. The FMEA method is expected to be particularly useful in the identification of subtle failure modes.

FMEAs are applied to develop a listing of all credible system component failures and their direct and indirect effects. The analysis begins with a complete listing of a system major components (i.e., valves, pumps, transmitters, etc.) and the possible failure modes of each (a valve can fail completely open, completely closed or in an "as is" or intermediate position). Three aspects of the failure mode are then evaluated and listed: possible causes of the failure, its direct and indirect effects, and possible remedial actions. Failure causes are useful in evaluating the potential for coupled failures (more than one failure mode resulting from a single initiating failure). Effects of the failure mode include both direct and indirect effects. For instance, the direct effect of a valve closure could be a complete loss of fluid flow. Indirect effects might include consequential failure of components in other systems. Remedial actions are evaluated and listed to aid in the evaluation of consequences. The availability of actions mitigating the effects of a failure mode generally tend to reduce the importance of that failure mode. On the other hand, effects that cannot be mitigated readily are of relatively greater importance.

The compiled list of the failure modes and their effects on the systems selected for component level FMEA typically is very large, presenting in detail all failure modes and not only those with potential safety implications. The tabulated effects of the FMEAs must be screened to identify the failure modes of potential safety significance.

Four principal criteria were used to identify and separately list those effects and their failure causes having potential safety implications:

1. potential for the failure mode to initiate or contribute to SG overfill.

2. potential for the failure mode to initiate or contribute to inadequate core cooling (RCS undercooling).

3. potential for the failure mode to initiate or contribute to RCS overcooling.

4. potential to affect recovery from design basis accidents.

In addition to the above criteria, the effects were evaluated to identify potentially significant effects not specifically addressed in the principal evaluation criteria.

Identifying and listing potentially significant failure modes provides a basis for development and evaluation of possible accident sequences incorporating the failure modes. The accident sequence development methodology is discussed in Sect. B.1.3.

B.1.3 Accident Sequence Development Methodology

A particular failure mode leading directly to an unmitigated accident would be a significant event. However, in addition to this unexpected class of events, control system failures would be considered significant to the extent that they may contribute to unmitigated accident sequences in conjunction with other postulated failures.

Evaluation of the safety significance of control system failures required development of accident sequences and incorporation of the control system failures into these sequences. Significant accident sequences were developed using "event tree" representation of an accident-initiating event and the subsequent success or failure operating states of required mitigating systems. An accident sequence is defined in the event tree as the initiating event and a unique combination of the operating states of the mitigating systems.

The event trees are then evaluated to assess the potential contribution of control system failures to unsafe or undefined plant states. Event trees involving control system actions with potential safety implications were selected based on the following criteria:

1. The existence of successful control system action required to achieve a safe plant state (or control system failures leading to potentially unsafe or undefined plant states).

2. The existence of control system failures requiring an operator action to achieve a safe plant state.

3. The existence of "as designed" control system actions potentially leading to unsafe conditions for which no safety system mitigation is available.

B.2. FMEA OF THE POWER CONVERSION SYSTEMS

Table

Table B.2.1. FMEA of the main steam and turbine bypass system

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Main Steam Safety Valves MS-1 through 16	One valve fails open	Mechanical failure, valve fails to close completely following turbine trip.	Steam leakage to atmosphere - possible effects bounded by a valve failing completely open which would result in potential overcooling of the RCS and require a forced plant shutdown.	Initiate plant shutdown. Isolation of feedwater to affected steam generator may be required to prevent exceeding RCS cooldown rate limit (100°F/hr).
	One valve fails to open on demand	Mechanical failure.	Minor increase in peak steam pressure following turbine trip.	Identify closed valve and repair following shutdown.
Turbine Bypass Valves MS-19, 22	One or both valves open and remain open	Instrumentation failure, valve fails to close following turbine trip	Steam diverted to condenser - depending on response of turbine controls and condenser could cause automatic turbine and reactor trip and potential overcooling of the RCS.	Identify open valve and manually close TBV or manually close isolation valve MS-17.
Turbine Bypass Valves MS-28, 31	One or both valves open and remain open	Instrumentation failure, valve fails to close following turbine trip	Steam diverted to condenser - depending on response of turbine controls and condenser could cause automatic turbine and reactor trip and potential overcooling of the RCS.	Identify open valve and manually close TBV or manually close isolation valve MS-26.
Turbine Bypass Valve MS-19, 22, 28, 31	One or more valves fail to open on demand	Instrumentation or valve failure, instrument air failure.	Possible challenge to main steam safety valves.	Identify closed valve, manually operate if required and repair following shutdown.

Table B.2.1. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Turbine Bypass Isolation Valve MS-17 or 26	Valve spuriously closes	Instrumentation failure, maintenance error.	No impact during power operation. Following turbine trip, the main steam safety valves on the affected line would be challenged.	Identify closed valve and manually open if possible.
Diversion of Steam to Startup Steam Header	Unknown - PO-28A-1 not available	Unknown	Steam diverted from HP turbine - may cause turbine and reactor trip and potential overcooling of the RCS.	Identify steam diversion and close isolation valves MS-24 and 33.
Startup Header Isolation Valves MS-24 or 33	Valve spuriously closes	Instrumentation failure, maintenance error.	No known impact during power operation. Steam would be supplied from other steam line during shutdown.	
Reheater Steam Supply Isolation Valves MS-76 or 79	Valve spuriously closes	Instrumentation failure, maintenance error.	Inefficiency in turbine cycle - effects bounded by turbine trip.	Identify closed valve and manually open if possible.
	Valve fails to close on demand	Instrumentation, valve or electric power failure.	Small impact, reheaters remain pressurized.	Identify open valve, manually close if possible and repair following shutdown.
FW Pump Turbine A Stop and Governor Valves MS-40, 41	Valves open spuriously	Instrumentation or valve operator failure.	Possible FW Pump A trip on overspeed and plant runback and/or trip.	Close isolation valve MS-35 and repair failure.

Table B.2.1. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
	Valve fails to open on demand	Instrumentation or valve operator failure.	FW pump A inoperability following turbine trip. Feedwater supplied by other FW pump.	Identify closed valve and repair following shutdown.
FW Pump Turbine A Isolation Valve MS-35	Valve fails to close on demand	Instrumentation, electric power or valve failure.	Minor inpact, line remains pressurized.	Identify open valve and repair following shutdown.
	Valve spuriously closes	Instrumentation failure, maintenance error.	Isolation of high pressure steam supply to FW pump turbine A. Following turbine trip, FW pump A will be inoperable.	Identify closed valve and manually reopen, if possible. An alternate supply of steam may be provided from the startup steam header.
FW Pump Turbine B Stop and Governor Valves MS-43, 44	Valves open spuriously	Instrumentation or valve operator failure.	Possible FW Pump B trip on overspeed and plant runback and/or trip.	Close isolation valve MS-36 and repair failure. Provide steam supply to condenser steam air ejectors via startup header.
	Valve fails to open on demand	Instrumentation or valve operator failure.	FW pump B inoperability following turbine trip. Feedwater supplied by other FW pump.	Identify closed valve and repair following shutdown.
FW Pump Turbine B Isolation Valve MS-36	Valve fails to close on demand	Instrumentation, electric power or valve failure.	Minor inpact, line remains pressurized.	Identify open valve and repair following shutdown.

Table B.2.1. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Condenser Steam Air Ejector and MFW Pump Turbine B Steam Supply Isolation Valve MS-36	Valve spuriously closes	Instrumentation failure, maintenance error.	Isolation of steam supply to condenser steam air ejectors A, B, and C, emergency air ejector and high pressure supply to FW pump turbine B. Loss of steam air ejectors eventually may cause a turbine trip and subsequently loss of MF Pump B.	Identify closed valve and manually open if possible. An alternate supply of steam may be provided from the startup steam header.
FW Pump Turbine Exhaust Valve MS-98, 100	Valve closes spuriously	Instrumentation, maintenance failure.	Trip of FW pump and plant runback and/or trip.	Repair failure.
Emergency FW Pump Turbine Steam Supply Isolation Valve MS-82 and/or 84	Valve spuriously closes	Instrumentation failure, maintenance error.	Possible isolation of high pressure steam supply to emergency FW pump turbine A. Closure of one valve has no effect on emergency FW pump turbine operability; closure of both valves will result in pump inoperability.	Identify closed valve and manually reopen.
Condenser Steam Air Ejector Supply Isolation Valve MS-47	Valve closes spuriously	Instrumentation, maintenance failure.	Isolation of steam supply to Air Ejectors A, B, and C eventually may cause turbine trip.	Identify closed valve and manually reopen. Alternatively, emergency steam air ejectors may be used or steam supplied from startup steam header.
Condenser Steam Air Ejector Control Valves MS-50, 59, 68	Valve closes spuriously	Instrumentation or valve operator failure.	Loss of one of three air ejectors not expected to result in turbine trip.	Repair failure.

Table B.2.2. FMEA of the main turbine generator system: turbine to feedwater heaters and feedwater pump turbines, HP turbines to steam reheaters, reheaters to LD turbines

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
HP Turbine Stop or Control Valve SV-1, 2, 3, 4, CV-1, 2, 3, 4	One or more valves spuriously close	Instrumentation, valve or valve operator failure.	Plant runback or trip.	Repair failure.
	One or more stop valves and one or more control valves fail to close on demand	Multiple instrumentation, valve or valve operator failure.	Possible turbine-generator overspeed, RCS overcooling.	Manually initiate closure of stop and/or control valves. Verify closure of LP turbine steam control valves or manually close.
LP Turbine Steam Control Valves CRV-1, 2, 3, 4, 5, 6	Valve spuriously closes	Instrumentation or valve operator failure.	Steam supply to one LP turbine shell isolated. Upset to normal turbine cycle expected. Whether the transient will result in turbine trip is not known.	Identify closed valve and manually reopen and/or repair.
	Valve fails to close on turbine trip	Instrumentation or valve operator failure.	Expansion of steam in HP turbine through one LP turbine resulting in possible overspeed.	Manually initiate closure of valves and repair.
FW Pump Turbine Steam Supply Isolation Valve LPE-12	Valve spuriously closes	Instrumentation or valve operator failure.	Isolation of low pressure steam supply to both FW pump turbines. Possible inoperability of both FW pumps and plant runback or trip. High pressure steam supply may maintain pump operability.	Identify closed valve and reopen or repair following shutdown.

Table B.2.2. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Pump Turbine A Stop and Gov. Valves LPE-19, 20	Valve spuriously closes	Instrumentation or valve operator failure.	Isolation of low pressure steam supply to FW pump turbine A. Possible inoperability of FW pump and plant runback or trip. High pressure steam supply may maintain pump operability.	Identify closed valve and reopen or repair following shutdown.
	Gov. valve spuriously opens	Instrumentation or valve operator failure.	Increased FW pump speed and possible overspeed trip. FW flowrate controlled by regulating valves. Trip of FW pump would result in plant runback or trip.	Identify open valve and repair following shutdown.
	Stop valve fails to close on demand	Instrumentation or valve operator failure.	Possible FW pump overspeed or SG overfill if pump trip signal generated in response to high SG level.	Manually trip FW pump or isolate steam supply by closing MS-35.
FW Pump Turbine B Stop and Gov. Valves LPE-22, 23	Valve spuriously closes	Instrumentation or valve operator failure.	Isolation of low pressure steam supply to FW pump turbine B. Possible inoperability of FW pump and plant runback or trip. High pressure steam supply may maintain pump operability.	Identify closed valve and reopen or repair following shutdown.

Table B.2.2. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
	Gov. valve spuriously opens	Instrumentation or valve operator failure.	Increased FW pump speed and possible overspeed trip. FW flowrate controlled by regulating valves. Trip of FW pump would result in plant runback or trip.	Identify open valve and repair following shutdown.
	Stop valve fails to close on demand	Instrumentation or valve operator failure.	Possible FW pump overspeed or SG overfill if pump trip signal generated in response to high SG level.	Manually trip FW pump or isolate steam supply by closing MS-35.
FW Heaters Steam Supply Isolation Valve MPE-5	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Steam supply to "A" FW heaters and 1st stage reheaters isolated. Upset to normal turbine cycle expected. Whether the transient will result in turbine trip is not known.	Identify closed valve and manually reopen and/or repair.
Other Steam Supply Isolation Valves (MPE-6, 10, 20, 24, 36, LPE-36, 10, MPE-15, 16, 17, 18)	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Steam supply to one FW heater isolated, loss of efficiency in turbine cycle.	Identify closed valve and manually reopen and/or repair.

Table B.2.3. FMEA of the main condenser system: condenser and upper surge tanks

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Vacuum Breaker Valve V-186 (?)	Valve spuriously opens	Instrumentation or maintenance failure.	Turbine trip, trip of MFW pump turbines and interlock of turbine bypass valves closed.	Identify open valve and manually close. Reestablish condenser vacuum.
Condenser Shell and Miscellaneous Connecting Piping	Crack resulting in excessive air in-leakage	Vibration, corrosion.	Bounded by turbine trip, trip of MFW pump turbines and interlock of turbine bypass valves closed.	Identify failure and repair.
Condensate Makeup Valve C-175, 187	Valve spuriously opens or remains open	Instrumentation, valve or valve operator failure.	Hotwell recirculation valve C-196 opens resulting in possibly decreased feedwater flow to steam generators. Plant power level limited. Effect on condensate booster or feedwater pumps unknown.	Identify open valve and manually close.
Hotwell Recirculation Valve C-196	Valve spuriously opens or remains open	Instrumentation, valve or valve operator failure.	Condensate makeup valve C-176 or 187 opens resulting in possibly decreased feedwater flow to steam generators. Plant power level limited. Effect on condensate booster or feedwater pumps unknown.	Identify open valve and manually close.
Condenser Steam Air Ejectors A, B or C	Inoperability of one or more air ejectors	Unspecified.	Failure of air ejectors may result in long term increases in condenser pressure possibly resulting in turbine trip.	Align and start condenser vacuum pumps if required.

Table B.2.4. FMEA of the condensate and feedwater system

(a. condenser to FW pumps)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Hotwell Pump Isolation Valves C-1, 2, 4, 5	Valve spuriously closes	Instrumentation, maintenance failure.	Less than 50% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen valve or reopen failure.
Hotwell Pump B, C	One or both pumps tripped, inoperable	Electric power, motor failure, loss of Recirc. Cooling Water flow to bearing coolers.	Failure of both pumps and failure of one pump at higher power levels result in FW pump, reactor trip and automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue following loss of one pump.	Identify and repair failure.
Condensate Valve C-10	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Trip of FW pumps and reactor. Automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.

Table B.2.4. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Demineralizer Bypass Valves C-14, 15	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Less than 30% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen or repair.
	Valve spuriously opens	Instrumentation, valve operator or maintenance failure.	Demineralizers bypassed which eventually will result in exceeding water quality specifications and may require plant shutdown.	Identify and repair failure.
Demineralizer A, B, C, D	Flow path blocked	Isolation valve closure, unspecified demineralize or resin trip plugging.	Increased condensate flow bypassing demineralizers.	Identify and restore flowpath.
Hydrazine or Ammonia Feed	Injection stopped	Unspecified.	Out of specification condensate pH or O_2 concentration. May require plant shutdown.	Identify and restore injection.
Generator Water Cooler Bypass Valve C-61	Valve spuriously closes	Instrumentation or valve operator failure.	Trip of FW pumps and reactor. Automatic initiation and control of emergency feedwater.	Identify closed valve and repair failure.

Table B.2.4. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
	Valve spuriously opens	Instrumentation or valve operator failure.	Increased bypass of condensate around generator water cooling and hydrogen coolers. Whether generator would eventually trip is unknown.	Identify open valve and repair failure.
Hydrogen Cooler Flow Control Valve C-59	Valve spuriously closes	Instrumentation or valve operator failure.	Probable generator and turbine trip.	Identify closed valve and repair failure.
	Valve spuriously opens	Instrumentation or valve operator failure.	No significant effect expected.	Identify open valve and repair.
Condensate Booster Pump Isolation Valves C-77, 80, 81, 84	Valve spuriously closes	Instrumentation, maintenance failure.	Less than 50% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen valve or reopen failure.

Table B.2.4. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Condensate Booster Pumps A, B	One or both pumps tripped, inoperable	Electric power, motor failure, loss of Recirc. cooling water flow to bearing coolers.	Failure of both pumps and failure of one pump at higher power levels result in FW pump, reactor trip and automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue following loss of one pump.	Identify and repair failure.
"F" Low Pressure FW Heater Isolation Valves C-89, 90, 91	Valve spuriously closes	Instrumentation or maintenance failure.	Less than 33% reduction in condensate flowrate. Probable FW pump and reactor trip at higher power level with automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
Low Pressure FW Heaters F1, F2, F3, D1, D2, C1, C2	Loss of steam supply	See FMEA of Main Steam System - Turbines to Feedwater Heaters, Other Steam Supply Valves.		
Low Pressure FW Heater Isolation Valves C-103, C-104, C-110, C-111, C-117, C-118	Valve spuriously closes	Instrumentation or maintenance failure.	Less than 50% production in condensate flowrate. Probable FW pump and reactor trip at higher power levels with automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
FW Pump Isolation Valve FDW-1, FDW-6	Valve spuriously closes	Instrumentation or maintenance failure.	Trip of one of two main FW pumps, plant runback and possible reactor trip.	Identify closed valve and manually reopen or repair.
FW Heater Drain System	Unspecified - Dwg. PO-123A not available	Unspecified - Dwg. PO-123A not available	Effects bounded by a trip to the main FW pumps and automatic initiation and control of emergency feedwater.	Identify failure and repair.

Table B.2.4. FMEA of the condensate and feedwater system
(b. FW pumps to steam generators)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Pumps A, B	Pump trip	Instrumentation failure, pump/turbine failure, high steam generator level, loss of Recirc. cooling water flow to oil coolers - see also FMEA of Condensate System and Main Steam System.	Trip of one pump will result in a plant runback and possible reactor trip at higher power levels (>50% power). Trip of both pumps results in reactor trip and automatic initiation and control of emergency feedwater.	Identify failure and repair.
	Spurious speed increase	Instrumentation or throttle valve operator failure.	Increased P across FW control valves.	Identify failure and repair.
	Spurious speed decrease	Instrumentation or throttle valve operator failure.	Possible decrease in feedwater flowrate resulting in plant runback and possible reactor trip.	Identify failure and repair.
FW Pump Isolation Valves FDW-4, FDW-3, FDW-9, FDW-8	Spurious valve closure	Instrumentation, valve operator or maintenance failure.	Reduction in FW flowrate by <50%. Plant runback and/or reactor trip at higher power levels.	Identify closed valves and manually reopen or repair failure.
FW Pump Recirculation Control Valve FDW-53, 55	Valve fails to open on low FW flowrate	Instrumentation or valve operator failure.	Following substantial feedwater flowrate decrease transients (e.g., reactor trip), failure to maintain minimum pump flowrate will result in pump trip or possible pump damage.	Identify failure and repair.

Table B.2.4b. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
High Pressure FW Heater Bypass Valve FDW-11, FDW-16, FDW-26, FDW-29	Valve spuriously bypasses flow around HP heater	Instrumentation or maintenance failure.	Reduced FW temperature and inefficiency in turbine cycle.	Identify mispositioned valve and manually reposition or repair
High Pressure FW Heater Isolation Valves FDW-14, FDW-19, FDW-21, FDW-29	Valve spuriously closes	Instrumentation or maintenance failure.	Reduction in FW flowrate by <50% resulting in possible reactor runback and/or reactor trip.	Identify closed valve and manually reopen or repair failure.
High Pressure FW Heaters A1, A2, B1, B2	Loss of steam supply	See FMEA of Main Steam System - Turbine to Feedwater Heaters, Steam Supply Valve MPE-5		
FW Block Valve FDW-31, FDW-40	Valve spuriously closes	Instrumentation or maintenance failure.	Reduction in FW flowrate by <50% results in reactor runback and/or reactor trip.	Identify closed valve and manually reopen or repair failure.
FW Control Valve FDW-32, FDW-41	One or both valves spuriously close	Instrumentation or valve operator failure	Reduction in FW flowrate to one or both steam generators which may result in plant runback and/or reactor trip.	Identify failure and repair.

Table B.2.4b. (continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
	Valve(s) open or fail to close on demand	Loss of instrument air pressure, instrumentation, or valve operator failure.	Valve(s) opening or remaining in position after reactor trip may result in a steam generator overfeed condition. Transient will be terminated by automatic trip of main FW pumps and initiation and control of emergency feedwater under manually controlled by the operator.	Identify closed valve and manually reopen or repair failure.
FW Startup Valve Isolation Valve FDW-36, FDW-45	Valve spuriously closes	Instrumentation or maintenance failure.	May produce erratic post-reactor trip steam generator level control.	Identify closed valve and manually reopen or repair failure.
FW Startup Valve FDW-35, FDW-44	Valve(s) spuriously closes	Instrumentation or valve operator failure.	Closure of FW block valve and loss of feedwater to one steam generator resulting in reactor trip.	Reestablish feedwater flow to isolated steam generator by manual control of startup and block valves or manual initiation of emergency feedwater.
	Valve(s) open or fail to close on demand	Loss of instrument air pressurize, instrumentation or valve operator failure.	Valve(s) remain in position following reactor trip which may result in a steam generator overfeed condition. Transient would be terminated by automatic trip of main FW pumps and initiation and control of emergency feedwater under manually controlled by the operator.	Identify failure and manually close startup or startup isolation valves.

B.3. FMEA OF THE MAKEUP AND PURIFICATION SYSTEM

Table

Table B.3.1. Letdown subsystem
(Reference: FSAR Figures 9.3-2 and 9-2A)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
1.1 Letdown Coolers:					
1.1.1 Miscellaneous Normally Closed, Manual Valves Such as HP-329 (Including Double Isolation Valves Such as HP-32 and HP-359)	1. Opened or fails open due to internal fault	Vent or Drain	Reduced letdown flow rate; RC leak	Some letdown flow is diverted to sumps; hence, reduced letdown flow to 3-way valve HP-14 (HP-V10) and RC leak	Though detection is difficult, close or repair when found
1.1.2 Valve HP-1 (NO) (HP-V1A)	1. Fails closed due to internal fault	--	Letdown flow to Ltdn Cooler HP-C1A obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-V1B and use Ltdn Cooler HP-C1B
	2. Spuriously closed	Control Signal	Letdown flow to Ltdn Cooler HP-C1A obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-V1A
	3. Fails to close when required due to internal fault	--	Unobstructed letdown flow to Ltdn Cooler HP-C1A. Ltdn Cooler HP-C1A cannot be isolated if valve HP-1 (HP-V1A) is open	If HP-C1A has experienced a loss of cooling water, then letdown fluid temperature will increase; letdown flow to 3-way valve HP-14 (HP-V10) will continue until series isolation valve HP-3 (HP-V2A) or HP-5 (HP-V3) is closed to protect HP-X1. If HP-C1A has experienced a tube rupture, then an RC leak to CCW system will occur	Close series isolation valve None
	4. Fails to close when required due to unavailability of electric power	Electric Power	Unobstructed letdown flow to Ltdn Cooler HP-C1A. Ltdn Cooler HP-C1A cannot be isolated if valve HP-1 (HP-V1A) is open	If HP-C1A has experienced a loss of cooling water, then letdown fluid temperature will increase; letdown flow to 3-way valve HP-14 (HP-V10) will continue until series isolation valve HP-3 (HP-V2A) (powered from separate bus or manually closed) or HP-5 (HP-V3) is closed to protect HP-X1. If HP-C1A has experienced a tube rupture, then an RC leak to CCW system will occur	Close series isolation valve Restore electric power

Table B.3.1. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
1.1.3	Valve HP-2 (NC) (HP-V1B)	1. Fails open due to internal fault	--	Unobstructed letdown flow to Ltdn Cooler HP-C1B	Unless component cooling water provided to Ltdn Cooler HP-C1B, letdown temperature will increase possibly resulting in letdown isolation, i.e., termination of letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-4 (HP-V2B)
		2. Spuriously opened	Control Signal	Unobstructed letdown flow to Ltdn Cooler HP-C1B	Unless component cooling water provided to Ltdn Cooler HP-C1B, letdown temperature will increase possibly resulting in letdown isolation, i.e., termination of letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-2 (HP-V1B), close HP-4 (HP-V2B)
		3. Fails to open when required due to internal fault	--	Use of Ltdn Cooler HP-C1B prevented	May result in increased letdown temperature or continued letdown isolation	None (isolate and repair)
		4. Fails to open when required due to unavailability of electric power	Electric Power	Use of Ltdn Cooler HP-C1B prevented	May result in increased letdown temperature or continued letdown isolation	Restore electric power
1.1.4	Operating Letdown Cooler HP-C1A (or HP-C1B)	1. Loss of cooling water flow	Component Cooling Water System	Increased letdown temperature. High temperature sensed on TT-3 resulting in automatic closure of isolation valve HP-5 (HP-V3) and indicated in control room	Increased letdown fluid temperature possibly resulting in automatic letdown flow isolation, i.e., termination of letdown flow to 3-way valve HP-14 (HP-V10)	Isolate HP-C1A and utilize HP-C1B if cooling water available to HP-C1B. Restore letdown flow if it has been isolated
		2. Reduction in heat transfer capability due to fouling	--	Increased letdown temperature. High temperature sensed on TT-3 and indicated in control room	Increased letdown fluid temperature	Isolate HP-C1A, utilize HP-C1B

Table B.3.1. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
		3. Tube rupture	Component Cooling Water System	Reduced letdown flow rate due to flow diversion	Reduced letdown flow to 3-way valve HP-14 (HP-V10). Loss of reactor coolant to CCW system. Decreasing Ltdn tank level, RCS pressure. Safety injection signal will not isolate letdown cooler. Increased CCW surge tank level, discharge of reactor coolant through CCW relief valves to RB	Close HP-1 (HP-V1A) and HP-3 (HP-V2A), and open path through HP-C1B
1.1.5	Standby Letdown Cooler HP-C1B (or HP-C1A)	1. Tube rupture	Component Cooling Water System	Reduced letdown flow rate due to flow diversion	Reduced letdown flow to 3-way valve HP-14 (HP-V10). Loss of reactor coolant to CCW system. Decreasing Ltdn tank level, RCS pressure. Safety injection signal will isolate letdown cooler. Increased CCW surge tank level, discharge of reactor coolant through CCW relief valves to RB	Close or verify closure of HP-4 (HP-V2B); letdown flow through HP-C1A is possible once leak is isolated
1.1.6	Valve HP-3 (NO) (HP-V2A)	1. Fails closed due to internal fault	--	Letdown flow through HP-C1A is obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Close HP-1 (HP-V1A), open HP-2 (HP-V1B) to divert letdown flow through HP-C1B
		2. Spuriously closed	Control Signal	Letdown flow through HP-C1A is obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-3 (HP-V2A)
		3. Fails to close when required due to internal fault	--	Prevents isolation of HP-C1A	If HP-C1A has experienced a tube rupture, HP-1 (HP-V1A) has been closed, and HP-C1B is to be used, then an RC leak to the CCW system will occur. If HP-C1A has experienced a loss of cooling water and HP-1 (HP-V1A) can not be closed, then letdown fluid temperature will increase and HP-5 (HP-V3) will close terminating letdown flow to HP-14 (HP-V10)	None Automatic closure of HP-5 (HP-V3); HP-C1A cannot be isolated until HP-3 (HP-V2A) is repaired

Table B.3.1. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
		4. Fails to close when requtred due to unavailability of power on bus 1EXS21	Electric Power	Prevents isolation of HP-C1A	If HP-C1A has experienced a tube rupture, HP-1 (HP-V1A) has been closed, and HP-C1B is to be used, then an RC leak to the CCW system will occur. If HP-C1A has experienced a loss of cooling water and HP-1 (HP-V1A) cannot be closed, then letdown fluid temperature will will increase and HP-5 (HP-V3) will close terminating letdown flow to HP-14 (HP-V10)	None Automatic closure of HP-5 (HP-V3); HP-C1A cannot be isolated until power is restored on bus 1EXS21
		5. Fails to close when required due to failure of ES signal	Engineered Safeguards Protective System (ESPS)	Prevents isolation of HP-C1A	If HP-C1A has experienced a tube rupture, HP-1 (HP-V1A) has been closed, and HP-C1B is to be used, then an RC leak to the CCW system will occur. If HP-C1A has experienced a loss of cooling water and HP-1 (HP-V1A) cannot be closed, then letdown fluid temperature will increase and HP-5 (HP-V3) will close terminating letdown flow to HP-14 (HP-V10)	None Automatic closure of HP-5 (HP-V3); HP-C1A cannot be isolated until ES signal is restored
1.1.7	Valve HP-4 (NO) (HP-V2B)	1. Fails closed due to internal fault	--	None	None	Close HP-2 (HP-V1B) to divert letdown flow through HP-C1A
		2. Spuriously closed	Control Signal	None	None	Open HP-4 (HP-V2B)
		3. Fails to close when required due to internal fault	--	Prevents isolation of HP-C1B	If HP-C1B has experienced a tube rupture, then an RC leak to the CCW system will occur	None; HP-C1B cannot be isolated until HP-4 (HP-V2B) is repaired
		4. Fails to close when required due to unavailability of power on bus 1EXS21	Electric Power	Prevents isolation of HP-C1D	If HP-C1B has experienced a tube rupture, then an RC leak to the CCW system will occur	None; HP-C1B cannot be isolated until power is restored on bus 1FXS21

Table B.3.1. (continued)

Component	Potential Failure Mode		Immediate Effects		
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	5. Fails to close when required due to failure of ES signal	Engineered Safeguards Protective System (ESPS)	Prevents isolation of HP-C1B	If HP-C1B has experienced a tube rupture, then an RC leak to the CCW system will occur	None; HP-C1B cannot be isolated until ES signal is restored
1.2 Block Orifice:					
1.2.1 Miscellaneous Normally Closed Manual Valves Such as HP-36 or HP-332	1. Opened or fails open due to internal fault	Vent or Drain	Reduced letdown flow rate	Reduced letdown flow to 3-way valve HP-14 (HP-V10)	Though detection is difficult, close or repair when found
1.2.2 Valve HP-5 (NO) (HP-V3)	1. Fails closed due to internal fault	--	Letdown flow terminated	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Close HP-3 (HP-V2A), HP-4 (HP-V2B), and HP-6 (HP-V4) and repair
	2. Spuriously closed	Control Signal	Letdown flow terminated	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-5 (HP-V3)
	3. Fails to close when required due to internal fault	--	High temperature letdown flow to purification demineralizer is unobstructed. Increased letdown fluid temperature may result in melting the resin beads in HP-X1 and thus blocking flow	High temperature letdown flow possibly causing flow blockage if resin beads in HP-X1 melt	Close HP-6 (HP-V4). If purification resins damaged, use standby demineralizer
	4. Spuriously closed due to unavailability of instrument air (assumed)	Instrument Air	Letdown flow terminated	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Restore instrument air, open HP-5 (HP-V3)
	5. Fails to close when required due to unavailability of letdown temperature interlock	Plant Instrumentation	High temperature letdown flow to purification demineralizer is unobstructed. Increased letdown fluid temperature may result in melting the resin beads in HP-X1 and thus blocking flow	High temperature letdown flow possibly causing flow blockage if resin beads in HP-X1 melt	Close HP-6 (HP-V4) and restore temperature interlock. If purification resins damaged, use standby demineralizer

Table B.3.1. (continued)

	Component	Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
		6. Fails to close when required due to unavailability of ES sig al	Engineered Safeguards Protective System (ESPS)	Failure of one of two redundant containment isolation valves. High temperature letdown flow to purification demineralizer is unobstructed. Increased letdown fluid temperature may result in melting the resin beads in HP-I1 and thus blocking flow	None, if HP-6 (HP-V4) successfully closes. Otherwise, high temperature letdown flow possibly causing flow blockage if resin beads in HP-I1 melt	Close HP-6 (HP-V4) and restore ES signal. If purification resins damaged, use standby demineralizer
1.2.3	Valve HP-6 (MO) (HP-V4)	1. Fails closed due to internal fault	--	Letdown flow to purification demineralizer is obstructed unless HP-42 or HP-7 (HP-V5) is open	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated unless HP-42 or HP-7 (HP-V5) is open	Utilize HP-7 (HP-V5) for letdown throttling
		2. Spuriously clo ed	Control Signal	Letdown flow to purification demineralizer is obstructed unless HP-42 or HP-7 (HP-V5) is opca	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated unless HP-42 or HP-7 (HP-V5) is open	Open HP-6 (HP-V4) or HP-7 (HP-V5)
		3. Fails to close when required due to internal fault	--	Letdown flow to block orifice is unobstructed	If HP-5 (HP-V3) has failed to close and the letdown flow has not been cooled, then temperature of letdown flow to HP-14 (HP-V10) will continue to increase and resin beads in HP-I1 may melt causing flow blockage	Close HP-8 (HP-V7) to protect purification demineralizer HP-I1
		4. Fails to close when required due to unavailability of instrument air (assumed)	Instrument Air	Letdown flow to block orifice is unobstructed	If HP-5 (HP-V3) has failed to close and the letdown flow has not been cooled, then temperature of letdown flow to HP-14 (HP-V10) will continue to increase and resin beads in HP-I1 may melt causing flow blockage	Close HP-8 (HP-V7) to protect purification demineralizer HP-I1; restore instrument air
1.2.4	Block Orifice	1. Fails plugged	--	Letdown flow to purification demineralizer is obstructed if HP-42 and HP-7 (HP-V5) are closed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated if HP-42 and HP-7 (HP-V5) are closed	Utilize HP-7 (HP-V5) for letdown flow throttling
1.2.5	Flow Transmitter FT-29	1. Internal fault results in incorrect signal	Plant Instrumentation	None	Incorrect information sen' to plant operators	Isolate and repair
		2. Fails due to loss of powrr	Electric Power	None	Incorrect information seul to plant operators	Restore electric power

Table B.3.1. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
1.2.6	Valve HP-39 (NO)	1. Fails closed due to internal fault	--	Letdown flow to purification demineralizer is obstructed if HP-42 and HP-7 (HP-V5) are closed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated if HP-42 and HP-7 (HP-V5) are closed	Open HP-7 (HP-V5)
1.2.7	Valve HP-42 (NC)	1. Fails open due to internal fault	--	Unobstructed letdown flow through orifice bypass to purification demineralizer	Increased letdown flow to 3-way valve HP-14 (HP-V10)	Isolate block orifice to reduce letdown flow
1.2.8	Valve HP-40 (NO)	1. Fails closed due to internal fault	--	Letdown flow to HP-7 (HP-V5) is obstructed	None, if HP-7 (HP-V5) (NC) is closed. Otherwise, reduced letdown flow to 3-way valve HP-14 (HP-V10)	Open HP-42, if required
1.2.9	Valve HP-7 (NC) (HP-V5)	1. Fails open due to internal fault	--	Block orifice bypassed, increased letdown flow	Increased letdown flow to 3-way valve HP-14 (HP-V10), and potentially increased letdown temperatures	Close HP-40 and/or HP-41 and repair
		2. Spuriously opened	Control Signal	Block orifice bypassed, increased letdown flow	Increased letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-7 (HP-V5)
		3. Fails to open when required due to internal fault	--	Additional letdown flow not provided	Additional letdown flow not provided	Open HP-42 if required, close HP-40 and HP-41 and repair
		4. Fails to open when required due to unavailability of instrument air (assumed)	Instrument Air	Additional letdown flow not provided	Additional letdown flow not provided	Utilize HP-42, if required; restore instrument air
1.2.10	Valve HP-41 (NO)	1. Fails closed due to internal fault	--	Obstructs letdown flow to purification demineralizer if HP-7 (HP-V5) is open	Reduced letdown flow to 3-way valve HP-14 (HP-V10) if HP-7 (HP-V5) is open	Utilize HP-42 if required
1.2.11	Radiation Monitor Loop	1. Normally closed manual drain valve opened, fails open, or not closed after main'-nance, or relief valve spuriously opens	High Activity Waste Tank, Miscellaneous Waste Tank	Diversion of letdown flow when radiation monitoring loop used	Reduced letdown flow to 3-way valve HP-14 (HP-V10); flow diverted to Miscellaneous Waste Tank or High Activity Waste Tank	Isolate Loop; close valve or repair when found; sampling available at other points in subsystem
		2. Loop becomes plugged	--	Reduced letdown flow; radiation monitoring prevented	Reduced letdown flow to 3-way valve HP-14 (HP-V10)	Unplug when found; sampling available at other points in subsystem

