



NUREG/CR-3692
ORNL/TM-9061

OAK RIDGE
NATIONAL
LABORATORY

MARTIN MARIETTA

**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

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

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

8409180488 840731
PDR ADDCK 05000269
P PDR

Printed in the United States of America. Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road, Springfield, Virginia 22161

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

NUREG/CR-3692
ORNL/TM-9061
NRC Dist. R1, R4, RG

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: July 1984

*Tennessee Technological University, Cookeville.

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

NRC Fin No. BC467

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

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	1
1.1.4 Outline of This Report.....	2
1.2 Steam Generator Overfill Summary.....	2
1.2.1 Scope of Steam Generator Overfill.....	2
1.2.2 Principal Results of Steam Generator Overfill Study.....	3
1.2.3 Methods Used.....	3
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.....	6
2.2.1 Operating Control.....	6
2.2.2 Steam Generator Level Limits and Sensors.....	13
2.2.3 High Level Main Feedwater Pump Trip Circuitry.....	15
3. Systems Selected.....	16
4. Control System Failures That Contribute To Steam Generator Overfill.....	18
4.1 Classification of Failures.....	19
4.2 Detailed Description of Failure Sequences.....	22
4.3 Simulation Recommendations.....	30
5. Possible Consequences of Steam Generator Overfill.....	32
5.1 Direct Primary Side Effects.....	32
5.2 Possible Secondary Side Damage.....	32
6. Tentative Conclusions.....	35
References.....	36
Appendix A - Information Sources.....	37
Appendix B - Steam Generator Tube Problems At Oconee 1.....	40
APPENDIX C - Review of Draft By Duke Power Co.....	41

LIST OF ACRONYMS

AFW	Auxiliary feedwater
B&W	Babcock and Wilcox
BWR	Boiling water reactor
CE	Combustion Engineering
FMEA	Failure mode and effects analysis
FSAR	Final Safety Analysis Report
FW	Feedwater
HPI	High-pressure injection
ICS	Integrated Control System
INEL	Idaho National Engineering Laboratory
LER	Licensee Event Report
LWR	Light water reeactor
MFW	Main feedwater
NNIS	Nonnuclear Instrumentation System
NPP	Nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
OTSG	Once-through steam generator
P&ID	Piping & instrumentation diagrams
PWR	Pressurized water reactor
RCS	Reactor cooling system
RC	Reactor coolant
SG	Steam Generator
SUV	Startup valve

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

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 overfill 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, 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 Sects. 2 through 4, but should in no event skip Sect. 2.2.2, 2.2.3, or 4.1. Section 5 considers some possible consequences of a steam generator overfill; Sect. 6 makes some observations about possible design or procedure changes if they are felt to be necessary.

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 shall 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 Sects. 2.2.2 and 2.2.3).
- b. Both of the above protection features receive level indication from the same instrumentation. They are, therefore, subject to common cause failure (See Sect. 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 might water from the MFW.

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 Sect. 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 Sect. 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 Sect. 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.-ID 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.-OD 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.-ID 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 which is 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.

