DRAFT

PDR

Instrumentation and Controls Division

DESIGNATED ORIGINAL

11/9/84

D. L. B.

Deimetrios L. Basdekas

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

DRAFT FINAL REPORT

Volume 1
Executive Summary

P. N. Austin[1]
R. E. Battle
R. S. Booth
D. P. Bozarth[1]
R. Broadwater[2]
F. H. Clark
N. E. Clapp
R. A. Hedrick[1]
L. L. Joyner[3]
J. Lewin
C. L. Mason[1]
A. F. McBride[1]
O. L. Smith
R. S. Stone

Manuscript Completed: September 30, 1984

Date Issued:

[1]Science Applications, Inc., Oak Ridge, TN
[2]Tennessee Technological University, Cookeville, TN
[3]Joyner Engineers and Trainers, P.C., Forest, VA

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

NRC Fin Nos. B0467 and B0816

Prepared by
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831
operated by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U. S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-840R21400

ABSTRACT

Control failures in the Oconee-1 Nuclear Plant were examined to determine the extent of which such failures can impact plant safety. Plant systems capable of initiating plant overcooling and undercooling were identified, as well as those with potential for overfilling events in the steam generators.

Failure mode and effects analyses were conducted on these candidate plant systems, with computer analysis applied where appropriate. This latter process utilized a detailed hybrid computer model of Oconee-1, developed as part of this program. Where failures with safety consequences were found, probabilities of the pertinent scenarios were developed. Recommendations for corrective actions complete the report.

Executive Summary

1.0 INTRODUCTION

1.1 OBJECTIVES

The overall program is intended to assess the safety implications of nuclear power plant control systems by examining the consequences of control system failures and action, both planned and unplanned. Criteria will be developed for establishing the relative importance to safety of control systems; design and operation criteria will then be recommended for these systems based on their relative importance to safety.

In performing these tasks, a major objective is to assist in the resolution of Unresolved Safety Issue (USI) A-47 on Safety Implications of Control Systems. The Task Action Plan for that USI states that its objective "...is to perform an indepth evaluation of the control systems that are typically used during normal plant operation and to verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent non-safety grade control system failures."

This study embodies all of the objectives of USI A-47. It goes beyond the objectives of A-47, however, since this study addresses operator errors, sabotage, and harsh environments to a degree not included in the guidelines for A-47. It is intended that this work shall be done in a plant-specific fashion, and the first task (described in this report) provides a careful examination of reactor transients in one specific plant of Babcock and Wilcox (B&W) design, i.e., Oconee 1.

1.2 APPROACH

A Failure Mode and Effects Analysis (FMEA) is the standard method used for a systematic qualitative search for significant failures and their consequences. It has commonly been applied to elements of the reactor protection system, and it is this same formalism that we are extending to failures in control systems. In this process we identify a failure class and then define broad functional conditions which must occur to produce the problem under consideration. Each system is then examined for modes of failure and for the effects of each such failure mode. It is from this part of the study that we identify the failures which produce the broadest effects, or define the minimum set of failures that leads to certain kinds of consequences. Many of the failures treated in the FMEA can be disposed of on an a priori basis. Other events will be found to be already considered elsewhere (e.g., in the PTS program, or in Chapter 15 studies for licensing reports).

There will remain some residuum of system failures with potential safety consequences. These will be addressed through computer simulations in an activity referred to as the "augmented FMEA." Two criteria must be satisfied for a scenario from the FMEA process to be selected for the computer program:

A. There must be potential for overfilling, overcooling, or overheating, as determined by the broad FMEA, but without certainty as to the extent of the consequences
B. There must be no satisfactory alternate source (e.g., the PTS program or Chapter 15 studies) for computations from which the consequences in question can be determined.

1.3 LIMITATIONS OF THE STUDIES

No external events have been considered in this controls study of the Oconee-1 NSSS. The neglected categories include earthquakes, fires, and floods (external and internal to the containment), as well as sabotage. These initiating events are important, and they will be addressed in a later extension of the program but are outside the scope of the present report. Actions that the operator could take were identified. However, all possibilities were not studied nor, in general, were alternatives beyond the first identified.

In part because disclosures of controls dynamics and configurations have not been required for licensing or for other regulatory oversight, the controls data required for this study have not been routinely available. Though the final computer model is exhaustively complete, some exacerbating or ameliorating features may be missing from some transients through lack of information or the time to acquire it.

It must be recognized that the effects of control system failures during accident or normal plant operation will differ from plant to plant, and therefore it may not be possible to develop generic solutions to such problems as are found on a plant-specific basis. It is reasonable, however, to expect generic criteria that can be used for the plant-specific reviews.

2.0 SUMMARY OF RESULTS

2.1 BROAD FMEAs

The plant systems comprising the Oconee Nuclear Station have been identified and evaluated to assess potential impacts of system failures on three plant failure modes: Steam Generator (SG) Overfilling, Reactor Coolant System (RCS) Overcooling, and Insufficient Core Cooling. The systems and impacts of their failure modes were evaluated in three tasks. The first task consisted of performing a preliminary screening of the plant systems to select those systems whose failure could cause or exacerbate the plant failure modes. The effects of support system failures on systems directly affecting RCS response were considered specifically in the selection of systems.

The screening process was undertaken by mapping the systems which had functional interfaces to the coolant system primary and secondary. Then systems with interfaces to those systems were mapped. Functional relations across interfaces were examined to determine which systems had controls whose failures might impact system cooling.

In the ease of steam generator overfill the problem was simplified because it had been reduced to a single kind of functional failure in a single sub-system, the steam generator. A top down analysis was made to identify all control system failures which might impact such a failure.

2.2 STEAM GENERATOR OVERFILL

Steam generator overfill comes about when the feedwater flow rate overbalances the inflow heat rate to the steam generator. Heat input can be diminished by a drop in feedwater temperature or a drop in core power. Water flow can be increased by failures in the steam generator/feedwater control system. Our studies indicate that credible decreases in main feedwater temperatures are well compensated by control system action and that substantial additional failures would be required to bring on a serious safety problem in the primary. Decrease in core power can aggravate steam generator overfill. Further, such a decrease will occur in most important overfills because scram is expected to occur. We have found that excess water feed, as a result of improper actions of steam generator or main feedwater controls, may induce serious overfill with a credibly small number of control failures.

Steam generator overfill is a concern because it appears to have the potential to

a. produce secondary side damage which might compromise safety equipment or produce a cascade of events which might have primary side effects including radiological leakage,
b. cause densification of primary coolant, reducing pressure, possibly losing pressurizer control, possibly vapor-locking the primary flow path, possibly introducing excess reactivity from cold flow, and
c. provide excess cooling which might in some cases contribute to PTS.

We have found that a number of control system failure scenarios can lead to water entry into the steam line. In one case a single failure causes this; in several other cases, a preexisting undetected failure and one additional failure can bring on the event. Such events have occurred and have caused extensive damage to the affected steam system. Items which can be damaged include turbine drives on main feedwater and emergency feedwater pumps, turbine bypass valves, steam safety valves, steam line supports and the steam line itself. If we assume a steam line, which is not qualified for this environment, could rupture, then a cascade of dependent events might follow, including multiple steam generator tube rupture with small break LOCA vented direct to the atmosphere.

2.3 OVERCOOLING OF PRIMARY COOLANT

Conditions that cause RCS temperature to drop 100°F or more in an hour are considered to be overcooling. Also, tentatively, RCS cooling to a degree that causes system variables to assume values that should cause ESPS actuation is considered overcooling. For purposes of performing the system FMEAs, less restrictive criteria have been followed in proposing failure sequences to ensure that potentially significant sequences would not be excluded prematurely. The selection criteria were accordingly expanded to include transients whose post reactor trip development might include unusual decreases in RC pressure and inventory as well as temperature.

To aid in subsequent analyses, the overcooling criteria were related to RCS transient classes. These classes were (1) a release of reactor coolant from the RCS, (2) opening the pressurizer spray valve, and (3) increased heat transfer through the steam generator tubes.

Failures judged to be significant include:

Class 1 - (a) PORV fails open or fails to close, producing a small break LOCA.
(b) RC pump seaks fail.
(c) Steam generator tube ruptures.

Class 2 - Pressurizer spray valve fails open or fails to close.

Class 3 - (a) Steam generator overfills - see steam generator overfill section.
(b) Turbine bypass valve or main steam safety valve fails open or fails to close.

Two failure modes resulting from failures of ICS Panelboard KI branch circuits have been identified as having multiple effects. The redundant pressurizer level, steam generator level and steam pressure transmitters are powered from branch circuits HEX and HEY. A single failure of branch circuit HEX or HEY can result in overfeeding the pressurizer and either or both steam generators. If manually selected, deenergized steam pressure transmitters could result in the turbine bypass valves closing and remaining closed, challenging the main steam safety valves.

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

2.4 OVERHEATING PRIMARY SYSTEM

Plant systems potentially affecting the ability to replace reactor coolant lost from the RCS or affecting the ability to remove heat through the steam generators were selected for detailed FMEA. These systems included the control system portions of the HPI system, the pressurizer, steam generator and RC pump subsystems of the RCS, the main feedwater and condensate system and the main steam system. Instrumentation and systems supporting the operation of these systems were included in the analysis.

Several failures were found to result in a loss of reactor coolant or a loss of main feedwater flow to the steam generators. Most of these failures resulted in automatic initiation of HPI safety injection or emergency feedwater injection which would prevent the insufficient core cooling failure mode. Three failure modes, however, were found to create a situation where operator action would be required to prevent insufficient core cooling.

The first two failure modes comprise failure of two ICS power supply branch circuits either (1) auto power or (2) hand power, which result in loss of automatic control of main feedwater flow. In this condition, the operator may manually block feedwater flow to prevent overfeeding the steam generators. In the case of hand power failure, the main feedwater pump speed is reduced and may develop insufficient head to pump feedwater to the steam generators. In either case, main feedwater flow may cease without tripping the main feedwater pumps and consequently without automatic initiation of emergency feedwater flow. If the steam generators are allowed to boil dry, core decay heat will be removed by boiling in the RCS and rejection of steam and/or liquid through the pressurizer PORV and/or safety valves. If the operator fails to manually initiate main or emergency feedwater flow to the steam generators early in the transient and fails to manually initiate HPI prior to losing reactor coolant inventory in the core region, insufficient core cooling will occur.

The third transient consists of a letdown cooler tube failure combined with operator failure to maintain adequate flow to the HPI pumps. Following a tube failure (an isolatable small LOCA or RCS leak), the operating HPI pumps will be transferring the inventory of the letdown storage tank (LST) to the RCS. To the extent the operator fails to recognize the failed tube or fails to isolate the leak once recognized, the reduction in LST inventory will continue. This transient may result in ESPS actuation which would automatically terminate the transient. However, if it does not and the operator allows the LST to drain, the operating HPI pumps will be damaged.

3.0 HYBRID COMPUTER SIMULATIONS

A simulation program for the Oconee-1 system was developed on the ORNL hybrid computer. This was a necessary step in order to study control system functions which are central to this task. Existing simulations do not deal with control systems with sufficient detail and fidelity. A number of transients have been simulated and the results are included in the preceding discussion of results.

4.0 RECOMMENDATIONS

Several suggestions have been offered which could make the plant less susceptible to unacceptable control system failures. Most important of these would make the high level main feedwater pump trip less apt to fail. Other suggestions included (1) greater use of the plant computer to identify inconsistent sensor readings, and (2) classification of emergency procedures to call upon the operator explicitly to consult backup instrumentation in certain situations.

Instrumentation and Controls Division

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

DRAFT FINAL REPORT

Volume 2
Methods and Conclusions

P. N. Austin[1]
R. E. Battle
R. S. Booth
D. P. Bozarth[1]
R. Broadwater[2]
F. H. Clark
N. E. Clapp
R. A. Hedrick[1]
L. L. Joyner[3]
J. Lewin
C. L. Mason[1]
A. F. McBride[1]
O. L. Smith
R. S. Stone

Manuscript Completed: September 30, 1984

Date Issued:

[1]Science Applications, Inc., Oak Ridge, TN
[2]Tennessee Technological University, Cookeville, TN
[3]Joyner Engineers and Trainers, P.C., Forest, VA

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

NRC Fin Nos. B0467 and B0816

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

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

LIST OF FIGURES

LIST OF FIGURES (continued)

LIST OF TABLES

GLOSSARY

ATOG	abnormal transient operating guidelines
B&W	Babcock & Wilcox
BMCo	Bailey Meter Company
BWR	boiling water reactor
BWST	Borated water storage tank
CCW	component cooling water
CE	Combustion Engineering
CVCS	chemical and volume control system
CRT	cathode ray tube
CF	coreflood
CFT	coreflood tank
ECCS	emergency core cooling system
EFW	emergency feedwater
EHC	electro-hydraulic control
ESFAS	engineered safety features actuation system
FMEA	Failure Mode and Effects Analysis
FW	Feedwater
FSAR	Final Safety Analysis Report
H/A	hand/auto
HCU	hydraulic control unit
HPCI/S	High-pressure core injection spray
HPCS	high-pressure core spray
HPI	high-pressure injection
HPIS	high-pressure injection system
HPSIS	high-pressure safety injection subsystem
HPSW	high-pressure service waqter
HVAC	heating, ventilating, and air conditioning
ICS	Integrated control system
LOCA	loss of coolant accident
LOFW	loss of feedwater
LPCS	low-pressure core spray
LPI	low-pressure injection
LPSIS	low-pressure safety injection system
LPSW	low-pressure service water
MFW	main feedwater
MFWV	main feedwater control valve
MOV	motor-operated valve
MU	makeup
MSIV	main stream isolation valves
NSS	nuclear steam supply
NSSS	nuclear steam supply system
OTSG	once through steam generator
PORV	power operated relief valve
PRA	probabilistic risk assessment
PTS	pressurized thermal shock
PWR	pressurized water reactor
RCP	reactor coolant pump
RHR	residual heat removal
RC	reactor coolant
RCIC	reactor core isolation cooling

RCS	reactor coolant system
RV	reactor vessel
SG	steam generator
SLB	single line break
SUFW	startup feedwater
SUFWV	startup feedwater control valve
ULD	unit load demand

1.0 INTRODUCTION

1.1 OBJECTIVES

The overall program is intended to assess the safety implications of nuclear power plant control systems by examining the consequences of control system failures and action, both planned and unplanned. A properly performing control system can correct for failure in other parts of the plant, thus aborting a challenge to the safety system; contrarily a malfunctioning control system can create such a challenge. A principle of nuclear plant design is that the safety system must be capable of countering any conceivable action or inaction of the control system without danger to the plant or to the public. These concepts are being examined in practice by means of a thorough analysis of control/safety dynamics and interactions from a plant system perspective. Criteria will be developed for establishing the relative importance to safety of control systems; design and operation criteria will then be recommended for these systems based on their relative importance to safety.

In performing these tasks, a major objective is to assist in the resolution of Unresolved Safety Issue (USI) A-47 on Safety Implications of Control Systems. The Task Action Plan for that USI states that its objective "...is to perform an indepth evaluation of the control systems that are typically used during normal plant operation and to verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent non-safety grade control system failures."

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

"...On this basis it is generally believed that control system failures are not likely to result in loss of safety functions that could lead to serious events or result in conditions that the safety systems are not able to mitigate. Indepth studies for all the non-safety grade systems have not been performed however, and there exists some potential for accidents or transients being made more severe than previously analyzed, as a result of some of these control system failures or malfunctions."

"...Two potential concerns have already been identified in which a failure or malfunction of the non-safety grade control system can (1) potentially cause a steam generator or reactor vessel overfill, or (2) can lead to a transient (in PWRs) in which the vessel could be subjected to severe overcooling. In addition, there is the potential for an independent event like a single failure, (such as a loss of power supply, a short circuit, open circuit, control sensor failure) or a common mode event (such as a harsh environment caused by an

accident or a seismic event) to cause a malfunction of one or several control systems which would lead to an undesirable control action, or provide misleading information to the plant operator. These concerns will be reviewed and evaluated..."

This study embodies all of the objectives of USI A-47, as described above in quotations from the Task Action Plan. It goes beyond the objectives of A-47, however, since this study addresses operator errors, sabotage, and harsh environments to a degree not included in the guidelines for A-47.

1.2 SCOPE OF PROGRAM

As described above, the objectives of the overall task define three interrelated goals:

- To assess the safety implications of control systems by examining the effects of control system malfunctions on plant dynamic behavior and by investigating the interactions of such malfunctioning controls with other plant systems.
- To formulate a method for assessing the failure mode and effects of control systems on the basis of common cause, common mode, and other multiple failures such as cascade failures.
- To develop criteria for establishing the relative importance of control systems important to safety and to recommend importance to safety classifications and any changes to regulatory requirements as may be indicated by the results of this work.

In its approach, this task is specifically responsive to the four principal foci of NRC Task Action Plan A-47:

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

It is intended that this work shall be done in a plant-specific fashion, and the first task (described in this report) provides a careful examination of reactor transients in one specific plant of Babcock and Wilcox (B&W) design, i.e., Oconee 1.

1.3 APPROACH

A Failure Mode and Effects Analysis (FMEA) is the standard method used for a systematic qualitative search for significant failures and their consequences. It has commonly been applied to elements of the reactor protection system, these being considered not only necessary but also sufficient for the security of the plant. It is this same formalism that we are extending to failures in control systems.

The standard FMEA* provides an orderly method for studying the possible failure modes of a single component in an important system, treating all the causes and consequences of each such failure mode. In a plant with components numbered in tens or hundreds of thousands it is manifestly impossible to cover each of them in such a study. Accordingly, a number of steps are taken to pre-focus the effort. Some systems are excluded from consideration by the scope of the study, e.g., safety systems. Some classes of events are excluded because they are studied elsewhere, e.g., ATWS. The most important focusing is accomplished by categorizing the kinds of system failures that we search for: steam generator overfill, primary coolant overcool, overheat.

Given a failure class, for example steam generator overfill, we then define broad functional conditions which must occur to produce the problem under consideration. Such broad conditions are: too little primary side power for the secondary water flow, or said the other way, too much secondary side water flow for the available primary heat. We then identify the subsystems and components (and the systems which contain them) which can bring on any of these functional conditions. We also identify those subsystems and components, largely trips and controls, which are provided to give protection against these functional failures.

Next we identify any subsystems or components which significantly interface any of these subsystems and components. This procedure is the system survey. Chains of interfacing components are thereby identified where each member of the chain has some significance to the failure understudy.

Each component of each chain is then examined for modes of failure and for the effects of each such failure mode. It is from this part of the study that we identify the failures which produce the broadest effects, or define the minimum set of failures that leads to certain kinds of consequences.

The first step in performing an FMEA is to define the system to be analyzed. In the present case, this has meant an exhaustive listing of every system in the nuclear plant under study. Until the systems under consideration are narrowed to the fine details of specific designs, all PWRs involve much the same functions. This has permitted us to create a so-called generic systems list. These descriptions and interface identifications are prepared for each system. On a plant-specific inquiry the listing continues to the finest system level. Such lists and interfaces are crucial to the FMEA process.It is unlikely that a serious failure mode will be uncovered if the system affected is omitted during system definition.

Having defined the plant systems and described their operation, it is necessary to limit the cases examined to a manageable set by identifying the failure categories which will be examined. This process will in general use the selection criteria identified above to eliminate broad classes of systems which

*IEEE Std. 352-1975.

are not involved in the failures of concern. Moreover, in the systems which are of concern, selection of specific failure classes will limit the scenarios which must be examined and hence remove from consideration large classes of failure modes. In limiting anotherwise unmanageable task this is a vital step.

At this point in our description of the FMEA process we have identified all of the systems in the plant, described their functions and interfaces, and selected the classes of failures which will be addressed. This is the point at which the first judgmental decisions are made. Those systems without input to the failure classes of interest are eliminated, using as basis the previously developed functional descriptions, interfaces, and criteria.

Here the FMEA process continues by conceptually failing each of the systems potentially contributory to one of the three classes of safety consequences, with the results determined (so far as this is possible) on an a priori basis. This process is referred to as a "broad FMEA." At this stage both single and double failures are postulated. Probabilities of these events will be estimated at a later time, but only for those which prove to be of interest.

Many of the failures lead to events which are clearly benign. These will be dropped from further consideration. Other events will be found to be precursors for accident sequences already considered elsewhere (e.g. in the PTS program, or in Chapter 15 studies for licensing reports). Where such cases have safety-related consequences the precursor events will be documented, but no further computer analysis need be done.

There will remain some residuum of system failures with potential safety consequences. These will be addressed through computer simulations in an activity referred to as the "augmented FMEA." As outlined above, two criteria must be satisfied for a scenario from the FMEA process to be selected for the computer program:

A. There must be potential for overfilling, overcooling, or overheating, as determined by the broad FMEA, but without certainty as to the extent of the consequences
B. There must be no satisfactory alternate source (e.g., the PTS program or Chapter 15 studies) for computations from which the consequences in question can be determined.

The above sequence is the primary approach to the FMEA process, i.e., an orderly assessment of the failure consequences of each identified system in the plant. Where failure of a control element produces actual or potential compromises to safety, interfacing systems are examined for contributions to the failure or to the consequences. Where a double failure is required to produce the hazard in question, common sources for the two failures will be sought, particularly in control logic sequence.

Systems which have a capability to impact the chosen failure classes are systematically examined for failure modes and the resulting first order effects. "First order" refers to those consequences which can be determined by logical inspection. For example, on a systems basis we may postulate a malfunction in

which a turbine bypass valve fails open, allowing the full steam flow to bypass the turbines. The effect on a first order basis will be loss of pressure in the steam generator with possible overcooling. There may be other effects related to the condenser. Quantitative outcomes describing specific pressures and temperatures in various parts of the system will not in general be available from this type of deductive analysis. For quantitative results, particularly for scenarios in which the affected system feeds back altered input conditions to the initiating event, failure effects must be determined by computer analysis.

The modality for computer analysis of the Oconee-1 plant is a hybrid computer model developed at ORNL. Before modeling or analysis could start, it was necessary to obtain detailed design information regarding the plant to be studied. The first task was to establish a collection of drawings and reports on each assigned plant. The information was obtained from the following sources:

- the applicable utility, where possible
- various dockets and resources of the NRC
- other ORNL projects
- staff experience
- subcontractors and their sources

The data collection effort was an extensive one in which the available material was examined as it came in, with requests made for additional material where gaps were indicated. Plant data were then input to a hybrid computer model whose methodology generally follows the structure of RELAP-4. The plant model is in general digital, the control model, analog.

Cases selected as requiring analysis were prioritized in order of estimated importance, grouping them in lots of similar runs to minimize programming changes. The results of these runs were then fed back to the (thus) augmented FMEA process for the final determination of the consequences of controls failures. Fig. 1.1 shows the overall flow chart for the entire process.

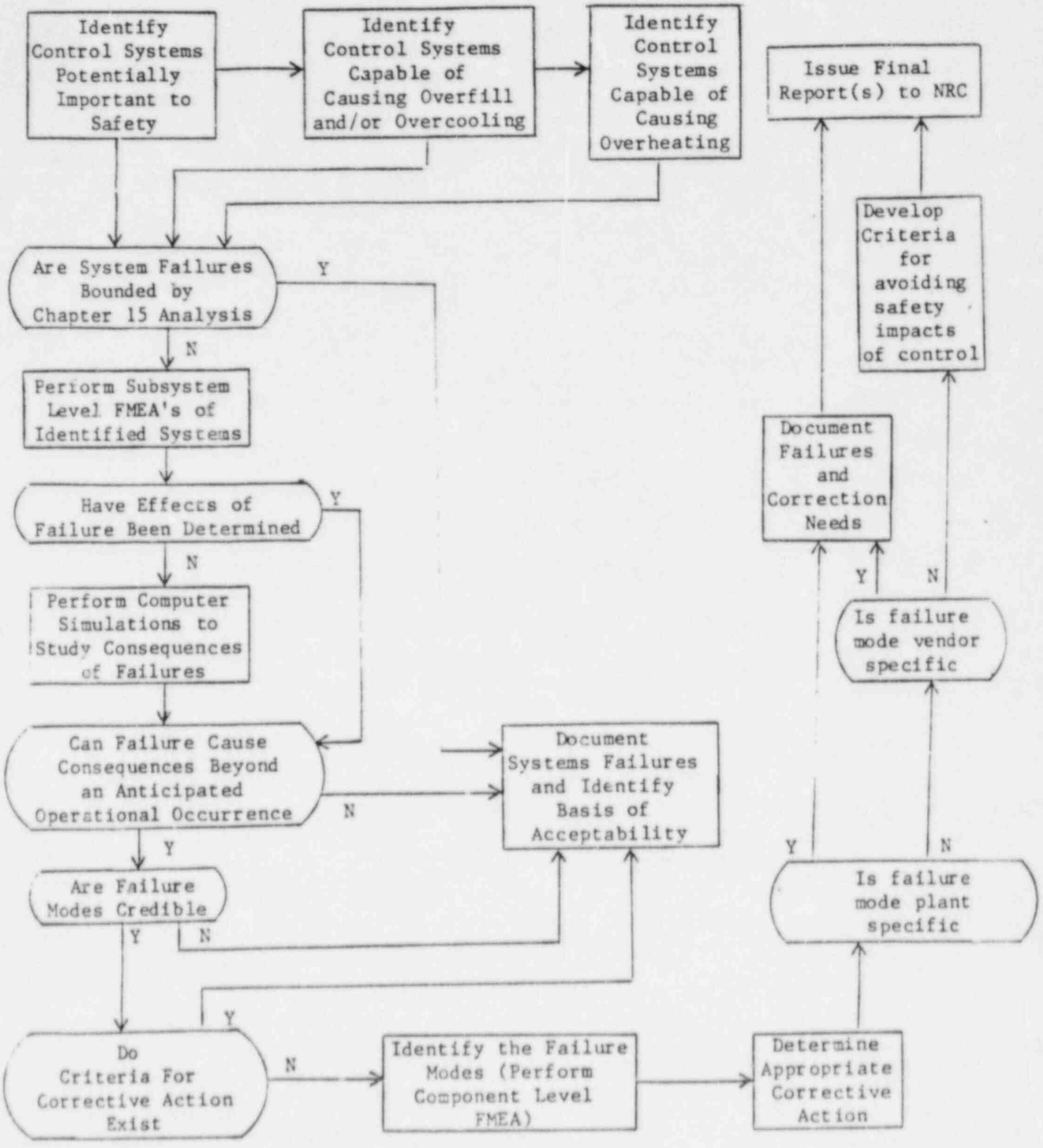
1.4 LIMITATIONS OF THE STUDIES

No external events have been considered in this controls study of the Oconee-1 NSSS. The neglected categories include earthquakes, fires, and floods (external and internal to the containment), as well as sabotage. These initiating events are important, and they will be addressed in a later extension of the program but are outside the scope of the present report. Actions that the operator could take were identified. However, all possibilities were not studied nor, in general, were alternatives beyond the first identified. Fully developed, this additional study could be a project in itself.

Figure 1-1

PROGRAM FLOW FOR STUDY OF SAFETY EFFECTS OF

NUCLEAR POWER PLANT CONTROL SYSTEM FAILURES



Any nuclear power station system-level analysis performed by itself will miss some system failure modes and interactions. Only two-at-a-time multiple failures were considered in the initial broad FMEA. Obviously, extension is possible, but this may not be meaningful (deterministically or stochastically) or practical for all combinations. Only single failures were considered in the second- and third-level FMEAs.

In part because disclosures of controls dynamics and configurations have not been required for licensing or for other regulatory oversight, the controls data required for this study have not been routinely available. Collection of this information has been a costly and time-consuming operation, and though the final computer model is exhaustively complete, some exacerbating or ameliorating features may be missing from some transients through lack of information or the time to acquire it.

This report does not reflect the results of sensitivity studies; these have been planned but not yet undertaken. The objective is to determine the effects of variations in input data, plant conditions, or parameter values (trip points, for example) on our conclusions and results. These variations can reflect limitations in detailed knowledge of the Oconee-1 plant but, more importantly, should allow for differences between Oconee-1 and other plants in its class. This latter requirement may be important when our major conclusions are examined for generic implications.

It must be recognized that the effects of control system failures during accident or normal plant operation will differ from plant to plant, and therefore it may not be possible to develop generic solutions to such problems as are found on a plant-specific basis. It is reasonable, however, to expect generic criteria that can be used for the plant-specific reviews.

1.5 SUMMARY OF RESULTS

1.5.1 Systems Selected

The plant systems comprising the Oconee Nuclear Station were identified and evaluated to assess potential impacts of system failures on three plant failure modes: Steam Generator (SG) Overfilling, Reactor Coolant System (RCS) Overcooling, and Insufficient Core Cooling. The first task consisted of performing a preliminary screening of the plant systems to select those systems whose failure could cause or exacerbate the plant failure modes. The effects of support system failures on systems directly affecting RCS response were considered specifically in the selection of systems.

The screening process was undertaken by mapping the systems which had functional interfaces to the coolant system primary and secondary. Then systems with interfaces to those systems were mapped. Functional relations across interfaces were examined to determine which systems had controls whose failures might impact system cooling.

In the case of steam generator overfill the problem was simplified because it had been reduced to a single kind of functional failure in a single sub-system, the steam generator. A top down analysis was made to identify all control system failures which might impact such a failure.

1.5.2 FMEA for Steam Generator Overfill

Steam generator overfill comes about when the feedwater flow rate overbalances the inflow heat rate to the steam generator to the degree that insufficient steam is formed and the water inventory rises. Heat input can be diminished by a drop in feedwater temperature or a drop in core power. Water flow can be increased by failures in the steam generator/feedwater control system. Our studies indicate that credible decreases in main feedwater temperatures are well compensated by control system action and that substantial additional failures would be required to bring on a serious safety problem in the primary. Decrease in core power can aggravate steam generator overfill. Further, such a decrease will occur in most important overfills because scram is expected to occur. We have found that excess water feed, as a result of improper actions of steam generator or main feedwater controls, may induce serious overfill with a credibly small number of control failures.

Steam generator overfill is a concern because it appears to have the potential to

a. produce secondary side damage which might compromise safety equipment or produce a cascade of events which might have primary side effects including radiological leakage,
b. cause densification of primary coolant, reducing pressure, possibly losing pressurizer control, possibly vapor-locking the primary flow path, possibly introducing excess reactivity from cold flow, and
c. provide excess cooling which might in some cases contribute to PTS.

We have found that a number of control system failure scenarios can lead to water entry into the steam line. In one case a single failure causes this; in several other cases, a preexisting undetected failure and one additional failure can bring on the event. Such events have occurred and have caused extensive damage to the affected steam system. Items which can be damaged include turbine drives on main feedwater and emergency feedwater pumps, turbine bypass valves, steam safety valves, steam line supports and the steam line itself. If we assume a steam line, which is not qualified for this environment, could rupture, then a cascade of dependent events might follow, including multiple steam generator tube rupture with small break LOCA vented direct to the atmosphere.

1.5.3 FMEA for Overcooling the Primary System

A number of failure modes have been identified which could cause the RCS temperature to decrease. The rate and amount of such decreases and their possible subsequent effects require simulation of the system's response to the control system failures. RCS overcooling is not of interest in this study until it approaches an amount which can have safety implications. Cooling associated with normal shutdown procedures, for instance, within Technical Specifications, is of no concern.

Conditions that cause RCS temperature to drop 100°F or more in an hour are considered to be overcooling. Also, tentatively, RCS cooling to a degree that causes system variables to assume values that should cause ESPS actuation is considered overcooling. For purposes of performing the system FMEAs, less restrictive criteria have been followed in proposing failure sequences to ensure that potentially significant sequences would not be excluded prematurely. The selection criteria were accordingly expanded to include transients whose post reactor trip development might include unusual decreases in RC pressure and inventory as well as temperature.

To aid in subsequent analyses, the overcooling criteria were related to RCS transient classes. These classes were (1) a release of reactor coolant from the RCS, (2) opening the pressurizer spray valve, and (3) increased heat transfer through the steam generator tubes.

Failures judged to be significant include:

Class 1 - (a) PORV fails open or fails to close, producing a small break LOCA.
(b) RC pump seaks fail.
(c) Steam generator tube ruptures.

Class 2 - Pressurizer spray valve fails open or fails to close.

Class 3 - (a) Steam generator overfills - see steam generator overfill section.
(b) Turbine bypass valve or main steam safety valve fails open or fails to close.

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

Two failure modes resulting from failures of ICS Panelboard KI branch circuits have been identified as having multiple effects. The redundant pressurizer level, steam generator level and steam pressure transmitters are powered from branch circuits HEX and HEY. One of the redundant transmitters is selected manually for each parameter for input to the control circuitry. Based on the transmitter selection, a single failure of branch circuit HEX or HEY can result in overfeeding the pressurizer and either or both steam generators. If manually selected, deenergized steam pressure transmitters could result in the turbine bypass valves closing and remaining closed, challenging the main steam safety valves.

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

1.5.4 FMEA for Overheating the Primary System

Plant systems potentially affecting the ability to replace reactor coolant lost from the RCS or affecting the ability to remove heat through the steam generators were selected for detailed FMEA. These systems included the control system portions of the HPI system, the pressurizer, steam generator and RC pump subsystems of the RCS, the main feedwater and condensate system and the main steam system. Instrumentation and systems supporting the operation of these systems were included in the analysis.

Several failures were found to result in a loss of reactor coolant or a loss of main feedwater flow to the steam generators. Most of these failures resulted in automatic initiation of HPI safety injection or emergency feedwater injection which would prevent the insufficient core cooling failure mode. Three failure modes, however, were found to create a situation where operator action would be required to prevent insufficient core cooling.

The first two failure modes comprise failure of two ICS power supply branch circuits either (1) auto power or (2) hand power, which result in loss of automatic control of main feedwater flow. In this condition, the operator may manually block feedwater flow to prevent overfeeding the steam generators. In the case of hand power failure, the main feedwater pump speed is reduced and may develop insufficient head to pump feedwater to the steam generators. In either case, main feedwater flow may cease without tripping the main feedwater pumps and consequently without automatic initiation of emergency feedwater flow. If the steam generators are allowed to boil dry, core decay heat will be removed by boiling in the RCS and rejection of steam and/or liquid through the pressurizer PORV and/or safety valves. If the operator fails to manually initiate main or emergency feedwater flow to the steam generators early in the transient and fails to manually initiate HPI prior to losing reactor coolant inventory in the core region, insufficient core cooling will occur.

The transients resulting from these power supply failures are expected to proceed relatively slowly. The operator is expected to have approximately one-half hour to reestablish steam generator cooling or approximately one hour to initiate HPI safety injection to avert insufficient core cooling. However, the transients are important for two reasons. First, the transients include inoperability of the operating system (main feedwater) simultaneous with the loss of automatic actuation for the emergency back-up systems. Second, both power supply failure cases result in numerous spurious control room alarms and indications. While these failures would not prevent successful operator action (e.g., defeat all indications of steam generator level and reactor coolant subcooling), they would tend to distract the operators and make successful ooperator action less likely.

The third transient consists of a letdown cooler tube failure combined with operator failure to maintain adequate flow to the HPI pumps. Following a tube failure (an isolatable small LOCA or RCS leak), the operating HPI pumps will be transferring the inventory of the letdown storage tank (LST) to the RCS. To the extent the operator fails to recognize the failed tube or fails to isolate the leak once recognized, the reduction in LST inventory will continue. This transient may result in ESPS actuation which would automatically terminate the transient. However, if it does not and the operator allows the LST to drain, the operating HPI pumps will be damaged.

Although recovery, even with a damaged HPI pump, is likely due to the HPI pump redundancy (three pumps), the transient does represent a case of a small LOCA potentially including degraded HPI safety injection. Furthermore, the transient does present the operator with the situation of decreasing pressurizer level and degraded makeup flowrate and the potential for a serious error. If the operator mistakenly starts the second or third HPI pumps, these pumps also would be damaged and the transient risk significantly increased.

1.5.5 Recommendations

Several suggestions are offered which could make the plant less susceptible to unacceptable control system failures. The most important of these would make the high level main feedwater pump trip less apt to fail. Other suggestions include (1) greater use of the plant computer to identify inconsistent sensor readings, and (2) classification of emergency procedures to call upon the operator explicitly to consult backup instrumentation in certain situations.

2. SELECTION OF PLANT SYSTEM FOR DETAILED EXAMINATION

2.1 CRITERIA FOR SYSTEM SELECTION

For this work the initial tasks are:

- Selection of nuclear plant systems with potential to initiate or aggravate over-filling of the steam generator
- Selection of nuclear plant systems with potential to initiate or aggravate overcooling the primary system
- Selection of nuclear plant systems with potential to initiate or aggravate core damage through overheating.

The selection criteria for steam generator (SG) overfill identify those control systems whose failure or misoperation can introduce feedwater in amounts sufficient to fill the SG to the degree that water enters the steam lines.

The criteria for primary overcool identify those control systems whose failure or misoperation can lead to uncontrolled primary heat removal at rates greater than the rate of heat production, to the extent that conditions inimical to safe operation may be produced.

In NSSS plants with vulnerable pressure vessels, the study of pressurized thermal shock (PTS) provides the most critical index of overcooling. This subject is separately addressed by the NRC as Unresolved Safety Issue A-49. Plant-specific overcooling criteria have been developed for each of the four nuclear plants examined in detail by the PTS program. These criteria are functions of the metallurgy of the reactor vessel concerned (particularly of the welds), of the radiation history (fluence) of the critical regions of the vessel at risk, of the internal vessel pressure at the time of the overcooling event and of the minimum temperature reached at the conclusion of the transient. Given these input parameters, a series of PTS fracture mechanics calculations has provided tables of maximum permissible rate of exponential temperature decay versus pressure and temperature. Both of the nuclear plants studied in the controls program have been subjects for PTS investigation, and for these plants, detailed and specific quantitative definitions are available for overcooling in a PTS context (ref. TM-7931). Although these PTS calculations quantitatively define the overcooling concerns for the Oconee-1 and Calvert Cliffs-1 nuclear stations, they are based on the unique metallurgy of two specific pressure vessels, and so are plant-specific rather than generic in nature. For a newer reactor vessel with a low accumulation of neutron fluence and/or negligible contents of nickel and copper, PTS concerns may be virtually nonexistent. In such a plant, overcooling limits will be dictated by loss of pressure, loss of volume, or cold slug reactivity considerations, and not by concern for vessel embrittlement. Even in the older plants, non-PTS concerns may supply the bounding limits for overcooling due to controls failures. Both PTS and non-PTS overcooling concerns will be addressed in the present study. In general, the control systems of concern are those which match steaming rate to power production, and comprise systems in both theprimary and secondary circuits.

Criteria for primary overheating are similar to those for primary overcooling, with the pertinent control systems being those whose failures result in heat rate inbalances wherein heat removal rates are less than the rate of power production to the extent that conditions inimical to safe operation (e.g., fuel melting) may be produced.

Because overcooling events are crucial determinants to the issue of pressurized thermal shock (PTS), and because steam generator overfill contributes to this chain as one potential instigator of overcooling, the first two tasks above interact strongly with the ongoing PTS program. Overfilling and overcooling scenarios developed in this program have been used as early inputs to PTS; dominant overcooling event sequences developed by the PTS program will be factored into the program for safety implications of control.

2.2 INPUT FROM THE HISTORICAL FAILURE RECORD

NRC IE Information Notices, LERs, and other historical records were examined and used to provide a background of control failure expectations. Under subcontract with ORNL, The University of California (UCLA) provided an extremely thorough background search, visiting seven plant sites in the process. The remainder of this section describes the data gathering done by UCLA.

A data base on control system failures was developed by a search of LER files for the period 1969 through 1981. This was supplemented with data derived from NUREG reports on Nuclear Power Plant operating experience such as plant outages, and other operating experience gleaned from a sampling of station records for several specific LWRs. Plant visits generated reasonably detailed information concerning the plant operating history, and for such plants the data is considered to be "complete". For the other plants, the information is partial, in that it is LER-based. UCLA accumulated 190 events that occurred at PWR plants in the period 1969 through 1981, of which only 94 are represented by LERs.

Through the cooperation of Combustion Engineering (CE), UCLA personnel were able to obtain information on shutdown and power reductions attributed to selected systems and components, extracted from CE's Reliability Data System (RDS). This system compiles information on PWR plants only.

Seven plant specific studies were made by visiting each site for several days. Each plant's operating and maintenance experience were reviewed by examining documents such as:

- Plant Incident Reports
- Abnormal Occurrences Reports
- Shutdown and Power Reduction Reports
- System Histories for Abnormal Occurrences
- Component Maintenance Logs

and a sample of six months' station logs to assure that the above mentioned reports reflect all the related occurrences. Each plant study has added new data to that which were obtained before; 41 new events at the 4 PWR plants and 25 new events at the 3 BWR plants were obtained.

Plant visits have generated the most detailed set of data of the visited plant operating history and this information is considered to be "complete", while for other plants, information is partial ("official") data in the sense that it is LER-based.

The Nuclear Safety Information Center (NSIC) compiled LERs for the purpose of this study. Bearing in mind that the definition of what is a safety-grade or non-safety-grade control system has changed with time, the NSIC search of LERs was made as general as possible and includes all the events that are related to control systems in general. The non-safety-grade control system failure events were sorted by hand.

The Nuclear Safety and Analysis Center (NSAC) search, which was done for the purpose of checking the NSIC search for completeness, generated new events and led to a problem in finding the proper keywords for the use of the NSIC data bank. It should be noted that the NSAC file is based on post 1977 events; thus, the NSIC search was checked vs. the NSAC file for the time period 1978 through 1981, and conclusions were drawn over the extrapolated time period of interest.

New searches with additional keywords for the following search were done at NSIC, exhausting this source of information. This entire process has accumulated 93 LER events that have occurred in PWR plants.

Control system failures do not necessarily require an LER if the Technical Specifications (TS) of the plant were not violated because either the plant protection system or the operator acted properly to overcome the transient condition. Potential failure of the protection or the heat removal systems may result in an occurrence which develops into a core integrity threat and thus must be included in our study. Thus other sources of information were needed.

The LER computer searches were supplemented with information derived from published reports. The only germane information is a list of forced outages and their causes regardless of whether the causes are attributed to safety-grade or non-safety-grade equipment failure. The sources of this information are the plant monthly operating reports. Unfortunately, if a non-safety failure does not result in a shutdown, it is not mentioned in the report. For the purpose of our study, the "Nuclear Power Plant Operating Experience for 19XX" reports summarizing forced outages and their causes for the years 1973 through 1980, are the most useful of all references analyzed. This source has added, as expected, new events to the data base because many outages are not necessarily LERs.

The tables in the NUREG reports include short descriptions of the events which are insufficient for the purpose of analysis. UCLA requested additional information from 22 PWR utilities (38 PWR plants), since there is no requirement to publish this information under the current USNRC rules and regulations. These requests resulted in selective cooperation from the utilities, and generated 42 new events that have occurred in PWR plants.

Based on the investigation described, a complete listing of controls - induced challenges to safety was provided to ORNL. This was used as a data base for possible candidate scenarios for safety analysis.

2.3 SELECTION OF PLANT SYSTEMS FOR THE STUDY OF OVERFILLING/OVERCOOLING EVENTS

Overfilling and overcooling events were first addressed in the context of pressurized thermal shock (PTS). Information on the resulting system selection process is presented in Appendix B. The systems selected as possible contributors to overfilling/overcooling are shown in Table B.3, reproduced for convenience below.

Table B.3. Generic Systems Involved in Overcooling Events

NO3[a]	Reactor coolant system
NO4	Reactor coolant system
NO7	Nuclear instrumentation system
NO8	Residual heat removal/low-pressure safety injection system
SO2	Engineered safety features actuation system
SO3	Safety injection system
SO5	Auxiliary feedwater system
C10	Containment spray system
EO3	Instrumentation and control power system
PO1	Main steam system
PO2	Turbine generator system
PO2.A[a]	Electro-hydraulic turbine control subsystem
PO3	Turbine bypass system
PO4	Condenser and condensate system
PO5[a]	Feedwater system
WO3	Cooling water systems
WO4	Service water systems
WO5	Refueling system

[a]Interfaces with B&W's Integrated Control System.

2.4 SELECTION OF PLANT SYSTEMS FOR THE STUDY OF INSUFFICIENT CORE COOLING AND RCS OVERCOOLING EVENTS

The impact of many plant systems on insufficient core cooling or RCS overcooling transients is expected to be minor. Thus, the purpose of a plant specific system list with clearly identified interfaces is to aid in the selection of only those systems having a potential impact on reactor coolant system (RCS) in general and these transients in particular. Due to the large number of systems and components in a nuclear power plant, this preliminary screening is necessary to determine which systems require detailed analysis.

An insufficient core cooling transient is defined, for purposes of this report, as a transient significantly impacting the ability of the RCS to remove the heat generated in the reactor core following reactor trip. RCS overcooling is defined as a transient resulting in an excessive rate of heat removal from the RCS. Since the response of the RCS to postulated initiating transients is integral to either the insufficient core cooling or RCS overcooling transients, it was concluded that, as a first screening criterion, any system having a direct interface with the reactor coolant system would be a candidate for further analysis. Specific selection of systems related to insufficient core cooling and RCS overcooling is described in Sections 2.4.3 and 2.4.4.

2.4.1 Oconee 1 Systems List

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

1. Nuclear Systems include the reactor core and those systems and subsystems which monitor and control core reactivity, remove heat from the core, and otherwise directly support the safe operation of the reactor.
2. Engineered Safeguards Systems include those systems, other than containment systems, which are used to mitigate the effects of reactor accidents such as those specified in the FSAR.

3. Containment Systems include the reactor building and those systems needed to prevent reactor building overpressure, to prevent excessive leakage from the reactor building to the environment, and to provide a habitable atmosphere inside the reactor building.
4. Power Conversion Systems include the systems and components that transform, or support the transformation of, heat energy produced by the reactor core into electrical energy.
5. Process Auxiliary Systems include those systems and subsystems that support the plant systems directly involved in the operation of the reactor coolant systems.
6. Plant Auxiliary Systems provide support to other plant activities and personnel.

The systems included in each grouping are shown in Tables 2.4.1 - 2.4.6. A system identification was assigned to each system in order to simplify the subsequent interface analysis. Note that electrical systems have not been included; the effects of electrical system failures on the plant are being analyzed separately from this study (References 3 and 4).

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

2.4.2 Systems Affecting Core Cooling

Based on the systems lists and interfaces, specific systems were identified as having a potential impact on insufficient core cooling or RCS overcooling transients. The selection criteria used are not specific to either transient; systems potentially affecting reactor coolant system transients, in general, are selected. The following criteria were used to identify these systems:

1. All systems having a direct (first order) interface with the reactor coolant system (including the pressurizer and the steam generator) were listed. These systems are shown in Table 2.4.7.

TABLE 2.4.1. OCONEE 1 NUCLEAR SYSTEMS (Nxx)

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

TABLE 2.4.2. OCONEE 1 ENGINEERED SAFEGUARDS SYSTEMS (Sxx)

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

TABLE 2.4.3. OCONEE 1 REACTOR BUILDING/CONTAINMENT SYSTEMS (Cxx)

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

TABLE 2.4.4. OCONEE 1 POWER CONVERSION SYSTEMS (Pxx)

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

TABLE 2.4.5. OCONEE 1 PROCESS AUXILIARY SYSTEMS (Wxx)

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

TABLE 2.4.6. OCONEE 1 PLANT AUXILIARY SYSTEMS (Xxx)

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

TABLE 2.4.7. FIRST ORDER REACTOR COOLANT SYSTEM INTERFACES

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

*1 = Interface <u>from</u> reactor coolant <u>to</u> interfacing system.
2 = Interface <u>to</u> reactor coolant <u>from</u> interfacing system.
3 = Interface <u>to</u> and <u>from</u> reactor coolant.

2. From this list, several systems were eliminated for reasons described below and shown in Table 2.4.7:
   (1) Only non-safety-qualified control systems have been selected. Safety systems were not included because these systems are being analyzed in detail under separate NRC programs (Reference 5).
   (2) Only those systems in operation or standby during normal plant power operation were included. Systems such as those required for refueling or shutdown decay heat removal thus were not included. These systems are manually placed in operation only after a controlled shutdown of the reactor coolant system to less than 300°F and less than 300 psi.
   (3) Only those systems directly affecting reactor coolant system response were selected. Those interfacing systems affected by but not affecting reactor coolant system response were eliminated. (It should be noted that some systems eliminated for this reason may be selected as an interfacing system - see Item 3 below.)
3. For the remaining systems, all systems interfacing with the systems selected in Table 2.4.7 were identified. This list of second order interfacing systems, excluding those also selected in Table 2.4.7, is shown in Table 2.4.8.

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

To ensure completeness and to verify the adequacy of the selection procedure, each of the systems eliminated was briefly evaluated again to assess their potential impact on reactor core cooling.

TABLE 2.4.8. SECOND ORDER REACTOR COOLANT SYSTEM INTERFACES

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

TABLE 2.4.8. (Continued)

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

*1 = Interface <u>from</u> first order system <u>to</u> second order system.
2 = Interface <u>to</u> first order system <u>from</u> second order system.
3 = Interface <u>to</u> and <u>from</u> first order system.
Note: Interfaces with direction = 1 have not been included.

2.4.3 Systems Affecting Insufficient Core Cooling

In Section 2.4.2, the systems which potentially affect the response of the Reactor Coolant System (RCS) have been identified. Of these systems, those potentially affecting core cooling are identified. Section 2.4.3.1 presents the definition of insufficient reactor core cooling for purposes of this analysis. In Section 2.4.3.2, the functions of the systems identified in Tables 2.4.7 and 2.4.8 are evaluated to identify those systems potential affecting core cooling cooling as defined.

2.4.3.1 Definition of Insufficient Reactor Core Cooling

The removal and transport of the heat generated in the reactor are the direct or indirect functions of most systems comprising a nuclear power station. Several operating modes can be defined to describe possible core removal processes:

1. Power Operation: With the core producing up to 103% of rated thermal power,* the plant operating systems transport the heat from the core to produce electric power and waste heat. This operating mode requires the proper operation of most plant control systems.

2. Normal Hot Shutdown: Failure of one or more operating systems can result in the Reactor Protection System (RPS) initiating a reactor trip which terminates critical operation of the core. The plant operating systems normally transport the core decay heat (<7% of rated power) to the condenser where it is rejected to the environment.

   Failure of the plant to trip (achieve core subcriticality) involves a failure of a safety system. This accident condition has been studied extensively in the Anticipated Transients Without Scram (ATWS) program and is considered beyond the scope of the insufficient core cooling analysis.

---

*103% of rated power is a control system limit. Safety system reactor trip limits up to 112% of rated power are possible.

