

DESIGNATED ORIGINAL

JUN 20 1984

DMB

PDR

DRAFT

PRELIMINARY DRAFT

Instrumentation and Controls Division

**EVALUATION OF CONTROL SYSTEM FAILURES
LEADING TO REACTOR COOLANT SYSTEM OVERCOOLING
IN THE OCONEE-1 POWER PLANT**

Arthur F. McBride*

Manuscript Completed: April 24, 1984

*Science Applications, Inc., Oak Ridge, TN

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

NRC Fin No. B0467

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. W-7405-eng-26

PRELIMINARY DRAFT

8406270390 840424
PDR ADOCK 05000269
P PDR

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
LIST OF TABLES	iii
1.0 INTRODUCTION	1
1.1 Background	1
1.2 Objective and Approach	2
1.3 Scope	2
2.0 SUMMARY OF RESULTS	4
3.0 SELECTION OF SYSTEMS FOR ANALYSIS	14
3.1 Oconee 1 Systems List	14
3.2 Systems Affecting the Reactor Coolant System	15
3.3 Systems Affecting Reactor Coolant System Overcooling	26
4.0 SYSTEM DESCRIPTIONS	40
4.1 Nuclear Systems	40
4.2 Power Conversion Systems	50
4.3 Process Auxiliary Systems	58
5.0 FMEA OF SELECTED SYSTEMS	62
5.1 Nuclear Systems	63
5.2 Power Conversion Systems	74
5.3 Process Auxiliary Systems	90
6.0 REFERENCES	92
APPENDIX A - OCONEE 1 SYSTEMS NOT SELECTED FOR RCS OVERCOOLING ANALYSIS	A-1
APPENDIX B - OCONEE 1 POWER CONVERSION SYSTEMS PROCESS AND INSTRUMENT DIAGRAMS	B-1
APPENDIX C - OCONEE 1 POWER CONVERSION SYSTEMS FAILURE MODES AND EFFECTS ANALYSIS TABLES	C-1

LIST OF TABLES

<u>Table</u>		<u>Page</u>
2.1	Summary of Potentially Significant RCS Overcooling Failure Modes	6
3.1	Oconee 1 Nuclear Systems (Nxx)	16
3.2	Oconee 1 Engineered Safeguards Systems (Sxx)	17
3.3	Oconee 1 Reactor Building/Containment Systems (Cxx)	18
3.4	Oconee 1 Power Conversion Systems (Pxx)	19
3.5	Oconee 1 Process Auxiliary Systems (Wxx)	20
3.6	Oconee 1 Plant Auxiliary Systems (Xxx)	21
3.7	First Order Reactor Coolant System Interfaces	23
3.8	Second Order Reactor Coolant System Interfaces	24
3.9	Overcooling Characteristics and Potential Initiating Causes	27
3.10	Potential Impacts of First and Second Order Reactor Coolant System Interface Systems on RCS Overcooling	36
5.1	Summary of RCS Subsystem Failure Modes	64
5.2	Summary of Pressurizer System FMEA: Failures Leading to or Affecting RCS Overcooling Transients	65
5.3	FMEA of RC Pumps: Failures Leading to or Affecting RCS Overcooling Transients	71
5.4	FMEA of Steam Generators: Failures Leading to or Affecting RCS Overcooling Transients	72
5.5	Summary of Main Steam and Turbine Bypass FMEA: Failures Leading to or Affecting RCS Overcooling	75
5.6	Summary of Condensate and Main Feedwater FMEA: Failures Leading to or Affecting RCS Overcooling Transients	82
5.7	Summary of Makeup and Purification System FMEA: Failures Leading to or Affecting RCS Overcooling Transients	91

1.0 INTRODUCTION

1.1 BACKGROUND

The implications of failures of safety systems on nuclear power plant safety have been studied extensively. Currently, the safety implications of control system failures in nuclear power plants are being investigated by the Oak Ridge National Laboratory. A major task in this effort is the preparation of Failure Modes and Effects Analyses (FMEA) of plant systems to aid in the analysis of control system malfunctions and identification of possible consequences to safety. Specifically, the studies are directed at identifying failures and scenarios contributing to reactor coolant overcooling, reactor coolant undercooling, steam generator overfilling or degradation of the ability of safety systems to respond on demand.

This work is conducted for Nuclear Regulatory Commission (NRC) under FIN B0467, Safety Implications of Control Systems. It supports Unresolved Safety Issue A-47. The purpose of this analysis is to evaluate whether nuclear power plant control systems, either operating as designed or with postulated malfunctions, may interfere with the action of safety systems or may put the plant into a failed state beyond the protection of the safety systems. The effort at Oak Ridge National Laboratory (ORNL) is limited to the study of Babcock and Wilcox Co. and Combustion Engineering Co. Nuclear Steam Supply Systems (NSSS). NSSS's produced by other vendors are under study at INEL. The study is intended to be generic by vendors. However, it is recognized that, for a study of this sort, detailed and realistic plant design information is essential. Data from two operating plants were used to represent designs of the two vendors. The Oconee unit 1 and Calvert Cliffs unit 1 plant designs were selected to represent, respectively, Babcock and Wilcox and Combustion Engineering. Although the thrust of the study as a whole is generic, some elements of the study may be plant specific.

A number of other activities supported by NRC are related to this analysis or have provided information related to this work. Included among them are:

1. Plant Electrical System Evaluation, FIN B0816.
2. Evaluation of Pressurized Thermal Shock, FIN B0468.

3. Precursors to Potential Severe Core Damage Accidents, FIN B1583.
4. In Plant Reliability Data Base for Nuclear Plant Components, FIN B0445.
5. System Interactions in Nuclear Power Plants, FIN B0789.

The general approach to this problem at ORNL is twofold: the development of a hybrid computer model for simulation of the Oconee 1 Nuclear Power Plant, and a Failure Modes and Effects Analysis (FMEA) based principally on plant design and procedure information, to identify scenarios which may lead to control system initiated plant failures. The plant simulation will quantitatively predict the responses of the plant control systems to the identified scenarios. The simulation will examine in detail important cases generated in the FMEA. The simulation methodology and results will be described fully in other reports.

The FMEA, as it relates to the overcooling of the Reactor Coolant System (RCS), is the subject of this report.

1.2 OBJECTIVE AND APPROACH

The objective of this study is to identify control system failures which can contribute to reactor coolant overcooling. The approach to achieving this objective consists of three steps:

1. Identify those systems which have interfaces with the reactor coolant and can impact the overcooling transient.
2. Conduct a detailed FMEA of those systems to identify specific system malfunctions and consequences to safety.
3. Based on the identified failures, develop scenarios which could lead to the reactor coolant overcooling transients.

This approach and the results of its application to the Oconee 1 nuclear plant are presented in this report.

1.3 SCOPE

Although the objectives of the broad study are generic, specific nuclear power plant systems' designs are required for the preparation of a detailed FMEA.

For this reason, the FMEA is being performed on systems of the Oconee Nuclear Power Station selected as pertinent to overcooling transients. This report summarizes the results of previous FMEAs and documents the results for systems not previously analyzed.

The major results of the study are summarized in Section 2.0. Selection of systems for detailed analysis is discussed in Section 3.0. Brief system descriptions of the selected systems and interfacing support systems are described in Section 4.0. The FMEA methodology and analysis results are described in Section 5.0.

2.0 SUMMARY OF RESULTS

An analysis to identify control system failures leading to reactor coolant system (RCS) overcooling has been performed on the Oconee Nuclear Station design. Due to the large number of systems and components comprising a nuclear power station, a systematic procedure was developed to identify and analyze these plant systems:

1. Specifically define RCS overcooling for purposes of the analysis.
2. Identify the Oconee plant systems and system-to-system interfaces.
3. Select the systems which could contribute to RCS overcooling based on an analysis of systems' functions and interfaces.
4. Perform failure modes and effects analysis (FMEA) to identify component level failure modes leading to RCS overcooling.

The purpose of this analysis, as noted in Section 1, is the identification of plant control system failure modes that might lead to RCS overcooling. A number of failure modes have been identified (and are presented in Section 5) which could cause the RCS temperature to decrease. The rate and amount of such decreases and its possible subsequent effects cannot be determined without simulation of the system's response to the control system failures. RCS overcooling is not of interest in this study until it approaches an amount which can have safety implications. Cooling associated with normal shutdown procedures within Technical Specifications is of no concern.

Any condition that causes RCS temperature to drop 100°F or more in an hour is considered to be overcooling. Also, tentatively, RCS cooling to a degree that causes system variables to assume values that should cause ESPS actuation is considered overcooling.

Until plant behavior has been simulated, the proposed control system failures which meet these conditions cannot be determined. Therefore, additional less restrictive criteria have been followed in proposing failure sequences to ensure that potentially significant sequences would not be excluded prematurely. The selection criteria were accordingly expanded to include

transients whose post reactor trip development might include unusual decreases in RC pressure and inventory as well as temperature (see Section 3.3).

To aid in subsequent analyses, the overcooling criteria were related to RCS transient behavior characteristics. The analogous RCS characteristics defined were a release of reactor coolant from the RCS, opening the pressurizer spray valve and increased heat transfer through the steam generator tubes.

Based on the RCS overcooling criteria and the systems' function and interface analysis, a number of key plant systems and subsystems were selected for the FMEA. They were the pressurizer, steam generator and reactor coolant (RC) pump subsystems of the RCS; the condensate and main feedwater system, the main steam and turbine bypass system and the makeup and purification system. The control instrumentation and required supporting systems for these fluid systems were analyzed as an integral part of the fluid systems selected.

The results of the FMEA's of the selected systems are presented in detail in Tables 5.1 through 5.7. The failure modes judged to be potentially significant have been summarized in Table 2.1. The failure modes are listed by RCS overcooling category: Release of Reactor Coolant, Pressurizer Spray Valve Opens and Increased Heat Transfer Through Steam Generators. A fourth category has been added to identify failure modes resulting in multiple RCS overcooling effects.

As part of the FMEA's, potentially undetected failures which could increase the severity of the effects of the overcooling transients have been identified. The effects of significant undetected failures in combination with the initiating failures have been identified in Table 2.1.

Transients which lead to release of reactor coolant transient may be initiated by a failed open pilot operated relief valve (PORV), failure of an RC pump's seals and steam generator tube ruptures. Once identified, an open PORV may be isolated by manual closure of the PORV block valve. Tube rupture and seal failures cannot be isolated. Although these transients are not expected to result from any particular control system failure, each could result from a

TABLE 2.1. SUMMARY OF POTENTIALLY SIGNIFICANT RCS OVERCOOLING FAILURE MODES

Failure	Potential Effects on RCS	Remedial Actions Available
<u>Release of Reactor Coolant</u>		
<p>1. Pilot Operated Relief Valve (PORV) Fails Open or Fails to Close (Failure of a pressurizer code safety valve to close after opening initiates a similar transient)</p>	<p>Small Loss of Coolant Accident (LOCA). RCS pressure and temperature decrease in response to the loss of reactor coolant. Pressurizer fills. Automatic Engineered Safeguards System (ESPS) actuation of High Pressure Injection (HPI) at 1500 psi RCS pressure. The transient would be complicated by undetected failures of the PORV acoustic monitor or discharge line thermocouples. An undetected "low" failure of a selected operate range steam generator level transmitter would result in a steam generator overflow transient following the procedurally required RC pump trip unless manually terminated by the operator.</p>	<p>Follow emergency procedures for small LOCA. Identify the open PORV and close the PORV block valve. Reestablish RCS pressure, temperature and pressurizer level.</p>
<p>2. Failure of RC Pump Seals</p>	<p>Small LOCA. Pressurizer empties. Automatic Engineered Safeguards System (ESPS) actuation of High Pressure Injection (HPI) at 1500 psi RCS pressure. An undetected "low" failure of a selected operate range steam generator level transmitter would result in a steam generator overflow following the procedurally required RC pump trip unless manually terminated by the operator.</p>	<p>If possible, trip affected RC pump prior to seal failure and achieve cold shutdown. Once seal failure occurs, follow emergency procedures for small LOCA's.</p>

TABLE 2.1. SUMMARY OF POTENTIALLY SIGNIFICANT RCS OVERCOOLING FAILURE MODES (Continued)

Failure	Potential Effects on RCS	Remedial Actions Available
3. Steam Generator Tube Rupture	<p>Small LOCA. Pressurizer empties. Automatic ESPS actuation of HPI. Rapid cooldown and depressurization of RCS manually initiated to terminate release of reactor coolant to condenser and environment. An undetected "low" failure of a selected operate range steam generator level transmitter would result in a steam generator overflow transient following the procedurally required RC pump trip unless manually terminated by the operator.</p>	<p>Follow emergency procedures of a steam generator tube rupture.</p>
<u>Pressurizer Spray Valve Opens</u>		
4. Pressurizer Spray Valve Fails Open or Fails to Close	<p>Slow depressurization of RCS. Rate of depressurization limited by automatic actuation of pressurizer heaters. The transient would be complicated by an undetected failure of the pressurizer spray block valve.</p>	<p>Identify open valve and close spray block valve.</p>

TABLE 2.1. SUMMARY OF POTENTIALLY SIGNIFICANT RCS OVERCOOLING FAILURE MODES (Continued)

Failure	Potential Effects on RCS	Remedial Actions Available
<u>Increased Heat Transfer Through Steam Generators</u>		
5. Turbine Bypass Valves on Either Steam Generator Fail Open or Fail to Close (Failure of a main steam code safety valve to close following turbine trip initiates a similar transient)	Depending on the response of the turbine and reactor, an RCS cooldown and depressurization transient could occur following reactor trip. A failed "high" steam line pressure transmitter causing the transient could be confusing to the operator and delay remedial action. An undetected failure of the associated isolation valve may present isolation depending on the cause of the open turbine bypass valves. If the RC pumps were tripped in response to an ESPS signal, an undetected "low" failure of a selected operate range steam generator level transmitter would result in a steam generator overfill transient following the procedurally required RC pump trip unless manually terminated by the operator.	Identify the open valves and manually close the turbine bypass valves or their isolation valve.
6. Main Turbines Fail to Trip Following Reactor Trip	RCS cooldown and depressurization transient occurs. If the RC pumps were tripped in response to an ESPS signal, an undetected "low" failure of a selected operate range steam generator level transmitter would result in a steam generator overfill transient following the procedurally required RC pump trip unless manually terminated by the operator.	Attempt to manually trip or throttle the high or low pressure turbines. Throttle feedwater if required to control RCS depressurization.

TABLE 2.1. SUMMARY OF POTENTIALLY SIGNIFICANT RCS OVERCOOLING FAILURE MODES (Continued)

Failure	Potential Effects on RCS	Remedial Actions Available
<p>7. Main Feedwater Control Valves Fail Open or Fail to Close Following Reactor Trip</p>	<p>Following reactor trip, rapidly increasing steam generator level(s) expected to result in RCS cooldown and depressurization. Transient expected to be terminated by a manual or automatic trip of the main feedwater pumps. If the transient were initiated by a crack in the lower steam generator startup range level transmitter level tap, the emergency feedwater system would continue to fill the affected steam generator following main feedwater pump trip. An undetected failure of the automatic high level trip circuit would result in continued main feedwater overfill unless the pumps are manually tripped by the operator.</p>	<p>Identify the open valves and manually throttle or trip the main feedwater pumps.</p>
<p><u>Combined Effect Failures</u></p>		
<p>8. Pressurizer Pressure Circuit Fails High</p>	<p>PORV and spray valve open and pressurizer heaters deenergized. Transient expected to be similar to "PORV Fails Open," Transient 1, complicated by the indicated and alarmed high RCS pressure.</p>	<p>Identify spurious pressure signal and manually control PORV, spray valve and pressurizer heaters.</p>

TABLE 2.1. SUMMARY OF POTENTIALLY SIGNIFICANT RCS OVERCOOLING FAILURE MODES (Continued)

Failure	Potential Effects on RCS	Remedial Actions Available
9. ICS Panelboard KI Branch HEX or HEY Fail	Depending on manual selection of pressurizer level, steam generator startup level and steam pressure transmitters, one or both steam generators and the pressurizer may be overfilled. Steam generator overfill expected to be automatically terminated by a high level trip of the main feedwater pumps unless an undetected failure of the trip circuit existed. Pressurizer overfill can be manually terminated. Spurious low steam generator and pressure indications and alarms may delay manual remedial actions.	Identify power failure and manually control steam generator and pressurizer level. If required, manually trip main feedwater pumps.
10. ICS Panelboard KI Branch H or H1 (Auto Power) Fails Following a Turbine Trip Transient	Turbine bypass valves and main feedwater control valves transfer to manual and remain in position. Since both the turbine bypass and feedwater control valves may be open, a combined steam generator depressurization and overfeed transient could occur. Steam generator overfeed automatically terminated by a high level feedwater pump trip unless the trip circuit was in an undetected failed state. The many spurious alarms and indications may delay manual remedial actions.	Identify power failure and manually throttle feedwater control and turbine bypass valves. Manually trip main feedwater pumps if required.

sequence of improper control actions over a period of time. As such, they have been retained as examples of unisolable LOCA's.

The overcooling effects of a failed open pressurizer spray valve are not expected to be significant with respect to other failure categories. This failure has been retained as an example of this category of overcooling transient.

Failures resulting in increased steam generator heat transfer fell into two sub-categories: those initiating steam generator depressurization and those initiating steam generator main feedwater overfeed. Steam generator depressurization is expected, following reactor trip, due to the turbine bypass valves failing open or a failure of the main turbine to trip on demand. With the exception of a postulated failure of one common setpoint module, the failures affecting the turbine bypass valves resulted only in the steam generator A or steam generator B turbine bypass valves failing open but not both. An open failure of one of the two sets of valves could result in a consequential reactor and turbine trip. However, defining the specific effects of these failures will require transient simulation. Once the reactor is tripped, however, RCS overcooling is expected unless the steam generator depressurization is terminated manually.

Failure to trip the turbine following reactor trip has been identified as a transient resulting in steam generator depressurization. However, due to the unavailability of turbine control instrumentation design, specific turbine trip failure modes could not be identified in detail. Failure of the reactor trip input signal was identified and could result in some degree of RCS overcooling; the specific response of the turbine controls to this failure in conjunction with other ICS control inputs could not be specified. The turbine trip failure has been retained as an example of a potentially large steam generator depressurization transient induced by control failures.

One or both main feedwater control valves failing open or failing to close will result in steam generator overfill and potentially significant RCS overcooling following reactor trip. The specific effect of a feedwater control valve opening while the reactor is at power will require transient

simulation. (For instance, if the high steam generator feedwater pump trip occurred prior to reactor trip, RCS overcooling would not be expected.)

The steam generator overfill transients are expected to be automatically terminated by the high steam generator level main feedwater pump trip circuit. Two failure modes have been identified resulting in continued overfeed. If the steam generator startup level transmitter sensing line developed a significant crack, the spurious low transmitter level signal would initiate steam generator overfeed. If the feedwater pumps were tripped on high steam generator (operate range) level, the emergency feedwater system would be automatically started. Since the main feedwater and emergency feedwater level transmitter have a common sensing line, the overfill would be continued by the spurious low level signal to the emergency feedwater controls.

The second failure mode involves a failure of the high level main feedwater pump trip circuit. Should this circuit fail, no immediate impact on plant operation may occur and the failure may remain undetected. In this state, an overfeed transient initiated by a feedwater control valve failing open or failing to close would not be automatically terminated. If the steam generator was allowed to fill, the injection of significant quantities of water into the steam lines could result in damage to the safety valves, the turbine bypass valves, the steam lines, and their supports in addition to initial RCS overcooling.

Three failure modes were identified which resulted in more than one effect on the RCS. Failure of the RCS narrow range pressure signal would result in both the PORV and spray valves opening and deenergizing the pressurizer heaters. The differences between this transient and the effects of the open PORV alone are not expected to be significant.

Two failure modes resulting from failures of ICS Panelboard KI branch circuits have been identified as having multiple effects. The redundant pressurizer level, steam generator level and steam pressure transmitters are powered from branch circuits HEX and HEY. One of the redundant transmitters is selected manually for each parameter for input to the control circuitry. Based on the transmitter selection, a single failure of branch circuit HEX or HEY may

result in overfeeding the pressurizer and either or both steam generators. If selected, the possibly deenergized steam pressure transmitters would result in the turbine bypass valves closing and remaining closed challenging the main steam safety valves.

Failure of branch circuit H or H1 (ICS Auto Power) results in transferring many ICS controls stations to manual and freezing the controlled components in position including the turbine bypass valves and main feedwater control valves. If the auto power failure occurred followed by a reactor trip, a steam generator overfeed transient would occur with the turbine bypass valves remaining closed. However, if the auto power were to fail following a turbine trip (possibly in response to the same initiating failure), both the turbine bypass and feedwater control valves may be held open resulting in a combined steam generator overfeed and steam generator depressurization transient. Although this sequence appears unlikely, similar sequenced power failures have occurred.