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

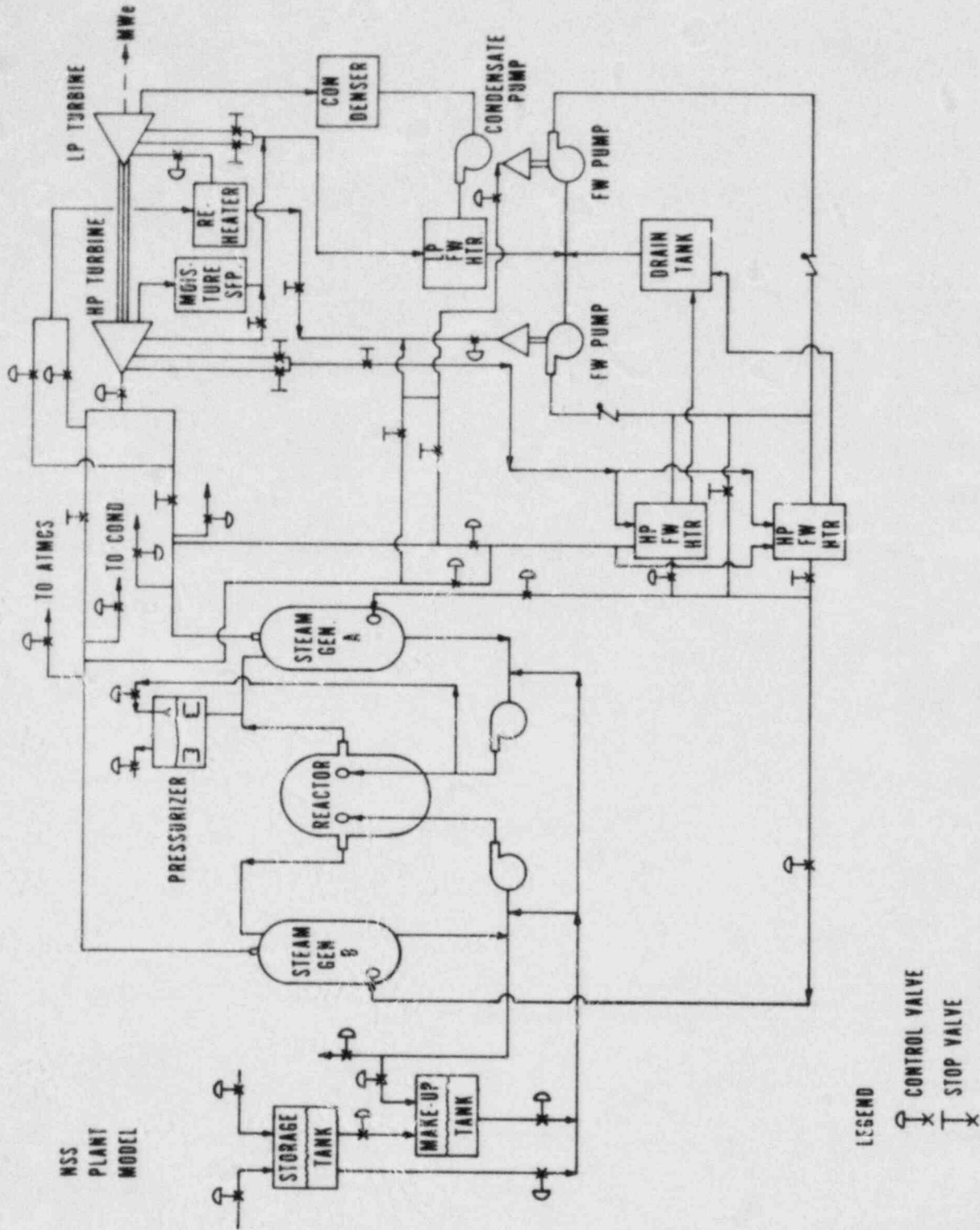


Fig. 1. Simplified schematic diagram of a nuclear power plant.

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 Fig. 2 - all references to Points and Blocks are on Fig. 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