Table B.3.1. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
1.2.12 Boron Meter Loop	1. Normally closed manual drain valve opened, fails open, or not closed after maintenance, or relief valve spuriously opens	High Activity DR Tank, Miscellaneous Waste Tank	Diversion of letdown flow when boron meter loop used	Reduced letdown flow to 3-way valve HP-14 (HP-V10); flow diverted to High Activity DR Tank or Miscellaneous Waste Tank	Isolate Loop; close valve or repair when found; sampling available at other points in subsystem
	2. Loop becomes plugged	--	Reduced letdown flow; boron content measurement prevented	Reduced letdown flow to 3-way valve HP-14 (HP-V10)	Unplug when found; sampling available at other points in subsystem
1.3 Purification Demineralizer:					
1.3.1 Flow Nozzle	1. Fail plugged	--	Letdown flow to purification demineralizer is obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is reduced or terminated	
1.3.2 Flow Transmitters FT-6, FT-6P, and FT-6A	1. Internal fault results in incorrect signal	Plant Instrumentation	None	None	Utilize FT-29 to determine letdown flow (requires HP-7 (HP-V5) and HP-42 be shut), repair transmitters; restore electric power
	2. Control power failure results in incorrect signal	Electric Power	None	None	
1.3.3 Pressure Gauge PG-73	1. Internal fault results in incorrect measurement	Plant Instrumentation	None	None	Repair when detected

Table B.3.1. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
1.3.4	Temperature Transmitter TT-3	1. Internal fault results in incorrect signal	Plant Instrumentation	If a spuriously high temperature signal is transmitted, HP-5 (HP-V3) is automatically closed, obstructing letdown flow to purification demineralizer	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-5 (HP-V3) after assessing failure; repair transmitter
				If a spuriously low temperature signal is transmitted, HP-5 (HP-V3) would not be automatically closed if required. Excessive letdown temperatures would result in purification demineralizer heating, or resin bead melting and flow blockage	High temperature letdown flow possibly causing flow blockage if resin beads in HP-I1 melt	Close HP-6 (HP-V4); repair transmitter
		2. Control power failure results in incorrect signal	Electric Power	If a spuriously high temperature signal is transmitted, HP-5 (HP-V3) is automatically closed, obstructing letdown flow to purification demineralizer	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-5 (HP-V3) after assessing failure; restore electric power
				If a spuriously low temperature signal is transmitted, HP-5 (HP-V3) would not be automatically closed if required. Excessive letdown temperatures would result in purification demineralizer heating, or resin bead melting and flow blockage	High temperature letdown flow possibly causing flow blockage if resin beads in HP-I1 melt	Close HP-6 (HP-V4); restore electric power
1.3.5	Miscellaneous Relief Valves Like RV-52 (HP-43) and Normally Closed, Manual Valves Like HP-44	1. Relief valve spuriously opens	Liquid Waste Drain	RC leak	Reduced letdown flow to 3-way valve HP-14 (HP-V10); RC leak	Isolate
		2. NC manual valve fails open due to internal fault	Sampling System	RC leak	Reduced letdown flow to 3-way valve HP-14 (HP-V10) if sample flow exists; RC leak	None (isolate and repair)
1.3.6	Valve HP-195 (NO)	1. Fails closed due to internal fault	--	Letdown flow to purification demineralizer is obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	None (isolate and repair)

Table B.3.1. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
1.3.7 Valve HP-196 (NC)	1. Fails open due to internal fault	Outlet of Letdown Filter HP-F1A	Reduced letdown flow to purification-demineralizer	Reduced letdown flow to 3-way valve HP-14 (HP-V10). (Letdown flow bypasses HP-I1 and HP-14 (HP-V10))	Close HP-57
1.3.8 Valve HP-197 (NC)	1. Fails open due to internal fault	Inlet of Letdown Filter HP-F1A	Reduced letdown flow to purification demineralizer	Reduced letdown flow to 3-way valve HP-14 (HP-V10). (Letdown flow bypasses HP-I1 and HP-14 (HP-V10))	Close HP-57
1.3.9 Valve HP-13 (NC) (HP-V6)	1. Fails open due to internal fault	--	Letdown flow bypasses the purification demineralizer; letdown flow chemistry altered	Letdown flow chemistry altered	None
	2. Spuriously opened	Control Signal	Letdown flow bypasses the purification demineralizer; letdown flow chemistry altered	Letdown flow chemistry altered	Close HP-13 (HP-V6)
	3. Fails to open when required due to internal fault	--	Purification demineralizer HP-I1 bypass unavailable if required	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated if HP-I1 is plugged	Open HP-9 (1HP-V8) and HP-11 (1HP-V9) and use HP-I2 if available
	4. Potential failure to open due to unavailability of instrument air (assumed)	Instrument Air	Purification demineralizer HP-I1 bypass unavailable if required	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated if HP-I1 is plugged	Restore instrument air; open HP-9 (1HP-V8) and HP-11 (1HP-V9) and use HP-I2 if available
1.3.10 Valve HP-8 (NO) (HP-V7)	1. Fails closed due to internal fault	--	Letdown flow through purification demineralizer HP-I1 is obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-9 (1HP-V8) and HP-11 (1HP-V9) and utilize purification demineralizer HP-I2 if not being used by Unit 2
	2. Spuriously closed	Control Signal	Letdown flow through purification demineralizer HP-I1 is obstructed	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Open HP-9 (1HP-V8) and HP-11 (1HP-V9) and utilize purification demineralizer HP-I2 if not being used by Unit 2

Table B.3.1. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
	3. Fails to close when required due to internal fault	--	Purification demineralizer HP-X1 isolation is unavailable	Continued letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-47
	4. Fails to close when required due to unavailability of instrument air (assumed)	Instrument Air	Purification demineralizer HP-X1 isolation is unavailable	Continued letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-47; restore instrument air
1.3.11 Purification Demineralizer HP-X1	1. Fail plugged	--	Letdown flow is blocked in purification demineralizer HP-X1	Letdown flow to 3-way valve HP-14 (HP-V10) is terminated	Isolate HP-X1 using HP-8 (HP-V7) and use HP-X2 if available or bypass by opening HP-13 (HP-V6) (reduced chemistry control)
1.3.12 Stop Check Valve HP-47	1. Fails plugged	--	Letdown flow through purification demineralizer HP-X1 is obstructed	Letuown flow to valve HP-14 (HP-V10) is terminated	Isolate HP-X1 using HP-8 (HP-V7) and use HP-X2 if available or bypass by opening HP-13 (HP-V6) (reduced chemistry control)
1.3.13 Valve HP-9 (NC) (1HP-V8)	1. Fails open due to internal fault	--	If purification demineralizer HP-X2 is being used by Unit 2, then the letdown flows of the two units may be mixed depending on the pressure difference between the two letdown flows	Increased or reduced letdown flow to 3-way valve HP-14 (HP-V10)	Remedial action dependent on Unit 2 operating requirements
	2. Spuriously opened	Control Signal	If purification demineralizer HP-X2 is being used by unit 2, then the letdown flows of the two units may be mixed depending on the pressure difference between the two letdown flows	Increased or reduced letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-9 (1HP-V8)

Table B.3.1. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	3. Fails to open when required due to internal fault	--	Prevents use of spare purification demineralizer HP-X2 by unit 1	Potential reduction in chemistry control	Continue to use HP-X1 if available or open HP-13 (HP-V6) and bypass HP-X1
	4. Potential failure to open due to unavailability of instrument air (assumed)	Instrument Air	Prevents use of spare purification demineralizer HP-X2 by unit 1	Potential reduction in chemistry control	Continue to use HP-X1 if available or open HP-13 (HP-V6) and bypass HP-X1; restore instrument air
1.3.14 Valve HP-11 (NC) (1HP-V9)	1. Fails open due to internal fault	--	If purification demineralizer HP-X2 is being used by unit 2, then the letdown flow of unit 2 will leak into the letdown flow of unit 1 if unit 2 letdown pressure is greater than unit 1 letdown pressure	Increased letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-10 (2HP-V8) and HP-12 (2HP-V9) depending on Unit 2 operating requirements
	2. Spuriously opened	Control Signal	If purification demineralizer HP-X2 is being used by unit 2, then the letdown flow of unit 2 will leak into the letdown flow of unit 1 if unit 2 letdown pressure is greater than unit 1 letdown pressure	Increased letdown flow to 3-way valve HP-14 (HP-V10)	Close HP-11 (1HP-V9)
	3. Fails to open when required due to internal fault	--	Prevents use of spare purification demineralizer HP-X2 by unit 1	Potential reduction in chemistry control	Continue to use HP-X1 if available or open HP-13 (HP-V6) and bypass HP-X1
	4. Potential failure to open due to unavailability of instrument air (assumed)	Instrument Air	Prevents use of spare purification demineralizer HP-X2 by unit 1	Potential reduction in chemistry control	Continue to use HP-X1 if available or open HP-13 (HP-V6) and bypass HP-X1; restore instrument air

Table B.3.2. RC pump seal water return
(Reference: FSAR Figure 9.3-2, Sheets 1 and 4)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
2.1	Seal Leak-off Line(s) (4 Total, 1/RCP):					
2.1.1	Pressure Transmitter(s) 1PT-19, 1PT-20, 1PT-21, 1PT-22	1. Instrument connection leak	--	Small loss of reactor coolant	Incorrect pressure signal to I&C system and control room	If accessible, repair component
		2. Transmitter failure due to internal faults	--	No effect	Incorrect pressure signal to I&C system and control room	If accessible, repair component
		3. Incorrect output due to loss of power	I&C System, Electric Power Supply	No effect	Incorrect pressure signal to I&C system and control room	Restore power supply
2.1.2	Motor Operated Isolation Valve(s) HP-228 (1HP-V43A), HP-232 (1HP-V43B), HP-226 (1HP-V43C), HP-230 (1HP-V43D)	1. Closes on spurious signal	I&C System	Flow stopped in single leak-off line	Seal leak-off flow from a single RC pump blocked, control room alarm	Attempt to open failed valve or open seal bypass valve (HP-275)
		2. Inadvertantly closed	--	Flow stopped in single leak-off line	Seal leak-off flow from a single RC pump blocked, control room alarm	Reopen valve
		3. Fails closed due to internal fault	--	Flow stopped in single leak-off line	Seal leak-off flow from a single RC pump blocked, control room alarm	Open seal bypass valve (HP-275)
		4. Valve fails to close when required due to control signal failure	I&C System	Flow not isolated	Subsystem not isolated from RCS	Close local valves on affected line
		5. Valve fails to close on demand	Electric Power Supply	Flow not isolated	Subsystem not isolated from RCS	Restore power, close local valves on affected line
		6. Valve fails to close on demand due to internal fault	--	Flow not isolated	Subsystem not isolated from RCS	Close local valves on affected line
2.1.3	Manual Isolation Valves (2/line) HP-205, HP-207, HP-212, HP-214, HP-219, HP-221, HP-259, HP-261	1. Valve failed closed (plugging, damaged, etc.)	--	Flow stopped in single leak-off line	Seal leak-off flow from a single RC pump blocked, control room alarm	Open bypass valve around failed valve (local action)
2.1.4	Flow Transmitter(s) 1FT-19, 1FT-20, 1FT-21, 1FT-22, 1FT-113, 1FT-114, 1FT-115, 1FT-116	1. Instrument connection leak	--	Small loss of reactor coolant	Incorrect flow signal to I&C system and control room	If accessible, isolate leaking transmitter(s), flow bypass available (local action just outside of secondary shielding)

Table B.3.2. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
2.1.4	Flow Transmitter(s) 1FT-19, 1FT-20, 1FT-21, 1FT-22, 1FT-113, 1FT-114, 1FT-115, 1FT-116 (cont'd)	2. Incorrect output due to loss of power	Electric Power Supply, I&C System	No effect	Incorrect flow signal to I&C system and control room	Restore power supply
		3. Transmitter failure due to internal fault	--	No effect	Incorrect flow signal to I&C system and control room	If accessible, utilize bypass, isolate component and repair (local action just outside of secondary shielding)
2.2	Seal Bypass Line(s) (Normally Closed, Open When #1 Seal-Leakoff Rate is Too Low) (4 Total, 1/RCP):					
2.2.1	Pressure Transmitter(s) 1PT-19, 1PT-20, 1PT-21, 1PT-22	1. Instrument connection leak	--	Small loss of reactor coolant	Incorrect pressure signal transmitted to I&C and control room	If accessible, repair component
		2. Incorrect output due to loss of power	Electric Power Supply, I&C System	No effect	Incorrect pressure signal transmitted to I&C and control room	Restore power supply
		3. Transmitter failure due to internal fault	--	No effect	Incorrect pressure signal transmitted to I&C and control room	If accessible, repair component
2.2.2	Check Valve(s) HP-263, HP-266, HP-269, HP-272	1. Valve failed closed (plugged, damaged, etc.)	--	Flow in a single bypass line stopped	Seal bypass flow path blocked from a single RC pump	If accessible, repair component
		2. Valve fails to prevent backflow	--	No effect during steady state	No effect during steady state	Repair component at shutdown
2.2.3	Manual Isolation Valves (2/line) HP-264, HP-265, HP-267, HP-268, HP-270, HP-271, HP-273, HP-274	1. Valve fails closed (plugged, damaged, etc.)	--	Flow in a single bypass line stopped	Seal bypass flow path blocked from a single RC pump	If accessible, repair component
2.2.4	Flow Transmitter(s) 1FT-109, 1FT-110, 1FT-111, 1FT-112	1. Instrument connection leak	--	Small loss of reactor coolant	Incorrect flow signal transmitted to I&C and control room	If accessible, repair component
		2. Transmitter failure due to internal fault	--	No effect	Incorrect flow signal transmitted to I&C and control room	If accessible, repair component
		3. Incorrect output due to loss of power	Electric Power Supply, I&C System	No effect	Incorrect flow signal transmitted to I&C and control room	Restore power supply

Table B.3.2. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
2.3 Seal Bypass Return Header:					
2.3.1 Motor Operated Isolation Valve HP-275 (HP-V48)	1. Valve fails to open when required due to control signal failure or closes on spurious signal	I&C System	Seal return bypass flow blocked	Seal return bypass flow path unavailable to all RC pumps	None
	2. Valve fails to open on demand or closes on spurious signal	Electric Power Supply	Seal return bypass flow blocked	Seal return bypass flow path unavailable to all RC pumps	Restore power
	3. Valve fails to open on demand due to internal fault	--	Seal return bypass flow blocked	Seal return bypass flow path unavailable to all RC pumps	Repair component if accessible
	4. Valve fails open or fails to close when required	I&C System, Electric Power Supply, Internal	No effect	No effect	Repair component if accessible
2.3.2 Motor Operated Isolation Valve to Stand Pipe Fill and Makeup HP-276 (HP-V49)	1. Valve fails open due to internal fault	--	Stand pipe fill lines open to seal return flow	Potential loss of vent on RCP vent seal	None
	2. Valve opens on spurious signal	I&C System	Stand pipe fill lines open to seal return flow	Potential loss of vent on RCP vent seal	None
2.4 Seal Water Cooler Inlet Header:					
2.4.1 Motor Operated Isolation Valve HP-20 (HP-V12)	1. Valve fails closed due to internal fault	--	Seal return flow stopped	Seal return flow from all RC pumps stopped	Repair component
	2. Valve closes on spurious signal	I&C System, ES	Seal return flow stopped	Seal return flow from all RC pumps stopped	None
	3. Valve inadvertantly closed	--	Seal return flow stopped	Seal return flow form all RC pumps stopped	Reopen valve
	4. Valve fails to close on demand	Electric Power Supply	Reactor building isolation degraded	Seal return flow continues to letdown storage tank	Restore power
	5. Valve fails to close when required	ES	Reactor building isolation degraded	No effect provided, redundant valve closes	None
	6. Valve fails to close when required	I&C System	Reactor building isolation degraded, seal return flow not isolated from coolers	Seal return flow continues to letdown storage tank	Utilize valve HP-21
	7. Valve fails to close on demand due to internal fault	--	Reactor building isolation degraded, seal return flow not isolated from coolers	Seal return flow continues to letdown storage tank	Utilize valve HP-21
2.4.2 Pneumatic Operated Isolation Valve HP-21 (HP-V13)	1. Valve fails closed (assuming valve is air-to-open)	Instrument Air	Seal return flow stopped	Seal return flow from all RC pumps stopped	Attempt to open valve locally
	2. Valve closes on spurious signal	I&C System	Seal return flow stopped	Seal return flow from all RC pumps stopped	Attempt to open valve locally
	3. Valve closes on spurious signal	ES	Seal return flow stopped	Seal return flow from all RC pumps stopped	Attempt to open valve locally

Table B.3.2. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	4. Valve fails closed due to internal fault	--	Seal return flow stopped	Seal return flow from all RC pumps stopped	Repair component
	5. Valve fails to close on demand due to internal fault	--	Reactor building isolation degraded, seal return flow not isolated from seal return coolers	Seal return flow continues to letdown storage tank	Utilize valve HP-20
	6. Valve fails to close when required	ES	Reactor building isolation degraded	No effect provided redundant valvs closes	None
	7. Valve fails to close when required	I&C System	Reactor building isolation degraded, seal return flow not isolated from coolers	Seal return flow continues to letdown storage tank	Utilize valve HP-20
2.4.3 Seal Return Filter Throttle Valve HP-277 (HP-V50)	1. Valve failed closed (plugged, damaged, etc.)	--	Seal return flow reduced or stopped	Seal return flow from all RC pumps reduced or stopped	Repair component
2.4.4 Seal Return Filter Isolation Valve(s) HP-278, HP-279	1. Valve failed closed (plugged, damaged, etc.)	--	Seal return flow reduced or stopped	Seal return flow from all RC pumps reduced or stopped	Open bypass valve (HP-280) around filter (local action)
2.4.5 Seal Return Filter	1. Filter plugged	--	Seal return flow reduced or stopped	Seal return flow from all RC pumps reduced or stopped high P transmitted on 1PT-114	Open bypass valve (HP-280) around filter (local action)
2.5 Seal Return Cooler(s):					
2.5.1 Manual Isolation Valve(s) HP-72, HP-74, HP-75, HP-77	1. Valve fails closed (plugging, damaged, stuck closed, etc.)	--	Seal return flow reduced or stopped	Seal water flow from all RC pumps reduced or stopped	Valve in spare cooler (local action)
2.5.2 Operating RC Seal Return Cooler HP-C1B (or Spare HP-C1A)	1. Heat exchanger tubes blocked	--	Seal return flow reduced or stopped	Seal water flow from all RC pumps reduced or stopped	Valve in spare cooler (local action) and repair blocked cooler
	2. Tube failure	RCW System	Loss of reactor coolant to RCW system	Reactor coolant leakage to RCW system, reduced seal water return to letdown storage tank	Valve in spare cooler (local action) or isolate seal return header from control room if required and take appropriate precautions for stopping seal return

Table B.3.2. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
	3. Loss of RCW	RCW System	Loss of seal return cooling (high cooler discharge temperature)	High temperature discharge to letdown storage tank, high temperature reading on TT-45 or TT-46	Valve in spare cooler if RCW is available to it (local action)
	4. Loss of heat transfer capability due to internal damage	--	Loss of seal return cooling (high cooler discharge temperature)	High temperature discharge to letdown storage tank, high temperature reading on TT-45 or TT-46	Isolate affected cooler and valve in spare (local action)
	5. Vapor lock in cooler	--	Reduction in seal return cooling capacity (high cooler discharge temperature)	High temperature discharge to letdown storage tank, high temperature reading on TT-45 or TT-46	Isolate affected cooler and valve in spare (local action)
2.5.3 Cooler Discharge Header Check Valve MP-189	1. Valve fails closed (plugging, damaged, etc.)	--	Seal return flow reduced or stopped	Seal return flow to letdown storage tank reduced or stopped, seal return flow from all RC pumps reduced or stopped	Repair component
	2. Valve fails to prevent backflow	Seal Water Coolers, Letdown Storage Tank, Makeup Filter(s) Discharge	No effect during steady state since pressures at outlet interfaces are lower than cooler discharge line pressure	No effect during steady state since pressures at outlet interfaces are lower than cooler discharge line pressure	No immediate action necessary, repair component
2.6 System Inlet Flows:					
2.6.1 Seal Injection Flow	1. Loss of flow	Seal Injection (Subsystem 4.0), RC Pumps	Seal return flow from RCS hotter than normal seal return	Slightly hotter discharge flow to letdown storage tank	None
2.6.2 HPI Pump Recirculation	1. Loss of flow	HPI Pumps (Subsystem 3.0)	Reduced flow through seal return coolers	Reduced flow and somewhat cooler discharge than normal to letdown storage tank	None
2.7 System Piping:					
2.7.1 Vents, Drains, Piping, Instrument Connections, etc.	1. System leaks	--	Loss of reactor coolant	Loss of reactor coolant, slightly reduced flow to letdown storage tank	Isolate leaks and repair as needed

Table B.3.3. HPI pump subsystem
(letdown storage tank (LST), inlet filters and HPI pumps)
(Reference: FSAR Figure 9.3-2, Sheet 1)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
3.1 Letdown (Makeup) Filters (2):					
3.1.1 Pneumatic Operated Inlet Valve(s) HP-17 (HP-V29A), HP-18 (HP-V29B)	1. Valve fails closed (assumed valve is air-to-open)	Instrument Air	Loss of flow to LST from letdown, chemical addition, and system makeup	Reduction and eventual loss of available makeup in LST	Utilize spare filter, open valve locally, bypass to LST, or switch to BWST if LST level is unacceptably low
	2. Valve fails closed due to internal fault	--	Loss of flow to LST from letdown, chemical addition, and system makeup	Reduction and eventual loss of available makeup in LST	Utilize spare filter, bypass to LST, or switch to BWST if LST level is unacceptably low
	3. Valve closes on spurious signal	I&C System	Loss of flow to LST from letdown, chemical addition, and system makeup	Reduction and eventual loss of available makeup in LST	Utilize spare filter, open valve locally, bypass to LST or switch to BWST if LST level is unacceptably low
	4. Valve inadvertently closed	--	Loss of flow to LST from letdown, chemical addition, and system makeup	Reduction and eventual loss of available makeup in LST	Reopen valve
	5. Valve fails to close when required	I&C, Electric Power Supply, Internal	Cannot isolate filter for maintenance	No effect	Repair component
3.1.2 Makeup Filter P Transmitter 1PT-15	1. Transmitter failure due to internal fault	--	Potential for undetected filter plugging	Incorrect pressure drop signal to I&C and control room	Monitor pressure drop with local gage
	2. Incorrect output due to loss of power	Electric Power Supply, I&C	Potential for undetected filter plugging	Incorrect pressure drop signal to I&C and control room	Monitor pressure drop with local gage
	3. Instrument connection leak	--	Small loss of reactor coolant and small reduction in flow to LST	Incorrect pressure drop signal to I&C and control room	Repair leak
3.1.3 Filter(s) HP-F1A, HP-F1B	1. Filter plugged	--	Letdown, chemical addition, and system makeup flow reduced or stopped	Reduced inventory in LST and high pressure drop signal to I&C from 1PT-15	Utilize spare filter or bypass filters via HP-19

Table B.3.3. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
3.1.4	Manual Filter Discharge Block Valve(s) HP-57, HP-58	1. Valve failed closed (plugging, damaged, etc.)	--	Loss of flow to LST from letdown, chemical addition, and system makeup	Reduction and eventual loss of available makeup in LST	Utilize spare filter path or bypass filters via HP-19
3.2	Letdown Storage Tank:					
3.2.1	Inlet Check Valve HP-78	1. Valve failed closed	Subsystem 2.0	Loss of all flow to LST, potential loss of NPSH to HPI pumps if LST level is too low	Reduction and eventual loss of available makeup in LST, flow blocked from seal return (Subsystem 2.0)	Monitor LST level, switch to BWST if LST level is unacceptably low
		2. Valve fails to prevent backflow	Subsystem 2.0 (Seal Return)	None during steady state	None since check valve HP-18 in Subsystem 2.0 is a backup	Repair component
3.2.2	Tank Vent Globe Valve HP-80	1. Valve failed closed (plugged, damaged, etc.)	Chemical Addition (Subsystem 6.0)	Loss of normal LST vent path, buildup of noncondensible gases in LST, potential reduction in H_2 mass transfer rate into reactor coolant	Potential reduction of H_2 concentration in reactor coolant and reduction in O_2 scavenging capability	Monitor LST pressure and level and repair component
3.2.3	Manual H_2/N_2 Supply/Isolation Valve H-111	1. Valve failed closed (plugged, damaged, etc.)	H_2 Bulk Storage, N_2 Blanketing System	Loss of H_2 addition to LST	Reduction in H_2 concentration in reactor coolant and reduction in O_2 scavenging capability	Repair component
3.2.4	Level Transmitters 1LT-33P1, 1LT-33P2	1. Transmitter failure due to internal fault	--	If selected transmitter indicates low flow from 3-way valve automatically transfers letdown flow to LST and operator may increase LST level with bleed holdup. Potential for LST tank overfilling, H_2 addition blockage, and lower H_2 concentration in RCS. If transmitter indicates high, operator may decrease letdown flow and potentially reduce NPSH on HPI pumps	Loss of or incorrect LST level indication, incorrect signal to 3-way valve interlock circuit and potential for reduced H_2 concentration in RCS. Operator response may also result in decreased letdown flow	Monitor with redundant transmitter

Table B.3.3. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
	2. Incorrect output due to loss of power to transmitter	Electric Power Supply, I&C System	If selected transmitter indicates low flow from 3-way valve automatically transfers letdown flow to LST and operator may increase LST level with bleed holdup. Potential for LST tank overfilling, H_2 addition blockage and lower H_2 concentration in RCS. If transmitter indicates high, operator may decrease letdown flow and potentially reduce NPSH on HPI pumps	Loss of or incorrect LST level indication, incorrect signal to 3-way valve interlock circuit and potential for reduced H_2 concentration in RCS. Operator response may also result in decreased letdown flow	Restore power supply or monitor with redundant transmitter if on a different power source
	3. Instrument connection leak	--	Small loss of LST inventory. Both transmitters affected. If selected transmitter indicates low flow from 3-way valve automatically transfers letdown flow to LST and operator may increase LST level with bleed holdup. Potential for LST tank overfilling, H_2 addition blockage, and lower H_2 concentration in RCS. If transmitter indicates high, operator may decrease letdown flow and potentially reduce NPSH on HPI pumps	Loss of or incorrect LST level indication, incorrect signal to 3-way valve interlock circuit and potential for reduced H_2 concentration in RCS. Operator response may also result in decreased letdown flow	Repair component
3.2.5 Pressure Transmitter 1PT-10	1. Incorrect output due to loss of power	Electric Power Supply, I&C System	No effect	Loss of or incorrect LST pressure indication	Restore power supply
	2. Transmitter failure	--	No effect	Loss of or incorrect LST pressure indication	Repair component
	3. Instrument connection leak	--	Small loss of LST inventory	Loss of or incorrect LST pressure indication	Repair component
3.3 HPI Pump Suction Headers:					
3.3.1 Motor Operated Isolation Valve HP-23 (HP-V21)	1. Valve fails closed	--	Flow to HPI pumps stopped, loss of NPSH to HPI pump resulting possible in pump damage	Immediate loss of flow to RC makeup and RC pump seals	Align supply from BWST via motor operated valves and align alternate HPI pump if required

Table B.3.3. (continued)

	Component	Potential Failure Mode		Immediate Effects		
		Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
		2. Valve closes on spurious signal	I&C System	Flow to HPI pumps stopped, loss of NPSH to HPI pump resulting possible in pump damage	Immediate loss of flow to RC makeup and RC pump seals	Manually open valve or align supply from BWST via motor operated valves and align alternate HPI pump if required
		3. Valve inadvertantly closed	--	Flow to HPI pumps stopped, loss of NPSH to HPI pump resulting possible in pump damage	Immediate loss of flow to RC makeup and RC pump seals	Reopen valve, align alternate HPI pump if required
		4. Valve fails to close when required	I&C System, Electric Power Supply, Internal Fault	LST discharge not isolated	No effect	Utilize local valves for isolation
3.3.2	Check Valve HP-97	1. Valve fails closed	--	Flow to HPI pump stopped, loss of NPSH to HPI pump resulting in possible pump damage	Immediate loss of flow to RC makeup and RC pump seals	Align supply from BWST via motor operated valves and align alternate HPI pump if required
		2. Valve fails to prevent backflow	--	No effect during steady state operation	No effect during steady state operation	Monitor pressure and level in LST. Isolate LST if BWST flow is aligned
3.3.3	Motor Operated Isolation Valve HP-98 (HP-V28A)	1. Valve fails closed	--	Flow to HPI pump 1A stopped, if in use pump 1A may be damaged	If HP-P1A in use, loss of flow to RC makeup and seal injection. If HP-P1B in use, no effect	Trip HPI pump 1A and use pump 1B
		2. Valve inadvertantly closed	--	Flow to HPI pump 1A stopped, if in use pump 1A may be damaged	If HP-P1A in use, loss of flow to RC makeup and seal injection. If HP-P1B in use, no effect	Trip HPI pump 1A and use pump 1B
		3. Valve closes on spurious signal	I&C System	Flow to HPI pump 1A stopped, if in use pump 1A may be damaged	If HP-P1A in use, loss of flow to RC makeup and seal injection. If HP-P1B in use, no effect	Trip HPI pump 1A and use pump 1B
		4. Valve fails to close on demand	--	Cannot remotely isolate pump HP-P1A for maintenance	No effect	Isolate pump HP-P1A with manual valves. If desired, utilize one of 2 remaining HPI pumps

Table B.3.3. (continued)

Component	Potential Failure Mode		Immediate Effects		
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	5. Valve fails to close when required	I&C System	Cannot remotely isolate pump HP-P1A for maintenance	No effect	Isolate pump HP-P1A with manual valves. If desired, utilize one of 2 remaining HPI pumps
	6. Valve fails to close when required	Electric Power Supply	Cannot remotely isolate pump HP-P1A for maintenance	No effect	Isolate pump HP-P1A with manual valves. If desired, utilize one of 2 remaining HPI pumps
3.3.4 Manual Isolation Valves HP-99 (HP-V28B), HP-100 (HP-V28C), HP-111 (HP-V26C)	1. Valve fails closed (plugging, damaged, etc.)	--	Suction to standby pump HP-P1C blocked. If pump is started, pump may be damaged	If pump HP-P1C in use, loss of flow to RC makeup and seal injection. If other pump in use, no effect	Utilize alternate HPI pump
3.3.5 Manual Isolation Valve HP-107 (HP-V26B)	1. Valve fails closed (plugging, damaged, etc.)	--	Suction to standby pump HP-P1B blocked. If pump is started, pump may be damaged	If pump HP-P1B in use, loss of flow to RC makeup and seal injection. If other pump in use, no effect	Utilize alternate HPI pump
3.3.6 Manual Isolation Valve HP-103 (HP-V26A)	1. Valve fails closed (plugging, damaged, etc.)	--	Flow to operating pump HP-P1A blocked. Unless pump is tripped, pump damage could occur	If pump HP-P1A in use, loss of flow to RC makeup and seal injection. If other pump in use, no effect	Trip HPI pump 1A and utilize pump 1B
3.4 HPI Pumps and Discharge Manifold:					
3.4.1 Operating HPI Pump HP-P1A	1. Mechanical failure to operate	--	No discharge flow from failed pump	No flow to RC makeup or RC pump seals	Utilize alternate HPI pump
	2. Pump fails due to loss of power	Electric Power Supply	No discharge flow from failed pump	No flow to RC makeup or RC pump seals	Restore power or utilize an alternate HPI pump on another power source
3.4.2 Spare HPI Pumps HP-P1B, HP-P1C	1. Pump fails to start due to signal failure	I&C System	No discharge flow from pump demanded	If pump is demanded because of failure with operating pump, no flow to RC makeup or RC pump seals. If pumps are just being switched, no effect	Utilize alternate HPI pump, repair circuit

Table B.3.3. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	2. Pump fails to start due to internal fault	--	No discharge flow from pump demanded	If pump is demanded because of failure with operating pump, no flow to RC makeup or RC pump seals. If pumps are just being switched, no effect	Utilize alternate HPI pump, repair pump
3.4.3 Discharge Check Valve(s) HP-105, HP-108	1. Valve in operating pump discharge fails closed (plugging, damaged, etc.)	--	No discharge flow through failed valve	No flow from operating HPI pump to RC makeup or RC pump seals	Utilize alternate HPI pump
	2. Valve in standby pump discharge fails to prevent backflow	--	Backflow through a nonoperating spare pump to suction of operating pump (potential HPI pump damage)	Reduced flow to seal injection and/or makeup	Isolate failed check valve (local action). Monitor critical flows
3.4.4 Recirculation Line(s) Associated With Pumps: HP-P1A, HP-P1B, HP-P1C	1. Line blockage due to plugged block valve or orifice	Seal Return Cooler Inlet (Subsystem 2.0)	Potential damage to HPI pump via pump deadheading if pump discharge to makeup and seal injection is not enough for pump operation	Potential loss of RC makeup and seal injection	Utilize alternate HPI pump (other action available from outside the subsystem)
3.4.5 Discharge Block Valve(s) HP-106 (HP-V34A), HF-110 (HP-V34B), HP-114 (HP-V34C)	1. Valve in operating pump discharge fails closed (plugged, damaged, etc.)	RCP Seals, Reactor Inlet Line Loops A, B and Crossovers A and B	No discharge flow through failed valve	No discharge flow from operating HPI pump to RC pumps seals or RC makeup	Utilize alternate HPI pump
3.4.6 Motor Operated Isolation Valve HP-115 (HP-V35A)	1. Valve closes on spurious signal	I&C System	If pump HP-P1A operating, flow to seal injection is stopped. If pump HP-P1B is operating, flow to normal RC makeup is stopped	If pump HP-P1A operating, flow to seal injection is stopped. If pump HP-P1B is operating, flow to normal RC makeup is stopped	If operating pump is HP-P1A, start pump HP-P1B. If operating pump is HP-P1B, start HP-P1A or (for unthrottled makeup) open valve HP-118 to reactor inlet LOOP B