3.0 SELECTION OF SYSTEMS FOR ANALYSIS

The objective of this work, as discussed in Section 1.0, is to conduct detailed FMEAs on systems having a major impact on overcooling. The method of achieving this objective consists of three steps:

1. Identify the Oconee 1 systems and functional interfaces.
2. Identify those systems which have a potential impact on the overcooling transient.
3. Conduct a detailed FMEA of the systems identified in (2) above.

The impact of most plant systems on an overcooling transient is minor. Thus, the purpose of a plant specific system list with clearly identified interfaces is to aid in the selection of only those systems having a potential impact on overcooling. Due to the large number of systems and components in a nuclear power plant, this preliminary screening is necessary to determine which systems require detailed analysis since it is not possible to make an in-depth study of all of them.

An overcooling transient is defined, for purposes of this report, as a transient resulting in a significant decrease in reactor coolant temperature following reactor trip. The criteria for the overcooling transients are discussed in Section 3.3. Since the response of reactor coolant system to postulated initiating transients is integral to any overcooling transient, it was concluded that, as a first screening criterion, any system having a direct interface with the reactor coolant system would be a candidate for further analysis. Other criteria for the final selection are discussed in Section 3.2 and 3.3.

3.1 OCONEE 1 SYSTEMS LIST

Based on the previously developed generic list of pressurized water reactor systems list (Reference 1) and the Oconee Unit 1 Final Safety Analysis Report (FSAR) (Reference 2), an Oconee systems list was developed to identify all systems which might contribute to overcooling transients. The systems and their associated subsystems are grouped according to six major functions:

1. Nuclear Systems include the reactor core and those systems and subsystems which monitor and control core reactivity, remove

heat from the core, and otherwise directly support the safe operation of the reactor.

2. Engineered Safeguards Systems include those systems, other than containment systems, which are used to mitigate the effects of reactor accidents such as those specified in the FSAR.
3. Containment Systems include the reactor building and those systems needed to prevent reactor building overpressure, to prevent excessive leakage from the reactor building to the environment, and to provide a habitable atmosphere inside the reactor building.
4. Power Conversion Systems include the systems and components that transform, or support the transformation of, heat energy produced by the reactor core into electrical energy.
5. Process Auxiliary Systems include those systems and subsystems that support the plant systems directly involved in the operation of the reactor coolant systems.
6. Plant Auxiliary Systems provide support to other plant activities and personnel.

The systems included in each grouping are shown in Tables 3.1 - 3.6. A system identification was assigned to each system in order to simplify the subsequent interface analysis. Note that electrical systems have not been included; the effects of electrical system failures on the plant are being analyzed separately from this study (References 3 and 4).

After the systems lists were generated, specific interfaces were identified, based on the system descriptions in Reference 2. Interfaces were identified for every system and include the direction (e.g., System A affects System B only, System A affects System B and System B affects System A, etc.) as well as interfacing system identification.

3.2 SYSTEMS AFFECTING OVERCOOLING

Based on the systems lists and interfaces, specific systems were identified as having a potential impact on overcooling transients. The selection criteria used are not specific to overcooling transients; systems potentially affecting

TABLE 3.1. OCONEE 1 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 Systems
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 3.2. OCONEE 1 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 3.3. OCONEE 1 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 3.4. OCONEE 1 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 3.5. OCONEE 1 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 3.6. OCONEE 1 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

reactor coolant system transients, in general, are selected. The following criteria were used to identify these systems:

1. All systems having a direct (first order) interface with the reactor coolant system (including the pressurizer and the steam generator) were listed. These systems are shown in Table 3.7.
2. From this list, several systems were eliminated for reasons described below and shown in Table 3.7:
 - (1) Only non-safety qualified control systems have been selected. Safety systems were not included because these systems are being analyzed in detail under separate NRC programs (Reference 5).
 - (2) Only those systems in operation or standby during normal plant power operation were included. Systems such as those required for refueling or shutdown decay heat removal thus were not included. These systems are manually placed in operation only after a controlled shutdown of the reactor coolant system to less than 300°F and less than 300 psi.
 - (3) Only those systems directly affecting reactor coolant system response were selected. Those interfacing systems affected by but not affecting reactor coolant system response were eliminated. (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 Table 3.7 were identified. This list of second order interfacing systems, excluding those also selected in Table 3.7, is shown in Table 3.8.

The list of systems initially selected for analysis includes all control systems which potentially affect reactor coolant system response during plant transients and all systems which potentially affect the response of these first order systems. The specific impact of these systems on reactor coolant system overcooling are evaluated in this report.

TABLE 3.7. FIRST ORDER REACTOR COOLANT SYSTEM INTERFACES

System ID	Oconee System Name	Direction*	Criteria for Elimination
N01	Reactor Core	2	--
N02	Regulation Systems	3	--
N03	Incore Monitoring	1	Interface is away from RCS
N04	Reactor Coolant System	-	Included
N05	Makeup and Purification	3	--
N06	Low Pressure Injection	3	Operates during shutdown only
N07	Reactor Protective	1	Safety system
N08	Nuclear Instrumentation	1	Interface is away from RCS
SXX	Engineered Safeguards Systems	1	Safety systems
C01	Reactor Building/Containment and Penetrations	3	Safety system
C02	Reactor Building Hydrogen Purge	1	Interface is away from RCS
C03	Reactor Building Ventilation	2	--
P01	Main Steam and Turbine Bypass	3	--
P04	Condensate and Feedwater	2	--
W01	Radioactive Waste System	1	Interface is away from RCS
W03	Reactor Building Component Cooling Water	3	--
W05.D	Fuel Handling	3	Operates during shutdown only

*1 = Interface from reactor coolant to interfacing system.

2 = Interface to reactor coolant from interfacing system.

3 = Interface to and from reactor coolant.

TABLE 3.8. SECOND ORDER REACTOR COOLANT SYSTEM INTERFACES

First Order System ID	Second Order System ID	System Name	Direction*	Criteria for Elimination
N01	N04	Reactor Coolant	3	--
	N03	Incore Monitoring System	1	Interface is away from Reactor Core
N02.A	N02.B	Integrated Control	2	--
N02.C	S04	Core Flood	2	Safety system
	C01	Reactor Building	2	Safety system
	W01	Radioactive Waste	2	--
N05	W04.C	Low Pressure Service Water	3	Safety system
	W07.B	Instrument Air System	2	--
C03	S07	Reactor Building Penetration Room Ventilation	3	Safety system
	S08	Reactor Building Isolation	3	Safety system
	X05.E	Reactor Building Cooling	3	--
P01	N02.B	Integrated Control	2	--
	P02	Turbine-Generator System	3	--
	P06	Auxiliary Steam System	3	Operates during shutdown only
P04	N02.B	Integrated Control	2	--
	P03	Main Condenser	3	--
	P04.A	Condensate Cleanup System	3	--
	W07.B	Instrument Air System	3	--
W03	W04.C	Low Pressure Service Water (LPSW) System	3	Safety System

TABLE 3.8. (Continued)

First Order System ID	Second Order System ID	System Name	Direction*	Criteria for Elimination
W04.D	N05.D	Post Accident Sampling	3	Operates during shutdown only
	W04.A	Condenser Circulating Water	2	--
	W05.C	Spent Fuel Pool Cooling	3	Operates during shutdown only

*1 = Interface from first order system to second order system.

2 = Interface to first order system from second order system.

3 = Interface to and from first order system.

Note: Interfaces with direction = 1 have not been included.

To ensure completeness and to verify the adequacy of the selection procedure, each of the systems eliminated were briefly evaluated again to assess their potential impact on reactor coolant system overcooling. The eliminated systems and the results of the reevaluation are presented in Appendix A.

3.3 SYSTEMS AFFECTING REACTOR COOLANT SYSTEM OVERCOOLING

In Section 3.2, the systems which potentially affect the response of the Reactor Coolant System (RCS) have been identified. Of these systems, those potentially affecting RCS overcooling are identified. Section 3.3.1 presents the definition of RCS overcooling for purposes of this analysis. In Section 3.3.2, the functions of the systems identified in Tables 3.7 and 3.8 are evaluated to identify those systems potential affecting RCS overcooling as defined.

3.3.1 Definition of Significant RCS Overcooling

RCS overcooling may be defined, in general, as a decrease in the RCS average temperature. For purposes of this analysis, however, the definition of overcooling should focus on the overcooling transients of potential significance. Two basic criteria are proposed to define significant overcooling for the purposes of systems selection and failure modes analyses:

1. Transients terminated by reactor trip and automatically established stable conditions of post-trip RCS pressure, temperature and reactor coolant inventory should be excluded.
2. Transients exhibiting the potential for continued post-trip decreases of RCS pressure, temperature or reactor coolant inventory should be included.

These criteria define transients of potential significance to RCS overcooling. Transient conditions defined by these criteria and subsequent failure mode analyses will be analyzed using the Oconee hybrid computer model to predict the resulting RCS response and the impact on plant safety.

An RCS overcooling transient, as defined above, is characterized by continuously decreasing RCS temperature, pressure or inventory following reactor trip. These defined overcooling characteristics are interrelated significantly as shown in Table 3.9.

TABLE 3.9. OVERCOOLING CHARACTERISTICS AND POTENTIAL INITIATING CAUSES

Overcooling Characteristic	Principal Causes	Secondary Causes	
1. Decrease in RCS Temperature	1.1 Net Heat Transfer From RCS	1.1.1 Increased Heat Transfer Through Steam Generator Tubes	
		1.1.2 Release of Reactor Coolant From the RCS	
2. Decrease in RCS Pressure	2.1 Decrease in Pressurizer Temperature	2.1.1 Increase in Pressurizer Spray Flowrate	
		2.1.2 Release of Steam (Reactor Coolant) From the Pressurizer	
	2.2 Decrease in Pressurizer Level	2.2.1 Release of Reactor Coolant From the RCS	
		2.2.2 Decrease in RCS Temperature	
	2.3 Release of Reactor Coolant From the RCS	2.3.1 PORV Opens and Remains Open	
		2.3.2 Pressurizer Safety Valve Opens and Remains Open	
		2.3.3 Net Release of Reactor Coolant From the RCS to the MU&P System	
		2.3.4 RC Pump Seal Failure Occurs	
	3. Decrease in RCS Inventory	3.1 Release of Reactor Coolant From the RCS	3.3.1 - 3.3.4 (See Items 2.3.1 - 2.3.4)

In Table 3.9, the three defined characteristics of RCS overcooling are expanded in terms of possible functional causes. Following reactor trip (which is an assumed necessary condition for an overcooling transient), the heat input from the subcritical core to the reactor coolant (decay heat) is a fixed decreasing function of time. To the extent heat is removed from the reactor coolant at a rate in excess of the decay heat, the total energy content of the coolant and its temperature will decrease. As shown in Table 3.9, a net heat transfer from the RCS could result from increased heat transfer through the steam generator tubes to the feedwater (secondary coolant) or a direct release of the high temperature reactor coolant from the RCS.

RCS pressure is controlled by regulating the saturation temperature of the pressurizer. The RCS pressure will decrease in response to a decreased pressurizer temperature (assuming saturation). The pressurizer saturation temperature can decrease in response to an increase in the pressurizer spray flowrate which condenses steam in the pressurizer or a direct release of steam from the pressurizer. A decrease in the pressurizer liquid level also may result in reduced RCS pressure due to the expansion of the steam volume. The pressurizer level can be reduced in response to a decrease in the reactor coolant temperature and resulting decrease in coolant volume or a direct release of reactor coolant from the RCS.

Decreases in RCS inventory results from a net release of reactor coolant from the RCS as discussed above.

Based on the functional expansion of the RCS overcooling characteristics, three functional causes can be identified:

1. Increased heat transfer through the steam generators in excess of the decay heat generation rate.
2. Opening the Pressurizer Spray Valve.
3. Net release of Reactor Coolant from the RCS.

These three overcooling characteristics are discussed in Sections 3.3.1.1, 3.3.1.2 and 3.3.1.3 to relate the physical overcooling processes occurring in the RCS in response to RCS and interfacing equipment operating modes.

3.3.1.1 Increased Heat Transfer Through the Steam Generators

Following reactor and turbine trip, heat transfer from the reactor pumped through the steam generator tubes is regulated by the mass flowrate and temperature of the feedwater addition to the steam generator "shell" side (outside the tubes) and the saturation pressure maintained in the shell side.

The core power following reactor trip is below 5% full power. This heat is removed, under normal conditions, in the two steam generators by regulating the feedwater flowrate to maintain a feedwater inventory equivalent to approximately 30" of water in the steam generators and regulating the saturation pressure of the steam generators' shell side at approximately 1025 psia using the turbine bypass valves. Under steady state conditions, the rate at which the feedwater is vaporized is proportional to the small and decreasing decay heat production rates. The reactor coolant temperatures are within a few degrees of the saturation temperature of the shell side of the steam generators.

The rate of heat transfer from the reactor coolant to the feedwater could be increased by either of two mechanisms: reducing the saturation temperature of the steam generator shell side or increasing the feedwater flowrate. A reduction in the saturation pressure could occur by opening the turbine bypass valves. This would result in a lower shell side saturation temperature, an increased temperature difference between the reactor coolant and the boiling feedwater and consequently an increased heat transfer rate. The reactor coolant temperature is expected to decrease under these conditions until a new equilibrium is established. It should be noted that as the saturation pressure is reduced the volumetric flowrate of steam will decrease. Furthermore, at the reduced saturation pressures and temperatures, the energy content per unit volume of steam released through the turbine bypass valves will be reduced due to increased specific volume (decreased density) of the steam. Due to these phenomena, the rate of reactor coolant temperature reduction will decrease as the temperature decreases. However, reactor

coolant temperatures of less than 300°F are considered possible after several hours.

An increase in the flowrate of feedwater also can result in a potentially significant decrease in heat transfer from the reactor coolant. Following reactor and turbine trip, the extraction steam to the feedwater heaters is isolated and the feedwater temperature will begin to decrease slowly. As the rate of feedwater injection increases, the rate of heat transfer from the reactor coolant required to heat the feedwater to saturation temperature increases. Although the rate of steam production will be reduced, the net rate of heat transfer from the reactor coolant can increase significantly due to the large capacity of the main feedwater system.

In addition to increased heat transfer through the steam generators, increased heat transfer through the letdown-makeup flowpath or increased convective heat transfer to the reactor building air is possible. In either case, however, the effects of these mechanisms on reactor coolant temperature are expected to be negligible.

3.3.1.2 Increased Pressurizer Spray Flowrate

During operation, the RCS pressure is controlled by regulating the saturation temperature in the pressurizer. Pressure is increased by heating the saturated water in pressurizer and decreased by spraying subcooled water from the RCS inlet pipes into the saturated pressurizer steam space. A continued spray flow, which could result from the pressurizer spray valve failing open, potentially results in a depressurization transient.

Following reactor trip, the RCS is controlled to a temperature of approximately 547°F and a pressure of approximately 2166 psig (pressurizer saturation temperature of 648°F). If the pressurizer spray valve opened and remained open, the 547°F water sprayed into the pressurizer steam space would result in a decrease in the pressurizer saturation temperature and RCS pressure. As the pressure decreases, the effect of the spray is counteracted by the 1638 KW pressurizer heaters.

It should be noted that the effect of increased spray flow is a potential decrease in RCS pressure with the RCS temperature remaining at 547°F. This transient is of interest due to the potential for initiating safety injection at the ESPS low RCS setpoint pressure of 1500 psi.

3.3.1.3 Release of Reactor Coolant

The release of reactor coolant potentially involves a reduction of reactor coolant pressure, temperature and inventory depending on the leak rate and the operation of other systems. Continued power operation typically is allowed with leak rates less than 10 gpm. Small and large loss of coolant accidents (LOCA's) in contrast, are significant hazards to nuclear power plant safety.

This study considers the effects of control systems failures. As such, arbitrarily postulated piping failures are not considered. Release of reactor coolant resulting from pressurizer relief or safety valves opening and remaining open, a net release of reactor coolant via the letdown piping or steam generator tube cracks is considered to the extent such a failure may result from a control system misoperation. In general release of reactor coolant falls in the category of RCS leaks or small LOCA's.

The response of nuclear power plants to a release of reactor coolant varies considerably depending on the rate of loss. Miscellaneous plant leakage, typically much lower than 1 gpm, is a normal occurrence. The operator routinely monitors the makeup tank level to determine the leak rate from the RCS. During the periodic adjustments to the reactor coolant boron concentration, the operator replaces a volume of reactor coolant with demineralized water. During this process, water would be added to the makeup tank to replace RCS leakage.

If the operator detects an RCS leak rate exceeding 1 gpm, he must determine the location of the leak or shut down the plant. Leakage through one or more of the pressurizer relief valves, for instance, can be identified by high temperature readings of the discharge line thermocouples. In addition, if the source of leakage exceeding 1 gpm is the steam generator tubes, the plant must be shutdown. Steam generator tube leaks are indicated by the monitored

radioactivity level of the main condenser "air" ejector discharge. All RCS leakage exceeding 10 gpm requires plant shutdown.

RCS leak rates within the makeup capability of the makeup and purification system (MU&P) are classified "RCS Leaks." RCS leaks exceeding the above leak rate limits require shutdown of the plant to a "cold shutdown" state and repair of the pressure boundary failure.

For RCS leaks in the pressurizer water space or the RCS loops, the mass flow rate from the RCS to the containment is balanced automatically by the makeup mass flow rate from the makeup tank to the RCS. Under this condition, RCS pressure is controlled by the operation of the spray valve and pressurizer heaters. Prior to the draining of the makeup tank, the operator must initiate makeup to the makeup tank or open the valves in the flowpath from the Borated Water Storage Tank (BWST) to the makeup pump(s).

The shutdown operation with "water space" RCS leaks (as opposed to "steam space" leaks) is similar to normal shutdown operations. The operator controls the rate of cooldown and the rate of depressurization to maintain the RCS within pre-established pressure and temperature limits for shutdown. The cooldown rate is maintained by operator control of the turbine bypass valves and the depressurization rate by operator control of the spray valve.

RCS leaks in the pressurizer steam space (>200 lbm/min) result in an initially uncontrolled depressurization of the RCS even with the pressurizer liquid level maintained. The operator is instructed to attempt to isolate the leak by manually closing the PORV and/or the PORV block valve.

If the leak is not isolated, the pressurizer heaters are capable of maintaining pressurizer pressure and temperature for leak rates less than 200 lbm/min. The required makeup rate for these transients is less than 27 gpm. Makeup rates greater than 10 gpm would require shutdown with conditions similar to "water space" leaks.

The operator can control the depressurization by manually increasing the makeup flow rate and filling the pressurizer. If the operator fails to take

this action, the RCS pressure will decrease to the safety injection setpoint (~1500 psi). At this pressure, the high pressure injection (HPI) mode of the MU&P will be automatically actuated and the pressurizer will be filled. Once the pressurizer is filled and the leak is in the water space, the RCS pressure is automatically controlled by the PORV and/or safety valves at approximately 2450 psi.

Once the RCS pressure is controlled, the operator can initiate shutdown procedures. With the RCS subcooled by at least 50°F, the operator can reestablish the pressurizer level by throttling the makeup flow. When the leak path is uncovered and steam discharged, the RCS will begin to depressurize. The cooldown is controlled by manual control of the turbine bypass valves. If the 50°F reactor coolant subcooling cannot be maintained with a cooldown rate of 100°F/hour, the operator must increase the MU&P/HPI flowrate until the required subcooling can be reestablished. During the depressurization, the leak rate will decrease due to the lower RCS pressures. If an increased rate of depressurization is required, the operator can manually open the spray valve or the PORV.

Breaks resulting in a leak rate in excess of the capacity of the makeup system are classified Loss of Coolant Accidents (LOCA's). A small break LOCA, such as a failed open PORV, generally will result in the RCS pressure decreasing rapidly to the saturation pressure (approximately 1200 psi) and then slowing considerably (the pressure will rise following very small breaks and limited steam generator cooling). At 1500 psi the HPI is automatically started and begins injecting borated water from the BWST. The operator is instructed to trip the reactor coolant pumps which results in the steam generators being automatically filled and maintained by the main or emergency feedwater systems at the natural circulation setpoint.

Core cooling is maintained by the continued operation of the HPI. Throttling the HPI is not permitted since the reactor coolant will not be 50°F subcooled. To enhance the RCS depressurization and cooldown, the operator may depressurize the steam generators by manually controlling the turbine bypass valves.