3. Emergency Hot Shutdown: In the event the normal operating systems fail to transport the decay heat to the condenser, emergency systems, including the emergency feedwater (EFW) system, can continue to provide a heat removal path through the steam generators. If the main condenser is unavailable, the heat will be rejected to the atmosphere via the main steam code safety valves.

4. Degraded Safe Shutdown: Achieving one of the hot shutdown operating modes is desirable in terms of recovery from the initiating failure and reestablishing power operation. However, adequate core heat transfer from a subcritical core only requires a sufficient inventory of reactor coolant in the core region. If a hot shutdown mode cannot be maintained, the heat transfer from the core to the reactor coolant will continue in a pool boiling mode. The heat will be rejected to the containment atmosphere via the pressurizer relief (PORV) or code safety valves. Reactor coolant inventory can be maintained in this mode from the high pressure injection (HPI) system.

From the above descriptions of the operating modes, insufficient core cooling can only occur if:

1. A hot shutdown mode (steam generator heat transfer) cannot be maintained.
2. Reactor coolant inventory is not maintained by the HPI system.

Although sufficient core cooling can be ensured by maintaining reactor coolant inventory regardless of the steam generator function, adequate steam generator cooling can eliminate the need to inject coolant with the HPI system. The exception to this is a transient involving a net loss of reactor coolant from the RCS. Loss of coolant requires HPI in the long term even if the steam generators are removing heat from the RCS. The correlation of the insufficient core cooling characteristics and possible system failure modes is outlined in Table 2.4.9.

TABLE 2.4.9. INSUFFICIENT CORE COOLING AND POTENTIAL INITIATING CAUSES

Insufficient Cooling Characteristics	Principal Causes	Secondary Causes
1. Loss of Steam Generator Cooling	1.1 Loss of Main and Emergency Feedwater Energy	1.1.1 Trip of Main Feedwater Pumps and Failure of Emergency Feedwater System
		1.1.2 Isolation of Main Feedwater Flow and Failure of Operator to Manually Initiate Emergency Feedwater
	1.2 Net Release of Reactor Coolant from the RCS	1.2.1 Failure of the HPI System following a Loss of Coolant Accident (LOCA) (Including Transient Induced LOCAs)
2. Insufficient Inventory of Reactor Coolant in the RCS	2.1 Failure of the HPI System following a LOCA (Including a Transient Induced LOCA)	2.1.1 Failure of the HPI following Control System Induced LOCAs: 1. PORV Opens and Remains Open 2. Pressurizer Safety Valve Opens and Remains Open 3. Net Release of Reactor Coolant from the RCS to the Makeup and Purification (MU&P) System 4. RC Pump Seal Failure Occurs

TABLE 2.4.9. (Continued)

Insufficient Cooling Characteristics	Principal Causes	Secondary Causes
	2.2 Failure to Manually Initiate HPI following a Loss of Steam Generator Cooling Transient	2.2.1 See Item 1.1 above

These failure modes define transients of potential significance to insufficient core cooling. Transient conditions defined by these failure modes (which are subsequently expanded in detailed failure mode analyses) will be functionally analyzed using the Oconee hybrid computer model to predict the resulting RCS response and the impacts on plant safety.

The characteristics of insufficient core cooling as described above and in Table 2.4.9 involve failures of safety systems. Although safety system failure modes are beyond the scope of the present study, the influence of control system failures on possible sequences of events leading to insufficient core cooling would be useful in assessing the impact of control system failures on plant safety.

As discussed above, control system failures can contribute to the initiation of both the loss of steam generator cooling sequences and the small LOCA sequences. Furthermore, control system failures may affect the ability of the safety systems to perform their function. The extent to which these control systems interactions affect the insufficient core cooling sequences in the Oconee design is the subject of this analysis. With respect to the failure modes identified, the control systems listed in Tables 2.4.7 and 2.4.8 have been reevaluated to assess their potential impact on insufficient core cooling. Those systems which cannot be excluded from contributing to insufficient core cooling, as shown in Table 2.4.10, are identified for further analysis. The results of the detailed FMEA of these systems are discussed in Section 3.3.

2.4.4 Systems Affecting Reactor Coolant System Overcooling

In Section 2.4.1 and 2.4.2, the systems which potentially affect the response of the RCS have been identified. Of these systems, those potentially affecting RCS overcooling are identified and discussed in Section 2.4.4. Section 2.4.4.1 presents the definition of RCS overcooling for purposes of this analysis. In Section 2.4.4.2, the functions of the systems identified in Tables 2.4.7 and 2.4.8 are evaluated to identify those systems potential affecting RCS overcooling as defined.

TABLE 2.4.10. POTENTIAL IMPACTS OF FIRST AND SECOND ORDER REACTOR COOLANT SYSTEM INTERFACE SYSTEMS ON INSUFFICIENT CORE COOLING

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

TABLE 2.4.10. (Continued)

System ID	System Name	Potential Impact on Insufficient Core Cooling
N05.B	Coolant Storage	
N05.C	Coolant Treatment System	
N05.D	Post Accident Sampling	
N05.E	High Pressure Injection	
C03	Reactor Building Ventilation	The effect of containment air temperature changes on heat transfer from the RCS is considered to be insignificant. The effects of loss of ventilation on component operability is considered to be beyond the scope of the study.
P01	Main Steam and Turbine Bypass	Power conversion systems and subsystems analyzed in detail.
P02	Turbine-Generator System	
P03	Main Condenser	
P04	Condensate and Feedwater	
W01	Radioactive Waste	System was selected based on its interface with the Non-Nuclear Instrumentation. However, the interface consists of providing parameter signals for display only. Failures of the Radioactive waste system not considered to have any significant impact on insufficient core cooling.
W03	Reactor Building Component Cooling Water	Potential impact due to first and second order interfaces. Cooling water failures considered as part of the process systems served.

TABLE 2.4.10. (Continued)

System ID	System Name	Potential Impact on Insufficient Core Cooling
W04.A	Condenser Circulating Water	Potential impact due to second order interfaces. Cooling water failures considered as part of the process systems served.
W04.D	Recirculated Cooling Water	Potential impact due to second order interfaces. Cooling water failures considered as part of the process systems served.
W07.B	Instrument Air	Potential impact due to first and second order interfaces. Instrument air failures considered as part of the fluid systems served (see Section 2.5.3).
X05.E	Reactor Building Cooling	The effect of containment air temperatures on RCS heat transfer is considered to be insignificant. The effects of high air temperatures on the operability is beyond the scope of this report.

2.4.4.1 Definition of Significant RCS Overcooling

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

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

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

An RCS overcooling transient, as defined above, is characterized by continuously decreasing RCS temperature, pressure or inventory following reactor trip. These defined overcooling characteristics are interrelated significantly as shown in Table 2.4.11.

In Table 2.4.11, the three defined characteristics of RCS overcooling are expanded in terms of possible functional causes. Following reactor trip (which is an assumed necessary condition for an overcooling transient), the heat input from the subcritical core to the reactor coolant (decay heat) is a fixed decreasing function of time. To the extent heat is removed from the reactor coolant at a rate in excess of the decay heat, the total energy content of the coolant and its temperature will decrease. As shown in Table 2.4.11, a net heat transfer from the RCS could result from increased heat transfer through the steam generator tubes to the feedwater (secondary coolant) or a direct release of the high temperature reactor coolant from the RCS.

TABLE 2.4.11. OVERCOOLING CHARACTERISTICS AND POTENTIAL INITIATING CAUSES

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

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

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

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

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

These three overcooling characteristics are discussed in Sections 2.4.4.1.1, 2.4.4.1.2 and 2.4.4.1.3 to relate the physical overcooling processes occurring in the RCS in response to RCS and interfacing equipment operating modes.

2.4.4.1.1 Increased Heat Transfer Through the Steam Generators

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

The core power following reactor trip is below 5% full power. This heat is removed, under normal conditions, in the two steam generators by regulating the feedwater flowrate to maintain a feedwater inventory equivalent to approximately 30" of water in the steam generators and regulating the saturation pressure of the steam generators' shell side at approximately 1025

psia using the turbine bypass valves. Under steady state conditions, the rate at which the feedwater is vaporized is proportional to the small and decreasing decay heat production rates. The reactor coolant temperatures are within a few degrees of the saturation temperature of the shell side of the steam generators.

The rate of heat transfer from the reactor coolant to the feedwater could be increased by either of two mechanisms: reducing the saturation temperature of the steam generator shell side or increasing the feedwater flowrate. A reduction in the saturation pressure could occur by opening the turbine bypass valves. This would result in a lower shell side saturation temperature, an increased temperature difference between the reactor coolant and the boiling feedwater and consequently an increased heat transfer rate. The reactor coolant temperature is expected to decrease under these conditions until a new equilibrium is established. It should be noted that as the saturation pressure is reduced the volumetric flowrate of steam will decrease. Furthermore, at the reduced saturation pressures and temperatures, the energy content per unit volume of steam released through the turbine bypass valves will be reduced due to increased specific volume (decreased density) of the steam. Due to these phenomena, the rate of reactor coolant temperature reduction will decrease as the temperature decreases. However, reactor coolant temperatures of less than 300°F are considered possible after several hours.

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

In addition to increased heat transfer through the steam generators, increased heat transfer through the letdown-makeup flowpath or increased convective heat

transfer to the reactor building air is possible. In either case, however, the effects of these mechanisms on reactor coolant temperature are expected to be negligible.

2.4.4.1.2 Increased Pressurizer Spray Flowrate

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

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

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

2.4.4.1.3 Release of Reactor Coolant

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

This study considers the effects of control systems failures. As such, arbitrarily postulated piping failures are not considered. Release of reactor coolant resulting from pressurizer relief or safety valves opening and remaining open, a net release of release of reactor coolant via the letdown

piping or steam generator tube cracks is considered to the extent such a failure may result from a control system misoperation. In general release of reactor coolant falls in the category of RCS leaks or small LOCA's.

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

If the operator detects an RCS leak rate exceeding 1 gpm, he must determine the location of the leak or shut down the plant. Leakage through one or more of the pressurizer relief valves, for instance, can be identified by high temperature readings of the discharge line thermocouples. In addition, if the source of leakage exceeding 1 gpm is the steam generator tubes, the plant must be shutdown. Steam generator tube leaks are indicated by the monitored radioactivity level of the main condenser "air" ejector discharge. All RCS leakage exceding 10 gpm requires plant shutdown.

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

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

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

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

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

The operator can control the depressurization by manually increasing the makeup flow rate and filling the pressurizer. If the operator fails to take this action, the RCS pressure will decrease to the safety injection setpoint (~1500 psi). At this pressure, the high pressure injection (HPI) mode of the MU&P will be automaticaly actuated and the pressurizer will be filled. Once the pressurizer is filled and the leak is in the water space, the RCS presure is automatically controlled by the PORV and/or safety valves at approximately 2450 psi.

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

If an increased rate of depressurization is required, the operator can manually open the spray valve or the PORV.

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

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

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

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

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

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

One particular small break LOCA or concern is the failed open PORV. Assuming the failed PORV remains unisolated for the initial phase of the accident, the vessel downcomer temperature will be low. If the operator then isolates the PORV, the continued injection of coolant and the heat generated in the core

will increase the RCS pressure to pressures of up to 2450 psi, which may be of significant PTS concern.

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

Detailed information describing the required equipment and operator actions following system leakage and LOCA's is provided in each plant's LOCA emergency procedure (e.g., Duke Power emergency procedure EP/0/A/1800/4, "Loss of Reactor Coolant" and OP/0/A/1106/35, "Inadequate Core Cooling"). The response characteristics of the RCS to LOCA's is described in vendor topical reports referenced in each plant's FSAR (Reference 2).

2.4.4.2 Evaluation of RCS Overcooling Response to Systems Failures

Based on the definition of RCS overcooling, the systems potentially affecting RCS response identified in Tables 2.4.7 and 2.4.8, were briefly evaluated to assess their potential impacts on RCS overcooling. The results of this evaluation are summarized in Table 2.4.12.

As indicated, most of the systems affecting RCS response have the potential for affecting RCS overcooling. These systems are analyzed in detail using a failure modes and effects analysis method to evaluate specific effects of system failures on RCS overcooling (see Section 3). The systems not selected for detailed analysis are discussed below.

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

The control rod drive mechanisms and the control rod drive control system influence to rate of core heat production during operation. However, once the

TABLE 2.4.12. POTENTIAL IMPACTS OF FIRST AND SECOND ORDER REACTOR COOLANT SYSTEM INTERFACE SYSTEMS ON RCS OVERCOOLING

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

TABLE 2.4.12. (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
N05.C	Coolant Treatment System	
N05.D	Post Accident Sampling	
N05.E	High Pressure Injection	
C03	Reactor Building Ventilation	The effect of containment air temperature changes on heat transfer from the RCS is considered to be insignificant. The effects of loss of ventilation on component operability is considered to be beyond the scope of the study.
P01	Main Steam and Turbine Bypass	Power conversion systems and subsystems analyzed in detail.
P02	Turbine-Generator System	
P03	Main Condenser	
P04	Condensate and Feedwater	
W01	Radioactive Waste	System was selected based on its interface with the Non-Nuclear Instrumentation. However, the interface consists of providing parameter signals for display only. Failures of the Radioactive waste system not considered to have any significant impact on RCS overcooling.
W03	Reactor Building Component Cooling Water	Potential impact due to first and second order interfaces. Cooling water failures considered as part of the process systems served.
WC4.A	Condenser Circulating Water	Potential impact due to second order interfaces. Cooling water failures considered as part of the process systems served.

TABLE 2.4.12. (Continued)

System ID	System Name	Potential Impact on RCS Overcooling
W04.D	Recirculated Cooling Water	Potential impact due to second order interfaces. Cooling water failures considered as part of the process systems served.
W07.B	Instrument Air	Potential impact due to first and second order interfaces. Instrument air failures considered as part of the fluid systems served (see Section 2.5.3).
X05.E	Reactor Building Cooling	The effect of containment air temperatures on RCS heat transfer is considered to be insignificant. The effects of high air temperatures on the operability is beyond the scope of this report.

reactor is tripped (control rods inserted) neither the drive mechanisms nor the drive control system can influence the resulting transient.

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

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

2.5 PLANT SYSTEMS WITH POTENTIAL FOR COMMON CAUSE FAILURES

2.5.1 Rationale

Because control systems by their nature depend upon external sources for actuating energy, failure of a single energy source may lead to misoperation of a group of control devices. Systems commonly dependent upon these sources must therefore be investigated in order to determine those multiple failures which can derive from a common loss of power. This section develops the common ties of control systems through electrical and pneumatic energy sources.

2.5.2 Electrical System

2.5.2.1 Power Distribution

The Oconee Nuclear Power Station ac distribution system internals to the units includes 6900V, 4160V, 600V, and 208/120V distribution buses. Most of the plant ac loads have normal and alternate power sources with automatic or manual transfer. The 600V MCCs have two self actuated breakers to protect against faults and overloads. There are lockout relays to prevent automatic transfer of an MCC if it trips because of overload or fault current.

There are no single failures of equipment that would cause multiple MCC failures, but failure of a 4160V power source and failure of a dc panelboard would result in a temporary loss of ac power to more than one MCC. Local, manual transfer to an alternate source would remain functional. Protection of the 600V MCCs is independent of dc control power.

Class 1E MCCs are connected through two normally open breakers, but administrative procedures are used to assure the three Class 1E divisions are not interconnected during normal operation. A common-cause failure potential exists because of the interconnection feature, but common-cause failure probabilities can be kept small by strong administrative procedures. With a few exceptions such as connection between Class 1E divisions, the Oconee electrical system has features similar to many other plants now operating.

The Instrumentation and Controls dc power supply system at Oconee Nuclear Power Station is unusual in that dc supplies are shared between units at the station and in that safety-related (Class 1E) circuits are mixed with non-safety circuits on the same buses and panelboards.

Although it is not clear whether these non-safety loads and their installations would conform to the current concept of "associated circuits" as defined in IEEE Std. 384, (Ref. 18), the overall effect of the configuration is to provide for a highly reliable and flexible dc-powered supply system provided that the components and installations of the non-safety related circuits are qualified for, and protected from environmental and other common cause stresses.

Although the sharing of batteries by three units is contrary to current regulatory concepts of good design practice, the operating record appears to be favorable and the isolating and transfer diode scheme of power source auctioneering should be studied for applicability to other multi-unit plants.

2.5.2.2 Electrical System

A detailed analysis of the effects of ICS/NNI electrical power supply failures was performed for the Oconee Unit 1 nuclear power plant.[1] This analysis consisted of determining the response of ICS/NNI output signals to single point failures in the power supply circuitry. From these degraded signal combinations, the automatic response of the plant's controlled components and possible responses of the plant operators to degraded control room parameter displays were evaluated.

The ICS/NNI is supplied with 120-V ac power through five major branch circuits from ICS Panelboard KI: auto power (branch H), hand power (branch HX), emergency power (branches HEX and HEY), emergency steam generator level control power (branch H-EL)* and reactor control system (RCS) narrow range pressure transmitter power (branch KI-10). Auto power and hand power are distributed to ICS/NNI components through branch circuits H1, H2, H4, H5, H8, H1X, H2X, and H3X (see Fig. 2.1). In addition, computer panelboard KU can provide power to selected NNI circuits by manual transfer or automatic transfer if panelboard KI is deenergized.

The results of the study are summarized in Tables 2.5.1 and 2.5.2 for the power supply branch circuit or combinations of branch circuits deenergized. Table 2.5.1 lists the principal automatic control circuit and plant responses to the power supply failures. The principal control room parameter display failures and possible operator responses resulting from power supply failures are listed in Table 2.5.2.

The conclusions resulting from the ICS/NNI power supply failure analysis are summarized below:

1. The automatic responses of the plant to power supply failures were not found to be severe. In part, this is due to the post-TMI modifications--in particular, the automatic trip of the main feedwater pumps on high steam generator level and subsequent automatic initiation and control of the emergency feedwater system. The principal spurious automatic responses were found to be:

   - Several power supply failures resulted in opening or holding open the main feedwater control valves, which may result in an automatic high steam generator trip of the main feedwater pumps and automatic initiation and control of emergency feedwater. Manual throttling of main feedwater could avoid the high level trip in many cases.

*The emergency feedwater control system is powered through the vital buses, not from H-EL.

[1]A. F. McBride and C. W. Mayo, "Failure Modes and Effects Analysis (FMEA) of the ICS/NNI Electric Power Distribution Circuitry at the Oconee 1 Nuclear Power Plant," NUREG/CR-3991, ORNL, to be published.

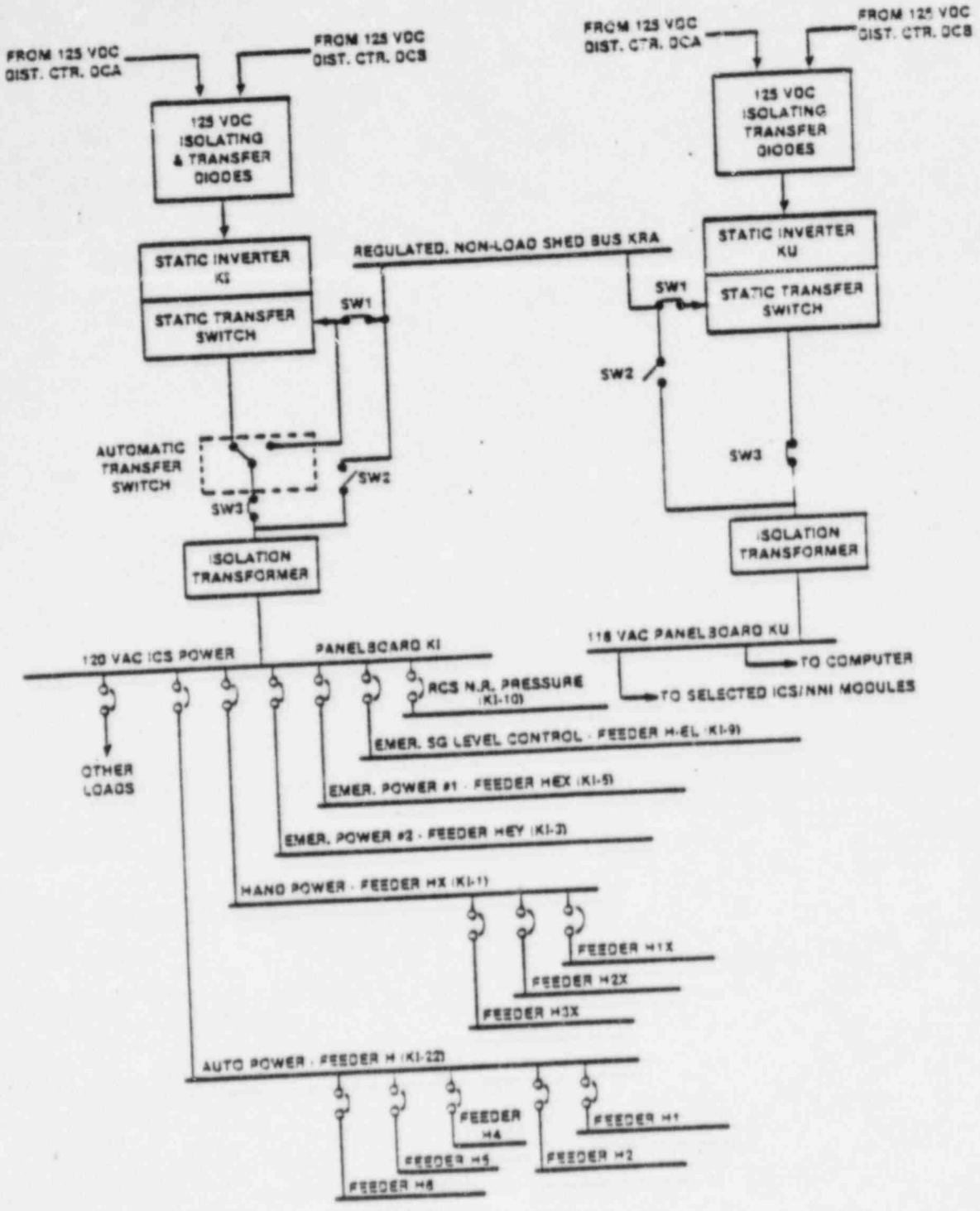


FIGURE 2.1 OCONEE 1 NUCLEAR STATION
ICS/NNI AC POWER SUPPLY

Table 2.5.1. Summary of spurious automatic system responses to ICS/NNI power supply failures

Branch circuit failure	NNI spurious failure	ICS spurious response	Transfer to manual	Automatic system response
H1	Yes	No	Reactor power Turbine throttle Main and startup feedwater valves Main feedwater pump Pressurized spray valves Pressurizer heater Makeup flow control	Continued short-term plant operation without automatic control. Reactor/turbine trip in response to perturbations, with possible high-SG-level feedwater pump trip.
H2	Yes	No	Seal injection flow	Interlock reactor coolant (RC) pumps from being started.
H4	No	No	None	None
H5	No	No	None	None
H8	No	No	None	None
H	Yes	No	Branches H1 through H8 denergized, see above.	Branches H1 through H8 deenergized. Response described above.
H1X	Yes	Yes	None	Possible closure of turbine throttle, increase or decrease of reactor power, and reduction of feedwater pump speed will result in reactor/turbine trip. High-SG-level trip of feedwater pumps possible.
H2X	Yes	No	None	No immediate plant transient. The power supply for the letdown, makeup, and RC pump seal injection control valves electro/pneumatic (E/P) transducers transfers automatically to panelboard KU. Letdown transferred automatically to letdown storage tank.
H3X	No	No	None	None
HX	Yes	Yes	None	Branches H1X, H2X, and H3X deenergized. Response described above.

Table 2.5.1 (continued)

Branch circuit failure	NNI spurious failure	ICS spurious response	Transfer to manual	Automatic system response
HEX	Yes	Yes	None	Pressurizer level and SG startup level and pressure transmitters are powered by branches HEX and HEY. If selected for control, a deenergized pressurizer level transmitter results in transferring coolant from the letdown storage tank to the pressurizer . A deenergized SG level transmitter results in increased main feedwater flow to the affected SG(s). A deenergized SG pressure transmitter results in loss of automatic control of turbine bypass valves.
HEY	Yes	Yes	None	See HEX above.
H-EL	No	Yes	None	No immediate plant transient. Startup feedwater control valves "freeze" in position.
KI	Yes	Yes	Branches H, HX, HEX, HEY, and H-EL deenergized. Letdown, makeup, and turbine bypass valve controls transferred to manual and energized via KU. Manual pressurizer spray and heater controls also available at ASP.	Branches H, HX, HEX, HEY, and H-EL deenergized. Automatic reacator, turbine, and feedwater pump trip. Automatic control of emergency feedwater and RC pump seal injection flow.
KU	Yes	No	None	If KU powered pressurizer level transmitter selected, coolant transferred from letdown storage tank to pressurizer.
KI-10	Yes	No	None	RCS narrow range pressure transmitter deenergized, resulting in a low indicated pressure. Pressurizer heaters would be energized and the pilot-operated relief valve (PORV) and spray valves closed, probably resulting in a high-pressure reactor trip.

Table 2.5.2. Summary of control room parameters displays' response to ICS/NNI power supply failures

Branch circuit failure	NNI response	ICS response	Spurious alarms	Deenergized indications	Expected plant control operator response*
H1	Yes	Yes	Hi, lo pressurizer level Hi, lo RC T_{avg} Low SG A, B startup levels	Cold leg dT RCS loop A, T_{avg} SG A wide range level Loops A, B startup feedwater flow rate Digital T_{avg} indication RCS T_{avg} recorder Loop A, B feedwater flow recorder	Trip plant or manually attempt controlled runback.
H2	Yes	No	Lo RC pump seal dP Lo, hi seal injection and outlet flow rates	Seal dP Seal injection and outlet flow Letdown flow	Manual trip of reactor and RC pump possible.
H4	No	No	Hi, lo (CFR) pressure	One of two core flood tank pressure meters	Continued plant operation.
H5	No	No	Hi quench tank T, P, level Hi, lo reactor building (RB) sump level	Quench tank T, P, level RB sump level Liquid, gaseous waste flow, flow recorder	Continued plant operation.
H8	No	No	Hi reactor building Pressure	RB pressure meter, recorder	Continued plant operation.
H	No	No	Branches H1 through H8 deenergized, see above	Branches H1 through H8 deenergized, see above	Loss of branch H (auto power) alarmed. Identification of cause of spurious indications increases likelihood of effective manual control by operator, including reactor trip and main feedwater control.
H1X	Yes	Yes	Hi, lo turbine hdr. pressure Hi, lo pressurizer level Hi SG level Hi RCS temperature, dT	Turbine hdr. pressure SG pressure SG level Main feedwater flow RCS temperature	Manual trip of reactor/turbine, manual trip of main feedwater pumps, and possible initiation of HPI.

Table 2.5.2 (continued)

Branch circuit failure	NNI response	ICS response	Spurious alarms	Deenergized indications	Expected plant control operator response*
H2X	Yes	No	Hi, lo letdown storage tank (LST) level	LST level LT-2	Opening flow path from borated water storage tank (BWST) to HPI pumps possible.
H3X	No	No	None	One of two CFT A, B pressure meters	Continued pump operation.
HX	Yes	Yes	Branches H1X, H2X, and H3X deenergized, see above	Branches H1X, H2X, and H3X deenergized, see above	Loss of branch HX (hand power) alarmed. Operator expected to trip reactor, turbine, and feedwater pumps and regain manual control of selected components by manually transferring to KU power supply.
HEX	Yes	Yes	Lo pressurizer level if selected Lo SG level if selected Lo SG pressure if selected	Lo pressurizer level if selected Lo SG level if selected Lo SG pressure if selected	Loss of branch HEX (emergency power) alarmed. Operator expected to select energized transmitters.
HEY	Yes	Yes	Lo pressurizer level if selected Lo SG level if selected Lo SG pressure if selected	Lo pressurizer level if selected Lo SG level if selected Lo SG pressure if selected	Loss of branch HEY (emergency power) alarmed. Operator expected to select energized transmitters.
H-EL	No	Yes	None	None	Loss of branch H-EL (emergency SG level control power) alarmed in control room. No operator actions required during power operations. Use of emergency feedwater may be required following shutdown.
KI	Yes	Yes	Branches H, HX, HEX, HEY, H-EL deenergized, see above	Same as H, HX, HEX, HEY, H-EL deenergized, see above	Loss of panelboard KI (ICS panelboard) alarmed in control room. Operator expected to follow emergency procedure EP/O/A/1800/31, loss of KI bus.

Table 2.5.2 (continued)

Branch circuit failure	NNI response	ICS response	Spurious alarms	Deenergized indications	Expected plant control operator response[a]
KU	Yes	No	Lo pressurizer level if selected	Pressurizer level if selected, all computer outputs	Follow procedure for loss of KU (computer panelboard).
KI-10	Yes	No	Lo RCS pressure	RCS pressure	Identify spurious low RCS narrow range signal from comparison with RPS signals. Manually control pressurizer heaters, spray valve, and PORV.

[a]Other responses include the identification and repair of power supply failure.

- Most power supply failures resulted in the makeup control valve freezing in position (with manual control available) without significantly affecting RCS inventory Failure of the power supply for the selected pressurizer level transmitter, however, opens the makeup valve. The operator, in this case, must manually control the makeup flow rate to prevent possible damage to the PORV and the operating high pressure injection (HPI) pump.

- Several power supply failures resulted in the pressurizer heaters remaining on or the pressurizer spray block valve remaining open if these components were energized or open at the time of power failure. The transient resulting is slow in either case; however, manual control is required.

2. Specific alarms were identified for failure of panelboard KI and branches H, HX, HEX, HEY, and H-EL. However, alarms for failure of lower level circuits (H1, H2, H4, H5, H8, H1X, H2X, and H3X) were not identified from available information. Alarms for these circuits, H1 and H1X in particular, are considered important to the rapid identification and manual mitigation of the resulting transients.

3. Possible operator responses to spurious control room displays resulting from power supply failures were evaluated qualitatively. In general, possible operator actions (or failures of the operator to perform an action) did not result in significant transients. Two potentially significant operator responses, however, were identified:

   - Following branch H, H1, or selected HEX or HEY failure at high reactor power and high steam generator level, the operator may close the main feedwater control valves. Due to the moderately long length of time that would elapse prior to requiring additional feedwater and the failure of the low-level alarm (spuriously energized by the power failure), the operator may fail to reopen the feedwater control valve prior to steam generator dryout. In this case automatic initiation of emergency feedwater is not expected since the main feedwater pumps are operating.

   - Failure of the selected pressurizer level transmitter power supply will result in spurious low-level alarm and indication of pressurizer level and opening the makeup control valve. Although the operator should be alerted to the power supply failure by the ICS/NNI emergency power (HEX, HEY) failure alarms and should transfer to an operable transmitter, other events may distract him. The same power supply failure may result in reactor/turbine trip, spurious low steam generator alarm and indication, increasing steam generator level, and main feedwater pump trip. If the pressurizer is allowed to

fill and liquid is discharged through the PORV, valve damage could occur. Also, if the LST is allowed to drain (LST level is separately alarmed) and an alternate supply of water is not provided, damage of the operating HPI pump would occur.

4. During the power supply failure analysis, several modifications were identified which would prevent or moderate the effects of power supply failures. These modifications are suggested for review:

   - o Transmitter selection relay power: The contact switches used to select one of two redundant transmitters frequently are powered by one of the transmitters' power supply in the ICS/NNI design. With proper selection, a power supply failure will result in an automatic transfer to the alternate energized transmitter. Modification of the HEX, HEY powered pressurizer and steam generator startup level transmitters' selection switches to this configuration is recommended (i.e., change the power supply of the transmitter selection relays to HEX or HEY and configure to allow automatic transfer on power supply failure. Also note, a more elegant, double-switch arrangement is used for the selection of the SGs' operate range level transmitters. This arrangement will allow automatic transfer on power supply failure regardless of the transmitter initially selected).
   - o Automatic trip of feedwater pumps: Failure of branch H, H1, HX, or H1X is expected to cause a transient resulting in main feedwater pump trip (on high steam generator level). It is recommended that the pumps be tripped directly on loss of any of these power supplies (as they are on loss of panelboard KI) to minimize the effect of the transient.
   - o Suppression of spurious alarms: The majority of alarm contacts are configured to alarm on power supply failure. The resulting spurious alarms are not expected to aid transient diagnosis and may mask operable alarms. It is recommended that the signal monitor alarm contacts be changed to an energize-to-alarm configuration.
   - o Power supply failure alarms: Alarms for failure of branch circuits H1, H2, H4, H5, H8, H1X, H2X, and H3X were not identified from available information. If these circuit failures are not alarmed, it is recommended that alarms for branch circuits H1 and H1X be considered.
   - o Power supply failure procedures: The "Loss of KI Bus" emergency procedure is expected to be very useful in the manual recovery from KI failures, particularly in the identification of operable controls and indications. It is recommended that the power supply failure procedures

be reviewed to determine whether lower-level power supply branch circuit failures are addressed and that specific instructions be added if they are not.

2.5.3 Pneumatic System

2.5.3.1 System Purpose and Design Basis

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

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

2.5.3.2 System Description

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

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

Instrument air supply

Figure 2.5.1 shows in a schematic fashion the major components of the instrument air supply. Three Worthington electric motor-driven compressors provide the normal source of instrument air through three air intakes and silencers. Each compressor is powered from a different 600-V ac motor-control center. Compressors A and B receive electric power from a unit 1 motor-control center, and compressor C receives power from a unit 2 motor control center. Each compressor is rated at 489 scfm at 100 psig.

Each compressor can be placed in either the BASE, STANDBY No. 1, or STANDBY No.2 operating mode. In the BASE mode, a compressor stops compressing at 100 psig while increasing and starts compressing at 95 psig while decreasing. In STANDBY No.1, a compressor starts compressing at 90 psig while decreasing and stops at approximately 100 psig while increasing. In STANDBY No. 2, a compressor starts compressing at approximately 85 psig while decreasing and stops at 100 psig while increasing. Depending upon the amount of air leakage and the system load, it may be necessary to run two or even all three compressors in BASE to maintain 100 psig. All three compressors are cross connected at their discharges and connected by 8-in. lines to aftercoolers. Each compressor can be isolated by manual valves.

The instrument air system has two air compressor aftercoolers that cool the compressed air leaving the station air compressors. The aftercoolers receive cooling water from the low-pressure service water (LPSW) system.

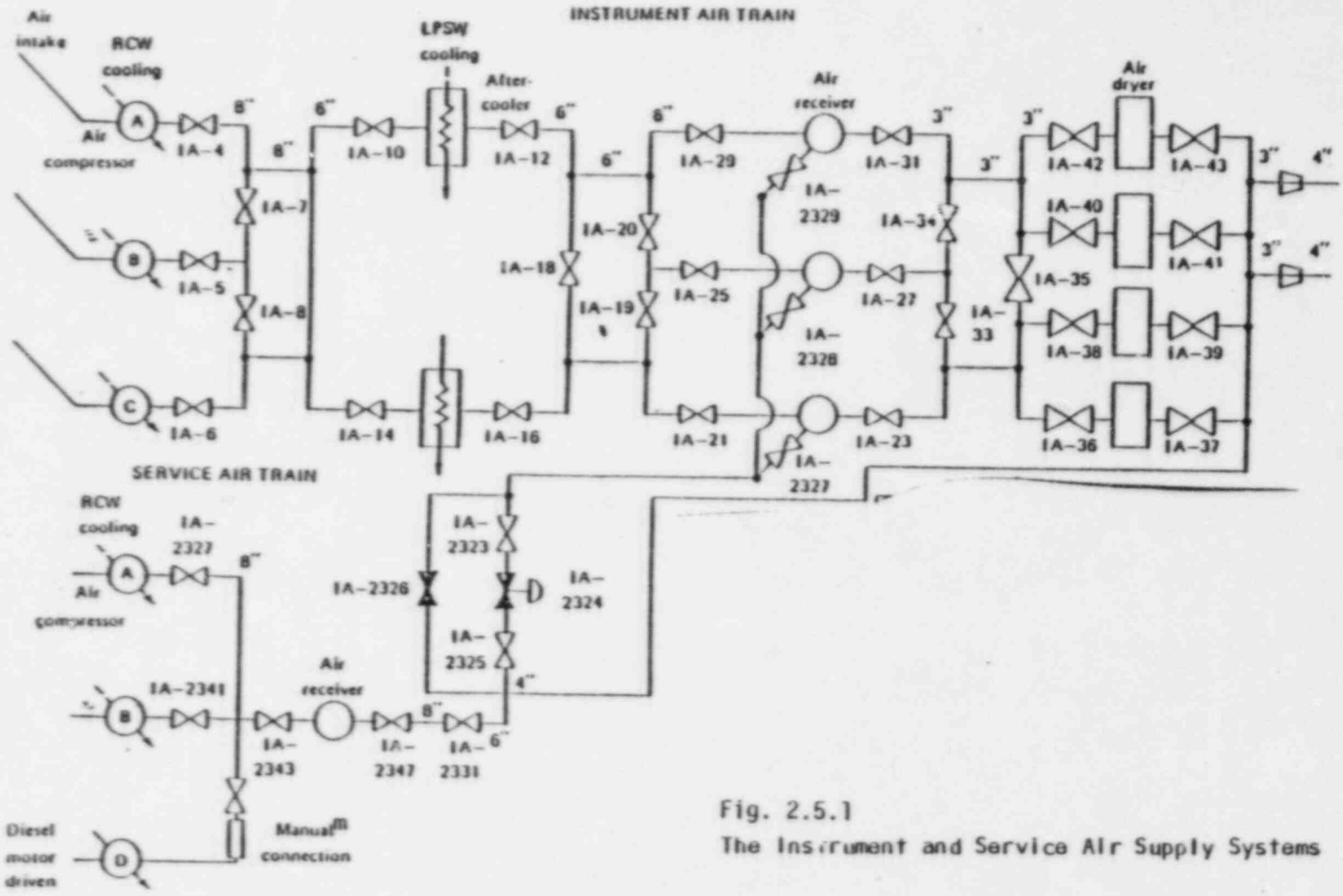


Fig. 2.5.1
The Instrument and Service Air Supply Systems

From the aftercoolers, air passes to three 302-ft³ air receivers that serve as air storage tanks to dampen system pressure variations. Each receiver is equipped with a safety-relief valve that can arrest excessive pressure increases in the system. The three receivers can be cross connected or isolated at both their inlets and outlets by manual valves. Three-inch lines pass from the receivers to the turbine maintenance area.

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

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

Service air supply

The service air system provides compressed air for miscellaneous uses at the station (i.e., tools, cleaning). The service air supply subsystem also serves as a backup for instrument air supply. An air operated-valve (1A-2324 in Fig.2.5.1) automatically connects the service air system to the air receivers in the instrument air supply subsystem anytime that instrument air pressure drops below 87 psig. Service air is supplied by two Sullair electric motor-operated compressors, each with a capacity of approximately 730 scfm at 100 psig. Power for each service air compressor and its controller is supplied by a different unit 3, 600-V motor-control center. Both Sullair compressors are located in the Unit 3 turbine building.

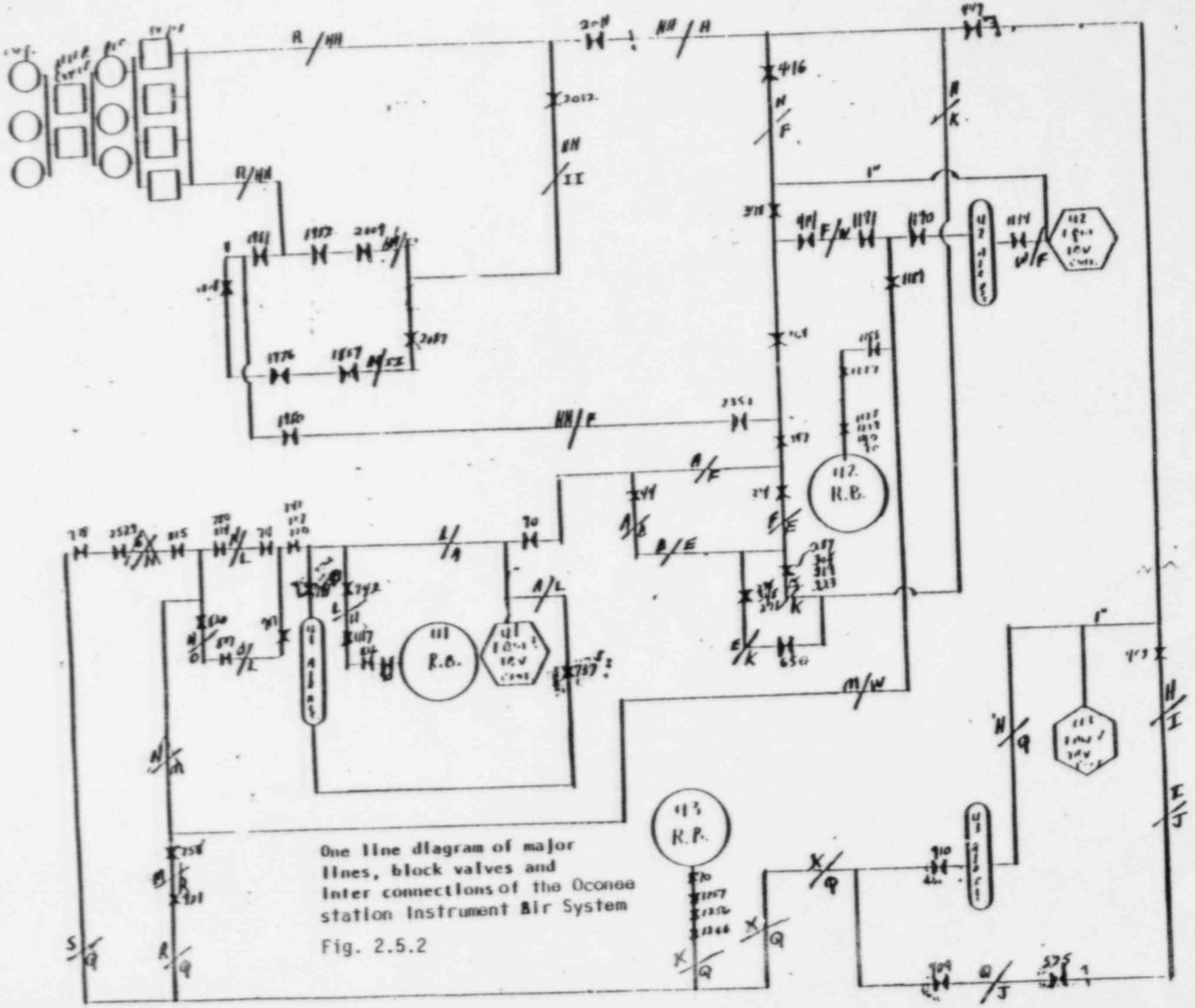
A third Sullair compressor is available to connect to the service air system. This portable diesel-driven compressor is located outside in the vicinity of the service air electric compressors. It is battery started and connects to the service air outlet lines by a flexible hose and manual valve. It has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

Instrument air distribution network

After exiting the air dryers, instrument air passes through one of two 4-in. lines that supply air to the three units. Figure 2.5.2 schematically shows the major interconnections and block valves in the distribution network. This drawing is greatly simplified, and all deadend feeder lines have been eliminated since the purpose of the drawing is solely to illustrate the interties of instrument air between units. This drawing is from the Oconee "Plant Compressed Air Procedure," ref. 3.

Alarms and gauges

Each unit has an alarm for low auxiliary building header instrument air pressure. The alarms are set at 90 psig decreasing, and they print out



One line diagram of major lines, block valves and inter connections of the Oconee station Instrument Air System

Fig. 2.5.2

on the alarm typer in addition to the control room annunciator panel. In addition, Unit 1 has an alarm for low instrument air pressure in the turbine building. This alarm prints on the alarm typer and is displayed as "1A System Trouble" on the Unit 1 annunciator panel. This pressure switch is located on column L-32 in the turbine building, the alarm is tapped off the outlet of the air receivers at the same location as the compressor pressure switches and is set at 80 psig decreasing.

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

2.5.3.4 Loads that Utilize Instrument Air

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

1. primary coolant letdown system,
2. RC pump seal injection flow,
3. RC pump seal No. 1 leakoff and bypass RB isolation valve,
4. pressurizer makeup,
5. letdown storage tank,
6. coolant treatment,
7. coolant storage,
8. gaseous waste disposal,
9. demineralizer water,
10. liquid waste disposal,
11. reactor building purge system,
12. component cooling,
13. main feedwater,
14. emergency feedwater,
15. main steam,
16. condensate,
17. recirculating cooling water,
18. low-pressure service water,
19. high-pressure service water,
20. auxiliary steam,
21. chemical addition and sampling,
22. air-conditioning system,
23. high-pressure injection,
24. high-pressure extraction (main turbine),
25. steam dump,
26. heater drain,
27. vacuum (main turbine condenser), and
28. low-pressure extraction (main turbine).

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

2.5.3.5 Impact of Air System Failures

Systems and Instrumentation Required for Transient Mitigation

In an attempt to evaluate the effects of loss of instrument air on the NSS, the abnormal transient operating guidelines (ATOG) for the Oconee station were studied. ATOG were prepared to assist in procedure preparation and in the training of Oconee operators to cope with abnormal transients (transients that might jeopardize plant safety). This review of ATOG identified components and systems that are believed to be of prime importance in dealing with abnormal transients. These system are

1. Main feedwater system
2. emergency feedwater system
3. steam line components
   - main steam safety valves
   - atmospheric exhaust valves
   - turbine bypass valves
4. Emergency core cooling system
   - makeup
   - HPI
   - LPI
5. Containment Cooling System
   - building spray
   - building coolers
6. Containment isolation
7. Components for RC pressure control
   - pressurizer heaters
   - pressurizer spray

ATOG were also studied to determine the instrumentation required to permit proper operation of the above systems. This study resulted in the identification of a minimum set of instrumentation. This minimum set includes the following:

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

Impact of air system failures on required system

The systems, components, and instrumentation described above were surveyed to determine the extent of their dependence on instrument air. The following is a discussion of the results of this survey.

Main feedwater (PO121A-1,121B-1)*.

The MFW, condensates, and heater drain systems are heavily dependent upon proper operation of a number of pneumatic valves, pneumatic instruments, and pneumatic controllers. Substantial pressure upsets or loss of adequate instrument air pressure to all or a subset of these values and controllers during power operation can result in significant condensate and main feedwater upsets. Depending upon the instrument air failure assumed different transients can result. The following is a brief discussion of two kinds of failures

a. Total loss of air compressors or failure of the instrument air supply line so that instrument air pressure decreases throughout the entire instrument air distribution network. When low instrument air pressure occurs, the interactions between the turbine extraction system, feedwater heater drain system, condensate system, and main feedwater system are extremely difficult to predict. A low 1A pressure transient occurred at the Oconee station on October 13, 1983. A brief description of the resulting nuclear steam supply transient was included in the Duke Power Company information submittal of May 7, 1984 (ref. 6). Units 1 and 3 were operating at power when the 1A pressure transient began. Instrument air pressure dropped to below 54 psig. Both Units 1 and 3 condensate and feedwater systems experienced perturbations. Unit 3 reactor tripped after the condensate booster pumps and MFW pumps tripped. Unit 1 NSS avoided reactor trip although main FW upsets occurred.

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

From the possibilities described, we can make several observations about the relationship between the instrument air system and the MFW system

- The MFW system cannot be depended upon for a reliable, controlled source of SG feedwater should and instrument air malfunction occur. This is because of the complexity of the MFW system and the large number of valves in the MFW system that depend upon instrument air. Also, the performance of the MFW system is very closely coupled with the performance of the condensate and heater drain systems, both of which depend heavily upon instrument air.
- Performance of the MFW system following instrument air malfunctions is difficult to predict since it is quite dependent

upon the particular malfunction assumed, the NSS operating conditions, flow rates in the secondary plant, operator response, and a hose of other variables. This was clearly pointed out by the instrument air transient at the Oconee station that occurred on October 13, 1983.

Emergency feedwater system (P0121A-1, 122A-1)

The EFW system depends upon 1A primarily through the two pneumatic valves used to modulate EFW flow rates to the two steam generators. These two valves, EFW-315 and EFW-316, have an automatic backup supply of nitrogen for control purposes should a loss of 1A pressure occur (see enclosure one to EP/O/A/1800/29, ref.2). If modulation of the EFW valves cannot be accomplished following loss of 1A pressure in spite of the nitrogen supply backup, steam generator level control can still be accomplished by varying EFW pump speed or by locally throttling EFW 315 and 316. Steam flow to the EFW pump turbine is controlled by pneumatic valves MS-93 and MS-87. These valves fail open on loss of instrument air, admitting steam to the EFW pump turbine stop and governor valves.

Normal EFW operation depends upon a continuous supply of air for the EFW control valves. To ensure that air is always available, Duke Power Company has provided a backup source of control air using bottled nitrogen. If both the 1A and backup supply fails for any reason, control of SG level can still be accomplished by varying EFW pump turbine speed or by locally throttling control valves FDW-315 and 316.

Steam line components (P0122A-1)

After turbine trip, steam generator pressure is controlled by the combined operation of main steam safety valves, atmospheric exhaust valves, and turbine bypass valves.

Main steam safety valves are mechanically operated and are independent of the instrument air system. The atmospheric exhaust valves have manual actuators and must be locally opened/closed by an operator if they are needed for pressure control. There are two atmospheric exhaust valves and accompanying block valves: one set of exhaust and block valves per steam generator.

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

Low 1A pressure has no effect upon either main steam safety valves or atmospheric exhaust valves; however, turbine bypass valves fail closed on low 1A pressure (approximately 70 psig). If 1A pressure is low, and the turbine bypass valves fail closed, steam pressure cannot be controlled from the control room; it must be controlled by an operator

who is physically located at the atmospheric exhaust valves. Of course, the main steam safety valves will open in a staged fashion when steam pressure exceeds approximately 1050 psig.

Emergency core cooling (PO101A-1, 101B-1)

Makeup and letdown system. Loss of 1A pressure isolates the normal RCS letdown and makeup paths because a number of valves in these paths fail closed (HP-5, 6, 7, 8, 9, 13 in the letdown path and HP 120 in the makeup (MU) path are most important). Also, RC pump seal injection flow increases to 60 gal/min from 32 gal/min due to the fail open action of HP-31, the seal injection control valve.

Because of the above misoperation of valves, the operator must manually control RCS inventory by throttling letdown, makeup, and seal injection flows if 1A pressure drops below approximately 70 psig. From this brief discussion, note that normal RCS inventory control depends upon 1A availability, and although backup manual actions are possible, they are demanding on the operator.