Table B.3.3. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	2. Valve fails closed due to internal fault	--	If pump HP-P1A operating, flow to seal injection is stopped. If pump HP-P1B is operating, flow to normal RC makeup is stopped	If pump HP-P1A operating, flow to seal injection is stopped. If pump HP-P1B is operating, flow to normal RC makeup is stopped	If operating pump is HP-P1A, start pump HP-P1B. If operating pump is HP-P1B, start HP-P1A or (for unthrottled makeup) open valve HP-118 to reactor inlet LOOP B
	3. Valve inadvertantly closed	--	If pump HP-P1A operating, flow to seal injection is stopped. If pump HP-P1B is operating, flow to normal RC makeup is stopped	If pump HP-P1A operating, flow to seal injection is stopped. If pump HP-P1B is operating, flow to normal RC makeup is stopped	Reopen valve
	4. Valve fails to close when required	I&C System, Electric Power Supply, or Internal Fault	Intended isolation not effected	No effect on steady state operation	Utilize local isolation valves
3.4.7 Isolation Valve HP-118 (HP-V35B)	1. Valve fails open (damaged, etc.)	--	Loss of separation between HPI injection paths A and B	No effect during normal operation since injection path B is normally closed	Utilize HP-117 for isolation
3.4.8 Isolation Valve HP-117 (HP-V35C)	1. Valve fails closed (plugging, damaged, etc.)	--	Loss of ability to use HP-P1B as spare for safety injection to cold leg B	Loss of ability to use HP-P1B as spare for safety injection to cold leg B	Repair component
3.5 System Inlet Flows:					
3.5.1 Reactor Coolant Letdown Inlet Flow	1. Loss of flow	Subsystem 1.0	Reduction and eventual loss of available makeup in LST, loss of letdown flow to subsystem	Loss of letdown flow to subsystem	Monitor LST level and utilize supply from BWST, bleed holdup tank, or boric acid tank
3.5.2 RC Bleed Makeup Feed Inlet Flow	1. Loss of flow	Subsystem 6.0	If in letdown/bleed and feed operating mode, reduction in LST level	Loss of batch inputs to LST from RC bleed makeup	Restore letdown flow to LST
3.5.3 RCP Seal Return Inlet Flow	1. Loss of flow	Subsystem 2.0	Partial loss of flow to LST, loss of HPI pump recirculation	Potential long-term loss of LST level and requirement to switch to BWST suction	Monitor LST level, utilize RC bleed makeup or BWST if required

Table B.3.3. (continued)

Component	Potential Failure Mode		Immediate Effects		
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
3.6 System Piping:					
3.6.1 Vents, Drains, Piping, Instrument Connections, etc.	1. System leaks	--	Loss of reactor coolant, potential for loss of NPSH to HPI pumps	Loss of reactor coolant, potential for slight reduction in makeup flow or seal injection	Isolate leak, utilize supply from BWST if required

Table B.3.4. RC pump seal return subsystem
(Reference: FSAR Figure 9.3-2, Sheets 1 and 4)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
4.1 RC Pumps Seal Injection Header:					
4.1.1 Seal Injection Header Manual Isolation Valve HP-126 (HP-V27B)	1. Valve fails closed (plugged, damaged, etc.)	--	Seal injection flow stopped	Seal injection flow to RC pumps stopped	Repair component
4.1.2 Seal Injection Header Pressure Transmitter 1PT-18	1. Incorrect output due to loss of power	I&C System, Electric Power Supply	No effect	Incorrect pressure signal	Repair component
	2. Instrument connection leak	--	Small loss of reactor coolant	Incorrect pressure signal	Repair component
	3. Transmitter failure due to internal fault	--	No effect	Incorrect pressure signal	Repair component
4.2 RC Pump Seal Filters:					
4.2.1 Operating Filter Manual Isolation Valves HP-29, HP-132, HP-133, HP-134	1. Valve fails closed (plugged, damaged, etc.)	--	Flow through filter stopped	Seal injection flow to RC pumps stopped	Valve in spare filter path, or bypass both main and standby filters (local action)
4.2.2 Operating Seal Filter HP-F-1B (HP-F-1A Standby)	1. Filter plugged	--	Flow through filter stopped	Seal injection flow to RC pumps stopped	Valve in spare filter path, or bypass both main and standby filters (local action)
4.2.3 Manual Isolation Valves for Standby Filter or Bypass HP-28, HP-135	1. Valve fails to open on demand	--	No effect during normal operation. Loss of spare or bypass capacity	No effect during normal operation when spare or bypass is not demanded	If one of these backups has failed, utilize the remaining one if required
4.2.4 Standby Filter Manual Isolation Valves HP-129, HP-130, HP-131	1. Valve fails closed (plugged, damaged, etc.)	--	Flow through standby filter prevented	No effect	Valve in filter bypass if required (local action)
4.3 Seal Injection Flow Control:					
4.3.1 Flow Orifice	1. Orifice plugged	--	Seal injection flow reduced or stopped and control signal to throttle valve incorrect	Seal injection flow to RC pumps stopped	Repair component

Table B.3.4. (continued)

	Component	Potential Failure Mode		Immediate Effects		
		Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
4.3.2	Flow Controller/ Transmitter 1FT-75	1. Transmitter failure	Electric Power Supply, I&C System, Internal Fault	Incorrect signal to flow control valve, potentially resulting in too much or too little flow.	Negligable effect for high flow since flow is throttled downstream. On low flow, reduced seal injection flow to RC pumps. Incorrect signal to I&C system	Monitor and control flow from individual seal injection lines if required
4.3.3	Flow Control Valve HP-31 (HP-V42)	1. Valve fails open (valve assumed air-to-close)	Instrument Air	Full HPI pump discharge flow to individual seal injection lines	Negligable effect on seal injection supply	Manually control seal flow with HP-140 or with individual seal injection line throttle valves (local action)
		2. Valve fails open	Control Signal from 1FT-75, Electric Power Supply	Full HPI pump discharge flow to individual seal injection lines	Negligable effect on seal injection supply	Manually control seal flow with HP-140 or with individual seal injection line throttle valves (local action)
		3. Valve fails open due to internal damage	--	Full HPI pump discharge flow to individual seal injection lines	Negligable effect on seal injection supply	Manually control seal flow with HP-140 or with individual seal injection line throttle valves (local action)
		4. Valve fails closed	Control Signal from 1FT-75, Electric Power Supply	Seal injection flow reduced or stopped	Seal injection flow to RC pumps stopped	Valve in bypass and manually control seal flow from header (HP-140) or from individual seal injection lines (local action)
		5. Valve fails closed due to internal damage or plugging, etc.	--	Seal injection flow reduced or stopped	Seal injection flow to RC pumps stopped	Valve in bypass and manually control seal flow from header (HP-140) or from individual seal injection lines (local action)

Table B.3.4. (continued)

Component	Potential Failure Mode		Immediate Effects		
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
4.3.4 Manual Isolation Valve(s) HP-138, HP-139	1. Valve fails closed (plugged, damaged, etc.)	--	Seal injection flow stopped	Seal injection flow to RC pumps stopped	Valve in bypass and manually control seal flow from header (HP-140) or from individual seal injection lines (local action)
4.4 Individual RC Pump Seal Injection Lines (4 Total, 1/RC Pump):					
4.4.1 Flow Transmitter(s) 1FT-101, 1FT-102, 1FT-103, 1FT-104	1. Incorrect output due to loss of power	I&C System, Electric Power Supply	No effect	Incorrect flow signal to control room	Restore power
	2. Instrument connection leak	--	Small loss of reactor coolant	Incorrect flow signal to control room	Repair component if accessible
	3. Transmitter failure due to internal fault	--	No effect	Incorrect flow signal to control room	Repair component if accessible
4.4.2 Manual Throttle Valve(s) HP-64, HP-65, HP-66, HP-67	1. Valve fails closed (plugged, damaged, etc.)	--	Seal injection flow in affected line stopped	Seal injection flow to one RC pump stopped	Repair component if accessible
	2. Valve fails open	--	Flow in affected line unthrottled	Seal injection flow to a single RC pump higher than setpoint	Repair component, utilize stop check valves in line on short term basis for flow throttling if required (local action)
4.4.3 Check Valves (2/line) HP-144, HP-145, HP-146, HP-147, HP-283, HP-284, HP-286, HP-393	1. Valve fails closed	--	Flow in affected seal injection line stopped	Seal injection flow to a single RC pump stopped	Repair component if accessible
	2. Valve fails to prevent backflow	--	No effect since there are 2 check valves per line (one inside and one outside RB)	No effect since there are 2 check valves per line	Repair component at shutdown
4.4.4 Manual Isolation Valves On Line to RC Pump HP-394, HP-285	1. Valve fails closed	--	Flow in affected Seal Injection line stopped	Seal injection flow to a single RC pump stopped	Repair component if accessible
4.5 System Inlet Flows:					
4.5.1 Seal Injection Flow From HPI Pumps	1. Loss of flow	Subsystem 3.0	No flow	Loss of Seal Injection to RC pumps	None

Table B.3.4. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
4.6 System Piping:					
4.6.1 Vents, Drains, Piping, Instrument Connections, etc.	1. System leaks	--	Loss of reactor coolant	Loss of reactor coolant, potential for slight reduction in seal injection rate if leak is downstream of flow control valve (HP-31)	Isolate leaks and repair as needed

Table B.3.5. Reactor coolant makeup subsystem
(Reference: FSAR Figure 9.3-2, Sheets 1 and 4)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
5.1 Reactor Inlet Line Loop & Header:					
5.1.1 Manual Isolation Valve HP-118 (HP-V27A)	1. Valve fails closed (plugging, damaged, etc.)	--	Makeup flow stopped	Loss of normal makeup flow	Repair component, if required provide makeup flow via Loop B injection path (open local HP-18 and throttle with remote HP-27)
5.1.2 Flow Transmitter 1FT-7, 7A and 7B	1. Transmitter failure due to internal fault	--	No effect	Incorrect flow signal on one transmitter	Repair component
	2. Incorrect output due to signal failure	I&C System, Electric Power Supply	No effect	Incorrect flow signal from all 3 transmitters	Restore power supply
	3. Instrument connection leak	--	Small loss of reactor coolant	Incorrect flow signals from all 3 transmitters	Repair component
5.1.3 Motor Operated Valve HP-26 (HP-V24A)	1. Valve opens on spurious signal	I&C System	Makeup flow is not throttled	Increased makeup flow, increased pressurizer level, drop in LST level, potential loss of HPI pump NPSH	Manually close valve (local action)
	2. Valve opens on spurious signal	ES	Makeup flow is not throttled	Increased makeup flow, increased pressurizer level, drop in LST level, potential loss of HPI pump NPSH	Manually close valve (local action)
	3. Valve inadvertantly opened	--	Makeup flow is not throttled	Increased makeup flow, increased pressurizer level, drop in LST level, potential loss of HPI pump NPSH	Close valve
	4. Valve fails open due to internal fault	--	Makeup flow is not throttled	Increased makeup flow, increased pressurizer level, drop in LST level, potential loss of HPI pump NPSH	Isolate with HP-118 (local action) (will stop makeup flow)
	(Modes involving failure to open are part of emergency HPI and not included here)				
5.2 Minimum Flow Bypass Loops:					
5.2.1 Manual Isolation Valve HP-234	1. Valve fails closed (plugging, damaged, etc.)	--	No flow through minimum flow loop	No cooling flow to pressurizer spray line or cold leg inlet nozzles, no effect on makeup capacity	Repair component

Table B.3.5. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
5.2.2	Flow Transmitters 1FT-117, 1FT-118	1. Instrument connection leak	--	Small loss of coolant	Incorrect flow signal to control room	Repair component
		2. Incorrect output due to loss of power	Electric Power Supply, I&C System	No effect	Incorrect flow signal to control room	Restore power supply
		3. Transmitter failure due to internal fault	--	No effect	Incorrect flow signal to control room	Repair component
5.2.3	Manual Throttle Valve HP-241	1. Valve fails closed (plugging, damaged, etc.)	--	Minimum flow path blocked to one of two reactor cold leg inlet nozzles	No cooling flow to one cold leg inlet nozzle	Repair component
		2. Valve fails open	--	Minimum flow path unthrottled to one of two reactor cold leg inlet nozzles, automatic reduction in flow through normal makeup valve	Excess flow (full HPI pump discharge to minimum flow loop) to one reactor cold leg inlet nozzle, potential drop in LST level	If required valve HP-234 available to block flow into loop (local action), repair component
5.2.4	Manual Throttle Valve HP-235	1. Valve fails closed (plugging, damaged, etc.)	--	Minimum flow path blocked to pressurizer spray line and one of two reactor cold leg inlet nozzles	No effect on reactor makeup, but no cooling flow to pressurizer spray line or to one cold leg inlet nozzle	Repair component
		2. Valve fails open	--	Minimum flow path unthrottled to pressurizer spray line and one of two reactor cold legs, automatic reduction in flow through normal makeup valve	Excess flow to pressurizer spray line and to one reactor cold leg inlet nozzle, potential drop in LST level	Close valve HP-234, or valves HP-340 and HP-356 in reactor building (local action)
5.2.5	Manual Isolation Valve HP-340	1. Valve fails closed (plugging, damage, etc.)	--	Minimum flow path blocked to pressurizer spray line	No bypass flow to pressurizer spray line	Repair component
5.2.6	Manual Isolation Valve HP-356	1. Valve fails closed (plugging, damage, etc.)	--	Minimum flow path blocked to one of two reactor cold legs	No bypass cooling flow to one of two reactor cold leg inlet nozzles (no effect on normal makeup)	Repair component
5.3	Normal Makeup Flow Control Loop:					
5.3.1	Flow Transmitter 1FT-10, 10A, 10B	1. Instrument connection leak	--	Small loss of coolant	Incorrect flow signal from all transmitters	Monitor flow with FT-7, repair component
		2. Incorrect output due due to loss of power	Electric Power Supply, I&C System	No effect	Incorrect flow signal from all transmitters	Monitor flow with FT-7, restore powere supply
		3. Transmitter failure	--	None	Incorrect flow signal from failed transmitter	Monitor flow with FT-7, repair component

Table B.3.5. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
5.3.2	Flow Control Valve HP-120 (HP-V23)	1. Valve fails closed (assuming valve is air-to-open)	Instrument Air	Normal flow to reactor inlets stopped, flow through minimum flow loop continues	Bypass flow continues. Overall significant reduction in makeup flow	If required, manually control with bypass valve HP-26
		2. Valve fails closed due to internal fault	--	Normal flow to reactor inlets stopped, flow through minimum flow loop continues	Bypass flow continues. Overall significant reduction in makeup flow	If required, manually control with bypass valve HP-26
		3. Valve closes down due to incorrect control signal	I&C System	Normal flow to reactor inlets reduced, flow through minimum flow loop continues	Bypass flow continues. Overall significant reduction in makeup flow	If required, manually control with bypass valve HP-26
		4. Valve fails open due to internal fault	--	HPI flow not throttled. Excess makeup flow to RCS	Excess makeup flow to RCS, temporary decreased bypass flow to pressurizer spray line, potential drop in LST holdup, potential loss of NPSH to HPI pump	Isolate valve HP-120 and manually control flow with bypass valve HP-26
		5. Valve opens up due to incorrect control signal	I&C System	HPI flow not throttled. Excess makeup flow to RCS	Excess makeup flow to RCS, temporary decreased bypass flow to pressurizer spray line, potential drop in LST holdup, potential loss of NPSH to HPI pump	Isolate valve HP-120 and manually control flow with bypass valve HP-26
5.3.3	Manual Isolation Valves HP-119, HP-121	1. Valve fails closed (plugging, damage, etc.)	--	Normal makeup flow to RCS stopped, bypass flow through minimum flow loop continues	Bypass flow continues. Overall significant reduction in makeup flow	Isolate valve HP-120 and manually control flow with bypass valve HP-26
5.3.4	Check Valve HP-194	1. Valve fails closed (plugging, damage, etc.)	--	Normal makeup flow to RCS stopped, bypass flow through minimum flow loop continues	Bypass flow continues Overall significant reduction in makeup flow	If required, provide makeup flow via Loop B injection path (open local HP-118 and throttle with remote HP-27)
		2. Valve fails to prevent backflow	--	No effect during steady state operation	No effect during steady state operation	Repair component at shutdown
5.3.5	Inlet Line Orifices	1. Orifice plugged	--	Normal flow to one of two cold legs stopped or reduced, increased flow to the other cold leg	Flow imbalance between the two reactor cold legs	Repair component

Table B.3.5. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
5.3.6 Inlet Line Check Valves HP-126, HP-127	1. Valve failed closed (plugging, damage, etc.)	--	Normal flow to one of two reactor cold legs stopped or reduced, increased flow to the other cold leg	Flow imbalance between the two reactor cold legs	Repair component
5.4 Subsystem Input:					
5.4.1 Flow From HPI Pumps	1. Loss of flow	Subsystem 3.0	Loss of makeup flow and flow to pressurizer spray line	Loss of makeup flow and bypass flow to pressurizer spray line	None
	2. Reduced flow	Subsystem 3.0	Reduced makeup flow and reduced flow to pressurizer spray line	Reduced makeup flow and bypass reduced flow to pressurizer spray line	None
5.5 System Piping:					
5.5.1 Vents, Drains, Piping, Instrument Connections, etc.	1. System leaks	--	Loss of reactor coolant	Loss of reactor coolant, potential for reduction in reactor coolant makeup rate	Isolate leaks and repair as needed

Table B.3.6. Chemical processing subsystem
(References: FSAR Figures 9.3-1, Sheet 1; 9.3-2, Sheet 3; 9.3-5, Sheet 1, 3, and 4)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.1 Chemical Addition:					
6.1.1 Manual Control Valve (N-83)	1. N_2 blanket system fails	N_2 Blanket	Possible N_2H_4 backflow; no N_2 blanket in N_2H_4 drum	No N_2H_4 available to makeup filters	Close oontrol valve N-83
	2. Valve fails closed	--	No N_2 blanket in N_2H_4 drum; possible explosive mixture	Probably none	
6.1.2 Check Valve (N-84)	1. Fails to prevent backflow	--	N_2H_4 backflow; possible explosive mixture	No N_2H_4 available to makeup filters	Close control valve N-83
6.1.3 Hydrazine Drum	1. Drum leaks	--	Possible explosive mixture; eventual loss of suction pressure to pump	Eventual loss of N_2H_4 available to makeup filters	Isolate drum and replace
	2. Drum emptied	--	No N_2H_4	No N_2H_4 available to makeup filters	Isolate drum and replace
6.1.4 Manual Isolation Valves (CA-88, CA-45)	1. Valves fail closed	--	No N_2H_4	No N_2H_4 available to makeup filters	None
6.1.5 Manual Isolation Valves (CA-52, CA-54)	1. Valves fail closed	--	No N_2H_4	None if alternate flow path available	Open CA-46; crossover to pump CA-P3
6.1.6 Hydrazine Pump (CA-P4)	1. Electric power supply fails	Electric Power	Pump stops; no N_2H_4	None if alternate flow path available	Open CA-46; crossover to pump CA-P3
	2. Pump fails	--	No N_2H_4	None if alternate flow path available	Open CA-46; crossover to pump CA-P3
6.1.7 Check Valve (CA-56)	1. Fails to prevent backflow	--	Possible backflow to drum if pump is not running	No N_2H_4 available to makeup filters	Close CA-54
6.1.8 Manual Isolation Valve (DW-121)	1. Demineralized water supply fails	Demineralized Water	No demineralized water to tank	No LiOH available to makeup filters	None
	2. Valve fails closed	--	No demineralized water to tank	No LiOH or incorrect LiOH concentration available to makeup filters	Concentration checked via sampling
	3. Valve fails open	--	Dilutes LiOH in tank	Incorrect LiOH concentration available to makeup filters	Concentration checked via sampling
6.1.9 LiOH Mix Tank (CA-T3)	1. Tank leaks	--	Eventual loss of suction pressure to pump	Eventual loss of LiOH available to makeup filters	None
	2. Tank empties	--	No LiOH	No LiOH available to makeup filters	None
6.1.10 Sampling, Waste Lines	1. Lines fail open	--	Decreased LiOH	Decreased LiOH available to makeup filters	None

Table B.3.6. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
6.1.11 Manual Isolation Valve (CA-44)	1. Valve fails closed	--	No LiOH	No LiOH available to makeup filters	None
6.1.12 Manual Isolation Valve (CA-47, CA-49)	1. Valves fail closed	--	No LiOH	None if alternate flow path available	Open CA-46; crossover to pump CA-P4
6.1.13 LiOH Pump (CA-P3)	1. Electric power supply fails	Electric Power	Pump stops; no LiOH	None if alternate flow path available	Open CA-46; crossover to pump CA-P4
	2. Pump fails	--	No LiOH	None if alternate flow path available	Open CA-46; crossover to pump CA-P4
6.1.14 Check Valve (CA-51)	1. Fails to prevent backflow	--	Possible backflow to tank if pump is not running	No LiOH available to makeup filters	Close CA-49
6.1.15 Manual Isolation Valve (DW-120)	1. Demineralized water supply fails	Demineralized Water	No demineralized water to tank; no caustic or incorrect caustic concentration available to boron recovery	No caustic or incorrect caustic concentration available to LPI pumps	Concentration checked via sampling
	2. Valve fails closed	--	No demineralized water to tank; no caustic or incorrect caustic concentration available to boron recovery	No caustic or incorrect caustic concentration available to LFI pumps	Concentration checked via sampling
	3. Valve fails open	--	Dilutes caustic in tank; incorrect caustic concentration available to boron recovery	Incorrect caustic concentration available to LPI pumps	Concentration checked via sampling
6.1.16 Caustic Mix Tank (CA-T1)	1. Tank leaks	--	Eventual loss of suction pressure to pump	Eventual loss of caustic available to LPI pumps	None
	2. Tank empties	--	No caustic available to boron recovery	No caustic available to LPI pumps	None
6.1.17 Manual Isolation Valves (CA-34, CA-35, CA-37)	1. Valves fail closed	--	No caustic available to boron recovery	No caustic available to LPI pumps	None
6.1.18 Caustic Pump (CA-P1)	1. Electric power supply fails	Electric Power	Pump stops; no caustic available to boron recovery	No caustic available to LPI pumps	None
	2. Pump fails	--	No caustic available to boron recovery	No caustic available to LPI pumps	None
6.1.19 Sampling, Waste Lines	1. Lines fail open	--	Decreased caustic available to boron recovery	Decreased caustic available to LPI pumps	None

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.2 Boric Acid Addition:					
6.2.1 Manual Isolation Valve (DW-118)	1. Demineralized water supply fails	Demineralized Water	No demineralized water to tank; no boric acid or incorreot boric acid concentration available to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Concentration checked via sampling
	2. Valve fails closed	--	No demineralized water to tank; no boric acid or incorrect boric acid concentration available to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Concentration checked via sampling
	3. Valve fails open	--	Dilutes boric acid; incorrect boric acid concentration to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Concentration checked via sampling
6.2.2 Boric Acid Mix Tank (CA-T2)	1. Electric power supply fails	Electric Power	Heater fails; boric acid may crystallize; small potential for plugging and loss of flow to storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Replace heater; unplug lines
	2. Heater fails	--	Boric acid may crystallize; small potential for plugging and loss of flow to storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Replace heater; unplug lines
	3. Tank leaks	--	Eventual loss of suction pressure to pumps	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	None
	4. Tank empties	--	No boric acid flow to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	None
6.2.3 Level Transmitter	1. Electric power supply fails	Electric Power	No local level indication	No level indication to I&C system	None
	2. Connection leaks	Process Signal	Incorrect signal to transmitter	No level indication to I&C system	None
	3. Transmitter fails	--	No local level indication	No level indication to I&C system	None

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.2.4 Temperature Transmitter	1. Electric power supply fails	Electric Power	No local temperature indication	None	None
	2. Connection leaks	Process Signal	Incorrect signal to transmitter	None	None
	3. Transmitter fails	--	No local temperature indication	None	None
6.2.5 Manual Isolation Valve (CA-4)	1. Valve fails closed	--	No boric acid to storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	None
6.2.6 Miscellaneous Piping	1. Electric power supply to trace heating fails	Electric Power	Boric acid may crystallize; small potential for plugging and loss of flow to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Restore trace heating; unplug lines
	2. Trace heating fails	--	Boric acid may crystallize; small potential for plugging and loss of flow to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	Restore trace heating; unplug lines
6.2.7 Manual Isolation Valve (CA-5)	1. Valve fails closed	--	No boric acid to concentrated boric storage tanks; alternate flow path available	None	Alternate flow path through CA-P2B available
6.2.8 LP Boric Acid Pump (CA-P2A)	1. Electric power supply fails	Electric Power	Pump stops; no boric acid to concentrated storage tanks; alternate flow path available	None	Alternate flow path through CA-P2B available
	2. Pump fails	--	No boric acid to concentrated boric acid storage tanks; alternate flow path available	None	Alternate flow path through CA-P2B available
6.2.9 Manual Isolation Valve (CA-7)	1. Valve fails closed	--	No boric acid to concentrated boric acid storage tanks; alternate flow path available	None	Alternate flow path through CA-P2B available
6.2.10 Check Valve (CA-15)	1. Fails to prevent backflow	--	Possible backflow to mix tank if pump is not running; alternate flow path available	None	Close isolation valve CA-7; alternate flow path through CA-P2B available

Table B.3.6. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.2.11	Manual Isolation Valves (1CA-16, 1CA-13, 1CS-18, etc.)	1. Valves fail closed	--	No boric acid to concentrated boric acid storage tanks	None if concentrated boric acid available from boron recovery or adequate concentrated boric acid storage tank inventory is available	None
6.2.12	Pressure Transmitter	1. Electric power supply fails	Electric Power	No local pressure indication	No pressure indication to I&C system	None
		2. Connection leaks	Process Signal	Incorrect signal to transmitter	No pressure indication to I&C system	None
		3. Transmitter fails	--	No local pressure indication	No pressure indication to I&C system	None
6.2.13	Check Valve (CA-85)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	None if concentrated boric acid available from concentrated boric acid transfer pumps	Close 1CA-16, 1CA-18
6.2.14	Manual Isolation Valve (CA-25)	1. Valve fails closed	--	No boric acid	No boric acid available to core flood tanks	None
6.2.15	HP Boric Acid Pump (CA-P5)	1. Electric power supply fails	Electric Power	Pump stops; no boric acid	No boric acid available to core flood tank	None
		2. Pump fails	--	No boric acid	No boric acid available to core flood tank	None
6.2.16	Manual Isolation Valves (1CA-26, 1CA-28)	1. Valves fail to open, fail closed	--	No boric acid	No boric acid available to core flood tank	None
6.2.17	Manual Control Valve (CS-62)	1. Valve fails closed	--	No boric acid to concentrated boric acid storage tanks	No boric acid available to makeup filters, BWST	Alternate flow path available
6.2.18	Concentrated Boric Acid Storage Tank (1WD-T22)	1. N_2 blanket system fails	N_2 Blanket	Possible boric acid backflow	None	Close control valve CS-62
		2. Electric power supply to trace heating fails	Electric Power	Boric acid crystallizes; potential plugging and loss of flow	No boric acid available to makeup filters, BWST	Alternate flow path available
		3. Trace heating fails	--	Boric acid crystallizes; potential plugging and loss of flow	No boric acid available to makeup filters, BWST	Alternate flow path available
		4. Inlet boric acid flow fails	Boric Acid From Mix Tank/RC Bleed Evaporator Concentrate Cooler	No boric acid	None unless concentrated boric acid storage tanks are empty	Alternate flow path available

Table B.3.6. (continued

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	5. Tank leaks	--	Possible flooding; eventual loss of suction pressure to pump	Eventual loss of boric acid available to makeup filters, BWST	Alternate flow path available
	6. Tank empties	--	No boric acid	No boric acid available to makeup filters, BWST	Alternate flow path available
	7. Tank vent, relief valves fail open	--	Cover gas release to vent header	None	None
	8. Drain, sample lines fail open	--	Decreased boric acid	Decreased boric acid available to makeup filters, BWST	Alternate flow path available
6.2.19 Level Transmitter	1. Electric power supply	Electric Power	No local level indication	No level indication to I&C system	None
	2. Connection leaks	Process Signal	Incorrect signal to transmitter	No level indication to I&C system	None
	3. Transmitter fails	--	No local level indication	No level indication to I&C system	None
6.2.20 Manual Isolation, Control Valves (CS-63, CS-64, CS-67)	1. Valves fail closed	--	No boric acid	No boric acid available to makeup filters, BWST	Alternate flow path available
6.2.21 Concentrated Boric Acid Transfer Pump (1WD-P22)	1. Electric power supply fails	Electric Power	Pump stops; no boric acid	No boric acid available to makeup filters, BWST	Alternate flow path available
	2. Pump fails	--	No boric acid	No boric acid available to makeup filters, BWST	Alternate flow path available
6.2.22 Manual Isolation Valve (CS-68)	1. Valve fails closed	--	No boric acid	No boric acid available to makeup filters, BWST	Alternate flow path available
6.2.23 Manual Isolation Valves (CS-72, CS-79)	1. Valves fail closed	--	No boric acid	No boric acid available to available to makeup filters, BWST	Alternate flow path available
6.2.24 Check Valve (CS-73)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	None if concentrated boric acid available from LP boric acid pump	Close CS-72
6.3 RC Bleed Holdup Tanks and Transfer Pumps:					
6.3.1 Manual Control Valve (CS-41)	1. RC Bleed flow fails	RC Bleed Flow	RC bleed holdup tank could empty; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Alternate bleed flow available
	2. Valve fails closed	--	RC bleed holdup tank could empty; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Bleed flow can be diverted to 2WD-T21A

Table B.3.6. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.3.2	RC Bleed Holdup Tank (1WD-T21A)	1. N_2 blanket system fails	N_2 Blanket	Tank cannot be purged; no impact since rest of subsystem operates only on demand	None if alternate flow path available	None
		2. Tank leaks	--	Possible flooding; eventual loss of suction pressure to pump; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Alternate bleed flow available
		3. Tank empties	--	No flow; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Alternate bleed flow available
		4. Tank vent, relief valves fail open	--	Cover gas release to vent header	None	None
6.3.3	Level Transmitter	1. Electric power supply fails	Electric Power	No local level indication	No level indication to I&C system	None
		2. Connection leak	Process Signal	Incorrect signal to transmitter	No level indication to I&C system	None
		3. Transmitter failure	--	No local level indication	No level indication to I&C system	None
6.3.4	Miscellaneous Piping	1. Electric power supply to trace heating fails	Electric Power	Boric acid may crystallize; small potential for plugging and loss of flow; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Restore trace heating; unplug lines; alternate bleed flow available
		2. Trace heating fails	--	Boric acid may crystallize; small potential for plugging and loss of flow; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Restore trace heating; unplug lines; alternate bleed flow available
6.3.5	Waste, Drain, Sample Lines	1. Lines fail open	--	Decreased flow; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Alternate bleed flow available
6.3.6	Manual Isolation Valves (CS-42, CS-148, CS-44)	1. Valves fail closed	--	No flow to pump; no impact since rest of subsystem operates only on demand	None if alternate flow path available	Alternate bleed flow available
6.3.7	RC Bleed Transfer Pump (1WD-P21A)	1. Electric power supply fails	Electric Power	Pump stops; no flow to boron recovery	None if alternate flow path available	Alternate bleed flow available
		2. Pump fails	--	No flow to boron recovery	None if alternate flow path available	Alternate bleed flow available
6.3.8	Check Valve (CS-45)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	None if alternate flow path available	Close control valve CS-46

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.3.9 Flow Orifice	1. Orifice plugs	--	No flow to boron recovery	None if alternate flow path available	Alternate bleed flow available
6.3.10 Flow Transmitter	1. Electric power supply fails	Electric Power	No local flow indication	No flow indication to I&C system	None
	2. Connection leak	Process Signal	Incorrect signal to transmitter	No flow indication to I&C system	None
	3. Transmitter failure	--	No local flow indication	No flow indication to I&C system	None
6.3.11 Manual Control Valve (CS-46)	1. Valve fails closed	--	No flow to boron recovery	None if alternate flow path available	Alternate bleed flow available
6.3.12 Manual Isolation Valves (CS-80, CS-172, CT-1)	1. Valves fail closed	--	No flow to boron recovery	None if alternate flow path available	Alternate bleed flow available
6.3.13 Manual Isolation Valve (CT-88)	1. Demineralized water supply fails	Demineralized Water	Demineralized water holdup tank could empty	No demineralized water to makeup filters	Alternate demineralized water flow path available
	2. Valve fails closed	--	Demineralized water holdup tank could empty	No demineralized water to makeup filters	Alternate demineralized water flow path available
6.3.14 RC Demineralized Water Holdup Tank (1WD-T21B)	1. N_2 blanket system fails	N_2 Blanket	Tank cannot be purged and is unavailable	No demineralized water to makeup filters	Alternate demineralized water flow path available
	2. Tank leaks	--	Possible flooding; eventual loss of suction pressure to pump	Eventual loss of demineralized water to makeup filters	Alternate demineralized water flow path available
	3. Tank empties	--	No demineralized water	No demineralized water to makeup filters	Alternate demineralized water flow path available
	4. Tank vent, relief valves fail open	--	Cover gas release to vent header	None	None
6.3.15 Level Transmitter	1. Electric power supply fails	Electric Power	No local level indication	No level indication to I&C system	None
	2. Connection leak	Process Signal	Incorrect signal to transmitter	No level indication to I&C system	None
	3. Transmitter failure	--	No local level indication	No level indication to I&C system	None
6.3.16 Waste, Drain, Sample Lines	1. Lines fail open	--	Decreased demineralized water	Decreased demineralized water to makeup filters	Alternate demineralized water flow path available

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.3.17 Miscellaneous Piping	1. Electric power supply to trace heating fails	Electric Power	Boric acid may crystallize; small potential for plugging and loss of flow	No demineralized water to makeup filters	Restore trace heating; unplug lines; alternate demineralized water flow path available
	2. Trace heating fails	--	Boric acid may crystallize; small potential for plugging and loss of flow	No demineralized water to makeup filters	Restore trace heating; unplug lines; alternate demineralized water flow path available
6.3.18 Manual Isolation Valves (CS-52, CS-149, CS-54)	1. Valves fail closed	--	No demineralized water to pump	No demineralized water to makeup filters	Alternate demineralized water flow path available
6.3.19 RC Bleed Transfer Pump (1WD-P21B)	1. Electric power supply fails	Electric Power	Pump stops; no demineralized water	No demineralized water to makeup filters	Alternate demineralized water flow path available
	2. Pump fails	--	No demineralized water	No demineralized water to makeup filters	Alternate demineralized water flow path available
6.3.20 Flow Orifice	1. Orifice plugs	--	Decreased demineralized water	Decreased demineralized water to makeup filters	Alternate demineralized water flow path available
6.3.21 Manual Control Valve (CS-56)	1. Valve fails closed	--	No demineralized water	No demineralized water to makeup filters	Alternate demineralized water flow path available
6.3.22 Flow Transmitter	1. Electric power supply fails	Electric Power	No local flow indication	No flow indication to I&C system	None
	2. Connection leak	Process Signal	Incorrect signal to transmitter	No flow indication to I&C system	None
	3. Transmitter failure	--	No local flow indication	No flow indication to I&C system	None
6.3.23 Check Valve (CS-55)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	No demineralized water to makeup filters	Close control valve CS-56

Table B.3.6. (continued)