Small break LOCA's result in a gradual net loss of reactor coolant until the RCS depressurizes to a pressure where the net loss is zero and refilling begins. Typically, the reactor coolant rapidly saturates at approximately 1000 psi. The subsequent response of the RCS depends on the decay (residual) heat generation rate of the core, the coolant mass and energy removal through the break, the rate of coolant mass injection, and the rate of heat removal through the steam generators. If the rate of core heat generation exceeds the rate of heat removal through the break plus the heat removal through the steam generators, the coolant pressure and temperature will increase. This will increase the heat loss through the break and result in thermal equilibrium. However, the increased pressure also results in an increase in the rate of coolant mass loss and a decrease in rate of coolant injection. If more heat is being removed from the RCS than generated in the core a reverse process takes place. In addition to the above phenomena, the rate of core heat generation is decreasing with time and the rate of heat transfer through the steam generators varies with the RCS coolant inventory.

The RCS coolant inventory typically decreases over the initial period of the LOCA, reaches a minimum and then increases. If this minimum inventory is sufficient to maintain the core covered with coolant, the plant will recover. However, if the minimum inventory results in a significant fraction of the core being uncovered, core damage will occur. Typically, nuclear power plants are designed to maintain an adequate minimum inventory following small break LOCA of any size even with assumed partial failures of the HPI and steam generator cooling functions and a conservatively large core heat generation rate.

In addition to the "classical" LOCA scenarios, a failure mode involving brittle failure of the reactor vessel wall has been postulated and is under investigation. In these Pressurized Thermal Shock (PTS) scenarios, a LOCA, or other initiating accident, results in a low temperature, high stress condition in the reactor vessel wall. The LOCA recovery actions described above are being analyzed to determine whether they produce conditions sufficiently severe to result in a large through-wall crack in the reactor vessel.

PTS is of some concern following small break LOCA's. Following a LOCA, the reactor coolant circulating pumps are tripped. Due to the net loss of reactor coolant inventory, natural circulation of liquid coolant from the reactor through the steam generators will cease. The major flow into the RCS will be from the low temperature BWST into the reactor inlet pipes. Over the course of the accident, the RCS pressure will be slowly decreasing and the temperature of the coolant in the vessel downcomer (which is thermally separated from the core region following outlet pipe and pressurizer breaks) will be decreasing. The combination of the relatively high RCS pressure and relatively low vessel wall temperatures may lead to brittle fracture in reactor vessels which are particularly sensitive to radiation embrittlement.

One particular small break LOCA of concern is the failed open PORV. Assuming the failed PORV remains unisolated for the initial phase of the accident, the vessel downcomer temperature will be low. If the operator then isolates the PORV, the continued injection of coolant and the heat generated in the core will increase the RCS pressure to pressures of up to 2500 psi, which may be of significant PTS concern.

The PTS phenomena is the subject of considerable current research and analysis. Detailed analysis to determine the pressures and temperatures occurring following small breaks and the response of reactor vessels to these conditions is required to assess the potential for vessel failure.

Detailed information describing the required equipment and operator actions following system leakage and LOCA's is provided in each plant's LOCA emergency procedure (e.g., Duke Power emergency procedure EP/O/A/1800/4, "Loss of Reactor Coolant" and OP/O/A/1106/35, "Inadequate Core Cooling"). The response characteristics of the RCS to LOCA's is described in vendor topical reports referenced in each plant's FSAR (Reference 2).

3.3.2 Evaluation of RCS Overcooling Response to Systems Failures

Based on the definition of RCS overcooling, the systems potentially affecting RCS response identified in Tables 3.7 and 3.8, were briefly evaluated to assess their potential impacts on RCS overcooling. The results of this evaluation are summarized in Table 3.10.

TABLE 3.10. POTENTIAL IMPACTS OF FIRST AND SECOND ORDER REACTOR COOLANT SYSTEM INTERFACE SYSTEMS ON RCS OVERCOOLING

System ID	System Name	Potential Impact on RCS Overcooling
N01	Reactor Core	The response of the reactor core can influence overcooling. However, "core failures" are considered to be beyond the scope of this study (see Section 4).
N02	Regulation Systems	
N02.A	Control Rod Drive Control	Control rod drive control system has no function in the post-trip mode (see Section 4).
N02.B	Integrated Control	Control signal failures considered as part of fluid systems controlled.
N02.C	Non-Nuclear Instrumentation	Control signal failures considered as part of fluid systems controlled.
N04	Reactor Coolant	
N04.A	Pressurizer	Analyzed in detail.
N04.B	Steam Generator	Analyzed in detail.
N04.C	Reactor Coolant Pumps	Analyzed in detail.
N04.D	Control Rod Drive Mechanisms	Control rod drive mechanisms have no function in the post-trip mode (see Section 4).
N05	Makeup and Purification	Makeup and Purification subsystems considered in detail with the exception of the sampling systems. The sampling systems are intermittently used under manual control with sample flowrates less than 1 gpm. Sampling system failures are not considered to have any significant impact on RCS overcooling.

TABLE 3.10. (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
N05.A	Chemical Addition and Sampling	
N05.B	Coolant Storage	
N05.C	Coolant Treatment System	
N05.D	Post Accident Sampling	
N05.E	High Pressure Injection	
C03	Reactor Building Ventilation	The effect of containment air temperature changes on heat transfer from the RCS is considered to be insignificant. The effects of loss of ventilation on component operability is considered to be beyond the scope of the study.
PC1	Main Steam and Turbine Bypass	Power conversion systems and subsystems analyzed in detail.
P02	Turbine-Generator System	
P03	Main Condenser	
P04	Condensate and Feedwater	
W01	Radioactive Waste	System was selected based on its interface with the Non-Nuclear Instrumentation. However, the interface consists of providing parameter signals for display only. Failures of the Radioactive waste system not considered to have any significant impact on RCS overcooling.
W03	Reactor Building Component Cooling Water	Potential impact due to first and second order interfaces. Cooling water failures considered as part of the process systems served.

TABLE 3.10. (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
W04.A	Condenser Circulating Water	Potential impact due to second order interfaces. Cooling water failures considered as part of the process systems served.
W04.D	Recirculated Cooling Water	Potential impact due to second order interfaces. Cooling water failures considered as part of the process systems served.
W07.B	Instrument Air	Potential impact due to first and second order interfaces. Instrument air failures considered as part of the fluid systems served.
X05.E	Reactor Building Cooling	The effect of containment air temperatures on RCS heat transfer is considered to be insignificant. The effects of high air temperatures on the operability is beyond the scope of this report.

As indicated, most of the systems affecting RCS response have the potential for affecting RCS overcooling. These systems are analyzed in detail using a failure modes and effects analysis method to evaluate specific effects of system failures on RCS overcooling (see Section 5). The systems not selected for detailed analysis are discussed below.

The heat production rate of the reactor core will affect the course of an RCS overcooling transient. However, the heat production rate will vary depending on external factors affecting the core rather than possible core failures. The potential effects of core failure mechanisms (e.g., cladding perforation, gross core movement) are beyond the scope of this analysis.

The control rod drive mechanisms and the control rod drive control system influence to rate of core heat production during operation. However, once the reactor is tripped (control rods inserted) neither the drive mechanisms nor the drive control system can influence the resulting transient. The reactor core, control rod drives and the control rod drive control system are discussed further in Section 4.

The reactor building ventilation system and the reactor building cooling system control the air temperature in the containment. The effect of containment air temperature or velocity changes are considered to have a negligible effect on heat transfer from the insulated RCS and consequently a negligible effect on RCS overcooling. Although it is recognized that long term operation of components in an adverse (high temperature) reactor building environment can effect their performance, the study of such effects is considered beyond the scope of this analysis.

The radioactive waste system is monitored by the non-nuclear instrumentation. However, the parameters monitored only are displayed and have no impact on the development of non-nuclear instrumentation control signals. As such, the radioactive waste system is considered to have no significant impact on RCS overcooling.

4.0 SYSTEM DESCRIPTIONS

Brief system descriptions are provided for each system identified in Section 3.2 as requiring detailed analysis. Support systems (e.g., instrument air and control systems) are discussed with each major system.

4.1 NUCLEAR SYSTEMS DESCRIPTIONS

The Nuclear Systems include the reactor core and those systems and subsystems which 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 Section 3.2 requiring detailed analysis are:

- 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.

4.1.1 Reactor Core

The reactor core consists of the 177 fuel assemblies which produce the thermal power ultimately used to produce electric power in the unit's main generator. The thermal power is produced by nuclear fission of the slightly enriched uranium in the core. The core fuel assemblies are supported by the reactor internals in the reactor vessel.

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

Although the response of the core to external parameters is important to a study of reactor coolant system overcooling, 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 start of externally initiated transients, and to respond to external factors as designed.

4.1.2 Reactor Coolant System

The Oconee reactor coolant system (RCS) is a B&W design nuclear steam supply system. It consists of or is impacted by the following major components:

1. A reactor vessel which houses and supports the reactor core.
2. Four reactor coolant pumps which circulate reactor through the reactor core and steam generators.
3. A pressurizer which is used to control RCS pressure and maintain the reactor coolant in a subcooled state.
4. Two steam generators which transfer heat from the reactor coolant to produce the steam to drive the plant turbines.
5. 61 Control Rod drive mechanisms which position the individual control rods.

Reactor coolant is pumped from the steam generators into the reactor vessel through the four "cold-leg" inlet pipes. The coolant flows upward through the pipes where 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 steam generators through one of the two "hot-leg" outlet pipes. Heat is transferred from the high temperature reactor coolant as it flows downward through the tubes of the two steam generators. The heat flowing across the steam generator tube walls vaporizes and slightly superheats the feedwater pumped into the shell side of the steam generators to produce steam. The reduced temperature reactor coolant flows from each steam generator through two pipes, 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, steam generators and associated equipment is discussed below.

4.1.2.1 Reactor Coolant Pumps

Each reactor coolant loop contains two vertical single stage centrifugal-type pumps which employ 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, discharged through passages in the guide vanes and out through a discharge in the side of the casing. The rotor-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 which directs 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 pumps is injected into the reactor coolant pump between the impeller and the controlled leakage seal. Part of the flow enters the Reactor Coolant System 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. A small amount which 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 high pressure injection 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 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. The motors have flywheels to increase the 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 eliminate reverse rotation when there is back flow. Prevention of back rotation also reduces motor starting time.

The motors are enclosed with water-to-air heat exchangers so as to provide a closed circuit air flow through the motor. Radial bearings are 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 where heat is rejected to the component cooling water flow through the heat exchanger. 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.

4.1.2.2 Pressurizer

The pressurizer in a pressurized water reactor 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 measure of the reactor coolant inventory. The pressure in the pressurizer (and the RCS) is controlled at a setpoint value to maintain the reactor coolant in the RCS in a subcooled state.

During transient reductions in the reactor coolant volume, the liquid level in the pressurizer and the RCS pressure both tend to decrease. The liquid level in the pressurizer is measured and the decrease below setpoint results in a

control circuit automatically increasing the net flow rate to the RCS from the Make-up and Purification System (MU&P) to restore the setpoint level. The decreased RCS pressure is measured and 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 and consequently the RCS pressure.

During transient increases in the reactor coolant volume, a reverse process will occur to reestablish setpoint values. The increased pressurizer liquid level results in a decrease in the net flow rate from the MU&P system. The 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 setpoint 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 valves' seats (no control circuit is required).

Pressurizer system interfaces, including power supplies and signal destinations, are discussed in detail in Reference 6.

4.1.2.3 Steam Generator

The steam generator is a vertical, straight tube, tube and shell heat exchanger which 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 outside 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. There are openings in the baffle at the feedwater inlet nozzle elevation to provide a path for steam to afford contact feedwater 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 feedwater inlet heating zone.

Vent, drain, and instrumentation nozzles, and inspection handholes are provided on the shell side of the unit. The reactor coolant side has manway openings in both the top and bottom heads, and a drain nozzle on the bottom head. Venting of the reactor coolant side of the unit is accomplished by a vent connection on the reactor coolant inlet pipe to each unit.

Feedwater is heated to saturation temperature by direct contact heat exchange. During normal power operation, the feedwater 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 feedwater 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 steam generator. The downcomer water level varies with steam flow from 15 - 100 percent load. A constant minimum level is held below 15 percent 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 counter-current to the 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 section gains surface from the nucleate and film boiling regions. Mass inventory in the steam generator increases with load as the length 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 the inventory requirements. If the inventory is greater than that required, the pressure increases. Inventory is controlled automatically as a function of load by the feedwater controls in the Integrated Control System.

In the event the main feedwater pumps trip, the emergency feedwater system injects feedwater into the emergency feedwater spray header located near the top of the steam generator. Main feedwater flow also may be injected through the emergency feedwater header by valve realignment. This action enhances natural circulation of reactor coolant in the event the reactor coolant pumps are tripped or deenergized.

4.1.2.4 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 (61) CRDM are divided into four safety banks and four 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 (or 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 banks control rods are released to fall into the core regardless of CRDCS or ICS control signals.

The 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 both are 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. 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 of interest to overcooling transients (i.e., decreasing RCS temperature, pressure or inventory following reactor trip). Mispositioning the control rods, at most, may 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 FSAR accident analysis. 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, at most, may result in a reactor trip signal and release of all control rods.

Reactor trip is an expected condition in the context of the overcooling transient considered in this study. Although malfunctions of the CRDM or CRDCS can produce a reactor trip transient, overcooling will occur only due to independent failures of other systems (reactor trip itself is not an overcooling transient). As such, detailed analysis of CRDM or CRDCS malfunctions is not required in the study of overcooling transients.

4.1.3 Regulation Systems

The operation of the RCS and key interfacing systems is controlled by three major instrumentation systems: the Control Rod Drive Control System (CRDCS), the Non-Nuclear Instrumentation System (NNI) and the Integrated Control System (ICS). The functions of these regulating systems, with emphasis on their relation to RCS overcooling are described below.

4.1.3.1 Control Rod Drive Control System

The CRDCS, as discussed in Section 4.1.2.4, applies power to the CRDM motors to insert or withdraw the control rods. The CRDCS inserts and withdraws the control rods in response to commands from the control room manual control station or automatic signals from the ICS during power operation. Additional CRDCS design information is provided in Reference 2.

Upon reactor trip, which occurs during any overcooling transient of interest, the CRDCS and the CRDM's are deenergized and cannot influence the course of

the subsequent transient. As such, failure modes of the CRDCS which relate to 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.

4.1.3.2 Non-Nuclear 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, the NNI contains control circuits used to control process variables such as RCS inventory (makeup flowrate control), RCS pressure (pressurizer spray, heater and relief valve control) and RC pump seal injection flowrate control. The NNI is described in detail in References 2 and 7.

The NNI is expected to have a significant influence on RCS overcooling transients. In particular, RCS pressure control circuit malfunctions could lead to actuation of the ESPS. Malfunctions of the steam pressure and steam generator level circuits supplying signals to the ICS could lead to continued RCS temperature reductions. Due to the potential impact on RCS overcooling, the NNI control and measurement circuits are analyzed in detail as part of the analysis of fluid system controlled components.

4.1.3.3 Integrated Control System

The principal function of the ICS is to develop coordinated control signals to regulate main feedwater flowrate, reactor power and steam pressure during power operation. Based on process parameter signals developed in the NNI, the ICS develops signals to modulate the main feedwater control valves, the 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 feedwater control valves to maintain the steam generators' water level and the turbine bypass valves to maintain steam line pressure. Either of these functions can have a significant influence on RCS overcooling and the ICS control circuits are analyzed in detail as part of the analysis of fluid

system controlled components for this reason. The ICS functions and circuitry is described in detail in References 2 and 7.

4.1.4 Makeup and Purification System

The functions performed by the Oconee High Pressure Injection, Coolant Storage, Coolant Treatment and Chemical Addition Systems are sequential and complementary. The equipment in these systems has been grouped to include a general makeup and purification system.

The Makeup and Purification (MU&P) System consists of the piping and process equipment required to remove, process and replace reactor coolant at the flowrates required to maintain constant Reactor Coolant System (RCS) coolant volume. The major functions performed by the MU&P System are:

1. Letdown Control: Controlled removal of reactor coolant from the RCS and reduction of coolant temperature and pressure at a preset flowrate.
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. Reactor Coolant Pump (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 pumps' shaft seals at a constant flowrate.
6. RC Makeup: Injection of processed letdown coolant to the RCS at a flowrate 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.

Detailed functional descriptions for these subsystems are provided in Reference 8.

4.2 POWER CONVERSION SYSTEMS DESCRIPTIONS

The Power Conversion Systems are designed to convert the heat produced in the reactor to electrical energy.

The superheated steam produced by the steam generators 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 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 feedwater heaters. The second stage reheaters are supplied with main steam and the condensed steam cascades to the A feedwater heaters. Heat for the feedwater 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 pump the condensate through three stages of intermediate pressure feedwater heaters (F, E, and D). The flow combines with the D heater drain pump discharge before the C feedwater heaters, divides to the suction of the steam generator feedwater pumps. The steam turbine driven

main feedwater pumps deliver feedwater through two stages of high pressure feedwater heaters (B and A), to a single feedwater distribution header where the feedwater flow is divided into two lines to the steam generators.

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

4.2.1 Main Steam and Turbine Bypass System

Main steam is generated in the two steam generators by feedwater absorbing heat from the Reactor Coolant System. Main steam is conveyed by two lines, one per steam generator, to the turbine inlet valves. A pressure equalization and steam distribution header is connected to each main steam line upstream of the turbine inlet valves. The main steam and turbine bypass system is shown in Oconee FSAR Figure 10.3-1, which is reproduced in Appendix B.

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

The turbine bypass system (TBS) is designed to reduce the 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 crossflow between the main steam lines.

High pressure steam supply piping provides steam from each main feedwater 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 the low pressure bleed steam flow. The high pressure governor and stop valves are designated MS-41 and 40 and MS-44 and 43 for feedwater pump turbines A and B, respectively. In addition to the steam supply to feedwater 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 emergency feedwater pump turbine. Check valves are installed to prevent cross flow between the main steam lines through the emergency feedwater 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.

4.2.2 Turbine-Generator System

The turbine-generator system converts the thermal energy of steam produced in the steam generators 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. The Oconee high and low pressure turbines, extraction steam piping and moisture separator-reheaters are shown in Oconee FSAR Figures 10.3-4 and 10.3-7 which are reproduced in Appendix B.

Main steam from the steam generators 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. 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 feedwater pumped to the steam generators. The "A" (highest pressure), "B" and "C" feedwater heaters are supplied from the high pressure turbine (or its exhaust). The "A" bleed lines also supplies the first stage reheater. The "D", "E" and "F" feedwater heaters are supplied from the low pressure turbines. The "D" bleed lines also supply the main feedwater 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 Integrated Control System. 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 in the event that 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 solenoid valves. These valves depressurize turbine hydraulic controls and result in closing the four high pressure turbine stop valves, 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.

4.2.3 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 which is stored in the condenser hotwell. The condenser also serves as a heat sink for the turbine bypass system and is capable of handling 25 percent of rated main steam flow. Rejected heat is removed from the main condenser by the Condenser Circulating Water System. The condenser and condenser evacuation systems are shown in Oconee FSAR Figures 10.4-1 and 10.4-4 which are reproduced in Appendix B.

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 feedwater 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 ten minutes of full load operation (nominally 142,000 gallons). The condenser provides for condensing of steam, scavenging and removal of noncondensable gases, and the deaeration of 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 approximately 18 percent 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 noncondensable 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 subsystem consists of three condenser steam air ejectors (CSAE) per unit. Normally each CSAE draws the noncondensable 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 after condenser 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 condenser steam air ejector 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 only used during startup since normal operation requires the use of the CSAE only.

4.2.4 Condensate and Feedwater System

The condensate and feedwater system purifies, heats and pumps the condensate from the condenser hotwells to the two steam generators to complete the steam-feedwater cycle. The condensate and feedwater system is shown on Oconee FSAR Figures 10.4-4, 10.4-7, 10.4-8 and 10.4-13 which are reproduced in Appendix B.

Two of the 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. The 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 feedwater heaters to the main feedwater pumps. The condensate is heated in four stages of low pressure feedwater 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 main feedwater pumps. The flowrate through the two feedwater pumps is controlled by the two main feedwater control valves based on reactor/turbine demand. To increase the efficiency of the pumps, the pressure drop across the feedwater control valves is limited to 35 psi by regulating the speed of the feedwater pumps. Under conditions of low flow demand with the control valves closing, the increasing pressure drop is measured and the pump speed 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 feedwater flowrate controls, the minimum flow through each pump is limited to approximately 2500 gpm to protect the pumps. Lower flowrates measured in the pump suction lines result in automatically opening bypass valves FDW-53(?) and FDW-45(?) which divert feedwater from the pump discharge lines to the upper surge tank.