High-pressure injection (PO101A-1, 101B-1). The high-pressure injection system (HPI) does not appear to have a direct dependence upon instrument air; however, HPI pumps do require cooling water for the pump lubricating oil coolers, and service water is also required for the pump's water-lubricated mechanical seals. Also, the makeup pump speed increasers require cooling water for the heat exchangers that cool the oil used to lubricate the speed increasers' bearings. HPI pump motors are air cooled.

Thus, the HPI pumps require a continuous source of HPSW and LPSW for proper operation. These system were surveyed to determine their dependence of the instrument air system, and results indicate that they should be able to operate satisfactorily following loss of instrument air.

Low-pressure injection (PO101B-1)

The low-pressure injection system also does not appear to have a direct dependence upon instrument air; however, as was true for the HPI pumps, service water is required for oil cooling and seal injection flow. LPI pump motors are identical to HPI motors and are air cooled.

2.5.3.6 Containment Cooling Systems

Reactor building spray (drawing No. PO103A-1, PO102A-1)

The reactor building spray system is designed to provide reactor building atmosphere cooling by directing borated water spray inside the reactor building. The system consists of two pumps, two spray headers, isolation valves, and the necessary piping, instrumentation and controls. Upon initial actuation of the building spray system, due to either high building pressure or operator initiation, the building spray pumps start and take suction from the BWST through the intertie with the LPI system.

If the BWST level drops to a low limit, spray pump suction can be transferred to the reactor building sump.

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

Building coolers (PO 1240)

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

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

2.5.3.7 Containment Isolation (Chapter 5 of Oconee FSAR)

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

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

2.5.3.8 Components for RC Pressure Control (PO 100A-1)

Pressurizer heaters

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

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

Pressurizer spray

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

Pilot operate relief valve (PORV)

The PORV can be used to relieve excess RC pressure during certain abnormal transients that result in insufficient primary-to-secondary heat transfer. The PORV is electrically actuated and is independent of instrument air.

RC pumps (Chapter 4, Oconee FSAR)

The RC pumps are mounted in the cold leg RCS piping and circulate water for removing heat from the reactor core. Proper operation of the RC pumps requires 13,800 V ac power, LPSW for motor and pump cooling and for oil cooling, HPI for seal injection, and various instrumentation and control circuits as necessary to monitor pump performance; however, the RC pumps do not appear to depend directly on the instrument air system.

2.5.3.8 Conclusions

Based upon a survey of the instrument air system as described above, the following conclusions were reached

- The Oconee station has one large, integrated instrument air system for all three units. Because of this interconnection it is quite possible that simultaneous, quite involved transients could be induced in more than one Oconee unit by instrument air malfunctions.
- Because of heavy dependence of the main feedwater, condensate, and heater drain systems on pneumatic valves and instrumentation, instrument air malfunctions are expected to cause substantial MFW upsets perhaps culminating in loss of MFW. Also, malfunction in the 1A system can conceivably result in MFW overfeed. Further, instrument air malfunctions in the MFW system can render the system inoperable without substantial operator manual actions.

- Normal operation of the EFW system is dependent upon a continuous supply of instrument air. A backup supply has been provided to allow continuous air in the event of loss of instrument air; however, the reliability of this backup scheme is questionable.
- Normal operation of the turbine bypass valves to control SG pressure after reactor trip is quite dependent upon 1A availability. Without adequate 1A pressure, steam generator pressure must be controlled by an operator locally throttling the atmospheric exhaust valves.
- The drawings associated with the instrument air system are hard to follow.
- Study of the information and drawings on the 1A system provided by Duke Power Company did not reveal and design features in the system that act to isolate nonessential 1A lines on low system pressure. This implies that a fault anywhere in the 1A system could affect pressure in the entire system.

REFERENCES

1. Oconee Nuclear Station Abnormal Transient Operating Guidelines.
2. Oconee Nuclear Station, "Loss of Instrument Air Procedure," EP/O/A/1800/29 - change 4.
3. Oconee Nuclear Station, "Plant Compressed Air Procedure," OP/O/A/1106/27 - change 6.
4. Oconee Nuclear Station, FSAR
5. Oconee Nuclear Station Drawings, "Diagramic Layout of Instrument Air Stations" PO-149-A, PO-149-B, PO-149-C, PO-149-D, PO-149-L, PO-149-U, PO-149-Z, PO-149-AA, PO-149-BB, PO-149-DD, PO-149-GG, PO-149-JJ.
6. Duke Power Company information submittal to A. P. Malinauskap May 7, 1984. Brief description of an instrument air system transient at the Oconee station of Oct. 13, 1983 and "Compressed Air System Description."
7. Oconee Nuclear Station Process and Instrumentation Drawings

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

3. BROAD FAILURE MODE AND EFFECTS ANALYSIS

3.1 PROCEDURE

Performance of complete third-level (component failure mode and effects analyses (FMEAs) on all nuclear plant systems is a Herculean task beyond any current plant probabilistic risk assessment (PRA) and certainly beyond the scope of this study. Even with the systems limited to those with a major role in selected events, third-level FMEAs present a monumental task when multiple failures and possible operator actions are considered. The approach taken here is a top-level (system) FMEA relying on superposition principle to limit the number of cases to be studied. This approach allows a large number of systems interactions to be analyzed and identifies those systems whose importance dictates a more detailed FMEA. Where more detailed FMEAs were warranted, they were performed. However, only single failures were considered at this time in the second- and third-level FMEAs.

3.2 BROAD FMEA FOR OVERFILLING AND OVERCOOLING

3.2.1 Systems-level Failure Modes and Effects Analysis

3.2.1.1 Major Systems Interfaces

There are over 100 major systems in a typical nuclear power station (Appendix A). Therefore, a selection criterion has to be used to limit the number of systems for initial study. The interfaces of the major systems pertinent to overcooling transients are shown in Fig. 3.1. Some systems not originally selected for this study (Appendix B) are included in this figure to provide a clearer interface definition.

3.2.1.2 Single Failures

The following table presents a systems-level, qualitative, loss-of-function, single-failure analysis. Functional definitions of the examined systems are found in Appendix A of this chapter.

3.2.1.3 Multiple Failures

Table 3.2.3.1 presents a systems-level, qualitative, loss-of-function, double-failure analysis. Those combined failures, which produce effects essentially equal to the sum of their single failures (superposition) or are series failures dominated by the last one in the series, are not presented. Such information is available from Sect. 3.2.2. Only those failures which can produce significantly different states from the superposition of the single failures are considered.

3.2.1.4 Cascades

The ultimate safety of a nuclear power station is in the hands of the operator. As has been seen, most transients result in reactor protection system actuation after which the operator must keep the core from overheating and the system from overcooling. He has many paths of

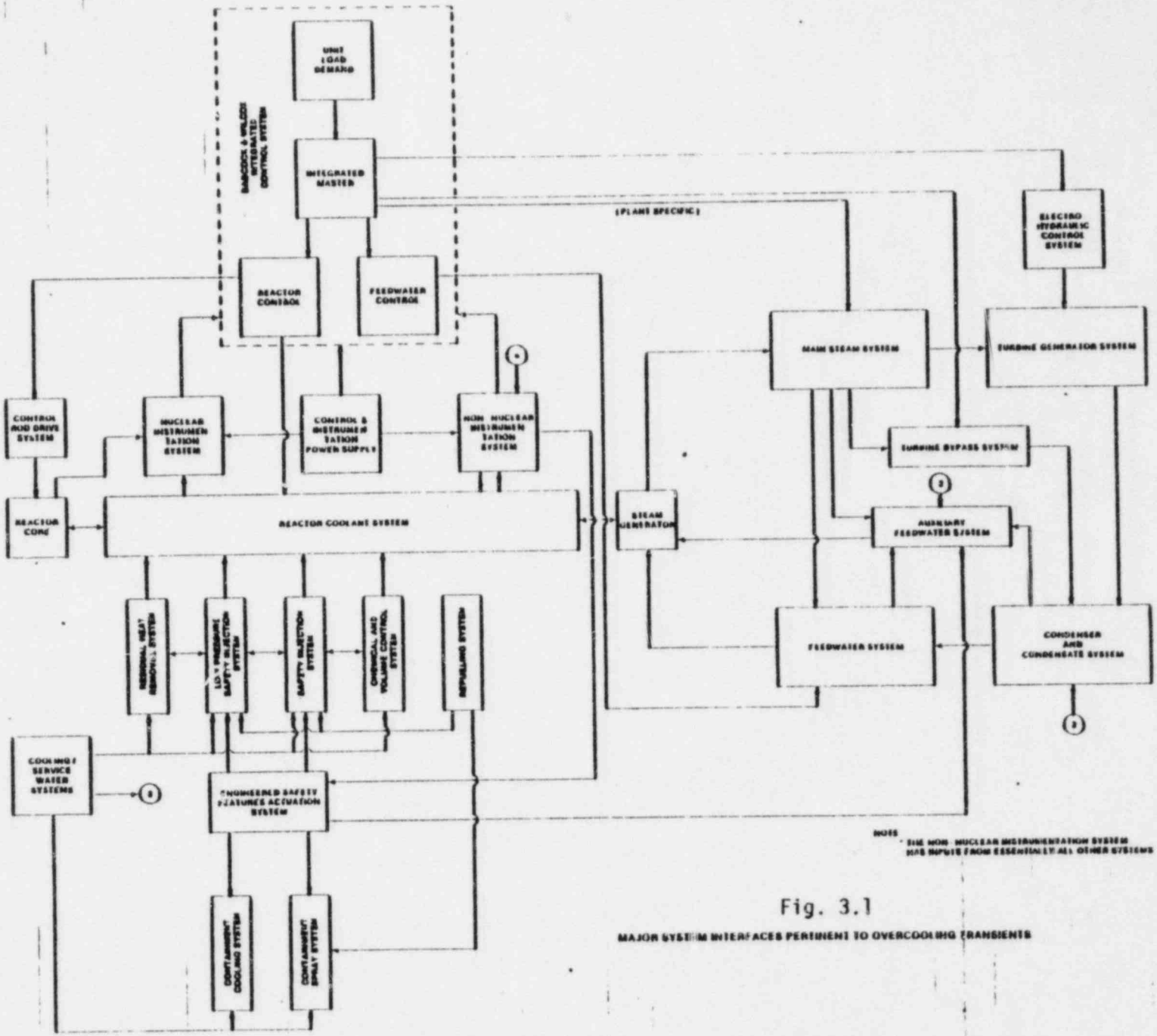


Fig. 3.1

MAJOR SYSTEM INTERFACES PERTINENT TO OVERCOOLING TRANSIENTS

Table 3.2.1.1. FMEA: Systems level single failures

System	Failure mode	Effect and remarks
ICS unit load demand	Fail high	Integrated master calls for more steam generation, more through turbine, without concomitant increase in turbine load. Probable reactor trip at power levels other than 100%
	Fail low	Integrated master calls for less steam generation, less through turbine, without concomitant decrease in turbine load. Reactor runback or trip
	Stuck	Turbine load could change without a corresponding change in steam. Possible reactor trip on load change
	Speed limiter failure	Load demand could change faster than the derivative limit, causing upsets to the plant, probably leading to reactor trip
ICS integrated master	Fail high to electro-hydraulic control system/fail low to turbine bypass system	Integrated master calls for more steam generation, more through turbine, without concomitant increase in turbine load. Probable reactor trip at power levels other than 100%
	Fail low to electro-hydraulic control system/fail high to turbine bypass system	Integrated master calls for less steam generation, less through turbine, without concomitant decrease in turbine load. Reactor runback or trip
	Stuck signal to electro-hydraulic control system	Turbine load could change without corresponding change in steam. Possible reactor trip on load change

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
	Fail high to reactor control system	Reactor run to full power, probable high-pressure trip
	Fail low to reactor control system	Reactor runback, probable low-pressure trip. Possible overcooling
	Fail high to feedwater control	Increase in feedwater flow. Might lead to overcooling after reactor trip
	Fail low to feedwater control	Decrease in feedwater flow. Will cause reactor trip, probably on high-pressure. Need emergency feedwater system to prevent drying steam generator
ICS feedwater control	Fail high	Increase in feedwater flow. Might load to overcooling after reactor trilp
	Fail low	Decrease in feedwater flow. Will cause reactor trip, probably on high-pressure. Need emergency feedwater system to prevent drying steam generator
ICS reactor control	Reactor coolant pump interlock	Would not allow startup of reactor coolant pumps after they trip. Certain overcooling events are mitigated by pump restart at 50°F subcooling margin
	Reactor coolant pump interlock off	Would allow start-up of reactor coolant pumps at any power. Reactivity transient induced. Probably not significant

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
	Control rod system high	Reactor run to full power, leads to high-pressure trip
	Control rod system low	Reactor runback, probable low-pressure trip. Possible overcooling
	Control rod system stuck	Loss of power control. Probable reactor trip on load change. Coolant system could be operated to take away proper amount of energy and boron used for power control and shutdown
Reactor coolant system	Pump(s) won't trip--high flowrate	Control rods and feedwater flow rate could be adjusted to compensate. Might result in overcooling and/or pump damage
	Pump(s) won't start--low flowrate	Control rods and feedwater flow rate could be adjusted to compensate. Might result in undercooling or overcooling. See reactor control
	Break	Depending on size, HPI pumps might compensate. Leads to reactor trip. Could lead to overcooling or undercooling. Large and small break LOCA have been extensively analyzed
Nuclear instrumentation system	Variable	Could cause control system to fail in any of ways under reactor control. Probable reactor trip
Nonnuclear instrumentation system		Not part of this study. Key candidate for another study. Not effectively addressable at a systems level. Likely to cascade

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
Control and instrumentation power system		Part of SANDIA study. Has been extensively analyzed by industry post-TMI and Rancho Seco
Main steam system	Boundary violation; open safety/ relief valve, break, etc.	Broad effects depending on size. Reactor trip on low pressure; blowdown of steam generator(s); overcooling; loss of feedwater heaters main feed pumps, turbine driven emergency feed pump; physical secondary loop damage. Production of uninhabitable environment in containment or turbine building
Turbine generator system	Steam flow blocked	Leads to reactor runback or trip. Steam flow can go through the turbine bypass system and atmospheric safety valves
	Boundary violation	Some loss of steam pressure. Breaks can be isolated
Electro-hydraulic control system	Calls for top turbine speed	Some loss of steam pressure. Can be isolated
	Trips turbines	Leads to reactor runback or trip. Steam flow can go through the turbine bypass system and atmospheric safety valves
Turbine bypass system	Fail open	Lets full flow bypass turbines. Loss of pressure in steam generator could lead to overcooling. See main steam system
	Fail closed	No effect at power greater than 20%. May lead to trip on high RCS pressure and opening of atmospheric safety valves upon load rejection/ turbine trip

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
Condenser and condensate system	Condensate too cold	Might lead to overcooling. Heaters available. Not significant
	Loss of condensate flow	Lose main feedwater flow. Have emergency feedwater system. Leads to reactor trilp
	Boundary violation	In addition to loss of flow, flooding of turbine building. Can be isolated
Feedwater system	Fail flow high	Might lead to overcooling, steam generator flood out
	Fail flow low	Have emergency feedwater system. Leads to reactor trip
	Boundary violation	In addition to low flow, flooding of containment or turbine building. Can be isolated
Emergency feedwater system	No flow	No effect in single failure mode. Loss of redundancy
	Fail on	May lead to overcooling and reactor trip
Residual heat removal system	Fail heat exchanger flow high	Might remove too much energy leading to overcooling
	Fail heat exchanger flow low	Might retard cooldown rate. Not a safety problem
	Boundary violation	In addition to loss of flow, flooding of containment or auxiliary building. Can put water on outside of vessel. Uninhabitable environment. Can be isolated

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
Low-pressure safety injection system	Pump failure	Common pumps with low-pressure safety injection system. Degrade both functions
	Fail flow low	Inadequate circulation could lead to overheating post-LOCA
	Boundary violation	In addition to loss of flow, flooding of containment or auxiliary building. Can put water on outside of vessel. Uninhabitable environment. Can be isolated
Chemical and volume control system	Pump failure	Common pumps with residual heat removal system. Degrade both functions
	Low RCS coolant volume	Low-pressure reactor trip
	High RCS coolant volume	High-pressure reactor trip. See high-pressure safety injection system
	Inadequate chemical control	No immediate damage. Possible primary coolant boundary damage and loss of satem generation efficiency will follow
	Boundary violation	Small break LOCA. Flooding of containment or auxiliary building. Uninhabitable environment. Flow is limited and can be isolated. Can put water on outside of vessel
High-pressure safety injection system	Pump failure	Common pumps with high-pressure safety injection system. Degrade both functions
	Fail on	High-pressure reactor trip. Could lead to overcooling

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
	Fail flow low	Possible undercooling after small break LOCA
	Boundary violation	Small break LOCA. Flooding of containment or auxiliary building. Uninhabitable environment. Flow is limited and can be isolated. Can put water on outside of vessel
	Pump failure	Common pumps with chemical and volume control system. Degrade both functions. Lose reactor coolant seal flow; must be trip pumps or physical damage can result
Engineered safety features actuation system	Fail off	No effect in single-failure mode
	Fail LPI system on	At high pressure, pumps deadhead into check valves. May damage pumps
	Fail HPI system on	Borated water injected, decreasing power. Coolant pressure increased until safety valves release. Causes reactor high-pressure trip
	Fail emergency feedwater system on	May lead to overcooling and reactor trip
	Fail containment spray system on	Water in containment. May lead to overcooling. Can put water on outside of vessel
Containment spray system	Fail off	No effect in single-failure mode
	Fail on	Water in reactor building. May lead to overcooling. Can put water on outside of vessel. Can be isolated
	Boundary violation	May flood auxiliary building

Table 3.2.1.1 (continued)

System	Failure mode	Effect and remarks
Cooling/service water systems	Fail low	Inadequate cooling and/or water source for residual heat removal, low-pressure safety injection, high-pressure safety injection, chemical and volume control, emergency feedwater system, and the condenser
	Boundary violation	In addition to loss of flow, flooding of containment or auxiliary building. Can put water on outside of vessel. Can be isolated
Refueling	Fail on	Containment floor flooded with borated water. Borated water storage tank empty. Lose source for high-pressure safety injection and containment spray systems. Can put water on outside of vessel
	Boundary violation	Containment floor may flood with borated water. Borated water storage tank empty. Lose source for high-pressure safety injection and containment spray system. Can put water on outside of vessel

Table 3.2.1.2. FMEA: Systems level multiple failures

System	Failure mode	Effect and remarks
ICS modules	Various	The ICS is designed to keep the plant in balance. There are various combinations of module failures to produce imbalance. The two of major importance are (1) pulling the control rods/ reducing feedwater or (2) inserting rods/increasing feedwater. These also result from massive nonnuclear instrumentation loss such as power failure. Both cases result in reactor trip: (1) high-pressure, (2) low-pressure. The operator must properly control the feedwater in both cases. He can either under- or overcool the system with improper action
ICS/reactor coolant system	S. G. overfeed/ LOCA	A small break LOCA coupled with high feedwater flow can lead to overcooling without operator action. Requires simulation
ICS/nonnuclear and nuclear instrumentation/control and instrument power system		See ICS modules
ICS/main steam system	S. G. overfeed/ boundary violation	Steam generator blowdown coupled with main feedwater overfeed could lead to overcooling without operator action. Requires simulation
ICS/turbine bypass system	S. G. overfeed/ fails open	Limited steam generator blowdown. Could lead to overcooling without operator action. Requires simulation
ICS/high-pressure safety injection system	S. G. overfeed/ fail flow low	Low-pressure reactor trip, possible loss of natural circulation, loss of primary pump seal water, possible core overheating. Operator may depressurize to restore circulation, might then overcool vessel with core flood tanks/low-pressure injection/ flooded steam generator(s). Requires simulation
ICS/ESFAS	Various/fails to actuate	Lose automatic actuation of mitigating systems. Operator can actuate all systems. ESFAS is designed to fail in the trip mode

Table 3.2.1.2 (continued)

System	Failure mode	Effect and remarks
Reactor coolant system/ main steam system	Break/break	A small break LOCA coupled with main steam line break could produce severe overcooling. Requires simulation
Reactor coolant system/ turbine bypass system	Break/fail open	Similar to RSC/main steam system with a 25% main steam line break. Main difference is secondary loop remains closed
Reactor coolant system/ feedwater system	Break/fail flow high	A small break LOCA coupled with high feedwater flow can lead to overcooling without operator action. Requires simulation
Reactor coolant system/ high-pressure safety injection system	Break/fail flow low	A small break LOCA leading to low-pressure reactor trip. Possible loss of natural circulation, loss of primary pump seal water, possible core overheating. Operator may depressurize to restore circulation, might then overcool vessel with core flood tanks/low-pressure injection/flooded steam generator(s). Requires simulation
Condenser and condensate system/high-pressure safety injection system	Loss of flow/ fail flow low	Partial loss of primary heat sink. Loss of primary coolant pump seal cooling. Operator will have to use emergency feedwater to establish natural circulation if not depressurize to use low-pressure safety injection system. Possibily of core overheating and vessel overcooling. Requires simulation
Condenser and condensate system/cooling-service water systems	Loss of flow/ fail flow low	Partial loss of primary heat sink. Inability to cool reactor coolant, HPI and LPI pumps, and containment. Operator will have to use emergency feedwater to establish natural circulation. Could lead to core overheating. Requires simulation
Feedwater system	Loss of flow	Has same systems coupling as condenser and condensate system. See system interactions above
Feedwater system/high-pressure safety injection system	Fail flow high/ fail flow low	Low-pressure reactor trip, possible loss of natural circulation. Loss of primary pump seal water, possible core overheating. Operator may depressurize to restore circulation, might then overcool vessel with core flood tanks and low-pressure injection. Requires simulation

Table 3.2.1.2 (continued)

System	Failure mode	Effect and remarks
Feedwater system/ cooling-service water systems	Fail flow high/ fail flow low	Low-pressure reactor trip, possible loss of natural circulation. Inability to cool reactor coolant, HPI and LPI pumps. Could lead to core overheating. Requires simulation
Feedwater system/ refueling system	Fail flow high/ boundary violation	Loss of borated water storage tank could make HPI ineffective. See feedwater system/high-pressure safety injection system. Also possible loss of LPI effectiveness

action and has been shown to take acceptable courses in the vast majority of cases. The cases where cascading events have occurred coupled with operator actions of commission or omission have been characterized by equipment in the wrong state (e.g., valves closed); equipment in "manual," preventing automatic action; failures which present incorrect information to the operator; and the operator's misinterpreting information he is given. These are in addition to outright failures. The number of combinations makes a complete study difficult. The most fruitful approach might be to use FMEAs to select systems which are "critical" and use event trees to include operator action when these systems are in use or required.

3.2.2 Integrated Control System

3.2.2.1 System Description: Integrated Control System

The integrated control system (ICS) controls the reactor, steam generator feedwater flow, and turbine under all operating conditions. The ICS attempts to optimize the generated power response to the unit load demand while recognizing the capabilities and limitations of the reactor, steam generator, feedwater system, and turbine. When any single portion of the plant is at an operating limit or an operator control station is in the manual mode, the ICS design uses the limit or manual station as a load-limiting condition.

The ICS controls reactor coolant temperature for loads between 15 and 100% rated power to a constant average and maintains constant steam pressure at all loads. Unit performance is optimized by limiting steam pressure variations; by limiting between the steam generator, turbine, and the reactor; and by limiting the unit load demand upon loss of the steam generator feed system, the reactor, or the turbine generator. The ICS ensures correlation among the generated load, turbine valves, feedwater flow, and reactor power.

The ICS includes four subsystems as shown in the top level ICS logic flow diagram (Fig. 3.2.2 foldout in pocket). The four subsystems are the unit load demand, the integrated master, the steam generator feedwater control, and the reactor control. Control of the plant is achieved through feed-forward control from the unit load demand subsystem. The unit load demand subsystem produces demands for parallel control of the turbine, reactor, and steam generator feedwater system through their respective subsystems.

The integrated master subsystem is capable of automatic turbine valve control from minimum turbine load to full output. The steam generator feedwater subsystem is capable of automatic or manual feedwater control from startup to full flow. The reactor control subsystem is designed for automatic or manual operation above 15% full power and for manual operation below 15% full power. The basic function of the ICS is to match generated power to the unit load demand.

3.2.2.2 Oconee I Integrated Control System Logic Flow Diagram

An ICS analog flow diagram (Fig. 3.2.3 foldout in pocket) for the Oconee I ICS has been prepared by Science Applications, Inc. from the Bailey Meter Company (BMCo) drawings and system descriptions.[2] The effects of the ICS transfer switches blocking certain signal paths under various plant conditions are shown directly on the logic flow diagram in order to aid in the interpretation of ICS functions during various operating modes and transient conditions. All hand/auto control stations are shown in order to assess the ability of the operator to control the plant with failed ICS inputs, outputs, or modules. This diagram is sufficiently detailed to serve as a basis for the ICS modeling effort as well as the basis for propagation of signals through the ICS for failure mode and effects analysis (FMEA).

3.2.2.3 Failure Mode and Effects Analysis for the Oconee I Integrated Control System

A FMEA has been completed for the Oconee I ICS as shown in the flow diagram (foldout in pocket). This analysis consisted of a detailed review and extension of the previous analysis of the ICS as performed by B&W. This FMEA extends the B&W effort in the following ways:

1. addresses both 721 and 820 series systems,

2. considers all inputs to and outputs from the ICS within the boundary of the ICS,

3. considers zero output failures for each item as well as high and low failures, and

4. considers multiple failures for undetected module failures.

Utilizing the results of this analysis and knowledge of the ICS and B&W nuclear steam supply system (NSSS) design details, failures of the following kinds were addressed:

1. Output was considered individually for each ICS input and output signal, and high, low, or zero functional module failure. Consideration of the effect of zero failures led to the conclusion that the transient induced will be no more severe than those caused by either high or low failure of the same item.

2. The effect of multiple failures was considered for modules whose failure may have no immediate effect and, therefore, will remain undetected until a subsequent event occurs. An example of this module type is the Btu limit module, which limits feedwater demand based on a set of limiting curves (see Fig. 3.2.4). If this module is failed high, then a subsequent failure or transient requiring the Btu limit on feedwater flow will have a different response than intended

3. Operator actions available to mitigate the results of the transient are noted in the FMEA tables. Operability of the hand/auto control stations after the failure was considered.

4. Common cause and common mode failures were not considered in this analysis because of the time and budget constraints of the project. In order to provide realistic assessments of these types of events, extremely detailed information such as the types of components used in various modules, interconnections between ICS cabinets, and the placement of sensors would be required.

> Note that the ICS power supply has been extensively studied as a result of IE Bulletin 79-27. This bulletin has led to modifications designed to mitigate the results of this type of failure.

Tables 3.2.2.1 through 3.2.2.3 contain, respectively, those failures of the inputs to, outputs from, and modules within the ICS that potentially lead to serious upsets in plant conditions or for which the consequences could not be adequately assessed. Those failures that lead to reactor trip without loss of normal ICS control action after trip are not included.

3.2.3 Condensate and Feedwater Systems

3.2.3.1 System Descriptions: Condensate and Feedwater Systems Condenser and Condensate System

The function of the condenser is to condense steam from the low-pressure turbine exhausts, the feedwater pump turbines, and the turbine bypass system. The condensate system takes condensed steam from the condenser and heater drains and delivers it to the feedwater system. Along the way, the condensate is purified and heated. The condenser and condensate system is a nonsafety system. See Appendix A for details.

The feedwater system takes condensate from the condensate system, heats it, raises its pressure, and delivers it to the steam generators to be boiled off as steam. The feedwater system is a nonsafety system that penetrates containment. See Appendix A for details.

3.2.3.2 Oconee I Functional Block Diagrams: Condensate and Feedwater Systems

Figures 3.2.5 through 3.2.17 are the functional block diagrams for the condensate and feedwater systems. The information was taken from drawing numbers PO-121A-1, PO-121B-1A, and PO-121B-1B. The analysis was done assuming full turbine trip conditions.

The figures labeled "COND. FBD" are condensed block diagrams incorporating the straight-line portions of the full diagrams into one block. This facilitates later failure mode and effects analysis. Where practical, the same block numbers were used, so that some condensed blocks have several numbers.

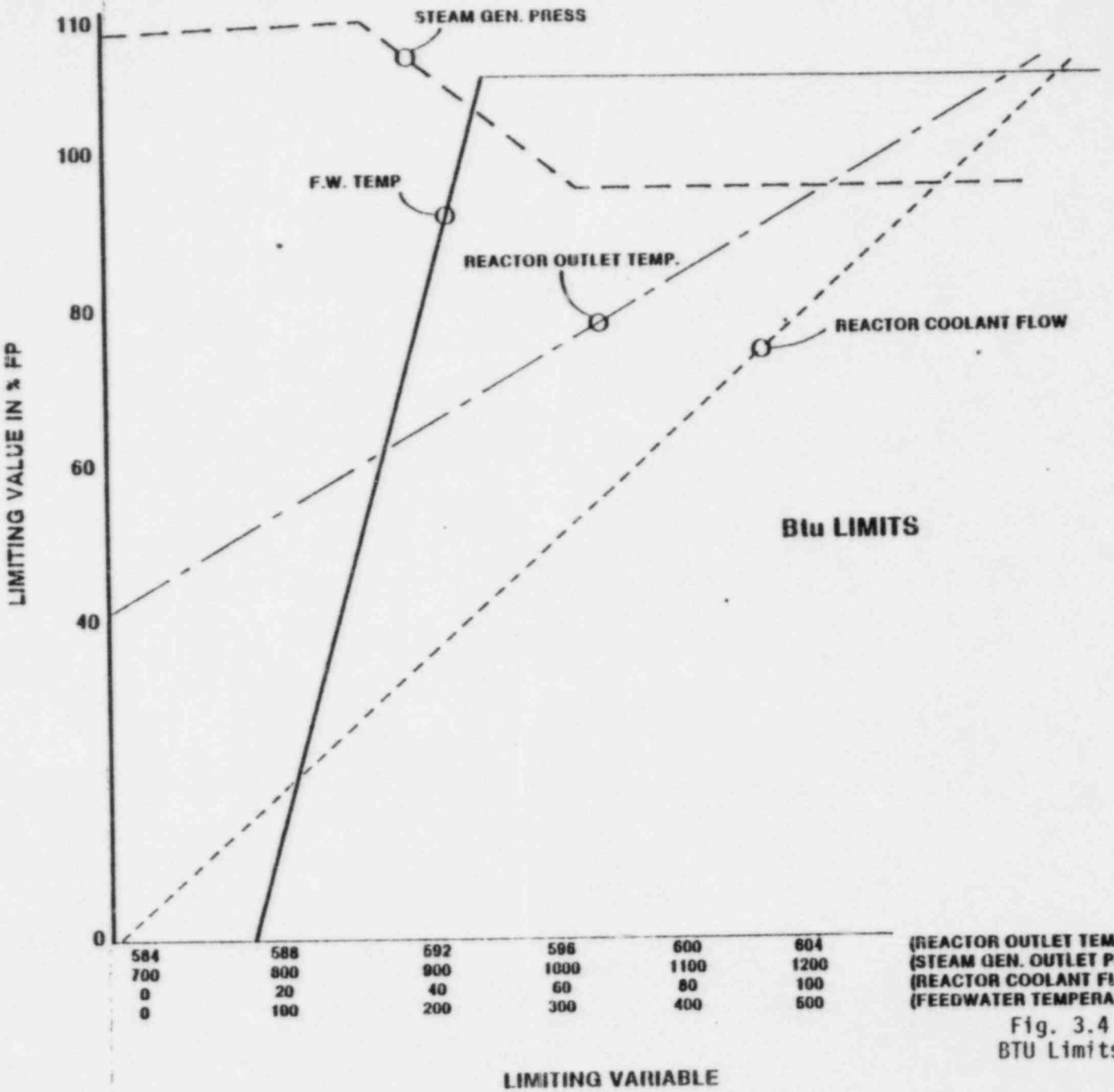


Fig. 3.4
BTU Limits

Table 3.2.2.1. FMEA: ICS Inputs

Item	Failure mode	Effects	Subsequent ICS control actions	Remarks
Power supply failure	Loss of power	Loss of FW transient	ICS control stations inoperative	System modifications and operating procedures modified per IE bulletin 79-27 to mitigate consequences of this failure
Turbine header pressure	Fails above set point	Atmos. vent and turbine bypass valves open fully for later plants. For earlier plants, including Oconee, open turbine throttle valves only	Manual control of valves is possible	Without operator action primary system overcooling will result. Extent requires simulation
	Fails below set point	Turbine throttle valve closes. Atmos. vent valves and turbine bypass valves held closed; steam line safety valve opens	Atmos. vent (if present) and turbine bypass valves can be controlled manually	Turbine throttle valve closure will cause trip of reactor due to high RC pressure
S.G. 'A' outlet pressure	Fails above set point	Turbine bypass valve 'A' opens, reduction in FW 'A' flow due to Btu limit	Bypass flow can be controlled by steam isolation valves (if present) or bypass valve control at auxiliary shutdown panel	MW electric tracks steam flow down. Loop 'A' bypass remains open after trip
S.G. 'B' outlet pressure	Fails above set point	Turbine bypass valve 'B' opens. Reduction in FW 'B' flow due to Btu limit	Bypass flow can be controlled by steam isolation valves (if present) or bypass valve control at auxiliary shutdown panel	MW electric tracks steam flow down. Loop 'B' bypass remains open after trip

Table 3.2.2.1 (continued)

Item	Failure mode	Effects	Subsequent ICS control actions	Remarks
FW temperature	Fails low	Loss of FW due to Btu limit reduction	Manual FW control possible	Use of single 'averaged' or selected FW temperature or both loop feedwater temperatures is plant dependent
FW flow 'A'	Fails low	Loop 'A' MFWV opens fully. Fill 01SG 'A' to high level limit	Unit response requires simulation	H/A station can be used to control FW flow
FW flow 'B'	Fails low	Loop 'B' MFWV opens fully. Fill 01SG 'B' to high level limit	Unit response requires simulation	H/A station can be used to control FW flow
Startup S.G. level 'A'	Fails low	Opens both MFWV and SUFWV 'A' fully. Valves will remain open and can lead to over-cooling	Evaluation of severity of overcooling transient requires simulation	Manual control of FW valves is possible. Some units will trip main FW pumps on high SG level. (Oconee 1, 2, and 3 non-ICS)
Startup S.G. level 'B'	Fails low	Opens both MFWV and SUFWV 'B' fully. Valves will remain open and can lead to overcooling	Evaluation of severity of overcooling transient requires simulation	Manual control of FW valves is possible. Some units will trip main FW pumps on high SG level. (Oconee 1, 2, and 3 non-ICS)
ULD rate of change	Fails low	Does not allow ULD to change	FW demand is limited by Btu limits following reactor trip. Manual FW control possible	Potential for overcooling following reactor trip
'A' and 'B' loop atmospheric exhaust valves (hand station)	Fails high	Atmospheric exhaust valves open fully	Control normal in automatic mode	Plant specific. (Not applicable to Oconee)

Table 3.2.2.1 (continued)

Item	Failure mode	Effects	Subsequent ICS control actions	Remarks
Turbine Hdr press. set point		See turbine header pressure		
$1T_0$ set point	Fails high or low	FW demand ratio at limit	Btu limits and SG level sensors control SG level	Manual FW control possible
MFW block valve open indication	Fails closed	Similar to failure low of MFW flow signal		

Table 3.2.2.2. FMEA: ICS Outputs

Item	Failure mode	Effects	Subsequent ICS control actions	Remarks
Turbine bypass valve	Fails open	Cannot control steam pressure, overcooling when reactor trips		Isolation valves (if present) can be closed manually to control steam pressure
Atmospheric vent valves	Fails open	Cannot control steam pressure, overcooling when reactor trips		Isolation valves (if present) can be closed manually to control steam pressure
Allow start of any RCP	Prevent start of pump	Cannot start any RC pump	No immediate effect	Undetected failure may exist. Could prevent restart if pumps were tripped during transient
Loop 'A' startup FW valve	Fails open	No immediate effect while at power	Can overfill SG 'A' if reactor were to trip	Startup block valve can be closed manually
Loop 'B' startup FW valve	Fails open	No immediate effect while at power	Can overfill SG 'B' if reactor were to trip	Startup block valve can be closed manually

Table 3.2.2.3. FMEA: ICS Modules

Item	Failure mode	Effects	Subsequent ICS control actions	Remarks
Turbine header pressure error	Fails high	Bypass and atmos. exhaust valves open fully. Primary system overcooling. For earlier plants, including Oconee, open turbine throttle valves only	Feedwater runback following reactor trip	Valves can be closed manually. Note that turbine header pressure error does not feed bypass valves at Oconee I
Steam pressure error 'A'	Fails high	Bypass and atmospheric exhaust valves 'A' open fully. Primary system overcooling	Feedwater runback following reactor trip	Valves can be closed manually. Note that steam pressure error feeds bypass valves only at Oconee I
Steam pressure error 'B'	Fails high	Bypass and atmospheric exhaust valves 'B' open fully. Primary system overcooling	Feedwater runback following reactor trip	Valves can be closed manually. Note that steam pressure error feeds bypass valves only at Oconee I
Loop 'A' atmospheric and bypass valves	Fails open	Bypass and atmospheric exhaust valves 'A' open fully. Primary system overcooling. (Atmospheric exhaust valves not present at Oconee I.)	Feedwater runback following reactor trip	Valves cannot be closed manually. Steam line isolation valves can be closed manually if available (not available at Oconee I)
Loop 'B' atmospheric and bypass valves	Fails open	Bypass and atmospheric exhaust valves 'B' opens fully. Primary system overcooling. (Atmospheric exhaust valves not present at Oconee I.)	Feedwater runback following reactor trip	Valves cannot be closed manually. Steam line isolation valves can be closed manually if available (not available at Oconee I)

Table 3.2.2.3 (continued)

Item	Failure mode	Effects	Subsequent ICS control actions	Remarks
Total feedwater demand	Fails high	Feedwater demand increases to Btu limit. Reactor power remains nearly constant, resulting in overcooling transient	Feedwater controlled at high level limit	Manual control of both FW demands can prevent over-cooling
Btu limit (A&B) auctioneer	Fails to select minimun valve	Feedwater flow limited by high level limit if transient requiring Btu limit control occurs subsequent to failure		Feedwater can be controlled manually. Failure of Btu limit would be undetected. Excessive feedwater flow will occur if feedwater demand failure occurs after Btu limit failure
Feedwater flow error (A&B)	Fails high	Failure causes feeding of one SG to high level limit		Overcooling can be averted by manual control of overcooled SG FW flow after trip

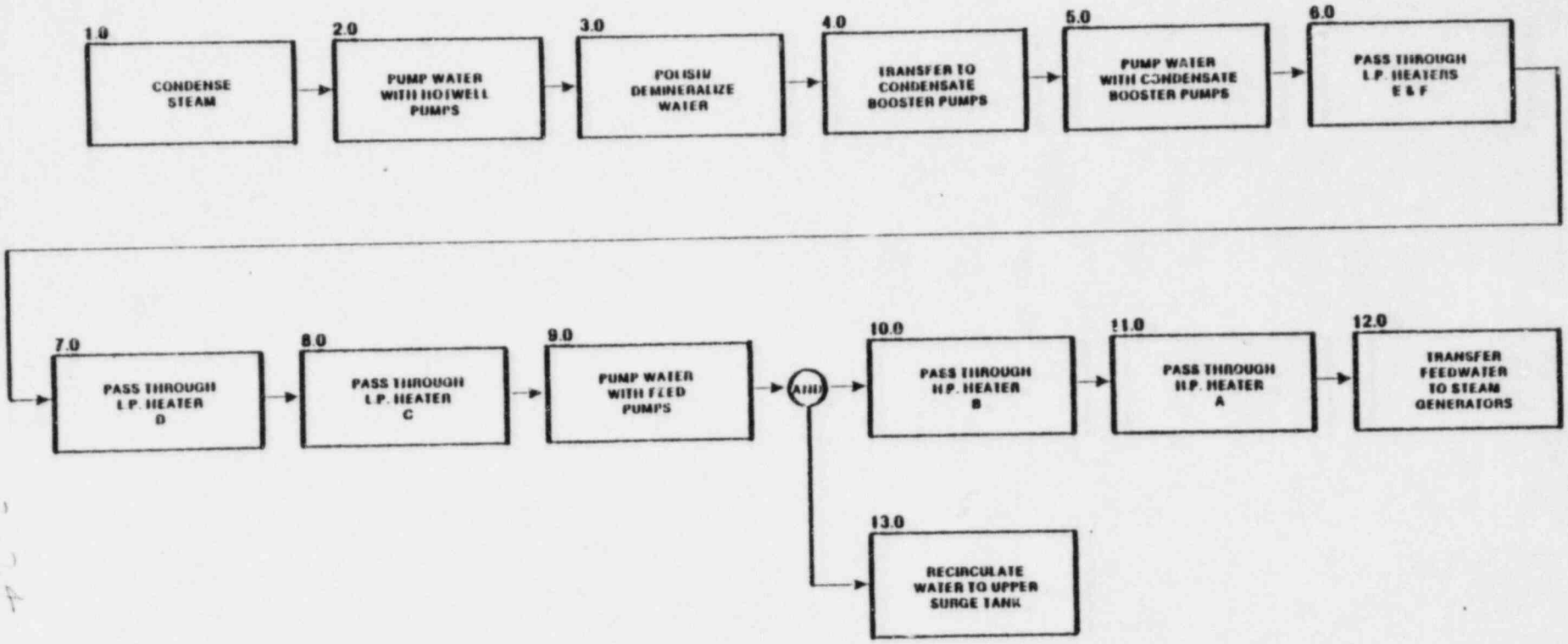
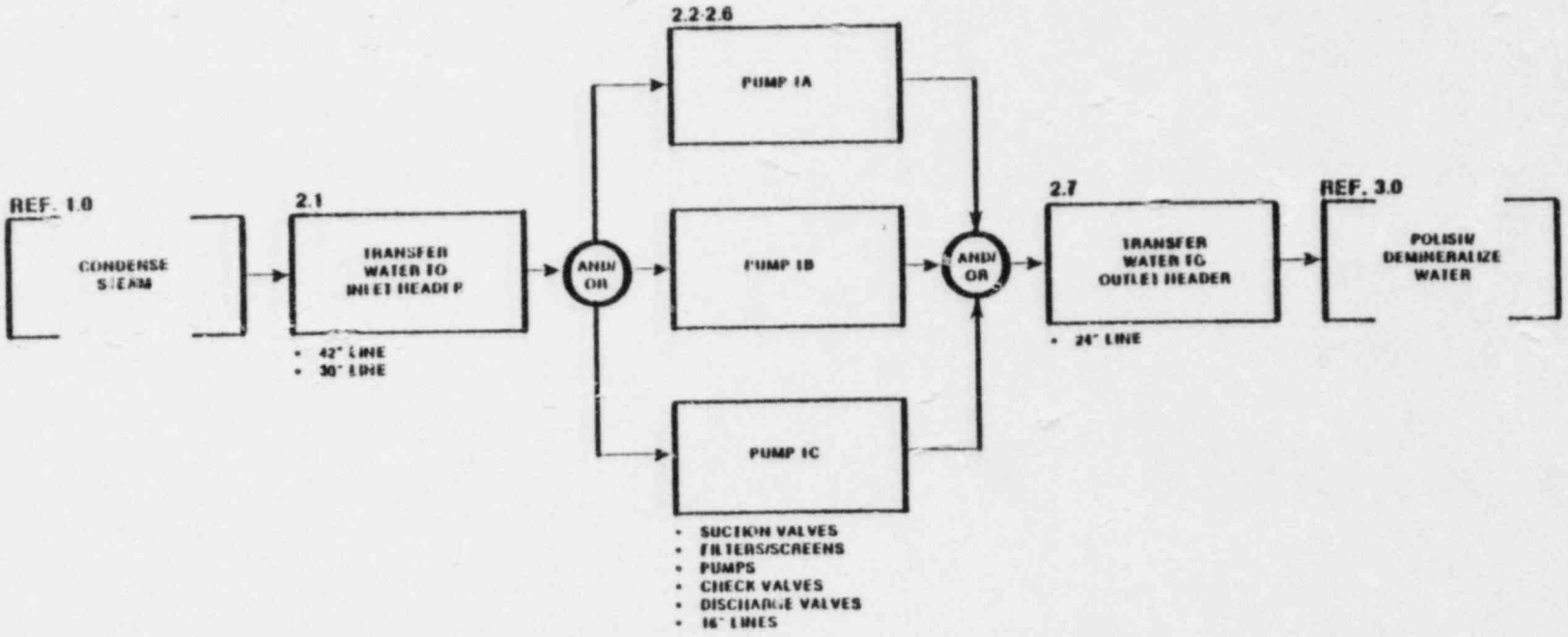


Fig. 3.5

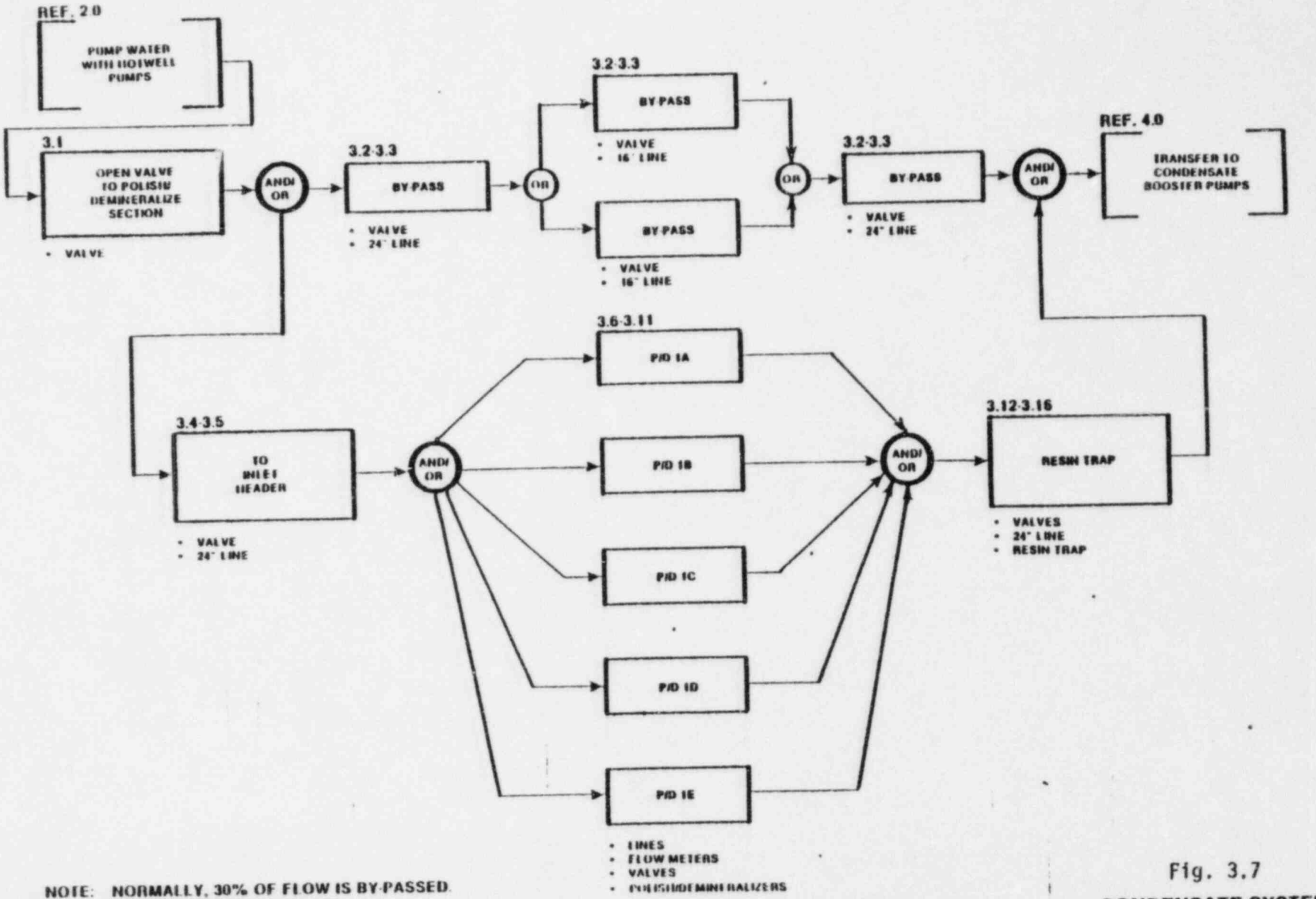
CONDENSATE AND FEEDWATER SYSTEMS TOP LEVEL



NOTE: LOGIC IS 2/3 UNDER NORMAL OPERATION, 1/3 IS OPTION FOR REDUCED FLOW.

Fig. 3.6

CONDENSATE SYSTEM
COND. FBD 2.0
PUMP WATER WITH
HOTWELL PUMPS



NOTE: NORMALLY, 30% OF FLOW IS BY-PASSED.
0% UNDER REDUCED FLOW.