Component		Potential Failure Mode		Immediate Effects		
		Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.3.24	Manual Isolation Valves (CS-83, CS-85, CS-100)	1. Valves fail closed	--	No demineralized water	No demineralized water to makeup filters	Alternate demineralized water flow available
6.3.25	Check Valve (CS-86)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	No demineralized water to makeup filters	Close CS-85
6.3.26	Control Valve (HP-15)	1. Control signal fails to open valve	Control Signal From Flow Orifice	Loss of flow to makeup filters	No demineralized water to makeup filters	None
		2. Control signal fails to close valve	Control Signal From Flow Orifice	Loss of flow control to makeup filters	Increase in demineralized water to makeup filters	Close manual isolation valves; close HP-136
		3. Instrument air supply fails	Instrument air	Loss of flow to makeup filters	No demineralized water to makeup filters	None
		4. Electric power supply fails	Electric Power	Loss of flow to makeup filters	No demineralized water to makeup filters	None
		5. Spurious signal to open valve	Control Signal From Flow Orifice	Loss of flow control to makeup filters	Increase in demineralized water to makeup filters	Close manual isolation valves; close HP-136
		6. Spurious signal to close valve	Control Signal From Flow Orifice	Loss of flow to makeup filters	No demineralized water to makeup filters	None
		7. Internal valve failure	--	Loss of flow to makeup filters	No demineralized water to makeup filters	None
6.3.27	Manual Isolation Valves (HP-191, HP-192)	1. Valves fail closed	--	No flow to flow orifice	No demineralized water to makeup filters	None
6.3.28	Manual Isolation Valves (HP-52, HP-53)	1. Valves fail closed	--	No flow to flow orifice; potential control signal failure	No demineralized water to makeup filters; alternate flow path available	Open HP-54
6.3.29	Manual Isolation Valve (HP-54)	1. Valve fails open	--	No flow to flow orifice; potential control signal failure	Loss of control of demineralized water to makeup filters	Close HP-136 if HP-15 should be closed
6.3.30	Flow Orifice	1. Orifice plugs	--	No flow; potential control signal failure	No demineralized water to makeup filters; alternate flow path available	Open HP-54
6.3.31	Flow Transmitter	1. Electric power supply fails	Electric Power	Incorrect signal to flow control valve (see 6.3.26)	No flow indication in I&C system	None
		2. Connection leaks	Process Signal	Incorrect signal to transmitter	No flow indication in I&C system	None

Table B.3.6. (continued)

Component	Potential Failure Mode		Immediate Effects		Remedial Action Within Subsystem
	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	
	3. Transmitter fails	--	Incorrect signal to flow control valve (see 6.3.26)	No flow indication in I&C system	None
6.3.32 Control Valve (HP-16)	1. Control signal fails to open valve	Control Signal From 3-Way Valve	Loss of flow to makeup filters	No demineralized water to makeup filters	None
	2. Control signal fails to close valve	Control Signal From 3-Way Valve	Loss of flow control to makeup filters	Increase in demineralized water to makeup filters	Close manual isolation valves; close HP-192
	3. Instrument air supply fails	Instrument Air	Loss of flow to makeup filters	No demineralized water to makeup filters	None
	4. Electric power supply fails	Electric Power	Loss of flow to makeup filters	No demineralized water to makeup filters	None
	5. Spurious signal to open valve	Control Signal From 3-Way Valve	Loss of flow control to makeup filters	Increase in demineralized water to makeup filters	Close manual isolation valves; close HP-192
	6. Spurious signal to close valve	Control Signal From 3-Way Valve	Loss of flow to makeup filters	No demineralized water to makeup filters	None
	7. Internal valve failure	--	Loss of flow to makeup filters	No demineralized water to makeup filters	None
6.4 Boron Recovery:					
6.4.1 Manual Isolation Valves (CT-3, CT-5)	1. RC bleed flow fails	RC Bleed Flow From Holdup Tank	No flow to feed tank. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	Alternate flow path available
	2. Valves fail closed	--	No flow to demineralizer; no effect since second demineralizer available	None if alternate flow path available	Alternate flow path available
6.4.2 RC Bleed Evaporator Demineralizer	1. Resin fill fails	Resin Fill	No demineralizing capacity; no effect since second demineralizer available	None if alternate flow path available	Alternate flow path available
	2. Tank leaks	--	Decreased flow; no effect since second demineralizer available	None if alternate flow path available	Alternate flow path available
	3. Tank vent fails open	--	Decreased flow; no effect since second demineralizer available	None if alternate flow path available	Alternate flow path available
6.4.3 Manual Isolation Valves (CT-4, CT-6)	1. Valves fail closed	--	No flow; no effect since second demineralizer available	None if alternate flow path available	Alternate flow path available
6.4.4 Manual Isolation Valve (CT-14)	1. Valve fails closed	--	No flow to feed tank. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	Establish recirculation flow from evaporator

Table B.3.6. (Continued

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.4.5	Miscellaneous Piping	1. Electric power supply fails	Electric Power	Boric acid may crystallize; small potential for plugging and loss of flow	None unless concentrated boric acid storage tanks are empty	Restore trace heating; unplug lines
		2. Trace heating fails	--	Boric acid may crystallize; small potential for plugging and loss of flow	None unless concentrated boric acid storage tanks are empty	Restore trace heating; unplug lines
6.4.6	Manual Isolation Valves (CT-16, CT-19, CA-88, CT-49, CT-36)	1. Evaporator demineralizer flow fails; CT-16 fails closed	Evaporator Demineralizer Flow	No flow to feed tank. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	Establish recirculation flow from evaporator
		2. Caustic flow fails; CA-88 fails closed	Caustic Flow	Chemical imbalance in boron recovery system	Chemical imbalance in boric acid to makeup filters, BWST	None
		3. Distillate flow fails; CT-49 fails closed	Distillate Cooler Flow	No flow to feed tank. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	Establish recirculation flow from evaporator
		4. Concentrate flow back to feed tank; CT-36 fails open	Concentrate Flow	Concentrated boric acid returned to feed tank; no boron recovery	None unless concentrated boric acid storage tanks are empty	Close CT-18 to force concentrate flow to concentrate cooler
		5. Valve CT-19 fails closed	--	No flow to feed tank. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	Establish recirculation flow from evaporator
6.4.7	Check Valves (CT-18, CT-37, CT-17)	1. Fail to prevent backflow	--	Possible backflow to concentrate pump, evaporator demineralizer	None unless concentrated boric acid storage tanks are empty	Close isolation valves CT-16 and CT-19
6.4.8	RC Bleed Evaporator Feed Tank (WD-T42)	1. Tank leaks	--	Decreased flow; eventual loss of suction pressure to pump. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	None
		2. Tank empties	--	No flow. Boron recovery stops until tank refilled	None unless concentrated boric acid storage tanks are empty	None
		3. Tank vent, relief valves fail open	--	Decreased flow. Tank has 8-hour capacity; boron recovery will continue until tank is empty	None if feed tank is full	None
6.4.9	Level Transmitter	1. Electric power supply fails	Electric Power	No local level indication	None	None
		2. Connection leak	Process Signal	Incorrect signal to transmitter	None	None
		3. Transmitter failure	--	No local level indication	None	None

Table B.3.6. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.4.10	Manual Isolation Valves (CT-22, CT-23)	1. Valves fail closed	--	No flow to evaporator feed pump. Recirculation flow path can be established through evaporator but boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow from evaporator
6.4.11	RC Bleed Evaporator Feed Pump (WD-P46)	1. Electric power supply fails	Electric Power	Pump stops; no flow to evaporator. Recirculation flow path can be established through evaporator but boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow from evaporator
		2. Pump fails	--	No flow to evaporator. Recirculation flow path can be established through evaporator but boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow from evaporoator
6.4.12	Pressure Transmitter Fails	1. Electric power supply fails	Electric Power	No local pressure indication	None	None
		2. Connection leak	Process Signal	Incorrect signal to transmitter	None	None
		3. Transmitter fails	--	No local pressure indication	None	None
6.4.13	Manual Isolation Valve (CT-24)	1. Valve fails closed	--	No flow to evaporator. Recirculation flow path can be established through evaporator but boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow from evaporator
6.4.14	Control Valve (CT-24)	1. Control signal fails to open/ valve close	Control Signal From Evaporator Level	Loss of flow control to evaporator. Could flood evaporator or allow dryout. Recirculation flow paths to feed tank or evaporator can be established. Boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow to feed tank or evaporator
		2. Instrument air supply fails	Instrument Air	Loss of flow control to evaporator. Could flood evaporator or allow dryout. Recirculation flow paths to feed tank or evaporator can be established. Boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow to feed tank or evaporator

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	3. Spurious signal to open/valve close	Control Signal From Evaporator Level	Loss of flow control to evaporator. Could flood evaporator or allow dryout. Recirculation flow paths to feed tank or evaporator can be established. Boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow to feed tank or evaporator
	4. Internal valve failure	--	Loss of flow control to evaporator. Could flood evaporator or allow dryout. Recirculation flow paths to feed tank or evaporator can be established. Boron recovery stops	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow to feed tank or evaporator
6.4.15 Check Valve (CT-29)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	None unless concentrated boric acid storage tanks are empty	Close control valve CT-28
6.4.16 Waste, Drain, Sample Lines	1. Lines fail open	--	Decreased flow to evaporator. Recirculation flow path can be established through evaporator but boron recovery stops	None unless concentration boric acid storage tanks are empty	Establish recirculation flow to evaporator if required
6.4.17 RC Bleed Evaporator (WD-EV1)	1. N_2 blanket system fails	N_2 Blanket	Possible explosive mixture forms	None	None
	2. Steam supply fails	Steam	Evaporator floods. No boron recovery	None unless concentrated boric acid storage tanks are empty	Establish recirculation path to feed tank
	3. Blocked tubes	--	Decreased heat transfer; decrease in boron recovery	None unless concentrated boric acid storage tanks are empty	Establish recirculation path to feed tank
	4. Tube rupture	--	Steam released to evaporator vapor space; decrease in boron recovery	None unless concentrated boric acid storage tanks are empty	Establish recirculation path to feed tank
	5. Loss of heat transfer capability	--	Evaporator floods. No boron recovery	None unless concentrated boric acid storage tanks are empty	Establish recirculation path to feed tank
	6. Electric power supply fails	Electric Power	Concentrate heater fails; potential plugging and loss of flow	None unless concentrated boric acid storage tanks are empty	Restore heater; unplug lines

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	7. Inlet flow from feed pump fails	--	No boron recovery	None unless concentrated boric acid storage tanks are empty	Establish recirculation flow path until feed flow restored
	8. Evaporator leaks	--	Eventual loss of suction pressure to pump	None unless concentrated boric acid storage tanks are empty	None
	9. Evaporator empties	--	Possible damage to evaporator; no boron recovery	None unless concentrated boric acid storage tanks are empty	Shut off steam flow
	10. Evaporator vent, relief valves fail open	--	Cover gas release to vent header	None	None
6.4.18 Evaporator Level Transmitter	1. Electric power supply fails	Electric Power	Incorrect signal to evaporator feed pump discharge flow control valve (see 6.4.14)	None unless concentrated boric acid storage tanks are empty	None
	2. Connection leaks	Process Signal	Incorrect signal to evaporator feed pump discharge flow control valve (see 6.4.14)	None unless concentrated boric acid storage tanks are empty	None
	3. Transmitter fails	--	Incorrect signal to evaporator feed pump discharge flow control valve (see 6.4.14)	None unless concentrated boric acid storage tanks are empty	None
6.4.19 Temperature Transmitter	1. Electric power supply fails	Electric Power	Incorrect signal to transmitter and concentrate cooler discharge flow control (see 6.4.26)	See 6.4.26	None
	2. Connection leaks	Process Signal	Incorrect signal to transmitter and concentrate cooler discharge flow control (see 6.4.26)	See 6.4.26	None
	3. Transmitter failure	--	Incorrect signal to transmitter and concentrate cooler discharge flow control (see 6.4.26); no local temperature indication	See 6.4.26	None
6.4.20 Distillate Cooler (WD-C9)	1. Cooling water supply fails	Cooling Water	High temperature distillate returned to feed tank	None	Establish recirculation path to feed tank
	2. Blocked tube	--	Decreased heat transfer; high temperature distillate returned to feed tank	None	Establish recirculation path to feed tank

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	3. Tube rupture	--	Cooling water released to distillate; dilutes feed tank concentration	None	Establish recirculation path to feed tank
	4. Loss of heat transfer capability	--	Decreased heat transfer; high temperature distillate returned to feed tank	None	Establish recirculation path to feed tank
	5. Cooler leaks	--	Decreased distillate flow	Decreased distillate available to condensate test tanks (demineralized water)	Establish recirculation path to feed tank
	6. Inlet flow fails	Evaporator Distillate	No distillate flow	No distillate available to condensate test tanks (demineralized water)	None
6.4.21 Concentrate (Recirc.) Pump	1. Electric power supply fails	Electric Power	Pump stops; no concentrate flow	None unless concentrated boric acid storage tanks are empty	None
(WD-P4)	2. Pump fails	--	No concentrate flow	None unless concentrated boric acid storage tanks are empty	None
6.4.22 Check Valve (CT-35)	1. Fails to prevent backflow	--	Possible backflow if pump is not running	None unless concentrated boric acid storage tanks are empty	Close CT-38, CT-40
6.4.23 Pressure Transmitter	1. Electric power supply fails	Electric Power	No local pressure indication	None	None
	2. Connection leaks	Process Signal	Incorrect signal to transmitter	None	None
	3. Transmitter fails	--	No local pressure indication	None	None
6.4.24 Manual Isolation Valve (CT-38)	1. Valve fails open	--	Concentrate flow recirculated to evaporator. No boron recovery; possible evaporator flooding	None unless concentrated boric acid storage tanks are empty	Open CT-40 to divert flow through concentrate cooler
	2. Valve fails closed	--	Possible flooding of concentrate cooler; loss of temperature control in evaporator	None	Flow can be diverted through CT-36 back to feed tank
6.4.25 Concentrate Cooler (WD-7)	1. Cooling water supply fails	Cooling Water	High temperature boric acid returned to concentrated boric acid storage tanks	None	Close control valve CT-40
	2. Blocked tube	--	Decreased heat transfer; high temperature boric acid returned to concentrated boric acid storage tanks	None	Close control valve CT-40

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	3. Tube rupture	--	Cooling water released to concentrate; dilutes boric acid concentration	None	Concentration can be adjusted from boric acid mix tank
	4. Loss of heat transfer capability	--	High temperature boric acid returned to concentrated boric acid storage tanks	None	Close control valve CT-40
	5. Cooler leaks	--	Decreased concentrate flow	None unless concentrated boric acid storage tanks are empty	None
	6. Inlet flow fails	Evaporator Concentrate	No concentrate flow	None unless concentrated boric acid storage tanks are empty	Close control valve CT-40
	7. Cooling water control valve fails	Control Signal From Concentrate Cooler Discharge Temperature	No concentrate flow	None unless concentrated boric acid storage tanks are empty	Close control valve CT-40
6.4.26 Temperature Transmitter	1. Electric power supply fails	Electric Power	No signal to cooling water control valve	No signal to cooling water control valve; see 6.4.24	See 6.4.24
	2. Connection leaks	Process Signal	No signal to transmitter	No signal to cooling water control valve; see 6.4.24	See 6.4.24
	3. Transmitter fails	--	No signal to cooling water control valve	No signal to cooling water control valve; see 6.4.24	See 6.4.24
6.4.27 Control Valve (CT-40)	1. Instrument air supply fails	Instrument Air	Loss of concentrate flow control	None unless concentrated boric acid storage tanks are empty	Close cooling water control valve; divert concentrate flow back to evaporator through CT-38 or to feed tank through CT-36
	2. Control signal fails to open/close valve	Control Signal From Evaporator Temperature Transmitter	Loss of concentrate flow control	None unless concentrated boric acid storage tanks are empty	Close cooling water control valve; divert concentrate flow back to evaporator through CT-38 or to feed tank through CT-36

Table B.3.6. (continued)

	Potential Failure Mode		Immediate Effects		
Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
	3. Spurious signal to open/close valve	Control Signal From Evaporator Temperature Transmitter	Loss of concentrate flow control	None unless concentrated boric acid storage tanks are empty	Close cooling water control valve; divert concentrate flow back to evaporator through CT-38 or tc feed tank through CT-35
	4. Internal valve failure	--	Loss of concentrate flow controi	None unless boric acid storage tanks are empty	Close cooling water control valve; divert concentrate flow back to evaporator through CT-38 or to feed tank through CT-36
6.5 Deborating Demineralizer:					
6.5.1 Manual Control Valve	1. RC Bleed flow fails	RC Bleed Flow	No flow to deborating demineralizer	No flow to makeup filters	None
	2. Valve fails closed	--	No flow to deborating demineralizer	None if alternate flow path available	Alternate flow path available
6.5.2 Manual Isolation Valve	1. Valve fails closed	--	No flow to deborating demineralizer	None if alternate flow path available	Alternate flow path available
6.5.3 Deborating Demineralizer	1. Tank leaks	--	Decreased bleed flow	None if alternate flow path available	Alternate flow path available
	2. Tank empties	--	No bleed flow	None if alternate flow path available	Alternate flow path available
	3. Tank vent, relief valves fail open	--	Decreased bleed flow	None if alternate flow path available	Alternate flow path available
	4. Resin saturates	--	No boron removal from bleed flow	None if alternate flow path available	Alternate flow path available
	5. Caustic flow fails	Caustic	No demineralizer regeneration	None if alternate flow path available	Alternate flow path available
6.5.4 Miscellaneous Piping	1. Electric power supply to trace heating fails	Electric Power	Boric acid may crystallize; small potential for plugging and loss of flow	None if alternate flow path available	Restore trace heating; unplug lines
	2. Trace heating fails	--	Boric acid may crystallize; small potential for plugging and loss of flow	None if alternate flow path available	Restore trace heating; unplug lines
6.5.5 Waste, Drain, Sample Lines	1. Lines fail open	--	Decreased bleed flow	None if alternate flow path available	Alternate flow path available
6.5.6 Manual Isolation Valves	1. Valves fail closed	--	No bleed flow	None if alternate flow path available	Alternate flow path available

Table B.3.6. (continued)

		Potential Failure Mode		Immediate Effects		
	Component	Mode	Interface Involved	Within Subsystem	At Subsystem Interface	Remedial Action Within Subsystem
6.5.7	Check Valve (Outlet)	1. Fails to prevent backflow	--	Possible backflow to deborating demineralizer	None if alternate flow path available	Close manual isolation valve
6.5.8	Check Valve (CS-123)	1. Fails to prevent backflow	--	Possible backflow to deborating demineralizer	No flow to makeup filters	Close HP.16

B.4. FMEA OF THE PRESSURIZER AND ASSOCIATED CONTROL SYSTEM

Table

Table B.4.1. Failures of the pressurizer pressure boundary

	Failure	Possible Causes	Effects	Remedial Action
1.	Pressurizer or Pressurizer Surge Line Failure	Material defects, thermal stress	Small to large hot leg LOCA	Emergency Procedures for LOCA's must be followed.
2.	Thermowell Failure	Material failure	RCS Leak. Indicated water temp. may be high. Ind. level may be high (small effect)	Emergency Procedures for RCS leaks must be followed. Other temp. element may be selected for indication based on a comparison to the saturation temperature at the indicated pressure.
3.	Heater Mounting Failure	Material defect, uncovered heater energized and subsequently shocked	Small to large hot leg LOCA	Emergency Procedures for LOCA's must be followed.
4.	Level Sensing Line Failure (Steam Space)	Material defects	RCS Leak. Affected instrument response high or unknown. Pressurizer may be filled.	Emergency Procedures for RCS leaks must be followed. One of the two operable level measurements may be selected for indication based on a comparison of the three indications.

Table B.4.1. (continued)

Failure	Possible Causes	Effects	Remedial Action
5. Level Sensing Line Failure (Water Space)	Material defects	RCS Leak. Affected inst. response low or unknown	Emergency Procedures for RCS leaks must be followed. One or the two operable level measurements may be selected for indication based on a comparison of the three indications.
6. Spray Line Failure	Material defects, thermal stress	Small LOCA. Pressurizer filled during RCS depressurization.	Emergency Procedures for small LOCA's must be followed.
7. High Pressure Safety or Relief Valve Line Failure, Safety Valve Failure	Material defect, mechanical stress	Small LOCA. Pressurizer filled during RCS depressurization.	Emergency Procedures for small LOCA's must be followed.
8. PORV Fails Open	Spurious signal maintains valve open, PORV failure to close after opening (See Failure of Inputs to Pressurizer System)	Small LOCA. Pressurizer filled during RCS depressurization.	Emergency Procedures for Small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block Valve, RC-V4.

Table B.4.2. Failure of pressurizer system equipment or outputs

Failure	Possible Causes	Effects	Remedial Action
1. Failure of Selected Level Transmitter Low	Transmitter failure	Low pressurizer level signal. Makeup valve opens. Pressurizer fills resulting in a probable high pressure trip. Letdown storage tank empties. Heater banks 2, 3 and 4 fail off due to indicated low level.	Operator can compare the three level measurements through the computer and select one or tne two operable transmitters for indication and/or control. Manual control of makeup valve possible. Operator must transfer makeup pump suction to BWST prior to draining makeup tank.
	A.C. Power failure		See Table 6, Failure of Pressurizer Inputs
2. Failure of Selected Level Transmitter High	Transmitter failure	Maximum pressurizer level signal. Makeup valve closes resulting in slow decrease in pressurizer level. RC pump seal injection continues.	Operator can compare the three level measurements through the computer and select one of the two operable transmitters for indication and/or control. Manual control of makeup valve possible.

Table B.4.2. (continued)

	Failure	Possible Causes	Effects	Remedial Action
3.	Failure of Selected Temperature Element High or Low	Element opens or shorts	Indicated higher or lower level. Makeup control valve modulates to achieve higher or lower setpoint level.	Operator can compare the two indicated temperatures through the computer to the saturation temperature at the indicated RCS pressure and select the operable transmitter.
4.	Failure of Relief/Safety Valve Discharge Line Thermocouple	T/C opens	Low indicated temperature. This failure would be confusing to the operator if the associated relief valve developed a leak.	Failure may be detected by a comparison of the three T/C readings and confirmed by test.
5.	Failure of Non-Selected Level Transmitter or Temperature Element High or Low	Transmitter or Element failure	No immediate effects unless operator switches to failed output (see Failure of Selected Transmitter).	Computer indication/ alarm available to operator for identification of failed transmitter.
6.	Failure of Spray Valve Closed	Failure of valve or solenoid	Loss of power operation pressure reduction control. May result in reactor trip.	Shutdown required for repair. Operator control of PORV required for depressurization to cold shutdown.
7.	Failure of Spray Valve Open	Failure of valve	Slow depressurization of RCS. Energizing of pressurizer heaters.	Shutdown required for repair. Operator may control depressurization by closing Spray Block Valve.

Table B.4.2. (continued)

Failure	Possible Causes	Effects	Remedial Action
8. Failure of PORV Closed (For Failure of PORV Open, See Table 4, Failure of Pressurizer Pressure Boundary)	Failure of valve or solenoid	PORV unavailable for high pressure transients. Increased safety valve actuations. No low pressure relief available during shutdown.	Shutdown required for repair. May be difficult to detect.
9. Failure of PORV or Spray Block Valves Open (For Failure of Valves Closed, See Table 6, Failures of Pressurizer Inputs)	Valve failures	Valves unavailable for isolating PORV or spray valve if either failed open.	May be difficult to detect. An unisolated, open PORV transient is controlled by Emergency Procedures for a small LOCA. An unisolated, open spray valve requires careful control of RCS temperature to reach cold shutdown.
10. Pressurizer Heater Element Fails	Corrosion, short circuit	Small reduction in heater capacity. May not be noticed.	Heater failure may be identified by a circuit breaker opening. Replacement during refueling shutdown required.

Table B.4.3. Failures of inputs to the pressurizer system

Failure	Possible Causes	Effects	Remedial Action
1. Power to Selected Level Transmitter fails (LT1 or LT2)	Breaker opens deenergizing KI Emergency #1 or Emergency #2 Feeders	Low pressurizer level signal. Makeup valve opens. Pressurizer fills resulting in probable high pressure trip. Makeup storage tank empties. Heater banks 2, 3 and 4 deenergized. Total effects of loss of KI "Emergency #1" or "Emergency #2" feeders unevaluated.	Other transmitters may be selected, Manual control or Makeup Valve required prior to selection of operable transmitter. See Failure or Pressurizer Equipment, Item 1, Failure of Selected Transmitter Low.
	Bus KI fails	Loss of Power to ICS. Heaters, PORV, Spray Valve are off or closed. Main Feedwater tripped. Makeup Control valve transfers to "hand control." Slow decrease in pressurizer level and pressure occurs prior to operator intervention.	Emergency Procedure for Loss of ICS Power must be followed. Manual control of PORV, spray valve, heaters and makeup valve available due to automatic transfer of selected loads to Bus KU. Emergency feedwater automatically actuated.
2. Power to Selected Level Transmitter LT3	Breaker Opens deenergizing KU feeder for transmitter (details unavailable).	Low pressurizer level signal. Makeup valve opens. Pressurizer fills resulting in probable high pressure trip. Makeup storage tank empties. Heater banks 2, 3 and 4 deenergized. Effects of loss of KU transmitter power supply unevaluated.	Other transmitters may be selected. See Failure or Pressurizer Equipment, Item 1, Failure or Selected Transmitter Low.
	Bus KU fails	Low pressurizer level signal. Makeup valve opens. Pressurizer fills resulting in probable high pressure trip. Makeup storage tank empties. Heater banks 2, 3 and 4 deenergized. Loss of plant computer. Effects of loss of KU not fully evaluated.	Other Transmitters may be selected. Operator can compare transmitter outputs by alternately selecting the three transmitter outputs for for indication and control.

Table B.4.3. (continued)

	Failure	Possible Causes	Effects	Remedial Action
3.	Power to Selected Temperature Element Fails	Fuse opens deenergizing temperature element	Low pressurizer water temperature signal. Makeup valve will open to maintain higher setpoint. Temperature corresponding to 0 MV signal from bridge circuit unknown.	Other temperature element may be selected based on comparison of the temperature signals through the computer to the saturation temperature at the indicated pressure.
		Bus KI fails	Loss of power to ICS. Heaters, PORV, spray valve are off or closed. Main feedwater tripped. Makeup control valve transfers to "hand control." Slow decrease in pressurizer level and pressure occurs prior to operator intervention.	Emergency Procedure for Loss of ICS Power must be followed. Manual Control of PORV, spray valve, heaters, and makeup valve available due to automatic transfer of selected loads to Bus KU. Emergency feedwater automatically actuated.
4.	Pressurizer Heater Power Fails Off			
	a) Single Heater Bank	Power feeder failure (Breaker opens), pressure switch failure	Less than 500 kW of 1500 kW capacity deenergized. Power operation may continue.	Repair during power operation possible.
	b) Single 600 VAC Bus Failure (XH, XI, XJ, XK, X5, X6, X7)	Breaker opens, bus failure	Approximately 500 kW of 1500 kW capacity deenergized. Power operation may continue.	Repair during power operation possible.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
c) Single 4160 VAC Bus Failure (TC, TD, TE)	Bus failure	Approximately 500 kW of 1500 kW capacity deenergized. Power operation may continue.	Repair during power operation possible.
d) Spurious Level Interlock	Selected level transmitter fails low, Misc. modules fail low	Heater Groups 3 and 4 off, Heater Group 1 operable, Heater Group 2 controllable from ASP. Pressurizer Lo-Lo level alarmed. See Failure of Pressurizer Outputs, Item 1, Failure of Selected Level Transmitter.	See Failure of Pressurizer Outputs, Item 1, Failure of Selected Level Transmitter Low.
e) Spurious High Failure of Pressure Signal	Selected narrow range pressure transmitter circuit fails high.	PORV and spray valve open creating small LOCA. Heaters deenergized. See Failure of Pressurizer Pressure Boundary, Item 8, PORV Fails Open.	The operator can compare the indicated pressure signal to the RPS narrow range pressure signals to identify the failure. PORV and spray valve may be manually controlled. Transfer to an RPS pressure signal for control or repair following the reactor trip is required.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
5. Heater Power Fails On			
a) Single Heater Bank	Pressure switch, controller fail on	Probable high pressure reactor trip. PORV and spray valve actuation.	Specific control room indication of energized heater unknown. Heater group(s) may be manually deenergized.
b) Multiple Heater Banks	Selected narrow range pressure transmitter circuit fails low.	PORV and spray valve close. Heaters energized. High pressure reactor trip. Operation of Code Safety valves possible.	The operator can compare the indicated pressure signals to the RPS narrow range pressure signals to identify the failure. Heater groups, PORV and spray valves may be manually controlled. Transfer to an RPS pressure signal for control or repair following reactor trip required.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
6. Power to Spray Valve Solenoid fails off	Pressure switch failure, controller failure	Spray Valve closes. Loss of power operation pressure reduction control, may result in reactor trip.	PORV operable if required, Manual control of spray valve may be possible. Repair following reactor shutdown or trip required.
	Selected narrow range pressure transmitter circuit fails low.	Spray valve and PORV close. Heaters energized. High pressure reactor trip.	The operator can compare the indicated pressure signals to the RPS narrow range pressure signals to identify the failure. Heater groups, PORV and spray valves may be manually controlled. Transfer to an RPS pressure signal for control or repair following reactor trip required.
	Failure of Bus KI	Loss of Power to ICS. Spray valve, PORV, heaters, are off or closed, main feedwater tripped, Makeup valve transfers to "hand control." Slow decrease in pressurizer level and pressure occurs prior to operator intervention.	Emergency procedure for Loss of ICS Power must be followed. Manual control of PORV, spray valve, heaters and Makeup valve available due to automatic transfer of selected loads to Bus KU. Emergency feedwater automatically actuated.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
7. Power to Spray Valve Solenoid fails on	Pressure switch, controller fails on	Spray valve opens. Slow depressurization of RCS. Energizing of pressurizer heaters.	Spray valve may be manually closed or isolated. See Failure of Pressurizer Equipment, Item 7, Failure of Spray Valve Open.
	Selected narrow range pressure transmitter circuit fails high.	PORV and spray valves open creating small LOCA. Heaters deenergized. See Failure of Pressurizer Pressure Boundary, Item 8, PORV Fails Open.	The operator can compare the indicated pressure signals to the RPS narrow range pressure signals to identify the failure. PORV and spray valve may be manually controlled. Transfer to an RPS pressure signal for control or repair following the reactor trip is required.
8. Power to Spray Block Valve fails on	Controller failure	Valve closes isolating spray and spray bypass flow. Loss of power operation pressure reduction control. Spray nozzle may be thermally stressed.	PORV may be manually controlled to avoid reactor trip or will be automatically controlled to limit RCS pressure following reactor trip. Control room indication of block valve closure unknown.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
9. Power to Spray Block Valve fails off	Controller or bus failure	No immediate effects. If the spray valve fails open, it cannot be isolated.	If identified, repair of bus or controller during power operation may be possible. See Failures of Pressurizer Equipment, Item 9, Failure of PORV or Spray Block Valves.
10. Power to PORV Block Valve fails off	Controller or bus failure (600 VAC XP)	No immediate effects. If PORV fails open, it cannot be isolated.	If identified, repair of bus or controller during power operation may be possible. See Failures of Pressurizer Equipment, Item 9, Failure of PORV or Spray Block Valves.
11. Power to PORV Block Valve fails on	Controller failure	Block valve closes. Possible safety valve actuation on high pressure transients.	Indication of block valve closure unknown. If identified, repair during power operation may be possible.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
12. Power to PORV Solenoid fails off	Pressure switch failure, controller failure, failure of Bus DIB	PORV closes. Possible safety valve actuation on high pressure transients	If identified, repair during power operation may be possible.
	Selected narrow range pressure transmitter circuit fails low.	Spray valve and PORV close, heaters energized. High pressure reactor trip.	The operator can compare tne indicated pressure signals to the RPS narrow range pressure signals to identify tne failure. Heater groups, PORV and spray valves may be manually controlled. Transfer to an RPS pressure signal for control or repair following reactor trip required.
	Failure of Bus K1	Loss of power to ICS. Spray Valve, PORV, heaters are off or closed. Main feedwater tripped. Makeup valve transfers to "hand control." Slow decrease in pressurizer level and pressure occurs prior to operator intervention.	Emergency procedure for Loss of ICS Power must be followed. Manual control of PORV, spray valve, heaters and Makeup valve available due to automatic transfer of selected loads to Bus K[illegible]. Emergency feedwater automatically actuated.

Table B.4.3. (continued)

Failure	Possible Causes	Effects	Remedial Action
13. Power to PORV Solenoid fails on	Pressure switch or controller failure	PORV opens creating small LOCA. Pressurizer fills.	See Failure or Pressurizer Pressure Boundary, Item 8, PORV Fails Open.
	Selected narrow range pressure transmitter circuit fails high.	PORV and spray valve open creating small LOCA. Pressurizer fills. Heaters deenergized. See Failure of Pressurizer Pressure Boundary, Item 8, PORV Fails Open.	The operator can compare the indicated pressure signals to the RPS narrow range pressure signals to identify the failure. PORV and Spray Valve may be manually controlled. Transfer to an RPS pressure signal for control or repair following the reactor trip is required.

B.5 CONTROL SYSTEM FAILURES THAT CONTRIBUTE TO STEAM GENERATOR OVERFILL

The Oconee 1 MFW control system has an overriding requirement to feed the SG as long as the differential pressure ("water level") is sensed below low level, [25 in. on the selected A-D (A'-D') sensor - see Fig. A.3]. Between 25 in. and 344 in., control is not based on level during normal operations. A complex of demand-related signals is met by the control system, and, within the specified operating range, most simple aberrations that might occur in a component are compensated by action of the ICS. When the sensed level exceeds 344 in., the ICS sends a signal to close the MFW control valve. If despite this the differential pressure level rises to 359 in., a signal is sent by circuitry outside the ICS (see Fig. A.4) to trip the MFW pumps. Note that this signal will cause actuation of the trip only if signals are sent from both the B-D and the B'-D' sensor sets. (See A.2.2.2 and A.2.2.3).

It is apparent, therefore, that the MFW cannot overfill a SG (above the 359-in. level) unless both high level protection features are defeated and an overfeed mechanism is initiated that is not controlled by cross limits or by any of the other compensatory features of the ICS. We have accordingly classified possible failures as they may cause one or another of these malfunctions (B.5.1).

Note that a number of SG overfeeds would reduce steam quality to the point where water enters the steam line even though the differential pressure on A-D did not cause either high level control or high level pump trip. However, significant accumulation requires defeat of both high level protection devices.

The AFW system is not subject to the high level protection features. Therefore, once the system is on AFW, less control system failure is required to bring on SG overfill. Two things should be borne in mind: (1) there must have been a prior failure or unusual circumstance to bring on the AFW, and (2) the AFW pumps water much more slowly than the MFW with a full open or nearly full open control valve. Hence, in the AFW case, there is more time for intervention and less potentially damaging momentum carried by the water.

B.5.1 Classification of Failures Leading to SG Overfill

Type A: Failures that place both the high level MFW pump trip and the high level control valve closure in a failed state. Since both of these systems depend on the same level detection equipment, a failure there would affect both equivalently. The following Type A failures are possible:

a. A sufficient leak in selected pressure tap B (B') or the connecting pipe from it, or in the packing of either blocking valve on which the connecting pipe terminates (A.2.2.2.2).

b. Failure of valve V (Fig. A.3) of the selected set in the closed position during operation (A.2.2.2.3).

c. Any failure of the selected B-D (B'-D') MFW ΔP cell--mechanical, hydraulic, or electrical--which causes the cell to read a low level when the level is actually high (A.2.2.2.4).