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

The equipment described above comprises the main flowpath from the condensers to the two main feedwater lines. However, the main flowrate pumped from the condenser hotwells (normal flowrate: 6.6×10^6 lbm/hr) is approximately half of the flowrate delivered to the two steam generators (normal flowrate: 11.3×10^6 lbm/hr). The balance of the flow is pumped into the condensate and feedwater lines by the heater drain system. The extraction steam condensed in the steam reheaters and the high and low pressure feedwater heaters is collected and pumped into the condensate lines at points of comparable temperature. The heater drain system is shown on Oconee FSAR Figure 10.3-7, included in this section, and Duke Power Drawing PO-123A which was not available for this analysis.

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

As described above, the feedwater flowrate is controlled by ICS control signals to the main and startup feedwater control valves. During power operation, the feedwater flowrates to the two steam generators 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 approximately 15% to 100% full power. The control signals are modified as functions of steam generator heat balances (BTU limits), the status of key plant equipment (e.g., turbine trip, RC pump trip) and steam generator level limits. The feedwater control valve demand signals are limited based on high steam generator level as measured by pressure drops in the steam generator. Exceeding the high level control limit in either steam generator will result in ICS generated signals which trip the main feedwater pumps.

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

As feedwater 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 main feedwater block valves. These valves are closed to prevent possible leakage through the main control valves from interfering with the control of the startup valves. The block valves are automatically opened as the startup valves are positioned more than 80% open.

Following reactor trip, the feedwater flowrate is controlled to maintain steam generator levels of approximately 30" with one or more RC pumps in operation. If all four RC pumps are tripped, the ICS automatically increases the minimum level setpoint to approximately 20 feet to maintain the desired rate of natural (convective) circulation of reactor coolant through the core.

4.3 PROCESS AUXILIARY SYSTEMS

Process Auxiliary Systems include those systems and subsystems that support the operation of the Nuclear System and Power Conversion Systems. The major systems and subsystems identified in Section 3.2 as requiring detailed analysis 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.

4.3.1 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 also provides an additional barrier between high pressure reactor coolant and service water to prevent an inadvertent release of activity.

The following is a brief functional description of the major components of the system.

Component Cooler. Each component cooler is designed for the total system heat load for a reactor unit. Ocone 1 and 2 each have a single component cooler with a shared common spare. Ocone 3 has two coolers. The coolers reject the heat load to the Low Pressure Service Water System.

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.

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 would provide a reservoir of component cooling water until a leaking cooling line can be isolated. Makeup water and corrosion inhibiting chemicals are added to the system in the surge tank.

4.3.2 Condenser Circulating Water (CCW)

The Little River arm of Lake Keowee is the source of water for the CCW systems. Each unit has four condenser circulating water pumps supplying water via two 11 ft. conduits into a common condenser intake header under 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 which can be manually removed for periodic cleaning.

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

The CCW system has a 48 inch 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 automatically open 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.

4.3.3 Recirculated Cooling Water (RCW)

This system provides inhibited closed cycle cooling water to various components outside the Reactor Building including:

- o RC pump seal return coolers
- o Spent fuel cooling
- o Sample coolers
- o Evaporator systems
- o Various pumps and coolers in the Turbine Building
- o 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 provides a surge volume to accommodate 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. Leakage of radioactive fluids from any of the coolers in the Auxiliary Building will be indicated by these monitors. 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.

5.0 FAILURE MODES AND EFFECTS ANALYSIS OF SELECTED SYSTEMS

The analysis results documented in this report have been developed using failure modes and effects analysis (FMEA) techniques. A FMEA identifies system level failure modes of concern and traces their effects on components, subsystems, and other systems. Emphasis is placed on identifying significant effects associated with specific failures. The advantage of the analysis technique is that while it is simple to apply, it provides for an orderly examination of potentially important failure modes throughout a plant.

In a FMEA, the impact or effect of a potential fault is documented in tables which identify the failure being considered. Support systems associated with the failure (for example, instrument air for pneumatic diaphragm operated valves) also must be considered. Potential component fault modes due to internal failures or unavailability of support systems, the impact of the fault on system operation, and potential remedial action if the fault occurs are listed in the FMEA tables. Analysis of the completed tables permits identification of failures which may have significant impact on system and plant operation.

The major systems identified in Section 3 as potentially affecting RCS overcooling have been analyzed using the FMEA techniques. The results of these analyses, including the effects of control instrumentation and supporting systems failures have been discussed in separate reports 6, 8 and 9.

The specific effects of failures in the systems identified in Table 3.10 as they relate to RCS overcooling are discussed in Section 5. The majority of these RCS overcooling effects have been obtained from the more general FMEA's of the identified systems. The RCS overcooling effects resulting from failures in the RCS subsystems (Pressurizer, RC Pumps and Steam Generators) and associated control instrumentation and support systems are identified and discussed in Section 5.1. The RCS overcooling effects of failures in the Power Conversion and Makeup and Purification systems are discussed in Sections 5.2 and 5.3, respectively.

5.1 REACTOR COOLANT SUBSYSTEMS

As discussed in Section 3, three RCS subsystems have been identified as potentially contributing to overcooling transients: the Pressurizer, RC Pump and Steam Generator subsystems. The overcooling failure modes and interfacing systems associated with the failure modes are listed for each RCS subsystem in Table 5.1. As noted, component level FMEA's of each of these subsystems are presented in Tables 5.2, 5.3 and 5.4. The results of the FMEA's are discussed below in Sections 5.1.1, 5.1.2 and 5.1.3 for the Pressurizer, RC Pump and Steam Generator subsystems.

5.1.1 Pressurizer Subsystem

Two overcooling failure modes have been identified for the pressurizer subsystem: Release of reactor coolant and excessive pressurizer spray flowrate. In Table 5.2 the specific component level failures leading to or contributing to these failure modes are identified with the potential causes of the failure, its effect on the RCS and possible remedial actions listed for each.

A release of reactor coolant (a small LOCA) will result initially from either the PORV or pressurizer code safety valve opening and failing to close. Code safety valves are passive devices which 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 (which 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 systems failures. If one of the safety valves does fail to close, the leak path cannot be isolated (see Item 1, PORV Fails Open).

The PORV (pilot operated relief valve) opens and closes in response to external control signals. The relief valve 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 opens the relief valve. The relief valve is closed by deenergizing the pilot valve solenoid.

TABLE 5.1. SUMMARY OF RCS SUBSYSTEM FAILURE MODES

RCS Subsystem	Overcooling 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 5.2.
		1.1.2 NNI	
		1.1.3 Pressurizer Code Safety Valve	
	1.2 Opening the Pressurizer Spray Valve	1.2.1 Pressurizer Spray Valve	
2. RC Pumps	2.1 Release of Reactor Coolant	1.2.2 NNI	FMEA of RC Pumps presented in Table 5.3.
		2.1.1 RC Pump Shaft Seals	
		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 5.4.
		3.1.2 Main Steam and Turbine Bypass System	
	3.2 Increased Heat Transfer	3.2.1 Main Steam and Turbine Bypass System	
		3.2.2 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 5.7.

TABLE 5.2. SUMMARY OF PRESSURIZER SYSTEM FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

Failure	Possible Causes	Effects	Remedial Actions
<u>Release of Reactor Coolant</u>			
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 acoustic 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.	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 acoustic 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.

TABLE 5.2. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	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 acoustic 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.
<u>Pressurizer Spray Valve Fails Open</u>			
4. Pressurizer Spray Valve, RC-V1 Fails Open	Mechanical failure of valve resulting in valve opening or failing to close once open.	Slow RCS depressurization with the pressurizer heaters energized. ESPS 1500 psi RCS pressure setpoint may be reached depending on the spray flowrate and heater capacity.	Identify open valve and close spray block valve, RC-V5.
5. Power to Spray Valve Solenoid Fails On	o NNI pressure switch, RC-PS3 or controller (RC-M1S1) failure.	Spray valve opens resulting in a slow RCS depressurization with the pressurizer heaters energized. ESPS 1500 psi RCS pressure setpoint may be reached depending on the spray flowrate and heater capacity.	Identify open valve and close spray block valve, RC-V5. Spray valve manual control may be operable.

TABLE 5.2. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	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 acoustic 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.

Contributing Failures

6. 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 5.3, FMEA of the Steam Generators). If the pressurizer is allowed to fill, the PORV will be opened and the possible liquid discharge through the valve could contribute to its 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 5.2. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
7. Failure of the Relief/Safety Valve Discharge Line Thermocouple	T/C opens or circuitry deenergized.	Low indicated discharge line temperature. This failure would be confusing to the operator if the associated valve leaked or failed open.	This failure may be difficult to detect and may remain undetected for some period of time. The failure may be detected by a comparison of the three T/C readings and confirmed by test (prior to a postulated relief or safety valve failure).
8. Failure of the PORV Acoustic Monitor	Monitors fail to operate (details unavailable).	Monitor incapable of detecting an open or leaking PORV. This failure would be confusing to the operator if the PORV leaked or failed open.	This failure may be difficult to detect and may remain undetected for some period of time. Failure may be detected by periodic surveillance testing (details unavailable).
9. Failure of PORV or Pressurizer Spray Valve Isolation Valve Open	Valve or valve motor power failure.	Isolation valve would be incapable of isolating the relief or spray flow in the event the associated PORV or spray valve failed open.	These failures may be difficult to detect and may remain undetected for some period of time. An unisolated open PORV transient is controlled by emergency procedures for a small LOCA. An unisolated spray valve could require tripping the associated RC lamp and using the PORV for depressurization or careful control of RCS temperature.

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 the pilot valve solenoid or fails to deenergize the solenoid (Item 3). Certain circuit failures such as a failure of the valve's 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 spurious high pressurizer pressure signal, will result in the PORV and spray valve opening and deenergizing the pressurizer heaters. In contrast to safety valve failures, a failed open PORV may be isolated by manually initiating PORV block valve closure. Closure of the block valve will terminate the release of reactor coolant.

Opening the pressurizer spray valve results in a flow of reactor coolant from the discharge of the reactor coolant pumps to the lower pressure pressurizer steam space. This results in a condensation of steam in the pressurizer and a reduction in RCS pressure. If the spray valve opened and failed to close, the resulting RCS pressure decrease could result in a reactor trip and possibly a spurious actuation of the ESPS.

The pressurizer spray valve is an "on-off" solenoid operated valve. When the high pressurizer pressure setpoint is reached, the solenoid is energized which opens the valve. Deenergizing the solenoid closes the valve.

As shown in Table 5.2, the pressurizer spray valve could fail open or fail to close due to mechanical failure of the valve or a control circuit failure energizing the solenoid. Circuit failures include failures of the pressure switch or valve control switch which result in the spray valve opening with other components remaining operable. The resulting pressure decrease will result in the pressurizer heaters being energized which may reduce significantly the rate of depressurization.

Failure of the pressurizer pressure transmitter or associated signal conditioning modules producing a spurious high pressurizer pressure signal also will result in the spray valve opening. 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.

In addition to failures which directly result in a potential overcooling transient, other Pressurizer System failures which may exacerbate the effects of such a transient have been identified in Table 5.2, Items 6-9. These failures include instrumentation failures which could impede the detection of an open relief or safety valve, failures of the PORV or spray valve isolation valves which could prevent rapid termination of a transient resulting from a failed open PORV or spray valve. Failure of the selected pressurizer level transmitter low has been included in this category since a pressurizer overfill transient could occur. If the overfill was allowed to result in liquid discharge through the PORV or safety valves, valve damage could occur.

5.1.2 RC Pump Subsystem

One RCS overcooling mechanism has been identified in the RC pump subsystem, a release of reactor coolant due to failure of the RC pump shaft seals. RC pump seal failures may result from several possible causes as shown in Table 5.3. 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.

5.1.3 Steam Generator Subsystem

Two potential overcooling mechanisms have been identified for the steam generator subsystem: release of reactor coolant due to steam generator tube failure and increased heat transfer rate across the steam generator tubes. The FMEA of the steam generator subsystem is presented in Table 5.4.

Steam generator tube leaks occur during normal operation typically due to a combination of causes as listed in Table 5.4. Although control system failures have not been identified as a single, sole cause of a tube leak or failure, control system failures may initiate a tube failure in combination with other existing conditions or increase the rate of tube degradation.

TABLE 5.3. FMEA OF RC PUMPS: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

Failure	Possible Causes	Effects	Remedial Actions
<u>Release of Reactor Coolant</u>			
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 5.4. FMEA OF STEAM GENERATORS: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

Failure	Possible Causes	Effects	Remedial Actions
<u>Release of Reactor Coolant</u>			
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.
<u>Increased Heat Transfer Rate</u>			
2. Depressurization of Main Steam System	o Turbine bypass valve(s) fail open.	Small steam line "break" accident. Rapid cooldown of RCS.	Identify leak path and isolate if possible. Follow emergency for steamline breaks. See FMEA of Main Steam Systems, Table 5.5.
	o Main steam code safety valve(s) fail open.	Same as above.	Same as above.
	o Failure to trip or runback turbine following reactor trip.	Same as above.	Same as above.

TABLE 5.4. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
3. Injection of Feedwater at Rates in Excess of RCS Requirements (Steam Generator Overfill)	o Main feedwater control valve fails open or fails to close.	Steam generator level increases until main feedwater pumps are tripped on high steam generator level. Emergency feedwater system automatically started and controlled.	Manually trip main feedwater pumps and confirm automatic initiation and control of emergency feedwater system. See FMEA of Main Condensate and Feedwater System, Table 5.6.
	o Startup feedwater control valve fails open or fails to close.	Same as above.	Same as above.

The impact on RCS overcooling depends on the rate of release of reactor coolant. The more common small leaks may not result in overcooling, as defined, if the makeup system is capable of injecting coolant at the tube leak rate. However, the less frequent tube rupture transients resulting in a leak rate of hundreds of gallons per minute are small LOCA's. In addition to the direct effects of the release of reactor coolant, steam generator tube rupture procedures typically require a rapid cooldown and depressurization of the RCS. Under these conditions, the potential for an overcooling transient resulting from improperly controlling the RCS cooldown exist even for smaller tube leak rates.

RCS overcooling transients resulting from increased steam generator heat transfer rate have been identified in Table 5.4, Items 2 and 3. In either case, however, the initiating control system failures occur in the main steam or main feedwater systems. These failures are considered, in detail, in the FMEA's of the Main Steam and Turbine Bypass System and the Condensate and Main Feedwater System discussed in Sections 5.2.1 and 5.2.2.

5.2 POWER CONVERSION SYSTEMS

As discussed in Section 5.1.3, the increased steam generator heat transfer RCS overcooling mechanism can be initiated by failures in the main steam and main feedwater systems. Specific failures in these systems leading to potential RCS overcooling are discussed in Sections 5.2.1 and 5.2.2.

5.2.1 Main Steam and Turbine Bypass System

The principal effect of failures in the main steam and turbine bypass system on RCS overcooling is the potential for depressurizing the steam generators. As discussed in Section 3, reducing the steam generators' pressure reduces the saturation temperature on the secondary side of the steam generators and increases the heat transfer rate from the RCS. Failures in the main steam and turbine bypass system depressurizing the main steam system and the resulting effects on the RCS are listed in Table 5.5. The information in this table was extracted from more general FMEA's of the Power Conversion Systems which are presented in Appendix C.

TABLE 5.5. SUMMARY OF MAIN STEAM AND TURBINE BYPASS FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING

Failure	Possible Causes	Effects	Remedial Actions
<u>Depressurization of Main Steam System</u>			
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 ^o 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 and 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.

TABLE 5.5. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
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.
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 valves and manually control. Close isolation valve MS-26 if required to limit 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-26 as required to control RCS cooldown rate.

TABLE 5.5. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
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 KI 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 - PO-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.
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. Feed-water 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.

TABLE 5.5. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
Contributing Failures			
10. Failure of Turbine Bypass or Startup Header Isolation Valves (MS-17, 26, 24, 33)	Mechanical failure of valve or operator, loss of electric power to valve.	Failure of normally open isolation valves may remain undetected during normal operation. Under these conditions, an open startup header or turbine bypass flow-path could not be isolated.	Identify and repair open valve. If a steam release should occur, follow emergency procedures for a steam line break.
11. Failure of a CRDCS Turbine Trip Contact to Open on Demand	Contact "sticks" in position.	The redundancy of turbine trip contacts would provide a turbine trip signal. However, failure of a contact would reduce the available redundancy.	Identify the closed contact and repair. This failure would be difficult to identify and may remain undetected for a significant period of time depending on the testing procedurally required.

The failures potentially resulting in depressurization of the main steam system include failures 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 sixteen main steam code safety valves (eight valves per steam generator) are spring loaded valves that open due to high steam pressure on the valve seat. As the steam pressure decreases, the valves automatically close due to the force of the springs on the valve seats. Following turbine trip, some of the safety valves are expected to open. Improper valve maintenance could result in one or more safety valves failing to close at their (closure) setpoint 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 steam generator 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, both valves on either steam line and, potentially, all four valves. Failure of a single valve open or its failure to close (Items 2 and 4) could be caused by a mechanical failure of the valve, its pneumatic operator or the associated E/P transducer. Failure of both valves on either steam line to open or their failure to close (Items 3 and 5) would be caused by failures in the common control instrumentation strings.

Two failure modes were identified which potentially could cause all four valves to open. Failure of the pressure setpoint module common to both instrument strings (Item 6) could result in both instrument strings signalling the four turbine bypass valves to open. The second failure mode resulting in the four turbine bypass valve failing to close (Item 7) 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 to transfer the turbine bypass valve to manual control. The valves would then remain in their existing position. If

the power failure occurred immediately following turbine trip, the four turbine bypass valves would be open and thus remain open. For the case of this particular power supply failure, the main feedwater control valves also transfer to manual and remain open (see Table 5.6).

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.

For 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 steam generators. 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 steam generator depressurization. However, the potential for such a transient to occur, while believed to be very unlikely, remain unevaluated due to unavailability of turbine control instrumentation design information. Following reactor trip, contacts in the 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. Whether other parameters input to the turbine controls (e.g., turbine speed) would override the ICS signal and maintain the turbine throttle valves open is

unknown. However, should the turbine trip and throttle valves fail to close following a reactor trip, RCS overcooling potentially could occur.

Two failures have been identified which would result in an immediate steam line depressurization but could increase the severity of other subsequent failures (Items 10 and 11). The failures identified are failures of the turbine bypass valves' isolation valves and a failure of a CRDCS turbine trip contact. It is believed that either failure could occur and remain undetected for a significant period of time.

5.2.2 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 steam generators. Following reactor trip, the potentially rapid increase in steam generator inventory is expected to result in RCS overcooling until manually or automatically terminated. Specific failures in the Condensate and Main Feedwater System leading to overfeeding the steam generators and the overall effects of these failures are identified in Table 5.6 and discussed below.

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

Failure of one of the two control valves to the open position 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 feedwater control circuit (Item 1). In the event one of the control valves failed open, the operator has the option of manually closing the main valve and controlling the startup valve, if possible, or tripping the main feedwater pumps. If the operator fails to control main feedwater flow, the main feedwater pumps will be tripped automatically on high level in either steam generator. The extent of RCS overcooling prior to automatic pump trip is unknown.

TABLE 5.6. SUMMARY OF CONDENSATE AND MAIN FEEDWATER PMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

Failure	Possible Causes	Effects	Remedial Actions
<u>Excessive Addition of Feedwater to Steam Generators</u>			
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.

TABLE 5.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	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.
2. Main Feedwater Control Valves FDW-32 and/or FDW-41 Fail Open	Power to selected startup level transmitter fails (ICS Panelboard K1, 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.

TABLE 5.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
3. Main Feedwater Control Valves FDW-32 and/or FDW-41 Fail 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 instrument air also results in 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 fall 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.

TABLE 5.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o Loss of ICS Panelboard KI Hand Power branch (HX, HIX) or unspecified failure of feedwater control valve or operator.	Main feedwater control valves freeze in position and main feedwater pumps run back to a speed corresponding to a 0 volt signal. Turbine bypass valves close and remain closed. Initial overfilling of steam generators and possible overcooling of RCS may occur. The transient would be terminated automatically by a high steam generator level trip of the main feedwater pumps or closure of the main feedwater block valves, FDW-31 and 40.	Manually trip main feedwater pumps if required to control RCS overcooling. Transfer power supplies to Panelboard KU to retain automatic control of makeup and turbine bypass valves.
<u>Contributing Failures</u>			
4. 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.
5. 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.

TABLE 5.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
6. 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, condensate booster or hotwell pumps to terminate overfill.
7. Cracks in Condenser Resulting in Air In-Leakage	Vibration corrosion.	Increased concentrations of oxygen in condensate. If not removed by the air ejectors or in the condensate system, the out-of-specification oxygen concentrations could have a deleterious effect on the steam generator tubes in the long term.	Monitor condenser pressure and condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.
8. Condensate Demineralizer Bypass Valves Spuriously Open	Instrumentation, valve operator or maintenance failure.	Increased condensate flow bypassing demineralizers possibly resulting in out-of-specification condensate water quality. This could have a deleterious effect on the steam generator tubes in the long term.	Monitor condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.
9. Condensate Demineralizers Allowed to Operate After Depletion	Maintenance/operations failure.	This operating mode could result in out-of-specification condensate water quality. This could have a deleterious effect on the steam generator tubes in the long term.	Monitor condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.