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

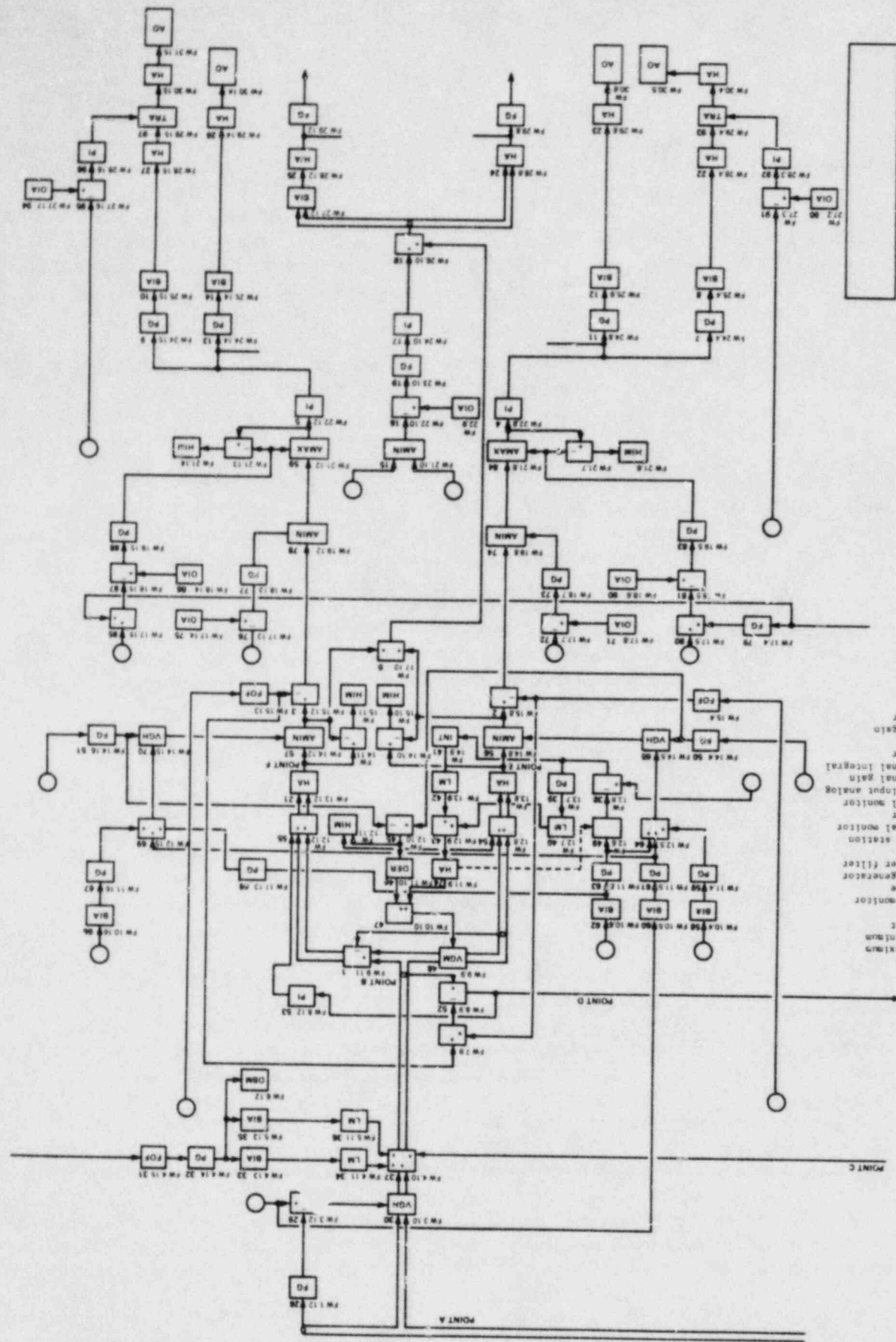


Fig. 2. Schematic diagram of Oconee-1 steam generator control system

- Legend:
- AMAX = select maximum
 - AO = analog out
 - BIA = bias
 - DEM = deadband monitor
 - DRV = derivative
 - FG = function generator
 - FOF = first-order filter
 - RV = feedback
 - HA = hand/auto reaction
 - HM = high signal monitor
 - INT = integrator
 - DIA = operator input analog
 - PC = proportional gain
 - PI = proportional integral controller
 - TMA = transfer
 - VOT = variable gain
 - MULT = multiplier

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 $\Delta T_c = T_{CA} - T_{CB} = 0$. 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 0, the tap heights are A,A' - 6 in., B,B' - 102 in., D,D' - 394 in., E - 606 in.