Further description of Type A failures appears in App. A.2.2.2. As observed there, since these are failures of level indications of the selected set, the indications brought to the control room display are inconsistent with other level indications displayed there. The failure should be detected when the operator notices and understands the inconsistency.

Type B: Failures that place the high level MFW pump trip in an undetected failed state. As noted before, the MFW pump trip circuitry is independent of the ICS, which controls the high level control valve closure. Further, the pump trip requires a confirming signal from the nonselected B-D (B'-D') set.

a. Any failure causing relay 2A or 3A (Fig. A.4) to fail with contacts open places SG A pump trip in an undetected failed state. Analogously, 2B and 3B for SG B (A.2.2.3.1).

b. Any failure causing relay FPTX (Fig. A.4) to fail with contacts open will put trip signals of both SGs in undetected failed state (A.2.2.3.2).

c. A sufficient leak in nonselected pressure tap B (B') or its connecting sense line, or in the packing of either blocking valve on which the connecting line terminates (A.2.2.2.2).

d. Failure of valve V (Fig. A.2.3) of the nonselected set in the closed position during operation (A.2.2.2.3).

e. Any failure of the nonselected B-D (B'-D') MFW ΔP cell--mechanical, hydraulic, or electrical--that causes the cell to read a low level when the level is actually high (A.2.2.2.4).

Failures a and b are undetected by their nature. Failures c, d, and e are undetected because they are failures of the nonselected set, which is not displayed in the control room.

Type C: Failures that block the high level MFW control valve closure and also initiate SG overfeed.

a. Selected low level signal fails low (B.5.2.r and A.2.2.2.1).

b. Hard limiter on turbine header pressure error signal fails, or the summer immediately downstream of the limiter produces a false signal. Either may have the effect of calling for increased flow.

c. Failure high of the low level set point (B.5.2.w).

Type D: Failures that may initiate fast overfeed by MFW. Simulations indicate that these failures are adequately controlled by the ICS.

a. ΔP measurement on FW control valve fails at 0 (B.5.2.a).

b. FW temperature measurement in one loop fails high (B.5.2.c).

c. MFW flow signal fails, showing no flow (B.5.2.d).

d. Hot-leg temperature measurement fails high (B.5.2.g).

e. ΔT_c signal fails either way (B.5.2.i).

f. T_{avg} determination fails high (B.5.2.j).

h. Neutron flux measurement fails high (B.5.2.k).

i. MFW blocking valve position indicator fails in closed position (B.5.2.m).

i. RC flow measurement fails low (B.5.2.u).

j. Main steam line safety, atmospheric, or turbine bypass valve fails open (B.5.2.v).

k. MFW control valve fails open, or valve control signal fails demanding valve opening (B.5.2.o).

Type E: Failures that would cause MFW overfeed at a relatively low rate. Simulations indicate that the ICS adequately deals with these failures.

a. ΔP signal across MFW control fails between zero and set point (B.5.2.b).

b. MFW flow measurement fails at low value greater than zero (B.5.2.e).

c. Reactor inlet temperature measurement in one loop fails low (B.5.2.h).

d. Startup FW control valve position indicator fails with valve less than 50% open (B.5.2.l).

e. MFW pump speed governor fails (B.5.2.n).

f. MFW startup valve fails open (B.5.2.p).

g. MW(e) demand fails high (B.5.2.s).

Type F: Single failure causing relatively slow overfill of SG.

a. A sufficient leak in selected pressure tap A (A') (see Fig. A.3) or the connecting pipe from that tap or in the packing of the blocking valves on which the connecting pipe terminates. (B.5.2.r and A.2.2.2.1).

The foregoing classification is useful in the further analysis of the consequences of the failures, either singly or in combination.

Type C failures, taken alone, should cause rapid filling of the SG to the 359-in. level followed by MFW pump, reactor, and turbine trip and initiation of AFW.

Type D and E failures, taken alone, may be controlled by the ICS. In some cases they will lead to system trips. Type D failures are expected to lead to greater and more rapid SG overfeeds than Type E failures.

Type A and B failures do not cause SG overfeed but block some or all of the high level protection. Type A failures, which bring inconsistent information to the control room display, are expected to be detected sooner than Type B failures, which do not.

The one Type F failure is a single failure that causes rapid filling of the SG to the 359-in. point and relatively slow continued overfilling thereafter.

Any Type A failure or any Type B failure followed by any Type C failure (coming before the detection and correction of the Type A or B failure) will cause rapid overfill of the SG with the MFW pumps operating at high speed.

No operator intervention (ameliorative or otherwise) has been assumed in the above discussion.

B.5.2 Detailed Descriptions of Failure Sequences

The component parts of the FW system, its controls and control signals, constitute a functional group in which failures could initiate a SG overfeed. This functional group was examined to find failures that can lead to overfill of the SG at Oconee, and it was found that all except one of the overfeed sequences identified would be terminated by successful action of the high level trip of the FW pumps. The exception is sequence r below, in which overfeed comes also from the AFW pump which does not have a high level trip.

The following event sets have been identified as having the potential to cause SG overfeed. In each case the initiating event appears to lead to an increase in the SG water level. The sequence of events suggested in each scenario beyond the initiating events is not intended to be taken as predictive; event sequences can depend upon many things, and surprising results often ensue. These scenarios are constructed and presented as guides for modelers and simulators to highlight features that may have special significance. Those indicated were analyzed on a system simulator in the next phase of this study: the augmented failure modes and effects analysis.

A most helpful source, which suggested a number of these sequences, was the Midland FMEA on the ICS.[1]

a. The ΔP signal across the FW control valves in loop A fails at its lowest value. The FW pumps go to high speed stop in an attempt to control the failed ΔP signal back to its set point. Excessive FW flow results from the increased pump speed. Throttle pressure will increase, T_{avg} will begin to fall, and the FW flow error will cause the FW valves to begin to close. Megawatts generated will begin to increase as the throttle valves move to control pressure back to its set point. The controls rods will pull, increasing reactor power, to bring T_{avg} back up to its set point.

However, as long as the tracking mode is not activated, the FW control valves should control the FW flow back to the original set point. Hence, the plant should return to its original condition, except that the high pump speed would result in a higher pressure drop across the FW control valves. Also, with the higher control valve pressure drop, the flow control would be more sensitive and would not be as smooth as normal. The FW valve flow control should be rapid enough to prevent a high level in the SGs. However, the high level pump trip protection is available if the FW control valves fails to act rapidly enough.

b. The ΔP signal across the FW control valve fails at some point below the set point. Qualitatively, the effects are the same as in (a). However, (a) appears to be the bounding case; the effects in this case should be less severe. A failure of the ΔP signal above the set-point value should not lead to SG overfeed.

c. The FW temperature measurement in loop A fails high at 500°F. FW temperature compensation will cause the total FW flow demand to increase, resulting in overfeeding both SGs and overcooling the core. T_{avg} will begin to drop, causing control rods to pull and reactor power to increase. Steam pressure will increase, causing the turbine valves to open and megawatt electric generation to increase. Because of negative megawatt electric error, the megawatt electric calibrating integral will cause the feed forward control demands to the reactor and FW to decrease. If the megawatt electric calibrating integral does not reach a low limit, the unit will settle out at its original condition. If the megawatt electric calibrating integral goes out onto its low limit (generally set at -5%), the plant will settle out at a higher power level than its original condition. If the FW temperature measurement failure occurs at a low load level, a higher probability of reactor trip due to low RC pressure exists than at a high load level. This is because at the low load level the FW temperature is lower than at the high load level. Hence, a greater percentage increase in FW flow will occur at the low load level. Further, at low load levels Btu limits are less restrictive.

d. The MFW flow signal in loop A fails, showing zero flow. The loop A FW control valve will open fully in an attempt to return FW flow to its set point. The ΔP across the loop AFW control valve will decrease below its set point, and the FW pumps will speed up to bring ΔP back to set point. SG A is overfed because control valve A opens fully and the pumps speed up. SG B is initially underfed when control valve A opens fully. It probably is overfed for a short period of time when the pumps speed up, but eventually FW control valve B should return loop B FW flow to its set point.

T_{avg} will fall and the control rods will pull to increase reactor power. The FW flow imbalance between loops A and B will cause a negative ΔT_c error. The ΔT_c control will start to decrease FW demand in loop A and increase FW demand in loop B. This transient may result in a reactor trip caused by low RC pressure, or trip of the FW pumps caused by a high level in SG A.

e. The MFW flow signal fails at a level between zero and demand. Transient proceeds as in (d) but is less severe.

f. This transient is initiated by the startup level signal in loop A failing low. As a result of this, the loop A FW valve opens fully and the FW pumps speed up in an attempt to restore the level in SG A. In order to control loop B flow, the loop B FW valve closes. Neither cross limits nor Btu limits are expected during this initial portion of the transient. Because of excessive FW flow, the primary system may be rapidly overcooled. A reactor trip may occur, probably due to low RC pressure. Also, a high SG level FW pump trip may occur to prevent SG overfill (expected to occur in SG A). A turbine trip would immediately follow the reactor trip. Because of excessive FW flow, steam pressure should be running high, and operation of steam relief as well as turbine bypass is expected to occur at moderate to high power levels. If the reactor trip occurs before the high SG level is reached, there is potential for continued overcooling of the primary due to the open relief valves and the failed level measurement causing the continuing supply of FW to SG A. Popping of the relief valves would cause rapid loss of steam pressure and high flows to be drawn from the SGs. A possible loss of pressurizer inventory along with initiation of HPI may occur. Following the turbine trip, the steam source for the FW pump turbines switches from the low pressure to the high pressure steam supply. Without the high trip, SG A should overfill.

g. This transient is initiated when one of the reactor hot-leg temperature measurements fails high. Let

T_{avg} = reactor average temperature measurement,

T_{hi} = hot-leg temperature measurement, i = A,B,

T_{ci} = cold-leg temperature measurement, i = A,B.

There are three methods of determining T_{avg}, namely,

1. $T_{avg} = \dfrac{T_{hA} + T_{hB} + T_{cA} + T_{cB}}{4}$

2. $T_{avg} = \dfrac{T_{hA} + T_{cA}}{2}$

3. $T_{avg} = \dfrac{T_{hB} + T_{cB}}{2}$

For a failure of T_{hA} high, method 3 above will give the least error in the calculation of T_{avg}, and method 2 will give the greatest error.

Two cases will be considered. The first case will consider complete automatic operation of the ICS. In the second case, the reactor H/A station is in manual, with all other H/A stations in automatic. In both cases, a failure of T_{hA} will cause T_{avg} to be computed erroneously high. Hence, the T_{avg} error in the ICS, given by

$$\text{Error } (T_{avg}) = \text{Set point} - T_{avg}$$

will be negative.

With the ICS in complete automatic, the T_{avg} signal modifies reactor demand. A negative T_{avg} will cause the control rods to insert. If T_{avg} is large enough, it can cause FW flow demand to be modified through the cross limits from neutron error to FW control. A sufficiently negative T_{avg} will cause the FW demand to be increased. Hence, with the power generation of the reactor decreasing and the FW flow increasing, this transient is in the direction of a SG overfill.

With the reactor H/A station in manual and all other H/A stations in automatic, the T_{avg} error signal modifies the total FW demand through a proportional/integral controller. A step increase in the T_{avg} signal, such as would be caused by T_{hA} failing high, has the potential for driving this control loop to an unstable state. The negative T_{avg} signal would initially cause the FW demand to increase rapidly while the reactor demand remains constant. Again, this transient is in the direction of a SG overfill.

h. This transient is initiated by the reactor inlet temperature measurement in loop A failing low. Proportional control action in the ΔT_c control will immediately cause the flow demand in loop A to decrease and the flow demand in loop B to increase. This proportional control action is limited to 5%. Integral action in the ΔT_c control will eventually cause the variable gain multiplier in the flow ratioing circuit to be decreased by an additional 20%. Hence, because of ΔT_c control, the flow demand for loop A flow equals (100% - 5% - 20%) times the total flow demand. The flow demand for loop B flow then equals 200% - (100% - 5% - 20%) times the total flow demand. Therefore, the flow demand in loop A is reduced by 25% and the flow demand in loop B is increased by 25% by ΔT_c control. The low failure of the reactor inlet temperature signal in loop A will also cause an error in the calculation of T_{avg}. As noted in sequence g, there are three methods of determining T_{avg}. (see Eqs. 1-3 above).

For a failure of T_{cA} low, method 3 will result in no error and method 2 will result in the greatest error in the calculation of T_{avg}. It will be assumed that method 1 or 2 is being used to calculate T_{avg}. For T_{cA} failing low, T_{avg} will be calculated low. This will cause reactor power to be increased. Also, low T_{avg} will, through the reactor cross limits to the FW system, cause total FW demand to be lowered. Hence, the reactor power increases; the T_{avg} control causes FW flow to SG B to decrease, and ΔT_c control cause FW flow to SG B to increase. Whether or not SG B will have excessive FW flow is not clear.

i. The reactor inlet temperature loop A-B difference ΔT_c fails high. A high failure of ΔT_c conveys the false information that on the primary side the temperature of cold leg A is higher than cold leg B. The ΔT_c error is apportioned equally in magnitude but opposite in sign to the loop A and loop B flow demands. However, the change in demand in each loop is limited to 25% of total flow demand.

   If the initial unit load is high enough, Btu limits will be activated and limit the increase in FW flow in loop A. This will cause a net reduction of the total FW flow and an increase in T_{avg}. The control rods will insert, reducing reactor power, to try to return T_{avg} to its set point. A reactor trip on high RC pressure is possible. If the plant is not at high load so that the Btu limits are not activated, the unit will probably settle out at a new steady state with a cold-leg temperature imbalance. Hence, for a high failure of ΔT_c, SG A will be overfed and SG B will be underfed.

j. The reactor average temperature measurement, T_{avg}, fails high. The high failure is assumed to be due to one of the following three failures:

   1. Failure of the hot-leg temperature measurement in primary side loop A (i.e., T_{hA}).

   2. Failure of the cold-leg temperature measurement in primary side loop A (i.e., T_{cA}).

   3. A high failure of T_{avg} for some reason other than (1) or (2).

Each of the three failures will be considered separately. Also, it is assumed that T_{avg} is calculated by (see scenario g):

$$T_{avg} = \frac{T_{hA} + T_{cA}}{2} \quad ,$$

for this results in the largest error in T_{avg} for the assumed failures. If T_{avg} fails high because T_{hA} fails high, scenario g applies. In this case, the high T_{hA} (assuming T_{hA} is the outlet temperature selected by the operator) will increase the allowable maximum FW flow demands calculated by the Btu limits. If T_{avg} is determined to be too high for some other reason, there should be no effect on the Btu limits.

If T_{avg} fails high as a result of T_{cA} failing high, scenario g must be modified to account for the effects of the ΔT_c control loop. With ΔT_c control coming into play, SG overfeed will not be symmetric as considered in scenario g. Instead, because ΔT_c control ratios the FW flows, overfeed of SG A will be greater than of SG B. Hence, with a high failure of T_{cA}, the overfeed of SG A should be worse than that considered in scenario g.

If a high failure of T_{avg} occurs for some reason other than a T_{avg} high failure of T_{hA} or T_{cA}, scenario g will again apply except for the above-mentioned effect on Btu limits.

With all three failure modes resulting in high failure of T_{avg}, the SGs are overfed. In every case there is the possibility that the reactor may trip on low RC pressure or the FW pumps may be tripped on high SG level.

k. The neutron flux density reading fails high. The control rods will begin to insert continuously, trying to reduce the neutron flux density reading. The lower the unit load, the larger the neutron error will be. Through the cross limits, the large neutron error calls for an increase in the FW flow. Both SGs are overfed, and the primary is overcooled. The Btu limits will probably be activated and will limit maximum FW flow demands. The cross limits will cause the unit to go into track mode, and because of the increased FW flow and steam pressure, the unit megawatt electric demand will track up. A reactor trip on low pressure is highl; probable. Following reactor trip, the turbine will trip and megawatt electric generation will go to zero. The unit is still in the track mode at this time, and FW demand from the integrated master goes to zero. However, following reactor trip, the cross limits from reactor control to FW control increase, calling for FW flow close to 100%. Hence, the Btu limits, and not the feed forward signal from the integrated master, must be relied upon to run back the FW system.

l. When the loop A startup FW control valve becomes less than 50% open, the loop A startup FW control valve position signal fails to indicate that the valve is less than 50% open. Hence, the MFW blocking valve in loop A does not receive a signal to close. The leakage through the loop A MFW control valve, if excessive, may cause SG A to be overfed. Also, since the MFW blocking valve in loop A does not close, the flow measurement used in FW control is not switched from the MFW flow measurement, which is highly inaccurate at such low flows, to the startup FW flow measurement. Thus, control will not be as smooth as normal. If the leakage through the MFW control valve is large enough, the startup FW valve may close completely while SG A continues to be overfed from the leakage. This condition would probably result in a SG high level trip of the FW pumps.

m. The MFW blocking valve in loop A is open, but its position indicator fails in closed position. This causes the ICS to take FW flow measurements from the sensor in the startup line. If reactor is at high power, a flow demand signal is sent causing a flow increase in both loops. Cross limits cause rod insertion signals. Btu limit may be actuated. SGs are overfed. Reactor may trip on low pressure.

n. The speed governor on FW pump A fails high. This will cause FW pump A to go to its high-speed stop, and FW flow to the SGs to increase. Flow control will cause the FW control valves to close to return the FW flows to their set point. As the control valves close, ΔP control will cause the speed of FW pump B to decrease. Concerning the operation of pump B during this transient, three conditions may occur: the plant may settle out with pump B at reduced speed with both pumps supplying flow to the SGs; the plant may settle out with the check valve in series with pump B closed and pump B supplying no flow to the SGs; or pump B may begin to operate in an oscillatory mode, with the check valve cycling open and closed. In any event, pump A will be at its high-speed stop. Also, a ΔP higher than the set point may exist across the control valves following the transient. Some overfeed of the SGs will occur, but a reactor trip is not anticipated.

o. The MFW control valve in loop A fails open. (This transient will be more serious if it is initiated well below full power--say at 25%). The flow in A increases with the valve full open. The low ΔP signal across control valve A leads to increased pump speed. The ΔT_c error will attempt to reduce flow in A and increase flow in B, and the total flow demand error will attempt to reduce flow in both A and B. Because of the valve failure, loop A is not affected by these signals. Because of the substantial increase in total flow (resulting from the loop A failure), the total flow demand error should dominate the ΔT_c error signal in loop B, either immediately or very quickly, and continue to do so. SG A therefore fills while SG B empties. If the SG B level drops to low level indication before high level pump trip occurs in SG A, the low level signals in

SG B will override and prevent the level from falling further. Hence, the low level signal in B, together with the total flow demand error signal, should keep the level in SG B at about the low level indicator until the pumps are tripped.

The MFW pumps should trip on a high level signal in SG A.

p. The loop A FW startup valve fails open. There would be no effect during operation at power, and probably the failure would not be detected. However, during plant shutdown the excessive flow in loop A would prevent the SGs from going on low level control. Appropriate manual control actions could be used to shut down the plant safely.

Following a reactor trip, this failure would result in overfeed of SG A if proper manual control actions are not taken. When the reactor trips, the turbine also trips; the steam system goes on bypass control; FW flow demand runs back to low value; and the SGs are supposed to go on low level control. With the startup valve in loop A failed wide open, SG A will be overfed. Without manual control intervention, FW pump trip on high level in SG A is likely. Simulation of this failure was required to determine the quantitative results, which are discussed in Sect. 4.

q. The control system summer that sums the startup level and turbine header pressure signal fails, giving low indication. This failure is equivalent to the corresponding failure in any of the component signals and causes increased flow to the SG. The high level FW pump trip occurs at high level indication.

r. A sufficient leak in selected SG pressure tap A (A') or in the pipe connecting it to blocking valves, or in the packing of either blocking valve at which the pipe terminates, will cause a low level signal and an overriding demand for FW. The SG will fill to the high level pump trip level, 394 in., and cause trip of the MFW pumps. The AFW will come on, and (with the low level signal still present and no high level constraints) the AFW will continue the overfeed, causing SG overfill. (Consult A.2.2.2.)

s. Failure of the MW(e) demand signal high will lead to demand for more FW flow and more reactor power. The FW demand response is much faster than the core power demand response. However, cross limits would be activated and limit the rate of increase of FW flow. Hence, the FW system response would be approximately coordinated with that of the reactor. That is, if the system energy balance is taken into account, the FW system should run just slightly ahead of the reactor. The cross limits should hold the FW system back. Some SG overfeed should result, but it should not be severe.

t. Under normal conditions, the turbine header pressure error signal compensates the startup level measurement. It is first put through a hard limiter to limit its effect on the level indication to not more than 8 in. However, a failure of the hard limiter signal could negate the limiting effect. This error is then potentially equivalent to sequence f.

u. Both high and low failures of RC flow measurement in loop A will be considered. Consider first a high failure. The reactor coolant flow imbalance FW ratioing circuit will immediately reratio the FW flows. The FW flow in loop A will be increased, and the FW flow in loop B will be decreased, leading to overfeed of SG A and underfeed of SG B. After a short time lag, the ΔT_c control will decrease FW flow in loop A and increase FW flow in loop B, thus providing some compensation for the original failure. Whether or not a reactor trip will occur during the course of events is uncertain.

Next consider the RC flow measurement in loop A falsely indicating zero flow. The low failure has a much larger effect than the high failure, because there is more room on the low side than on the high side of the RC flow measurement range. A front-end runback to a lower load level will be implemented immediately in the unit load demand load limit circuitry. Again, the reactor coolant flow imbalance FW ratioing circuit will immediately reratio FW loop flows. In this case, however, reratioing will be in the opposite direction and much larger. The FW flow in loop A should be decreased to the point that SG A goes on low level control. In loop B, the Btu limits should be activated and thus restrain the increase in FW flow. Hence, in this case, overfeed of SG B and underfeed of SG A occur.

When loop B goes on Btu limits, cross limits to the reactor will reduce reactor power, and the unit will also go into the track mode. During the initial phase of this transient, there is a net reduction in FW flow when SG B goes on Btu limits, and a reactor trip on high RC pressure is probable.

v. Failure in the open position of the atmospheric dump, turbine bypass, or any safety valve in the main steam line will cause an increase in the pressure drop across the SG and an initial increase in the feed of the SG. This event is bounded by the small break in the main steam line.

w. The low level set point fails, giving a reading at its highest level. This failure is functionally equivalent to r.

APPENDIX B REFERENCE

1. R. W. Enzinna, R. W. Winks, S. D. Swartzell, R. P. Broadwater, M. S. Kai, and W. E. Wilson, "Failure Modes and Effects Analysis of the Midland NNI and ICS," Babcock & Wilcox Co. Report BAW 1743 (July 1982).

APPENDIX C

Details of Hybrid Simulation Model Validation and Results

APPENDIX C

Details of Hybrid Simulation Model Validation and Results

C.1 MODEL VALIDATION DETAILS

As noted in Sect. 4.3 of this report, model validation activities included comparisons of results with both data from B&W plants and calculations from other codes.

Figure C.1 shows SG water level measured in a B&W plant similar to Oconee 1; the level indication is obtained from the pressure difference between taps and is the sum of static and dynamic heads. Simulation of this measurement as a function of load is seen to be in agreement with plant data.

Figure C.2 shows the primary and secondary temperature profiles in the Oconee-type once-through generator, and Fig. C.3 indicates the heat transfer surface utilization, that is, the fraction of tube length in the boiling mode as a function of load. The measured values were taken from standard B&W design reports, and the model tracks closely.

Figure C.4 shows the measured and calculated FW temperature as a function of feed flow after turbine trip and reactor runback in a plant very similar to Oconee 1 in design and operation. Feed flow was a boundary condition in this test of the balance-of-plant portion of the model. Because the measurements were made near the input to the SG and the calculations are upstream of this point by ~20 s, there is a small delay before the measured values begin to decline.

Figure C.5 compares the core flood tank simulation with an Electric Power Research Institute analysis of a transient at Three Mile Island Unit 2.[1] The right scale is coolant injection as a function of primary pressure. The left side is the nitrogen over-volume during tank evacuation.

In March 1980 a turbine trip at Oconee 3, sister plant to Oconee 1, was accompanied by an ICS malfunction that resulted in overfeed of the SGs. (see Table C.1). Overfilling continued for ~112 s until the high level trip in SG A caused feed-pump trip. Data from the first 180 s of the transient were available for model testing. No design data for Oconee 3 were available, and the Oconee 1 design was assumed. Secondary side information included FW flow and pressure and water levels for both SGs. Primary side data included power level, pressurizer water level, pressure, and hot- and cold-leg temperatures of both loops. The hybrid model is compared with these in Figs. C.6 through C.14. In general, the model tracked closely, with the exception of the SG B water level which fell below the measured value after the first minute.

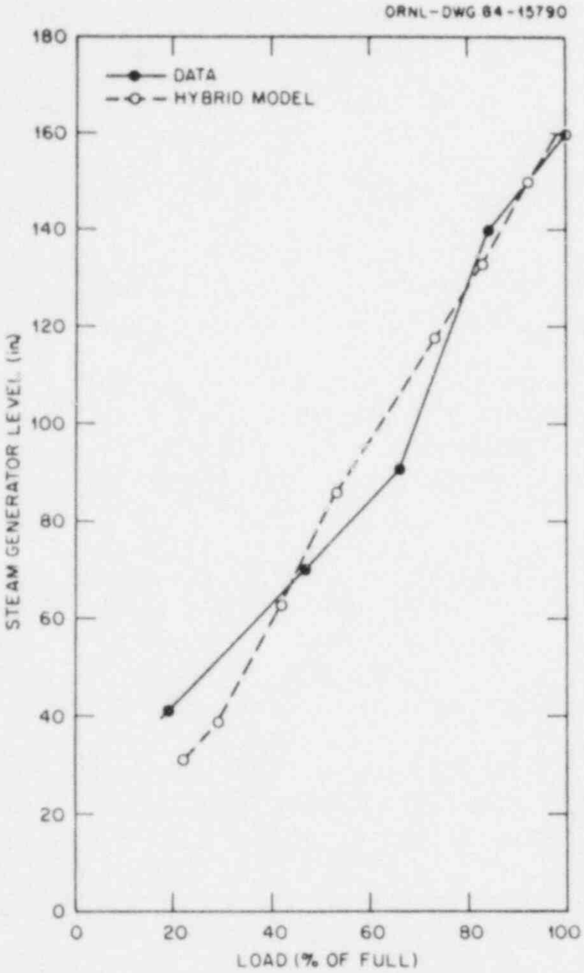


Fig. C.1. Steam generator ΔP signal versus load.

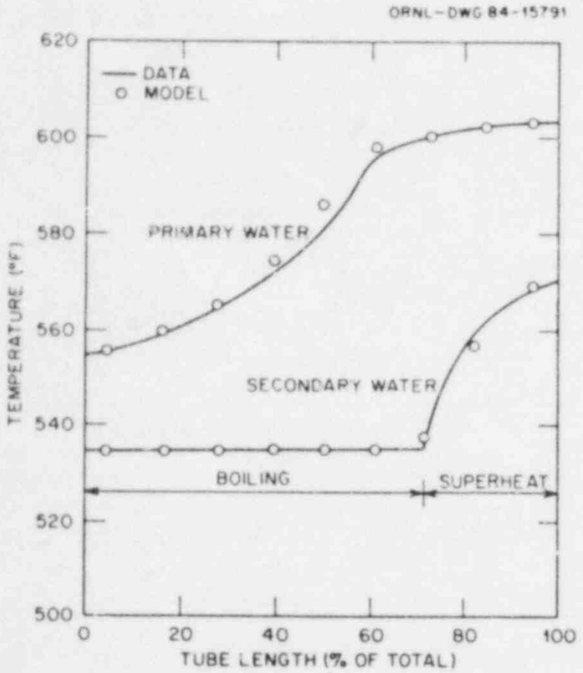


Fig. C.2. Primary and secondary temperature profiles in the steam generator at 100% load.

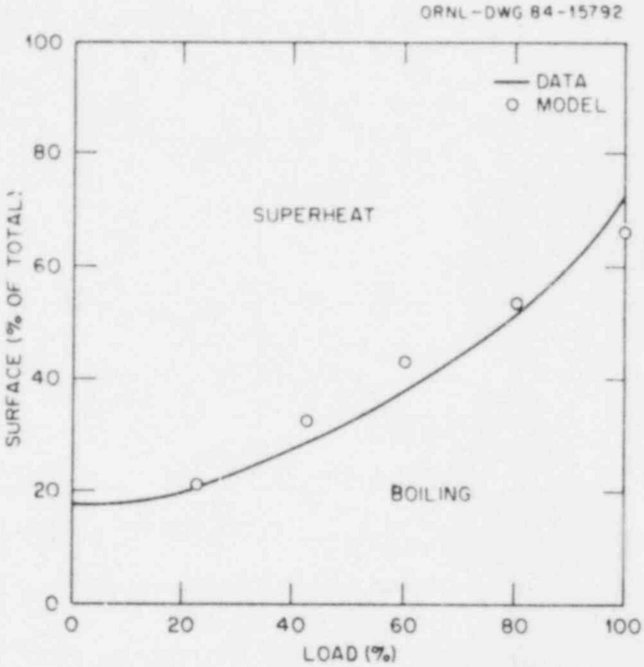


Fig. C.3. Steam generator surface utilization (heat transfer) versus flow.

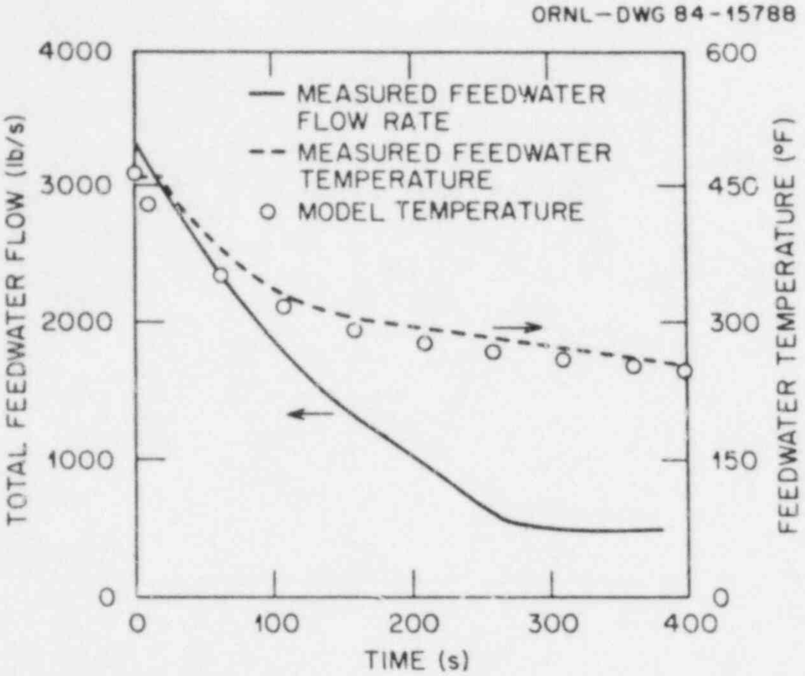


Fig. C.4. Comparison of model with measured feedwater temperaturę in a B&W nuclear plant.

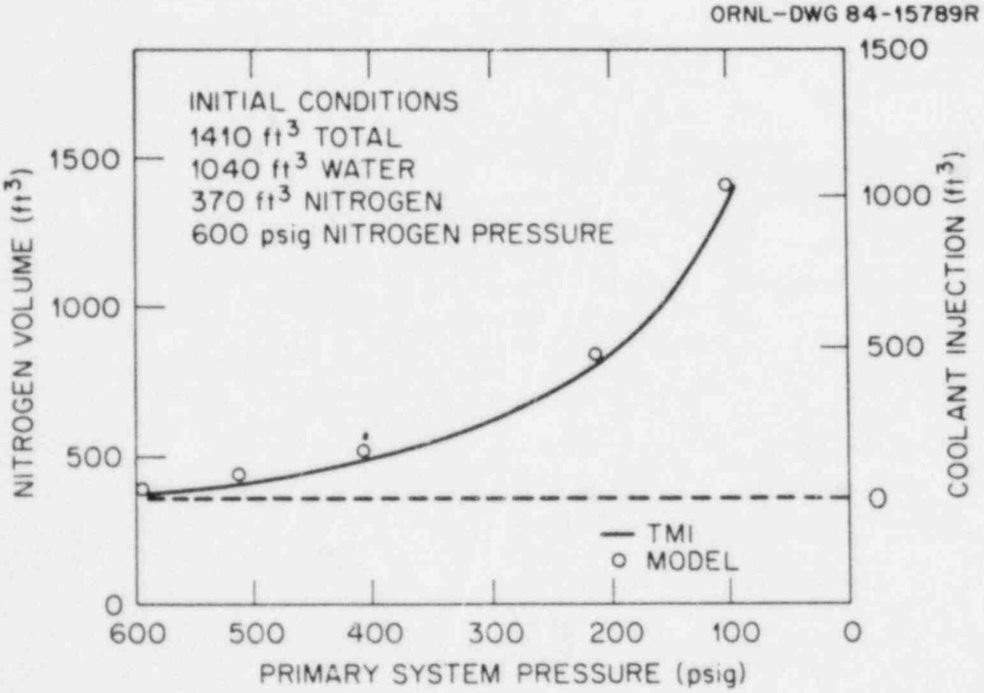


Fig. C.5. Core flood tank capacity versus primary coolant system pressure.

As part of the Pressurized Thermal Shock (PTS) Program, this overfill transient was also run on both the TRAC PF1 and RELAP5 codes. The TRAC results[2] are included in Figs. C.6 through C.14. The RELAP5 results,[3] together with the hybrid model results, are given in Figs. C.15 through C.22. TRAC and RELAP5 show good agreement with the plant data except for the SG B water level which fell below the measured value after the first minute, as was found with the hybrid model. The PTS study speculated that the EFW system may have been running, though this is not detectable in the available information, possibly explaining the higher measured water level in SG B. The hybrid model shows the same degree of agreement with the Oconee 3 data as TRAC and RELAP5, and consequently compares well with these validated production codes.

Table C.1. Oconee 3 overfeed transient of March 1980

Event	Time (s)
Reactor and turbine tripped	0
Steam block valves closed	0.5
Steam bypass valves opened	2
Feed train heater drains closed	5
Feed flow to SG A zeroed by steam pressure buildup	20
Feed flow to SG B minimized by steam pressure buildup	2-30
High pressure injection initiated on low primary pressure	30
Feedwater to SG A increased to ~8% flow	40
FW to SG B increased to ~26% flow	40
Pressurizer water level and pressure bottomed, began to rise	60
Feed pumps tripped on high SG A water level	112

The hybrid model was used to calculate guillotine-type main steam line breaks (MSLB), compounded by SG tube rupture of varying degrees (see Sect. 4.8). The PTS program also explored several steam line break sequences with the TRAC and RELAP codes. Although tube rupture was not part of the PTS scenarios, the first minutes (particularly the blowdown phase) of the PTS scenario labeled MSL86[4] were similar to the hybrid MSLB in other major characteristics. (After the first 5 min, the PTS and hybrid scenarios purposely followed different paths.) Comparison of important variables during blowdown is shown in Table C.2. Both models calculated SG dryout in ~20 s. Minimum primary pressures were 1500 psia in the PTS case and 1535 psia for the hybrid model. The maximum temperature drop during blowdown was 45°F in the PTS calculation and

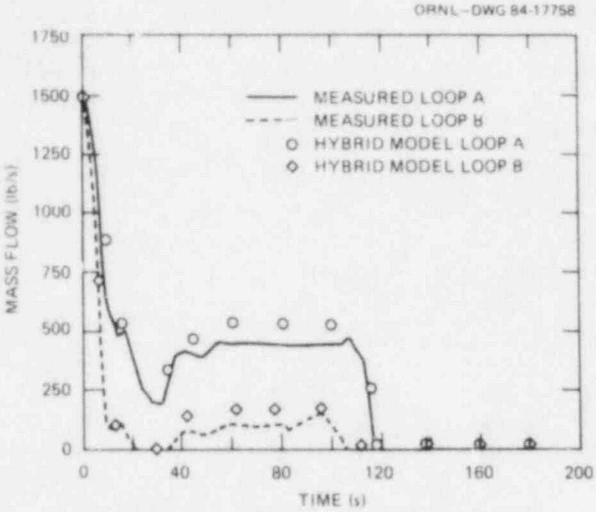


Fig. C.6. Main feedwater flow rate. Feedwater flow and temperature treated as boundary conditions in TRAC calculation.