TABLE 5.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
10. Hydrazine Feed Isolated	Unspecified (PO-115G) unavailable.	Increased concentrations of oxygen in condensate. The out-of-specification oxygen concentrations could have a deleterious effect on the steam generator tubes in the long term.	Monitor condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.

Single failures in the common loop A and B control circuitry are not expected to result in RCS overcooling due to downstream, loop specific signal modification (ICS BTU limits or RCS Tav 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 manually controlling the main and startup feedwater control valves in each loop or tripping the feedwater pumps if required.

Loss of the instrument air system or failure of selected ICS Panelboard KI branch circuits will result in the loop A and loop B main feedwater control valves failing in an "as is" position (Item 3). Loss of instrument air or failure of Panelboard KI branch HX, H1X (ICS Hand Power), result in the feedwater control valves failing as is, the turbine bypass valves closing and the reactor subsequently tripping. The resulting steam generator overfeed transient is terminated by manual or automatic trip of the main feedwater pumps. Failure of Panelboard KI branch H, H1 (ICS Auto Power) results in many plant components, including the feedwater 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 manually trip the reactor. Once the reactor is tripped, the steam generators will be initially overfed. The operator has the option of manually controlling the feedwater control valves or tripping the feedwater pumps. The feedwater pumps will be automatically tripped on high steam generator level if the level is not manually controlled. As noted in Table 5.6 and 5.5, if the loss of Auto Power occurred following a turbine/reactor trip transient, the turbine bypass valves would be open. The loss of Auto Power, in this case, would transfer the turbine bypass valves to manual control while they were open. This could result in a combined steam generator depressurization, steam generator overfeed transient initially. The operator can manually control both the turbine bypass and feedwater control valves. If required, to control steam generator level, the operator may trip the main feedwater pumps and verify the automatic initiation and control of emergency feedwater.

In addition to Condensate and Feedwater system failures which directly result in overfeeding the steam generators, a number of failures could increase the severity of a transient in combination with other failures. These contributing failures are listed in Table 5.6, Items 4 through 10.

Of the failures listed, possibly the most significant is the failure of the automatic high steam generator level main feedwater pump trip. This failure, Item 4, in combination with steam generator overfeed failures (Items 1, 2, and 3), could result in the introduction of significant quantities of water into the steam lines unless the overfeed was manually terminated by the operator. The specific effects of overfilling the steam generators have been addressed in Reference 9. These effects include, in addition to the increased severity of RCS overcooling, possible damage of the main steam safety and turbine bypass valves and significantly increased stresses imposed 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 5). Following a trip of the four pumps, the control of the startup feedwater valves transfers to the operate range level transmitters at a 20 foot steam generator level setpoint. This action alone may produce some degree of RCS overcooling. However, the increased level is required to promote material circulation in the RCS and the rate of increase in steam generator would be less rapid than following transients initiated by the main feedwater valves failing open or failing to close. If the selected operate range level transmitter on either steam generator were in a failed low state, the feedwater flowrate to the affected steam generator would continue beyond the 20 foot level setpoint and the automatic steam generator high level feedwater pump trip would be defeated.

Other contributing failures include failure of the main feedwater block valves and failures potentially resulting in exceeding feedwater chemistry

specifications. As noted in Table 5.4, adverse feedwater chemistry could contribute to long term degradation of the steam generator tube integrity.

5.3 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 the RC pumps' seal injection flow.

A detailed FMEA of the MU&P system has been performed and the effects of MU&P equipment failures identified (Reference 8). The MU&P failures potentially affecting RCS overcooling have been summarized in Table 5.7.

The failures listed result in or contribute to the release of reactor coolant RCS overcooling mechanism. An isolatable small LOCA can result from a letdown cooler tube failure (Item 1). Two failures (Items 2 and 3) have been identified which contribute to the potential for a small LOCA. If a drain path from the standby letdown cooler were left open following maintenance, the failure may remain undetected since 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 would result in automatic isolation of letdown flow. If the letdown storage tank (LST) was allowed to drain resulting in damage to the operating HPI pumps or the HPI pumps were manually tripped to protect them, a simultaneous loss of RC pump seal injection and cooling water flow would occur. As identified in Table 5.3, this condition could lead to RC pump seal failures.

For the three MU&P failures listed, 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 ESPS setpoint 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 LOCA's.

TABLE 5.7. SUMMARY OF MAKEUP AND PURIFICATION SYSTEM FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

Failure	Possible Causes	Effects	Remedial Actions
<u>Release of Reactor Coolant</u>			
1. Letdown Cooler Tube Failure	Corrosion, stress on tubes.	Isolatable small LOCA or RC leak. Prior to ESPS 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.
<u>Contributing Failures</u>			
2. Open Letdown Cooler Drain Path	Undetected, improper maintenance resulting in open drain path from an isolated cooler and subsequently placing the cooler into operation.	Isolatable small LOCA or RC leak. Prior to ESPS 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.
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.

6.0 REFERENCES

1. A Ranking of Nuclear Plant Systems for Failure Modes and Effects Analysis, ORNL #62B-13819C/62X-30, SAI #1-245-08-492-02, December 31, 1982.
2. Final Safety Analysis Report, Duke Power Company Oconee Nuclear Station.
3. Oconee 1 Electrical Distribution Control and Protection Design Features, ORNL Letter Report, March 29, 1984.
4. Failure Modes and Effects Analysis of the ICS/NNI Electric Power Distribution Circuitry, SAI #1-147-08-701-00, March 1984.
5. In addition to plant specific studies of safety systems performed and reported in FSAR's, numerous generic safety system studies have been sponsored by the U.S. NRC such as the Auxiliary Feedwater and Residual Heat Removal System evaluations.
6. Failure Modes and Effects Analysis of the Pressurizer and Associated Equipment, SAI Letter Report, May 31, 1983.
7. Instruction Book for Integrated Control and Non-Nuclear Instrumentation Systems, Oconee Nuclear Plant, Unit 1, Bailey Meter Company, March 15, 1977.
8. Failure Modes and Effects Analysis for the Oconee 1 Nuclear Power Station Makeup and Purification System, ORNL #62B-13819C/62X-30, SAI #1-147-08-492-00, October 28, 1983.
9. Nuclear Power Plant Steam Generator Overfill Resulting from Control Action, F. H. Clark, N. E. Clapp, R. Broadwater, NUREG/CR-3692, ORNL/TM-9061, February 28, 1984.

APPENDIX A

OCONEE 1 SYSTEMS NOT SELECTED FOR RCS OVERCOOLING ANALYSIS

APPENDIX A

OCONEE 1 SYSTEMS NOT SELECTED FOR RCS OVERCOOLING ANALYSIS

System ID	System Name	Potential Impact on RCS Overcooling
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 overcooling apparent.
N05.D	Post-Accident Sampling System	System only operates in the post-accident, RCS shutdown mode. No impact on RCS overcooling 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 overcooling.
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 overcooling.
N09	Emergency Feedwater Control System	System potentially may have a significant impact on RCS overcooling but it is a safety system and beyond the scope of this study.

APPENDIX A (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
S01	Engineered Safeguards Protective System	Engineered safeguards systems may have significant impacts on RCS overcooling but are safety systems and beyond the scope of this study.
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	
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 overcooling 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. Other impacts on RCS overcooling apparent.

APPENDIX A (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
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 overcooling are apparent.
P03.A	Main Condenser Evacuation System	The function of the evacuation system is to remove non-condensable gases from the condenser. Failure of the system may result in turbine trip; however, no impacts on RCS overcooling are apparent.
P05	Emergency Feedwater System	The emergency feedwater system may have significant impact on RCS overcooling. 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 overcooling are apparent.

APPENDIX A (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
W01	Radioactive Waste System	The redirective waste system collects and processes redirective materials prior to reuse or disposal. Interfaces with the RCS are isolated during operation. No impacts on RCS overcooling are apparent.
W02	Radiation Monitoring System	The radiative monitoring system detects the release of radioactivity. No impacts on RCS overcooling are apparent.
W04.B	High Pressure Service Water (HPSW) System	The HPSW is a safety system designed to suppress plant fires and serve as a backup to the LPSW. No impacts on RCS overcooling 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 overcooling 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	

APPENDIX A (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
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 overcooling are apparent.
W07.A	Service Air System	
W08	Plant Gas System	
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	

APPENDIX B

OCONEE 1 POWER CONVERSION SYSTEMS PROCESS AND INSTRUMENT DIAGRAMS

(LATER)

APPENDIX C

OCONEE 1 POWER CONVERSION SYSTEMS

FAILURE MODES AND EFFECTS ANALYSIS TABLES

(LATER)

DESIGNATED ORIGINAL

JUN 20 1984

DVB

PDR

NUREG/CR-3692
ORNL/TM-9061
NRC Dist. R1

Instrumentation and Controls Division

POSSIBLE MODES OF STEAM GENERATOR OVERFILL
RESULTING FROM CONTROL SYSTEM MALFUNCTIONS
AT THE OCONEE-1 NUCLEAR PLANT

F. H. Clark
N. E. Clapp
R. Broadwater*

Manuscript Completed: February 28, 1984

Date Issued

*Tennessee Technological University, Cookeville.

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

NRC Fin No. B0467

Prepared by the
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831
operated by
UNION CARBIDE CORPORATION
for the
U.S. DEPARTMENT OF ENERGY
under Contract No. W-7405-eng-26

CONTENTS

1. Introduction.....	1
1.1 General Considerations.....	1
1.1.1 Work Scope.....	1
1.1.2 Related Work Efforts.....	1
1.1.3 Approach to Program.....	1
1.1.4 Outline of This Report.....	2
1.2 Steam Generator Overfill Summary.....	3
1.2.1 Scope of Steam Generator Overfill.....	3
1.2.2 Principal Results of Steam Generator Overfill Study.....	3
1.2.3 Methods Used.....	4
1.2.4 Effects of Steam Generator Overfill.....	4
2. Description Of Once Through Steam Generator.....	5
2.1 Functional Design of Steam Generator.....	5
2.2 Steam Generator Controls.....	8
2.2.1 Operating Control.....	8
2.2.2 Steam Generator Level Limits and Sensors.....	14
2.2.3 High Level Main Feedwater Pump Trip Circuitry.....	17
3. Systems Selected.....	19
4. Control System Failures That Contribute To Steam Generator Overfill.....	21
4.1 Classification of Failures.....	21
4.2 Detailed Description of Failure Sequences.....	25
4.3 Simulation Recommendations.....	34
5. Possible Consequences of Steam Generator Overfill.....	35
5.1 Direct Primary Side Effects.....	35
5.2 Possible Secondary Side Damage.....	36
6. Tentative Conclusions.....	38
References.....	39
Appendix A - Information Sources.....	40
Appendix B - Steam Generator Tube Problems At Oconee 1.....	43
APPENDIX C - Review of Draft By Duke Power Co.....	44

ABSTRACT

A study has been made of control system failures which might lead to overfill of the steam generator in Babcock and Wilcox nuclear plants. The steam generator and its control system are described. Only one sequence has been found in which a single failure would lead to overfill, and in that case the final stages of the overfill would proceed rather slowly. Because of high level protective features all other failure sequences we have examined require at least two failures to produce overfill beyond the point of high level protection. Several sequences are described in which high level protection features can be placed in an undetected failed state by a control system failure; a subsequent additional failure, occurring prior to the detection and correction of the first failure, could then produce system overfill. Mechanical damage is identified which might be consequent upon steam generator overfill and water entry into the main steam line. Several ways of reducing the probability of steam generator overfill are suggested. No assessment has been made of the probability of occurrence of any of the sequences.

1. INTRODUCTION

1.1 GENERAL CONSIDERATIONS

1.1.1 Work Scope

This work is conducted for the U.S. Nuclear Regulatory Commission (NRC) under FIN No. B0467, Safety Implications of Control Systems. It supports the resolution of Unresolved Safety Issue A-47. The purpose of this contract is to determine whether nuclear power plant control systems, either in designed interaction or in credible malfunction, may interfere with the action of safety systems or may put the plant into a failed state beyond the protection of the safety systems. The effort at Oak Ridge National Laboratory is limited to the study of Babcock and Wilcox Co. and Combustion Engineering Co. plants. Plants designed by other vendors are under study at the Idaho National Engineering Laboratory (INEL). The study is, therefore, intended to be generic by vendor. Because it is recognized that detailed and realistic plant descriptive information is essential for a study of this sort, data from two existing nuclear power plants, Oconee-1 and Calvert Cliffs-1, were used to represent the designs of Babcock and Wilcox and Combustion Engineering respectively. While some elements of the study may be unavoidably plant specific, the thrust of the study as a whole is generic. Work to date covers only the Babcock and Wilcox design as represented by Oconee-1.

1.1.2 Related Work Efforts

A number of other activities supported by NRC are related to or develop information related to this work. We have maintained close liaison with them. Included among them are:

- a. Plant Electrical System Evaluation, FIN B0816
- b. Evaluation of Pressurized Thermal Shock, FIN B0468
- c. Precursors to Potential Severe Core Damage Accidents, FIN B1583
- d. In Plant Reliability Data Base For Nuclear Plant Components, FIN B0445.
- e. System Interactions In Nuclear Power Plants, FIN B0789

1.1.3 Approach to Program

The general approach to this problem at ORNL is twofold: (1) a study of scenarios which could lead to control system initiated plant failures, produced in the failure mode and effects (FMEA) format, and based on plant design and procedure information, and (2) the supportive development of a hybrid computer model for simulation of the nuclear power plant. The plant simulation details much more explicitly than is customary the plant control system and its capabilities and effects. The simulation will examine in detail important cases generated in the FMEA study. The simulation will be described fully in another report.

The FMEA study, as it relates to the Babcock and Wilcox steam generator overflow problem, is the subject of this report, and the remainder of this report will deal with it.

1.1.4 Outline of This Report

Section 1, this section, the Introduction, deals with general program objectives and with some of the results of this study. Section 2 is concerned with description of the Steam Generator and its controls. Section 3 relates what systems received the most emphasis and why. Section 4 presents the failure modes considered along with some possible failure scenarios. The more casual reader might wish to skip some of the material in Section 2 through 4, but should in no event skip Section 2.2.2, 2.2.3, or 4.1. Section 5 considers some possible consequences of a Steam Generator overfill; Section 6 makes some observations about possible design or procedure changes if they are felt to be necessary.

The Appendices A, B, and C deal, respectively, with Information Sources, past Steam Generator tube problems at Oconee 1, and a review by Duke Power Co. of an early draft of this report.

1.2 STEAM GENERATOR OVERFILL SUMMARY

1.2.1 Scope of Steam Generator Overfill

There are four conditions of Steam Generator misoperation of interest to this project.

- a. Overfeed of the Steam Generator to the point where liquid water issues from its outlet. We shall consider this overfill.
- b. Overfeed of steam generator beyond pump trip level. We shall consider this overfill.
- c. Overfeed of the Steam Generator without exceeding pump trip level. However, primary coolant temperatures are lowered and thermodynamic conditions at the turbine inlet may be off their operational norms. We will consider this overcool.
- d. Underfeed of the Steam Generator. Primary coolant temperatures are increased, and thermodynamic conditions at the turbine inlet may be off their operational norms. In severe cases the Steam Generator may dry out.

This report will concern itself principally with (a) and (b). Succeeding reports will deal with (c) and (d).

1.2.2 Principal Results of Steam Generator Overfill Study

The following are the major results of the Steam Generator overfill study.

- a. There are two high level protection features: a high level Main Feedwater pump trip and a high level Main Feedwater control valve closure. The system will not overfill under Main Feedwater action unless these features are defeated. They do not act on the Auxiliary Feedwater. (See Sect. 2.2.2 and 2.2.3).
- b. Both the above protection features receive level indication from the same instrumentation. They are, therefore, subject to common cause failure (See Section 2.2.2).
- c. The Main Feedwater pump trip circuitry is separate from the Integrated Control System (ICS). Hence, a failure in this circuitry would affect the pump trip but not the high level control valve closure which is governed by the ICS. There are several ways that the pump trip circuitry can be placed in undetected failed state. (See Sect. 2.2.3).
- d. A low level indication overrides the high level control valve closure signal and creates a flow demand signal.

- e. A sufficient leak in the selected low level pressure tap, or its connecting pipe, or the packing of either blocking valve to which it connects can lead to Steam Generator overfill by the Auxiliary Feedwater system (AFW). Such an overfill would be the result of a single failure. However, overfill by the AFW proceeds more slowly than overfill by the MFW, affording more time for corrective measures. The water pumped by the AFW, having less velocity, is likely to cause less mechanical damage than water from the MFW might.

All MFW overfill scenarios we have found require more than one failure. We have identified a number which are brought about by two failures, the first of which leaves part of the system in an undetected failed state. (See Section 4.1).

1.2.3 Methods Used

Initially over one hundred plant systems were screened to estimate their probable importance to Steam Generator overfill. They were classified according to:

- a. potential to be the proximate cause of SG overfeed
- b. potential to disable high level protection systems
- c. potential to affect the function of (a) or (b) type systems
- d. whether they are administratively removed from consideration, (by reason of being dealt with in other contracts).

This classification is dealt with in Section 3.

The systems identified as important were then subject to intensive study. Among the most important systems were the Integrated Control System, the Non Nuclear Instrument System, the Feedwater system, the Main Steam system, the Reactor Coolant system, and the Instrument Air system.

1.2.4 Effects of Steam Generator Overfill

The assessment of mechanical damage is not a part of the scope of this project. We have, however, indicated some areas on the secondary side that would be subject to unusual stresses and possible damage in the event of a serious overfill. See Section 5. Direct primary side effects stemming from Steam Generator overfill would initially be an overcooling and would require simulation for adequate assessment.

2. DESCRIPTION OF ONCE THROUGH STEAM GENERATOR

This section describes the functional design and the controls of the Steam Generator.

2.1 FUNCTIONAL DESIGN OF STEAM GENERATOR

The Once Through Steam Generator (OTSG) is a straight-tube, straight-shell heat exchanger. The reactor coolant is on the tube side, and the secondary fluid is on the shell side. The reactor coolant from the reactor outlet enters the 36-in. OTSG primary inlet nozzle at a temperature of about 603°F. The reactor coolant gives up heat to the secondary fluid as it flows through the tubes and leaves through the two 28-in.-i.d. outlet nozzles at a temperature of 555°F.

The tubes are supported by tube support plates which have broached openings to permit flow between the plate and the tube. The support plates are fixed longitudinally by a system of support rods that are welded to the lower tubesheet. Spacer tubes are installed over the support rods between each pair of adjacent support plates. This system permits positive placement of the supports within the cylindrical baffle.

The cylindrical baffle comprises two pieces: the lower section is bolted to the bottom tubesheet, and the upper section is welded to the shell just below the steam outlet nozzles. Alignment pins hold both sections radially in the shell.

Feedwater enters the OTSG through 32 spray nozzles connected to the 14-in.-o.d. main feedwater header. The condensing action of the cold feedwater (455°F at full load) draws steam through the circumferential space between the upper and lower cylindrical baffles. This steam heats the feedwater rapidly to the saturation temperature of about 535°F; this prevents thermal shocking of the shell. The flow of bleed steam is inherently self-regulating. Any change in feedwater flow changes the rate of condensation, thus changing the rate of bleed steam flow.

A mixture of saturated steam and water forms in the downcomer of the OTSG. The level and density of the downcomer fluid are set by the static head and pressure drop between the bottom of the tube nest and the bleed point. There is an adjustable orifice in the lower section of the downcomer to ensure the dynamic stability of the recirculated loop. The fluid enters the tube nest through the ports in the lower portion of the cylindrical baffle (or wrapper). Since the fluid is at saturation temperature it begins to boil as soon as it comes in contact with the hot tubes. The boiling fluid flows upward in counterflow with the primary fluid.