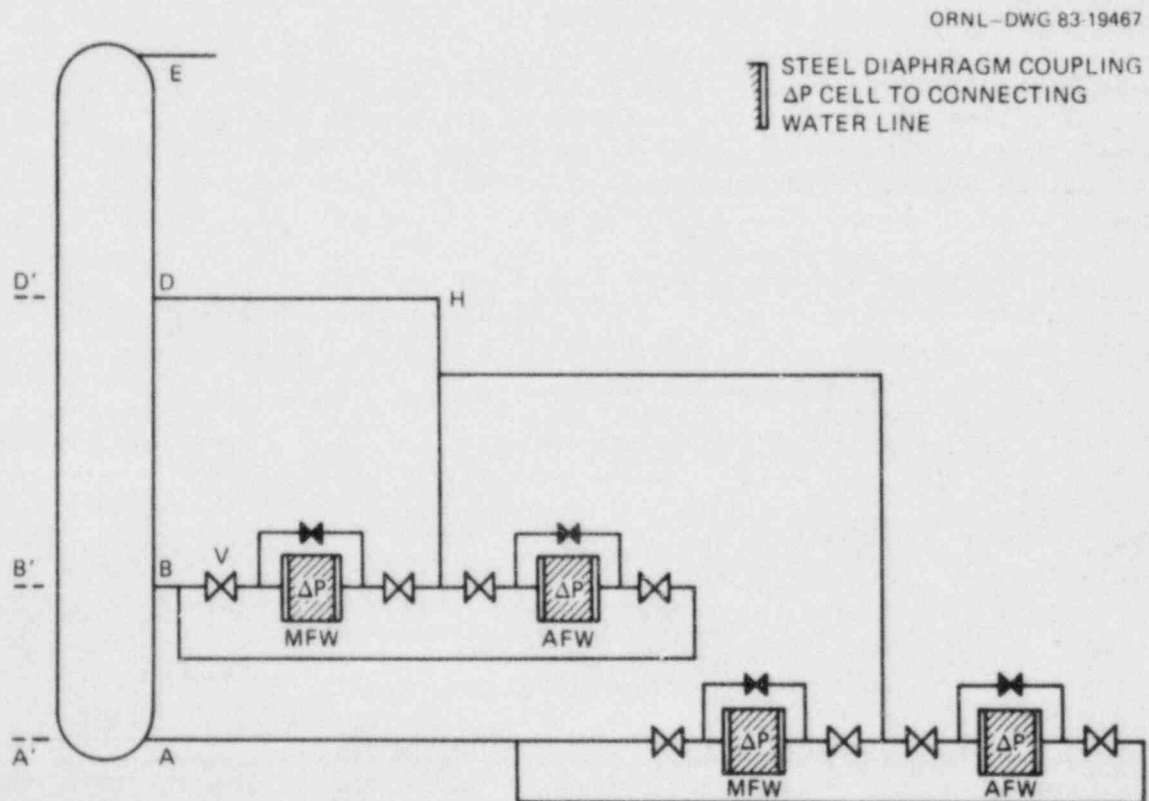


Fig. 3. Schematic diagram of steam generator pressure taps and ΔP cells.

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 (Fig. 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 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) A sufficient leak in the selected A,A' tap or the connecting pipe or 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 Fig. 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 (Ref. 1).

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 oper.

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

The circuitry of Fig. 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.

3. SYSTEMS SELECTED

The 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
Nonnuclear 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 System
Reactor Building Service Water System	Compressed Air System
Instrument Air System	Heating, Ventilation and Air Conditioning
Reactor Core	

Class E - This class contains all other systems.

Class E Systems

Control Rod Drive System	Chemical and Volume Control System
Radioactive Waste System	Liquid Radwaste System
Gaseous Radwaste System	Radiation Monitoring System
Solid Radwaste System	Environmental Radiation Monitors
Plant Area Radiation Monitors	Refueling System
Process Radiation Monitors	Fuel Pool Cooling and Cleanup System
Spent Fuel Storage System	Plant Gas System
Service Air System	Hydrogen System
Process Sampling System	Fire Protection System
Nitrogen System	Water System (Fire)
Potable and Sanitary Water System	Communication System
Carbon Dioxide System	Diesel Bldg Ventilation System
Control Room Habitability System	Non Radioactive Waste System
Fuel Bldg Ventilation System	Liquid Waste
Gaseous Waste	Turbine Gland Seal System
Solid Waste	Stator Cooling System
Turbine Lubrication System	Condenser Evacuation System
Hydrogen Seal Oil System	Condensate Heater Drain System
Condensate Cleanup/Polishing 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 Fig. 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 Fig. 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 Sects. 2.2.2 and 2.2.3.)

It is apparent, therefore, that the MFW cannot overflow 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.