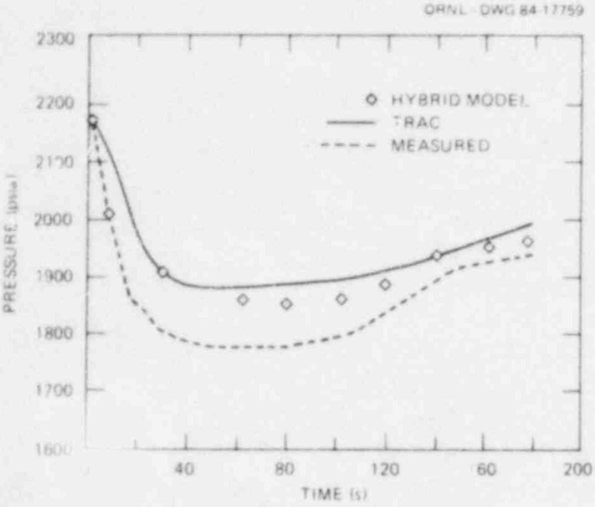


Fig. C.7. Primary pressure.

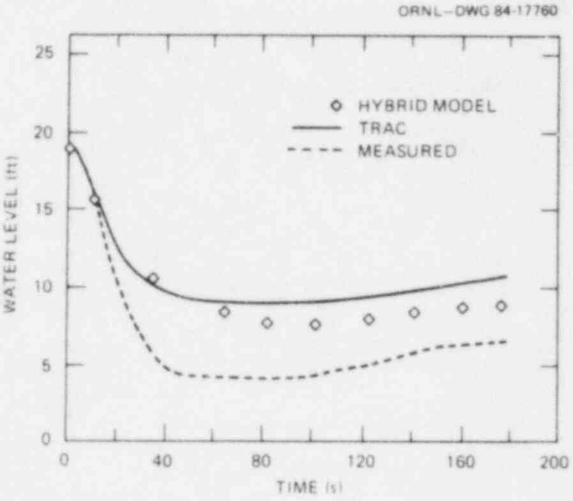


Fig. C.8. Pressurizer water level.

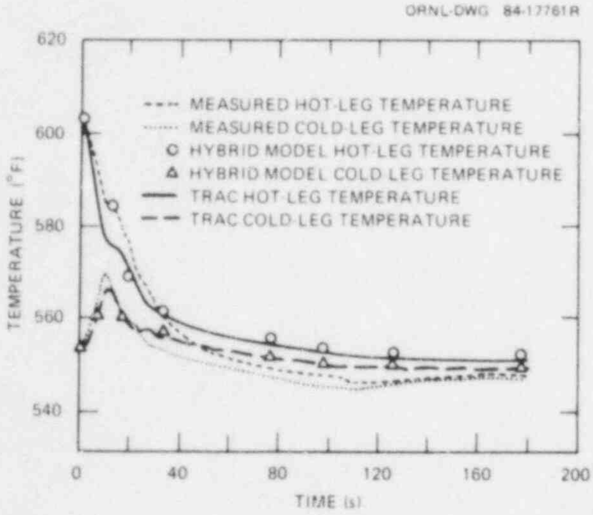


Fig. C.9. Hot- and cold-leg temperatures, Loop A.

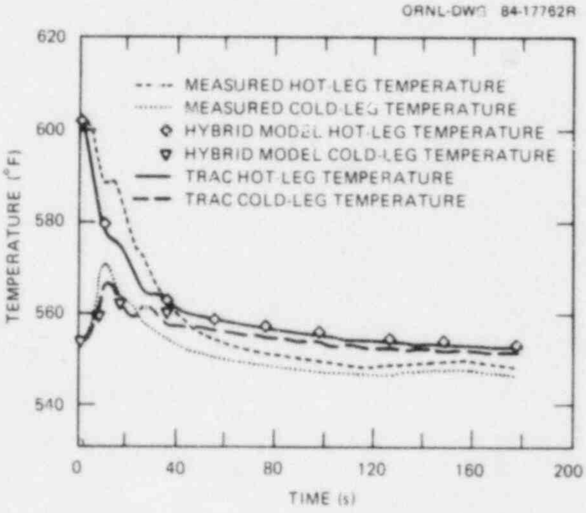


Fig. C.10. Hot- and cold-leg coolant temperatures, Loop B.

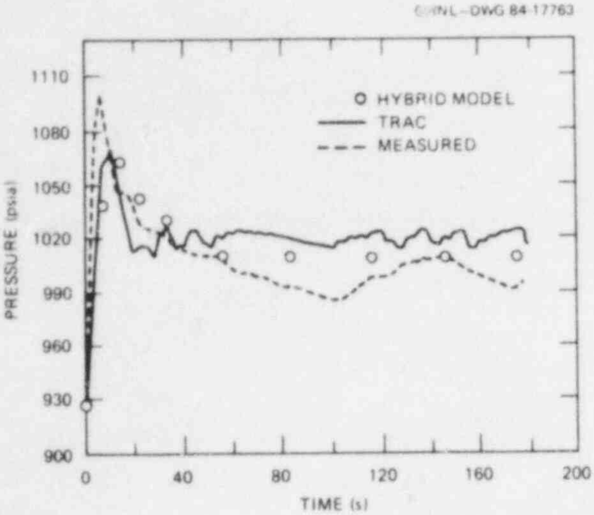


Fig. C.11. Steam generator A secondary pressure.

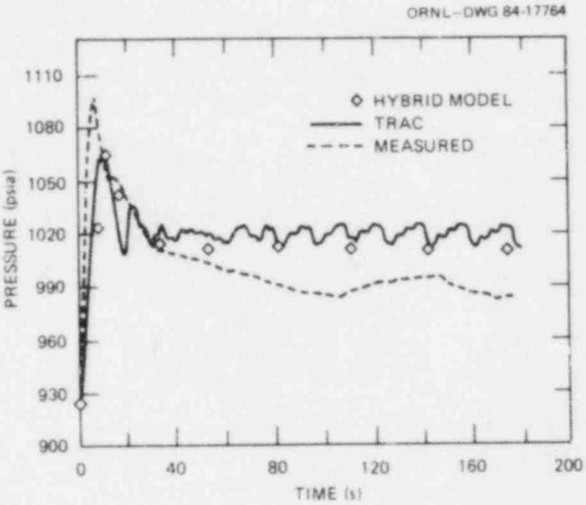


Fig. C.12. Steam generator B secondary pressure.

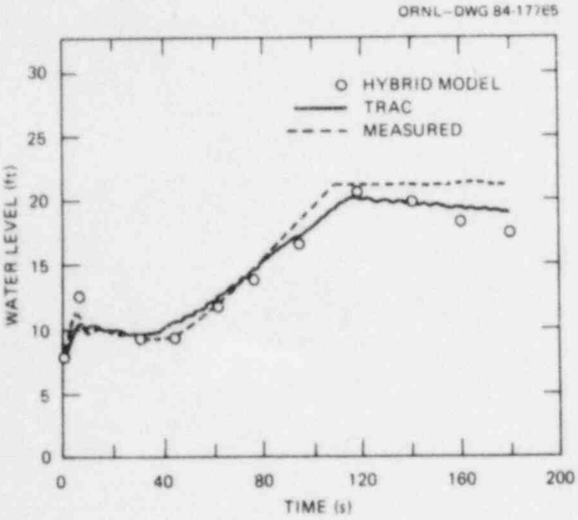


Fig. C.13. Water level in SG A.

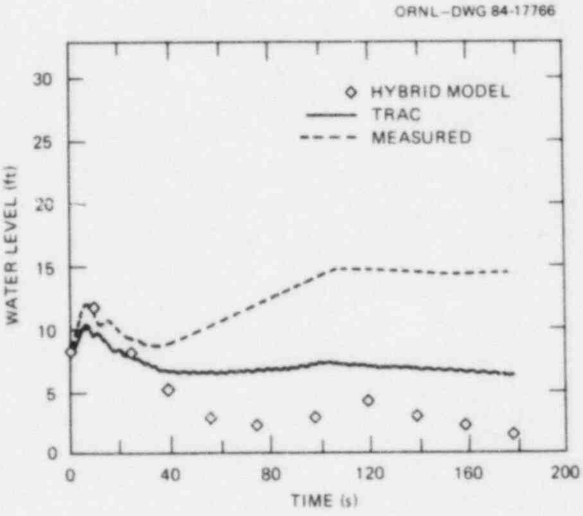


Fig. C.14. Water level in SG B.

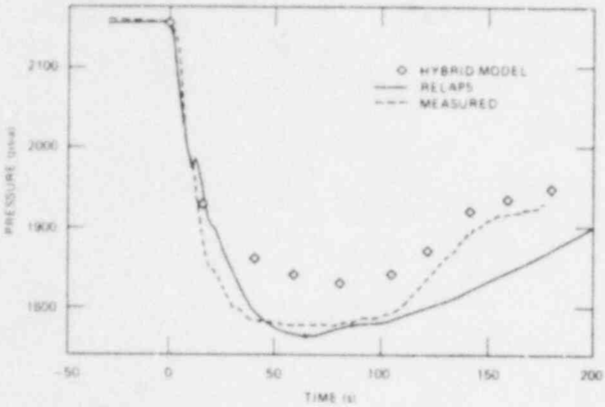


Fig. C.15. Primary pressure.

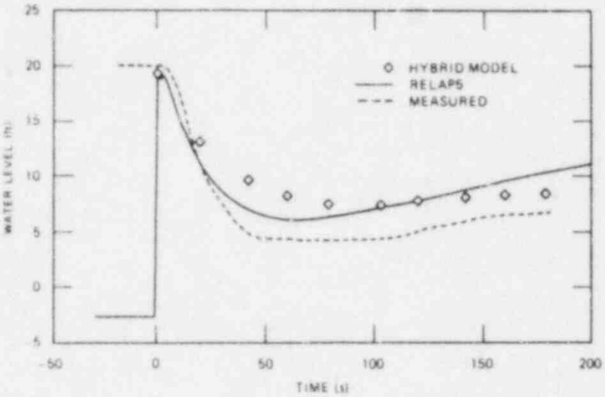


Fig. C.16. Pressurizer water level.

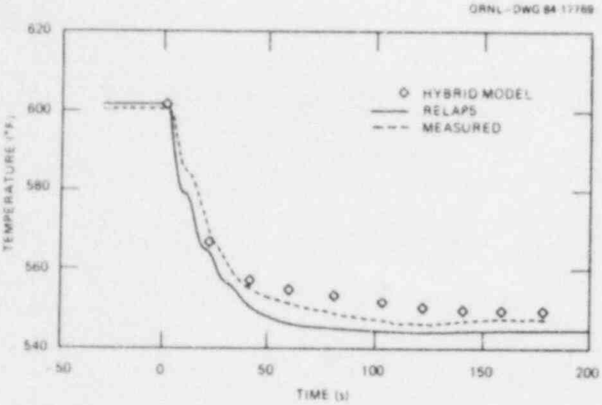


Fig. C.17. Hot-leg coolant temperature, Loop A.

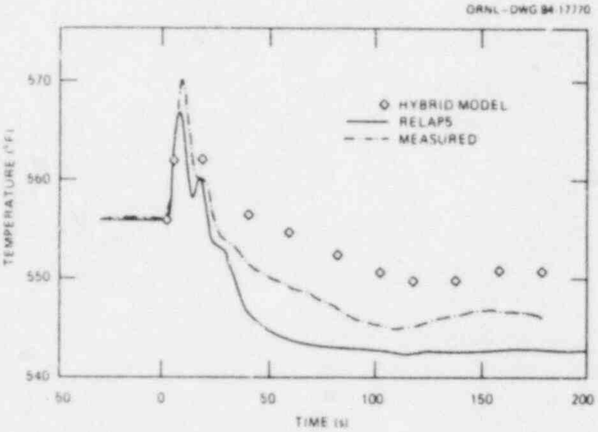


Fig. C.18. Cold-leg coclant temperatures, Loop A.

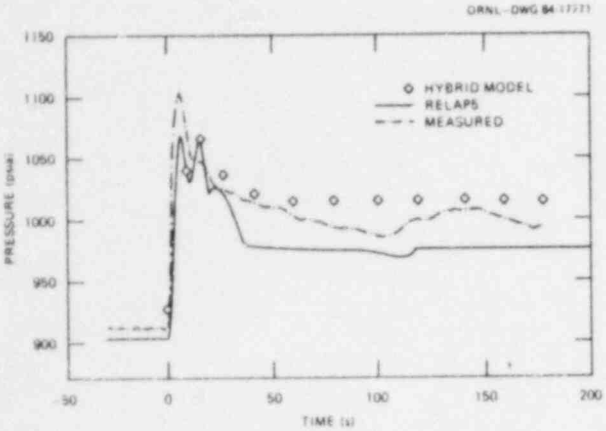


Fig. C.19. Steam generator A secondary pressure.

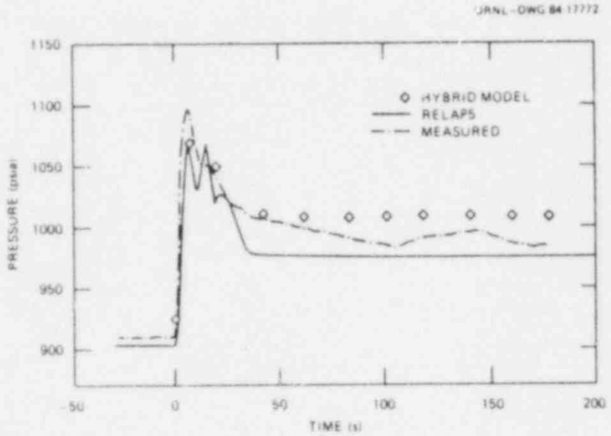


Fig. C.20. Steam generator B secondary pressure.

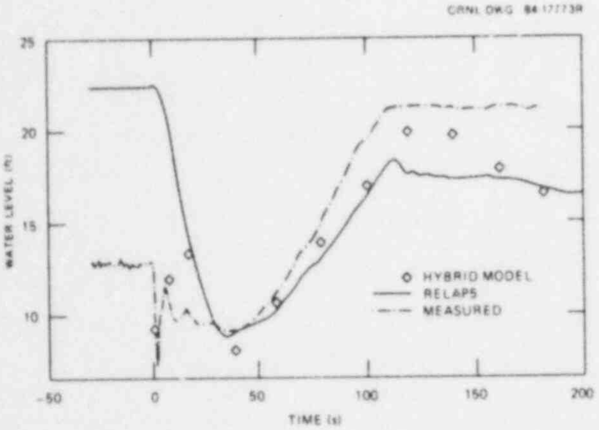


Fig. C.21. Water level in SG A.

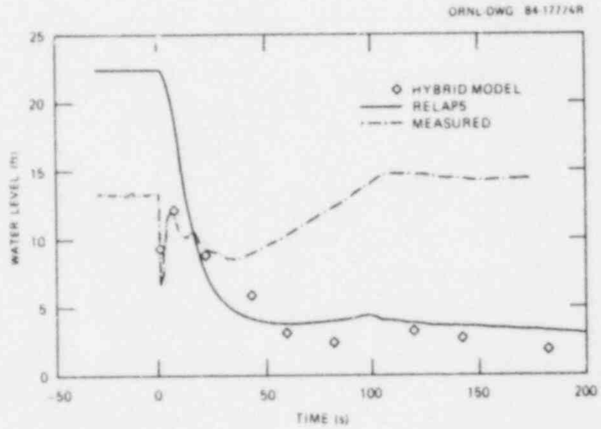


Fig. C.22. Water level in SG B.

56°F in the hybrid calculation. The comparisons indicated that the hybrid model, particularly the SG submodel, performed appropriately during the relatively severe blowdown process.

Table C.2. Comparison of TRAC/RELAP and hybrid model calculations of the blowdown phase of a main steam line break event

Steam Generator Dryout Time (s)		Maximum Downcomer Temperature Drop (°F)		Minimum Primary Pressure (psia)	
MSLB6	Hybrid	MSLB6	Hybrid	MLSB6	Hybrid
20	21	45	56	1500	1535

C.2 DETAILS OF HYBRID SIMULATION RESULTS

The results of the four groups of events considered in the augmented FMEAs are described in Sect. 4 of the report as follows: SG overfill transients (4.5); Secondary side depressurization transients (4.6); Overheating transients (4.7); and SG tube rupture transient (4.8). Backup information for these descriptions are included in Figs. C.23 through C.93. References to the respective sections of the report, as well as descriptions of the events simulated, are included in the figure captions.

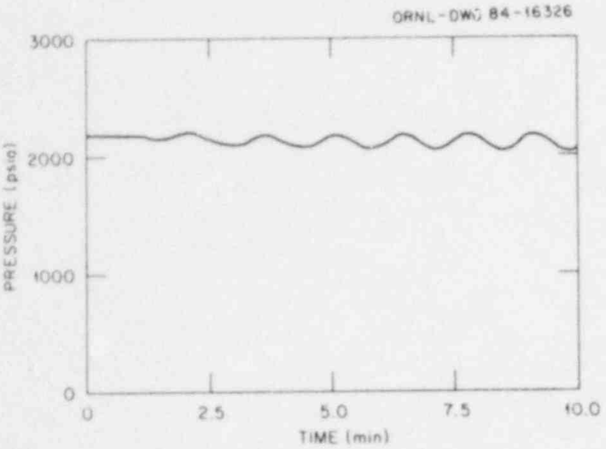


Fig. C.23. Pressurizer pressure: overfill (Class 1)* at 100% power. Intermediate overfeed failure insufficient to active SG level protective features other than ICS interaction.

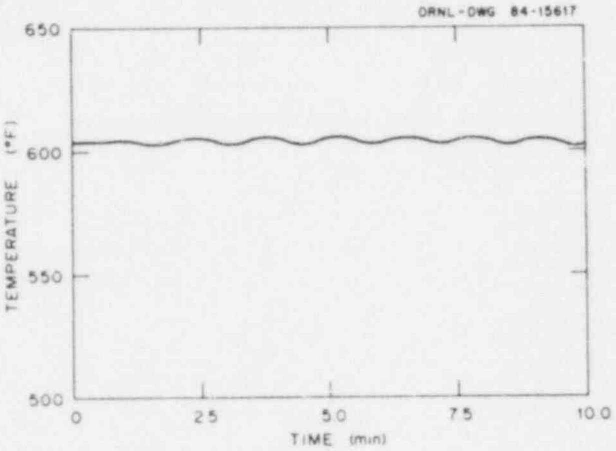


Fig. C.24. Core outlet coolant temperature: overfill (Class 1) at 100% power. Intermediate overfeed failure insufficient to activate SG level protective features other than ICS interaction.

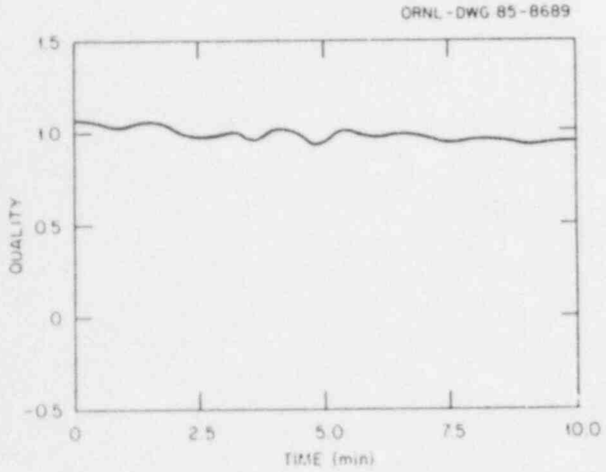


Fig. C.25. SG A outlet quality: overfill (Class 1) at 50% power. Intermediate overfeed failure insufficient to activate SG level protective features other than ICS interaction.

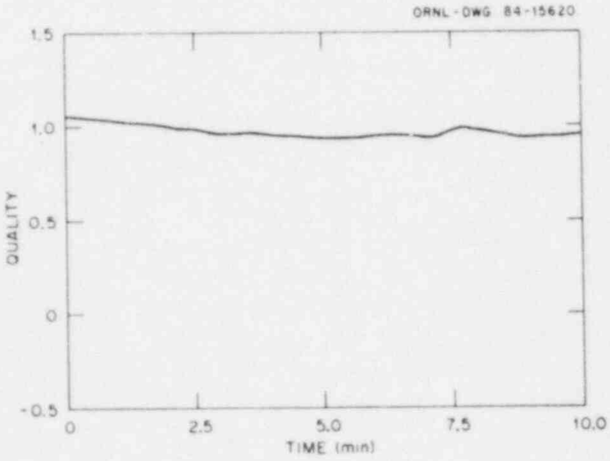


Fig. C.26. SG A outlet quality: overfill (Class 2) at 100% power. Cverfeed failure when high-level control transfer is approached but not reached.

*Failure classes are described in Sect. 4.5.

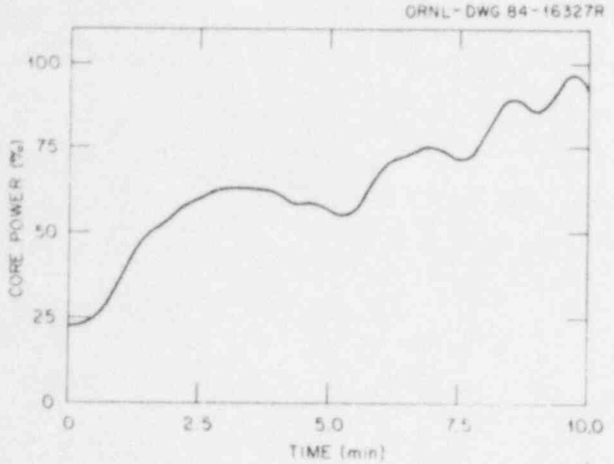


Fig. C.27. Core power fraction: overfill (Class 3) at 20% power. MFW control valve action in combination with overfeed failure when high-level contro' transfer is approached but not reached.

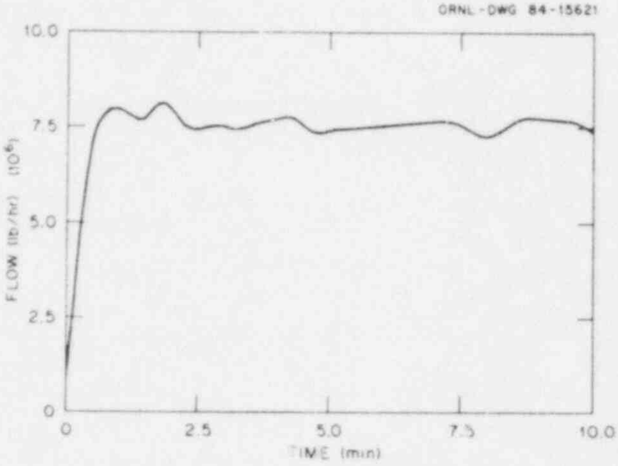


Fig. C.28. SG A feedwater flow: overfill (Class 5) a: 20% power. Overfeed with failed high-level control transfer and pump trip.

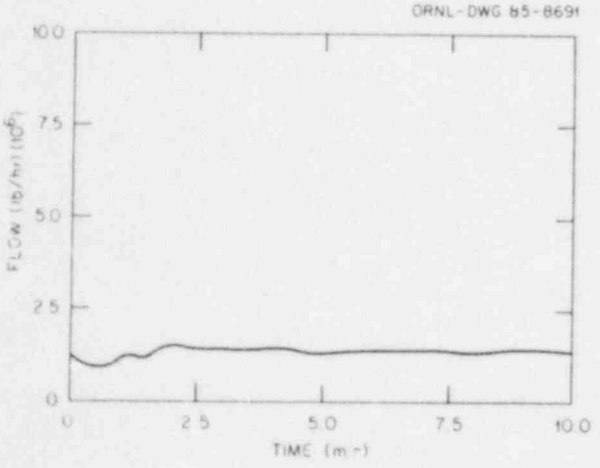


Fig. C.29. SG B FW flow: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

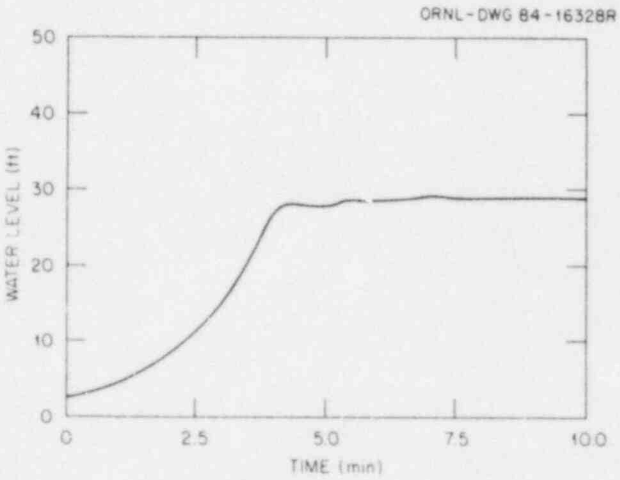


Fig. C.30. SG A water level: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

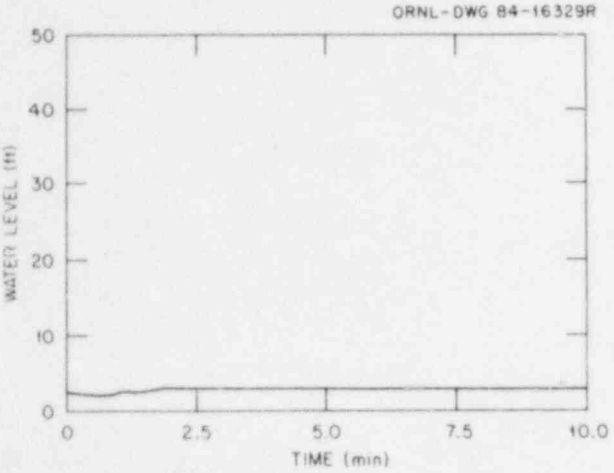


Fig. C.31. SG B water level: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

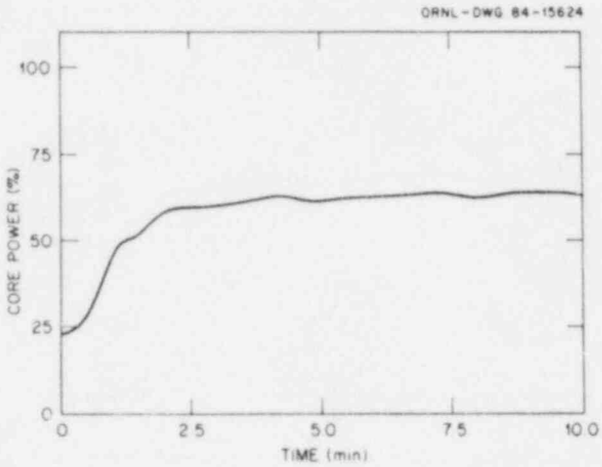


Fig. C.32. Core power fraction: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

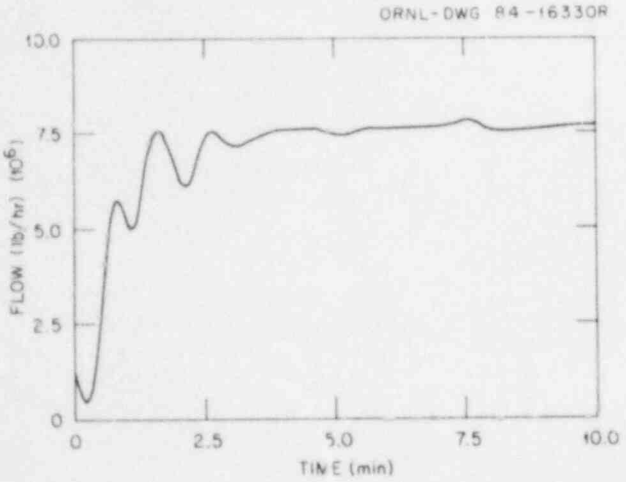


Fig. C.33. SG A steam flow: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

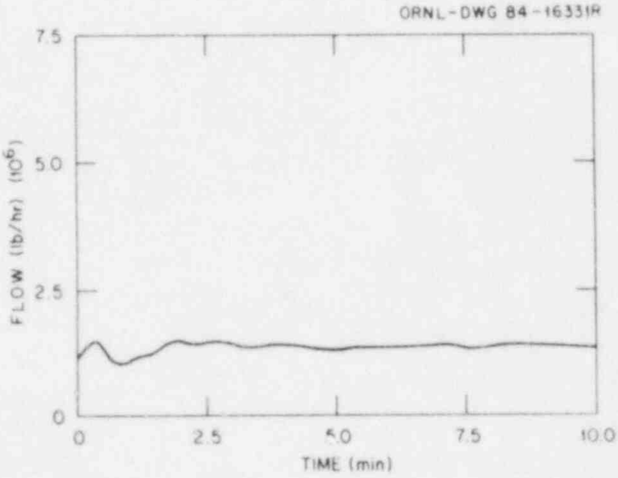


Fig. C.34. SG A steam flow: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

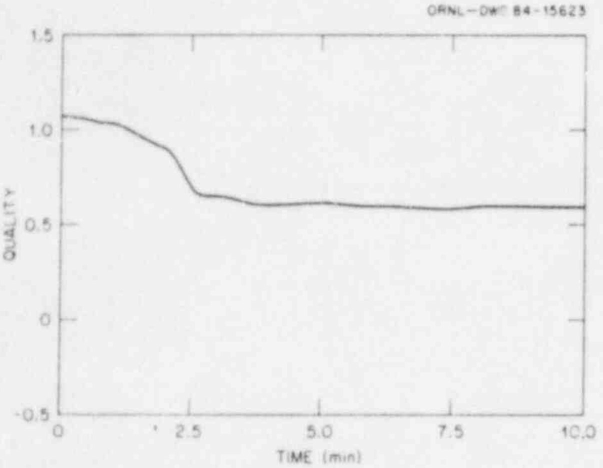


Fig. C.35. SG A outlet quality: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

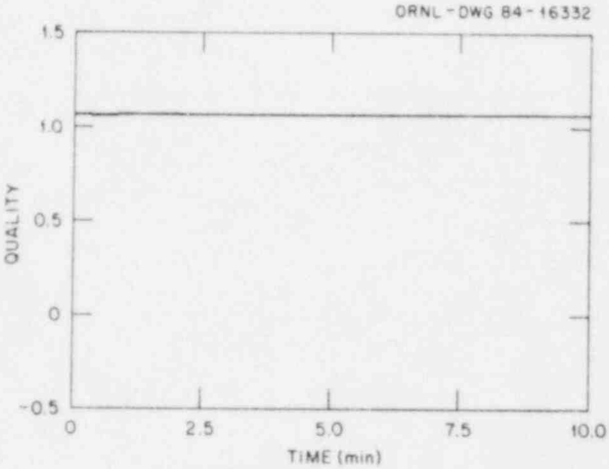


Fig. C.36. SG B outlet quality: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

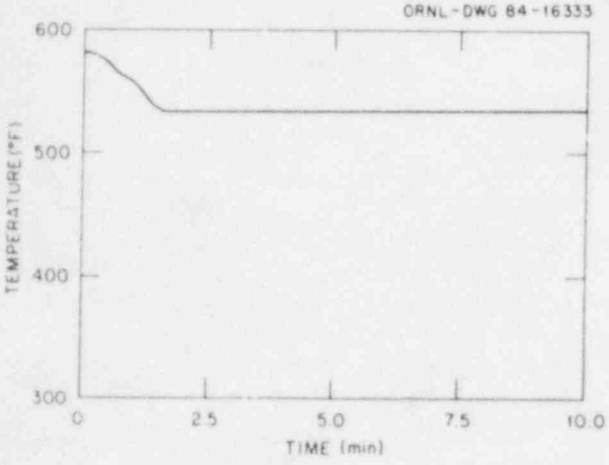


Fig. C.37. SG A outlet temperature: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

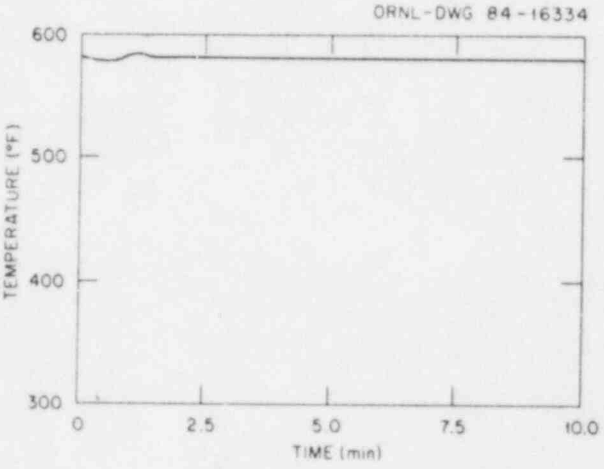


Fig. C.38. SG B outlet temperature: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

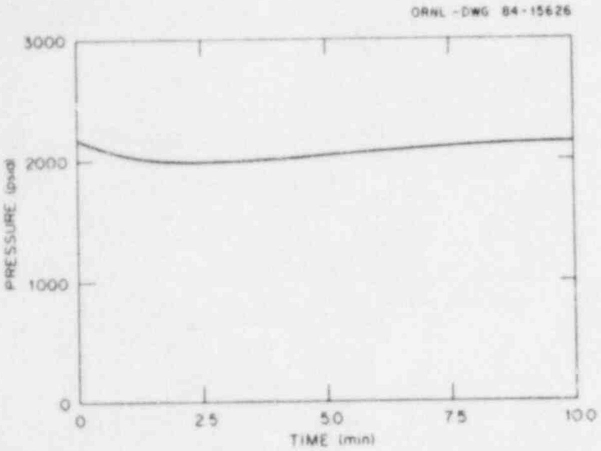


Fig. C.39. Pressurizer pressure: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

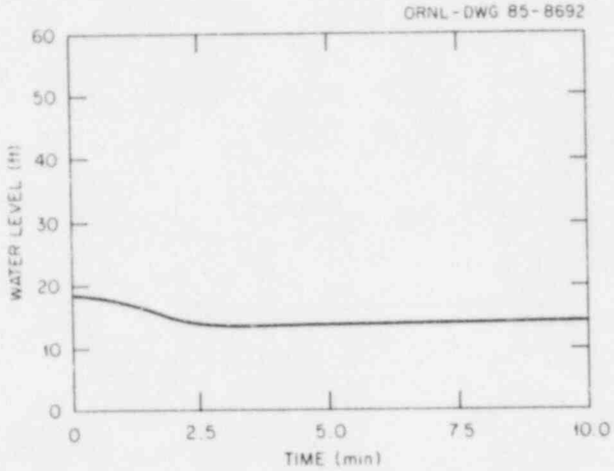


Fig. C.40. Pressurizer level: overfill (Class 5) at 20% power. Overfeed with failed high-level control transfer and pump trip.