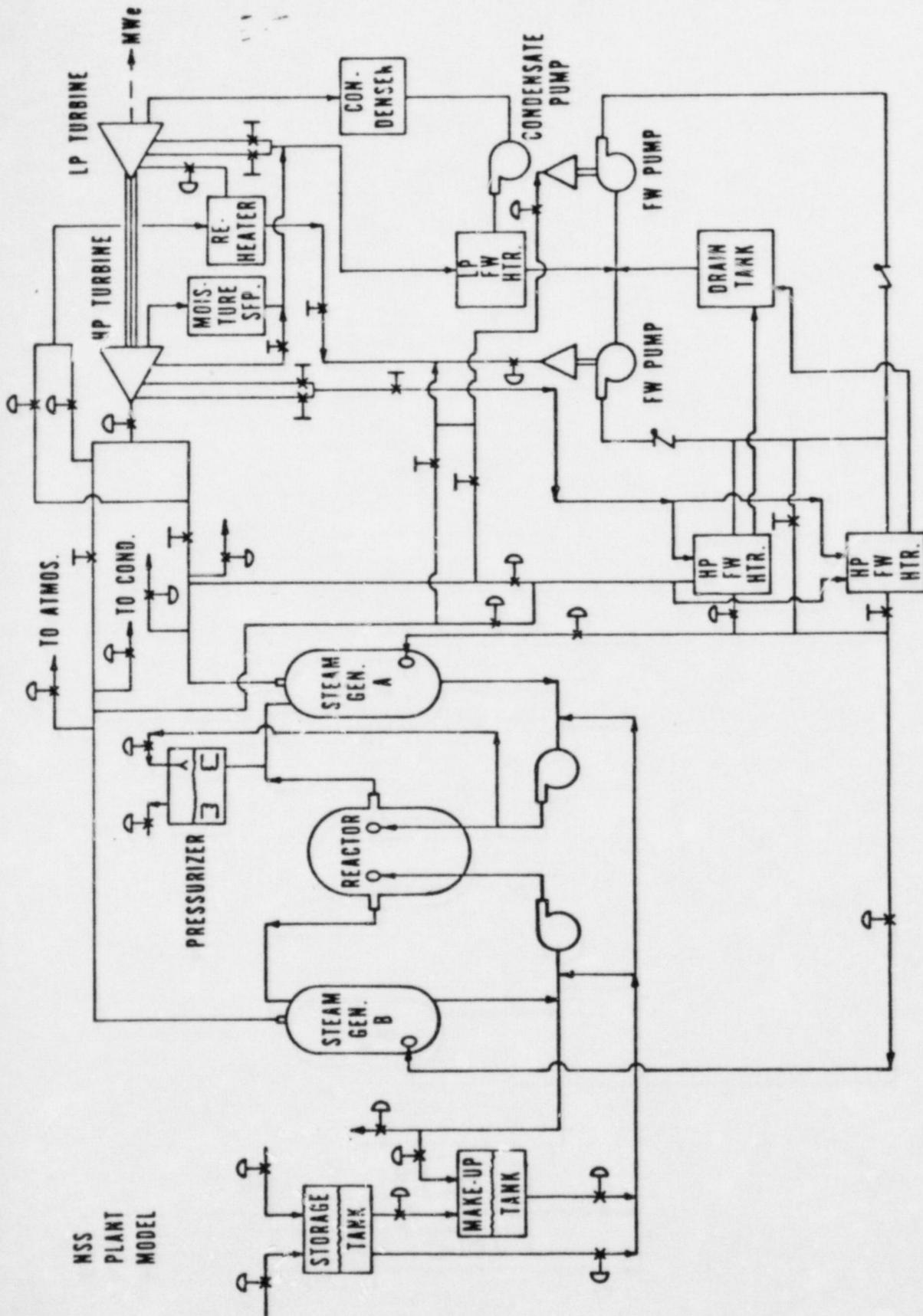
The boiling taking place in the lower section is in the regime called nucleate boiling. The tubes are wetted and small bubbles rapidly form and break away from the surface. Nucleate boiling provides a very high heat transfer

coefficient because of the turbulence resulting from bubble formation. Most of the heat is transferred in this region of the boiler. Nucleate boiling continues until enough water has vaporized to allow a blanket of superheated steam to form on the tubes; this condition is called film boiling. The steam blanket forms gradually as the steam quality reaches a high value. It is fully developed in only a very short section of the boiler.

The steam quality at the top of the film boiling region is 100%. This saturated steam is then heated to at least 35°F above saturation temperature in the superheat section of the boiler. The full-load steam temperature at the outlet nozzle will approach 590°F with a clean boiler; the steam temperature will change as the boiler fouls. At the top of the tube nest the steam flows into the annulus between the upper wrapper and the shell. The steam heats the upper part of the shell to the steam temperature; this minimizes the tube-to-shell temperature difference. The steam exits through the two 24-in.-i.d. steam outlet nozzles.

The steam generator is fed water from the feedwater systems, main or auxiliary, and heat from the primary loop. It is built to operate with liquid water and steam each occupying approximately half of its secondary side volume. If the pumps and valving systems which supply water to the steam generator supply it at a rate greater than the heat from the primary side is able to vaporize it, the steam generator will begin to overflow. Hence, the proper operation and control of the steam generator depends upon a balanced flow of mass through the secondary loop and energy from the primary to the secondary loop.

Figure 1 is an outline sketch of the thermohydraulic aspects of the pressurized water reactor system of the Oconee plant. Much of it would apply to any B&W PWR system. Generally, the lower half of the diagram along with the secondary sides of the steam generators comprise the feedwater 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. In each loop there is a startup valve and a main FW valve in parallel. There is a flowmeter in the startup leg sensitive to low flows, and downstream beyond where the two legs have come together is a flowmeter receiving the combined flow through both valves. This meter may be relatively inaccurate at low flows.



NSS
PLANT
MODEL

LEGEND

-  CONTROL VALVE
-  STOP VALVE

Fig. 1. B&W Thermohydraulic System Schematic

2.2 STEAM GENERATOR CONTROLS

2.2.1 Operating Controls

Control of the feedwater system is provided through the MFW and start up valves and the FW pump speed. Sensed signals which are sent to the Integrated Control System (ICS) and there processed to produce control signals for the FW system include the following:

1. Feedwater 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. Reactor coolant average temperature error
11. Pressure drops across FW valves

In maintaining total feedwater flow equal to total feedwater demand, the Feedwater Control subsystem manipulates two start-up valves, two main valves, and two pumps. The Feedwater Control includes the following considerations, each of which will be discussed below (see Figure 2 - all references to Points and Blocks are on Figure 2):

normal control mode

feedwater temperature compensation

high and low cross limits with the reactor power level

T_{AVG} control to feedwater

correct feedwater flow ratio between the two steam generators for control of inlet reactor temperatures

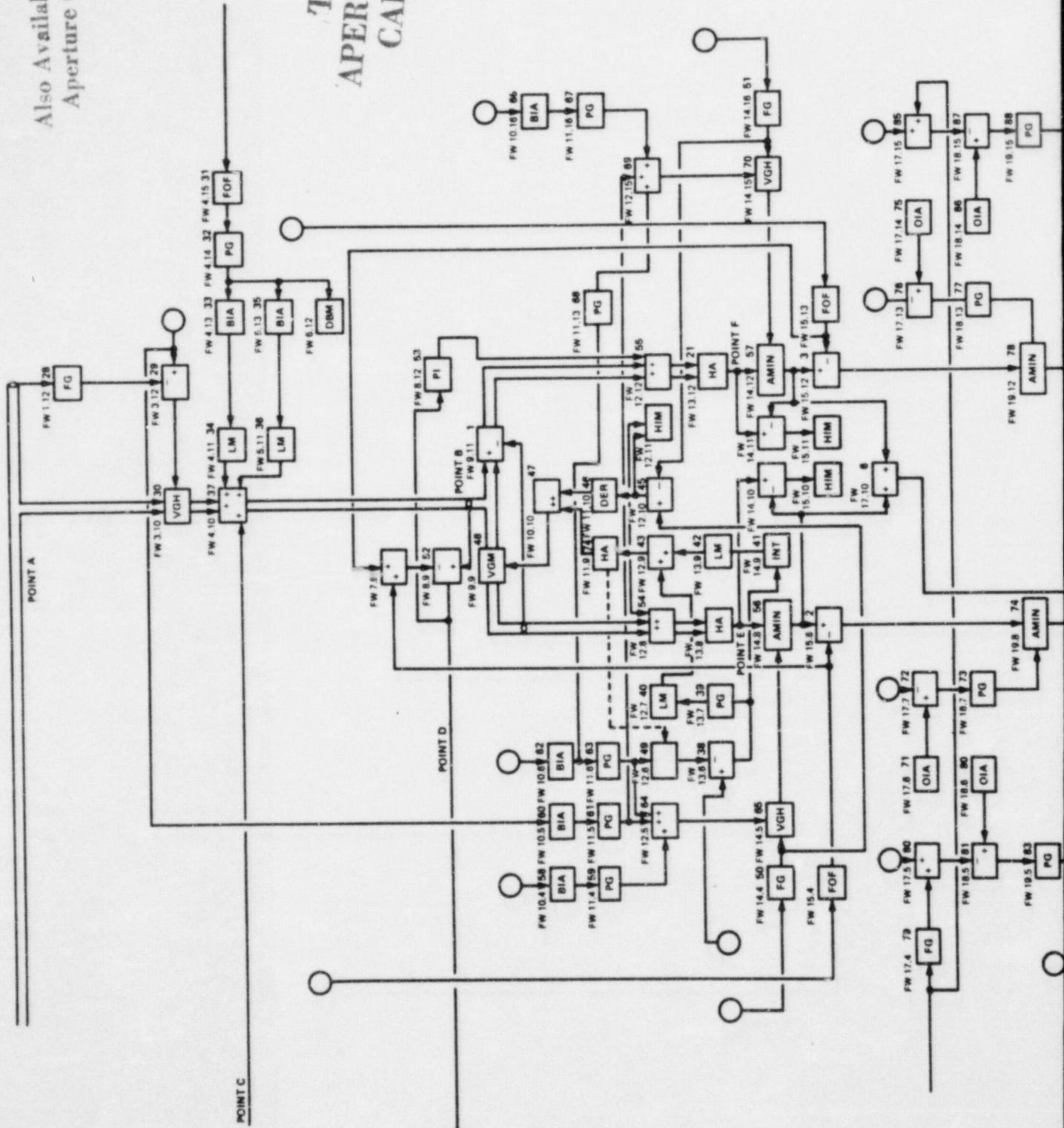
total flow control on large reactor coolant flow error

minimum steam generator degrees superheat limits

minimum and maximum steam generator level limits

Also Available On Aperture Card

TI APERTURE CARD



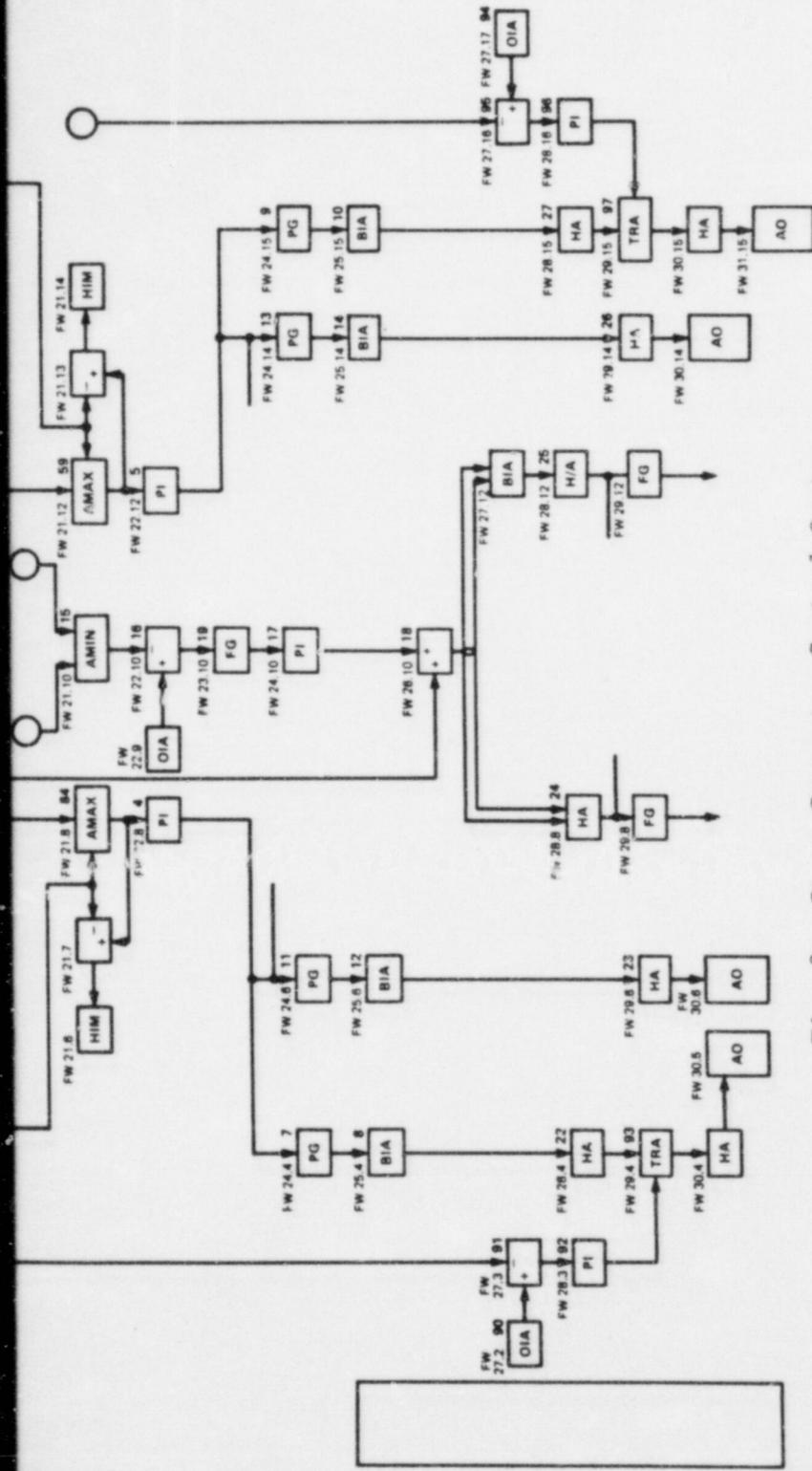


Fig. 2. Steam Generator Control System Block Diagram

8406270376-01

Legend for Fig. 2

FG = function generator
VGM = variable gain multiplier
BIA = bias
PG = proportional gain
FOF = first order filter
DBM = deadband monitor
HA = hand-auto station
DER = derivative
LM = low signal monitor
INT = integrator
AMIN1 = select minimum
OIA = operator input analog
AMAX1 = select maximum
HIM = high signal monitor
TRA = transfer
AO = analog out
PI = proportional integral controller

Normal Control Mode

In this mode, the feedwater 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, the total feedwater demand from the Integrated Master is split evenly between feedwater loops A and B (Point B and Block 1). The measured feedwater flow to each steam generator is compared with the individual loop demand; the individual (Blocks 2 and 3) feedwater errors then pass through proportional plus integral controllers (Blocks 4 and 5) to establish the control valve positions. The individual loop demands are summed together (Block 6) and used to generate a feedforward pump speed demand signal.

The operations of the start up valve and main valve in each loop are sequenced. Normally, as the loop demand varies from 0 to 15%, the start-up valve gain is adjusted to cause the start-up 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 start up valve becomes 80% open, a block valve in series with the main valve is opened, and 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 feedwater pump speed demand. The minimum pressure drop is compared with a setpoint, 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).

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

Feedwater Temperature Compensation

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

Cross Limits With Reactor

Cross limits are used to maintain the feedwater flow in percent within a certain ratio of the reactor power in percent (Blocks 31 through 36). Whenever the measured neutron power is more than 5% different from the neutron power demand, a correction is made to increase or decrease the feedwater flow demand accordingly. For instance, if the neutron power error is -7%, then the cross limits will cause the feedwater flow demand to be decreased by 2% (Blocks 33 and 34). If the neutron power error is 6%, then the cross limits will cause the feedwater 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 T_{AVG} (i.e., reactor coolant average temperature). One such condition occurs when the reactor Hand/Automatic station is in manual. When the Reactor Control subsystem cannot control T_{AVG} , conditions are satisfied, T_{AVG} control is transferred to the Feedwater Control subsystem. When this occurs 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 feedwater demand (Block 37).

Plant conditions which would prevent Feedwater Control from accepting the control of T_{AVG} are:

- both steam generators meeting level limits
- either steam generator on a Btu limit
- both feedwater Hand/Automatic master stations in manual.

Delta- T_c Control

To insure a uniform reactor inlet temperature distribution, the Feedwater Control ratios the two feedwater loop flows in such a manner as 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 $\text{delta-}T_c = T_{CA} - T_{CB} = 0$. Ratioing the feedwater flow between the two steam generators for the control of reactor inlet temperature is referred to as delta- T_c control. Both reactor coolant cold leg temperature measurements and reactor coolant flow measurements are used in implementing feedback control of delta- T_c . A variable gain is modified by the delta- T_c feedback control signals and applied to loop A feedwater demand (Block 48). The loop A demand is then subtracted from the total demand (Block 1) to create the loop B demand modified by delta- T_c feedback.

The delta- T_c setpoint is normally entered as zero (Block 49). A proportional gain, a calibrating integral, and high/low limiters operate on the cold leg temperature difference delta- T_c error (Blocks 38 through 43).

Both the proportional and calibrating integral actions are blocked if either feedwater loop Hand/Automatic station is in manual or if either steam generator 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 Hand/Automatic station (Block 44) may be used to replace the demand created by ΔT_C feedback error with manual ratioing of the feedwater flow demands.

There are four reactor coolant pumps, with two pumps operating in parallel in each loop. If an imbalance in the primary flows through the steam generators exists, as when the number of reactor coolant pumps running in each of the two primary loops are not equal, then ΔT_C will deviate from zero unless the feedwater 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 the reactor coolant flows (Blocks 45 and 46, 50 and 51). The feedbacks due to ΔT_C error and primary loop flow imbalance are summed (Block 47) to create the variable gain applied to loop A feedwater demand (Block 48).

Total Flow Control

If the reactor coolant flow error becomes greater than 10% (Point D), then the total feedwater 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 then the controller output is bled to 0% with a 60 s time constant. If steam generator A is on low level control and steam generator B is on manual control then 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 and when both steam generators A and B are on low level control.

Btu Limits

To insure steam with a minimum specified number of degrees superheat (usually $19.4^\circ\text{C}=35^\circ\text{F}$) BTU limit calculations are implemented. The BTU limits are the maximum allowable feedwater flow demands for each loop. A low auctioneer is used in implementing the BTU limits in each loop (Blocks 56 through 57). Feedwater flow demands higher than the BTU limit would result in the degrees superheat at the outlet of the steam generator falling below the minimum specified degrees superheat.

The BTU limit calculations are based upon measurements of the reactor coolant flow, primary coolant temperature at the reactor outlet, the feedwater temperature, and the steam generator outlet pressure (Blocks 58 through 70). These variables are used to determine the amount of energy available from the steam generator at the desired steam temperature. If the normal feedwater

demands (Points E and F) are calling for the removal of more energy from the steam generators than is available for the desired steam temperature, then the BTU limits override the normal feedwater demands.

2.2.2 Steam Generator Level Limits and Sensors

Low and high level limits are imposed on the operation of the steam generators. In the high level limit control, a low auctioneer is used to compare the feedwater 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 the low level limit control, a high auctioneer is used to compare the feedwater flow error against an appropriately gained start-up 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 pre-selected high and low points. Note further that a low level error signal, if present, will dominate.

Figure 3 shows a schematic of the Oconee 1 Steam Generator, water level sensing pressure taps (labeled A,A',B,B',D,D', and e), the MFW and AFW delta-P cells associated with the A,B,D taps, and the valves and pipes that connect the taps to the cells. There is an identical set of valves, cells and pipes associated with taps A',B', D'. Referenced from the bottom tube sheet as O, the tap heights are A,A' - 6 in., B,B' - 102 in., D,D' - 394 in., E - 606 in.

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

The path from each pressure tap to the (normally open) blocking valves (Figure 3) is open as shown, 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 (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 following 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. The failure would be undetected until the operator observed the inconsistency and deduced its cause.