Fig. 3.7

CONDENSATE SYSTEM
COND. FBD 3.0
POLISH/DEMINERALIZE WATER

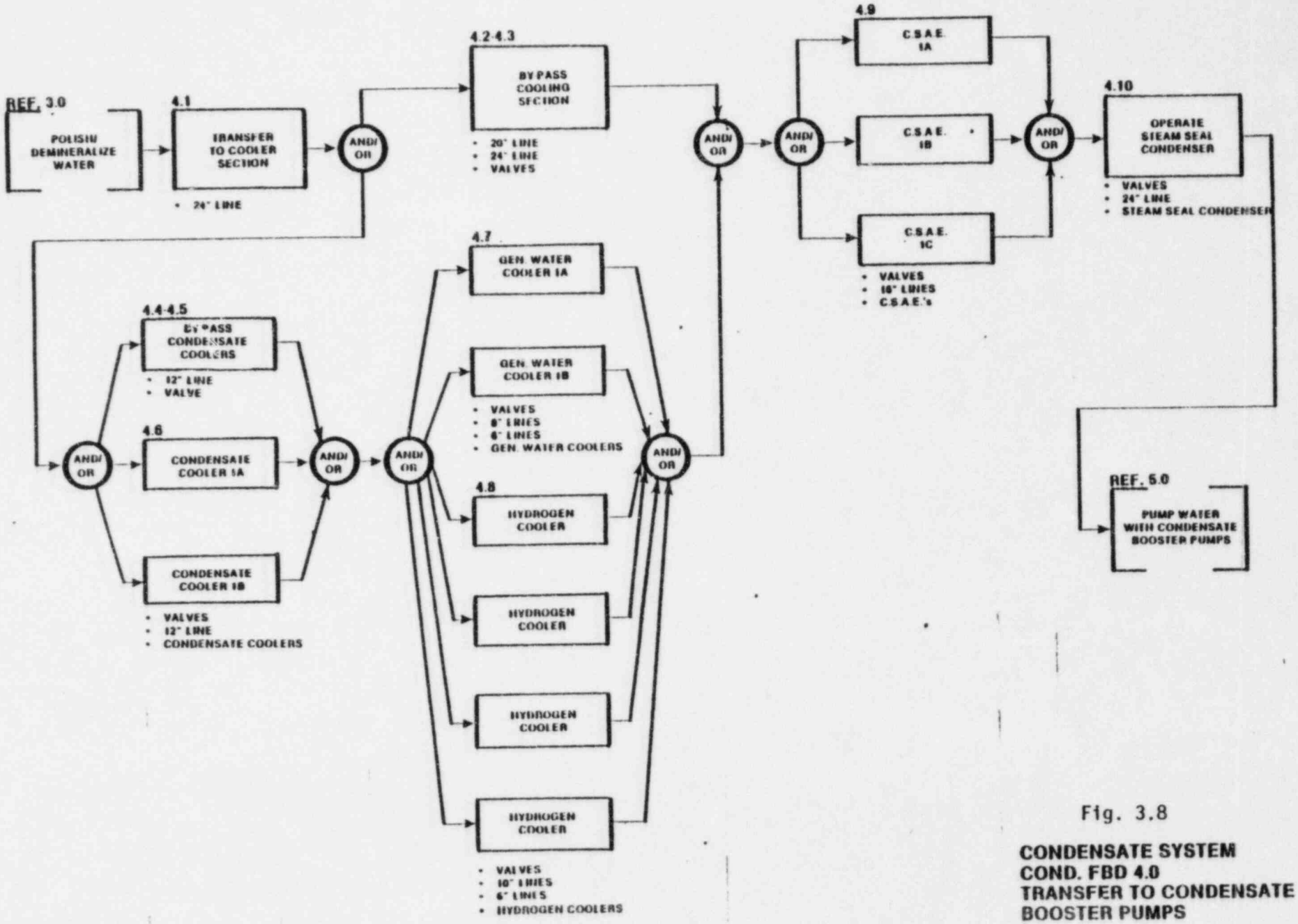


Fig. 3.8

CONDENSATE SYSTEM
COND. FBD 4.0
TRANSFER TO CONDENSATE BOOSTER PUMPS

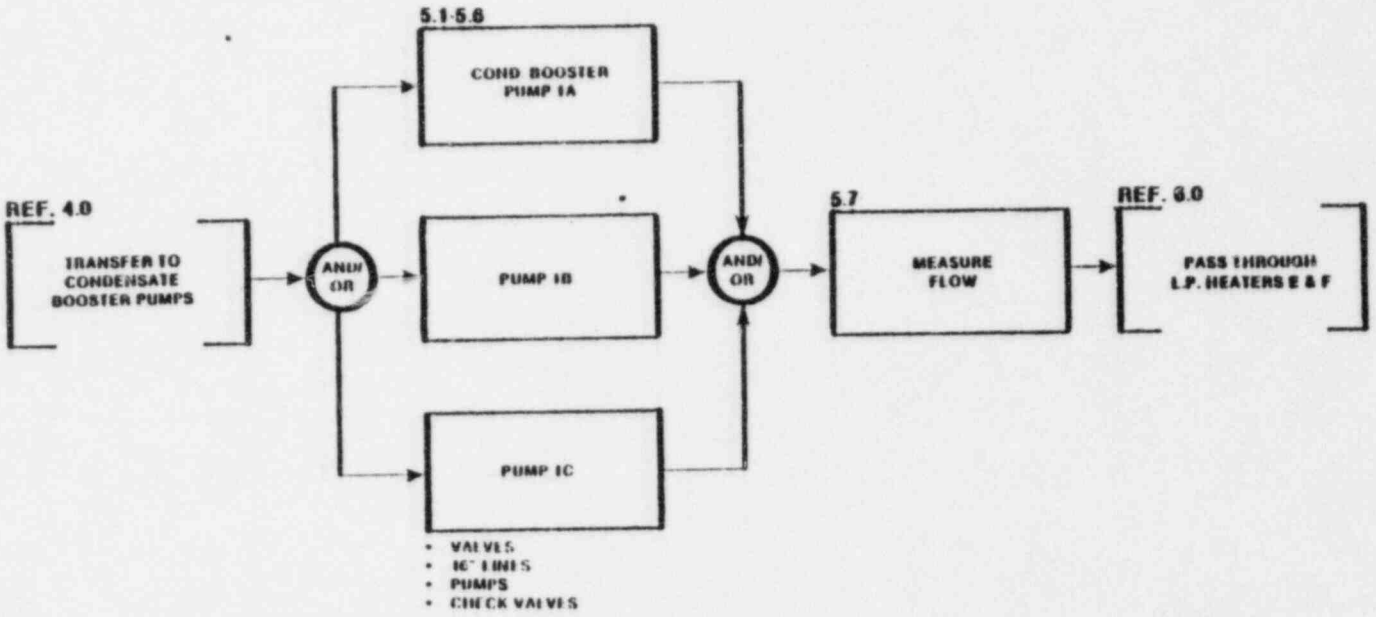
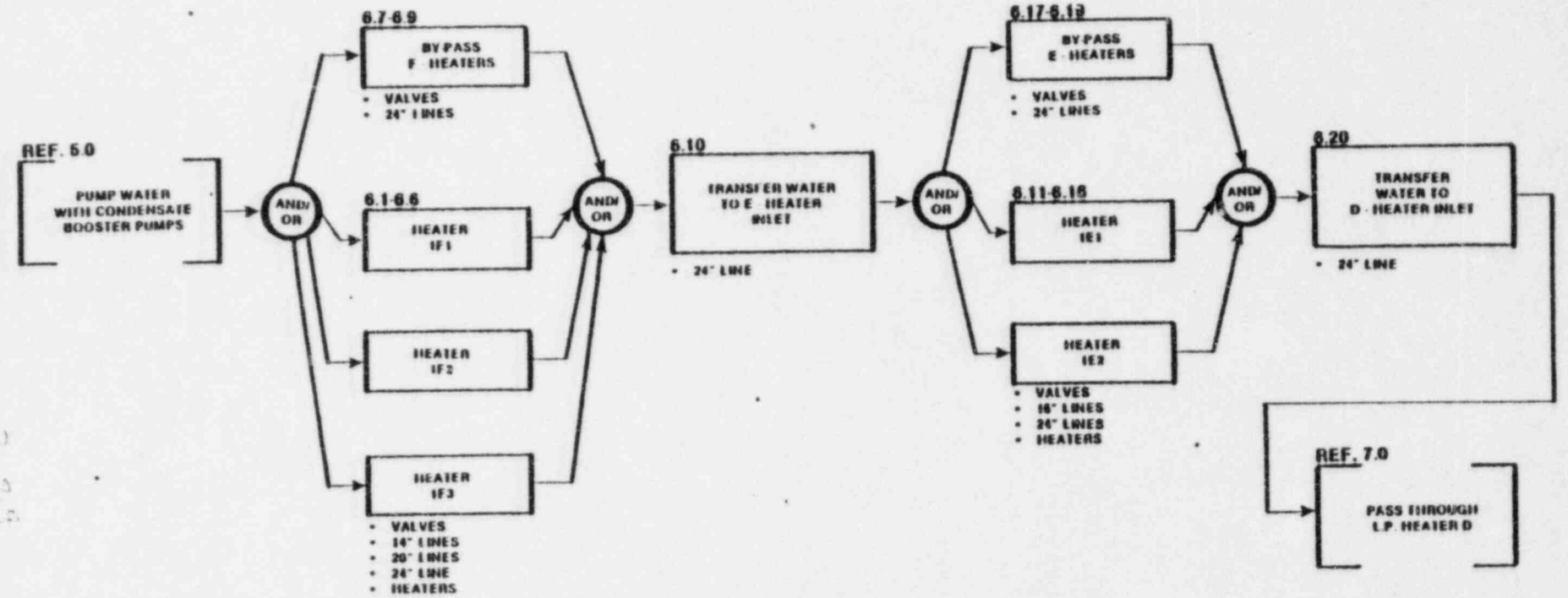


Fig. 3.9

CONDENSATE SYSTEM
COND. FBD 5.0
PUMP WATER WITH
CONDENSATE BOOSTER PUMPS



NOTE: NO HEATING STEAM AVAILABLE

Fig. 3.10

CONDENSATE SYSTEM
COND. FBD 6.0
PASS THROUGH L.P.
HEATERS E & F

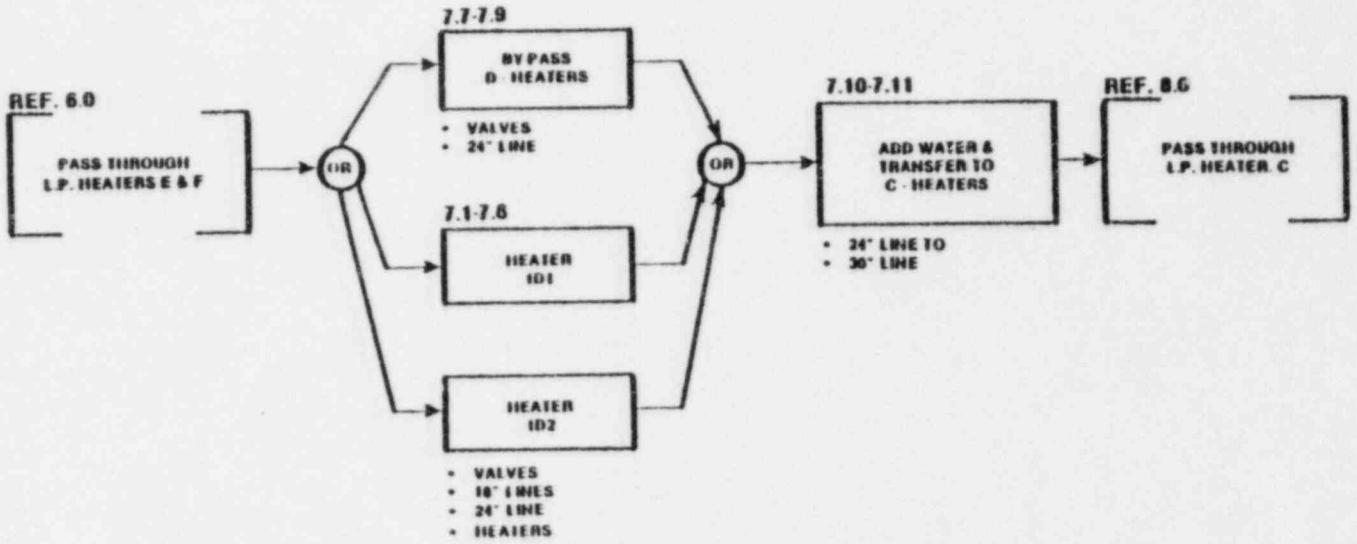


Fig. 3.11

CONDENSATE SYSTEM
COND. FBD 7.0
PASS THROUGH
L.P. HEATER D

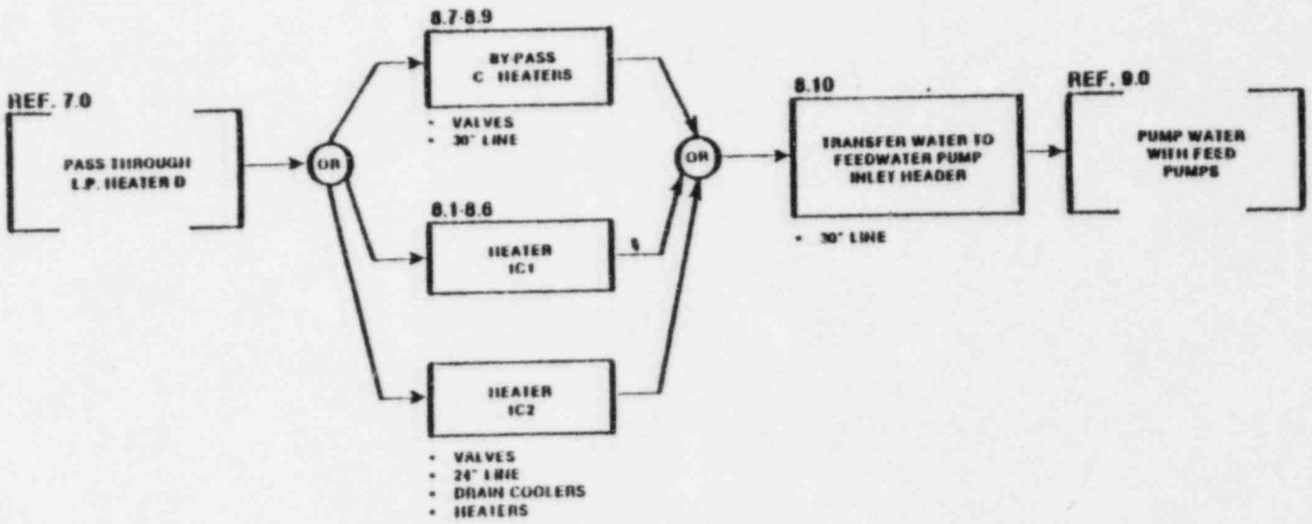


Fig. 3.12

CONDENSATE SYSTEM
COND. FBD 8.0
PASS THROUGH
L.P. HEATER C

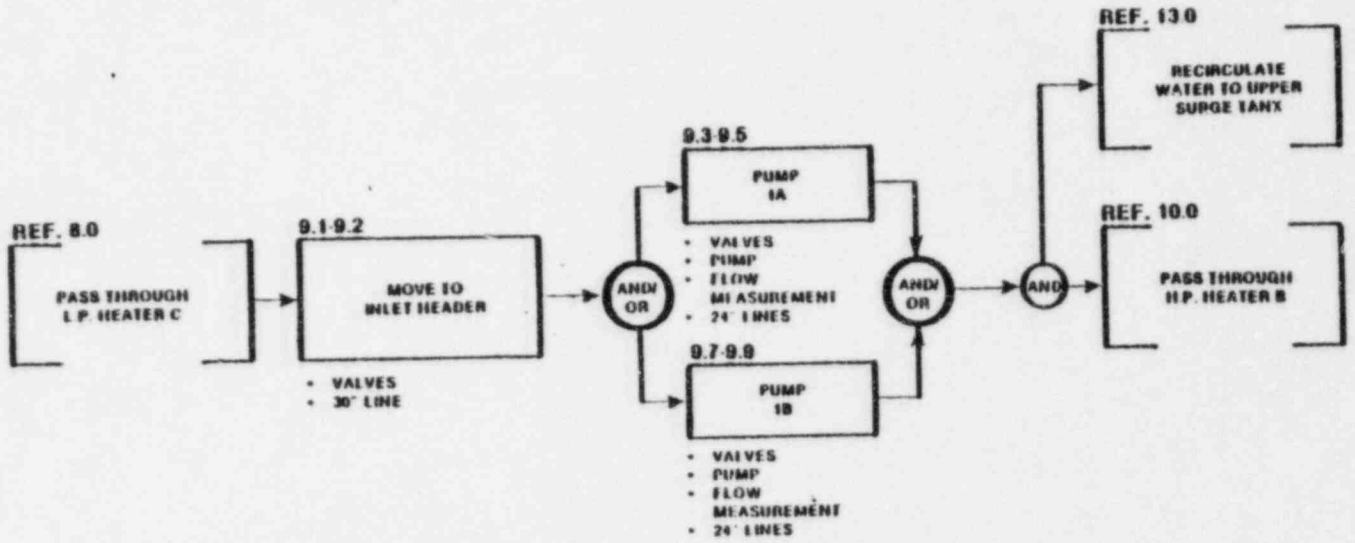


Fig. 3.13

FEEDWATER SYSTEM COND. FBD 9.0 PUMP WATER WITH FEED PUMPS

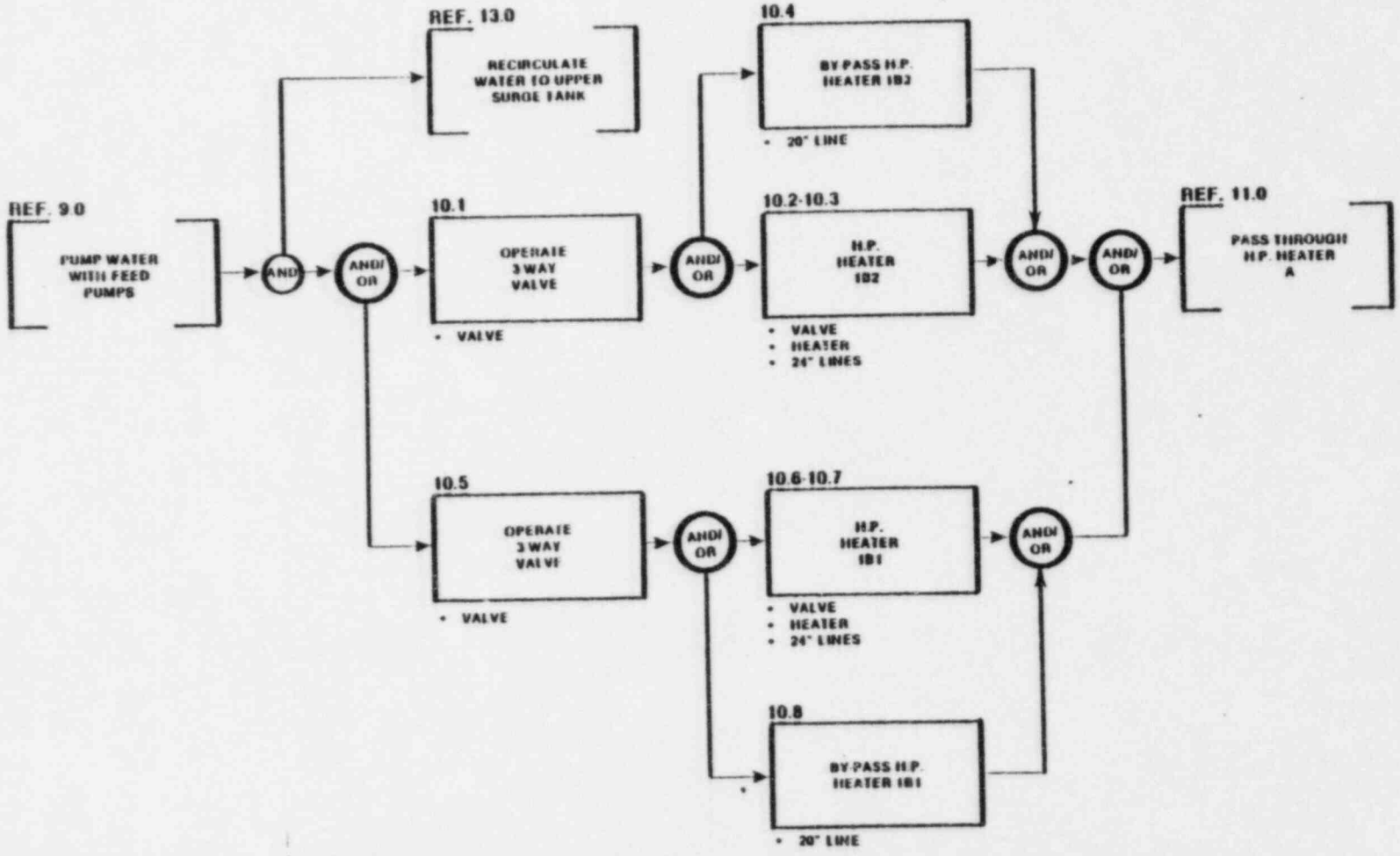


Fig. 3.14

FEEDWATER SYSTEM
COND. FBD 10.0
PASS THROUGH
H.P. HEATER B

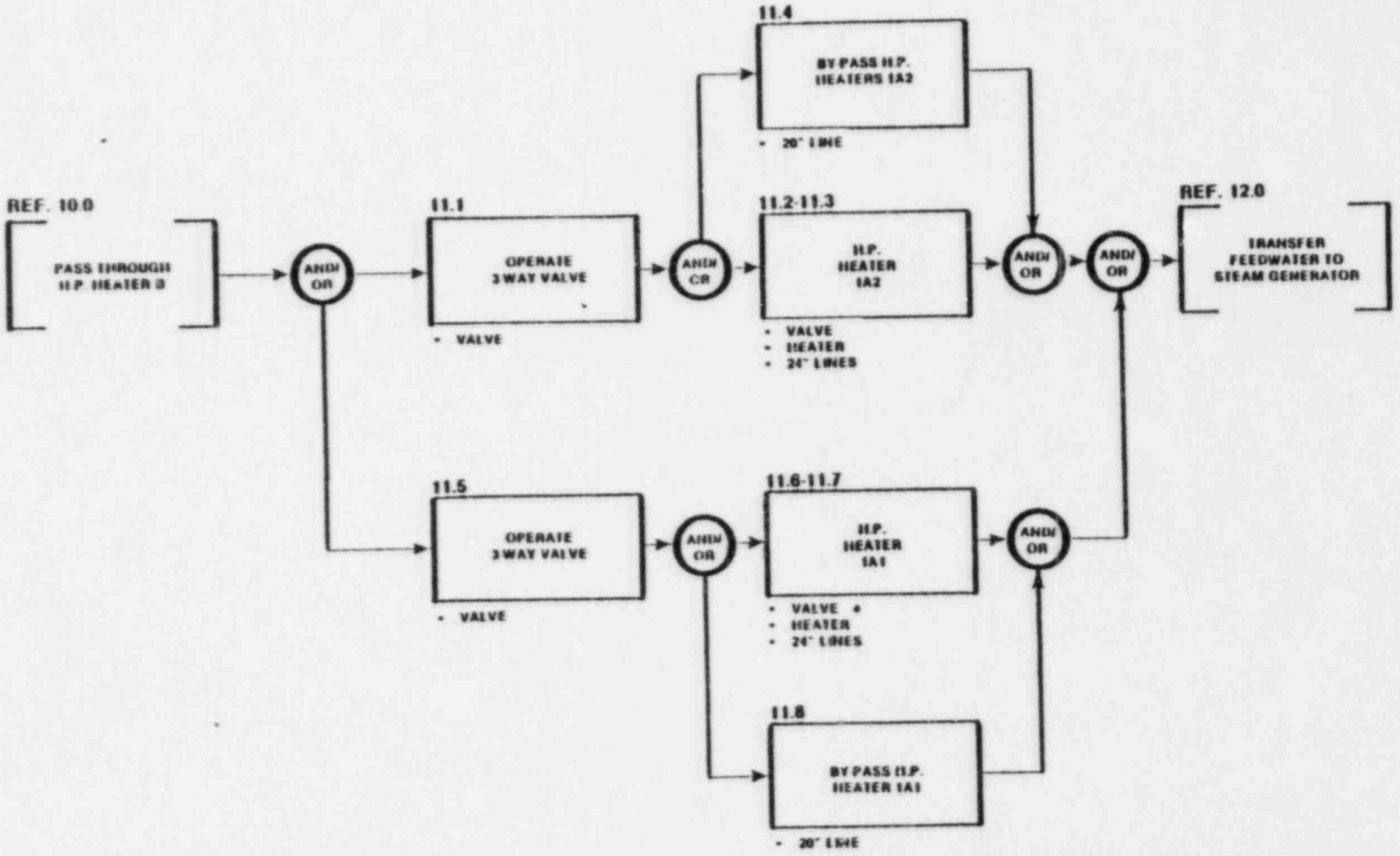


Fig. 3.15

**FEEDWATER SYSTEM
COND. FBD 11.0
PASS THROUGH
H.P. HEATER A**

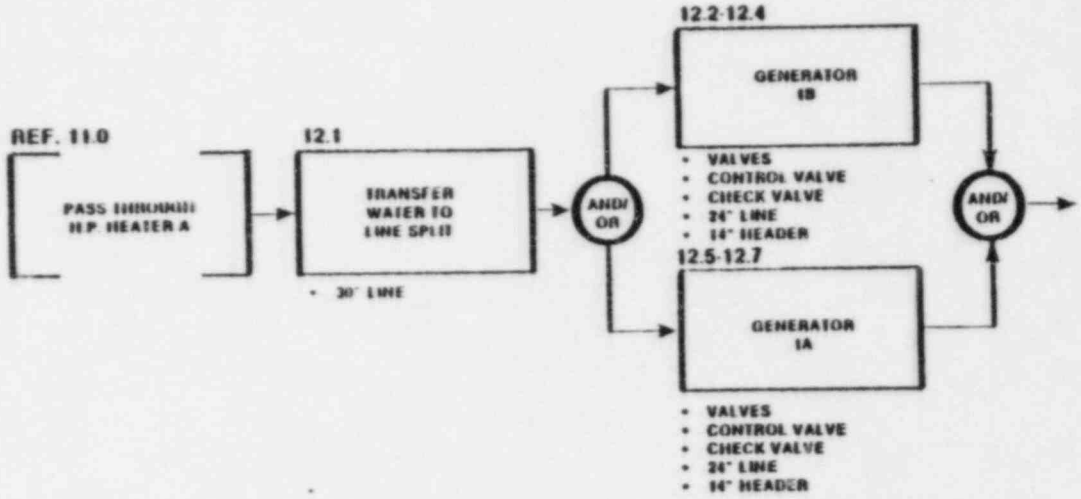


Fig. 3.16

FEEDWATER SYSTEM
COND. FBD 12.0
TRANSFER FEEDWATER
TO STEAM GENERATORS

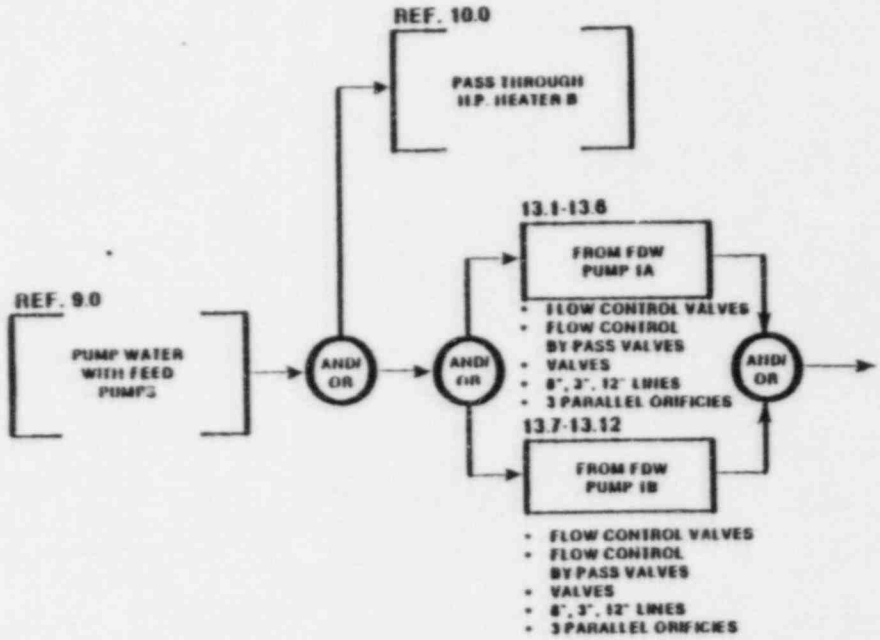


Fig. 3.17

FEEDWATER SYSTEM COND. FBD 13.0 RECIRCULATE WATER TO UPPER SURGE TANK

Table 3.2.3.1. FMEA: Condensate and feedwater systems

No.	Component	Failure mode	Effects and remarks
2.1	Line to hotwell pump inlet heater	Break	Loss of condenser vacuum. Loss of condensate, leading to loss of normal feedwater flow. This should lead to reactor trip and emergency feedwater startup. Emergency feedwater will have to come from upper surge tank
		Block	Loss of condensate, leading to loss of normal feedwater flow. This should lead to reactor trip and emergency feedwater startup
2.2-6	Three parallel hotwell pump lines	Pump failure	No effect, spare is available
		Block	No effect, spare line is available
		Break	Check valve isolates from downstream side, motor-operated valve available to isolate condenser side. If isolated, no effect as spare is available. If not, lose condenser vacuum and normal feedwater flow. Emergency feedwater must come from upper surge tank. (May drain hotwell pump)
3.1	Line from hotwell pump heater to polish/demineralizer	Break/block	Loss of condensate, leading to loss of normal feedwater flow. This should lead to reactor trip and emergency feedwater startup. (Emergency feedwater can come from condenser, as check valves protect downstream side.)
3.2.3	Polish/demineralizer bypass	Block	Little effect, as the full stream can flow through the polish/demineralizer
		Break	If the break is near the flow control valves, it can be isolated, so the same effect as a block. If not, condensate flow will be lost, leading to reactor trip and emergency feedwater startup
3.4.5	Line to polish/demineralizer inlet heater	Block	Little immediate effect, as full flow can be bypassed. Water quality will deteriorate
		Break	If before isolation valve, condensate flow will be lost, leading to reactor trip and emergency feedwater startup. If after isolation valve, full flow can be bypassed. Water quality will deteriorate

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
3.6-11	Five parallel polish/ demineralizer lines	Block	Possibly reduced flow through total polish/demineralizer section, depending on design capacity. This would lead to reduced water quality. More likely, each is oversized so the loss of one will have little effect
		Break	Isolation valves are present so a break can be contained. Result will then be same as for block. May drain polish/demineralizer unit
		Polish/ demineralizer failure	Depending on design capacity, loss of one polish/demineralizer could reduce water quality. More likely, each is oversized so the loss of one will have little effect
3.12-16	Resin trap	Block	Little immediate effect, as full flow can bypass polish/demineralizer section. Water quality will deteriorate
		Break	If before the last isolation valve, the break can be isolated. If after, condensate flow will be lost, leading to reactor trip and emergency feedwater startup. May drain trap
		Failure	Resin beads could flow on to harm downstream equipment. Clog valves, heat exchangers, damage pump impellers, etc.
4.1	Line to cooler section	Block	Loss of condensate, leading to loss of normal feedwater flow. This should lead to reactor trip and emergency feedwater startup
		Break	Loss of condensate, as in block
4.2.3	Cooling section bypass	Block	Cooler section not capable of full flow, so system would have to go to a reduced-flow condition
		Break	If break is near flow control valve, it can be isolated. If not, loss of condensate, leading to loss of normal feedwater flow. This should lead to reactor trip and emergency feedwater startup

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
4.4.5	Condensate cooler bypass	Block	Little effect. The combination of cooling section bypass and condensate coolers can handle total flow
		Break	If before bypass valve, have loss of condensate, leading to reactor trip and emergency feedwater startup. If after bypass, valve can isolate break
		Break	Little effect, as both coolers have isolation valves. May drain cooler
4.7	Gen. water cooler	Block	Little effect, as in break below
		Break	Little effect, depending on the location. Individual coolers have isolation valves. Before these, both gen. water coolers could be affected, which might result in insufficient cooling. May drain cooler
		Failure	Possible insufficient cooling
4.8	Hydrogen cooler	Block	Same as gen. water cooler
		Break	Same as gen. water cooler
		Failure	Same as gen. water cooler
4.9	C.S.A.E.	Block	If before header, condensate flow is lost, resulting in reactor trip and emergency feed startup. If after heater, one of the three C.S.A.Es is lost. Depending on design capacity this could have little effect, or it could reduce flow, resulting in reactor runback
		Break	Same as block above, as isolation valves are around each ejector
		Failure	If undetected, probably would have minor immediate effect. Possible equipment damage and loss of steam generation efficiency will follow. If detected, same effect as block after header above

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
5.10	Steam seal condenser	Block	Loss of condensate, resulting in reactor trip and emergency feedwater startup
		Break	Same as block. May drain condenser
		Failure	Depends on failure mode. All require plant shutdown. Some will require trip of secondary equipment
5.1-6	Three parallel condensate booster pump lines	Pump failure	No effect; spare is available
		Block	No effect; spare is available
		Break	If inside isolation valves can be contained. If outside isolation valves, have loss of flow, leading to reactor trip and emergency feedwater startup. May drain pump
5.7	Flow meter	Block	Loss of condensate flow, leading to reactor trip and emergency feedwater startup
		Break	Can be isolated, but might drain the F-heaters. Leads to loss of condensate flow, reactor trip and emergency feedwater startup
6.1-6	F-heaters	Block	Flow can be bypassed, but may result in insufficient heating
		Break	Depending on location, may be isolated from other heaters, giving same effect as block, but might drain heater. If outside isolation valves, lose condensate flow, resulting in reactor trip and emergency feedwater startup
		Heater failure	Might result in insufficient heating
6.7-9	F-heater bypass	Block	No effect, as full flow can go through heaters

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
		Break	Loss of condensate flow, leading to reactor trip and emergency feedwater startup. Can be isolated, but may drain heaters
6.10	E-heater inlet time	Block	Loss of condensate flow, leading to reactor trip and emergency feedwater startup
		Break	Can be isolated, so same effect as block
6.11-16	E-heaters	Block	Flow can be bypassed, but may result in insufficient heating
		Break	Depending on location, may be isolated from other heater, giving same effect as block, but might drain heater. If outside isolation valves lose condensate flow, resulting in reactor trip and emergency feedwater startup
		Heater failure	Might result in insufficient heating
6.17-19	E-heater bypass	Block	Reduced flow, as full flow cannot go through heaters. Results in reactor runback or trip
		Break	Loss of condensate flow, leading to reactor trip and emergency feedwater startup. Can be isolated, but may drain heaters
6.20	D-heater inlet line	Block	Loss of condensate flow, leading to reactor trip and emergency feedwater startup
		Break	Can be isolated, so same effect as block
7.1-6	D-heaters	Block	Flow can be bypassed, but may result in insufficient heating
		Break	Depoending on location, may be isolated from other heater, giving same effect as block, but might drain heater. If outside isolation valves, lose condensate flow, resulting in reactor trip and emergency feedwater startup

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
		Heater failure	Might result in insufficient heating
7.7-9	D-heater bypass	Block	Little effect (possibly reduced flow) as most of the flow can go through the heaters
		Break	Loss of condensate flow, leading to reactor trip and emergency feedwater startup. Can be isolated, but may drain heaters
7.10-11	C-heater inlet line	Block	Loss of condensate flow, leading to reactor trip and emergency feedwater startup
		Break	Can be isolated, so same effect as block
8.1-6	C-heaters	Block	Flow can be bypassed, but may result in insufficient heating
		Break	Depending on location, may be isolated from other heater, giving same effect as block, but might drain heater. If outside isolation valves, lose condensate flow, resulting in reactor trip and emergency feedwater startup
		Heater failure	Might result in insufficient heating
8.7-9	C-heater bypass	Block	No effect, as full flow can go through heaters
		Break	Loss of condensate flow, leading to reactor trip and emergency feedwater startup. Can be isolated, but may drain heaters
8.10-9.2	Line to feed pump inlet header	Block	Loss of condensate flow, leading to reactor trip and emergency feedwater startup
		Break	Can be isolated with same effect as block
9.3-9	Main feed pump	Break	Depending on location, can be isolated; treat same as block below. May drain pump or cause total loss of condensate flow, resulting in reactor trip and emergency feedwater startup

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
11.2-3, 11.6-7	A-heater	Break	Can be isolated, same effect as block. May drain heater
		Block	Most flow can be bypassed. May result in some flow reduction. May result in inadequate heating
		Heater failure	May result in inadequate heating
11.4.8	A-heater bypass	Block	No effect as full flow can go through heaters
		Break	Lose total flow, resulting in reactor trip and emergency feedwater startup
12.1	Line to steam generators	Block	Loss of condensate flow, resulting in reactor trip and emergency feedwater startup
		Break	Can be isolated, treat same as block
12.2-7	Line to steam generators	Block	Loss of condensate flow to one of two steam generators, resulting in reactor runback or trip
		Break	If before check valve, same effect as block. If after check valve, may result in steam generator depressurization

Table 3.2.3.1 (continued)

No.	Component	Failure mode	Effects and remarks
		Block	Lose part of flow, causes reactor runback or trip
		Pump failure	Same as block above
13.1-12	Recirculation to upper surge tank	Block	Little effect under normal operation, as no water is required from upper surge tank
		Break	In most locations break can be isolated, giving same effect as block. Near the pump could disrupt pump operation, and after isolation, may drain pump
10.1.5	3-way valve	Block	Lose part of flow, causing reactor runback or trip
		Break	Lose total flow, resulting in reactor trip and emergency feedwater startup
		Stuck on bypass	Possibly inadequate heating
10.2-3, 10.6-7	H-heater	Break	Can be isolated, same effect as block. May drain heater
		Block	Most flow can be bypassed. May result in some flow reduction. May result in inadequate heating
		Heater failure	May result in inadequate heating
10.4.8	B-heater bypass	Block	No effect as full flow can go through heaters
		Break	Can be isolated, but half of flow is lost. Results in reactor runback or trip
11.1.5	3-way valve	Block	Lose part of flow, causing reactor runback or trip
		Break	Lose part of flow, causing reactor runback or trip
		Stuck on bypass	Possibly inadequate heating

3.2.3.3 Failure Mode and Effects Analysis for the Oconee I condensate and Feedwater Systems

3.2.4 Auxiliary Feedwater System

The auxiliary feedwater system (called the emergency feedwater system by Oconee) is designed to provide an adequate supply of cooling water to the steam generators so that they can act as heat sinks for decay heat removal from the reactor core in the event of a loss of power, a feedwater line malfunction, a small LOCA, or a main steam line break. The system is a Safety Class 3 system with the exception of the piping between the isolation valves and the connections to the feedwater piping. These sections of piping are Safety Class 2. The emergency feedwater system generally penetrates containment. Electrical power is provided by essential ac distribution subsystem.

A turbine-driven pump is supplied steam from taps on the main steam lines. The emergency feedwater system is actuated by its own control system. Actuation may be initiated by a loss of ac power, a decrease in feedwater header pressure, a safety injection signal, low level in the steam generators, or a manual signal. During startup, the emergency feedwater system is used to increase steam generator pressure by drawing suction from the condensate storage tank. This provides enough steam to start the main feedwater pumps.

The emergency feedwater system consists of two motor-driven feedwater pumps and one steam turbine-driven feedwater pump. All three pumps are sized for 100% capacity; operation of only one pump is needed. All start on the actuation signal. The turbine-driven pump will operate as long as steam is available from the main steam lines and dc control power is available. The pump draws suction from two sources: the upper surge tank and the condenser hotwell. The pumps' discharge passes through a common header before entering the piping connected to the main feedwater lines. There is one emergency feedwater line for each main feedwater line. Flow control in each emergency feedwater line is established by a flow-control valve.

The following systems interface with the emergency feedwater system:

- main steam system,
- feedwater system,
- essential ac distribution system,
- dc power system (for pump control circuitry),
- engineered safety features actuation system,
- condensate system,
- condenser storage system,
- demineralized water system (makeup to the auxiliary feedwater storage tank), and
- instrument air system (for pneumatic valves).

3.2.4.2 Oconee I Functional Block Diagrams: Auxiliary Feedwater System

Figures 3.2.18 through 3.2.22 are the functional block diagrams for the auxiliary feedwater system. Information on emergency feedwater pump

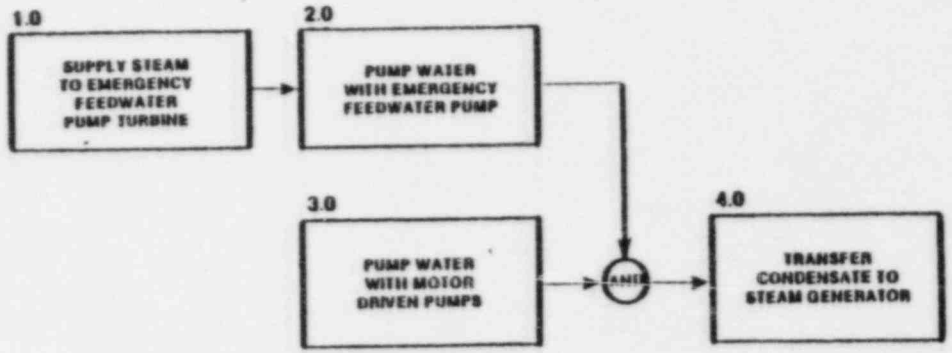


Fig. 3.18

AUXILIARY FEEDWATER SYSTEM TOP LEVEL

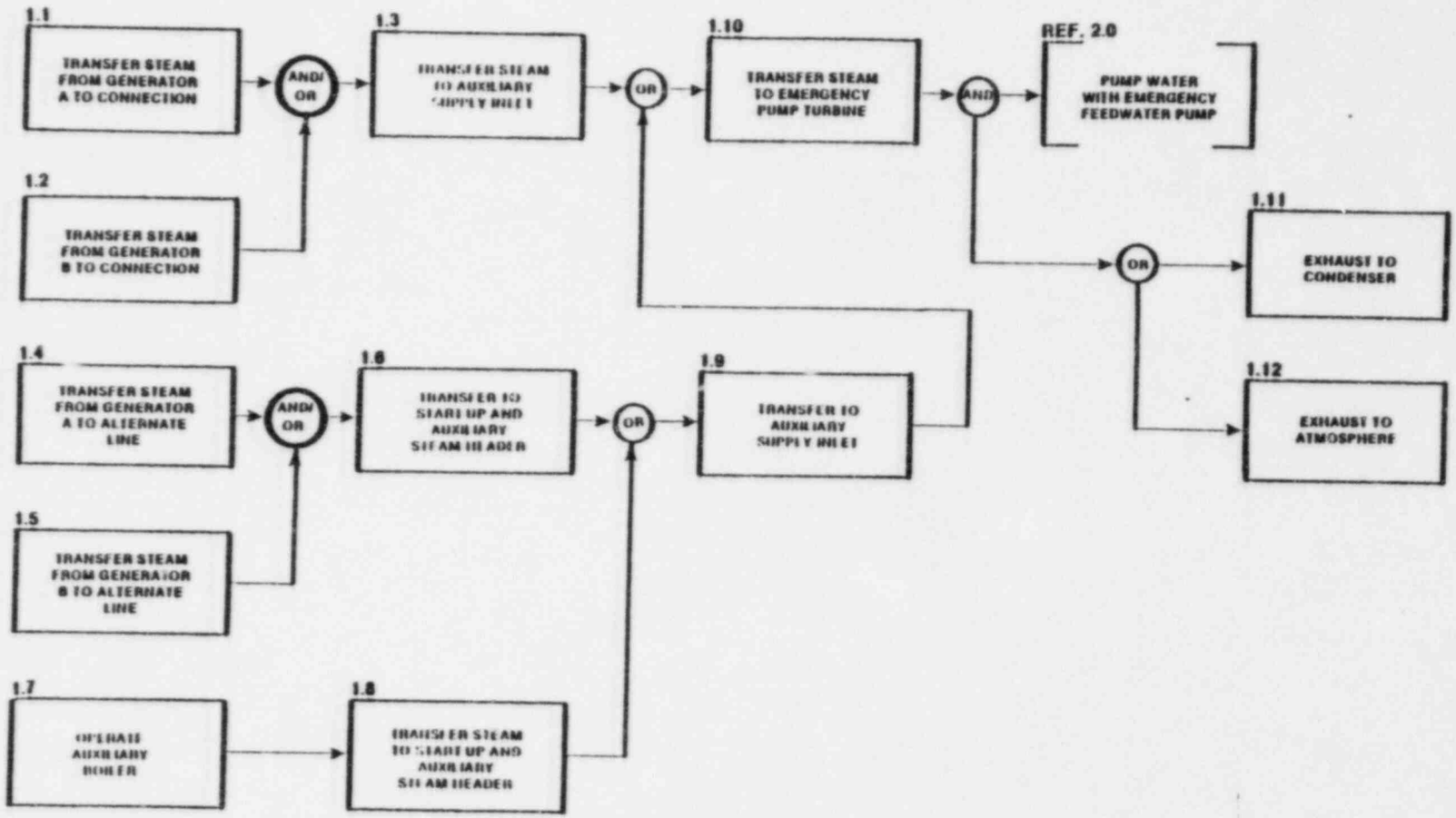


Fig. 3.19

AUXILIARY FEEDWATER SYSTEM
1.0
SUPPLY STEAM TO EMERGENCY
FEEDWATER PUMP TURBINE

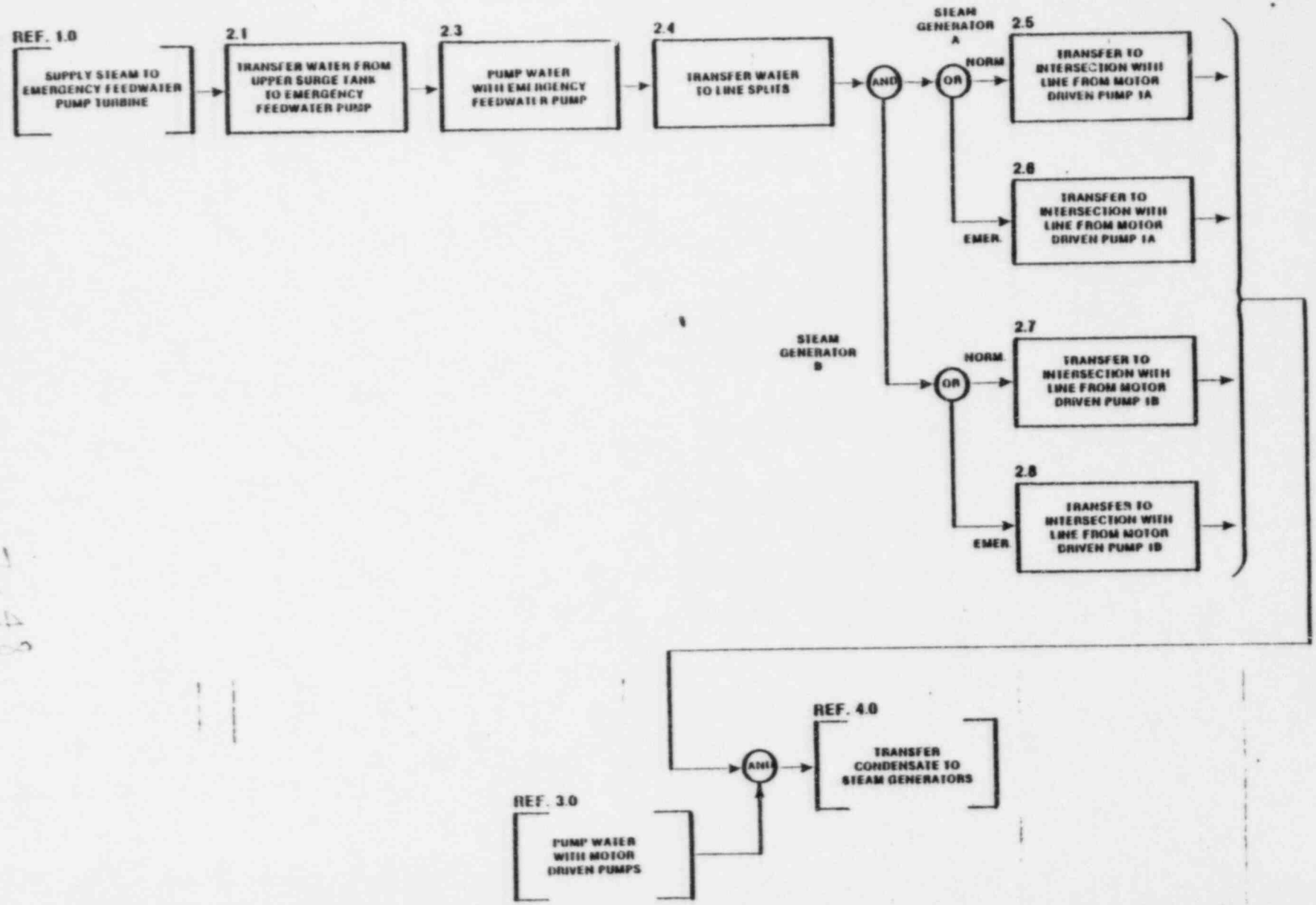


Fig. 3.20

AUXILIARY FEEDWATER SYSTEM
2.0
PUMP WATER WITH EMERGENCY FEEDWATER PUMPS

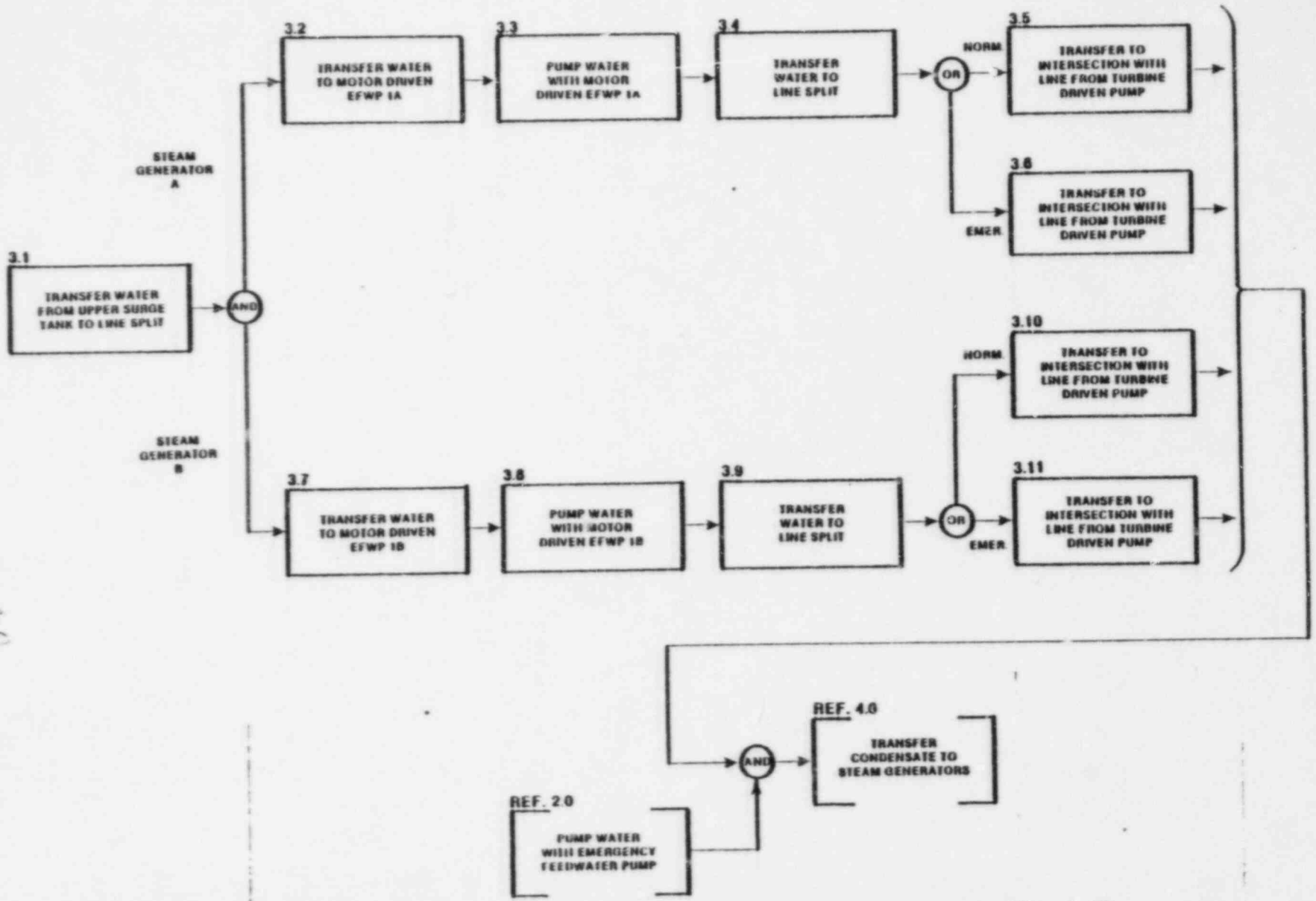


Fig. 3.21

AUXILIARY FEEDWATER SYSTEM
3.0
PUMP WATER WITH MOTOR DRIVEN PUMPS

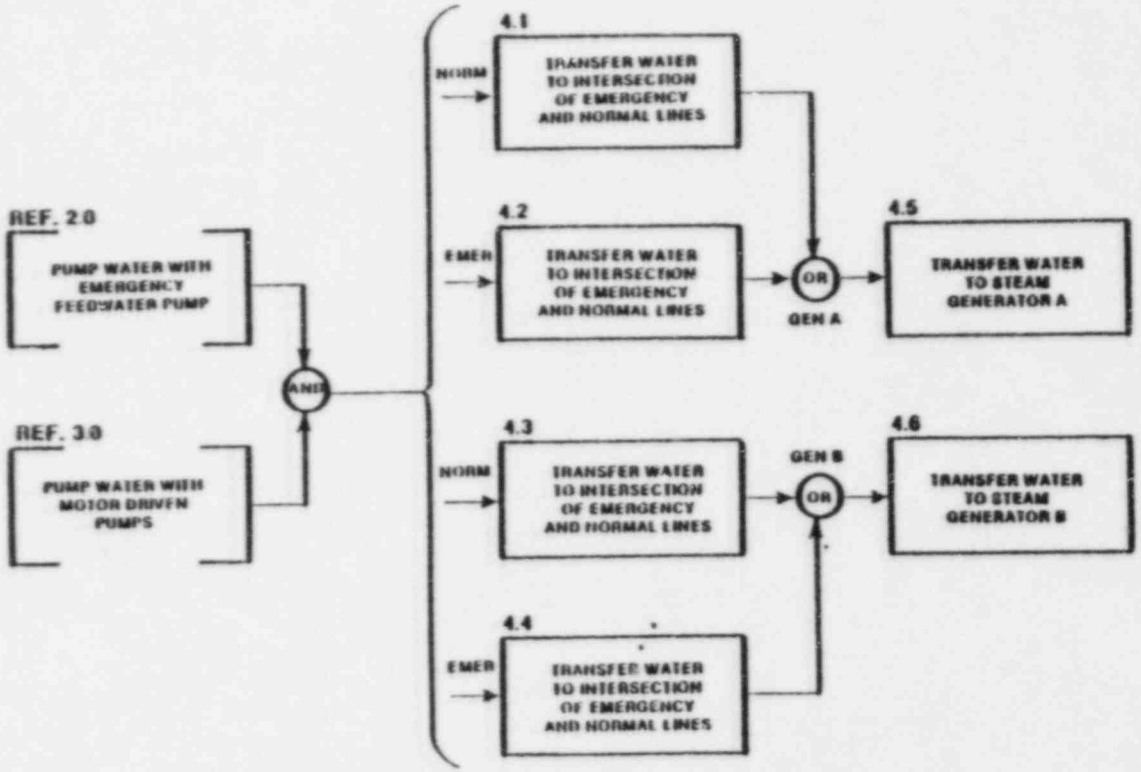


Fig. 3.22

AUXILIARY FEEDWATER SYSTEM
4.0
TRANSFER CONDENSATE TO STEAM GENERATORS

Table 3.2.4.1. FMEA: Auxiliary feedwater system

No.	Component	Failure mode	Effects and remarks
1.1	Line from steam generator A	Block	Little effect as steam generator B would be available. Should not result in reduced flow
		Break	Can be isolated, giving same effect as block. If not isolated, might result in steam generator A depressurization
1.2	Line from steam generator B	Block	Little effect as steam generator A would be available. Should not result in reduced flow
		Break	Can be isolated, giving same effect as block. If not isolated, might result in steam generator B depressurization
1.3	Line to auxiliary supply inlet	Block	Little effect as steam available from startup and auxiliary steam hands
		Break	Little effect if before check valve. If after, lose steam to emergency feedwater (EFW) pump turbine, and thus emergency feedwater pump. Still have motor driven EFW pumps
1.4	Line from steam generator A to alternate	Block	Little effect as steam available from steam generator B
		Break	If before check valve, steam available from steam generator B. If after check valve, no flow to startup and auxiliary steam header. Steam available from main steam lines, however. If not isolated, may cause steam generator depressurization
1.5	Line from steam generator B to alternate	Block	Little effect as steam available from steam generator A
		Break	If before check valve, steam available from steam generator A. If after check valve, no flow to startup and auxiliary steam header. Steam available from main steam lines, however. If not isolated, may cause steam generator depressurization
1.6	Line to startup and auxiliary header	Block/break	Check valve makes effect of break same as block: little effect as steam available from main steam lines