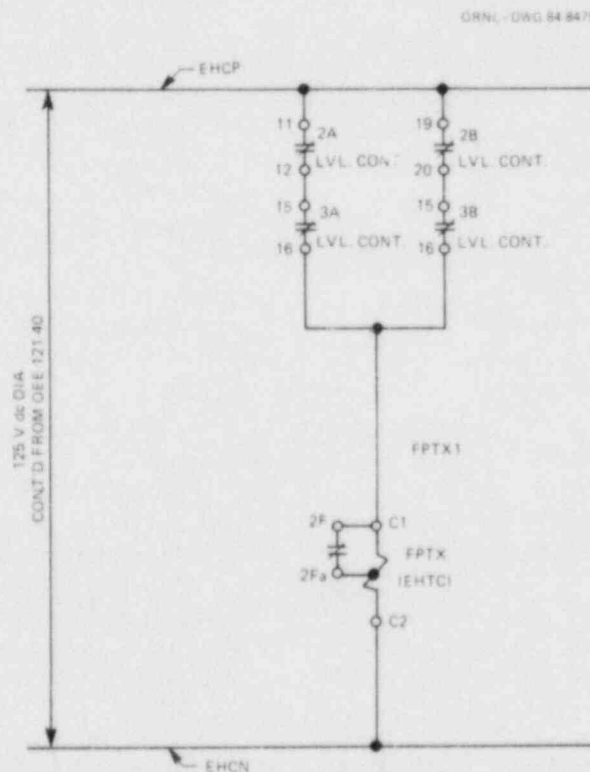


Fig. 4. Main feedwater pump high-level trip circuit.

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 of 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 (Fig. 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 Sect. 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 nonselected B-D (B'-D') set.

- a. Any failure causing relay 2A or 3A (Fig. 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 (Fig. 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 nonselected 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 (Fig. 3) of the nonselected set in the closed position during operation - 2.2.2, c
- e. Any failure of the nonselected 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 nonselected 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. Startup 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 Startup 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 Fig. 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, singly or 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 (FMEA)

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 falling 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 SG-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 SG-A should overfill.

g. This transient is initiated when one of the reactor hot leg temperature measurements fails high. Let

T_{AVG} = reactor average temperature measurement

T_{Hi} = hot leg temperature measurement, $i = A, B$

T_{Ci} = cold leg temperature measurement, $i = A, B$.

There are 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 ΔT_c control will immediately cause the flow demand in loop A to decrease and the flow demand in loop B to increase. This proportional control action is limited to 5%. Integral action in the ΔT_c control will eventually cause the variable gain multiplier in the flow ratioing circuit to be decreased by an additional 20%. Hence, because of the ΔT_c control, the flow demand for loop A flow equals (100% - 5% - 20%) times the total flow demand. The flow demand for loop B flow then equals 200% (100% - 5% - 20%) times the total flow demand. Therefore, the flow demand in loop A is reduced by 25% and the flow demand in loop B is increased by 25% on account of ΔT_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 delta- T_c control causes the FW flow to SG-B to increase. Whether or not SG-B will have excessive FW flow is not clear.

i. The reactor inlet temperature loop A-B difference delta- T_c fails high. A high failure of delta- T_c conveys the false information that on the primary side, the temperature of cold leg A is higher than cold leg B. The delta- T_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 delta- T_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} fails 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 reratios 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 AVG 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 startup 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 startup 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 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 startup level and turbine header pressure signal fails, giving low indication. This failure is equivalent to the corresponding failure in any of the component signals and causes increased flow to the SG. The high level FW pump trip occurs at high level indication.

r. A sufficient leak in selected SG pressure tap A (A') or in the pipe connecting it to blocking valves, or in the packing of either blocking valve 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 Sect. 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 in. However, a failure of the hard limiter signal could negate the limiting effect. This error is then potentially equivalent to sequence f.

u. Both high and low failures of 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 ratioing 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 of 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/or 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 in 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 Sect. 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 (Sect. 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 countermeasures. 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&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 (Refs. 3-5). 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 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 SG 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 a 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 SG 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 SG 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 (Sect. 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 SG, 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 (Refs. 6-10).