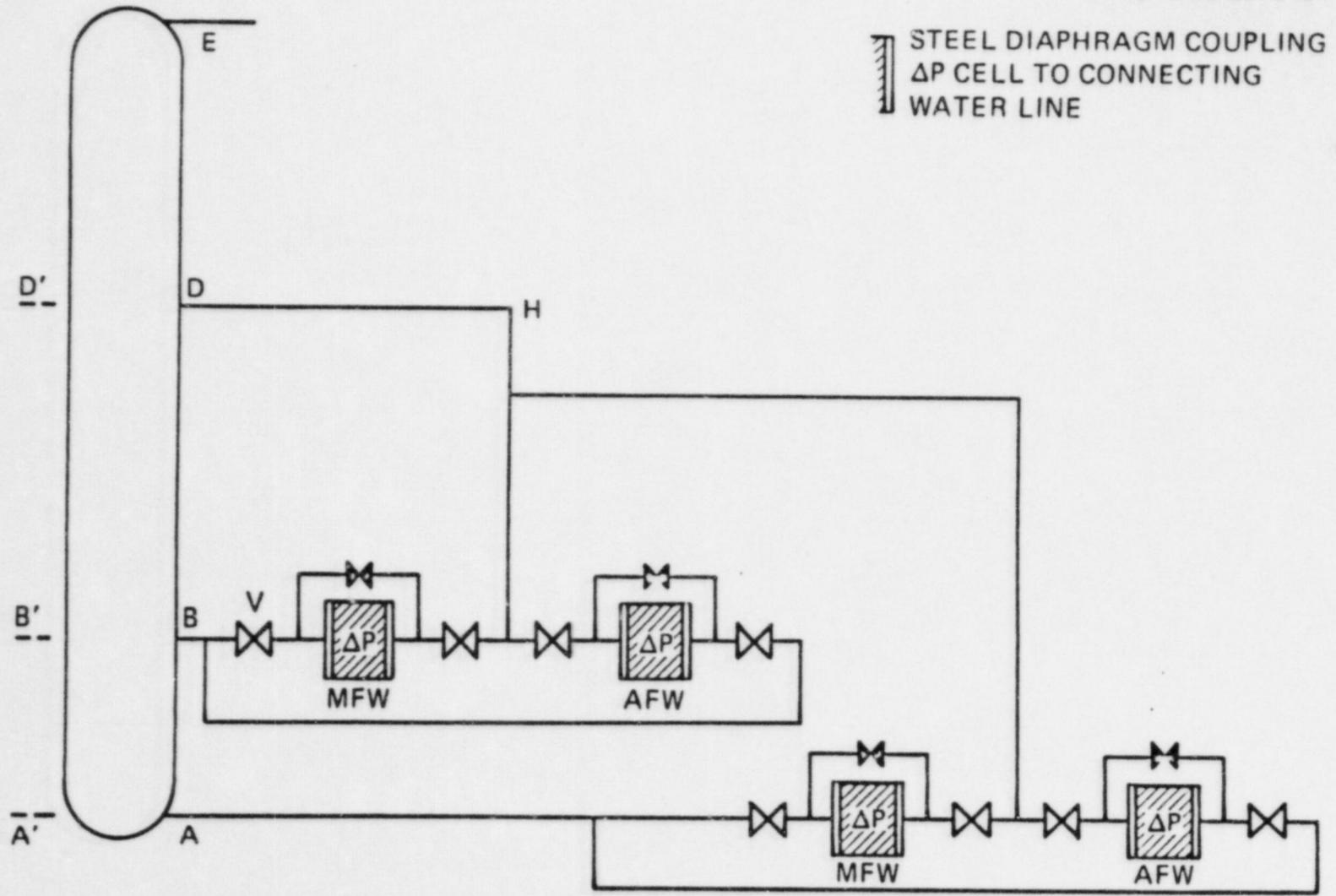
(a) sufficient leak in the selected A,A' tap or the connecting pipe or the packing of the packing of the blocking valves between the tap and the corresponding AFW or MFW delta-P cell can cause an apparent drop in the sensed

low level of the SG and bring on an overriding requirement to increase feedwater flow. This misinformation would go to both AFW and MFW controls.

(b) 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.

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

(d) The blocking valve in the selected set, marked V in Figure 3, if failed into a closed position during operation, will isolate the B-D MFW delta-P 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.¹



SCHEMATIC OF STEAM GENERATOR PRESSURE TAPS AND ΔP CELLS

Fig. 3

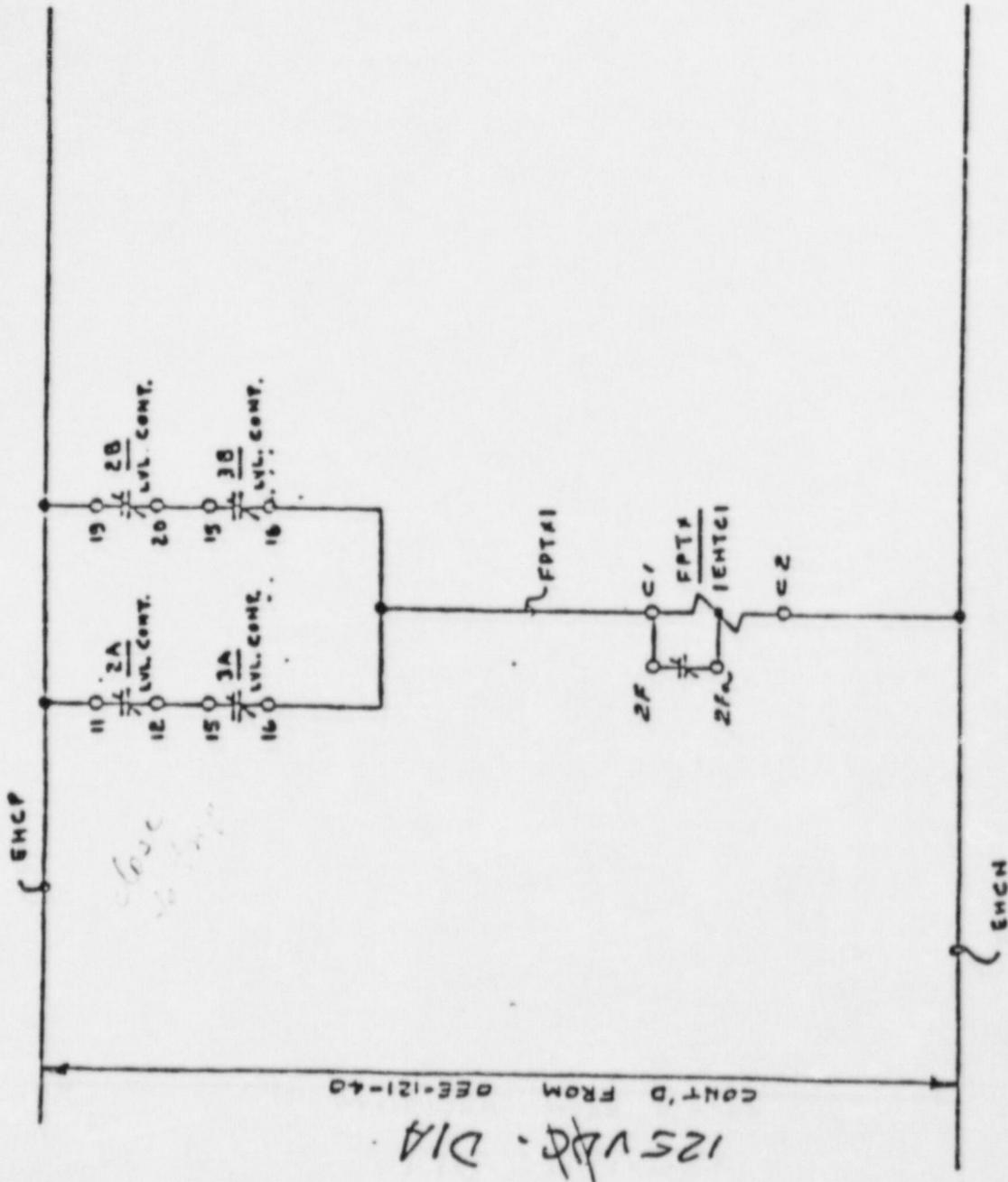
2.2.3 High Level Main Feedwater Pump Trip Circuitry

Figure 4 is a schematic 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.

(a) For purposes of high level MFW pump trip and high level alarm the signals from both pairs B-D and B'-D' are used. The signals B-D and B'-D' from SG-A (Fig.3) go respectively to contacts 2A and 3A (Fig. 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.

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

The circuitry of Figure 4 is not part of the Integrated Control System. Hence, failures within this circuitry will not fail protective features, like the high level main feedwater control valve closure, which are operated from the ICS.



125V AC - DIA
CONT'D FROM DEE-121-40

Fig. 4 High Level MFW Pump Trip Circuit

3. SYSTEMS SELECTED

Search for possible safety problems in the operation or malfunction of control systems requires deep and detailed examination of possibly offending systems or components. This is because nuclear power plants are designed with great care for safety; they are further subject to severe original and continuing scrutiny by the regulatory authorities for safe design and operation. It is therefore most unlikely that serious problems will be found with less than an in-depth search. The number of systems and components in the plant is so great that it would not be possible within allocated resources to make an in-depth study of all of them. Hence, a preliminary screening of systems was necessary to determine where the deeper effort should be applied.

Approximately 100 systems in the Oconee 1 nuclear plant were considered to determine whether they might have a significant effect on Steam Generator overfill. The systems were put into five classes as follows:

Class A - This class consists of those systems which, for administrative reasons, are excluded from consideration. It includes most safety systems and all plant electrical systems. The reason for the exclusion is that responsibility for consideration of these systems has been placed elsewhere. In the case of a few safety systems, for example, the Auxiliary Feedwater System, we have been unable to avoid some consideration. A total of 24 electrical and 7 safety systems were placed in Class A.

Class B - This class consists of systems which contain components whose function or malfunction can directly increase the pressure difference between the main feedwater pump discharge and the Steam Generator or decrease the flow of heat from the primary coolant to the secondary side of the Steam Generator. Also in this class we include the control signals which motivate such components and the control circuitry associated with them.

Class B Systems

Main Steam System	Turbine Generator System
Main Feedwater System	Turbine Bypass System
Auxiliary Feedwater System	Reactor Coolant System
Integrated Control System	

Class C - This class consists of systems which generate signals that are sent to the control systems (which, in turn, generate the signals which motivate the Class B components).

Class C Systems

Nuclear Instrumentation	Turbine Generator System
Non Nuclear Instrumentation System	Feedwater System
Main Steam System	Steam Generator
	Reactor Protection System

Class D - This class consists of systems having components whose operation or malfunction can directly affect the performance of Class B or Class C components.

Class D Systems

Cooling Water System	Essential Service Water
Reactor Bldg Service	System
Water System	Compressed Air System
Instrument Air System	Heating, Ventilation and
Reactor Core	Air Conditioning

Class E - This class contains all other systems.

Class E Systems

Control Rod Drive System	Chemical and Volume Control
Radioactive Waste System	System
Gaseous Radwaste System	Liquid Radwaste System
Solid Radwaste System	Radiation Monitoring System
Plant Area Radiation	Environmental Radiation
Monitors	Monitors
Process Radiation Monitors	Refueling System
Spent Fuel Storage System	Fuel Pool Cooling and Cleanup
Service Air System	System
Process Sampling System	Plant Gas System
Nitrogen System	Hydrogen System
Potable and Sanitary Water	Fire Protection System
System	Water System (Fire)
Carbon Dioxide System	Communication System
Control Room Habitability	Diesel Bldg Ventilation
System	System
Fuel Bldg Ventilation System	Non Radioactive Waste System
Gaseous Waste	Liquid Waste
Solid Waste	Turbine Gland Seal System
Turbine Lubrication System	Stator Cooling System
Hydrogen Seal Oil System	Condenser Evacuation System
Condensate Cleanup/Polishing	Condensate Heater Drain System
System	Feedwater Heater Drain System
Auxiliary Steam System	Nine Containment Systems

4. CONTROL SYSTEM FAILURES THAT CONTRIBUTE TO STEAM GENERATOR OVERFILL

The Oconee 1 MFW control system has an overriding requirement to feed the Steam Generator as long as the water level is sensed below low level, (36 in. on the selected A-D (A'-D') sensor - see Figure 3). Between 36 in. and 282 in. control is not based on level during normal operations. A complex of demand related signals is met by the control system. Most simple aberrations that might occur in a component are compensated by action of the Integrated Control System in this region. When the sensed level exceeds 282 in. the ICS sends a signal to close the MFW control valve. If despite this the level rises to 394 in. a signal is sent by circuitry outside the ICS (see Figure 4) to trip the MFW pumps. Note that this last signal will cause actuation of the trip only if signals are sent from both the B-D and the B'-D' sensor sets. (See Sections 2.2.2 and 2.2.3.)

It is apparent, therefore, that the MFW cannot overfill a Steam Generator (above the 394" level) unless both high level protection features are defeated and an overfeed mechanism is initiated which is not controlled by cross limits or any of the other compensatory features of the ICS. We have accordingly classified possible failures as they may cause one or another of these.

The Auxiliary Feedwater system (AFW) 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. There must have been a prior failure or unusual circumstance to bring on the AFW. And the AFW pumps water much more slowly than the MFW with 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.

4.1 CLASSIFICATION OF FAILURES

Type A - Failures Which Place Both The High Level MFW Pump Trip and The High Level Control Valve Closure In Failed State - Since both these systems depend on the same level detection equipment, a failure there would affect both equivalently.

- a. a sufficient leak in selected pressure tap B (B') or connecting pipe from it or packing of either blocking valve on which the connecting pipe terminates - 2.2.2, b
- b. failure of valve V (Figure 3) of the selected set in the closed position during operation - 2.2.2, c
- c. any failure of the selected B-D (B'-D') MFW delta-P cell, mechanical, hydraulic, or electrical, which causes the cell to read a low level when the level is high - 2.2.2, d

Further description of these failures appears in Section 2.2.2. As observed there, since these are failures of level indications of the selected set, the indications are brought to the control

room display where they are inconsistent with other level indications displayed there. The failure should be detected when the operator notices and understands the inconsistency.

Type B - Failures Which Place The High Level MFW Pump Trip In 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 non-selected B-D (B'-D') set.

- a. Any failure causing relay 2A or 3A (Figure 4) to fail with contacts open places SG-A pump trip in undetected failed state. Analogously, 2B and 3B for SG-B. 2.2.3, a
- b. Any failure causing relay FPTX (Figure 4) to fail with contacts open will put trip signals of both SGs in undetected failed state. 2.2.3, b
- c. A sufficient leak in non selected pressure tap B (B') or connecting pipe from it or packing of either blocking valve on which the connecting pipe terminates - 2.2.2, b
- d. Failure of valve V (Figure 3) of the non selected set in the closed position during operation - 2.2.2, c
- e. Any failure of the non selected B-D (B'-D') MFW delta-P cell, mechanical, hydraulic, or electrical, which causes the cell to read a low level when the level is high - 2.2.2, d

Failures a and b are undetected by their nature. Failures c, d, and e are undetected because they are failures of the non selected set which is not displayed in the control room.

Type C - Failures Which Block the High Level MFW Control Valve Closure and Also Initiate Steam Generator Overfeed

- a. Selected low level signal fails low. - Sect. 4.2, r; 2.2.2, a
- 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 setpoint. - Sect. 4.2 w

Type D - Failures Which May Initiate Fast Overfeed By MFW - Whether or not these failures would be controlled by the ICS and cross limits prior to challenging high levels is not clear. Simulation is required to determine this. - Sect. 4.2, q, t

- a. Delta-P measurement on FW control valve fails at 0. Sect. 4.2, a.
- b. FW temperature measurement in one loop fails high. Sect. 4.2, c.
- c. MFW flow signal fails showing no flow. Sect. 4.2, d.
- d. Hot leg temperature measurement fails high. - Sect. 4.2, g.
- e. Delta-T_C signal fails either way. - Sect. 4.2, i.
- f. T_{AVG} determination fails high. - Sect. 4.2, j.
- g. Neutron flux measurement fails high. - Sect. 4.2, k.
- h. MFW blocking valve position indicator fails in closed position. - Sect. 4.2, m
- i. Reactor Coolant flow measurement fails low. - Sect. 4.2, u.
- j. Main Steam Line Safety, Atmospheric, or Turbine Bypass Valve fails open. - Sect. 4.2, v.
- k. MFW control valve fails open or valve control signal fails demanding valve opening. - Sect. 4.2, o

Type E - Failures That Would Cause MFW Overfeed At Relatively Low Rate - These would afford more time for intervention. If water were ejected from the SG it would be with relatively less energy and momentum than in the foregoing cases.

- a. Delta-P signal across MFW control fails between 0 and set point. - Sect. 4.2, b.
- b. MFW flow measurement fails at low value greater than zero. - Sect. 4.2, e.
- c. Reactor inlet temperature measurement in one loop fails low. - Sect. 4.2, h.
- d. Start up FW control valve position indicator fails with valve less than 50% open. - Sect. 4.2, l.
- e. MFW pump speed governor fails. - Sect. 4.2, n.
- f. MFW Start Up valve fails open. - Sect. 4.2, p.
- g. MWe demand fails high. - Sect. 4.2, s.

Type F - Single Failure Causing Relatively Slow Overfill of Steam Generator

A sufficient leak in selected pressure tap A (A') - see Figure 3 - or the connecting pipe from that tap or the packing of the blocking valves on which the connecting pipe terminates. Sect. 4.2, r; 2.2.2, a.

The foregoing classification is useful in the further analysis of the consequences of the failures or the failures in combination.

Type C failures, taken alone, should cause a rapid filling of the Steam Generator to the 394 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.

There is one Type F failure. This is a single failure which causes the rapid filling of the SG to the 394 in. point and the relatively slow continued overfilling of it 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/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. We have made no estimate of the probabilities of these failures.

4.2 DETAILED DESCRIPTIONS OF FAILURE SEQUENCES

The component parts of the FW system, its controls and control signals, constitute a functional group that could have failures which could initiate a SG overfeed. We have examined this group to find failures that can lead to overfill of the SG at Oconee. All but one of the overfeed sequences we have found 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 auxiliary FW pump, which does not have a high level trip.

The following event sets have been identified as having the potential to cause steam generator overfeed. In each case the initiating event appears to lead to increase of the steam generator 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 the modelers and simulators to highlight features that may have special significance. Where indicated they will be analyzed on a system simulator in the next phase of this study which will be the augmented Failure Modes and Effects Analysis.

A most helpful source, which suggested a number of these sequences, was reference (2).

a. The delta-P 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 delta-P signal back to setpoint. Excessive feedwater flow results from the increased pump speed. Throttle pressure will increase, T_{AVG} will start 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 setpoint. The control rods will pull, increasing reactor power, to control T_{AVG} back up to setpoint.

However, as long as the tracking mode is not activated, the FW control valves should control the FW flow back to the original setpoint. Hence, the plant should settle out at 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 steam generators from occurring. However, failure of the FW control valves to act rapidly enough still leaves the high level pump trip protection.

b. The delta-P signal across the FW control valve fails at some point below the setpoint. Qualitatively, the effects are the same as in (a). However, (a) appears to be the bounding case; so the effects should be less severe. A failure of the delta-P signal above the setpoint 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 steam generators and overcooling the core. T_{AVG} will start to drop, causing control rods to pull and reactor power to increase. The steam pressure will increase, causing the turbine valves to open and the megawatt electric generation to increase. Because of negative megawatt electric error, the megawatt electric calibrating integral will cause the feedforward control demands to the reactor and feedwater to decrease. If the megawatt electric calibrating integral does not reach a low limit, then the unit will settle out at its original condition. If the megawatt electric calibrating integral goes onto its low limit (generally set at -5%), then 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 main FW flow signal in loop A fails showing zero flow. The loop A FW control valve will open fully trying to control the FW flow to setpoint. The delta-P across the loop AFW control valve will decrease below setpoint, and the FW pumps will speed up to control the delta-P back to setpoint. Steam generator A is overfed because control valve A goes fully open and the pumps speed up. Steam generator B is initially underfed when control valve A goes fully open, is probably overfed for a short period of time when the pumps speed up, and eventually FW control valve B should control loop B FW flow to setpoint.

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 delta- T_c error. The delta- T_c control will start to decrease the FW demand in loop A and increase the FW demand in loop B. This transient may result in a reactor trip caused by low RC pressure or the trip of the FW pumps caused by a high level in steam generator A.

e. Main FW flow signal fails at a level between 0 and demand. Transient proceeds as in (d) but less severe.

f. This transient is initiated by the startup level signal in loop A failing low. As a result of this, 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, 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 steam generator level is reached there is the potential for

continued overcooling of the primary due to the open relief valves and the failed level measurement causing the continuing supply of feedwater to SC-A. Popping of the relief valves would cause rapid loss of steam pressure and high flows to be drawn from the steam generators. 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 SGA 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 3 methods of determining T_{AVG} : namely,

$$1. \quad T_{AVG} = \frac{T_{HA} + T_{HB} + T_{CA} + T_{CB}}{4}$$

$$2. \quad T_{AVG} = \frac{T_{HA} + T_{CA}}{2}$$

$$3. \quad T_{AVG} = \frac{T_{HB} + T_{CB}}{2}$$

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 (i.e., Hand/Auto) 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

$$\text{Error } (T_{AVG}) = \text{Setpoint} - T_{AVG}$$

will be negative.