Table 3.2.4.1 (continued)

No.	Component	Failure mode	Effects and remarks
1.7.8	Auxiliary boiler	Block/break/ failure	Check valve makes all effects same: little effect as steam available from main steam lines or alternate steam lines
1.9	Auxiliary supply inlet	Block	Little effect as steam available from main steam lines
		Break	Little effect if before check valve. If after, lose steam to emergency feedwater pump turbine, and thus emergency feedwater pump. Still have motor-driven EFW pumps
1.10	Line to EFW pump turbine	Block	Lose steam to emergency feedwater pump turbine, and thus emergency feedwater pump. Still have motor driven EFW pumps
		Break	Same effect as block
1.11	Condenser exhaust	Block	Little effect as atmospheric exhaust available
		Break	No effect
1.12	Atmospheric exhaust	Block	Little effect as condenser exhaust available
		Break	No effect
2.1	Line to turbine driven EFW pump	Block	Lose feedwater flow from turbine-driven emergency feedwater pump. Still have flow from both motor-driven pumps
		Break	Lose feedwater flow from turbine-driven emergency feedwater pump. Still have flow from both motor-driven pumps. May drain pump. Assume this will not disrupt flow to motor-driven pumps
2.3	Turbine driven EFW pump	Failure	Lose feedwater flow from turbine driven emergency feedwater pump. Still have flow from both motor driven pumps
2.4	Discharge line from turbine driven EFW pump	Block/break	Check valves give break same effect as block; lose feedwater flow from turbine-driven emergency feedwater pump. Still have flow from both motor-driven pumps

Table 3.2.4.1 (continued)

No.	Component	Failure mode	Effects and remarks
2.5.6	Normal/emergency feed lines to steam generator A	Block/break to one of the lines	Little effect as alternate available
2.7.8	Normal/emergency feed lines to steam generator B	Block/break to one of the lines	Little effect as alternate available
3.1	Line to split	Block	Lose feedwater flow from both motor-driven pumps. Still have flow from turbine-driven pump
		Break	Lose feedwater flow from both motor driven pumps. Assume this will not disrupt flow to turbine-driven pump. May drain pumps
3.2	Line to motor-driven pump A	Block	Lose motor driven flow to steam generator A. Still have turbine-driven flow
		Break	Lose motor driven flow to steam generator A. Depending on location, may lose motor driven flow to steam generator B. May drain pump
3.3	Motor-driven pump 1A	Failure	Lose motor driven to steam generator A. Still have turbine driven flow
3.4	Line to split	Block/break	Check valves make effect of break same as block: lose motor-driven flow to steam generator A. Still have turbine-driven flow
3.5.6	Normal/emergency feed lines to steam generator A	Block/break to one of the lines	Little effect as alternate available
3.7	Line to motor-driven pump B	Block	Lose motor-driven flow to steam generator B. Still have turbine-driven flow
		Break	Lose motor-driven flow to steam generator B. Depending on location, may lose motor-driven flow to steam generator A. May drain pump

Table 3.2.4.1 (continued)

	Component	Failure mode	Effects and remarks
3.8	Motor-driven pump 1B	Failure	Lose motor-driven flow to steam generator B. Still have turbine-driven flow
3.9	Line to split	Block/break	Check valves make effect of break same as block: lose motor-driven flow to steam generator B. Still have turbine driven flow
3.10.11	Normal/emergency feed lines to steam generator B	Block/break to one of the lines	Little effect as alternate available
4.1.2	Normal/emergency feed lines to steam generator A	Block/break to one of the lines	Little effect as alternate available
4.5	Line to steam generator A	Block	Lose emergency flow to steam generator A. May result in dry generator
		Break	If before check valve, same effect as block. If after, could result in steam generator depressurization
4.3.4	Normal/emergency feed lines to steam generator B	Block/break to one of the lines	Little effect as alternate available
4.6	Line to steam generator B	Block	Lose emergency flow to steam generator B. May result in dry generator
		Break	If before check valve, same effect as block. If after, could result in steam generator depressurization

turbine steam supply was taken from Oconee FSAR Figure 10-3. The balance of the system was from drawing number PO-121D-1. Emergency feedwater was assumed available from the upper surge tank only.

3.2.4.3 Failure Mode and Effects Analysis for the Oconee I Auxiliary Feedwater System

3.2.5 High-Pressure Injection System

3.2.5.1 System Description: High-Pressure Injection System

The high-pressure injection system (HPIS) is designed to operate for small LOCAs when reactor coolant pressure has not been significantly reduced. In this circumstance, the HPIS injects borated water into the reactor coolant system to provide cooling to limit core damage and fission product release and to ensure an adequate shutdown margin. The HPIS is actuated by the Engineered Safety Features Actuation System (ESFAS) and is powered electrically by the essential ac distribution subsystem. The HPIS is a Safety Class 2 system.

The HPIS has three redundant trains. A typical train consists of a high head pump, which draws suction from the borated water storage or volume control tank. All pumps are started upon an initiation signal. The pump discharge flows into the cold legs of each reactor coolant loop.

The HPIS interfaces with the following systems:

- engineered safety features actuation system,
- essential ac distribution subsystem,
- dc power system (for pump and valve control circuitry),
- chemical and volume control system or the refueling system, and
- residual heat removal/low-pressure injection system (for alternate suction).

3.2.5.2 Oconee I Functional Block Diagrams: High-Pressure Injection System

Figures 3.2.23 and 3.2.24 are the functional block diagrams for the high-pressure injection system. The information was taken from drawing number PO-101-A-2 and Oconee FSAR Figure 9-2. For high-pressure safety injection, water is assumed to come from the borated water storage tank, thus in this analysis the pumps are not used as part of the chemical and volume control system.

3.2.5.3 Failure Mode and Effects Analysis for the Oconee I High-Pressure Injection System

3.2.6 Residual Heat Removal/Low-Pressure Injection System

3.2.6.1 System Description: Residual Heat Removal/Low-Pressure Injection System

The residual heat removal/low-pressure injection (RHR/LPI) system performs several functions during the various states of reactor

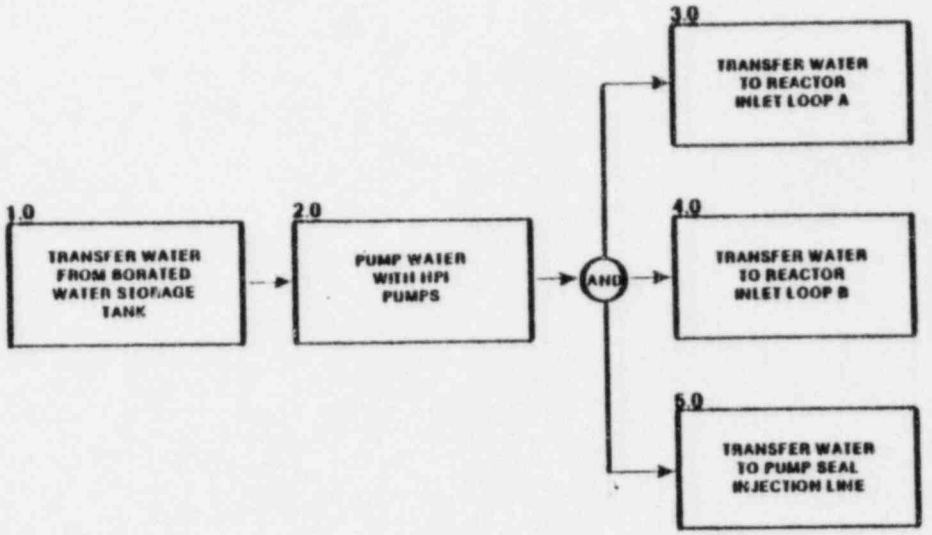


Fig. 3.23

HIGH PRESSURE INJECTION SYSTEM TOP LEVEL

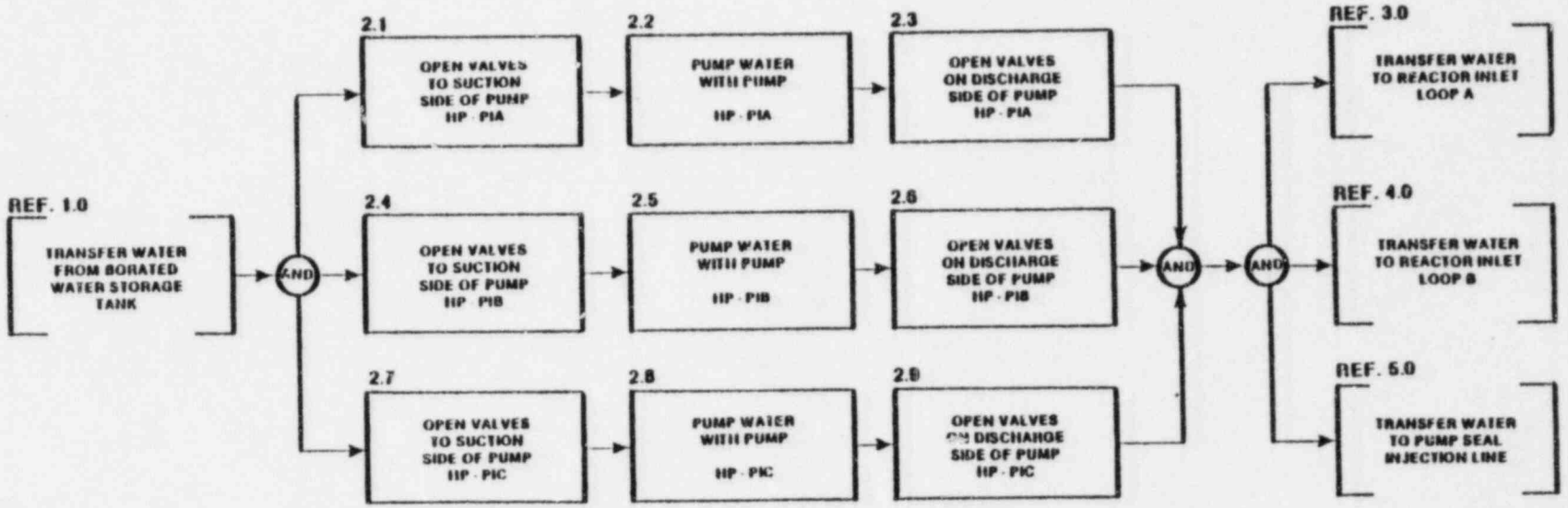


Fig. 3.24

HIGH PRESSURE INJECTION SYSTEM
2.0
PUMP WATER WITH HPI PUMPS

Table 3.2.5.1. FMEA: High-pressure injection system

No.	Component	Failure mode	Effects and remarks
1.0	Line from borated water storage tank	Block	Lose flow from borated water storage tank. Results in loss of high-pressure safety injection capability requiring reactor shutdown
		Break	Check valve gives same effect as block
2.1-3	Pump HP-P1A line	Block/break/ pump failure	Check valves make all effects the same: lose pump HP-P1A line. Two others available
2.4-6	Pump HP-P1B line	Block/break/ pump failure	Check valves make all effects the same: lose pump HP-P1B line. Two others available
2.7-9	Pump HP-P1C line	Block/break/ pump failure	Check valves make all effects the same: lose pump HP-P1C line. Two others available
3.0	Line to reactor inlet loop A	Block	Lose high-pressure injection into reactor inlet loop A. Still have high-pressure injection into reactor inlet loop B
		Break	Check valve gives same effect as block
4.0	Line to reactor inlet loop B	Block	Lose high-pressure injection into reactor inlet loop B. Still have high-pressure injection into reactor inlet loop A
		Break	Check valve gives same effect as block
5.0	Line to pump seals	Block	Lose flow to pump seals, possibly lose primary coolant loop pumps. Requires reactor shutdown
		Break	Can be isolated. Gives same effect as block

operation. Its primary function is to remove heat from the reactor core during normal shutdown, loss-of-coolant accident (LOCA), and post-LOCA conditions. For additional information see Appendix A.

For Oconee, each train of the two-train design has 100% capacity and is redundant to the other train. Each train consists of a pump and a heat exchanger with their associated valves.

During a normal shutdown, valve alignment directs flow from the reactor coolant system hot leg through the RHR pumps and heat exchangers into the reactor vessel. Following a large LOCA, the LPI system goes into a coolant injection mode when reactor vessel pressure gets below 200 psig or the reactor building pressure gets above 4 psig. In this case, valve alignment directs suction from the borated water storage tank through the pumps, heat exchangers, and piping to the reactor vessel. When the water level in the borated water storage tank falls to 6% height, suction is changed over to the containment sump, and the storage tank is usually valved out to prevent pump cavitation. This phase of operation is known as the recirculation mode.

3.2.6.2 Oconee I Functional Block Diagrams: Low-Pressure Injection System

Figure 3.2.25 through 3.2.29 are the functional block diagrams for the LPI system. The information was taken from drawing number PO-102 A-2 and Oconee FSAR Figure 9-6. This information also covers the residual heat removal function.

3.2.6.3 Failure Mode and Effects Analysis for the Oconee I Low-Pressure Injection System

3.2.7 Containment Spray System

3.2.7.1 System Description: Containment Spray System

The containment spray system (called reactor building spray system by Oconee) provides a water spray to the containment following a LOCA or steam line break to limit containment pressure and to minimize the release of radioactive iodine and particulates to the environment. For additional information see Appendix A.

The reactor building spray system is a two-train system which draws suction first from the borated water storage tank, then the emergency sump. Each of the two piping trains has a reactor building spray pump which discharges into a spray header inside the containment. The occurrence of high (about 4 psig) reactor building pressure causes the engineered safety features actuation system (ESFAS) to actuate containment spray.

3.2.7.2 Oconee I Functional Block Diagrams: Containment Spray System

Figure 3.2.30 shows the Functional Block Diagrams for the containment spray system. The information came from Oconee FSAR Figure 6-3. Water

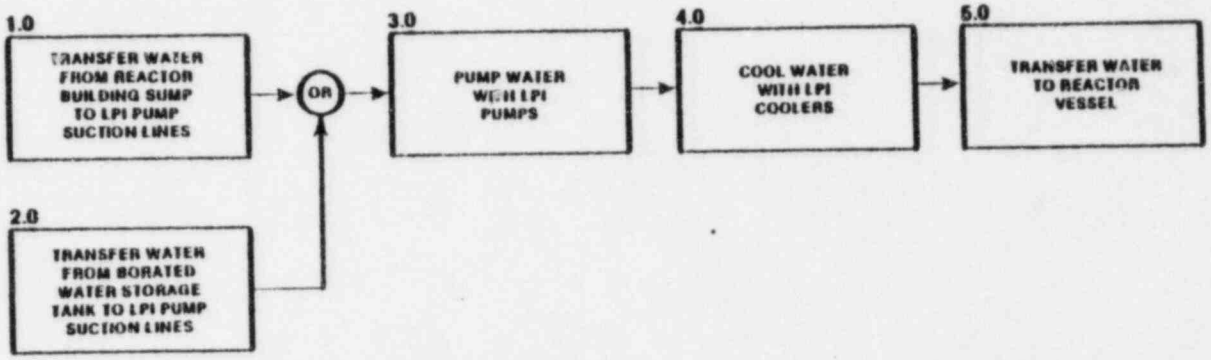
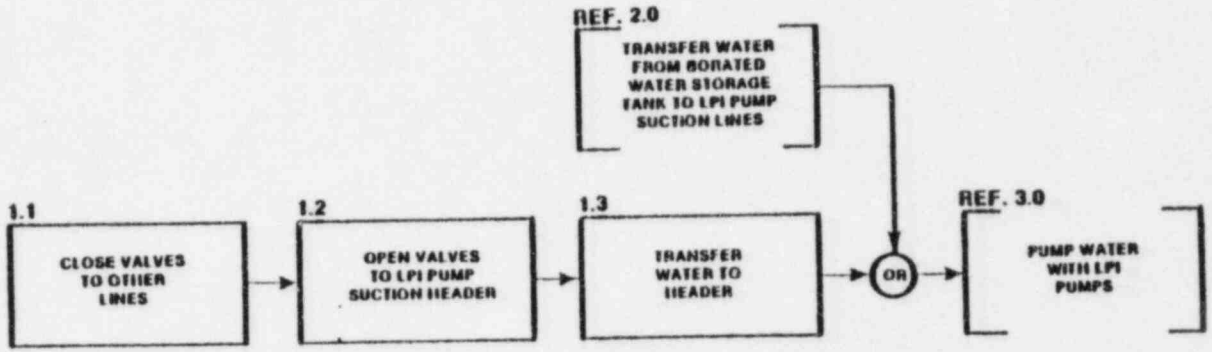


Fig. 3.25
LOW PRESSURE INJECTION SYSTEM TOP LEVEL



NOTE: TWO PARALLEL LINES.

Fig. 3.26

LOW PRESSURE INJECTION SYSTEM 1.0 TRANSFER WATER FROM REACTOR BUILDING SUMP TO LPI PUMP SUCTION LINES

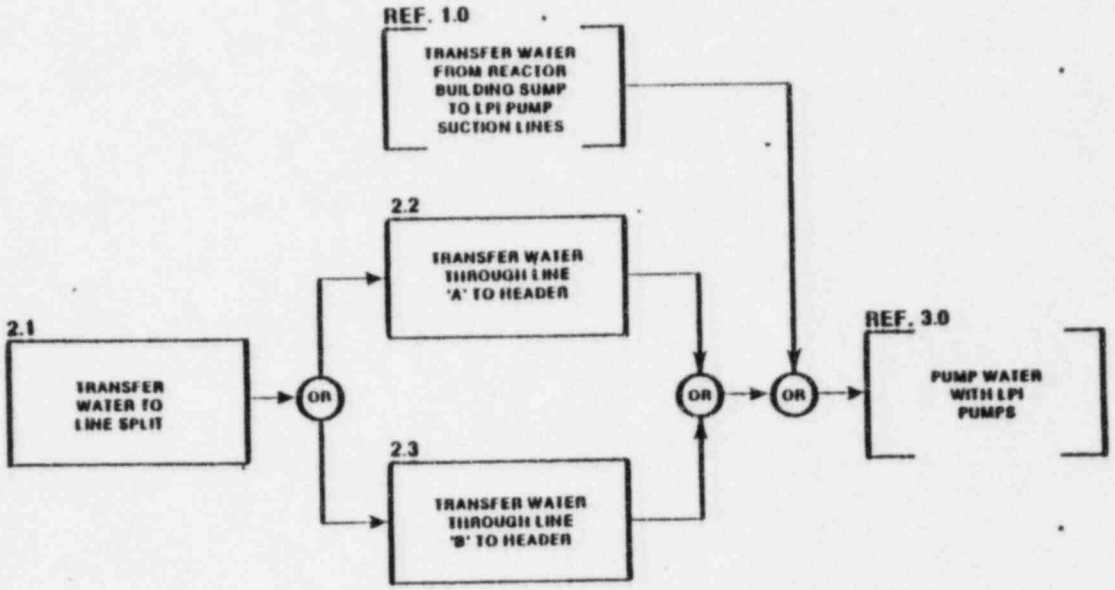
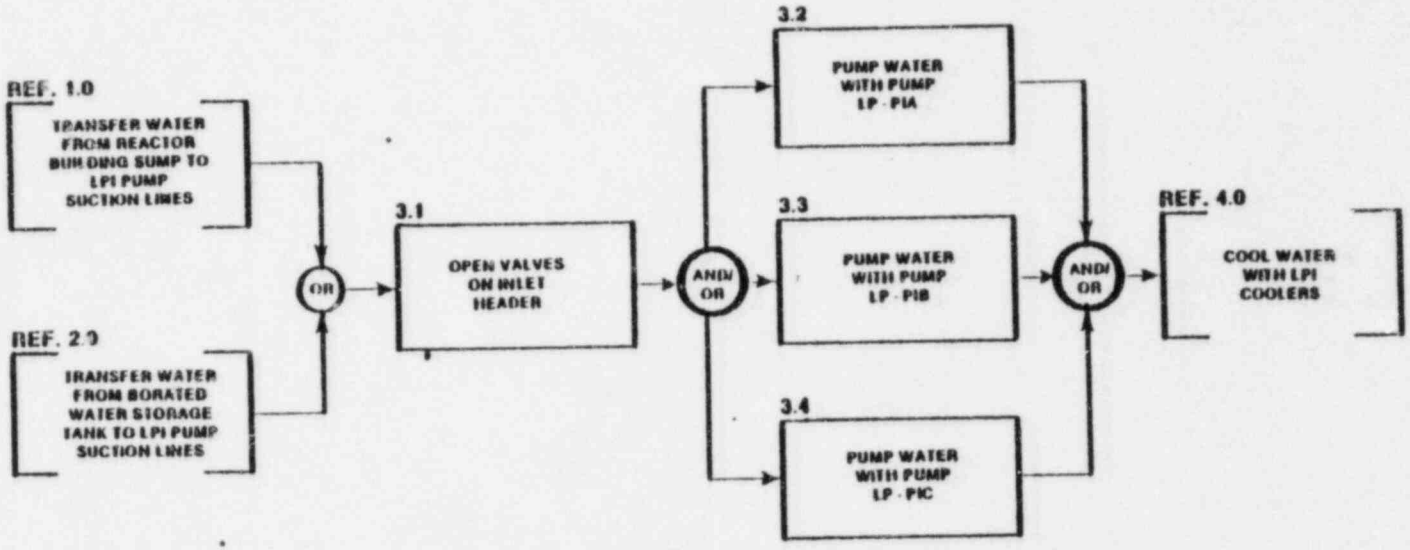


Fig. 3.27

LOW PRESSURE INJECTION SYSTEM 2.0 TRANSFER WATER FROM BORATED WATER STORAGE TANK TO LPI PUMP SUCTION LINES



NOTE: TWO OUT OF THREE PUMPS REQUIRED.

Fig. 3.28

LOW PRESSURE INJECTION SYSTEM 3.0 PUMP WATER WITH LPI PUMPS

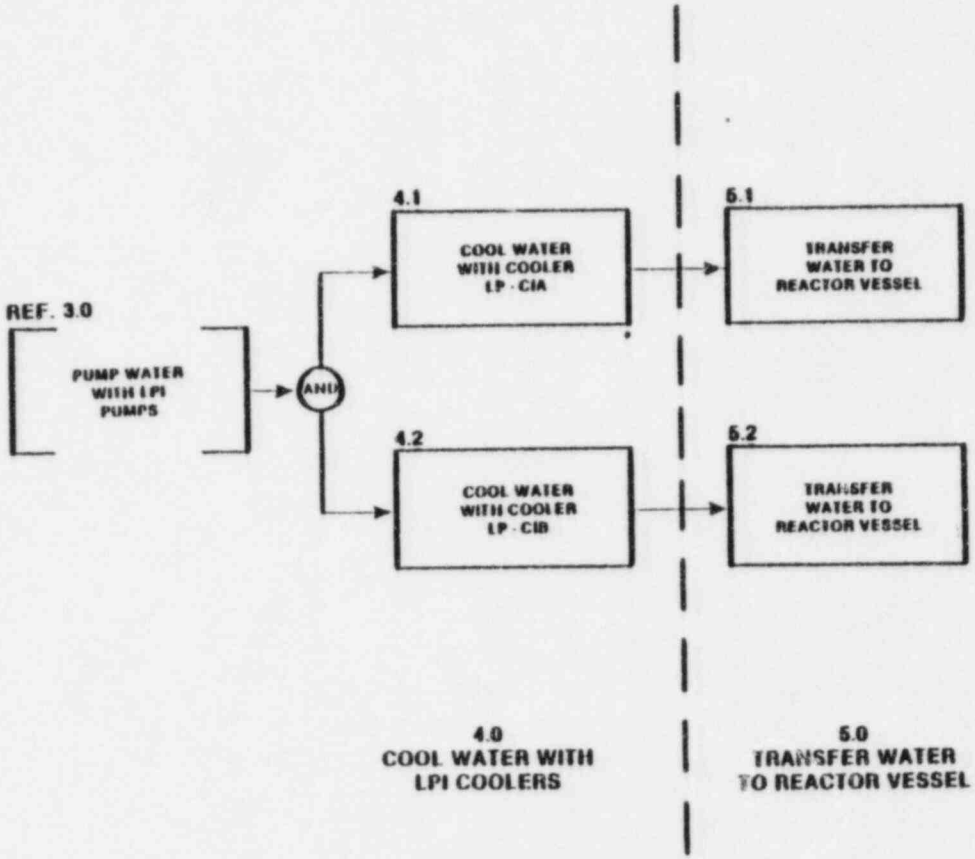
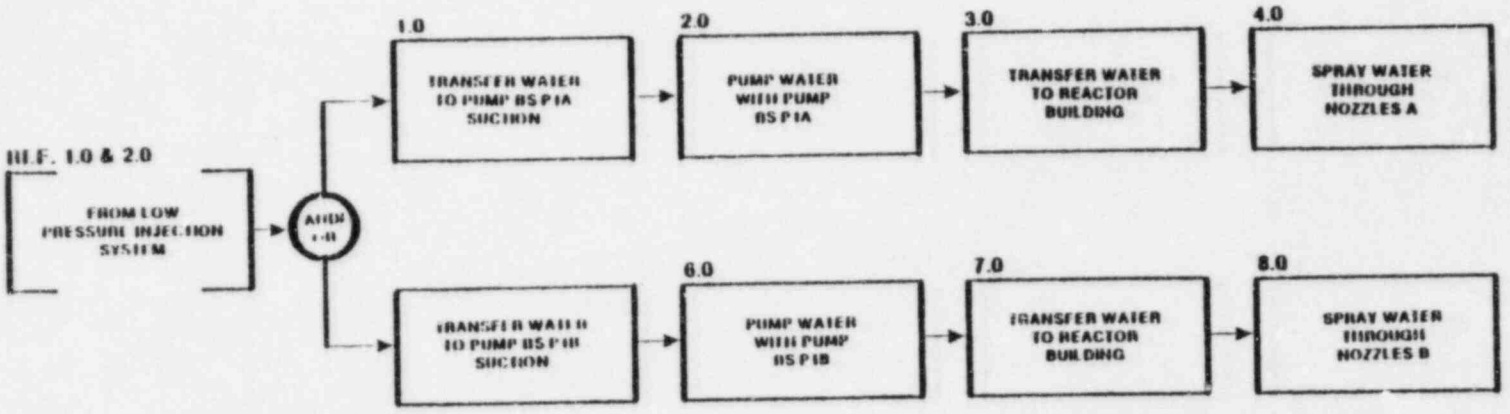


Fig. 3.29

LOW PRESSURE INJECTION SYSTEM 4.0 & 5.0

Table 3.2.6.1. FMEA: Low-pressure injection system

No.	Component	Failure mode	Effects and remarks
1.1-1.3	Line to LPI pump suction header	Block	Lose flow through that line. Alternate is available, with capacity of full flow
		Break	Valves can isolate break, giving same effect as block. If after last valve in line to "C" pump, lose that pump, but alternate available
		Other lines not closed off	Same as break or block
2.1	Line from BWSI	Block	Lose flow from borated water storage tank (BWST). Water available from pump line
		Break	Check valves isolate break, giving same effect as block
2.2.3	Parallel lines to LPI pump suction header	Block	Little effect, as alternate is available
		Break	Can be isolated, giving same effect as block. If in line B, lose pump LP-PIC, but have two left
3.1-3.4	Three parallel pump lines	Block	Lose use of one pump, but have two left (little effect)
		Break	For single-failure condition, can be isolated giving same effect as block
		Pump failure	Lose pump, but have two left (little effect)
4.1.2	Parallel cooler lines	Block	Have alternate line, but probably reduced flow. Possible inadequate core cooling
		Break	Can be isolated, giving same effect as block
		Cooler failure	Possibly inadequate core cooling
5.1.2	Parallel lines to reactor vessel	Block	Have alternate line, but probably reduced flow. Possibly inadequate core cooling
		Break	Check valves give same effect as block



NOTE: WATER IS TAKEN FROM LPI PUMP SUCTION HEADER. THIS COMES INITIALLY FROM THE BORATED WATER STORAGE TANK, THEN FROM THE REACTOR BUILDING SUMP.

Fig. 3.30

CONTAINMENT SPRAY SYSTEM TOP LEVEL

is supplied to this system from the low-pressure injection pump suction header.

3.2.7.3 Failure Mode and Effects Analysis for the Oconee I Containment Spray System

3.2.8 Low-Pressure Service Water System

3.2.8.1 System Description: Low-Pressure Service Water System

Reactor Building Service Water System

The reactor building service water system provides an intermediate cooling loop for removing heat from the engineered safety systems and transferring it to the essential service water system. The reactor building cooling water system is designated as Safety Class 3 and is subdivided into two distinct trains. Electric power for each train is provided through separate 4160-V emergency buses. The reactor building cooling water system penetrates containment.

A train of the reactor building cooling water system shares (with Oconee Unit 2), three 15,000 gal/min pumps and their associated motors connected in series with a heat exchanger for transferring heat to the essential service water system and several parallel 24-in. piping legs which connect to the various engineered safety systems.

Systems which interface with the reactor building cooling water system are shown in Appendix A.

Turbine Building Service Water System

The turbine building service water system provides an intermediate cooling loop for removing heat from components located inside the turbine and auxiliary buildings and transferring it to the nonessential service water system.

The turbine building cooling water system uses the same 15,000 gal/min pumps as the reactor building cooling water system. Pump discharge flows through the tube side of a turbine building cooling water heat exchanger before entering a common header. Several parallel piping legs leave the header and pass through the shell side of various heat exchangers. For additional information see Appendix A.

3.2.8.2 Oconee I Functional Block Diagrams: Low-Pressure Service Water System

Figures 3.2.31 through 3.2.37 are the functional block diagrams for the low-pressure service water system. The information was taken from Oconee FSAR Figures 6-10, 9-4, 9-8, and 9-9. This system includes both the reactor building cooling units and the low-pressure injection coolers.

3.2.8 Failure Mode and Effects Analysis for the Oconee I Low-Pressure Service Water System

Table 3.2.7.1. FMEA: Containment spray system

No.	Component	Failure mode	Effects and remarks
1.0-3.0	Line, Pump A	Block	Lose flow to half the 240 nozzles. The other half are available, may be adequate
		Break	Can be isolated, giving same effect as block
		Pump failure	Same effect as block
4.0,8.0	Nozzles	Failure of one	Insignificant impact, as 239 more are available
5.01-7.0	Line, Pump B	Block	Lose flow to half the 240 nozzles. The other half are available, may be adequate
		Break	Can be isolated, giving same effect as block
		Pump failure	Same effect as block

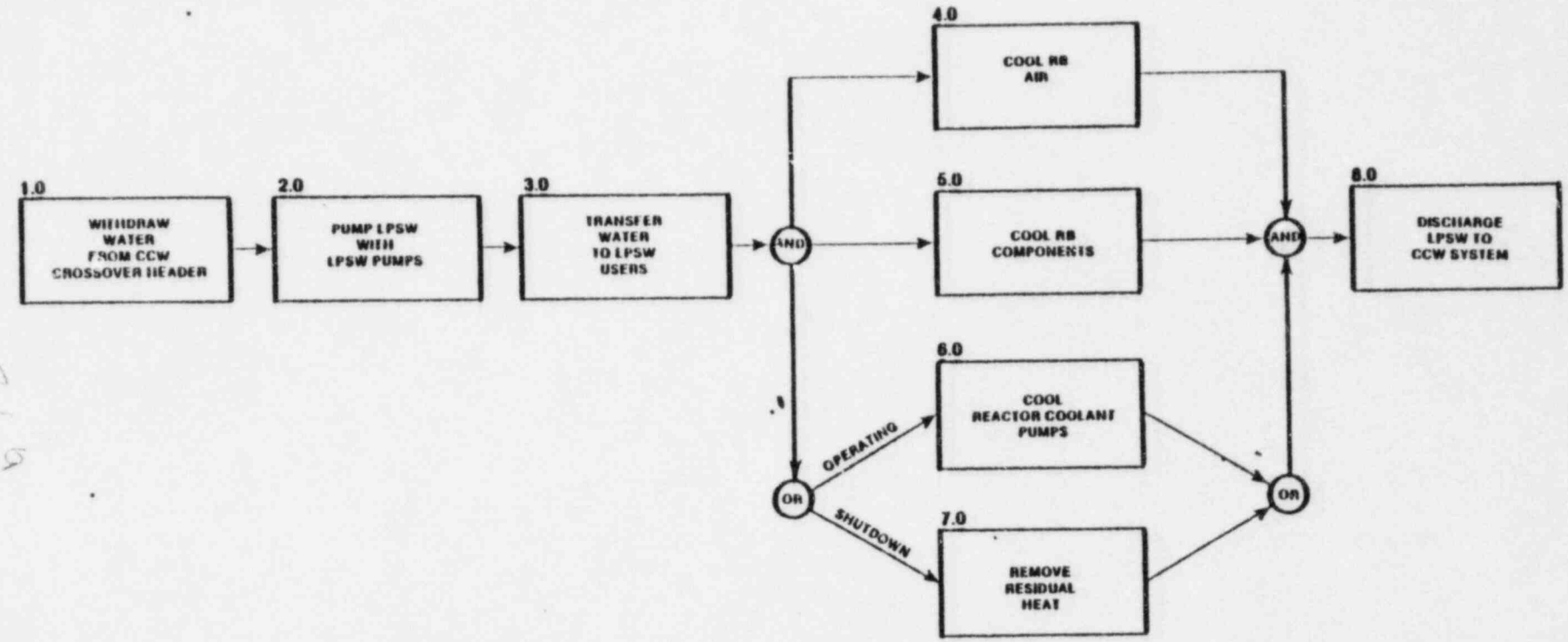


Fig. 3.31

LOW PRESSURE SERVICE WATER SYSTEM TOP LEVEL

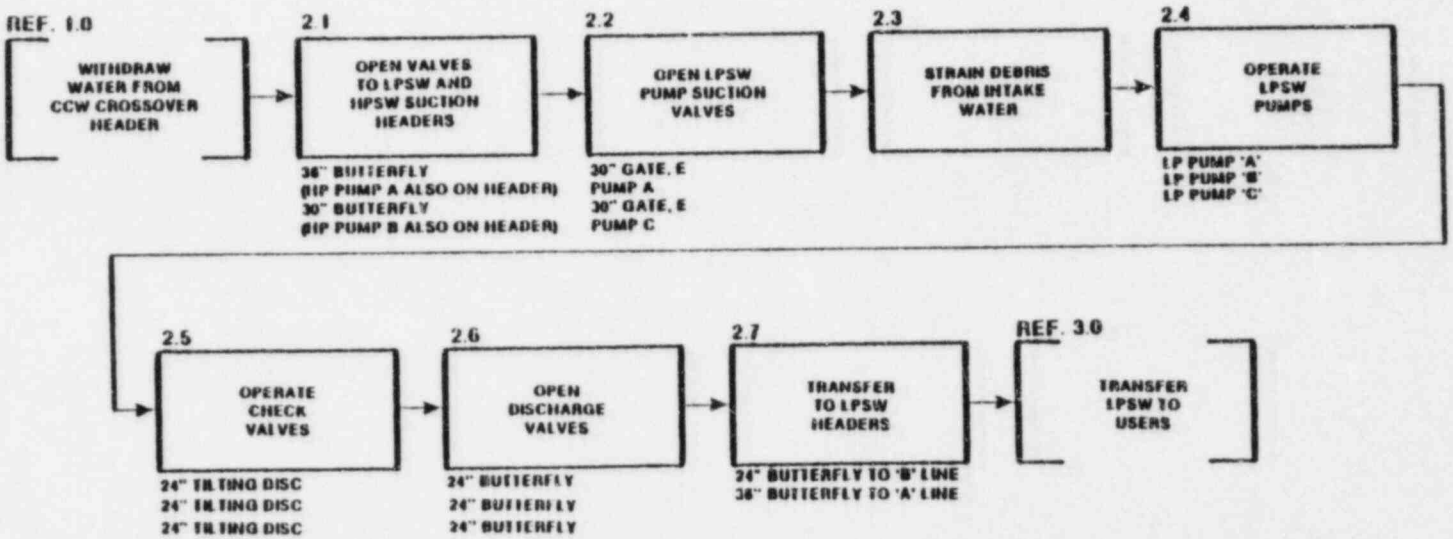


Fig. 3.32

LOW PRESSURE SERVICE WATER SYSTEM 2.0 PUMP LPSW WITH LPSW PUMPS

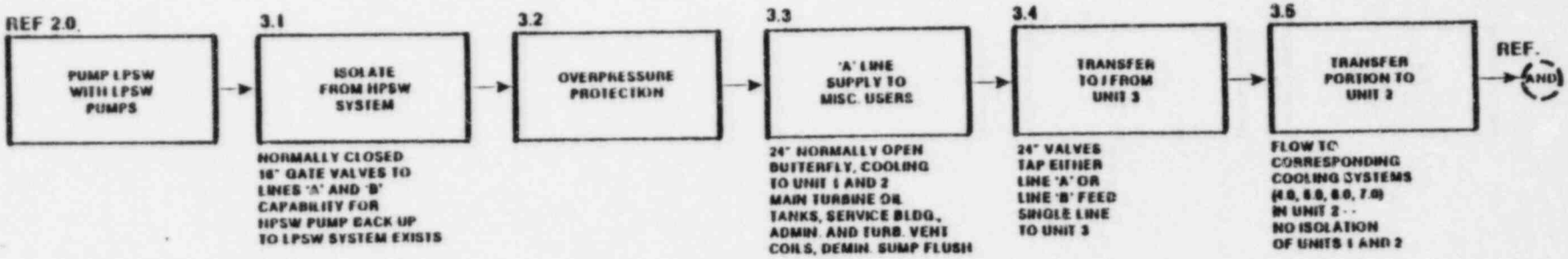


Fig. 3.33

LOW PRESSURE SERVICE WATER SYSTEM 3.0 TRANSFER WATER TO LPSW USERS

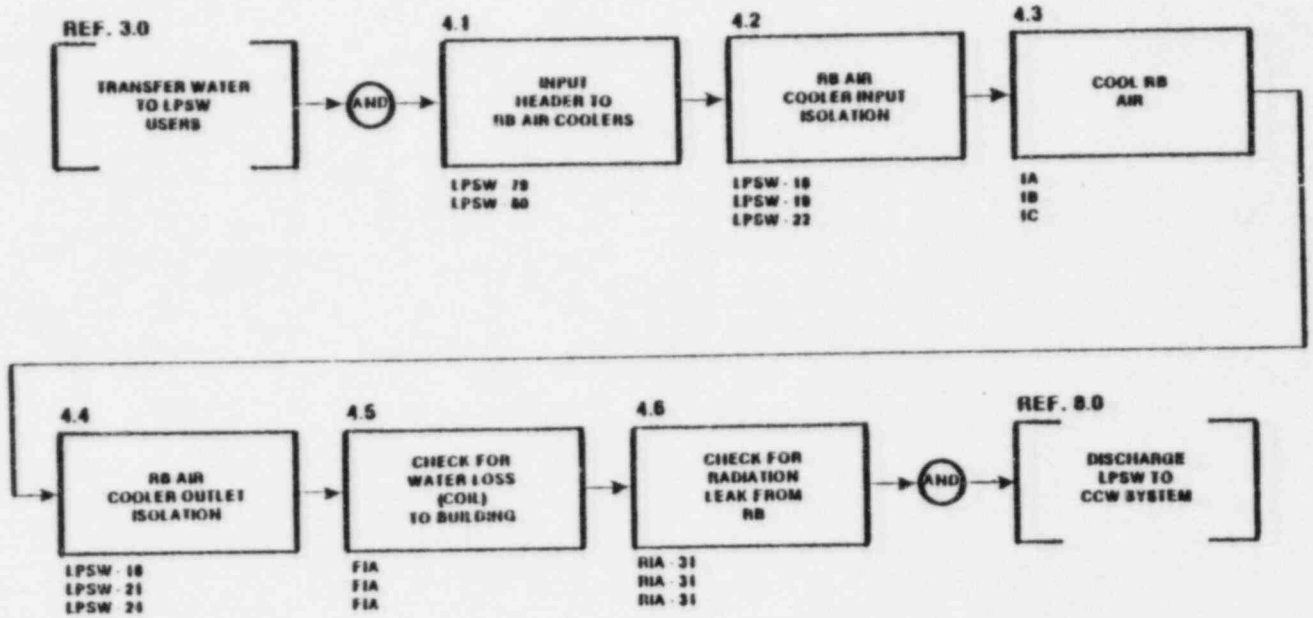


Fig. 3.34

LOW PRESSURE SERVICE WATER SYSTEM 4.0 COOL REACTOR BUILDING AIR

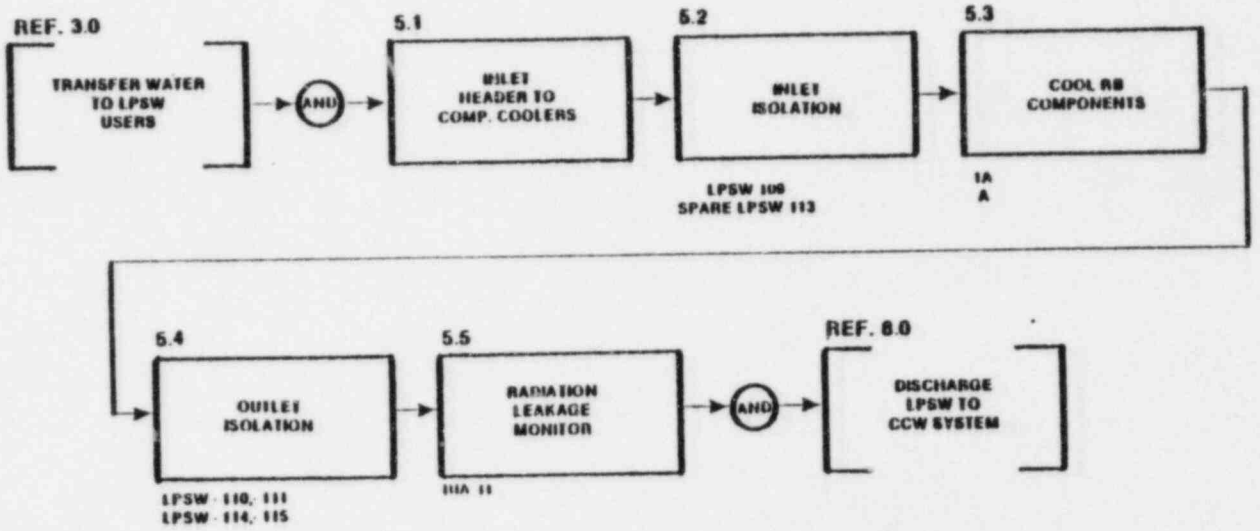


Fig. 3.35

LOW PRESSURE SERVICE WATER SYSTEM 5.0 COOL REACTOR BUILDING COMPONENTS

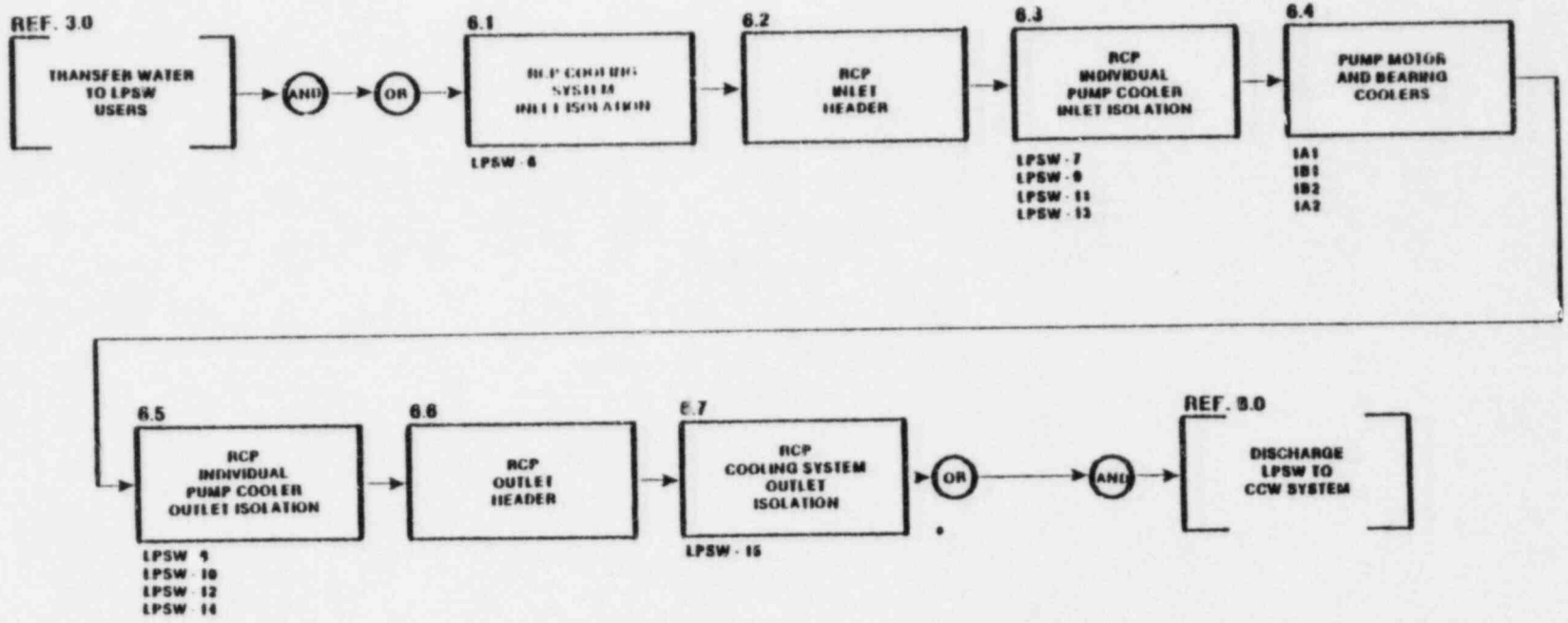


Fig. 3.36

LOW PRESSURE SERVICE WATER SYSTEM
6.0
COOL REACTOR COOLANT PUMPS

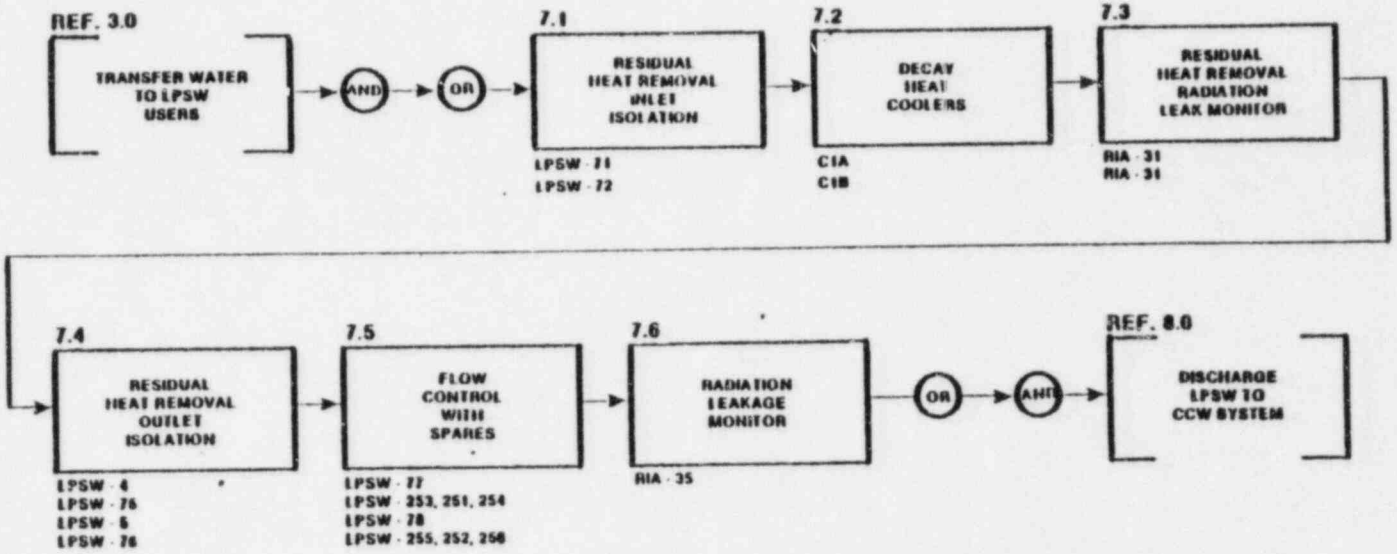


Fig. 3.37

LOW PRESSURE SERVICE WATER SYSTEM 7.0 REMOVE RESIDUAL HEAT

Table 3.2.8.1. FMEA: Low-pressure service water system

No.	Component	Failure mode	Effects and remarks
2.1	Suction header valves (2 headers)	Block Break	Reduced cooling water flow. HPSW and Unit 3 LPSW transfers can make up difference
2.2	Pump suction valves (3 parallel pumps)	Block	Loss of pump flow. May be offset by spare capacity, HPSW and Unit 3 LPSW transfers
		Break	Loss of pump flow. Possible interference with other pump(s) on header. Spare capacity available
2.3	Strainer (3 parallel pumps)	Plug	No effect. Spare pumping capacity available unless simultaneous plugs occur in all pumps
		Fail (pass objects)	Debris may damage or plug downstream components, extent unknown
2.4	Low-pressure service water pumps (3 parallel)	Fail	No effect, spare available
2.5	Pump discharge check valves (3 parallel)	Block	No effect. Spare pumping capacity available
		Fail open	None unless associated pump fails or is turned off. Resulting back flow through pump will reduce pressure and water flow to LPSW users. However, valve can be isolated by closing discharge valve
2.6	Pump discharge valves	Break	Loss of flow to "A" line ("B" pump discharge valve break) or to "B" line ("A" pump discharge valve break). Resulting loss of cooling may force shutdown or result in turbine and/or reactor trips due to component overheating
		Block	No effect, spare available