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. R. W. Enzina, R. W. Winks, S. D. Swartzell, R. P. Broadwater, M. S. Kai, and W. E. Wilson, "Failure Modes and Effects Analysis of the Midland NNI and ICS," Babcock & Wilcox Co. Report BAW 1743 (July 1982).
3. NRC Memo, Richard H. Vollmer to Thomas Novak, "Power Reactor Events - Steam Generator Overfill," May 13, 1981.
4. Letter, K. S. Canady, Duke Power Co., to A. L. Lotts, Oak Ridge National Laboratory, August 31, 1983.
5. B&W Owners Group, "Probabilistic Evaluation of Pressurized Thermal Shock, Phase 1 Report," Babcock & Wilcox Co. Report BAW 1791, pp. 6-48, June 1983.
6. "NRC Report on the January 25, 1982, Steam Generator Tube Rupture at R. E. Ginna Nuclear Power Plant," NRC Report NUREG-0909, April 1982.
7. L. B. Marsh, "Evaluation of Steam Generator Tube Rupture Events," NRC Report NUREG-0651, 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. Michels, "Case Study of the Abnormal Transient Operating Guidelines (ATOG) as Applied to the April 1981, Overfill Event at Arkansas Nuclear One, Unit 1," NRC Memorandum, August 30, 1982.
10. 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," Electric Power Research Institute Report EPRI-3065, 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

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
Duke Power

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. Particularly in the early phases of the program 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 licensee event report (LER) literature covering the period 1973-1983. 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, item 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 1973-1983 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 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-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

<u>DATE/LER</u>	<u>SG</u>	<u>No. of Tubes</u>	<u>Remark</u>
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

Appendix C - Review of Draft by Duke Power Company

An earlier draft version of this report was sent to the licensee, Duke Power Co., for their comments. We found the licensee's response very useful. A number of misconceptions were corrected. We are grateful for the obviously substantial effort expended by the licensee and have made use of the material supplied.

This report has been substantially revised since the early draft was reviewed by the licensee. The principal thrust of the revision was to conform with an NRC request for greater emphasis on sequences arising when an additional failure occurs with the system in an undetected failed state. The revisions have been so extensive that it is not possible to make a section-by-section correspondence between the revised draft and the review letter. A number of comments in the review have been rendered moot by the revision. In keeping with current NRC policy, we reproduce here those parts of the licensee's response which have resulted in changes to the report.

Other comments made by the licensee, noted, but not incorporated in the report, included matters where different judgments were possible, situations with multiple possible outcomes dependent upon initial conditions, references to calculations or data not available to us, and comments on the proper limits of the study.

Specific comments referenced by page and paragraph follow.

<u>Page/Scenario</u>	<u>Comments</u>
7/2	The statement "total flow control on large feedwater error" is incorrect. It should read "total feedwater flow control on a large reactor coolant flow error."
13/3	The total flow control circuit comes into play when reactor coolant (RC) flow error becomes greater than 10%, provided that: 1) both RC pumps on a steam generator are not tripped; 2) one steam generator is not on low level control and the other is; and 3) the steam generator not on low level control is under automatic control.
15/2, 3	Auxiliary feedwater control is part of the safety grade AFW system and independent of the ICS. Below is a description of the AFW control system:

Page/ScenarioComments

The AFW level control system consists of two Rosemount #1152DP differential pressure transmitters connected to the 0 in. and 388 in. taps of each OTSG, a two-bay

Westinghouse 7300 series control cabinet per unit, and interfaces with pneumatic control valves FDW-315 and FDW-316.

The system is designed to provide automatic OTSG water level control while the emergency feedwater pumps are supplying water to the OTSGs. Two setpoints are provided: (a) a setpoint corresponding to 25 in. of level in the OTSG, which is used after the reactor has tripped and reactor coolant pumps continue to operate and (b) a setpoint corresponding to 240 in. of level in the OTSG, which is automatically engaged when the RCP power monitoring system detects that all four RCPs have tripped in order that natural circulation can be established.

Each OTSG is provided with two independent control systems, each of which consists of a level transmitter, controller, control system power supply, and E/P converter to supply a signal to that OTSGs emergency level control valve.

16-20/Sect. 4

One of the concerns listed was steam in primary flow passages with possible partial choking of flow. Considering the large pipe areas and low pressure differentials in the RCS, there is no possibility for choked flow to occur.

17, 18

Only two of the plant events discussed were caused by control system failures.

21/(1.)

The statement about the total feedwater flow controller is in error and should be deleted from this section. It does not affect the course of the event.

The action of the Btu limits and cross limits should be accounted for. Their effect is to limit allowed feedwater demand.