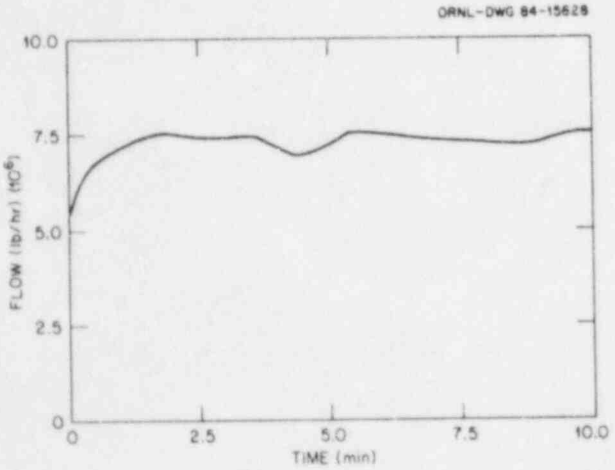


Fig. C.41. SG A feedwater flow: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

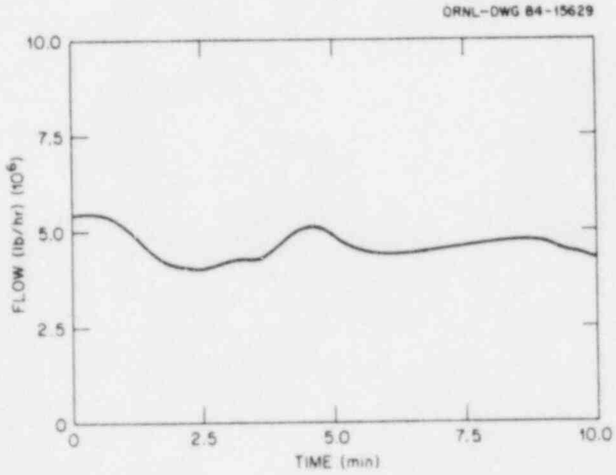


Fig. C.42. SG B feedwater flow: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

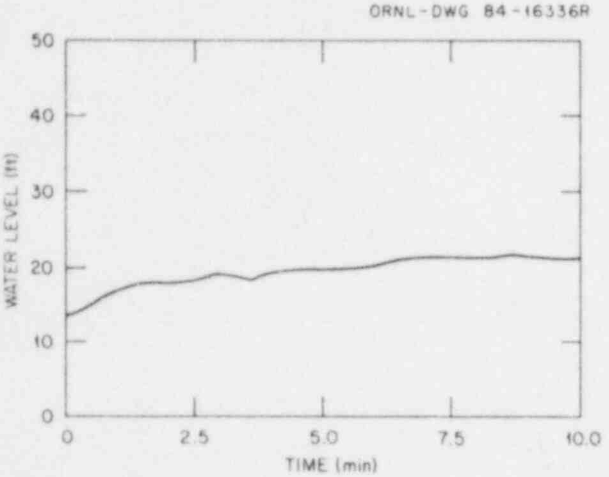


Fig. C.43. SG A water level: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

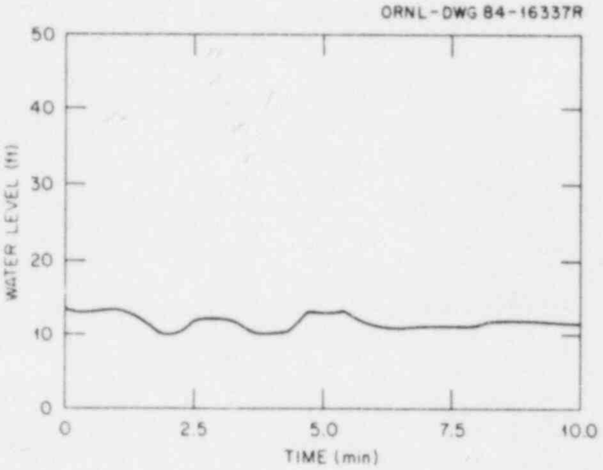


Fig. C.44. SG B water level: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

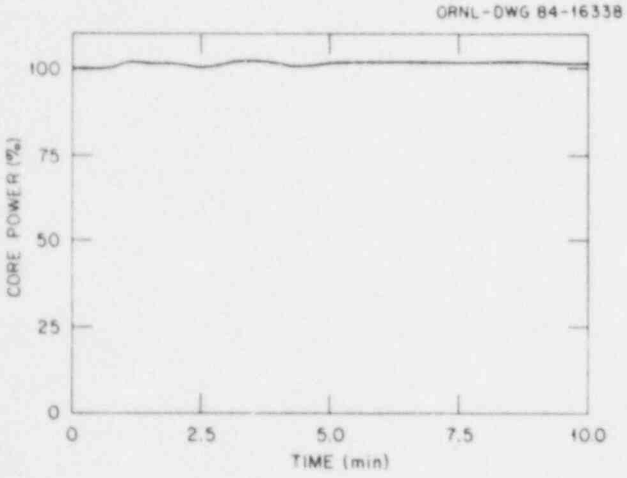


Fig. C.45. Core power fraction: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

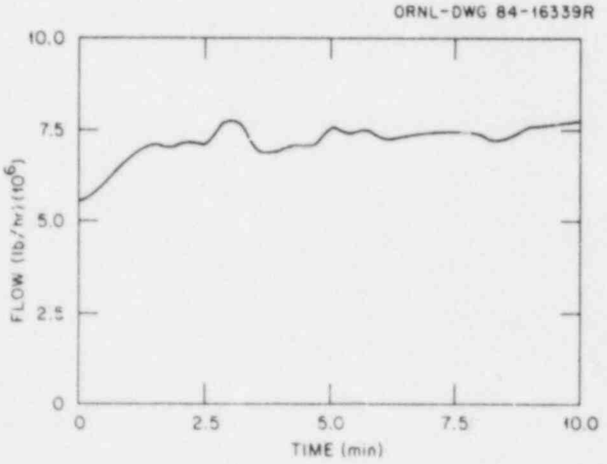


Fig. C.46. SG A steam flow: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

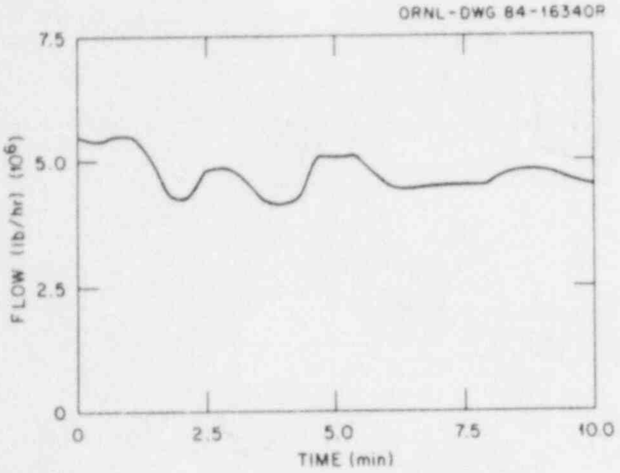


Fig. C.47. SG B steam flow: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

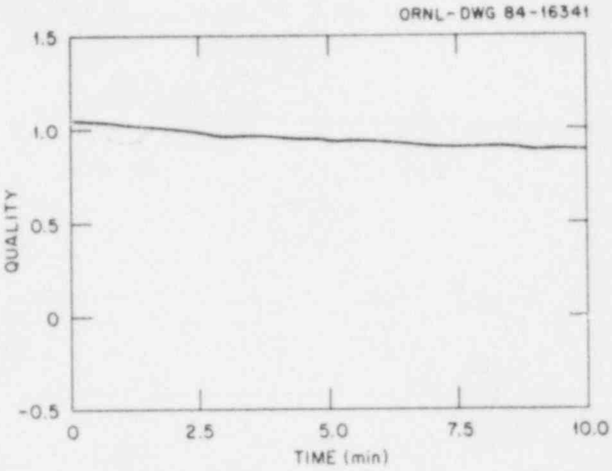


Fig. C.48. SG A outlet quality: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

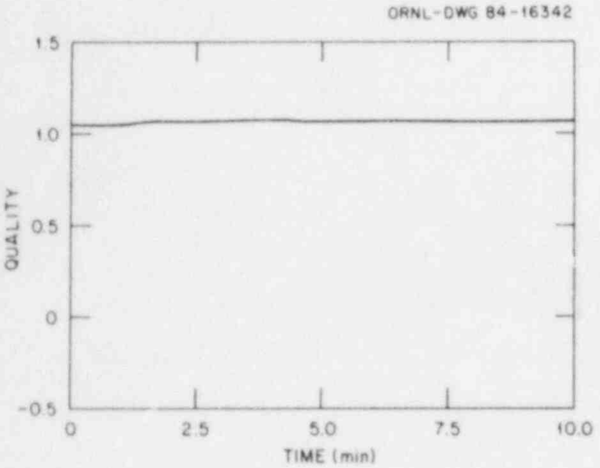


Fig. C.49. SG B outlet quality: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

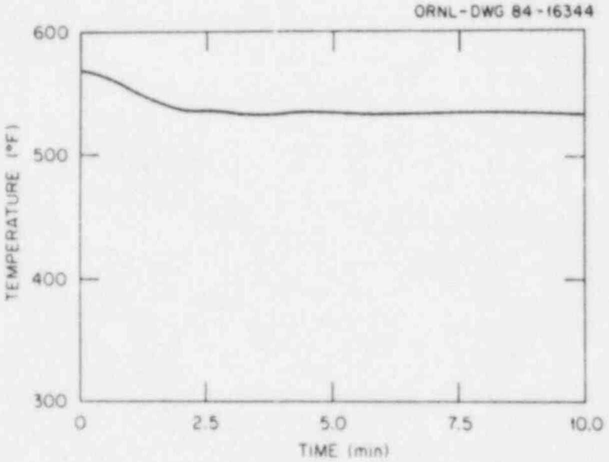


Fig. C.50. SG A outlet temperature: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

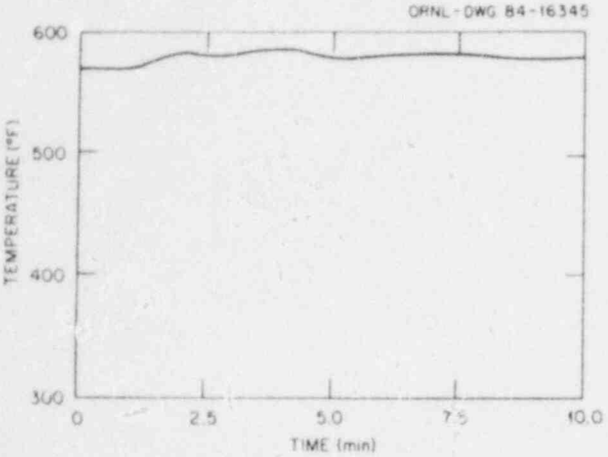


Fig. C.51. SG B outlet temperature: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

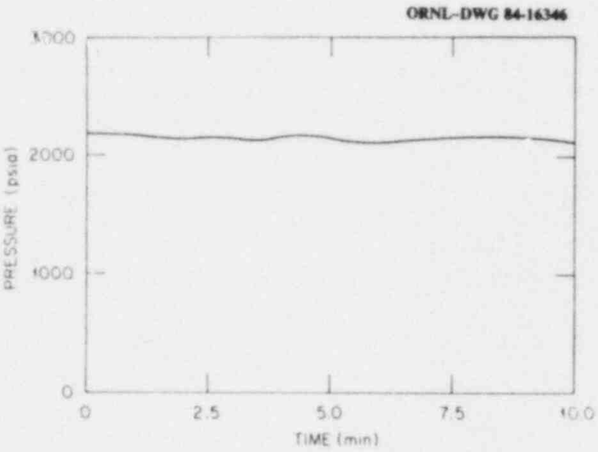


Fig. C.52. Pressurizer pressure: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

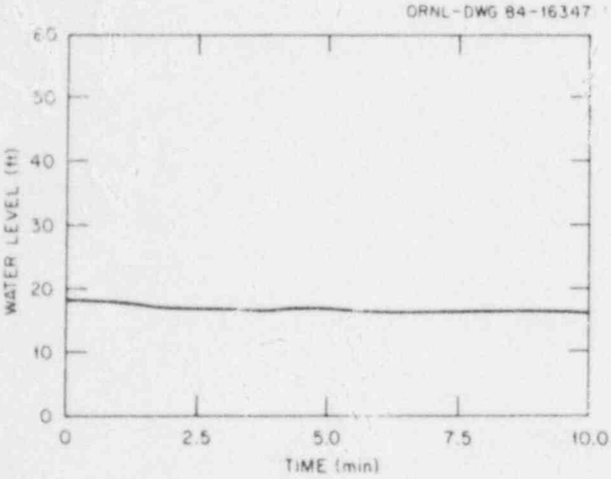


Fig. C.53. Pressurizer water level: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

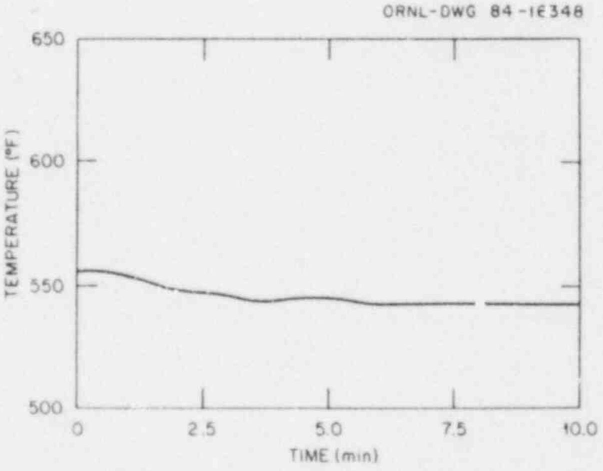


Fig. C.54. Loop A cold-leg temperature: overfill (Class 5) at 100% power. Overfeed with failed high-level control transfer and pump trip.

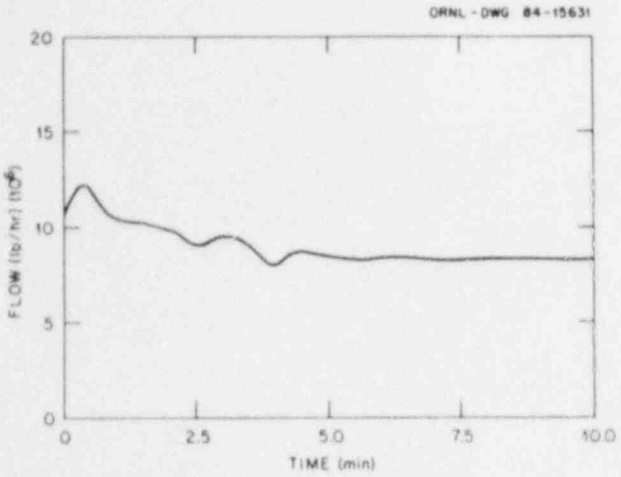


Fig. C.55. Total FW flow: overfill (Class 7). MFW blocking valve position indicator falsely indicated closed; flow reading taken the startup meter in Loop A.

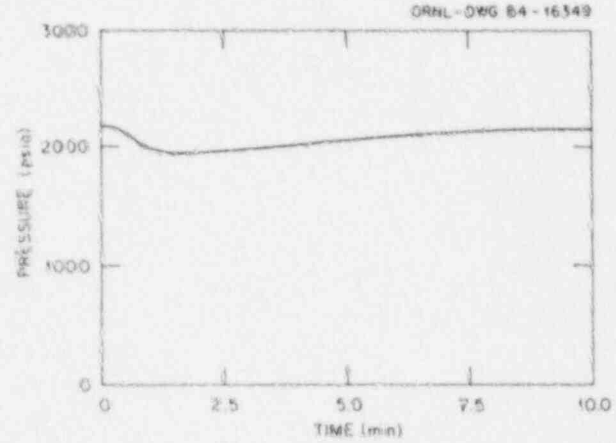


Fig. C.56. Pressurizer pressure: overfill (Class 7). MFW blocking valve position indicator falsely indicated closed; flow reading taken the startup meter in Loop A.

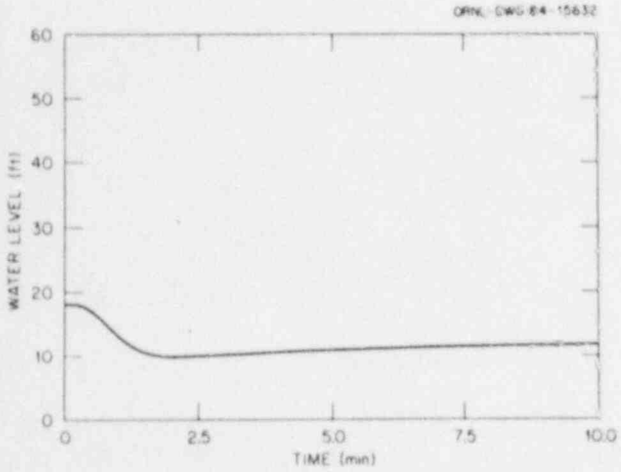


Fig. C.57. Pressurizer water level: overfill (Class 7). MFW blocking valve position indicator falsely indicated closed; flow reading taken the startup meter in Loop A.

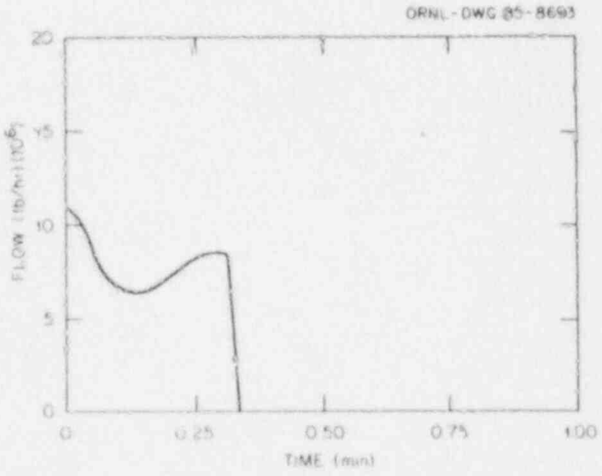


Fig. C.58. Total MFW flow: overfill (Class 8) at 100% power. Two-generator overfeed with turbine trip.

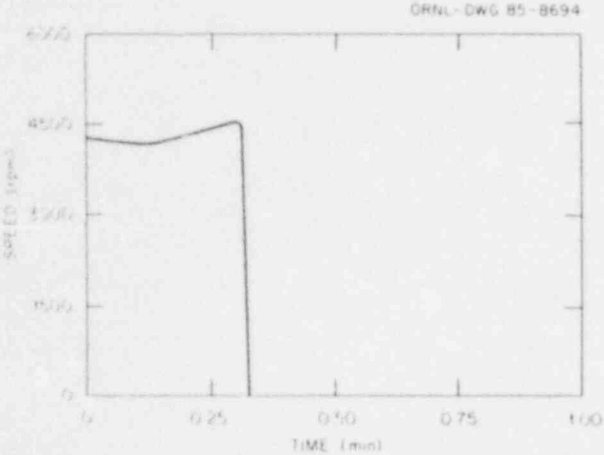


Fig. C.59. Main feedpump flow: overfill (Class 8) at 100% power. Two-generator overfeed with turbine trip.

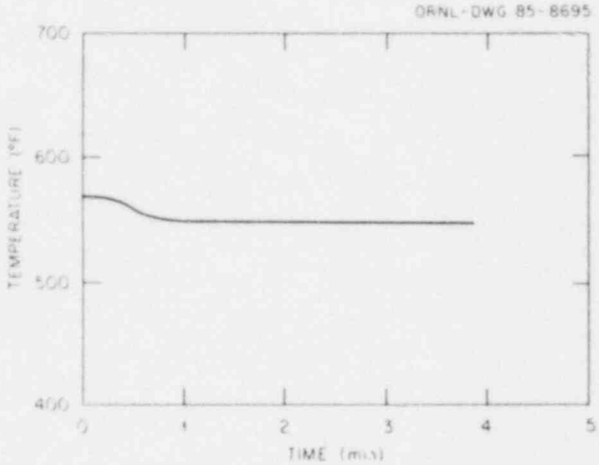


Fig. C.60. Core average coolant temperature as measured by sensors in Loop A: overfill (Class 8) at 50% power. One-generator overfeed with turbine trip.

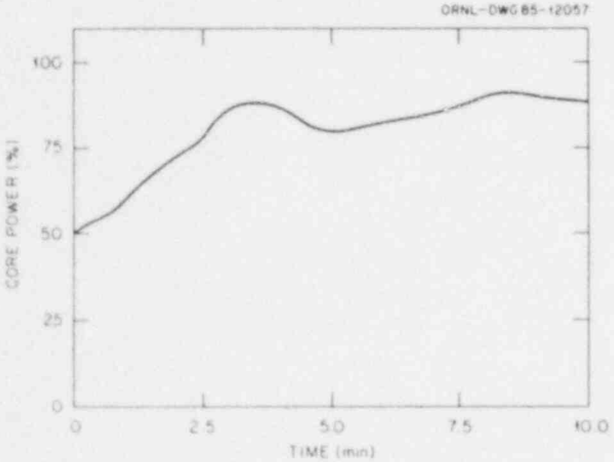


Fig. C.61. Core power fraction: overfill (Class 9); initial power 50%. Overfeed with MFW valve A 80% open.

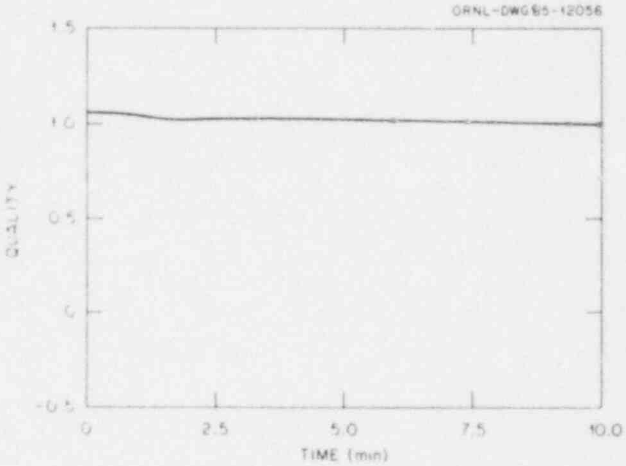


Fig. C.62. SG A outlet quality: overfill (Class 9). Overfeed with MFW valve A 80% open.

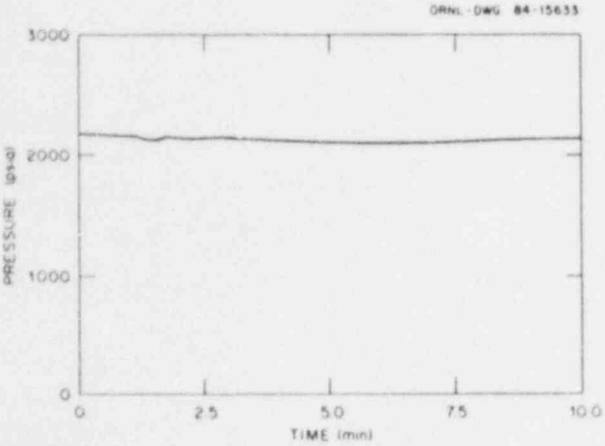


Fig. C.63. Pressurizer pressure: secondary side depressurization at 20% power.* Transient induced by partial steam line rupture or valves failing open in Loop A.

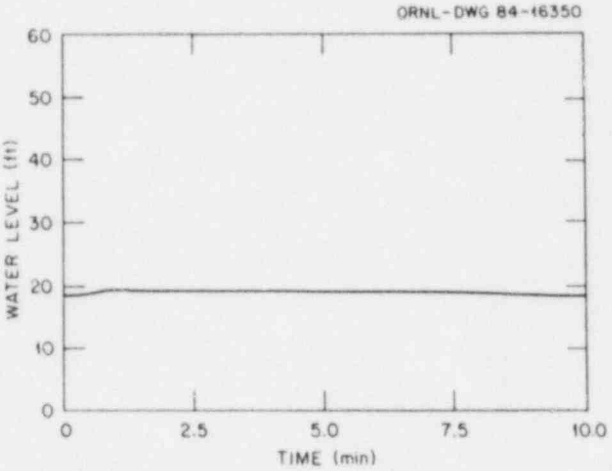


Fig. C.64. Pressurizer water level: secondary side depressurization at 20% power. Transient induced by partial steam line rupture or valves failing open in Loop A.

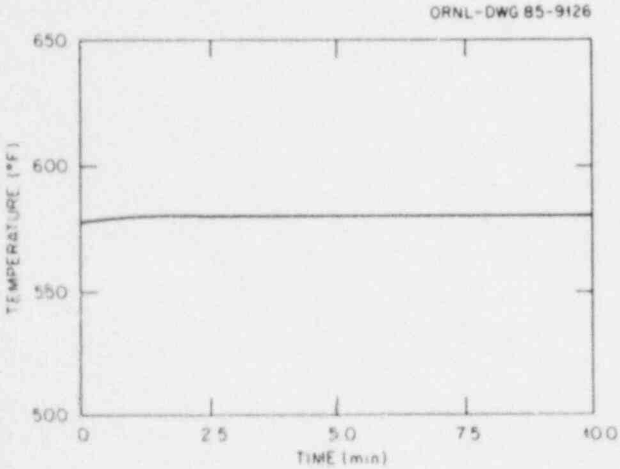


Fig. C.65. Core average coolant temperature at 20% power as measured by sensors in Loop A. Secondary side depressurization induced by partial steam line rupture or valves failing open in Loop A.

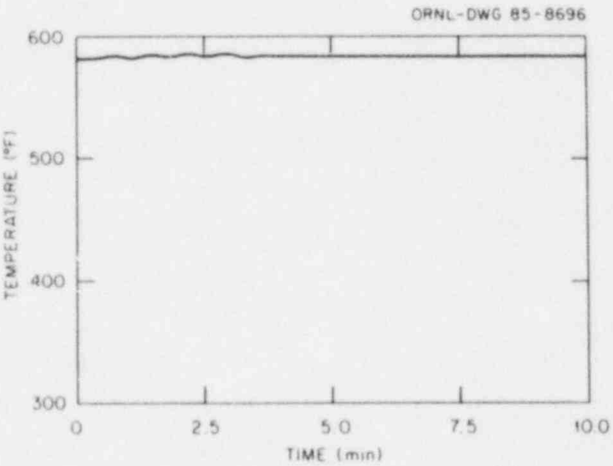


Fig. C.66. SG A outlet temperature: secondary side depressurization at 20% power. Transient induced by partial steam line rupture or valves failing open in Loop A.

*Failure classes are described in Sect. 4.6.

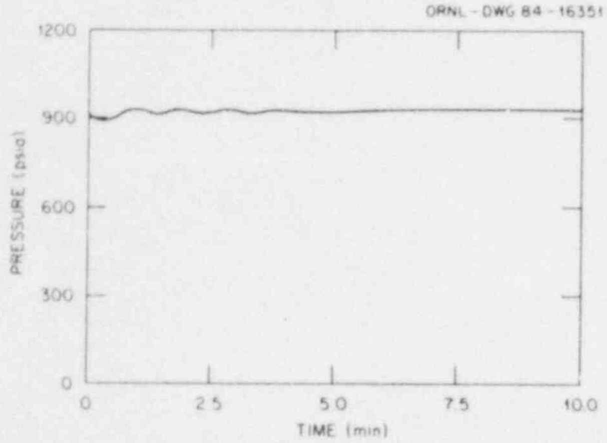


Fig. C.67. SG A outlet pressure: secondary side depressurization at 20% power. Transient induced by partial steam line rupture or valves failing oper in Loop A.

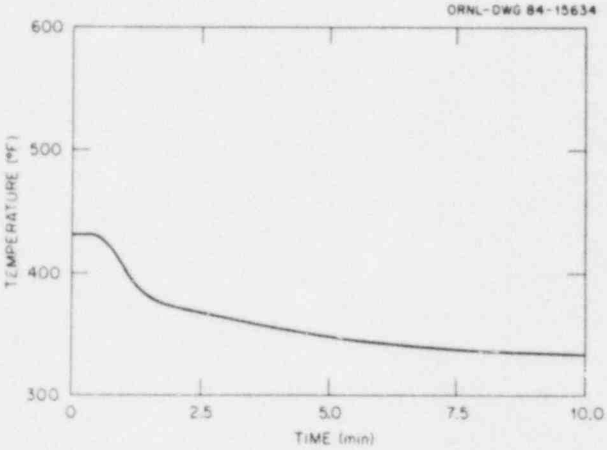


Fig. C.68. SG A FW temperature: secondary side depressurization at 100% power. Transient induced by partial steam line rupture or valves failing open in Loop A.

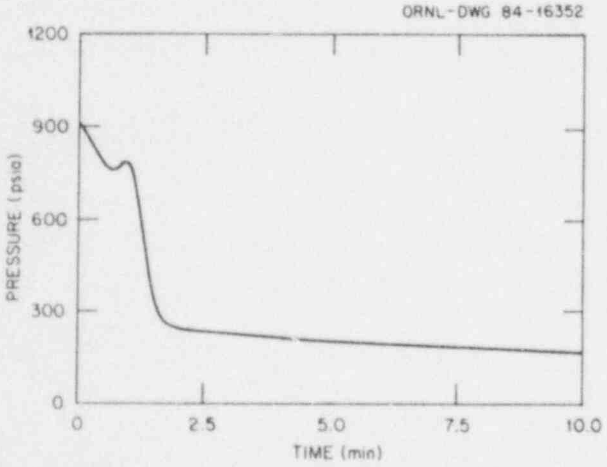


Fig. C.69. Steam line A pressure: secondary side depressurization at 100% power. Transient induced by partial steam line rupture or valves failing open in Loop A in combination with loop B.

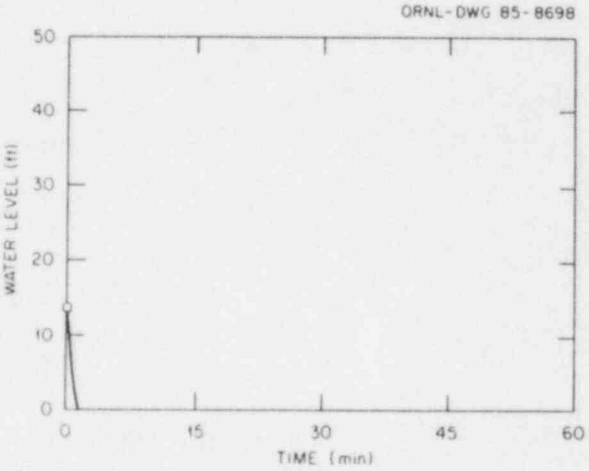


Fig. C.70. SG A water leve': overheating at 100% power.* Transient induced by loss of all FW to SGs.

*Failure classes are described in Sect. 4.7.

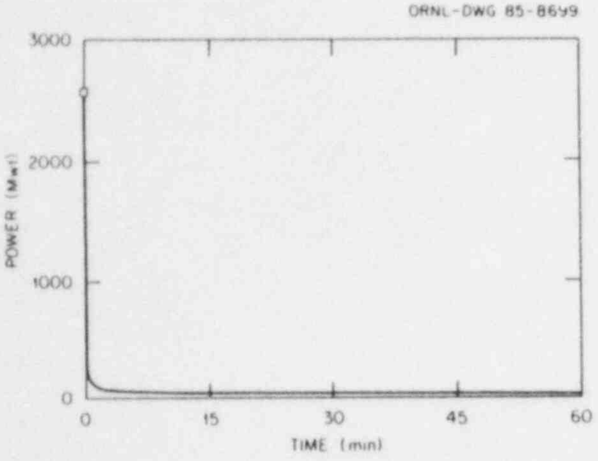


Fig. C.71. Core power: overheating at 100% power. Transient induced by loss of all FW to SGs.

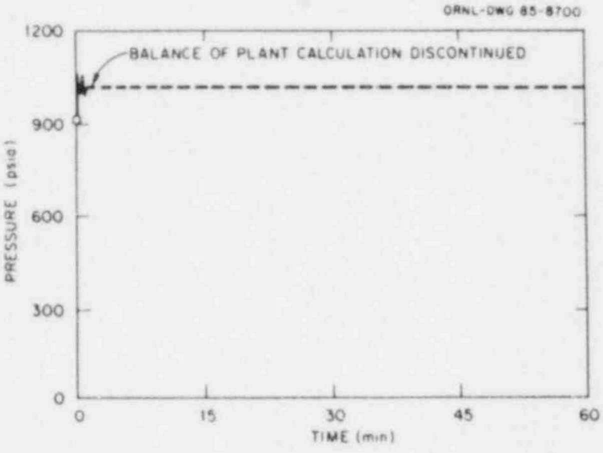


Fig. C.72. SG A pressure: overheating at 100% power. Transient induced by loss of all FW to SGs.

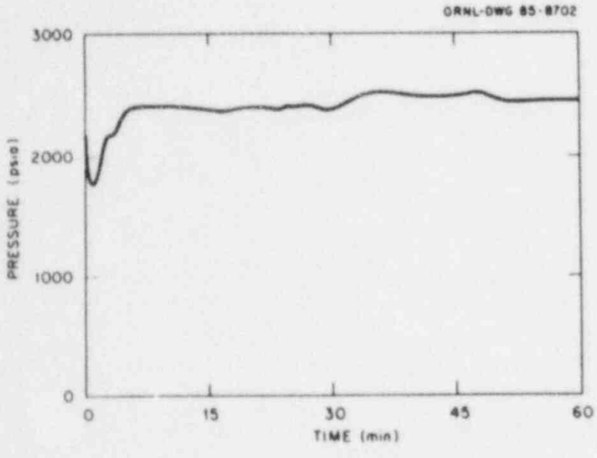


Fig. C.73. Pressurizer pressure: overheating at 100% power. Transient induced by loss of all FW to SGs.

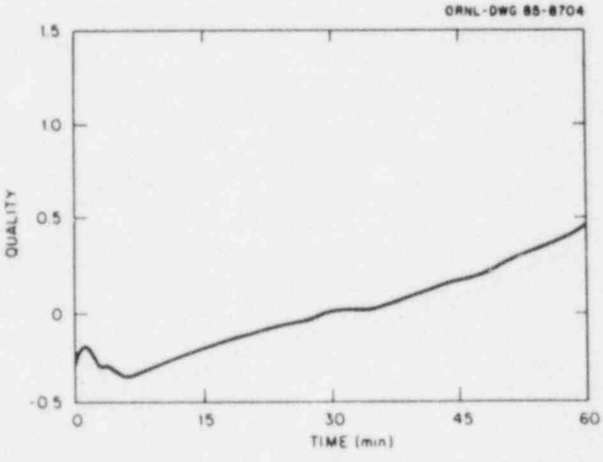


Fig. C.74. Upper core coolant quality: overheating at 100% power. Transient induced by loss of all FW to SGs.