Table 3.2.8.1 (continued)

No.	Component	Failure mode	Effects and remarks
2.7	LPSW pump discharge header with valves	Break	Loss of flow to "A" line ("B" pump discharge valve break) or to "B" line ("A" pump discharge valve break). Resulting loss of cooling may force shutdown or result in turbine and/or reactor trips due to component overheating
		Valve block	Inability to switch pump C between LPSW lines "A" and "B" (i.e., loss of redundant pumping capacity)
3.1	HPSW isolation valves (2)	Block	Loss of redundant pumping capacity
		Break	Potential flooding of pump room. Loss of coolant flow as in discharge valve break
3.2	Pressure relief valves	Allow high pressures	Could burst cooling coils in reactor building causing flow into sump. Could burst oil cooler coils causing water contamination of turbine oil or RCP bearing oil. Pipe break not likely
		Leak or fail at low pressure	Reduce cooling water flow, extent unknown
3.3	Valve and line from "A" line to miscellaneous coolers	Block	Loss of cooling to turbine oil eventually causing turbine trip
		Break	Loss of cooling to turbine oil as above. Loss of cooling water flow in line "A"
3.4	Isolation valves and lines to Unit 3	Block	No effect on Unit 1
		Valve break	Loss of cooling water flow from line containing broken valve
		Break	Loss of cooling water flow
3.5	Headers to Unit 2	Break	Loss of cooling water flow

Table 3.2.8.1 (continued)

No.	Component	Failure mode	Effects and remarks
4.1	Input headers to RB air coolers (with 2 valves)	Break	Loss of some cooling water flow. Header valves allow isolation of 2 of 3 coolers from site of leak for continued operation
		Block	No effect unless both header valves blocked causing loss of flow to cooler 1B
4.2	RB cooler inlet isolation valves (3 parallel)	Block	Loss of flow to cooler but other two coolers still operable
		Break	Loss of cooling water flow. Leakage to turbine room sump. Loss of cooler
		Fail open	No control of cooler. Would cause water accumulation in reactor building sump in case of cooling coil failure
4.3	RB air cooling coil (3 parallel)	Block	Loss of cooler, other two coolers compensate
		Break	Loss of water to reactor sump
4.4	RB cooler outlet isolation valves (3 parallel)	Block	Loss of cooler
		Break	Loss of water to turbine building sump, no effect on cooling system performance
		Fail open	If pressure head sufficient, may allow backflow into RB sump through ruptured RB cooler coil during attempts at cooler isolation
4.5	Flow monitors (RB air cooler water flow) (3 parallel)	False indication of leak	Unnecessary isolation of RB air cooler
		Failure to detect leak	Uncontrolled loss of LPSW to RB sump. Liquid detector in RB sump is backup
4.6	Radiation monitors (3 parallel)	False indication of leak	Unnecessary isolation of RB air cooler

Table 3.2.8.1 (continued)

No.	Component	Failure mode	Effects and remarks
		Failure to detect leak	Uncontrolled loss of FP gases, etc., to CCW. (Accident conditions only.)
5.1	Component cooler header	Break	Loss of water flow to component coolers (affecting RC pump seal water return and letdown coolers). Decreased flow and pressure to other coolers on line "B"
5.2	Inlet isolation valve (2 parallel)	Block	Loss of component cooler function, spare provided
		Break	Loss of water flow to component coolers (affecting RC pump seal water return and letdown coolers). Decreased flow and pressure to other coolers on line "B"
5.3	Component cooler (1 active, 1 spare)	Block	Loss of cooler function. Spare provided
		Leak	Cooler may be isolated. Spare provided
5.4	Outlet isolation	Block	Loss of cooler function. Spare provided
		Break	Leakage to turbine building sump
5.5	Radia[illegible]onitor	False indication of leak	No effect. Sample valve allows verification
		Failure to detect leak	Release of radiation to CCW. May be discovered by regular sampling
6.1	RCP cooler inlet isolation valve	Block	All RCPs overheat, reactor trips
		Break	Same with water loss to turbine building sump

Table 3.2.8.1 (continued)

No.	Component	Failure mode	Effects and remarks
6.2	RCP inlet header	Break	All RCPs overheat, reactor trips
		Leak	Near normal cooling achieved but water is lost to RB sump
6.3	Pump cooler inlet isolation valve (4 parallel pumps)	Block	Individual RCP overheats, trips. Reactor runback
		Break	Same as block except water is lost to RB sump
6.4	Pump motor and bearing coolers (4 parallel pumps)	Block	Individual RCP overheats, trips
		Leak	Water contamination of oil and air in pumps
6.5	Pump cooler outlet isolation valve (4 parallel pumps)	Block	Individual RCP overheats, trips. Reactor runback
		Break	Undetected low-pressure leak to RB sump
6.6	RCP cooler outlet header	Break	Undetected low-pressure leak to RB sump
		Leak	Undetected low-pressure leak to RB sump
6.7	RCP cooler outlet isolation valve	Block	All RCLPs overheat, reactor trips
		Break	Same with water loss to turbine building sump
7.1	Residual heat removal inlet isolation (2 parallel valves)	Block	Loss of cooler function. May allow reheating of RCS at low pressure
		Break	Loss of cooler function and cooling water flow and pressure to other coolers. Leakage to turbine building sump. May allow reheating of RCS at low pressure

Table 3.2.8.1 (continued)

No.	Component	Failure mode	Effects and remarks
7.2	Residual heat removal coolers (2 in parallel)	Block	Loss of cooler function. May allow reheating of RCS at low pressure
		Leak (tube failure)	Radioactive RC water enters LPSW system
7.3	Radiation monitor (2 in parallel)	False indication of leak	Unnecessary isolation of cooler causing RCS rehea ing
		Failure to detect leak	Downstream radiation monitor backs up unit
7.4	Outlet isolation valves (2 parallel strings of an EOV followed by a check valve)	Block (fail closed)	Loss of cooler function. May allow reheating of RCS at low pressure
		Break	Loss of cooler control. Leakage to turbine building sump
		Fail open	No effect, flow control valves can isolate system
7.5	Water flow control valves (2 parallel valves per outlet line)	Fail open	Overcool, RCS at low pressure
		Fail low flow	No effect, spare valve available
7.6	Radiation monitor	Fails	No effect backup monitors provided upstream

3.2.9 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 differential pressure ("water level") is sensed below low level, (30 in. on the selected A-D (A'-D') sensor - see Fig. A.2.3). Between 30 in. and 344 in. control is not based on level during normal operations. A complex of demand-related signals is met by the control system. 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 344 in. the ICS sends a signal to close the MFW control valve. If despite this the differential pressure level rises to 359 in. a signal is sent by circuitry outside the ICS (see Fig. A.2.4) 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 App. A.2.2.2 and A.2.2.3.)

It is apparent, therefore, that the MFW cannot overfill a steam generator (above the 359" 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 (Sect. 3.2.9.1).

Note that a number of SG overfeeds would reduce steam quality to the point where water enters the steam line even though the differential pressure on A-D did not cause either high level control or high level pump trip. However, for significant accumulation it is necessary to defeat the two high level protection devices.

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.

3.2.9.1 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 A.2.2.2, b

b. Failure of valve V (Fig. A.2.3) of the selected set in the closed position during operation A.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 A.2.2.2, d

Further description of these failures appears in App. A.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. A.2.4) to fail with contacts open places SG-A pump trip in undetected failed state. Analogously, 2B and 3B for SG-B. A.2.2.3, a

b. Any failure causing relay FPTX (Fig. A.2.4) to fail with contacts open will put trip signals of both SGs in undetected failed state. A.2.2.3, b

c. A sufficient leak in nonselected pressure tap B (B') or its connecting sense line or packing of either blocking valve on which the connecting line terminates A.2.2.2,b

d. Failure of valve V (Fig. A.2.3) of the nonselected set in the closed position during operation A.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 A.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. 3.2.9.2, r; A.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. - Sec. 3.2.9.2, 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. 3.2.9.2, q, t

a. Delta-P measurement on FW control valve fails at 0. Sect. 3.2.9.2, a.

b. FW temperature measurement in one loop fails high. Sect. 3.2.9.2, c.

c. MFW flow signal fails showing no flow. Sect. 3.2.9.2, d.

d. Hot leg temperature measurement fails high. - Sect. 3.2.9.2, g.

e. Delta-T_c signal fails either way. - Sect. 3.2.9.2, i.

f. T_{AVG} determination fails high. - Sect. 3.2.9.2, j.

g. Neutron flux measurement fails high. - Sect. 3.2.9.2, k.

h. MFW blocking valve position indicator fails in closed position. - Sect. 3.2.9.2, m.

i. Reactor coolant flow measurement fails low. - Sect. 3.2.9.2, u.

j. Main steam line safety, atmospheric, or turbine bypass valve fails open. - Sect. 3.2.9.2, v.

k. MFW control valve fails open or valve control signal fails demanding valve opening. - Sect. 3.2.9.2, 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. 3.2.9.2, b.

b. MFW flow measurement fails at low valve greater than zero. - Sect. 3.2.9.2, e.

c. Reactor inlet temperature measurement in one loop fails low. - Sect. 3.2.9.2, h.

d. Startup FW control valve position indicator fails with valve less than 50% open. - Sect. 3.2.9.2, 1.

e. MFW pump speed governor fails. - Sect. 3.2.9.2, n.

f. MFW Startup valve fails open. - Sect. 3.2.9.2, p.

g. MWe demand fails high. - Sect. 3.2.9.2, s.

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

A sufficient leak in selected pressure tap A (A') - see Fig. A.2.3 - or the connecting pipe from that tap or the packing of the blocking valves on which the connecting pipe terminates. Sect. 3.2.9.2, r A.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 359 in. level followed by MFW pump, reactor, and turbine trip and initiation of AFW.

Type D and E failures, taken alone, may be controlled by the ICS. In some cases they will lead to system trips. Type D failures are expected to lead to greater and more rapid SG overfeeds than Type E failures.

Type A and B failures do not cause SG overfeed but block some or all of the high level protection. Type A failures, which bring inconsistent information to the control room display, are expected to be detected sooner than Type B failures, which do not.

There is one Type F failure. This is a single failure which causes the rapid filling of the SG to the 359-in. point and the relatively slow continued coverfilling 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.

3.2.9.2 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 the Midland FMEA on the Midland FMEA on the ICS.[1]

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.

---

[1]R. W. Enzinna, R. W. Winks, S. D. Swartzell, R. P. Broadwater, M. S. Kai, and W. E. Wilson, "Failure Modes and Effects Analysis of the Midland NNI and ICS," Babcock & Wilcox Co. Report BAW 1743 (July 1982).

However, as long as the tracking mode is not activated, the FW control valves should control the FW flow back to the original setpoint. Hence, the plant should settle out at its original condition, except that the high pump speed would result in a higher pressure drop across the FW control valves. Also, with the higher control valve pressure drop, the flow control would be more sensitive and would not be as smooth as normal. The FW valve flow control should be rapid enough to prevent a high level in the steam generators from occurring. However, failure of the FW control valves to act rapidly enough still leaves the high level pump trip protection.

b. The delta-P signal across the FW control valve fails at some point below the setpoint. Qualitatively, the effects are the same as in (a). However, (a) appears to be the bounding case; so the effects should be less severe. A failure of the delta-P signal above the setpoint value should not lead to SG overfeed.

c. The FW temperature measurement in loop A fails high at 500°F. FW temperature compensation will cause the total FW flow demand to increase, resulting in overfeeding both steam generators and overcooling the core. T_{AVG} will start to drop, causing control rods to pull and reactor power to increase. The steam pressure will increase, causing the turbine valves to open and the megawatt electric generation to increase. Because of negative megawatt electric error, the megawatt electric calibrating integral will cause the feedforward control demands to the reactor and feedwater to decrease. If the megawatt electric calibrating integral does not reach a low limit, then the unit will settle out at its original condition. If the megawatt electric calibrating integral goes onto its low limit (generally set at -5%), then the plant will settle out at a higher power level than its original condition. If the FW temperature measurement failure occurs at a low load level, a higher probability of reactor trip due to low RC pressure exists than at a high load level. This is because at the low load level the FW temperature is lower than at the high load level. Hence, a greater percentage increase in FW flow will occur at the low load level. Further, at low load levels BTU limits are less restrictive.

d. The main FW flow signal in loop A fails showing zero flow. The loop A FW control valve will open fully trying to control the FW flow to setpoint. The delta-P across the loop AFW control valve will decrease below setpoint, and the FW pumps will speed up to control the delta-P back to setpoint. Steam generator A is overfed because control valve A goes fully open and the pumps speed up. Steam generator B is initially underfed when control valve A goes fully open, is probably overfed for a short period of time when the pumps speed up, and eventually FW control valve B should control loop B FW flow to setpoint.

T_{AVG} will fall and the control rods will pull to increase reactor power. The FW flow imbalance between loops A and B will cause a

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

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

f. This transient is initiated by the startup level signal in loop A failing low. As a result of this, loop A FW valve opens fully and the FW pumps speed up in an attempt to restore the level in SG-A. In order to control loop B flow, loop B FW valve closes. Neither cross limits nor BTU limits are expected during this initial portion of the transient. Because of excessive FW flow, the primary system may be rapidly overcooled. A reactor trip may occur, probably due to low RC pressure. Also, a high SG level FW pump trip may occur to prevent SG overfill (expected to occur in SG-A). A turbine trip would immediately follow the reactor trip. Because of excessive FW flow, steam pressure should be running high, and operation of steam relief as well as turbine bypass is expected to occur at moderate to high power levels. If the reactor trip occurs before the high steam generator level is reached, there is the potential for continued overcooling of the primary due to the open relief valves and the failed level measurement causing the continuing supply of feedwater to 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. $$T_{AVG} = \frac{T_{HA} + T_{HB} + T_{CA} + T_{CB}}{4}$$

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

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

For a failure of T_{HA} high, method 3 above will give the least error in the calculation of T_{AVG}, and method 2 will give the greatest error.

Two cases will be considered. The first case will consider complete automatic operation of the ICS. In the second case, the reactor H/A (i.e., Hand/Auto) station is in manual with all other H/A stations in automatic. In both cases, a failure of T_{HA} will cause T_{AVG} to be computed erroneously high. Hence, the T_{AVG} error in the ICS, given by

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

will be negative.

With the ICS in complete automatic, the T_{AVG} signal modifies the reactor demand. A negative T_{AVG} will cause the control rods to insert. If T_{AVG} is large enough it can cause the feedwater flow demand to be modified through the cross limits from neutron error to feedwater control. A sufficiently negative T_{AVG} will cause the feedwater demand to be increased. Hence, with the power generation of the reactor decreasing and the feedwater flow increasing, this transient is in the direction of a steam generator overfill.

With the reactor H/A station in manual and all other H/A stations in automatic, the T_{AVG} error signal modifies the total feedwater demand through a proportional/integral controller. A step increase in the T_{AVG} signal, such as would be caused by T_{HA} failing high, has the potential for driving this control loop unstable. The negative T_{AVG} signal would initially cause the feedwater demand to increase rapidly while the reactor demand remains constant. Again, this transient is in the direction of a steam generator overfill.

h. This transient is initiated by the reactor inlet temperature in loop A failing low. Proportional control action in the delta-T_c control will immediately cause the flow demand in loop A to decrease and the flow demand in loop B to increase. This proportional control action is limited to 5%. Integral action in the delta-T_c control will eventually cause the variable gain multiplier in the flow ratioing circuit to be decreased by an additional 20%. Hence, because of the delta-T_c control, the flow demand for loop A flow equals (100% - 5% - 20%) times the total flow demand. The flow demand for loop B flow then equals 200% (100% - 5% - 20%) times the total flow demand. Therefore, the flow demand in loop A is reduced by 25% and the flow demand in loop B is increased by 25% on account of delta-T_c control. The low failure of the reactor inlet temperature in loop A will also cause an error in the calculation of T_{AVG}. There are three methods of determining T_{AVG}. They are

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

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

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

For a failure of T_{CA} low, method (3) will result in no error and method (2) will result in the greatest error in the calculation of T_{AVG}. It will be assumed that either method (1) or (2) is being used to calculate T_{AVG}. For T_{CA} failing low, T_{AVG} will be calculated low. This will cause the reactor power to be increased. Also, the low T_{AVG} will, through the reactor cross limits to the FW system, cause the total FW demand to be lowered. Hence, the reactor power increases; the T_{AVG} control causes the FW flow to SG-B to decrease, and the 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 TAVG 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 ratios 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 A.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 delta-T_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.

3.2.10 Control System Failures That Contribute to Reactor Coolant System Overcooling

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

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

The major systems identified in Section 2.4.4 as potentially affecting RCS overcooling have been analyzed using the FMEA techniques. The results of these analyses, including the effects of control instrumentation and supporting systems failures have been discussed in separate reports 1, 2 and 3.

The specific effects of failures in the systems identified in Table 2.4.12 as they relate to RCS overcooling are discussed in Section 3.2.10. The majority of these RCS overcooling effects have been obtained from the more general FMEA's of the identified systems. The RCS overcooling effects resulting from failures in the RCS subsystems (Pressurizer, RC Pumps and Steam Generators) and associated control instrumentation and support systems are identified and discussed in Section 3.2.10.1. The RCS overcooling effects of failures in the Power Conversion and Makeup and Purification systems are discussed in Sections 3.2.10.2 and 3.2.10.3, respectively.

3.2.10.1 Reactor Coolant Subsystems

As discussed in Section 2.4, three RCS subsystems have been identified as potentially contributing to overcooling transients: the Pressurizer, RC Pump and Steam Generator subsystems. The overcooling failure modes and interfacing systems associated with the failure modes are listed for each RCS subsystem in Table 3.2.10.1. As noted, component level FMEA's of each of these subsystems are presented in Tables 3.2.10.2, 3.2.10.3 and 3.2.10.4. The results of the FMEA's are discussed below in Sections 3.2.10.1.1, 3.2.10.1.2 and 3.2.10.1.3 for the Pressurizer, RC Pump and Steam Generator subsystems.

3.2.10.1.1 Pressurizer Subsystem

Two overcooling failure modes have been identified for the pressurizer subsystem: Release of reactor coolant and excessive pressurizer spray flowrate. In Table 3.2.10.2 the specific component level failures leading to or contributing to these failure modes are identified with the potential causes of the failure, its effect on the RCS and possible remedial actions listed for each.

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

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

TABLE 3.2.10.1. SUMMARY OF RCS SUBSYSTEM FAILURE MODES POTENTIALLY CONTRIBUTING TO RCS OVERCOOLING

RCS Subsystem	RCS Overcooling Failure Mode	Interfacing Systems and Components Affecting Failure Mode	Comments
1. Pressurizer	1.1 Release of Reactor Coolant	1.1.1 PORV	FMEA of Pressurizer System presented in Table 3.2.10.2.
		1.1.2 NNI	
		1.1.3 Pressurizer Code Safety Valve	
	1.2 Opening the Pressurizer Spray Valve	1.2.1 Pressurizer Spray Valve	
		1.2.2 NNI	
2. RC Pumps	2.1 Release of Reactor Coolant	2.1.1 RC Pump Shaft Seals	FMEA of RC Pumps presented in Table 3.2.10.3.
		2.1.2 RB Component Cooling Water System	
		2.1.3 MU&P System	
3. Steam Generators	3.1 Release of Reactor Coolant	3.1.1 Steam Generator Tubes	FMEA of Steam Generators presented in Table 3.2.10.4.
		3.1.2 Main Steam and Turbine Bypass System (Excessive Cooldown Possibly Contributing to Tube Failure)	

TABLE 3.2.10.1. (Continued)

RCS Subsystem	RCS Overcooling Failure Mode	Interfacing Systems and Components Affecting Failure Mode	Comments
	3.2 Increased Heat Transfer	3.2.1 Main Steam and Turbine Bypass System	
		3.2.2 Feedwater and Condensate System	
4. Balance of RCS	4.1 Release of Reactor Coolant	4.1.1 MU&P System	FMEA of MU&P System presented in Table 3.2.10.7.

TABLE 3.2.10.2. SUMMARY OF PRESSURIZER SYSTEM FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

	Failure	Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant				
1.	PORV RC-RV3 Fails Open	Mechanical failure of valve resulting in valve opening or failure to close once open.	Small LOCA. Pressurizer fills during RCS depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block valve, RC-4.
2.	Pressurizer Code Safety Valve Fails to Close	Mechanical failure of valve(s) to close after opening.	Small LOCA or RCS leak. Pressurizer fills during depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA must be followed. Open valve may be identified by discharge pipe high temperature indication.
3.	Power to PORV Solenoid Fails On	o NNI Pressure Switch (RC3-PS8) or Controller (RC3-MIS2) Failure	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block valve, RC-4. PORV manual control may be operable.

TABLE 3.2.10.2. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o NNI narrow range RCS pressure transmitter or signal conditioning modules produce spurious high RCS pressure signal.	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer spray valve RC-V1 opens and pressurizer heaters are deenergized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by manual closure of the PORV, RC-RV3 or its block valve RC-4. The pressurizer spray valve, RC-V1, may be manually closed and the pressurizer heaters manually controlled.
Pressurizer Spray Valve Fails Open			
4. Pressurizer Spray Valve, RC-V1 Fails Open	Mechanical failure of valve resulting in valve opening or failing to close once open.	Slow RCS depressurization with the pressurizer heaters energized. ESPS 1500 psi RCS pressure setpoint may be reached depending on the spray flowrate and heater capacity.	Identify open valve and close spray block valve, RC-V5.
5. Power to Spray Valve Solenoid Fails On	o NNI pressure switch, RC-PS3 or controller (RC-MIS1) failure.	Spray valve opens resulting in a slow RCS depressurization with the pressurizer heaters energized. ESPS 1500 psi RCS pressure setpoint may be reached depending on the spray flowrate and heater capacity.	Identify open valve and close spray block valve, RC-V5. Spray valve manual control may be operable.

TABLE 3.2.10.2. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o NNI narrow range RCS pressure transmitter or signal conditioning modules produce spurious high RCS pressure signal.	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer spray valve RC-V1 opens and pressurizer heaters are deenergized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by manual closure of the PORV, RC-RV3 or its block valve RC-4. The pressurizer spray valve, RC-V1, may be manually closed and the pressurizer heaters manually controlled.
Contributing Failures			
6. Failure of Selected Pressurizer Level Transmitter Output Signal Low	Transmitter failure or a failure of the selected transmitter's power supply (ICS Panelboard KI branches HEX, HEY or Computer Panelboard KU)	A selected low pressurizer level signal results in the makeup valve opening and filling the pressurizer, deenergizing the pressurizer heaters and possibly initiating a steam generator overfill transient (see Table 3.3.3, FMEA of the Steam Generators). If the pressurizer is allowed to fill, the PORV will be opened and the possible liquid discharge through the valve could contribute to its failure.	The operator can compare the three pressurizer level measurements through the computer and manually select an operable transmitter for control and indication. Manual control of the makeup valve (and feedwater control valves) is available. The loss of a transmitter power supply is alarmed in the control room.

TABLE 3.2.10.2. (Continued)

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

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

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

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

As shown in Table 3.2.10.2, the pressurizer spray valve could fail open or fail to close due to mechanical failure of the valve or a control circuit failure energizing the solenoid. Circuit failures include failures of the pressure switch or valve control switch which result in the spray valve opening with other components remaining operable. The resulting pressure decrease will result in the pressurizer heaters being energized which may reduce significantly the rate of depressurization.

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

pressure signal include opening the PORV (a small LOCA) and deenergizing the pressurizer heaters in addition to opening the spray valve.

In addition to failures which directly result in an RCS overcooling transient, other Pressurizer System failures which may exacerbate the effects of such a transient have been identified in Table 3.2.10.2, Items 6-9. These failures include instrumentation failures which could impede the detection of an open relief or safety valve, failures of the PORV isolation valve which could prevent rapid termination of a transient resulting from a failed open PORV. Failure of the selected pressurizer level transmitter low has been included in this category since a pressurizer overfill transient could occur. If the overfill was allowed to result in liquid discharge through the PORV or safety valves, valve damage could occur.

3.2.10.1.2 RC Pump Subsystem

One RCS overcooling initiator has been identified in the RC pump subsystem, a release of reactor coolant due to failure of the RC pump shaft seals. RC pump seal failures may result from several possible causes as shown in Table 3.2.10.3. If degraded performance of the RC pump seals is recognized by the operator prior to complete failure of the seals, seal failure may be delayed by tripping the affected pump. Once seal failure occurs, however, the resulting small LOCA cannot be isolated.

3.2.10.1.3 Steam Generator Subsystem

Two potential overcooling mechanisms have been identified for the steam generator subsystem: release of reactor coolant due to steam generator tube failure and insufficient heat transfer rate across the steam generator tubes. The FMEA of the steam generator subsystem is presented in Table 3.2.10.4.

Steam generator tube leaks occur during normal operation typically due to a combination of causes as listed in Table 3.2.10.4. Although control system failures have not been identified as a single, sole cause of a tube leak or failure, control system failures may initiate a tube failure in combination with other existing conditions or increase the rate of tube degradation.

TABLE 3.2.10.3. FMEA OF RC PUMPS: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

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

TABLE 3.2.10.4. FMEA OF STEAM GENERATORS: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

	Failure	Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant				
1.	Steam Generator Tube Failure	o Material defects in tubes.	Steam generator tube rupture accident: a small break LOCA with the reactor coolant released to the main steam system and condenser.	Emergency procedures for steam generator tube rupture accident must be followed.
		o Long term operation with adverse feedwater chemistry.	Same as above.	Same as above.
		o Excessive magnitude/ frequency of compression and tension cycles on tubes with undetected defects in tube material.	Same as above.	Same as above.
		o Severe cooldown of RCS with undetected defects in tube material.	Same as above.	Same as above.
Increased Heat Transfer Rate				
2.	Depressuri-zation of Main Steam System	o Turbine bypass valve(s) fail open.	Small steam line "break" accident. Rapid cooldown of RCS.	Identify leak path and isolate if possible. Follow emergency for steamline breaks. See FMEA of Main Steam Systems, Table 3.2.10.5.
		o Main steam code safety valve(s) fail open.	Same as above.	Same as above.

TABLE 3.2.10.4. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
		o Failure to trip or runback turbine following reactor trip.	Same as above.	Same as above.
3.	Injection of Feedwater at Rates in Excess of RCS Requirements (Steam Generator Overfill)	o Main feedwater control valve fails open or fails to close.	Steam generator level increases until main feedwater pumps are tripped on high steam generator level. Emergency feedwater system automatically started and controlled.	Manually trip main feedwater pumps and confirm automatic initiation and control of emergency feedwater system. See FMEA of Main Condensate and Feedwater System, Table 3.2.10.6.
		o Startup feedwater control valve fails open or fails to close.	Same as above.	Same as above.

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

RCS overcooling transients resulting from increased steam generator heat transfer rate have been identified in Table 3.2.10.4, Items 2 and 3. In either case, however, the initiating control system failures occur in the main steam or main feedwater systems. These failures are considered, in detail, in the FMEA's of the Main Steam and Turbine Bypass System and the Condensate and Main Feedwater System discussed in Sections 3.2.10.2.1 and 3.2.10.2.2.

3.2.10.2 Power Conversion Systems

As discussed in Section 3.2.10.1.3, the increased steam generator heat transfer RCS overcooling mechanism can be initiated by failures in the main steam and main feedwater systems. Specific failures in these systems contributing to potential RCS overcooling transients are discussed in Sections 3.2.10.2.1 and 3.2.10.2.2.

3.2.10.2.1 Main Steam and Turbine Bypass System

The principal effect of failures in the main steam and turbine bypass system on RCS overcooling is the potential for depressurizing the steam generators. As discussed in Section 2.4, reducing the steam generators' pressure reduces the saturation temperature on the secondary side of the steam generators and increases the heat transfer rate from the RCS. Failures in the main steam and turbine bypass system depressurizing the main steam system and the resulting effects on the RCS are listed in Table 3.2.10.5. The information in this table was extracted from more general FMEA's of the Power Conversion Systems.

TABLE 3.2.10-5. SUMMARY OF MAIN STEAM AND TURBINE BYPASS FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING

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

TABLE 3.2.10.5. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
		o Spurious high output from selected steam generator A outlet pressure transmitter (SS6A-PT1 or PT2) or train A control circuit modules.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor turbine trip and potentially overcooling of RCS could occur.	Identify open valves and manually control. Close isolation valve MS-17 if required to limit RCS cooldown rate.
4.	One or Both Steam Generator B Turbine Bypass Valves (MS-28, 31) Fail Open or Fail to Close Following Turbine Trip	Mechanical failure of valve(s) or transducers, improper maintenance.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-26 as required to control RCS cooldown rate.
5.	Both Steam Generator B Turbine Bypass Valves (MS-28, 31) Open in Response to a Spurious Control Signal	o Spurious output of manual control station SS15A-MC (aux. shutdown panel) signal valves to open.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-26 as required to control RCS cooldown rate.
		o Spurious high output from selected steam generator B outlet pressure transmitter (SS6A-PT1 or PT2) or train A control circuit modules.	Steam diverted to condenser. Depending on the response of the turbine and reactor controls and the main condenser, automatic reactor and turbine trip and potentially overcooling of RCS could occur.	Identify open valve(s) and manually close isolation valve MS-26 as required to control RCS cooldown rate.

TABLE 3.2.10.5. (Continued)

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

TABLE 3.2.10.5. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
9.	Main Turbines Fail to Trip Following Reactor Trip	o Contacts in CRDCS fail to open on reactor trip.	Following reactor trip, continued steam flow through the turbines would result in depressurization of the turbine header, throttling of the turbine governor valve and possible overcooling of the RCS. Feedwater flowrate to steam generators initially throttled until low steam generator level setpoint is reached. The extent of RCS overcooling following this transient is unknown.	Attempt to manually trip the high and/or low pressure turbines. Manually throttle main feedwater to control RCS depressurization if required.
		o Unspecified failures in turbine control system (details of turbine control instrumentation unavailable).	Same as above.	Same as above.
Contributing Failures				
10.	Failure of Turbine Bypass or Startup Header Isolation Valves (MS-17, 26, 24, 33)	Mechanical failure of valve or operator, loss of electric power to valve.	Failure of normally open isolated valves may remain undetected during normal operation. Under these conditions, an open startup header or turbine bypass flowpath could not be isolated.	Identify and repair open valve. If a steam release should occur, follow emergency procedures for a steam line break.

TABLE 3.2.10.5. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
11.	Failure of a CRDCS Turbine Trip Contact to Open on Demand	Contact "sticks" in position.	The redundancy of turbine trip contacts would provide a turbine trip signal. However, failure of a contact would reduced the available redundancy.	Identify the closed contact and repair. This failure would be difficult to identify and may remain undetected for a significant period of time depending on the testing procedurally required.

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

The sixteen main steam code safety valves (eight valves per steam generator) are spring loaded valves that open due to high steam pressure on the valve seat. As the steam pressure decreases, the valves automatically close due to the force of the springs on the valve seats. Following turbine trip, some of the safety valves are expected to open. Improper valve maintenance could result in one or more safety valves failing to close at their (closure) setpoint pressure potentially leading to RCS overcooling.

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

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

Two failure modes were identified which potentially could cause all four valves to open. Failure of the pressure setpoint module common to both instrument strings (Item 6) could result in both instrument strings signalling the four turbine bypass valves to open. The second failure mode resulting in the four turbine bypass valve failing to close (Item 7) involves a sequenced loss of the ICS Panelboard KI branch H or H1 (auto power). The specific effect of a loss of auto power is to transfer the turbine bypass valve to manual control. The valves would then remain in their existing position. If

the power failure occurred immediately following turbine trip, the four turbine bypass valves would be open and thus remain open. For the case of this particular power supply failure, the main feedwater control valves also transfer to manual and remain open (see Table 3.2.10.6).

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

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

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

Failure of the main turbine to trip following reactor trip has been identified as a possible cause of significant steam generator depressurization. However, the potential for such a transient to occur, while believed to be very unlikely, remain unevaluated due to unavailability of turbine control instrumentation design information. Following reactor trip, contacts in the CRDCS open to signal the turbine controls to automatically trip the turbine. Should the CRDCS turbine trip contacts fail, the steam lines will begin to depressurize. The lower steam pressure would be sensed by ICS and a signal sent to the turbine controls to close the turbine throttle valves. Whether other parameters input to the turbine controls (e.g., turbine speed) would override the ICS signal and maintain the turbine throttle valves open is

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

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

3.2.10.2.2 Condensate and Main Feedwater System

The principal effect of failures in the Condensate and Main Feedwater system on RCS overcooling is the potential for overfeeding the steam generators. Following reactor trip, the potentially rapid increase in steam generator inventory is expected to result in RCS overcooling until manually or automatically terminated. Specific failures in the Condensate and Main Feedwater System leading to overfeeding the steam generators and the overall effects of these failures are identified in Table 3.2.10.6 and discussed below.

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

Failure of one of the two control valves to the open position could occur due to a mechanical failure of the valve or its operator, failure of the E/P transducer or failure of the associated ICS loop A or loop B feedwater control circuit (Item 1). In the event one of the control valves failed open, the operator has the option of manually closing the main valve and controlling the startup valve, if possible, or tripping the main feedwater pumps. If the operator fails to control main feedwater flow, the main feedwater pumps will be tripped automatically on high level in either steam generator. The extent of RCS overcooling prior to automatic pump trip is unknown.

TABLE 3.2.10.6. SUMMARY OF CONDENSATE AND MAIN FEEDWATER FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

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

TABLE 3.2.10.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o Failure of Steam Generator Startup Range Level Transmitter Sensing Tap.	Steam generator A or B level increases possibly resulting in reactor trip. Continued feedwater injection following reactor trip expected to result in RCS overcooling until terminated by high steam generator level control setpoint or high steam generator level trip of main feedwater pumps and subsequent automatic initiation of emergency feedwater. Emergency feedwater continues to overfill affected steam generator.	Manually close main feedwater control valve and manually control startup control valve in the affected loop. Trip main feedwater pumps manually if required to control RCS overcooling. Confirm automatic initiating and control of emergency feedwater. Manually control emergency feedwater based on steam generator operator range level signals.

TABLE 3.2.10.6. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
2.	Main Feedwater Control Valves FDW-32 and/or FDW-41 Fail Open	Power to selected startup level transmitter fails (ICS Panelboard KI, branch HEX or HEY).	Depending on the manual selection of the HEX or HEY powered startup level transmitters, either or both main feedwater control valves open resulting in overfeeding of the associated steam generators and possible RCS overcooling. The transient is automatically terminated by high steam generator level trip of the main feedwater pumps and automatic initiation and control of emergency feedwater. In addition to effects on feedwater control, these power failures could result in opening the makeup control valve and closing the loop A and/or B turbine bypass valves depending on manual transmitter selection.	Manually close main feedwater control and startup valves and makeup control valves. Automatic control may be restored by manual selection of operable steam generator startup level and pressure transmitters and pressurizer level transmitters.

TABLE 3.2.10.6. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
3.	Main Feedwater Control Valves FDW-32 and/or FDW-41 Fails to Close Following Reactor Trip	o Loss of Instrument Air Pressure.	Following reactor trip, the supply of feedwater to the steam generators exceeds the RCS demand resulting in increasing steam generator levels and possible RCS overcooling. The transient is terminated by an automatic high steam generator level trip of the main feedwater pumps and automatic initiation and control of emergency feedwater using the backup nitrogen system. Loss of closure of the turbine bypass valves, the makeup control valve and RC pump seal return valve and opening the RC pump seal injection control valve.	Manually trip main feedwater pumps if required to control RCS overcooling. Follow emergency procedure for loss of instrument air.

TABLE 3.2.10.6. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o Loss of ICS Panelboard KI Auto Power branch (H, H1) or manual transfer of main feedwater control valve to manual control.	Following reactor trip, the steam generators will be overfed resulting in possible RCS overcooling. The transient terminated automatically by a high steam generator level trip of the main feedwater pumps. Loss of auto power also results in the makeup, RC pump seal injection and turbine bypass valves transferring to manual and freezing in position. If the power failure occurred following turbine trip, the turbine bypass valves could fail in an open position resulting in a steam generator depressurization.	Manually close main feedwater control valves and manually control main feedwater startup turbine bypass and makeup control valves if required.
	o Loss of ICS Panelboard KI Hand Power branch (HX, H1X) or unspecified failure of feedwater control valve or operator.	Main feedwater control valves freeze in position and main feedwater pumps run back to a speed corresponding to a 0 volt signal. Turbine bypass valves close and remain closed. Initial overfilling of steam generators and possible overcooling of RCS may occur. The transient would be terminated automatically by a high steam generator level trip of the main feedwater pumps or closure of the main feedwater block valves, FDW-31 and 40.	Manually trip main feedwater pumps if required to control RCS overcooling. Transfer power supplies to Panelboard KU to retain automatic control of makeup and turbine bypass valves.

TABLE 3.2.10.6. (Continued)

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

TABLE 3.2.10.6. (Continued)

	Failure	Possible Causes	Effects	Remedial Actions
7.	Cracks in Condenser Resulting in Air-In-Leakage	Vibration corrosion.	Increased concentrations of oxygen in condensate. If not removed by the air ejectors or in the condensate system, the out-of-specification oxygen concentrations could have a deleterious effect on the steam generator tubes in the long term.	Monitor condenser pressure and condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.
8.	Condensate Demineralizer Bypass Valves Spuriously Open	Instrumentation, valve operator or maintenance failure.	Increased condensate flow bypassing demineralizers possibly resulting in out-of-specification condensate water quality. This could have a deleterious effect on the steam generator tubes in the long term.	Monitor condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.
9.	Condensate Demineralizers Allowed to Operate After Depletion	Maintenance/operations failure.	This operating mode could result in out-of-specification condensate water quality. This could have a deleterious effect on the steam generator tubes in the long term.	Monitor condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.
10.	Hydrazine Feed Isolated	Unspecified (PO-115G) unavailable.	Increased concentrations of oxygen in condensate. The out-of-specification oxygen concentrations could have a deleterious effect on the steam generator tubes in the long term.	Monitor condensate water quality to identify the problem and repair. If condensate impurities exceed specifications, shut down the reactor.

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

Loss of the instrument air system or failure of selected ICS Panelboard KI branch circuits will result in the loop A and loop B main feedwater control valves failing in an "as is" position (Item 3). Loss of instrument air or failure of Panelboard KI branch HX, H1X (ICS Hand Power), result in the feedwater control valves failing as is, the turbine bypass valves closing, the feedwater pump speed being reduced, and the reactor subsequently tripping. If a steam generator overfeed transient results, it can be terminated by manual or automatic trip of the main feedwater pumps. Failure of Panelboard KI branch H, H1 (ICS Auto Power) results in many plant components, including the feedwater control valves, automatically transferring to manual control and remaining in position. If the plant was in steady state operation prior to the auto power, an automatic reactor trip may not occur in the short term. However, other effects of the loss of Auto Power such as the generation of many spurious control room alarms, may induce the operator to manually trip the reactor. Once the reactor is tripped, the steam generators will be initially overfed. The operator has the option of manually controlling the feedwater control valves or tripping the feedwater pumps. The feedwater pumps will be automatically tripped on high steam generator level if the level is not manually controlled. As noted in Table 3.2.10.6 and 3.2.10.5, if the loss of Auto Power occurred following a turbine/reactor trip transient, the turbine bypass valves would be open. The loss of Auto Power, in this case, would transfer the turbine bypass valves to manual control while they were open. This could result in a combined steam generator depressurization, steam generator overfeed transient initially. The operator can manually control both the turbine bypass and feedwater control valves. If required, to control

steam generator level, the operator may trip the main feedwater pumps and verify the automatic initiation and control of emergency feedwater.

In addition to Condensate and Feedwater system failures which directly result in overfeeding the steam generators, a number of failures could increase the severity of a transient in combination with other failures. These contributing failures are listed in Table 3.2.10.6, Items 4 through 10.

Of the failures listed, possibly the most significant is the failure of the automatic high steam generator level main feedwater pump trip. This failure, Item 4, in combination with steam generator overfeed failures (Items 1, 2, and 3), could result in the introduction of significant quantities of water into the steam lines unless the overfeed was manually terminated by the operator. The specific effects of overfilling the steam generators have been addressed in Reference 3. These effects include, in addition to the increased severity of RCS overcooling, possible damage of the main steam safety and turbine bypass valves and significantly increased stresses imposed on the main steam lines and their supports. Although the effects of increased stresses, possibly intensified by the opening and closing of turbine bypass or safety valves, have not been evaluated in detail, the conditional probability of consequential steam line failure would be increased.

Trip of the four RC pumps has been listed as a contributing failure (Item 5). Following a trip of the four pumps, the control of the startup feedwater valves transfers to the operate range level transmitters at a 20 foot steam generator level setpoint. This action alone may produce some degree of RCS overcooling. However, the increased level is required to promote natural circulation in the RCS and the rate of increase in steam generator level would be less rapid than following transients initiated by the main feedwater valves failing open or failing to close. If the selected operate range level transmitter on either steam generator were in a failed low state, the feedwater flowrate to the affected steam generator would continue beyond the 20 foot level setpoint and the automatic steam generator high level feedwater pump trip would be defeated.

Other contributing failures include failure of the main feedwater block valves and failures potentially resulting in exceeding feedwater chemistry specifications. As noted in Table 3.2.10.4, adverse feedwater chemistry could contribute to long term degradation of the steam generator tube integrity.

3.2.10.3 Makeup and Purification System

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

A detailed FMEA of the MU&P system has been performed and the effects of MU&P equipment failures identified (Reference 2). The MU&P failures potentially affecting insufficient core cooling have been summarized in Table 3.2.10.7.

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

Failure of the operating reactor building component cooling water flow results in isolation of cooling water to the letdown coolers and RC pumps. This failure would result in automatic isolation of letdown flow. If the letdown storage tank (LST) was allowed to drain resulting in damage to the operating HPI pumps or the HPI pumps were manually tripped to protect them, a simultaneous loss of RC pump seal injection and cooling water flow would occur. As identified in Table 3.2.10.3, this condition could lead to RC pump seal failures.

For the three MU&P failures listed, the LST will be drained unless an alternate supply of water is provided to the HPI pumps. Following a small LOCA, this action may occur automatically if the 1500 psi ESPS setpoint is reached prior to draining the LST. If the LST is allowed to drain, the

TABLE 3.2.10.7. SUMMARY OF MAKEUP AND PURIFICATION SYSTEM FMEA: FAILURES LEADING TO OR AFFECTING RCS OVERCOOLING TRANSIENTS

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

operating HPI pump would be damaged degrading the HPI safety function required for mitigation of small LOCA's.

3.2.10.4 References

1. Failure Modes and Effects Analysis of the Pressurizer and Associated Equipment, SAI Letter Report, May 31, 1983.

2. Failure Modes and Effects Analysis for the Oconee 1 Nuclear Power Station Makeup and Purification System, ORNL #62B-13819C/62X-30, SAI #1-147-08-492-00, October 28, 1983.

3. Nuclear Power Plant Steam Generator Overfill Resulting from Control Action, F. H. Clark, N. E. Clapp, R. Broadwater, NUREG/CR-3692, ORNL/TM-9061, February 28, 1984.

3.3 BROAD FMEA FOR OVERHEATING

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

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

The major systems identified in Section 2.4 as potentially affecting insufficient core cooling have been analyzed using the FMEA techniques. The results of these analyses, including the effects of control instrumentation and supporting systems failures have been discussed (References 6, 8, 9).

The specific effects of failures in the systems identified in Table 2.4.10 as they relate to insufficient core cooling are discussed in Section 3.3. The majority of these effects have been obtained from the more general FMEA's of the identified systems. The insufficient core cooling effects resulting from failures in the RCS subsystems (Pressurizer, RC Pumps and Steam Generators) and associated control instrumentation and support systems are identified and discussed in Section 3.3.1. The insufficient core cooling effects of failures in the Power Conversion and Makeup and Purification systems are discussed in Sections 3.3.2 and 3.3.3, respectively.

3.3.1 Reactor Coolant Subsystems

As discussed in Section 2.4, three RCS subsystems have been identified as potentially contributing to insufficient core cooling transients: the Pressurizer, RC Pump and Steam Generator subsystems. The insufficient cooling failure modes and interfacing systems associated with the failure modes are listed for each RCS subsystem in Table 3.3.1. As noted, component level FMEA's of each of these subsystems are presented in Tables 3.3.2, 3.3.3 and 3.3.4. The results of the FMEA's are discussed below in Sections 3.3.1.1, 3.3.1.2 and 3.3.1.3 for the Pressurizer, RC Pump and Steam Generator subsystems.

3.3.1.1 Pressurizer Subsystem

Release of reactor coolant (a small LOCA) has been identified as an insufficient cooling initiator for the pressurizer subsystem. In Table 3.3.2 the specific component level failures leading to or contributing to this failure mode are identified with the potential causes of the failure, its effect on the RCS and possible remedial actions listed for each.

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

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

TABLE 3.3.1. SUMMARY OF RCS SUBSYSTEM FAILURE MODES

RCS Subsystem	Insufficient Cooling Failure Mode	Interfacing Systems and Components Affecting Failure Mode	Comments
1. Pressurizer	1.1 Release of Reactor Coolant	1.1.1 PORV	FMEA of Pressurizer System presented in Table 3.3.2.
		1.1.2 NNI	
		1.1.3 Pressurizer Code Safety Valve	
2. RC Pumps	2.1 Release of Reactor Coolant	2.1.1 RC Pump Shaft Seals	FMEA of RC Pumps presented in Table 3.3.3.
		2.1.2 RB Component Cooling Water System	
		2.1.3 MU&P System	
3. Steam Generators	3.1 Release of Reactor Coolant	3.1.1 Steam Generator Tubes	FMEA of Steam Generators presented in Table 3.3.4.
		3.1.2 Main Steam and Turbine Bypass System (Excessive Cooldown Possibly Contributing Tube Failure)	
	3.2 Loss of Steam Generator Cooling	3.2.1 Feedwater and Condensate System	
4. Balance of RCS	4.1 Release of Reactor Coolant	4.1.1 MU&P System	FMEA of MU&P System presented in Table 3.3.7.