<u>Page/Scenario</u>	<u>Comments</u>
23/(5.)	There is no feedwater flow "setpoint."
24/(6.)	Neither sequence of events showed a tendency toward steam generator overfill; overfeeding is limited.
24/(7.)	Delta- T_c control is blocked when either steam generator is on low level control.
27/(8.)	The control loop for T_{avg} control to feedwater has exhibited sluggish control in that it can be slow to respond and may subsequently overcorrect. However, it is not unstable in the sense of increasingly wider swings. It has exhibited poor tuning, not "stability problems."
29/(9.)	The Delta- T_c circuit may be blocked if one steam generator goes on level control.
29/(10.)	The statement about the total flow control circuit is in error and should be deleted.
33/(15.)	The frequency error modification to the ULD circuit is not in use at Oconee, and is physically disconnected.
34/(17.)	The reference to the total flow controller is in error and should be deleted.
36/(18.)	In the absence of manual action, the high level pump trip will prevent overfill.

INTERNAL DISTRIBUTION

- | | | | |
|--------|--------------------------------|--------|---------------------------------|
| 1-5. | N. E. Clapp | 28. | P. F. McCrea (Advisory Comm.) |
| 6-10. | F. H. Clark | 29. | P. W. Murrill (Advisory Comm.) |
| 11. | B. G. Eads | 30. | H. M. Paynter (Advisory Comm.) |
| 12. | D. M. Eissenberg | 31. | H. E. Trammell (Advisory Comm.) |
| 13. | A. P. Malinauskas | 32. | ORNL Patent Office |
| 14. | F. R. Mynatt | 33-34. | Central Research Library |
| 15. | L. C. Oakes | 35. | Y-12 Document Reference Section |
| 16-25. | R. S. Stone | 36-37. | Laboratory Records Department |
| 26. | J. D. White | 38. | Laboratory Records (RC) |
| 27. | M. J. Kopp
(Advisory Comm.) | 39. | I&C Publications Office |

EXTERNAL DISTRIBUTION

- 40. Assistant Manager for Energy Research and Development, DOE-ORO, Oak Ridge, TN 37831
- 41-90. D. L. Basdekas, NRC Project Manager
- 91-95. R. P. Broadwater, Tennessee Technical University, Cookeville, TN 38501
- 96. A. F. McBride, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
- 97-98. Technical Information Center, DOE, Oak Ridge, TN 37831
- 99-533. Given distribution as shown in NUREG-0550/Rev. 2, NRC Categories for Water Reactor Safety Research: R1 Basic, R4 Analysis Development, and RG Systems and Reliability Reports

NRC FORM 335 <small>(11-81)</small>		U.S. NUCLEAR REGULATORY COMMISSION BIBLIOGRAPHIC DATA SHEET		1. REPORT NUMBER (Assigned by DDC) NUREG/CR-3692 ORNL/TM-9061	
4. TITLE AND SUBTITLE (Add Volume No., if appropriate) Possible Modes of Steam Generator Overfill Resulting from Control System Malfunctions at the Oconee-1 Nuclear Plant				2. (Leave blank)	
				3. RECIPIENT'S ACCESSION NO.	
7. AUTHOR(S) F. H. Clark, N. E. Clapp, R. Broadwater *				5. DATE REPORT COMPLETED MONTH YEAR February 1984	
9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Oak Ridge National Laboratory P. O. Box X Oak Ridge, TN 37831 * Tennessee Technological University, Cookeville, Tenn.				DATE REPORT ISSUED MONTH YEAR	
				6. (Leave blank)	
				8. (Leave blank)	
12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code) Division of Engineering Technology Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission Washington, DC 20555				10. PROJECT/TASK/WORK UNIT NO	
				11. FIN NO. B0467	
13. TYPE OF REPORT NUREG			PERIOD COVERED (Inclusive dates)		
15. SUPPLEMENTARY NOTES				14. (Leave blank)	
16. ABSTRACT (200 words or less) <p>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.</p>					
17. KEY WORDS AND DOCUMENT ANALYSIS			17a DESCRIPTORS		
17b IDENTIFIERS OPEN-ENDED TERMS					
18. AVAILABILITY STATEMENT			19. SECURITY CLASS (This report)		21. NO. OF PAGES 50
			20. SECURITY CLASS (This page)		22. PRICE \$

120555078877 1 1ANIR11R41RG
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555