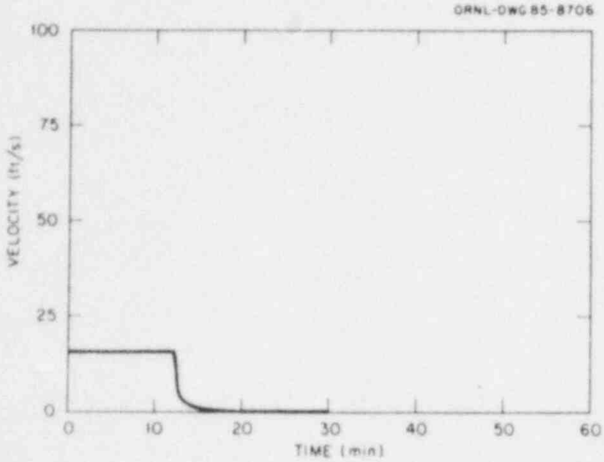


Fig. C.75. Core coolant flow: overheating at 100% power. Transient induced by loss of all FW to SGs. Primary pumps tripped on low subcooling margin.

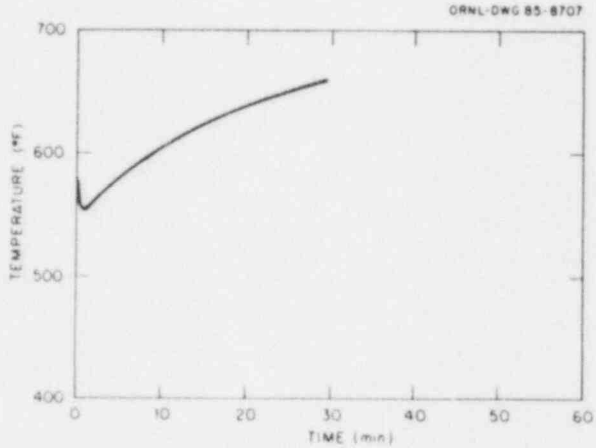


Fig. C.76. Core average coolant temperature: overheating at 100% power. Transient induced by loss of all FW to SGs. Primary pumps tripped on low subcooling margin.

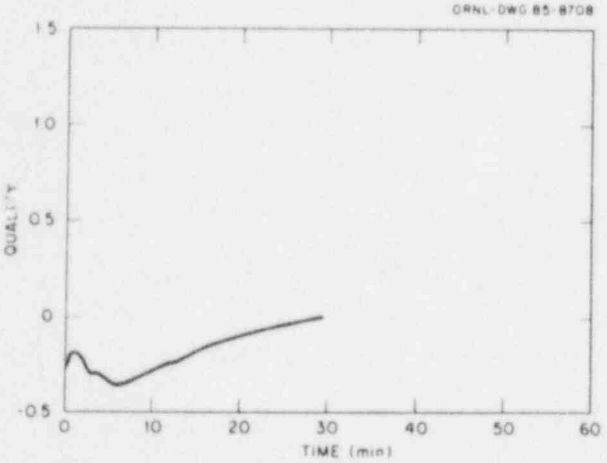


Fig. C.77. Upper core coolant quality: overheating at 100% power. Transient induced by loss of all FW to SGs. Primary pumps tripped on low subcooling margin.

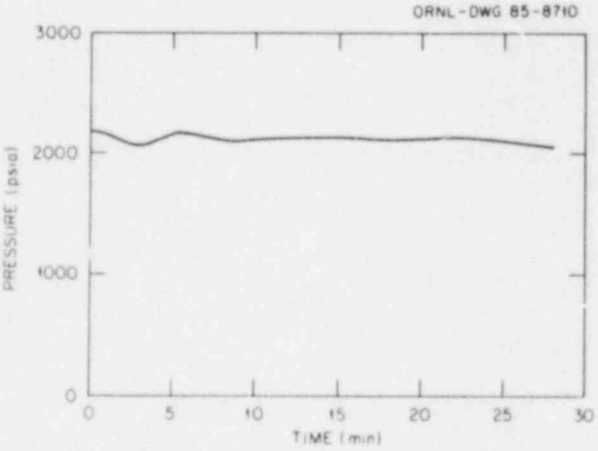


Fig. C.78. Pressurizer pressure: SG tube ruptures.* Overfill of SG A followed by partial rupture of one tube.

*Failure classes are described in Sect. 4.8.

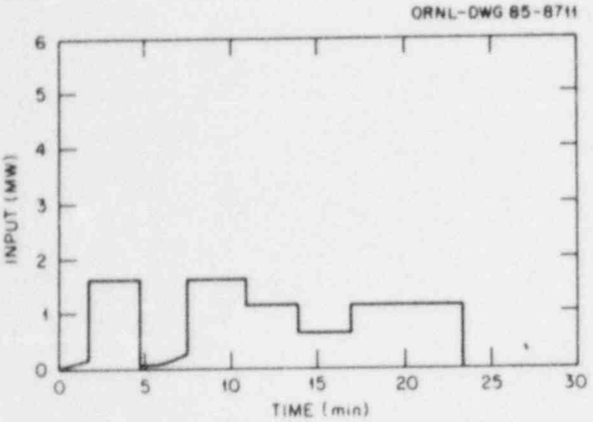


Fig. C.79. Pressurizer heaters input: SG tube ruptures. Overfill of SG A followed by partial rupture of one tube.

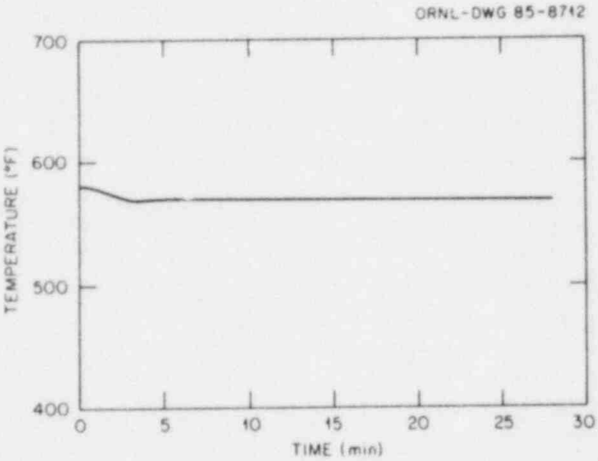


Fig. C.80. Core average coolant temperature as indicated by sensors in Loop A: SG tube ruptures. Overfill of SG A followed by partial rupture of one tube.

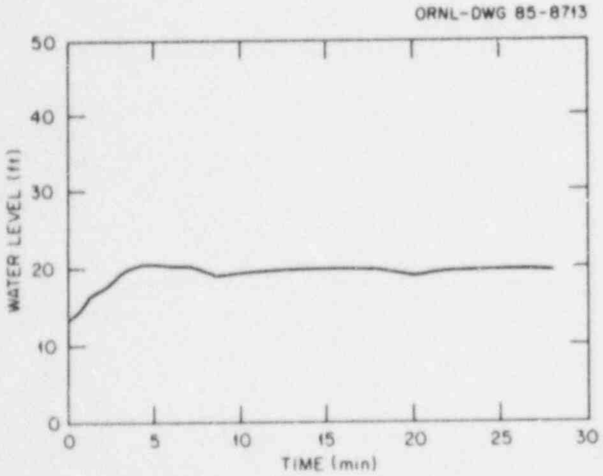


Fig. C.81. SG A water level: SG tube ruptures. Overfill of SG A followed by partial rupture of one tube.

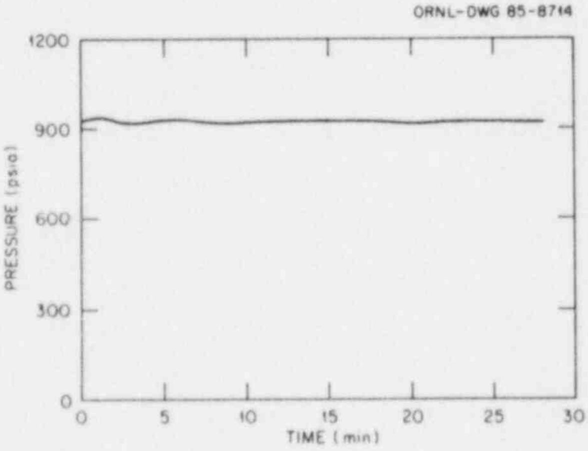


Fig. C.82. SG A pressure: SG tube ruptures. Overfill of SG A followed by partial rupture of one tube.

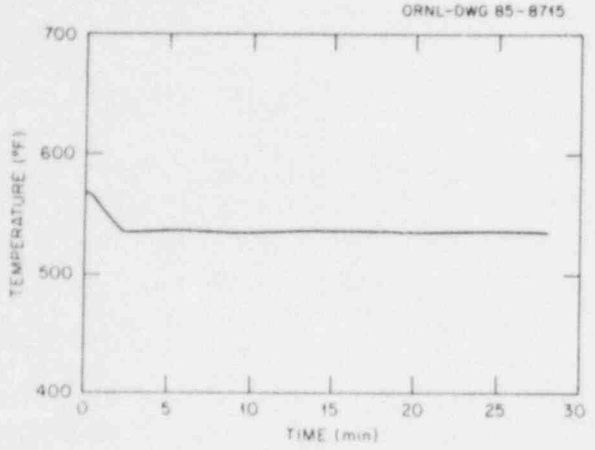


Fig. C.83. SG A outlet temperature: SG tube ruptures. Overfill of SG A followed by partial rupture of one tube.

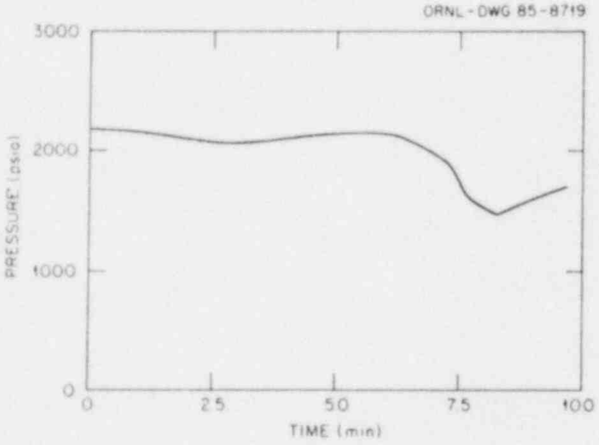


Fig. C.84. Pressurizer pressure: SG tube ruptures. Overfill of SG A followed by full rupture of three tube.

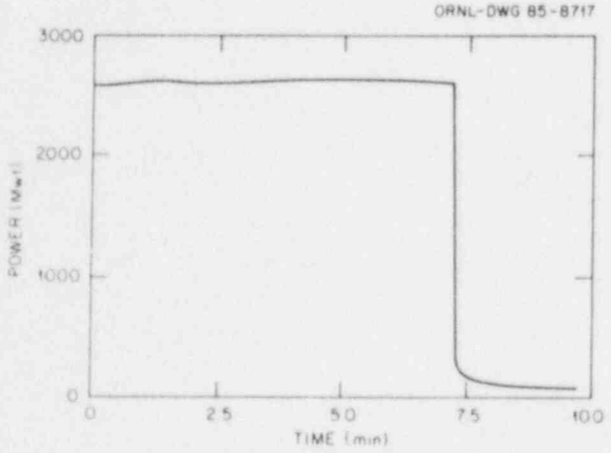


Fig. C.85. Core power: SG tube ruptures. Overfill of SG A followed by full rupture of three tubes.

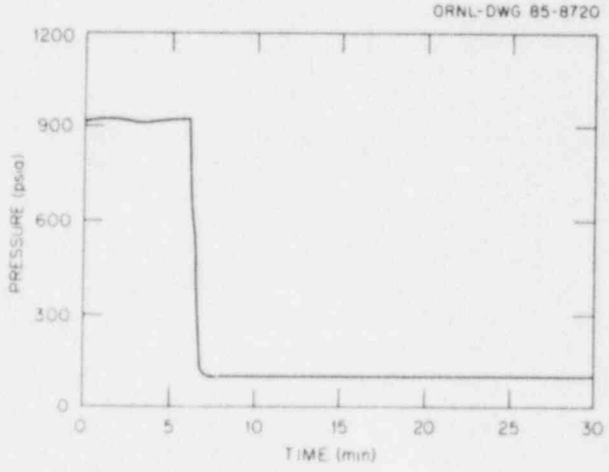


Fig. C.86. SG A pressure: SG tube ruptures. Overfill of SG A followed by full rupture of one tube and total steam line break.

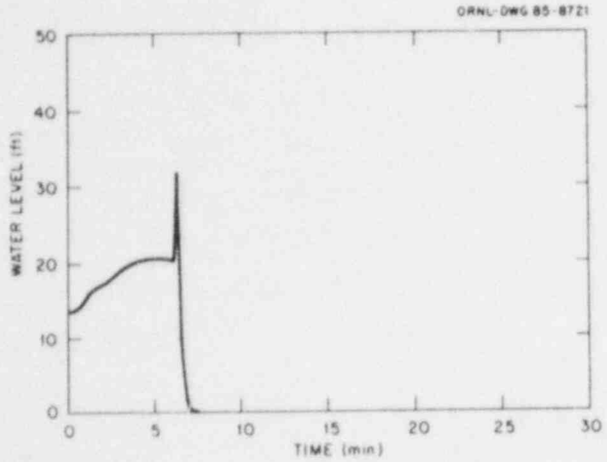


Fig. C.87. SG A water level: SG tube ruptures. Overfill of SG A followed by full rupture of one tube and total steam line break.

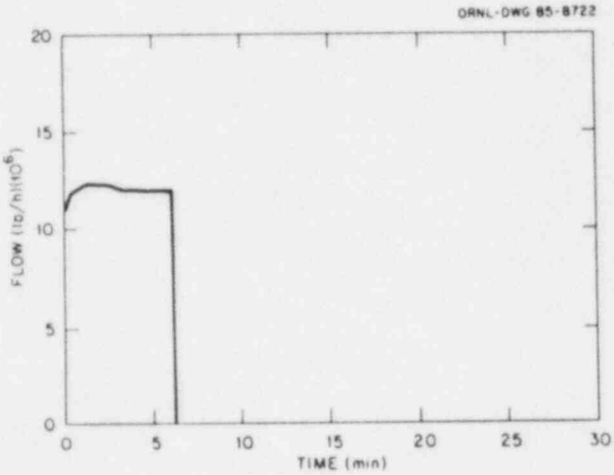


Fig. C.88. Total MFW flow: SG tube ruptures. Overfill of SG A followed by full rupture of one tube and total steam line break.

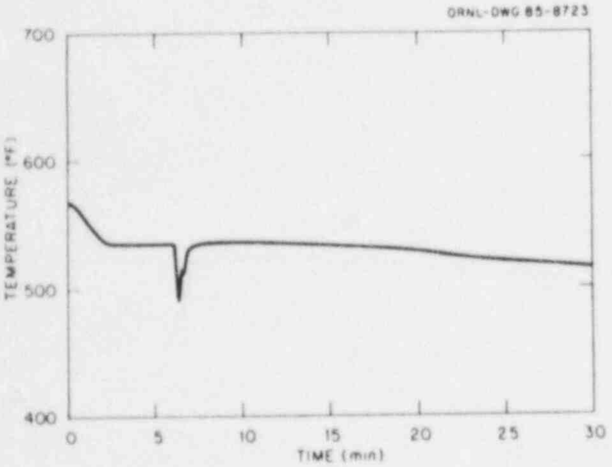


Fig. C.89. SG A outlet temperature: SG tube ruptures. Overfill of SG A followed by full rupture of one tube and total steam line break.

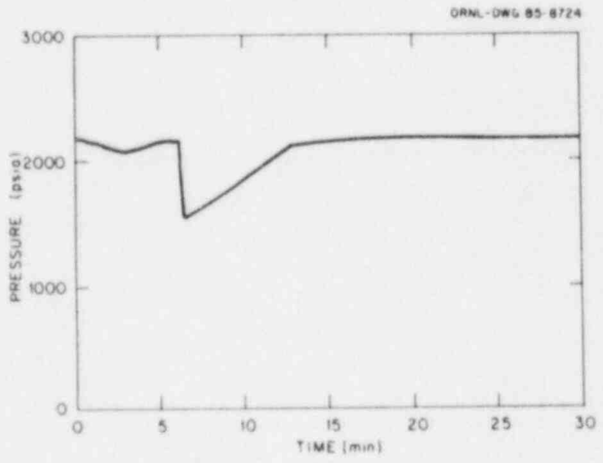


Fig. C.90. Pressurizer pressure: SG tube ruptures. Overfill of SG A followed by full rupture of one tube and total steam line break.

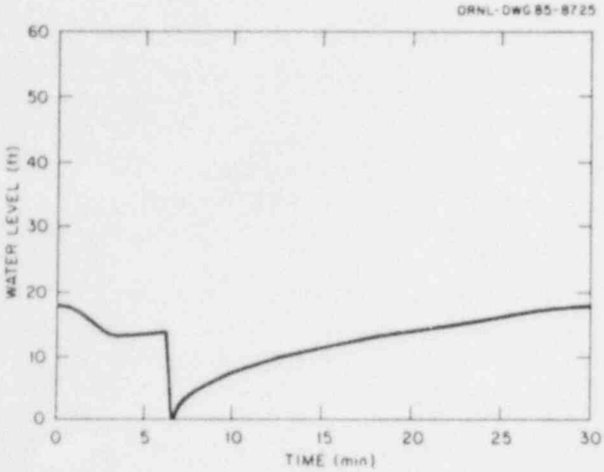


Fig. C.91. Pressurizer water level: SG tube ruptures. Overfill of SG A followed by full rupture of one tube and total steam line break.

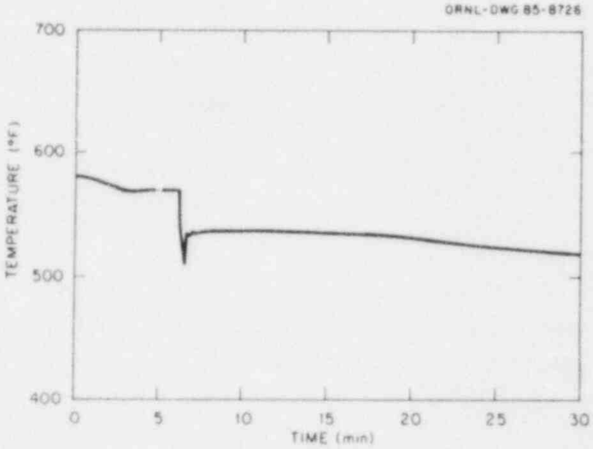


Fig. C.92. Core average coolant temperature as indicated by sensors in Loop A: SG tube rupture. Overfill of SG A followed by full rupture of one tube and total steam line break.

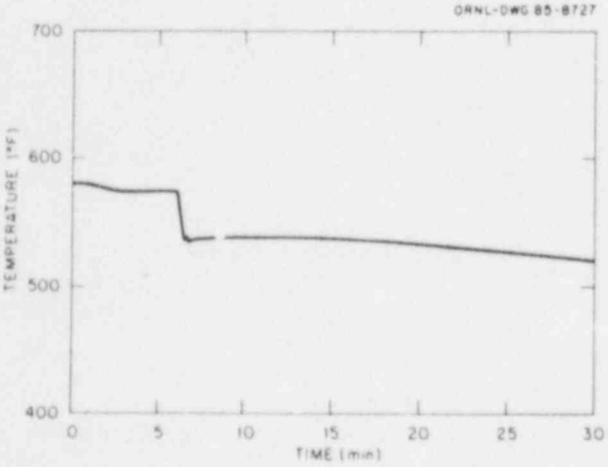


Fig. C.93. Core average coolant temperature as indicated by sensors in Loop B: SG tube rupture. Overfill of SG A followed by full rupture of one tube and total steam line break.

APPENDIX C REFERENCES

1. Analysis of Three Mile Island, Unit 2 Accident, NSAC-1, Nuclear Safety Analysis Center, Electric Power Research Institute, Palo Alto, July 1979.

2. Ireland, J. R., Comp., "TRAC Analysis of Severe Overcooling Transient for the Oconee-1 PWR," NUREG/CR-3706, Los Alamos National Laboratory, May 1985.

3. Bolander, M. A. et al., "RELAP5 Analysis of Oconee-1 Pressurized Water Reactor Transients for the Pressurized Thermal Shock Integration Study," EGG-NTAP-6190, Idaho National Engineering Laboratory, Idaho Falls, March 1983. Interim report.

4. Burns, T. J., "Pressurized Thermal Shock Evaluation of the Oconee-1 Nuclear Power Plant," NUREG/CR-3770, TM-9176 (Draft), Oak Ridge National Laboratory, April 1984.

APPENDIX D

Review of Draft Report by Duke Power Company

APPENDIX D

Review of Draft Report by Duke Power Company

A draft version of this report was sent to the licensee, Duke Power Company, for their comments. We found their response very useful, and a number of misconceptions were corrected. We are grateful for the obviously substantial effort expended by the licensee and have made use of the material supplied.

This report has been revised substantially since the early draft was reviewed by the licensee. The revisions have been so extensive that it is not always possible to make a section-by-section correspondence between the revised draft and the review comments. A number of comments in the review have been rendered moot by the revision. In keeping with current NRC policy, we reproduce here those parts of the licensee's response that resulted in revisions to the report.

Other licensee comments which were noted but not incorporated in the report include matters where more than one judgment is possible, situations with multiple possible outcomes dependent upon initial conditions, references to calculations or data not available to us, and comments on the proper limits of the study.

Specific comments referenced by page and paragraph follow.

Review of draft report by Duke Power Company

Draft Report Page/Paragraph	Duke Power Comments	Alterations to This Report
Executive Summary	Various objections to choices of language.	The executive summary has been entirely rewritten, rendering moot the suggestions made as to phraseology.
Executive Summary	Technical issues as detailed below.	The rewrite attempted to avoid any technical errors pointed out in Duke Power comments. See below.
p. XS-3	Overfill events which have occurred and caused extensive damage to the affected steam system should be identified and substantiated instead of alluded to. None of these events have happened at domestic B&W reactors.	Text did not intend to imply that the events occurred at Oconee or at any other domestic B&W plants. New reference is more specific. (Page viii)
p. XS-5, 2.3	The letdown storage tank (LDST) is well instrumented and alarmed to alert the operators to low levels. In addition, there is a nuclear station modification in progress which will automatically provide a suction source for the HPI pumps if the LDST empties.	The latter modification has been initiated since publication of the draft report. Its pending existence is acknowledged in the body of the new report.
Introduction		
p. 1-9, 1.5.3	"ESPS" is probably meant to be ESFAS.	ESFAS is a preferable term. Time may not permit hunting down and changing all the instances of "ESPS," which we originally adopted because it is the term used in Oconee's FSAR.
	Again, the pressurizer spray valve failing open and steam generator tube rupture events are not overcooling transients. Specifically, a stuck open spray valve is a depressurization transient which will be mitigated by operator action or Engineered Safeguards actuation. What was the basis for selecting a temperature drop of 100°F or more as a criterium for an overcooling event?	In the rewrite of this section, we have dropped this particular scenario. The 100°F was a PTS consideration.
p. 1-10, 1.5.4	There is an automatic actuation of the emergency feedwater upon detection of a low MFWP discharge pressure. (<750 psig on both pumps.) Therefore, if the MFW flow would cease without tripping tne MFWPs, the EFW would still be automatically started.	In general, we restrict this listing to comments that led to (or were coincident with) changes in our report. In this case, although no change was made, we believe an explanation is in order. Although everything in the comment is true, our simulation did not bring us even close to the 750-psig trip point.

Section 2

p. 2-28	The post-trip setpoint for the SG level is 25" not 30".	Accounted for where pertinent.
p. 2-30	Post-trip RCS temperature is 555°F not 547°F, and is determined by the post-trip secondary steam pressure of 1010 psig.	Accounted for where pertinent.
p. 2-34	The discussion of PTS relating to small break LOCAs should include mention of the mitigating effect of the reactor vessel vent valves.	Included.
p. 2-34 (also 3-96)	The statement is made in the last paragraph that a low vessel downcomer temperature will occur in the initial phase of a failed open PORV transient. This statement has no basis in fact. The A-49 work does not support this remark.	Lower temperatures do occur. However, no PTS conditions were threatened; the remark does not appear in the new edition.
p. 2-59	Atmospheric exhaust valves at Oconee are manually operated and are normally always closed, i.e., they are not used for steam generator pressure control after turbine trip.	Corrected.
p. 2-62	RC pumps require 6900 VAC, not 13800 VAC.	Corrected.
p. 3-21	The turbine bypass valves do have block isolation valves.	Noted.
	Atmospheric vent valves are not part of the ICS.	True. Removed from ICS outputs.
p. 3-45	Emergency feedwater is automatically actuated by only two signals: both MFW pumps tripped or low MFW pump discharge pressure.	Corrected.
	As we have repeatedly told Oak Ridge, the EFW pumps are not used during a startup.	Corrected.
	EFW is actuated by a safety grade 2/4 logic system. The EFW control system controls 25 inches level, but does not start the EFW pumps.	Corrections made.
	Low level is not an EFW actuation signal.	
	Loss of both MFWP also starts all EFW pumps.	

p. 3-59	Setpoints for LPI actuations are: 550 psig RC pressure or 3 psig RB pressure.	Corrections made.
	RB spray actuates on 10 psig RB pressure (not 4 psig).	
	LPI actuates at RCS pressure less than 500 psig or reactor building pressure greater than 4 psig. However, the shutoff head for the pumps is 150 psig.	
p. 3-67	The headline 3.2.7.3 "Failure Mode and Effects Analysis... Sprays System" is followed by no further text. Its meaning is not obvious. Same applies to the previous systems (HPI, LPI...) and to the Paragraph 3.2.8 (should this be 3.2.8.3?).	Fixed in final version.
p. 3-82	The minimum level controlled by the main feedwater as well as AFW is presently 25 inches, not 30 inches.	Correction made.
p. 3-82, 3.2.9	The MFW low level limit is 25 inches, not 30 inches.	Correction made.
p. 3-86 through 3-94	No information was given concerning the initial conditions assumed for the simulation runs. If 35°F superheat was assumed (based on BTU limit conditions) then this is a gross underestimation of the actual superheat obtained at Oconee. Between 15-100% load, Oconee's superheat consistently runs between 48-63°F. Starting with these superheat conditions could drastically change the simulation run results and thus the major conclusions of the report.	Simulations were run with altered conditions. Discussed in Section 4.9.
p. 3-104, 3.2.10.1.3	The first sentence of this section cites "...insufficient heat transfer rate across the steam generator tubes..." as an overcooling mechanism. Obviously this is wrong. Overcooling is a result of too much SG heat transfer.	Slip of the pen. Fixed.
p. 3-169	Appendix C was not found.	The material originally intended for Appendix C instead went into the body of the draft report. Appendices have been restructured.
p. 3-170 (also p. 5-2)	There is no steam quality trip at Oconee.	We originally got contradictory stories regarding quality trip. We take these comments as the final answer.
	Oconee has no steam quality turbine trip.	
	Figure 4.2.1, 4.2.2, etc., should be 4.5.1, 4.5.2, etc.	Figure numbers have been fixed.

Chapter 4	There are significant problems with the hybrid simulation model. The first problem is that no slip between the vapor and liquid phases is modeled in the steam generator secondary side. Realistically the steam will move faster than liquid water. Furthermore, the initial conditions are inconsistent with the Oconee-1 plant. Fig. 4.3.2 shows superheat beginning at more than 70% up the tube bundle. SG outlet temperature is only 570°F. Manufacturers information, borne out by plant data, indicates that superheat begins at about 55% up the tube bundle. The actual steam outlet temperature is about 595°F. The effect of these modeling deficiencies is to underpredict the steam outlet quality and therefore overpredict the amount of water in the steam lines during the transient simulations. Therefore, any conclusions based on the amount of water predicted to carry over into the steam lines by the hybrid model are not well grounded.	We saw no cases in our simulation of the generally phase-separated once-through steam generator in which treatment of slip would have been significant to our results. The question of these new initial conditions, however, was taken very seriously. We revised the model and made some additional runs. See Section 4.9 of the revised report.
p. 4-4	I. Core: It is not obvious from this description which method was selected for the simulation of the core.	Additional explanation added.
p. 4-5	More details on the SG simulation are desirable. The statement that B&W design characteristics were used for the initial model implies that a change is foreseen. What will be used in later models?	Additional information provided.
p. 4-8	Was the plant data from a "clean" steam generator? Operational experience shows that a significant increase in SG P can result due to deposits in the steam generator tube support plates, without significantly influencing other plant variables.	Data used were those provided by Duke Power Company. They were for a typical operating steam generator.
p. 4-13	It would be highly desirable to provide the comparison of the model with the cited Oconee-3 data.	Comparison made to turbine trip.
	The model should be benchmarked against some typical Oconee-1 transients, for which sufficient data base exists.	Duke Power responded negatively to our requests for these data.

p. 4-15	Does the model predict that the high level MFWP trip setpoint cannot be reached? This is not in agreement with Oconee data.	Nothing was done in response to this question, but as a point of information, saying MFWP trip set point cannot be reached is to strong a statement. The response depends on the specific transient. In the runs we made, trip-point was closely approached but never reached.
p. 4-33	The scale on the Y-axis seems to be in error by a factor of 10.	Yes. This has been corrected.
p. 5-12	"ESAS" is an unknown acronym. "ESFAS" is probably the correct term.	Changed.
p. B-6	The top sentence fragment makes no sense.	True. This has all been changed.
p. B-20	There is no automatic termination of MFW on low RCS pressure at Oconee.	Right. We have removed that statement.
General Comment	The comments contained in K. S. Canady's letter of 12/5/84 to R. S. Stone apply to the Executive Summary, which is essentially the same as the paper.	All of Mr. Canady's comments which have resulted in changes are covered in the page-specific remarks above.
	The recommended actions have not been analyzed for their potential negative effects, which could ultimately outweigh the positive.	True. Our recommendations are now less specific than in the original draft.

ADDITIONAL COMMENTS

General Comment	There are many typos and missing words and/or phrases. The report needs a good editing.	True. We hope the final edition is improved in this regard.
Section 2	The abbreviation for instrument air is 1A in Sect. 2.5.3 (Pneumatic System.) Why not IA which is the Oconee designation?	Fixed.
Sections 5.1 thru 5.4	The fault trees (FT's) contain several event names that use abbreviations whose meanings are not clear, e.g., "BAL (?) PMP (?) TRIP INST," "EITHER SG OR RG (?) LEVEL TRANS FAILS," EITHER MULT (?) MOD (?) FAILS," or "BAL (?) HI LEV. INT. (?) INST FAILED," or "ICS III (?) FW DEMAND." There should be a table included in this	Within space limitations we have tried to improve readability.

Sections 5.1 thru 5.4 (continued)	section of the report that defines the basic and undeveloped event names and provides an appropriate level of detailed information for each event. The amount of detail provided should be guided by the condition that a reader, knowledgeable of fault trees (FT's) and the ICS, being able to reconstruct the FT logic using only the information contained in the FT's and the suggested table.	
	The development of the values used in the quantification of the FT's needs to be supported by the specifics concerning the calculational methods used, assumptions made, and data sources consulted. Suggest that an appendix be included in the report to address the above need for specifics. The values used in the quantification of the FT's are very important in providing the perspective in which the safety concern raised by this report is viewed in context of overall plant safety. Therefore, these values deserve a high level of scrutability and traceability.	More information provided.
Section 5.4	It is not appropriate for a report of this stature to make such an off-handed comment like "both (a) and (b) would, of course, increase the likelihood of spurious pump trips."	We agree. We have pointed out some possible problems; specific remedies should be the responsibility of the concerned utility.
	The purpose of the report was to evaluate such non-safety related control effects on plant safety. However, appearing in the report is a final recommendation to make unevaluated circuit changes. These changes may create more safety implications than the present design.	

NUREG/CR-4047
ORNL/TM-9444
Distribution Category
R1, R4, RG, 12

INTERNAL DISTRIBUTION

1. S. J. Ball
2. R. E. Battle
3. R. S. Booth
4. N. E. Clapp, Jr.
5. F. H. Clark
6. W. G. Craddick
7. F. C. Difilippo
8. B. G. Eads
9. D. M. Eissenberg
10. E. W. Hagen
11. R. M. Harrington
12. A. P. Malinauskas
13. D. G. Morris
14. F. R. Mynatt
15. L. C. Oakes
16. J. P. Renier
17. D. L. Selby
18. O. L. Smith
19. A. Sozer
20-34. R. S. Stone
35. J. D. White
36. R. S. Wiltshire
37. M. J. Kopp (Advisor)
38. P. F. McCrea (Advisor)
39. H. M. Paynter (Advisor)
40. H. E. Trammell (Advisor)
41. Central Research Library
42. Y-12 Document Reference Section
43. I&C Publications Office
44. I&C IPC
45. Laboratory Records Department
46. Laboratory Records Department, RC
47. ORNL Patent Section

EXTERNAL DISTRIBUTION

48. Assistant Manager for Energy Research and Development, DOE-ORO, Oak Ridge, TN 37831
49. P. N. Austin, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
50-59. D. L. Basdekas, NRC Project Manager, U.S. Nuclear Regulatory Commission, 5650 Nicholson Lane, MS1130SS, Division of Engineering Technology, Washington, DC 20555
60-61. W. E. Bickford, Pacific Northwest Laboratories, Richland, WA 99352
62. D. P. Bozarth, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
63. R. P. Broadwater, Route 4, Box 11, Cookeville, TN 38501
64-69. S. J. Bruske, INEL, P.O. Box 1625, Idaho Falls, ID 83415
70. R. D. Dabbs, Technology for Energy, P.O. Box 15202, Knoxville, TN 37901
71. D. F. Sullivan, Elect. Eng. Branch, Division of Engineering Technology Office of RES, USNRC, Washington, DC 20555
72-75. Paul Guill, Nuclear Production Department, Duke Power Company, P.O. Box 33189, Charlotte, NC 28242.
76. R. A. Hedrick, Technology for Energy, P.O. Box 15202, Knoxville, TN 37901
77. L. L. Joyner, Joyner Engineers and Trainers, P.C., Route 2, Box 1072, Forest, VA 24551
78. W. E. Kastenberg, University of California at Los Angeles, 5532 Boelter Hall, School of Engineering and Applied Science, Los Angeles, CA 90024

79. R. Kubik, EPRI Nuclear Power Division, P.O. Box 10412,
Palo Alto, CA 94303

80. J. Lewin, 109 Albany Rd, Oak Ridge, TN 37830

81. C. L. Mason, Science Applications, Inc., 800 Oak Ridge
Turnpike, Oak Ridge, TN 37830

82. C. W. Mayo, Science Applications, Inc., 800 Oak Ridge
Turnpike, Oak Ridge, TN 37830

83. A. F. McBride, Science Applications International Corporation,
800 Oak Ridge Turnpike, Oak Ridge, TN 37830

84. F. J. Mustoe, PWR Systems and Safety Department, National
Nuclear Corporation Limited, Booths Hall, Chelford Road,
Knutsford, Cheshire, WA16 8QZ, England

85. Office of Scientific and Technical Information, Oak Ridge,
TN 37831

86. P. Pan, Los Alamos National Laboratory, MS K557, Los Alamos,
NM 87544

87. M. A. Shultz, Consultant, 124 Lakeshore Drive, Apt. 730,
N. Palm Beach, FL 33408

88. B. K. M. Sun, EPRI Nuclear Power Division, P.O. Box 10412,
Palo Alto, CA 94303

89-113. A. J. Szukiewicz, U.S. Nuclear Regulatory Commission,
Office of NRR, Washington, DC 20555

114-548. Given NRC Category distribution R1, R4, RG, and 12