TABLE 3.3.2. SUMMARY OF PRESSURIZER SYSTEM FMEA: FAILURES LEADING TO OR AFFECTING INSUFFICIENT CORE COOLING TRANSIENTS

	Failure	Possible Causes	Effects	Remedial Actions
Release of Reactor Coolant				
1.	PORV RC-RV3 Fails Open	Mechanical failure of valve resulting in valve opening or failure to close once open.	Small LOCA. Pressurizer fills during RCS depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block valve, RC-4.
2.	Pressurizer Code Safety Valve Fails to Close	Mechanical failure of valve(s) to close after opening.	Small LOCA or RCS leak. Pressurizer fills during depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA must be followed. Open valve may be identified by discharge pipe high temperature indication.
3.	Power to PORV Solenoid Fails On	o NNI Pressure Switch (RC3-PS8) or Controller (RC3-MIS2) Failure	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer heaters energized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by closure of the PORV Block valve, RC-4. PORV manual control may be operable.

TABLE 3.3.2. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o NNI narrow range RCS pressure transmitter or signal conditioning modules produce spurious high RCS pressure signal.	PORV opens resulting in a small LOCA. Pressurizer fills during depressurization. Pressurizer spray valve RC-V1 opens and pressurizer heaters are deenergized.	Emergency procedures for small LOCA's must be followed. Open PORV may be identified by PORV accoustic monitor (details unavailable) and/or discharge pipe high temp. indication. LOCA may be terminated by manual closure of the PORV, RC-RV3 or its block valve RC-4. The pressurizer spray valve, RC-V1, may be manually closed and the pressurizer heaters manually controlled.
Contributing Failures			
6. Failure of Selected Pressurizer Level Transmitter Output Signal Low	Transmitter failure or a failure of the selected transmitter's power supply (ICS Panelboard KI branches HEX, HEY or Computer Panelboard KU)	A selected low pressurizer level signal results in the makeup valve opening and filling the pressurizer, deenergizing the pressurizer heaters and possibly initiating a steam generator overfill transient (see Table 3.3.3, FMEA of the Steam Generators). If the pressurizer is allowed to fill, the PORV will be opened and the possible liquid discharge through the valve could contribute to its failure.	The operator can compare the three pressurizer level measurements through the computer and manually select an operable transmitter for control and indication. Manual control of the makeup valve (and feedwater control valves) is available. The loss of a transmitter power supply is alarmed in the control room.

TABLE 3.3.2. (Continued)

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

TABLE 3.3.3. FMEA OF RC PUMPS: FAILURES LEADING TO OR AFFECTING INSUFFICIENT CORE COOLING TRANSIENTS

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

TABLE 3.3 (5.4). FMEA OF STEAM GENERATORS: FAILURES LEADING TO OR AFFECTING INSUFFICIENT CORE COOLING TRANSIENTS

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

TABLE 3.3.4. (Continued)

Failure	Possible Causes	Effects	Remedial Actions
	o Main Feedwater flow isolated (Main and Startup Valves Closed).	Steam generator dryout occurs with subsequent pressurization of the RCS and opening of the PORV and/or pressurizer safety valves.	Manually initiate Emergency Feedwater and confirm subsequent closure of PORV. If low reactor coolant subcooling occurs, manually initiate HPI.

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

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

In addition to failures which directly result in a potential insufficient core cooling transient, other Pressurizer System failures which may exacerbate the effects of such a transient have been identified in Table 3.3.2, Items 6-9. These failures include instrumentation failures which could impede the detection of an open relief or safety valve, failures of the PORV isolation valve which could prevent rapid termination of a transient resulting from a failed open PORV. Failure of the selected pressurizer level transmitter low has been included in this category since a pressurizer overfill transient could occur. If the overfill was allowed to result in liquid discharge through the PORV or safety valves, valve damage could occur.

3.3.1.2 RC Pump Subsystem

One insufficient cooling initiator has been identified in the RC pump subsystem, a release of reactor coolant due to failure of the RC pump shaft seals. RC pump seal failures may result from several possible causes as shown in Table 3.3.3. If degraded performance of the RC pump seals is recognized by the operator prior to complete failure of the seals, seal failure may be

delayed by tripping the affected pump. Once seal failure occurs, however, the resulting small LOCA cannot be isolated.

3.3.1.3 Steam Generator Subsystem

Two potential insufficient cooling initiators have been identified for the steam generator subsystem: release of reactor coolant due to steam generator tube failure and insufficient heat transfer rate across the steam generator tubes. The FMEA of the steam generator subsystem is presented in Table 3.3.4.

Steam generator tube leaks occur during normal operation typically due to a combination of causes as listed in Table 3.3.4. Although control system failures have not been identified as a single, sole cause of a tube leak or failure, control system failures may initiate a tube failure in combination with other existing conditions or increase the rate of tube degradation.

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

Insufficient core cooling transients resulting from a loss of steam generator cooling has been identified in Table 3.3.4, Item 2. The feedwater pump trip and main feedwater isolation cases are considered, in detail, in the FMEA of the Main Steam and Turbine Bypass System and the Condensate and Main Feedwater System discussed in Sections 3.3.2.1 and 3.3.2.2.

3.3.2 Power Conversion Systems

As discussed in Section 3.3.1.3, the loss of steam generator heat transfer insufficient cooling mechanism can be initiated by failures in the main feedwater systems. Specific failures in these systems contributing to potential insufficient core cooling transients are discussed in Sections 3.3.2.1 and 3.3.2.2.

TABLE 3.3.5. SUMMARY OF MAIN STEAM AND TURBINE BYPASS FMEA: FAILURES LEADING TO OR AFFECTING INSUFFICIENT CORE COOLING

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Pump Turbine A Stop and Governor Valves MS-40, 41	Valves open spuriously	Instrumentation or valve operator failure.	Possible FW Pump A trip on overspeed and plant runback and/or trip.	Close isolation valve MS-35 and repair failure.
	Valve fails to open on demand	Instrumentation or valve operator failure.	FW pump A inoperability following turbine trip. Feedwater supplied by other FW pump.	Identify closed valve and repair following shutdown.
FW Pump Turbine A Isolation Valve MS-35	Valve spuriously closes	Instrumentation failure, maintenance error.	Isolation of high pressure steam supply to FW pump turbine A. Following turbine trip, FW pump A will be inoperable.	Identify closed valve and manually reopen, if possible. An alternate supply of steam may be provided from the startup steam header.
FW Pump Turbine B Stop and Governor Valves MS-43, 44	Valves open spuriously	Instrumentation or valve operator failure.	Possible FW Pump B trip on overspeed and plant runback and/or trip.	Close isolation valve MS-36 and repair failure. Provide steam supply to condenser steam air ejectors via startup header.
	Valve fails to open on demand	Instrumentation or valve operator failure.	FW pump B inoperability following turbine trip. Feedwater supplied by other FW pump.	Identify closed valve and repair following shutdown.

TABLE 3.3.5. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Condenser Steam Air Ejector and MFW Pump Turbine B Steam Supply Isolation Valve MS-36	Valve spuriously closes	Instrumentation failure, maintenance error.	Isolation of steam supply to condenser steam air ejectors A, B, and C, emergency air ejector and high pressure supply to FW pump turbine B. Loss of steam air ejectors eventually may cause a turbine trip and subsequently loss of MF Pump B.	Identify closed valve and manually open if possible. An alternate supply of steam may be provided from the startup steam header.
FW Pump Turbine Exhaust Valve MS-98, 100	Valve closes spuriously	Instrumentation, maintenance failure.	Trip of FW pump and plant runback and/or trip.	Repair failure.
Emergency FW Pump Turbine Steam Supply Isolation Valve MS-82 and/or 84	Valve spuriously closes	Instrumentation failure, maintenance error.	Possible isolation of high pressure steam supply to emergency FW pump turbine A. Closure of one valve has no effect on emergency FW pump turbine operability; closure of both valves will result in pump inoperability.	Identify closed valve and manually reopen.

TABLE 3.3.6. SUMMARY OF CONDENSATE AND MAIN FEEDWATER FMEA: FAILURES LEADING TO OR AFFECTING INSUFFICIENT CORE COOLING TRANSIENTS

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Pump Turbine Steam Supply Isolation Valve LPE-12	Valve spuriously closes	Instrumentation or valve operator failure.	Isolation of low pressure steam supply to both FW pump turbines. Possible inoperability of both FW pumps and plant runback or trip. High pressure steam supply may maintain pump operability.	Identify closed valve and reopen or repair following shutdown.
FW Pump Turbine A Stop and Gov. Valves LPE-19, 20	Valve spuriously closes	Instrumentation or valve operator failure.	Isolation of low pressure steam supply to FW pump turbine A. Possible inoperability of FW pump and plant runback or trip. High pressure steam supply may maintain pump operability.	Identify closed valve and reopen or repair following shutdown.
	Gov. valve spuriously opens	Instrumentation or valve operator failure.	Increased FW pump speed and possible overspeed trip. FW flowrate controlled by regulating valves. Trip of FW pump would result in plant runback or trip.	Identify open valve and repair following shutdown.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Pump Turbine B Stop and Gov. Valves LPE-22, 23	Valve spuriously closes	Instrumentation or valve operator failure.	Isolation of low pressure steam supply to FW pump turbine B. Possible inoperability of FW pump and plant runback or trip. High pressure steam supply may maintain pump operability.	Identify closed valve and reopen or repair following shutdown.
	Gov. valve spuriously opens	Instrumentation or valve operator failure.	Increased FW pump speed and possible overspeed trip. FW flowrate controlled by regulating valves. Trip of FW pump would result in plant runback or trip.	Identify open valve and repair following shutdown.
Vacuum Breaker Valve V-186 (?)	Valve spuriously opens	Instrumentation or maintenance failure.	Turbine trip, trip of MFW pump turbines and interlock of turbine bypass valves closed.	Identify open valve and manually close. Reestablish condenser vacuum.
Condenser Shell and Miscellaneous Connecting Piping	Crack resulting in excessive air in-leakage	Vibration, corrosion.	Bounded by turbine trip, trip of MFW pump turbines and interlock of turbine bypass valves closed.	Identify failure and repair.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Hotwell Pump Isolation Valves C-1, 2, 4, 5	Valve spuriously closes	Instrumentation, maintenance failure.	Less than 50% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen valve or reopen failure.
Hotwell Pump B, C	One or both pumps tripped, inoperable	Electric power, motor failure, loss of Recirc. Cooling Water flow to bearing coolers.	Failure of both pumps and failure of one pump at higher power levels result in FW pump, reactor trip and automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue following loss of one pump.	Identify and repair failure.
Condensate Valve C-10	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Trip of FW pumps and reactor. Automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Demineralizer Bypass Valves C-14, 15	Valve spuriously closes	Instrumentation, valve operator or maintenance failure.	Less than 30% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen or repair.
	Valve spuriously opens	Instrumentation, valve operator or maintenance failure.	Demineralizers bypassed which eventually will result in exceeding water quality specifications and may require plant shutdown.	Identify and repair failure.
Generator Water Cooler Bypass Valve C-61	Valve spuriously closes	Instrumentation or valve operator failure.	Trip of FW pumps and reactor. Automatic initiation and control of emergency feedwater.	Identify closed valve and repair failure.
Condensate Booster Pump Isolation Valves C-77, 80, 81, 84	Valve spuriously closes	Instrumentation, maintenance failure.	Less than 50% reduction in condensate flowrate and probable FW pump and reactor trip at higher power levels. Automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue.	Identify closed valve and manually reopen valve or reopen failure.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
Condensate Booster Pumps A, B	One or both pumps tripped, inoperable	Electric power, motor failure, loss of Recirc. cooling water flow to bearing coolers.	Failure of both pumps and failure of one pump at higher power levels result in FW pump, reactor trip and automatic initiation and control of emergency feedwater. At lower power levels (<50% power) operation expected to continue following loss of one pump.	Identify and repair failure.
"F" Low Pressure FW Heater Isolation Valves C-89, 90, 91	Valve spuriously closes	Instrumentation or maintenance failure.	Less than 33% reduction in condensate flowrate. Probable FW pump and reactor trip at higher power level with automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
Low Pressure FW Heater Isolation Valves C-103, C-104, C-110, C-111, C-117, C-118	Valve spuriously closes	Instrumentation or maintenance failure.	Less than 50% production in condensate flowrate. Probable FW pump and reactor trip at higher power levels with automatic initiation and control of emergency feedwater.	Identify closed valve and manually reopen or repair.
FW Pump Isolation Valve FDW-1, FDW-6	Valve spuriously closes	Instrumentation or maintenance failure.	Trip of one of two main FW pumps, plant runback and possible reactor trip.	Identify closed valve and manually reopen or repair.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Heater Drain System	Unspecified - Dwg. PO-123A not available	Unspecified - Dwg. PO-123A not available	Effects bounded by a trip to the main FW pumps and automatic initiation and control of emergency feedwater.	Identify failure and repair.
FW Pumps A, B	Pump trip	Instrumentation failure, pump/turbine failure, high steam generator level, loss of Recirc. cooling water flow to oil coolers - see also FMEA of Condensate System and Main Steam System.	Trip of one pump will result in a plant runback and possible reactor trip at higher power levels (>50% power). Trip of both pumps results in reactor trip and automatic initiation and control of emergency feedwater.	Identify failure and repair.
	Spurious speed decrease	Instrumentation or throttle valve operator failure.	Possible decrease in feedwater flowrate resulting in plant runback and possible reactor trip.	Identify failure and repair.
FW Pump Isolation Valves FDW-4, FDW-3, FDW-9, FDW-8	Spurious valve closure	Instrumentation, valve operator or maintenance failure.	Reduction in FW flowrate by <50%. Plant runback and/or reactor trip at higher power levels.	Identify closed valves and manually reopen or repair failure.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
FW Pump Recirculation Control Valve FDW-53, 55	Valve fails to open on low FW flowrate	Instrumentation or valve operator failure.	Following substantial feedwater flowrate decrease transients (e.g., reactor trip), failure to maintain minimum pump flowrate will result in pump trip or possible pump damage.	Identify failure and repair.
FW Control Valve FDW-32, FDW-41	One or both valves spuriously close	Instrumentation or valve operators' failure.	Reduction in FW flowrate to one or both steam generators which may result in plant runback and/or reactor trip.	Identify failure and repair.
	Valve(s) open or fail to close on demand	Loss of instrument air pressure, instrumentation, or valve operator failure.	Valve(s) opening or remaining in position after reactor trip may result in a steam generator overfeed condition. Transient will be terminated by automatic trip of main FW pumps and initiation and control of emergency feedwater under manually controlled by the operator.	Identify closed valve and manually reopen or repair failure.
FW Startup Valve FDW-35, FDW-44	Valve(s) spuriously closes	Instrumentation or valve operator failure.	Closure of FW block valve and loss of feedwater to one steam generator resulting in reactor trip.	Reestablish feedwater flow to isolated steam generator by manual control of startup and block valves or manual initiation of emergency feedwater.

TABLE 3.3.6. (Continued)

Component	Failure Mode	Potential Causes	Effect on Plant	Remedial Actions
	Valve(s) open or fail to close on demand	Loss of instrument air pressurize, instrumentation or valve operator failure.	Valve(s) remain in position following reactor trip which may result in a steam generator overfeed condition. Transient would be terminated by automatic trip of main FW pumps and initiation and control of emergency feedwater under manually controlled by the operator.	Identify failure and manually close startup or startup isolation valves.

3.3.2.1 Main Steam and Turbine Bypass System

The main steam and turbine bypass system transports the steam generated in the steam generators to the high pressure turbines or diverts it directly to the atmosphere or condenser. In addition to piping, the system consists of sixteen spring loaded code safety valves, four pneumatic turbine bypass valves, the high pressure turbine stop and governor valves and high pressure steam supply lines to the main feedwater and emergency feedwater pump turbines. Component failure modes potentially affecting loss of steam generator cooling are summarized in Table 3.3.5.

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

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

3.3.2.2 Condensate and Main Feedwater System

Failures in the condensate and main feedwater systems have two principal effects of significance to inadequate core cooling: a trip of both main feedwater pumps and isolation of the feedwater flow to both steam generators. Component failures leading to these conditions are identified in Table 3.3.6 and discussed below.

Many single failures have been identified which are expected to result in trip of both main feedwater pumps. This includes loss of condenser vacuum failures, flow blockages upstream of the main feedwater pumps, or failures of the hotwell or condensate booster pumps. In addition, single failures in the

feedwater control valves or the ICS feedwater control circuits resulting in a high level in either steam generator cause an automatic trip of both feedwater pumps. Failures in the pump trip circuitry or selected ICS power supplies also result in feedwater pump trip. Trip of the main feedwater pumps result in automatic initiation and control of the emergency feedwater system.

Although failures can be identified which would isolate the feedwater flow to one or the other steam generator, single component failures isolating both steam generators could not be identified. However, two ICS power supply failures, failures of the "auto power" (H1 or H circuits) of the "hand power" (H1X or HX circuits) may result in isolation of main feedwater.

Loss of hand power results in the main feedwater pump speed decreasing to 2800 RPM (0 volt speed signal in a ±10 volt range) and the turbine bypass valves closing and remaining closed. In this condition, if the reduced shutoff head of the main feedwater pumps is less than the lowest setpoint pressure of the main steam code safety valves, the flow to both steam generators will stop. (If the pumps' shutoff head is higher than this value, the steam generator level may increase slowly to the feedwater pump trip setpoint.)

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

With either of the power supply failures, the feedwater flow to both steam generators may be terminated without tripping the main feedwater pumps and consequently without an automatic initiation of emergency feedwater. Although the operator would be able to manually initiate and automatically control emergency feedwater, the spurious alarms and deenergized indicators may be confusing. Furthermore, the initial steam generator feedwater levels may be initially high. As a result, the time delay from the initial loss of power supply to the time feedwater flowrate must be reestablished to prevent steam generator dryout could also impede the decision to manually initiate emergency feedwater.

If the steam generators were allowed to dryout, the operator would be expected to manually initiate HPI on low reactor coolant subcooling. However, the existing conditions already had resulted in the operator failing to manually initiate emergency feedwater. A subsequent failure to manually initiate HPI under these conditions would be significantly more likely than otherwise might be the case.

3.3.3 Makeup and Purification System

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

A detailed FMEA of the MU&P system has been performed and the effects of MU&P equipment failures identified (Reference 8). The MU&P failures potentially affecting insufficient core cooling have been summarized in Table 3.3.7.

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

Failure of the operating reactor building component cooling water flow results in isolation of cooling water to the letdown coolers and RC pumps. This failure would result in automatic isolation of letdown flow. If the letdown storage tank (LST) was allowed to drain resulting in damage to the operating HPI pumps or the HPI pumps were manually tripped to protect them, a simultaneous loss of RC pump seal injection and cooling water flow would occur. As identified in Table 3.3.3, this condition could lead to RC pump seal failures.

TABLE 3.3.7. SUMMARY OF MAKEUP AND PURIFICATION SYSTEM FMEA: FAILURES LEADING TO OR AFFECTING INSUFFICIENT CORE COOLING TRANSIENTS

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

For the three MU&P failures listed, the LST will be drained unless an alternate supply of water is provided to the HPI pumps. Following a small LOCA, this action may occur automatically if the 1500 psi ESPS setpoint is reached prior to draining the LST. If the LST is allowed to drain, the operating HPI pump would be damaged degrading the HPI safety function required for mitigation of small LOCA's.

3.4 BROAD FMEA FOR EXACERBATION OF ONGOING UPSET CONDITIONS

A brief evaluation has been made to assess the potential for the failure of control systems adversely impacting the recovery from design basis accidents. The evaluation was based on design information and transient analyses presented in the Oconee Nuclear Station Final Safety Analysis Report (FSAR).

The evaluation found that the operation of certain control systems has been assumed in some of the accident analyses reported in Chapter 15 of the FSAR. These included the post accident main feedwater flow control, main steam isolation and pressure controls, and the pressurizer spray and/or Pilot Operated Relief Valve (PORV) controls. Failure modes of these control systems adverse to the transient, would result in a more severe transient. However, simulation is required to assess the degree acceptability of the resulting impact on the reactor core or reactor coolant system (RCS). A summary of potentially adverse control system failures is presented in Table 1. The FSAR Chapter 15 accidents and the potential impact of control system failures are discussed below.

The Chapter 15 transients fell into three categories: miscellaneous non-reactor accidents, accidents terminated by reactor trip and accidents exhibiting significant post trip transient behavior. Accidents assigned to these categories are listed in Tables 2, 3 and 4.

The waste gas decay tank rupture and fuel handling accidents, Table 2, involve the release of radioactivity to the auxiliary building and to the environment from the auxiliary building vents. Control system mitigation of these transients was not identified in the analyses described in the FSAR.

Six of the listed accidents involved a core reactivity excursion terminated by reactor trip. These accidents are listed in Table 3. In each case, the accident is detected by the reactor protective system (RPS) which initiates reactor trip. Once trip occurs, a normal hot shutdown condition will result. Although control system failures could impact the hot shutdown, their impact

TABLE 1. SUMMARY OF POTENTIALLY ADVERSE CONTROL SYSTEM FAILURES

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

TABLE 2. MISCELLANEOUS NON-REACTOR ACCIDENTS

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

TABLE 3. ACCIDENTS TERMINATED BY REACTOR TRIP

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

TABLE 4. ACCIDENTS EXHIBITING SIGNIFICANT POST-TRIP TRANSIENT BEHAVIOR

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

would not be significantly different had the design basis accident not occurred. The impacts of such control system failures are addressed in separate reports.

Table 4 lists the design basis accidents exhibiting significant post-trip transient behavior. These accidents and the potential impacts of control system failures are discussed below:

Loss of Coolant Accidents

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

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

Following large LOCA's, the RCS will depressurize rapidly and the accident is mitigated solely by safety systems. Small break LOCA's, however, may require steam generator heat transfer to aid the RCS depressurization. In the Oconee design, the ICS regulates the flow of main feedwater, following the LOCA induced reactor trip, to maintain a level of approximately two feet in each steam generator. This level will be maintained until the reactor coolant pumps (RCP's) are tripped manually following ESAS actuation. Upon RCS trip, the ICS modifies the level setpoint to maintain a twenty foot level in each steam generator.

Two ICS/main feedwater control valve failure modes may affect the mitigation of the small break LOCA: failure to initially maintain the two foot steam generator levels and failure to transfer to the emergency feedwater nozzles and maintain twenty foot levels after the RC pumps are tripped. Manual

initiation of emergency feedwater, a safety system, would ensure the steam generator levels are maintained.

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

The Maximum Hypothetical Accident and Post-Accident Hydrogen Control sections of the FSAR address post-LOCA containment conditions and do not involve control systems interactions to the event described.

The Rod Ejection Accident is a failure of a control rod drive pressure boundary resulting in rapidly removing a control rod from the core and creating a small break LOCA. The core reactivity transient is terminated by reactor trip. Once the core is subcritical, the transient is similar to a small break LOCA discussed above.

The Steam Generator Tube Rupture Accident is a small break LOCA which results in a release of reactor coolant to the environment via the steam generators and main steam safety valves and/or main condenser. Mitigation of the tube rupture accident involves a manually initiated rapid cooldown and depressurization of the RCS to minimize the flow of reactor coolant from the RCS through the ruptured steam generator tube.

The cooldown and depressurization of the RCS requires the operation of control systems. The primary supply of feedwater to the steam generators is provided by the main feedwater system. The supply of feedwater can be provided by the emergency feedwater (safety) system based on automatic actuation in most cases and manual actuation in all cases.

The isolation of the affected steam generator and regulation of main steam pressure requires turbine trip and control of the turbine bypass valves. Turbine trip is initiated by auxiliary relays and contacts located in the control rod drive control system (CRDCS). Although the turbine trip relays

and contacts are redundant (a single failed relay or contact will not initiate or prevent a turbine trip signal), it is not known whether they are designed and tested as a safety system. Unless tested regularly, one or more of these devices may be failed and not be detected following successful turbine trips.

Cooldown of the RCS requires the use of the non-safety Turbine Bypass Valves (TBV), the condenser and associated condenser support systems (principally the condenser circulating water system). Although steam may be released to the atmosphere via the manual steam dump valves, the use of these valves is expected to delay the cooldown significantly.

The required depressurization of the RCS following a tube rupture can be accomplished using the pressurizer spray valve (if the RC pumps are not tripped) or the pressurizer pilot operated relief valve (PORV). Opening the PORV or spray valve is considered a non-safety function in the Oconee design.

In summary, the operation of several control systems has been assumed in the mitigation of small LOCA's. Although failures of these control systems is not expected to have a significant effect on core integrity, they could significantly affect the resulting offsite dose following steam generator tube ruptures. Whether the increased dose is of concern cannot be determined without simulation.

Steam Line Break Accident

The steam line break (SLB) accident involves a postulated failure of a steam line resulting in a very rapid cooldown of the RCS. Of stated concern in the FSAR was the potential for core criticality possibly impeding continued core cooling and the potential for a steam generator tube rupture to be caused by the SLB.

Mitigation of the SLB requires a reactor trip, a turbine trip to isolate one of the two steam generators from the break, isolation of feedwater to the depressurized steam generator and controlled injection of feedwater to the pressurized steam generator. The analyses of SLB's presented in the FSAR cover three postulated operating modes of the ICS and plant operator control of main feedwater:

1. The ICS initially throttles main feedwater flow and the operator prevents the ICS from automatically reopening the control valves.
2. The ICS initially throttles main feedwater but the operator allows the ICS to reopen the control valves to maintain minimum steam generator level.
3. The ICS and the operator fail to throttle feedwater flow.

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

The analysis results presented show that the core could return to 35% of rated power for case 2, the worst case. Unacceptable fuel damage was not reported for this case. Although adverse failure of control systems assumed to operate in these analyses could increase the severity of the RCS cooldown, the impact on core response would be mitigated by increased boric acid injection. Furthermore, the core responses presented each assume the most worthy control rod failed to insert - a very conservative assumption.

The reactor building pressure responses to a SLB presented in the FSAR indicate that the building design pressure is not exceeded for any of the feedwater control failures presented. Additional adverse control system failures were not identified.

An analysis of the effect of the SLB on the steam generator tubes was presented in the FSAR. It is not clear that the analysis assumptions bound the worst-case RCS cooldown. As such, adverse control system failures may increase the potential for consequential damage of the steam generator tubes following a SLB.

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

Loss of Coolant Flow Accidents

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

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

Failure of the ICS to maintain the increased steam generator levels would require manual initiation of emergency feedwater.

Loss of Electrical Power Accidents

Two cases of loss of electric power are addressed in Chapter 15 and additional results of loss of electric power analyses are addressed in Chapter 10 of the FSAR.

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

2.1b4

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

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

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

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

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

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

The possible initial RCS cooldown and/or loss of reactor coolant via the letdown line may result in the pressurizer draining. The effect of the pressurizer draining on natural circulation may be adverse but the extent of the impact cannot be determined without simulation.

There are certain conditions common to a number of transients that could be exacerbated by control failures.

1. Ongoing Condition - Plant cooldown with one steam generator dry (for example, steam line break with the affected steam generator subsequently isolated).

   The plant is cooled principally through the unaffected steam generator. There is an operational limit of 100°F and an emergency limit of 150°F on steam generator tube-sheet temperature differences. The affected steam generator is cooled by the circulating primary fluid. The massive tube supports cool very slowly. If the tubes in the affected steam generator were cooled too rapidly (as they might be if the emergency temperature differential were exceeded for an extended period), there could be single or multiple tube rupture resulting from thermally induced tensile stresses.

   Failure - Any sensor or other failure that causes the tube-to-sheet temperature differential in the affected steam generator to be underestimated could lead to a thermal stress condition that might cause tube ruptures.

2. Ongoing Condition - Any transient in which primary subcooling is lost and at least one steam generator remains an effective heat sink. (A small break LOCA may in some circumstances produce the conditions for this transient, particularly if not well managed initially.)

   Procedures require that water levels in the effective steam generator(s) be raised to 95% on the operating level scale. This would be off scale on the startup level. The level also must be raised manually.

   Failure - If the selected operating level indicator is reading low the steam generator can be overfilled with consequent threat to the integrity of the steam lines, the valves contained thereon and turbines driving MFW or EFW pumps which may draw their steam feed therefrom.

3.5 SELECTION OF TRANSIENTS FOR SIMULATION

3.5.1 BASIS FOR SELECTION

A priori analysis of the transient response of large, controlled, thermal-hydraulic systems, such as nuclear power stations, is only possible in a qualitative manner, and then only until feedback occurs. Without simulation this analysis is limited. Therefore, since this is a controls system study, the FMEA Tables 3.2.2.1 through 3.2.2.3 in Section 3.2 for the integrated control system were searched for simulation candidates. Events were selected based on potential severity, need to determine event sequence, and need to assess the time available to the operator for corrective action. These events are presented by priority in Table 3.5.1. Other cases requiring nuclear power station simulation were noted in Table 3.2.1.2.

3.5.2 RECOMMENDATIONS FOR OVERFILL

The criteria which we follow in recommending that overfill 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.

It becomes evident on examination of overfill sequences that they could be conveniently grouped and bounded by relatively few simulations. They were grouped as follows:

a. Those for which the high level control signal did not fail;

b. Those for which the high level control signal failed; but the overfill was not sufficient to reach the high level pump trip;

c. Those for which both the high level control signal and the high level pump trip failed.

Table 3.5.1 Candidate Transients for Simulation

Priority	Initiating Failure	Remarks
1	Turbine header pressure error; signal fails high	For those systems in which e_{PHDR} feeds forward to the feedwater control system, this failure can lead to flooding both SG A and B by opening MFW and SUFW valves.
2	Either SG operating level or SG startup level; high level limit fails high	Failure holds MFW and SUFW valves full open in one loop. (This failure may not be significant at Oconee due to FW pump trip on SG high level.)
3	Turbine bypass valves stay open (and atmospheric dump valves if present)	Leads to rapid steam system depressurization. (RPS may pick up if plant has SG rupture protection system.)
4	Unit load demand rate limiter fails low or FW demand fails high above the loop A/B ratio controller	These failures lead to a constant high FW demand. System relies on Btu limits for FW flow control.
5	Startup feedwater control valve (SWFW) remains open	Potential for overcooling after reactor trip. Early operator recognition of the failure may not occur due to the relatively low flow rate.

4. AUGMENTED FAILURE MODE AND EFFECTS ANALYSIS

4.1 HYBRID SIMULATION

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

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

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

The simulation is being used primarily to address mild to moderate transients that can occur at least partially under action of the non-safety control system. Attention initially focused on overfill events that assumed single or multiple failures of feed valves or the generator low and high level set points and the trips that regulate these valves. Cases were run at 20%, 50%, and 100% initial power levels, with failures occuring either in loop A or in loop A in combination with loop B. The following classes of events were considered. In the first six sets the initiating event was failure high of the low level set point.

1. Intermediate overfeed failures insufficient to activate steam generator level protective features other than ICS interaction.
2. Overfeed failure when the high level control transfer is approached but not reached.
3. Slow main feedwater control valve action in combination with overfeed failure when the high level control transfer is approached but not reached.
4. Overfeed in which high level control transfer fails and the high level pump trip is approached but not reached.
5. Overfeed with high level control transfer and high level pump trip failed.

6. Overfeed with high level control transfer and high level pump trip failed in combination with a steam leak in line A.
7. Main feedwater blocking valve position indicator falsely indicated closed; flow reading taken from the startup meter in loop A.

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

Other events studied with the model include depressurization of the secondary side and overheating of the primary:

8. Secondary side depressurization induced by steam line rupture or by dump valves or turbine bypass valves failing open in loop A or in combination with loop B at low and high power levels.
9. Insufficient main feedwater cooling induced by steam generator high level setpoint failing low, potentially drying out the generator.

4.2 SIMULATION RESULTS

In this section the above classes of events will be described in more detail. Transients were normally run for ten minutes of plant time; the model has restart capabilities for continuation. Although all available information on plant trips was included, it is possible that trips unknown to the authors would terminate some of the transients. In particular, recent information suggests that the turbine may have a steam quality trip. Possible action of this trip was not provided in the simulation, but was examined in the FMEA process. Also excluded was operator intervention.

Class 1: Intermediate overfeed failure insufficient to activate steam generator level protective features other than ICS interaction. In these cases the low level setpoint in steam generator A was assumed to fail high at 198 in. on the operating range. None of the high level setpoints was approached. At 100% power the impact of this degree of overfill on the primary side was minor as shown by the pressurizer pressure (Fig. 4.2.1) and core outlet temperature (Fig. 4.2.2). At 50% power (and lower) overcooling remained minor, but as generator A filled to the setpoint, the outlet quality* decreased below 1 (Fig. 4.2.3), and liquid was injected into the steam line (Fig. 4.2.4). Fig. 4.2.4 is the time integral of liquid exiting the generator, indicating the total water passing into but not necessarily accumulating in the line. Phase separation and any attendant accumulation were not considered. Loss of superheat at lower power levels results from the larger incremental rise in generator water level necessary to reach the spurious setpoint.

*Throughout this chapter quality is defined as the thermodynamic quality.

Class 2: Overfeed failure when the high level control transfer is approached but not reached. In these cases the low level setpoint in generator A is failed to a higher value than previously: 240 in., near but below the high level setpoint. Because of the greater water loading in the generator, even at 100% power the steam quality at the generator outlet dropped below 1 at approximately 2.5 min. (Fig. 4.2.5), and water was injected into the steam line (Fig. 4.2.6). Runs at 20% and 50% power showed approximately half as much injection into line A in 10 min. As in class 1 events the impact on the primary side appeared minor.

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

Class 3: Slow main feedwater valve action combined with overfeed in which the high level control was approached but not reached. These cases were a repeat of the class 2 events with an added feedwater control valve malfunction in which the stroke rate was significantly slower than normal. Full stroke time was assumed to be 60 seconds rather than the nominal five to ten seconds. At full power, sluggish valve action reduced water injection by 50% compared with normal valve action. Conditions on the primary side were largely unchanged. However, at lower power (20%) the ICS also increased reactor output in attempting to match overfeed (Fig. 4.2.7). Because of the higher power and flow, water injection doubled in comparison with normal valve action.

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

Class 5: Overfeed in which high level control transfer and high level pump trip failed. In these cases the low level set point in generator A was assumed to fail arbitrarily high; a value of 700 in. was used in the simulation. All high level control points in generator A were thus exceeded and assumed failed. Depending upon initial power level, the ICS took different courses of action to reestablish balance between reactor power and feedwater flow. At 20% power the failed setpoint caused the generator A feed valve to run full open in a few seconds (Figs. 4.2.8, 4.2.9). Generator level (Figs. 4.2.10, 4.2.11) increased to 350 in. and stabilized below the failed setpoint because 1) the maximum pumping power in line A was reached, and 2) balance between power and flow was reestablished at 60% (Fig. 4.2.12), with most of the heat transferred in generator A (Figs. 4.2.13, 4.2.14). Superheat in generator A was lost in approximately 1 min. (Figs. 4.2.15, 4.2.16). Total water injection was 38,000 lbs. after 10 min. (Fig. 4.2.17). Coolant temperatures at steam generator outlets are shown in Figs. 4.2.18 and 4.2.19. On the primary side, pressurizer pressure decreased 200 psi in 2.5 min. and recovered (Fig. 4.2.20). Pressurizer level indication dropped 5 ft. and was beginning to rise when the simulation was terminated (Fig. 4.2.21). The cold leg temperature of the affected loop decreased 35°F in 2.5 min. (Fig. 4.2.22).

At 100% initial power (Figs. 4.2.23 through 4.2.37) the ICS was limited in its capacity to adjust power to match overfeed (Fig. 4.2.27). In this case the control system reduced flow to generator B to compensate for the increase in A (Figs. 4.2.23, 4.2.24). The level indication in generator A stabilized near 260 in. (Fig. 4.2.25). Water injected into line A was 68,000 lbs in 10 min. (Fig. 4.2.32). Primary and secondary temperature variations (Figs. 4.2.33, 4.2.34, 4.2.37) are generally smaller than at 20% power since the overfeed at 100% is a smaller percentage change in flow.

In both of these transients, action of the ICS to match power and feed flow resulted in a stabilized system with the generator water level below the failed low level setpoint. If the turbine does not trip on low quality, this configuration may be sustainable.

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

Class 7: Main feedwater blocking valve position indicator falsely indicated closed; flow reading taken from the startup meter in loop A. Initial power was 100%. The feedwater flow signal for generator A was 15%. The ICS reduced reactor power to 65% (Fig. 4.2.38). Total feed flow was reduced less rapidly (Fig. 4.2.39) and some overcooling of the primary occurred. Primary pressure decreased 230 psi (Fig. 4.2.40), and pressurizer level fell from 18 ft to 9 ft in 2 min. (Fig. 4.2.41). Core average temperature as calculated from the hot and cold legs of the affected loop decreased 18°F in 1.5 min. and then began a slow recovery. Water injection into steam line A was 20,000 lbs in 10 min.

Class 8: Secondary side depressurization induced by partial dump valve failure or steam line rupture in loop A or in combination with loop B, at low and high power levels. At 20% power a fault in steam line A was sized to accommodate the line's total available flow. An initial modest pressure reduction in the generator resulted in a temporary increase in feed flow. The ICS increased reactor output and reestablished equilibrium at 35% power. The ICS maintained header pressure by throttling turbine flow, forcing virtually all line A flow through the fault. Impact on the primary and secondary pressures and temperature was minor (Figs. 4.2.42 through 4.2.45). Plant conditions appeared to remain manageable by the ICS. Without operator intervention, the system would be expected to trip on depleted feedwater inventory.

At 100% power, over the time interval considered, the ICS appeared to be capable of managing single line faults that released up to 100% of one line's nominal flow. Perhaps the most noteworthy imbalance was the substantial downtrend in feedwater temperature that resulted from loss of half of the bleed steam to the heaters (Fig. 4.2.46). Leaks of this magnitude or larger in both lines resulted in depressurization of the secondary side and system trip within one minute on low steam flow to the turbine (Fig. 4.2.47).

4.4

4.2 MODEL VALIDATION

4.2.1 Steady State Matching of Plant Behavior

Because of the key role played by the steam generator in the overfill scenarios of interest to this program, special attention has been paid to the fidelity of the steam generator representation in the hybrid model.

Figure 4.1 represents the ΔP ("level") signal from the steam generator pressure taps, plotted as a function of load. This ΔP signal has two components, one representing the water level (static load), the other the dynamic pressure drop across the generator. Points listed as "B&W Plant Behavior" were supplied to us by Dr. Luther Joyner, a former B&W controls engineer, as typical of B&W plant behavior. The hybrid model matches plant ΔP indication to within 25% at low power and to within 5% above 75% power.

Figure 4.2 represents the primary and secondary temperature profiles along the steam generator at 100% load. "Plant data" comes from the Oconee FSAR. The hybrid model duplicates secondary temperatures virtually perfectly, with maximum errors of 4° (out of 580°) for a few points on the primary.

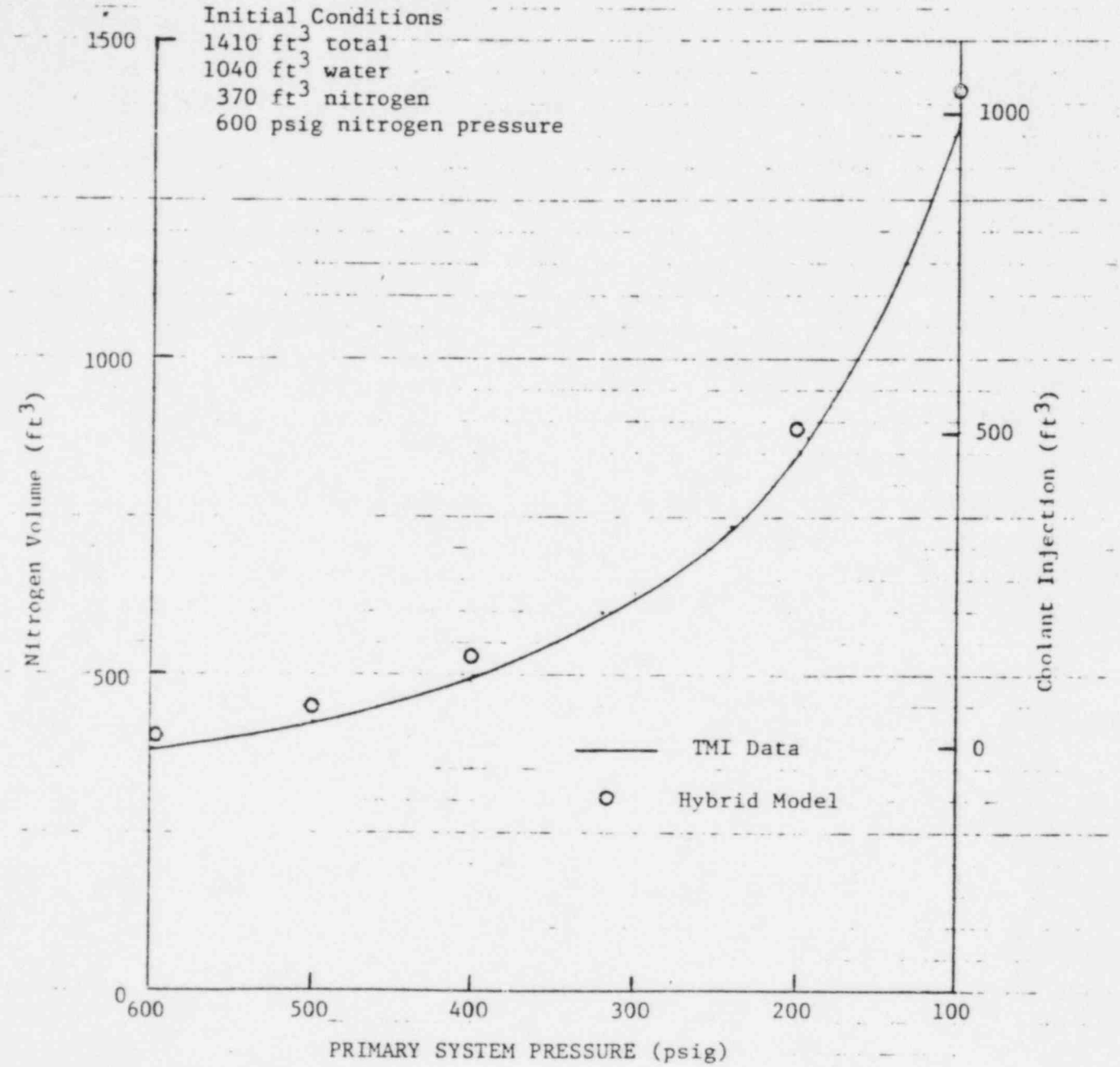
Figure 4.3 represents the steam generator heat transfer area versus load, the plant data again typical B&W values for Dr. Joyner. Water level in the SG increases with load, automatically increasing the boiling heat transfer area. The hybrid model tracks plant behavior well, showing a maximum error of about 12%.

Figure 4.4 is for the core flood tank, plotting its nitrogen (or water) volume as a function of pressure. "TMI data" comes from Table 6.1 in the TMI FSAR. Again the hybrid model matches the data to within 10%.

4.2.2 Transient Modeling of Plant Behavior

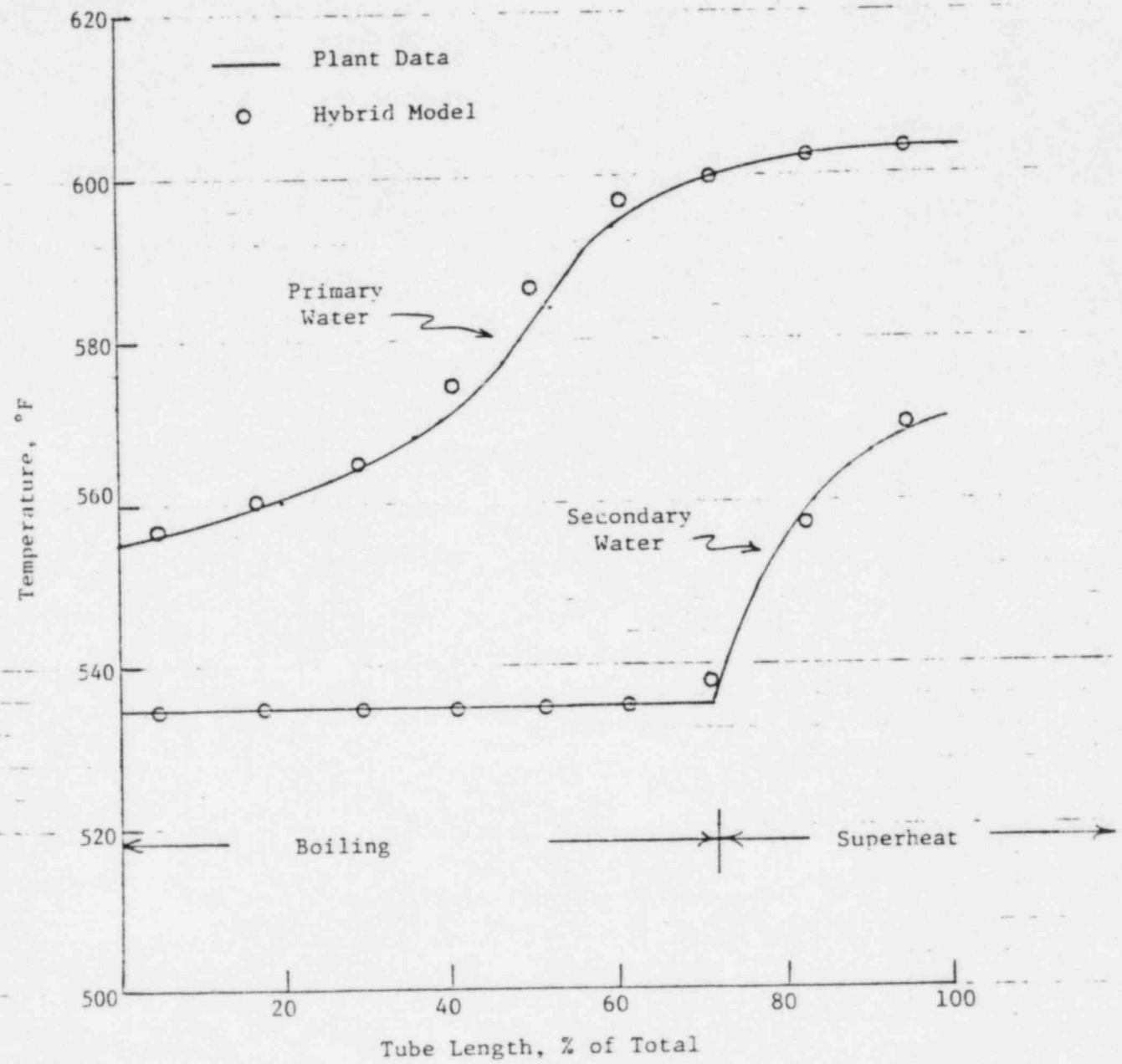
Validation of hybrid model transient behavior will be done on two bases. One will be a comparison of hybrid runs against data available from a turbine trip experienced and recorded at Oconee-3. These runs will be complete in time for the final report.

The other basis will be comparison with RETRAN calculations of some of the same transients run on the hybrid. These are awaiting completion of the RETRAN model, and will also be available in time for this final report.



Core Flood Tank Capacity vs. Primary Coolant System Pressure

Fig. 4.4



Primary and Secondary Temperature Profiles
in the Steam Generator at 100% Load

Fig. 4.2

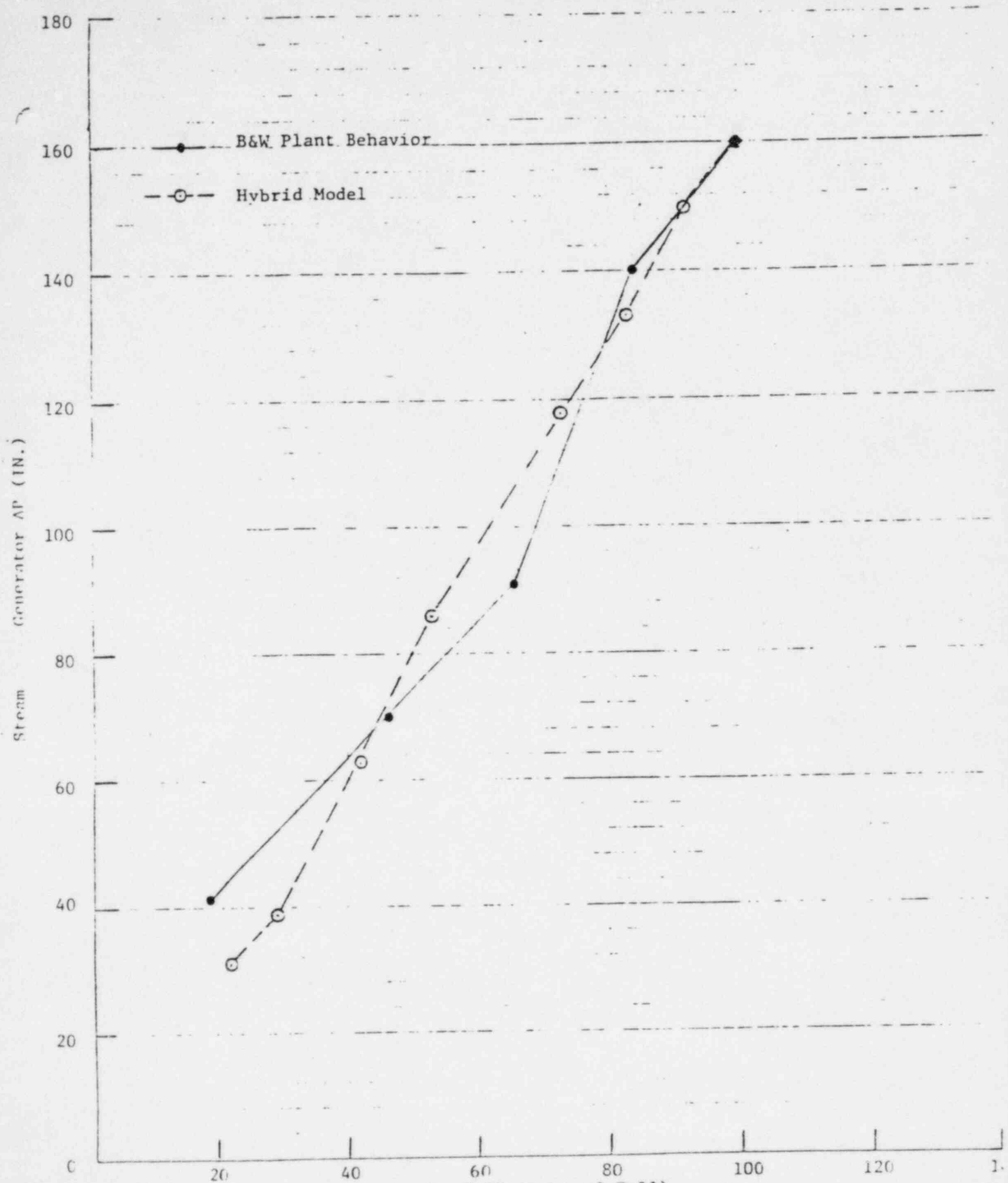


Fig. 4.1

Steam Generator ΔP Signal vs Load

(Hybrid Model vs Plant Data)

4.3 PRELIMINARY CONCLUSIONS

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

In a substantial number of the simulations, superheat was lost, steam generator quality fell below 1, and water was injected into the steam lines. While these cases presume no quality trip, conditions could exist in which the quality hovered just above any trip setpoint and injected water into the lines for a sustained period. For example, in the class 2 event in which the low level set point in generator A failed to 240 in., the quality was marginally below unity (Fig. 4.2.5), water was injected into the line (Fig. 4.2.6), and the condition appeared sustainable in the absence of operator intervention.