With the ICS in complete automatic, the T_{AVG} signal modifies the reactor demand. A negative T_{AVG} will cause the control rods to insert. If T_{AVG}

is large enough it can cause the feedwater flow demand to be modified through the cross limits from neutron error to feedwater control. A sufficiently negative T_{AVG} will cause the feedwater demand to be increased. Hence, with the power generation of the reactor decreasing and the feedwater flow increasing, this transient is in the direction of a steam generator 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 feedwater 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 unstable. The negative T_{AVG} signal would initially cause the feedwater demand to increase rapidly while the reactor demand remains constant. Again, this transient is in the direction of a steam generator overfill.

h. This transient is initiated by the reactor inlet temperature in loop A failing low. Proportional control action in the delta- T_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 delta- T_c control will eventually cause the variable gain multiplier in the flow ratioing circuit to be decreased by an additional 20%. Hence, because of the delta- T_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% on account of delta- T_c control. The low failure of the reactor inlet temperature in loop A will also cause an error in the calculation of T_{AVG} . There are three methods of determining T_{AVG} . They are

$$1. T_{AVG} = \frac{T_{HA} + T_{HB} + T_{CA} + T_{CB}}{4}$$

$$2. T_{AVG} = \frac{T_{HA} + T_{CA}}{2}$$

$$3. T_{AVG} = \frac{T_{HB} + T_{CB}}{2}$$

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 either 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 the reactor power to be increased. Also, the low T_{AVG} will, through the reactor cross limits to the FW system, cause the total FW demand to be lowered. Hence, the reactor power

increases; the T_{AVG} control causes the FW flow to SG-B to decrease, and the ΔT_C control causes the FW flow to SG-B to increase. Whether or not SG-B will have excessive FW flow is not clear.

1. 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 in equal magnitude but opposite sign to the loop A and loop B flow demands. However, the change in demand in each loop is limited to 25% of the total flow demand.

If the initial unit load is high enough, the Btu limits will be activated and limit the increased 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 control T_{AVG} back to setpoint. 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, then 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 , steam generator A will be overfed and steam generator B will be underfed.

j. The reactor average temperature, 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):

$$T_{AVG} = \frac{T_{HA} + T_{CA}}{2}$$

for this results in the largest error in T_{AVG} for the assumed failures. If T_{AVG} fails high because T_{HA} fails high then 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} falls high as a result of T_{CA} failing high, then scenario g must be modified to account for the effects of the delta- T_c control loop. With delta- T_c control coming into play, the steam generator overfeed will not be symmetric as considered in scenario g. Instead, because delta- T_c control rerates the FW flows, overfeed of steam generator A will be greater than of steam generator B. Hence, with a high failure of T_{CA} , the overfeed of steam generator A should be worse than that considered in scenario g.

If a high failure of T_{AVG} occurs for some reason other than a high failure of T_{HA} or T_{CA} , then scenario g will again apply except for the above mentioned effect on the Btu limits.

With all three failure modes resulting in high failure of T_{AVG} , the steam generators 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 steam generator level.

k. The neutron flux density reading fails high. The control rods will begin to insert continuously in trying to reduce the failed 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 steam generators are overfed and the primary is overcooled. The Btu limits will probably be activated and will limit the maximum feedwater flow demands. The cross limits will cause the unit to go into the 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 highly probable. Following the reactor trip, the turbine will trip and the megawatt electric generation will go to zero. The unit is still in the track mode at this time, and the feedwater demand from the integrated master goes to zero. However, following the reactor trip, the cross limits from reactor control to feedwater control increase, calling for feedwater flow close to 100%. Hence, the Btu limits, and not the feedforward signal from the integrated master, must be relied upon to run the FW system back.

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 main feedwater blocking valve in loop A does not receive a signal to close. The leakage through loop A main FW control valve, if excessive, may cause steam generator A to be overfed. Also, since the main feedwater blocking valve in loop A does not close, the flow measurement used in feedwater control is not switched from the main FW flow measurement, which is highly inaccurate at such low flows, to the start-up FW flow measurement. Thus, control will not be as smooth as normal. If the leakage through the main FW control valve is large enough, the start-up FW valve may close completely while steam generator A continues to be overfed from the leakage. This condition would probably result in a steam generator high level trip of the FW pumps.

m. MFW blocking valve in loop A is open, but its position indicator fails in closed position. This causes ICS to take flow measures from startup line. If reactor is at high power a flow demand signal is sent causing increase in flow 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 the feedwater flow to the steam generators to increase. Flow control will cause the feedwater control valves to close to control the feedwater flows back to setpoint. As the control valves close, delta-P control will cause the speed of feedwater 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 a reduced speed, with both pumps supplying flow to the steam generators, or the plant may settle out with the check valve in series with pump B closed, and pump B supplying no flow to the steam generators. Finally, pump B may end up operating 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 delta-P higher than setpoint may exist across the control valves following the transient. Some overfeed of the steam generators 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 delta-P signal across control valve A leads to pump speed up. The delta-T_C error will attempt to reduce flow in A and increase flow in B. 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. On account of the substantial increase in total flow (resulting from the loop A failure) the total flow demand error should dominate the delta-T_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 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 along with the total flow demand error signal should between them 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 feedwater 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 steam generators from going on low level control. Appropriate manual control actions could be used to shut the plant down safely.

Following a reactor trip, this failure would result in overfeed of steam generator A if proper manual control actions are not taken. When the reactor trips, the turbine also trips; the steam system goes on bypass control; the feedwater flow demand runs back to low value and the steam generators are

are supposed to go on low level control. With the start up valve in loop A failed wide open, steam generator A will be overfed. Without manual control intervention, feedwater pump trip on high level in steam generator A is likely. Simulation of failure with reactor trip is needed.

q. The control system summer which sums the start up 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 trips 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 on which the pipe terminates will cause a low level signal and an overriding demand for feedwater. 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 Section 2.2.2.

s. Failure of the MWe 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 feedwater flow. Hence, the feedwater system response would be approximately coordinated with that of the reactor. That is, if the system energy balance is taken into account the feedwater system should run just slightly ahead of the reactor. The cross limits should hold the feedwater system back. Some steam generator 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 inches. 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 the RC flow measurement in loop A will be considered. Consider first a high failure. The reactor coolant flow imbalance feedwater ratioing circuit will immediately reratio the feedwater flows. The feedwater flow in loop A will be increased and the feedwater flow in loop B will be decreased. This will lead to overfeed of steam generator A and underfeed of steam generator B. After a short time lag, the ΔT_C control will decrease the feedwater flow in loop A and increase the feedwater 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 immediately be implemented in the unit load demand load limit circuitry. Again, the reactor coolant flow imbalance feedwater ratiocing circuit will immediately reratio the feedwater loop flows. However, in this case the reratioing will be in the opposite direction and much larger. The feedwater flow in loop A should be decreased to the point that steam generator A goes on low level control. In loop B, the Btu limits should be activated and thus restrain the increase in feedwater flow. Hence, in this case, overfeed of steam generator B and underfeed of steam generator 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 feedwater flow when steam generator B goes on Btu limits, and a reactor trip on high RC pressure is probable. Simulation, especially initialized at high load, is needed.

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 Steam Generator and an initial increase in feed of the SG. This event is bounded by the small break in the Main Steam Line.

w. The low level setpoint fails giving a reading at its highest level. This failure is functionally equivalent to r.

4.3 SIMULATION RECOMMENDATIONS

The criteria which we follow in recommending that sequences be simulated are as follows:

- a. The scenario is sufficiently complex that we cannot be sure our speculations as to its course are correct both in magnitude and in sequence of events. These uncertainties are especially pronounced in those events where compensatory ICS action is initiated.
- b. Primary side effects cannot be quantitatively evaluated without simulation. If primary side effects seem significant simulation is indicated.
- c. If there are strong arguments that the event is insignificant it need not be simulated.
- d. If there are strong arguments that the event is bounded by another and if simulation shows the bounding event is not significant the bounded event need not be simulated. This would be a special case of c. However, if the bounding event proves significant, the bounded event should then be simulated.
- e. An event sufficiently similar to a simulated event need not be simulated.

With these criteria, our recommendations for simulation at present are as follows.

- (1) Any one Type C (Sect. 4.1) event.
- (2) Any one Type A or B (Sect. 4.1) event followed by any one Type C event while the A/B is still undetected.
- (3) The single Type F (Sect. 4.1) event.
- (4) We cannot eliminate from consideration at this time any of the following: Sect. 4.2 c,d,g,i,j,k,m,u. All these are Type D (Sect. 4.1). We expect that exploratory calculations will permit us to eliminate a number of them on the basis of similarity or bounding.
- (5) We recommend no Type E (Sect. 4.1) simulations at this time in anticipation that a number of them will be shown to be bounded and insignificant.

5. POSSIBLE CONSEQUENCES OF STEAM GENERATOR OVERFILL

Steam generator overfill can produce both primary side and secondary side effects which may have safety consequences for the plant. Secondary side effects may indirectly produce significant primary side effects.

5.1 DIRECT PRIMARY SIDE EFFECTS

Overfilling of the steam generator will produce overcooling of the primary coolant. This, in turn, can in some instances produce one or more of the following results:

- a. density increase and liquid phase shrinkage with attendant increase reactor coolant pressure
- b. pressurizer dryout
- c. steam in primary flow passages with possible blockage of flow
- d. possible loss of natural circulation
- e. possible reactivity insertion from high density moderation

5.2 POSSIBLE SECONDARY SIDE DAMAGE

Overfill of the Steam Generator to the point where liquid water enters the Main Steam Line may cause damage on the secondary side. In Section 4.1 we have classified, in various ways, control system failures that can lead to Steam Generator overfill. One way was according to the rate at which the overfill occurred. Overfills brought on by Type E and F failures (Section 4.1) are expected to occur rather slowly: E because the MFW pumps and control valve are not wide open, and F because the final overfill mechanism is the AFW. Type C overfills would involve control valves fully open or nearly so and MFW pumps operating at high speed. These would be rapid overfills. Type D events are not yet sufficiently analyzed and may prove to produce overfills of either kind.

The rapid overfill appears more threatening for two reasons. First, it permits minimal time for effective recognition and counter measures. Second, it injects water into the Main Steam Line at maximum speed and therefore with the maximum kinetic energy/momentum that the MFW pumps are able to provide, only minimally dissipated in the open control valve.

All references we have found relating to the ability of a B. and W. Main Steam Line to withstand stresses from liquid water deal only with the static load of the water, that is, motionless water, zero energy/momentum.^{3,4,5} There appear to have been no tests made of the ability of these lines to bear the dynamic stresses associated with the influx of water of high energy/momentum content such as might come from a Type C failure. (In fact, there appear to be no tests to show whether the dynamic stresses from a Type E or F failure could be borne.) Under the circumstances, it would not be prudent to assume that the probability of Main Steam Line rupture in that dynamically stressful environment is negligible.

The possible results of such a rupture should be considered.

Main Steam Line Rupture is one of the accidents analyzed in the Oconee-1 FSAR. We are particularly interested here in the effect such a rupture can have on the Steam Generator tubes. The tubes are subject to considerable wear and damage during normal operation. There are approximately 16,000 of them in an Oconee 1 Steam Generator. Oconee has experienced a number of observed tube leaks, and a number of tubes have been plugged as a precautionary measure during maintenance on account of observed wear. Appendix B summarizes references to a number of Steam Generator tube problems which have occurred at Oconee.

During normal operation the tubes and the massive supporting tube sheets are at elevated temperatures, and, consequently, in thermally expanded state. If now the tubes are suddenly cooled more rapidly than the supporting tube sheets, the tubes, in attempting to contract, are placed under tensile stress. A Main Steam Line Break causes the water in the Steam Generator to flash, suddenly cooling the tubes. The water is in more contact with the tubes than with the tube sheets. Further, the tube sheets, being massive, would have longer thermal time characteristics and would cool more slowly. All the tubes in the Steam Generator are simultaneously subject to the added thermal stress. It is apparent that for large stresses in these circumstances multiple tube ruptures could occur.

The Oconee 1 FSAR examines this effect (on SG tubes) in its Main Steam Line Break analysis (Section 15.13.5, Oconee 1, FSAR). In that section the additional stress (maximum) on SG tubes due to the flashing of the water in the SG when the Steam Line Break occurs is given as 39 ksi. That is compared with 42 ksi, said to be the "maximum allowable stress", but otherwise undefined. This analysis initiated the Steam Line Break with the Steam Generator less than two-thirds full of water. Apparently no account was taken of the severe vibrational stresses that would be experienced during the blowdown of the secondary side through the ruptured steam line.

In the scenario proposed here a Steam Generator fills with high energy/momentum content water; the water enters the Steam Line producing dynamic stresses that lead to rupture of the line. Hence, the Steam Line Break occurs with a full Steam Generator, 50% more water content than in the case computed in the Oconee 1 FSAR. With that much additional water flashing in the Steam Generator there should be substantially more Steam Generator tube cooling and substantially more resultant thermal stress.

These additional thermal stresses and the vibrational stresses of blowdown, when considered in analysis, may show that there is sufficient additional stress present to cause multiple tube rupture in the steam generator.

Multiple tube rupture taken together with main stream line rupture provides a leakage path through and out of the secondary system for radioactive materials contained in the primary fluid.^{6,7,8,9,10}

6. TENTATIVE CONCLUSIONS

This study has not proceeded to a point where serious system inadequacies have been demonstrated. In the course of this study, however, we have, we believe, uncovered some potential concerns, in particular, control system failure that might lead to the failure sequence discussed in Section 5. We have made no assessment of the probability of occurrence of any of these things. Therefore, it would be premature to suggest that any corrective measures are required. We have noted some places where improvements might be made if it is found they are desirable. We present them here for consideration.

a. The high level MFW pump trip originating in each steam generator is of primary importance in preventing steam generator overfill. We have already noted that contacts 2A and 3A in Figure 4 are in series as are contacts 2B and 3B. Revising these circuits to parallel configuration would afford important redundancy to this circuit.

b. Also in Figure 4, functional replication in parallel of the FPTX solenoid/contact would provide additional important redundancy.

Both a and b would, of course, increase the likelihood of spurious pump trips.

c. We have observed that pressure taps and some connecting equipment are shared in common by the MFW and the AFW. It may be useful to examine the desirability of modifying the gang selection switching so that when the operator selects A-B-D (Figure 3) for MFW, A'-B'-D' is selected for AFW.

d. The plant computer could be programmed to track both sets of signals in c for consistency and to provide appropriate alarms when an inconsistency is noted.

e. The full range Steam Generator level sensor, which makes use of information from tap E, Figure 3, is the only sensor providing level information once the SG water level exceeds the high level pump trip height (level D,D' in Figure 3). This information does not go to the control system, but it is available to the operator. It is apparently not explicitly referenced in the procedures governing steam generator overfills. An explicit reference might be useful.

REFERENCES

1. Delta-P Transmitter For Nuclear Service, Product Instruction, E21-20, Bailey Meter Co.
2. BAW 1743, 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, July 1982, Babcock & Wilcox Co.
3. NRC Memo, Power Reactor Events - Steam Generator Overfill, Richard H. Vollmer to Thomas Novak, May 13, 1981.
4. Letter, K. S. Canady, Duke Power Co., to A. L. Lotts, ORNL, August 31, 1983.
5. B. & W. Owners Group, Probabilistic Evaluation of Pressurized Thermal Shock, Phase 1 Report, BAW 1791, June 1983, ppg 6-48, Babcock & Wilcox Co.
6. NUREG-0909, NRC Report on the January 25, 1982, Steam Generator Tube Rupture at R. E. Ginna Nuclear Power Plant, April 1982.
7. NUREG-0651, L. B. Marsh, Evaluation of Steam Generator Tube Rupture Events, March 1980.
8. Preliminary Notification of Event-PNO-V-82-45A, November 15, 1982, San Onofre Unit 2, Excessive Cooldown Transient and Automatic Initiation of Safety Injection.
9. C. Michelson, Case Study of the Abnormal Transient Operating Guidelines (ATOG) as Applied to the April 1981, Overfill Event at Arkansas Nuclear One, Unit 1, USNRC, August 30, 1982.
10. EPRI 3065, C. S. Davis, J. M. Thomas, S. W. Winder, D. E. Allison, Engineering and Probabilistic Analysis of Tube Cracking Performance in Once Through Steam Generators, Vol 1, July 1983.

Appendix A - Information Sources

This program has the major aim of identifying control system malfunctions which might significantly impact safety systems and lead to a serious transient, or which might cause a transient for which there has been inadequate provision in the safety systems. With such a mission it is clear that our major sources of information would, of necessity, be design and procedural data.

In fact, this has proved to be the case. Documentation that has been of "mainstream" use to us has included the following.

Duke Power Company
Oconee Nuclear Station
Final Safety Analysis Report

Oconee Nuclear Station P&IDs
(very limited number available)

Bailey Instruction Book

Duke Power Company
Oconee Nuclear Plant, Unit No. 1
Manual IC/NNI System, Vol. 4

Oconee Nuclear Plant No. 1
Integrated Control system Reliability
Analysis, prepared for NRC by B&W

Abnormal Transient Operating Guidelines,

BWNP-20807 Babcock and Wilcox
Control of a Nuclear Power Plant with Once
Through Steam Generator, ASME, 80-WA/DSC-24
L. L. Joyner, R. P. Broadwater

Oconee Units 1, 2, and 3
Training Manual

In addition, there have been numerous conversations with former employees of B&W and of Duke Power. There has also been much examination of "loose" copies of circuits, sometimes poorly identified as to source.

We have made a number of searches of the LER literature covering the period 1973-83. LERs have not provided one of the more useful primary sources for this report. There are several reasons for this.

1. As noted above, design and procedure are the major areas investigated for failure in this work. LERs deal very little with these two topics.
2. Steam generator overfill as such has not been a required LER reportable event. Hence, not only when they occur alone may such events go unreported, but also when they occur in conjunction with other reportable events the steam generator overfill aspect may be neglected. In those cases where we have found it reported its extent and consequences are not detailed.
3. LERs are written with a brevity that tends to render their descriptions of events too incomplete for a study of this kind.

On account of the above considerations, 2 in particular, retrieval of useful steam generator overfill information from the LER data base has not been especially productive. Searches on various steam generator related conditions for the period 1973-83 produced 70 LER references of which 21 were found to be related to performance of once through steam generators. The LERs did not produce any failure modes in addition to those deduced from study of design and procedure documents. They confirmed experience with certain kinds of failure. Their usefulness to this project probably will lie in their provision of counts of certain kinds of failures for aid in quantification.

Since SG overfill has not of itself constituted a requirement for submission of an LER in the past, we have no assured method of identifying all or most such events which have occurred. A number of LER searches along with resort to secondary sources have disclosed 21 cases of SG overfill of some kind in once through steam generators. We have identified only three events where water definitely entered the main steam line: San Onofre 11/9/82, Ginna 1/25/82, and Arkansas Nuclear One 4/8/81. Of these, only the last involved a once through SG. In none of these cases was there any reported damage to steam line or to supports as a result of the influx of water. (However, operation of a safety valve was compromised in the Ginna case). On the other hand, conversations with workers in the field suggest to us that there may have been a number of additional SG overfill events not documented in the available literature.

Various secondary sources, some of them heavily based on LERs, have been useful. These are reports of NRC and NRC contractors which clarify, and to some extent, quantify various kinds of failures or which make in-depth studies of particular failures which have occurred.

Prominent among these are:

- NUREG/CR-2497, Precursors to Potential Severe Core Accidents
Summary of Event Tree Development, Branch Probability Estimation
and Sequence Qualification for the Oconee Pressurized Thermal
Shock Evaluation, SAI
- NUREG-0909, NRC report on January 25, 1982 Steam Generator Tube
Rupture at R. E. Ginna Nuclear Plant

NUREG-0651 Evaluation of Steam Generator Tube Rupture Events
Case Study of the Abnormal Transient Operating Guidelines as Applied to the April 1981 Overfill Event at Arkansas Nuclear One. USNRC, August 30, 1982.

Current Events Power Reactors, USNRC, 1 March-30 April 1978,
Loss of Non-Nuclear Instruments (Rancho Seco).

Also of considerable use have been:

BAW 1743, Failure Modes and Effect Analysis of Midland NNI and ICS
Control of a Nuclear Power Plant with once through Steam Generator,
ASME 1980.

Appendix B -SG Tube Leak Problems at Oconee 1

DATE/LER	SG	No. of Tubes	Remark
3/6/82 LER	1B	1	0.08 gpm leak
2/9/82 LER	1A	1	0.11 gpm leak
5/29/80 NSIC 00Z0158256			Deficiency in FSAR analysis of tube rupture
7/23/79 LER	1B	1	0.3 gpm leak
10/12/78 LER			Tubes misplugged
4/20/78 LER		4	Leak observed
1977 NSIC 00Z0128689			Status report on tube
5/7/77 LER	1B	2	Leak observed
3/27/77 LER		1-6	Leak observed
2/28/77		1-6	Leaks observed
12/22/76 LER	1B	1-3	Leak observed
1976 NSIC 00Z0120234	1A	2	Leak observed