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

In the majority of the cases studied, overfill of the generators appeared to have minor effects on the temperatures and pressures of the primary side. An exception appeared to be the class 7 event in which the main feedwater blocking valve position indicator falsely indicated closed and the flow reading was taken from the startup meter in loop A. The ICS ran the power back more rapidly than feed flow, and primary pressures and temperatures dropped significantly.

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

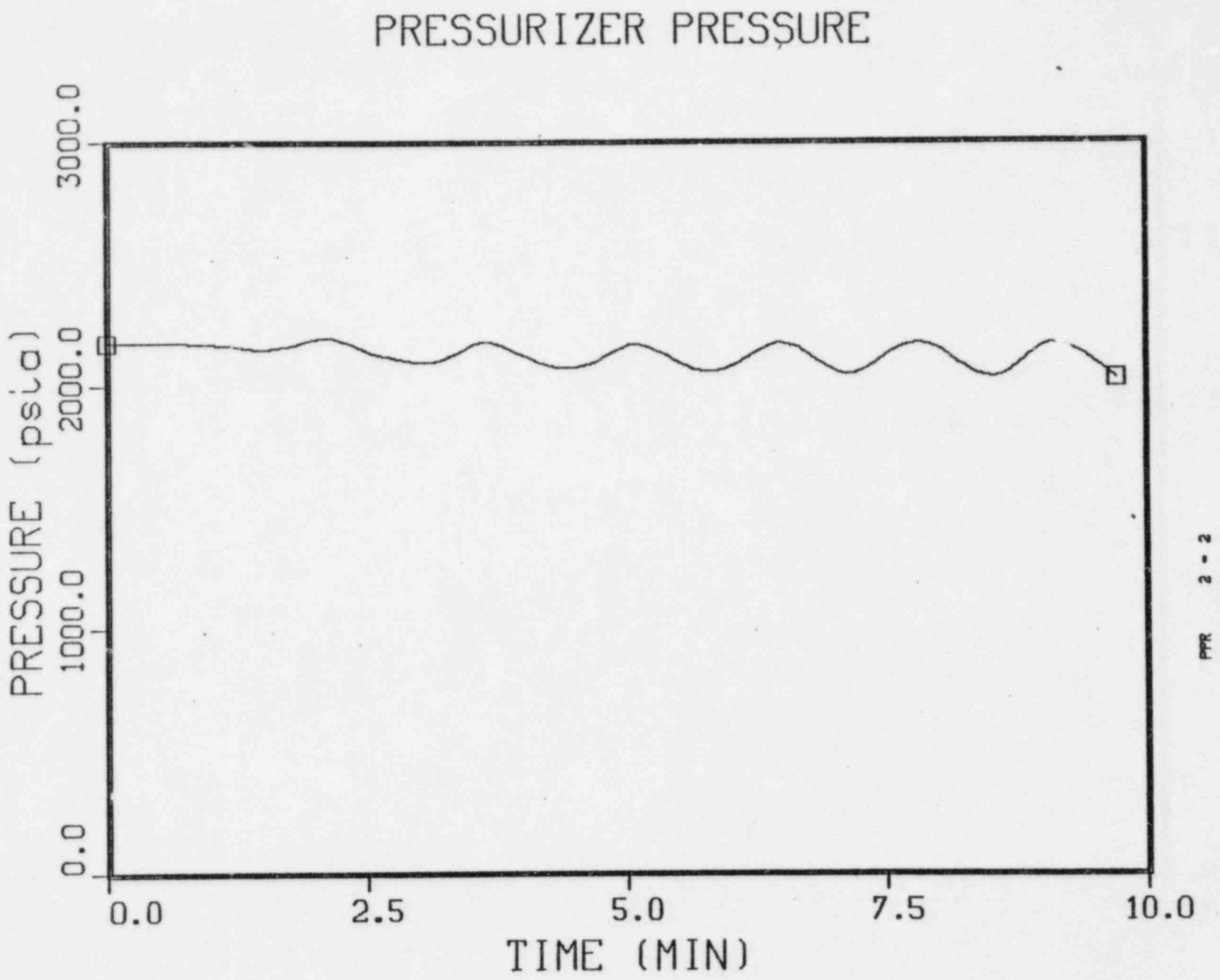


Fig. 4.2.1 Class 1 pressurizer pressure

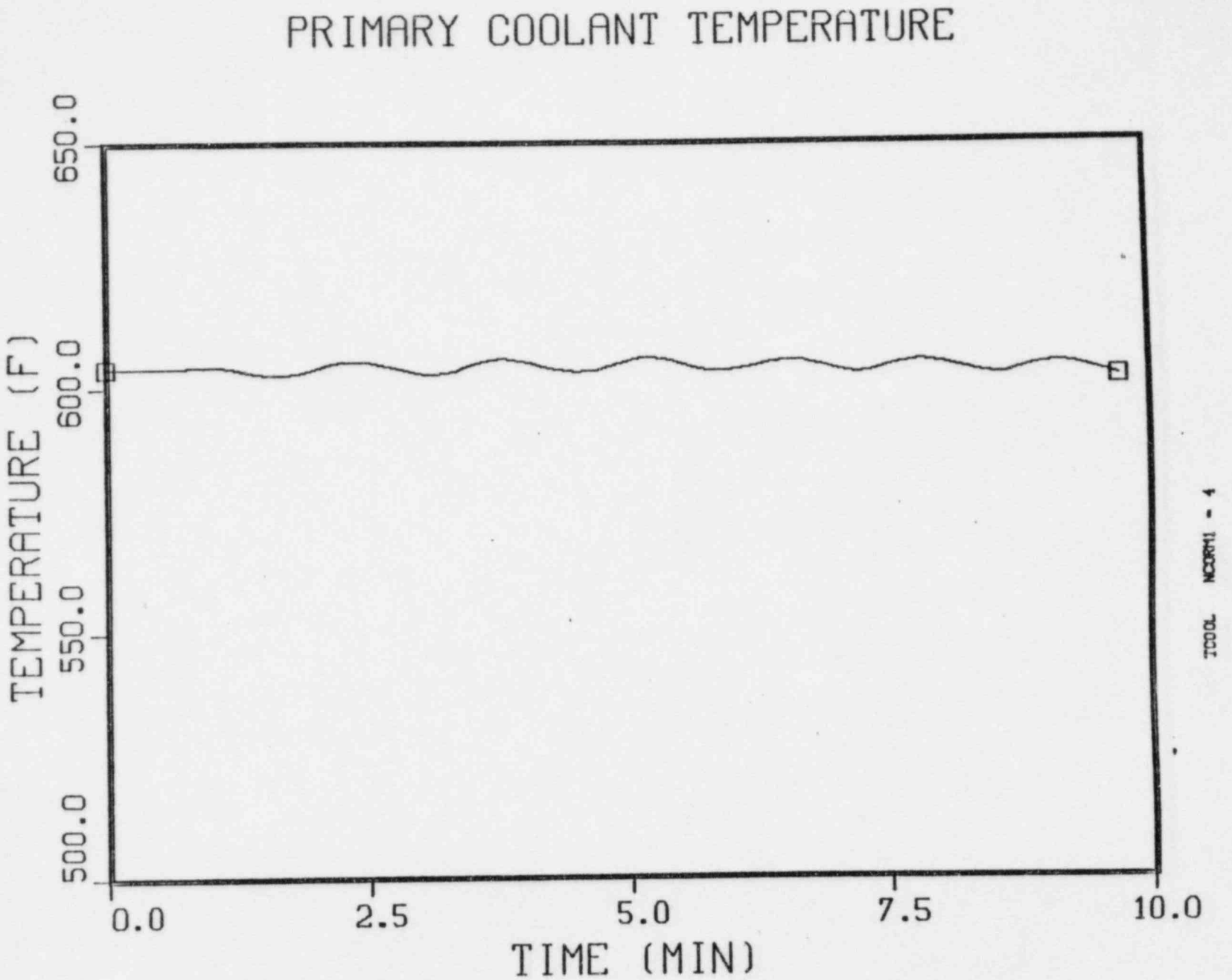


Fig. 4.2.2 Class 1 core outlet temperature

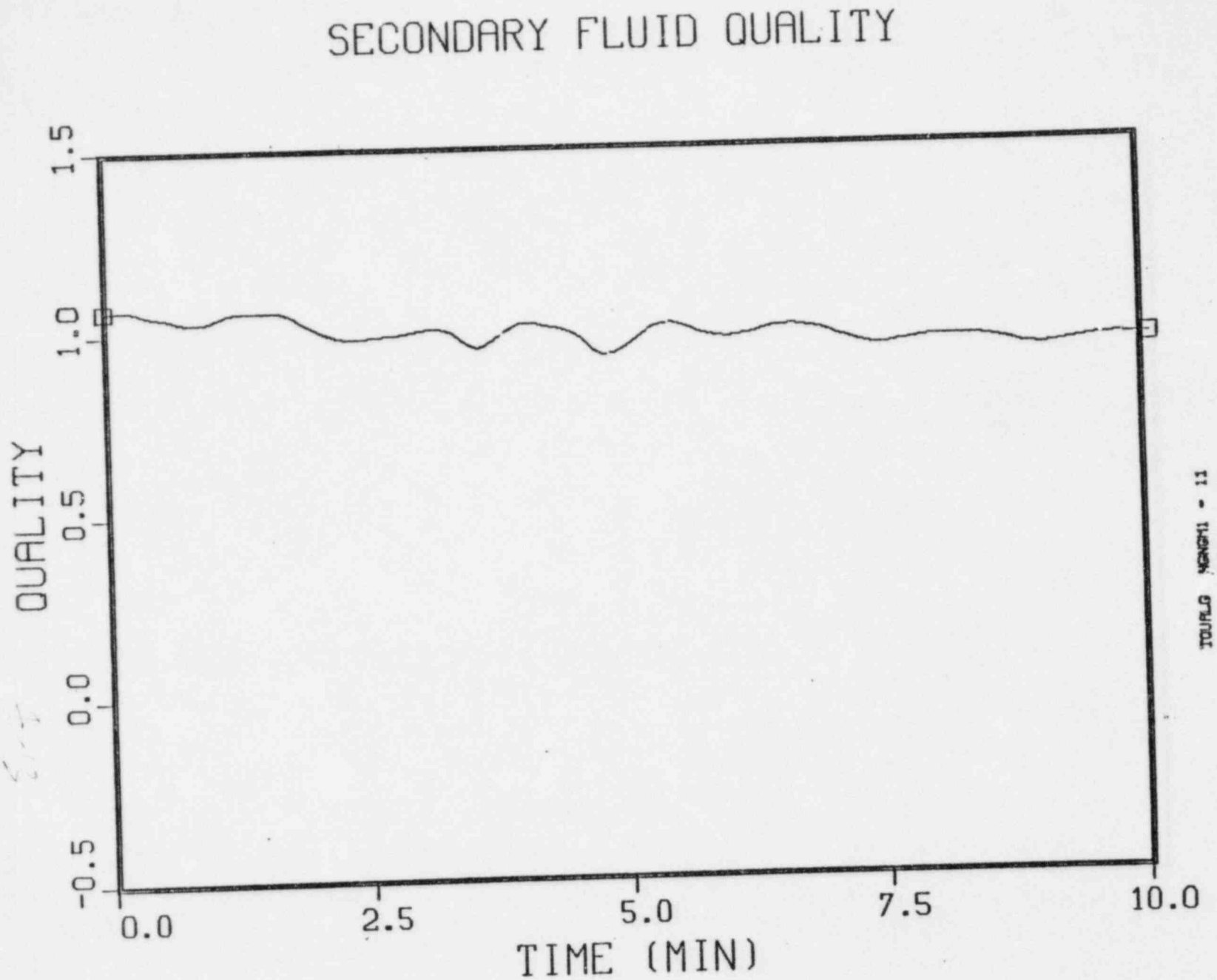


Fig. 4.2.3 Class 1 steam generator A outlet quality

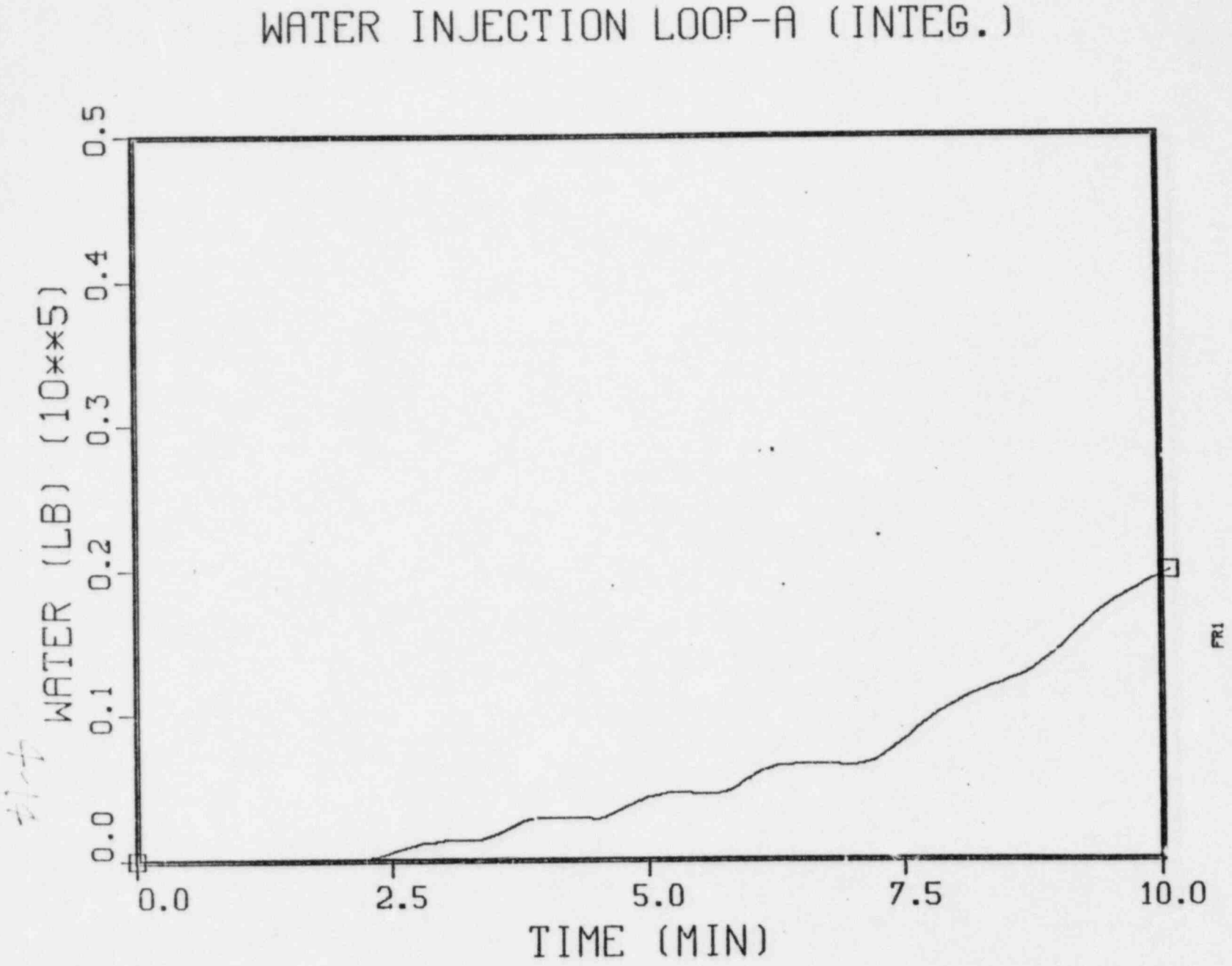


Fig. 4.2.4 Class 1 water injection into steam line A

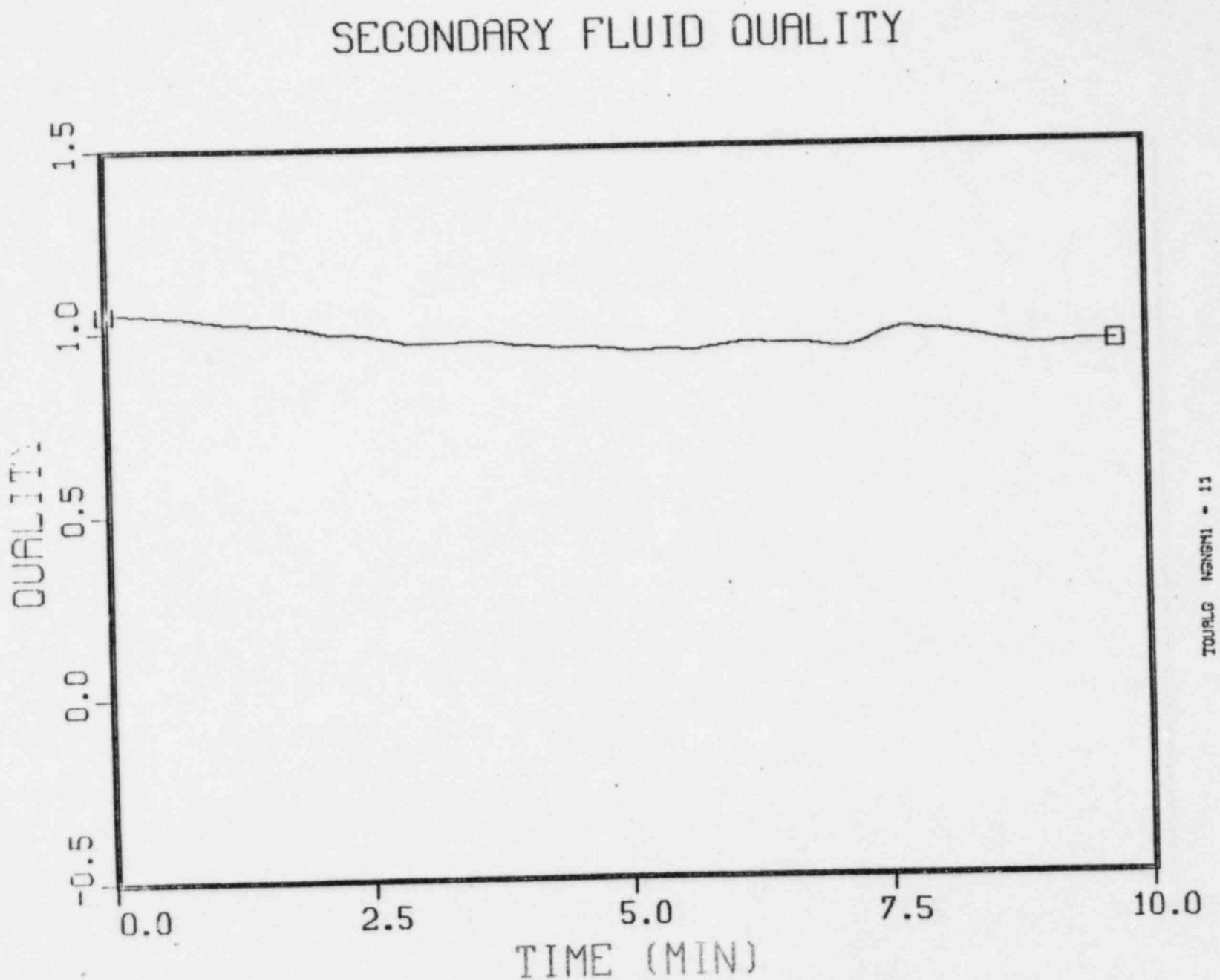


Fig. 4.2.5 Class 2 steam generator A outlet quality

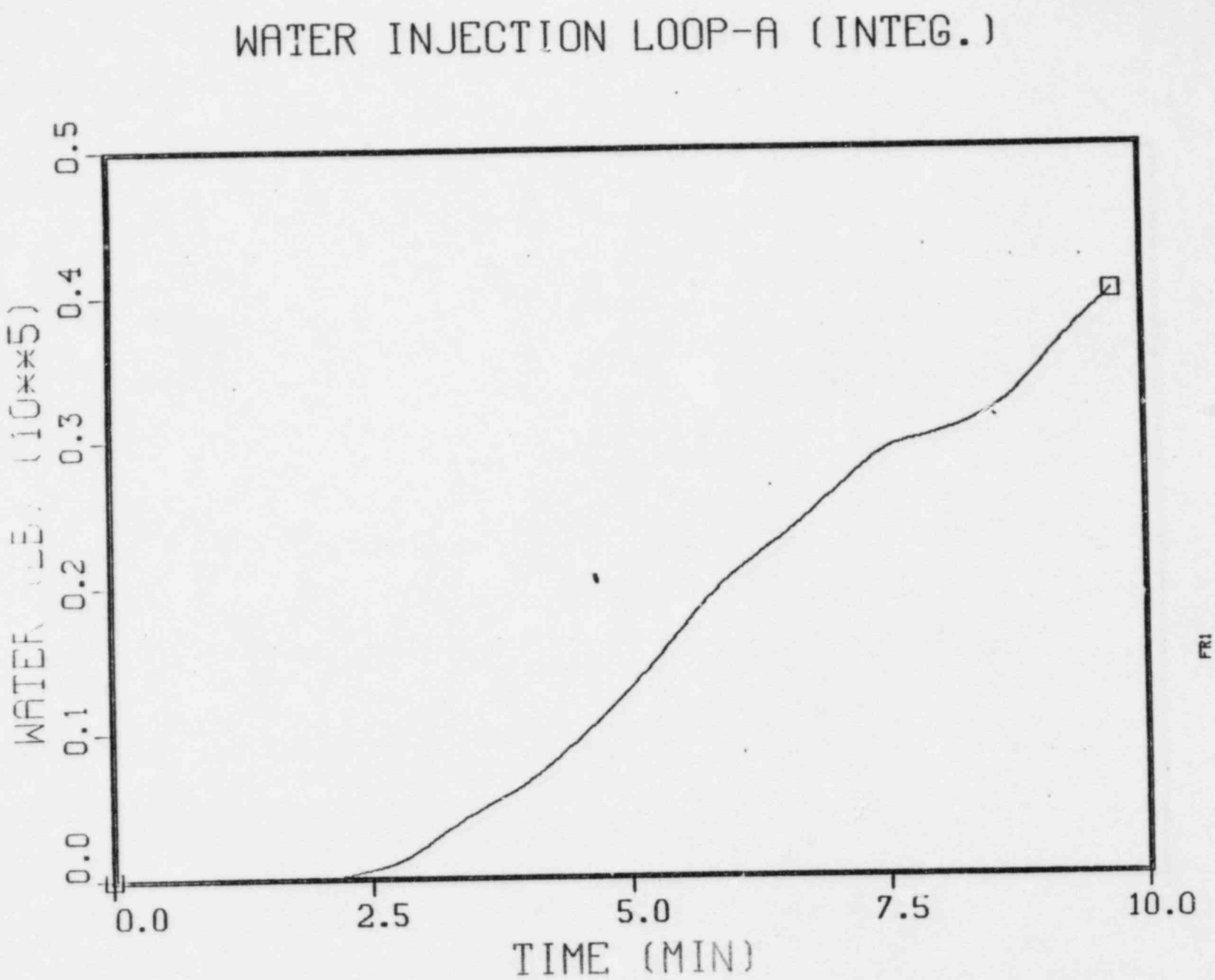


Fig. 4.2.6 Class 2 water injection into steam line A

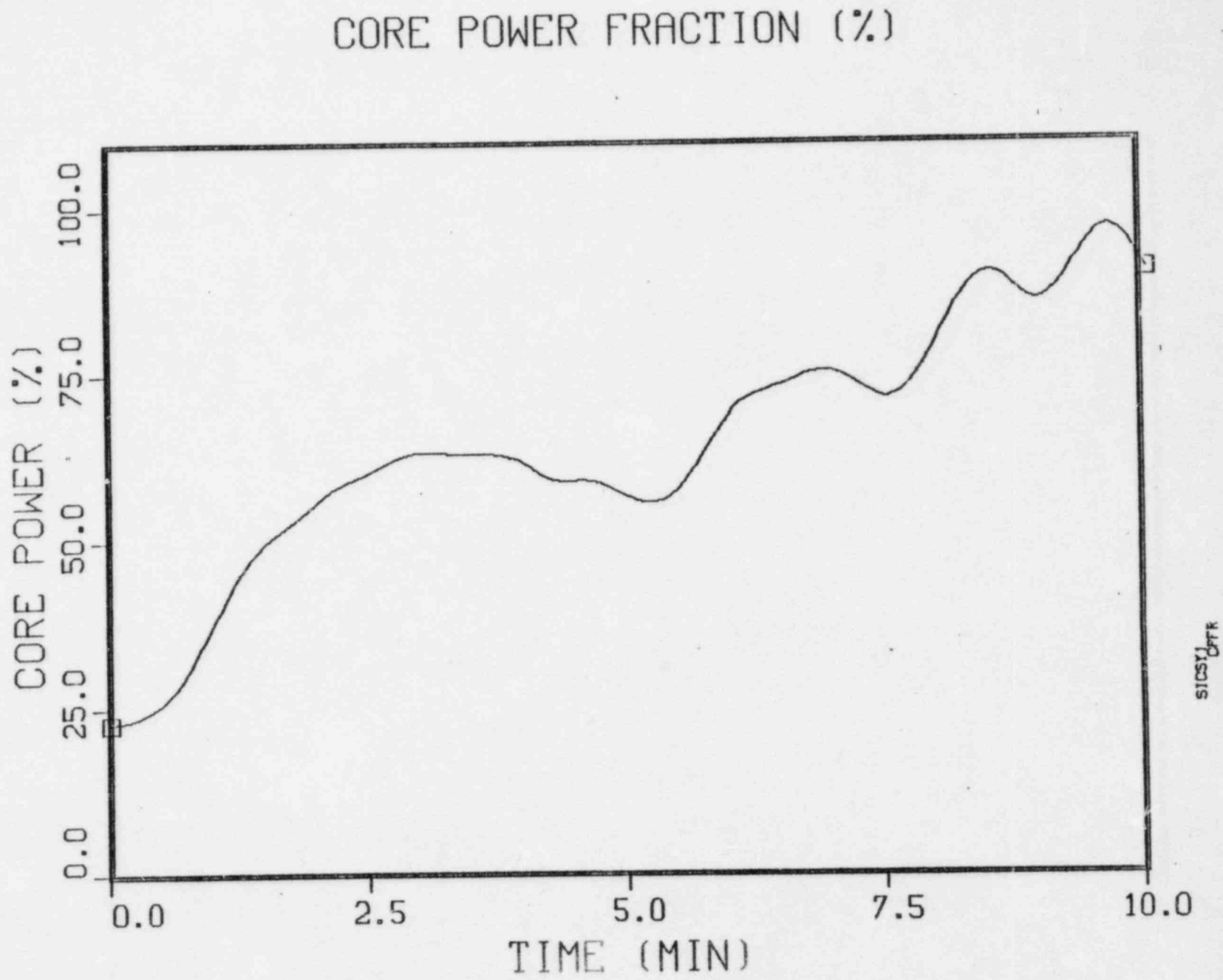


Fig: 4.2.7 Class 3 core power fraction

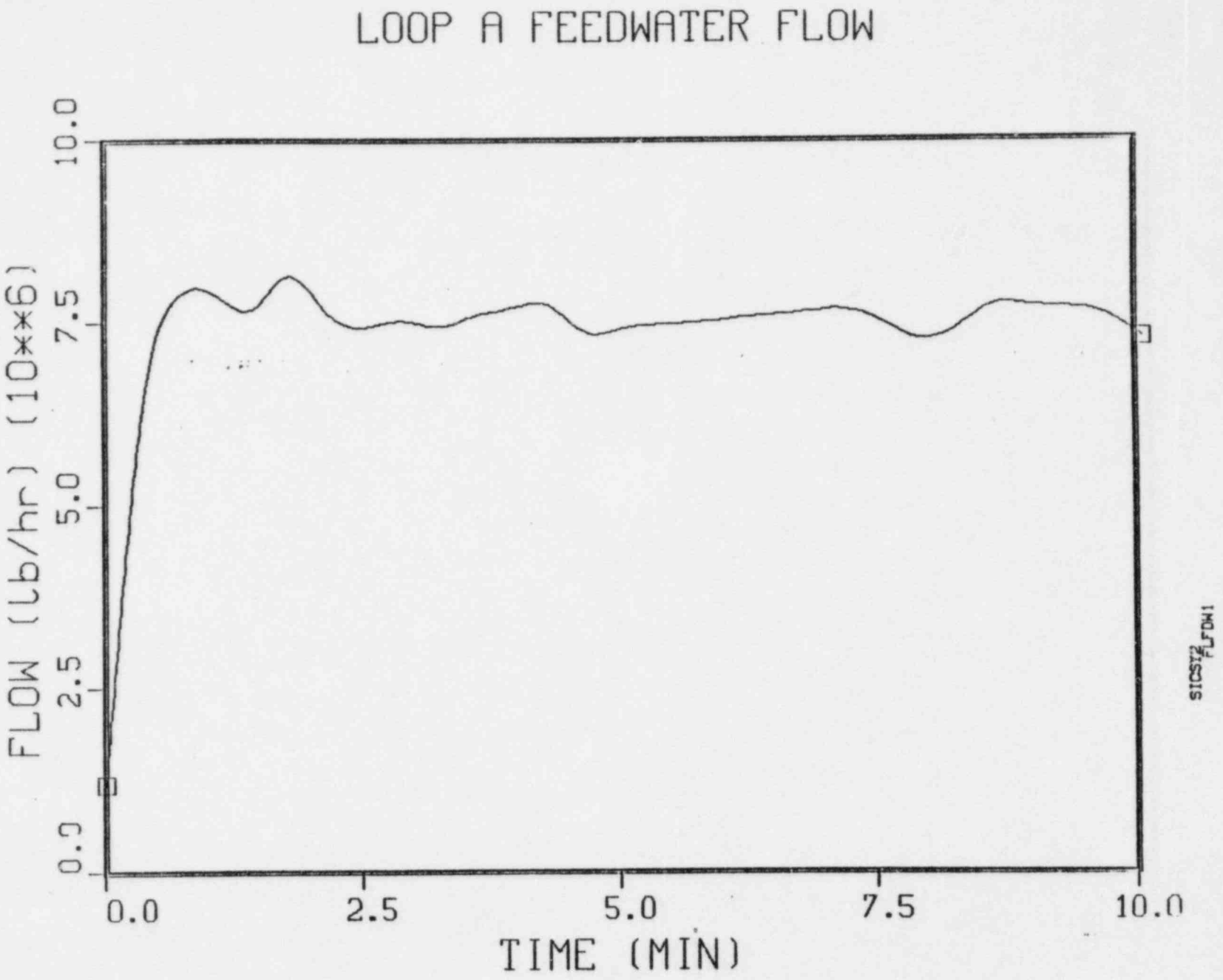


Fig. 4.2.8 Class 5 (20% power) steam generator A feedwater flow

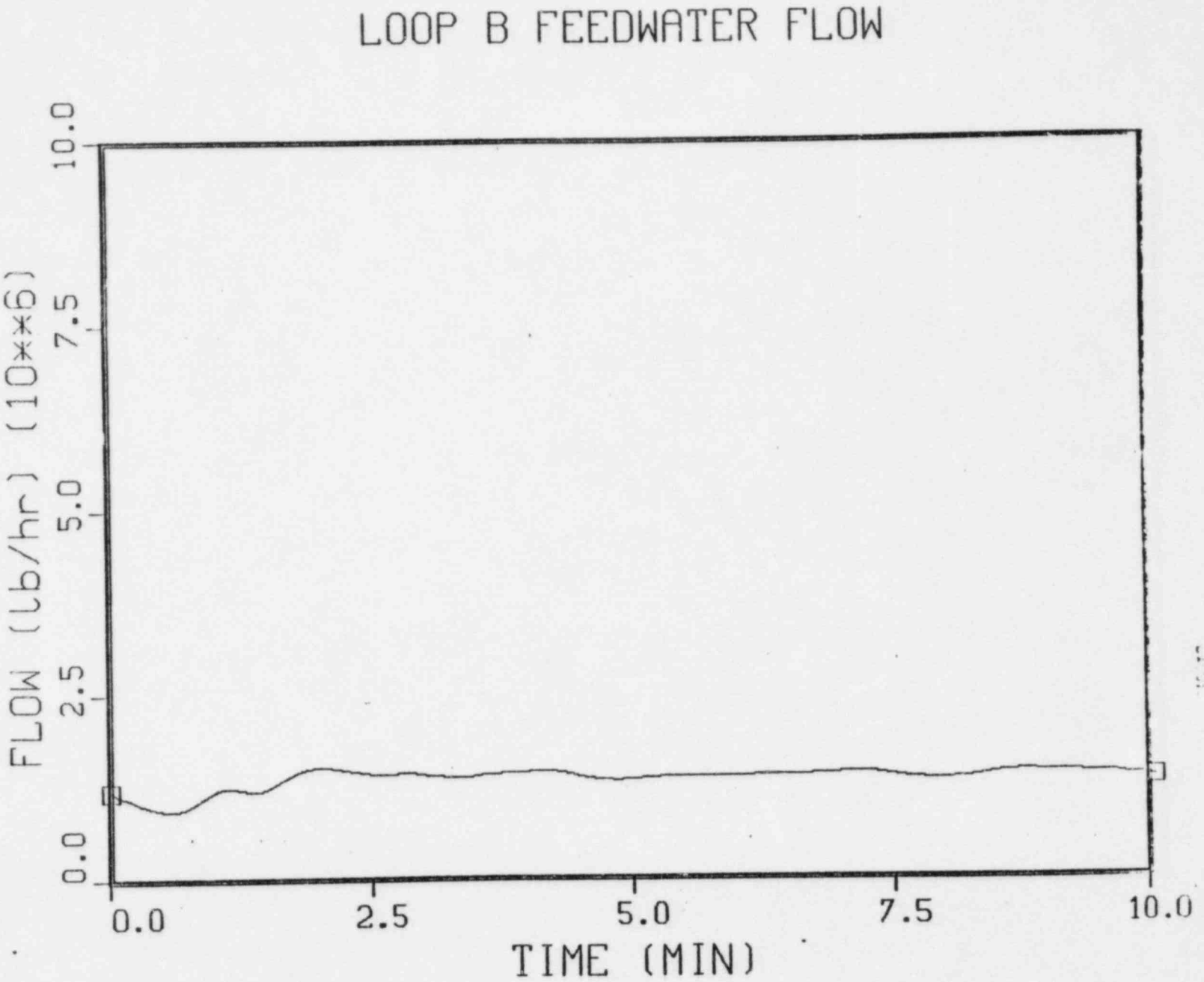


Fig 4.2.9 Class 5 (20% power) steamgenerator B feedwater flow

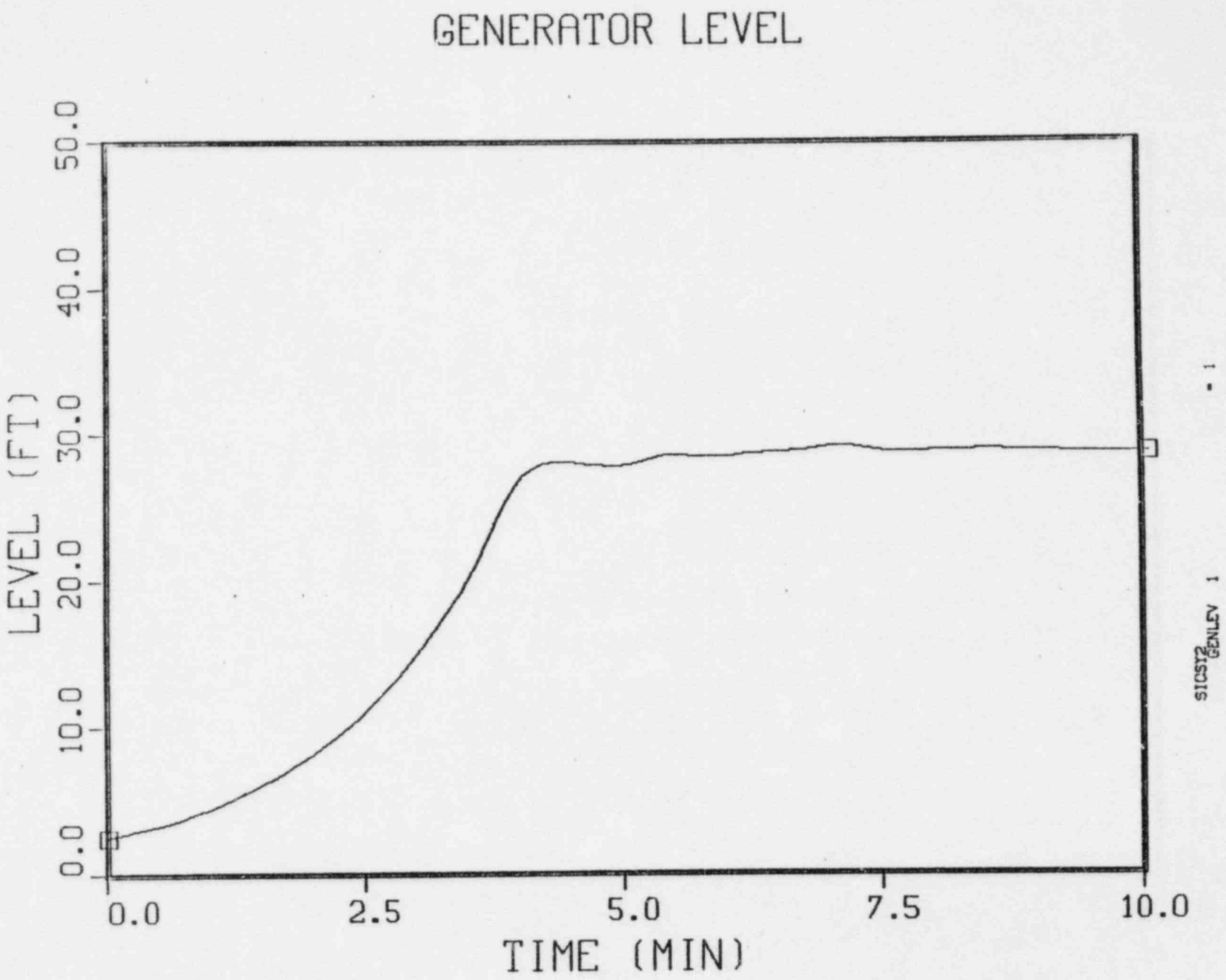


Fig. 4.2.10 Class 5 (20% power) steam generator A water level

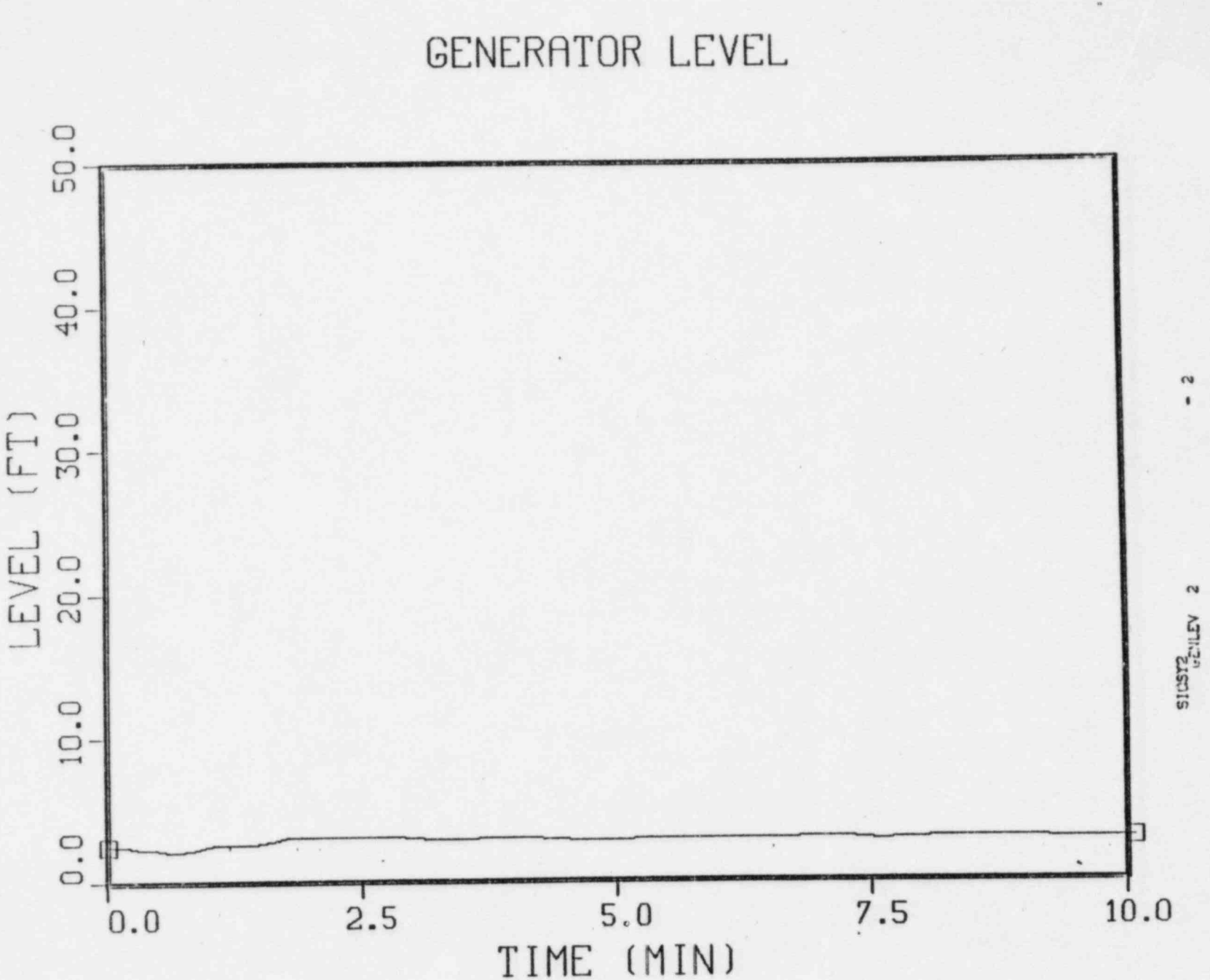


Fig. 4.2.11 Class 5 (20% power) steam generator B water level

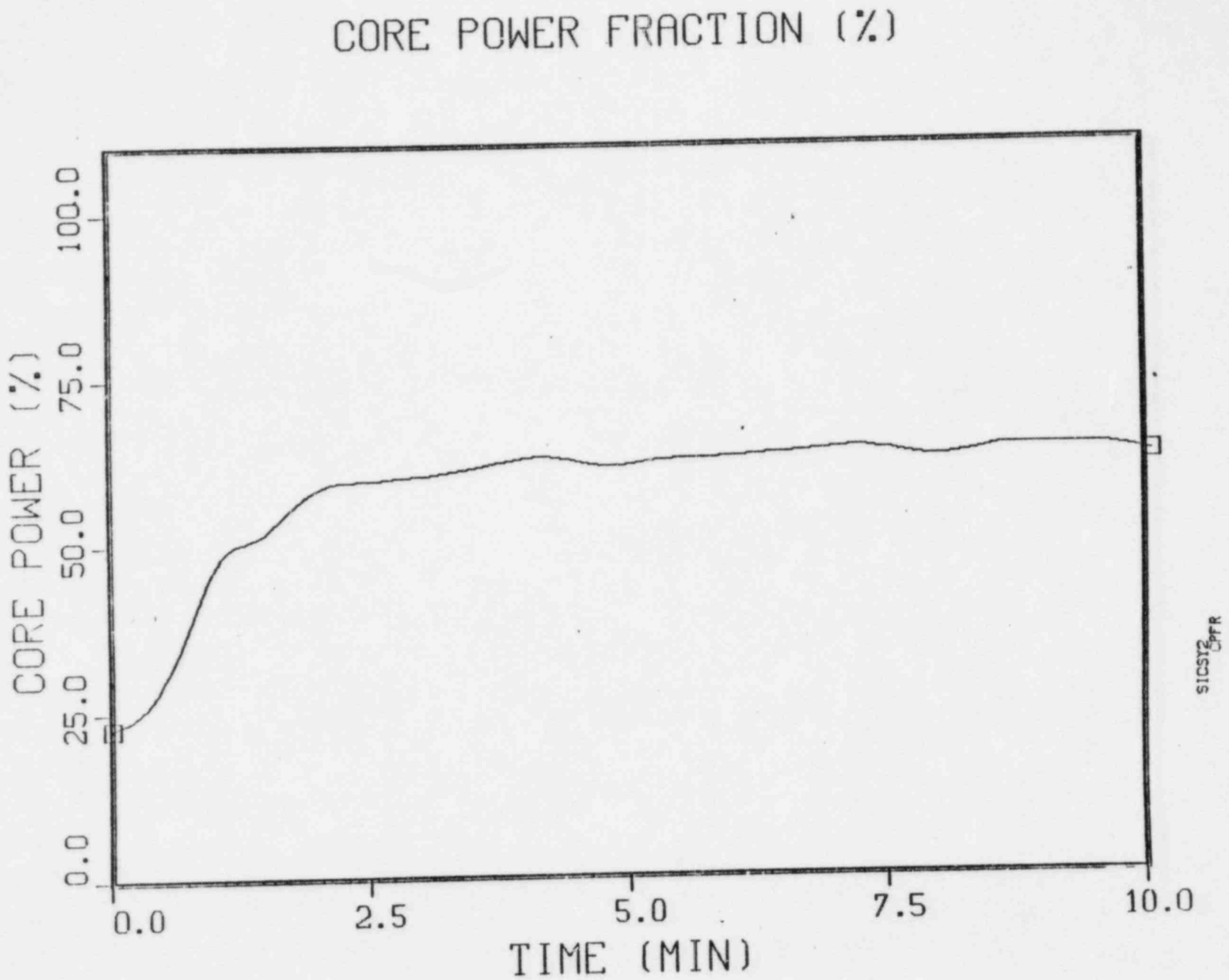


Fig. 4.2.12 Class 5 (20% power) core power fraction

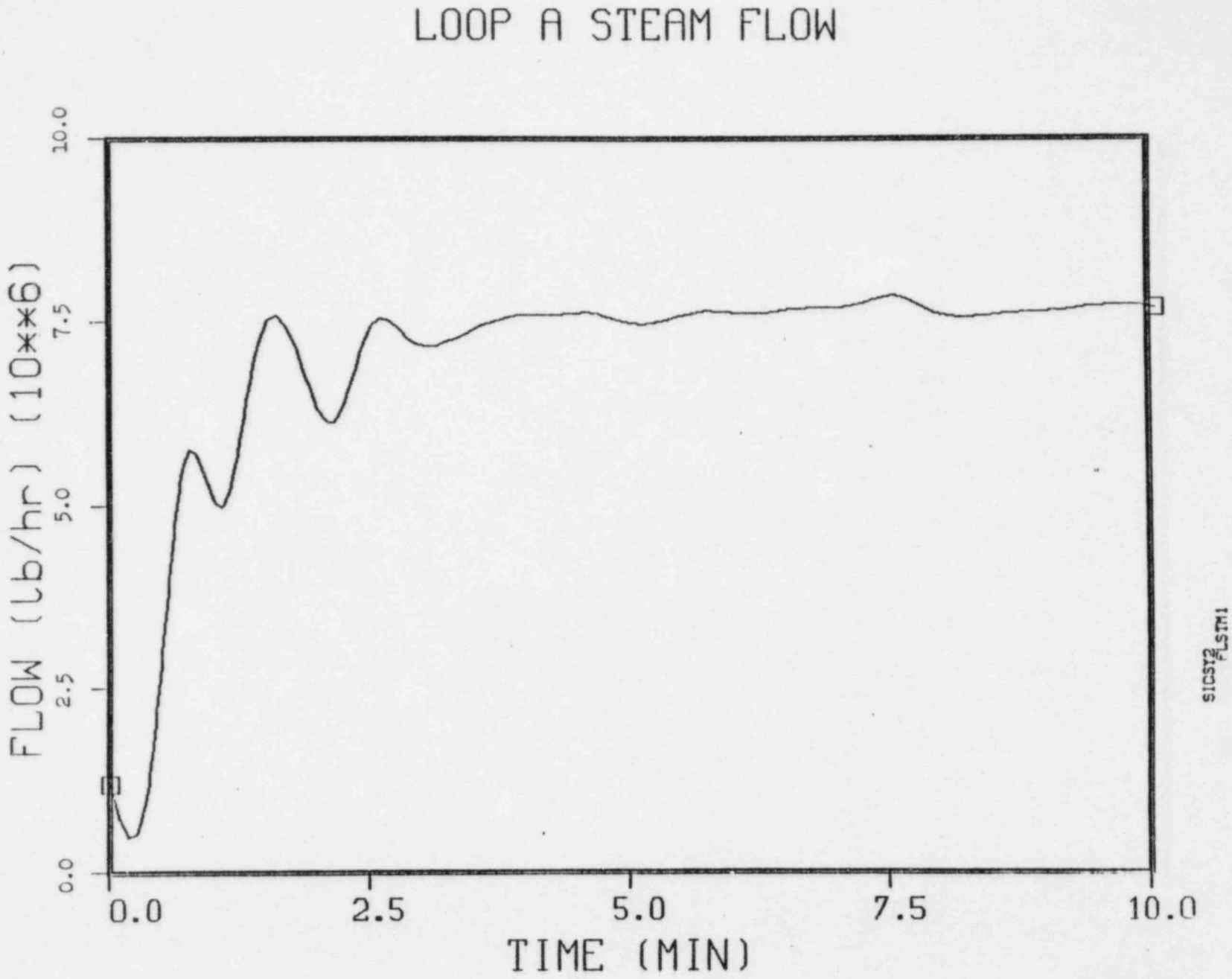


Fig. 4.2.13 Class 5 (20% power) steam generator A steam flow

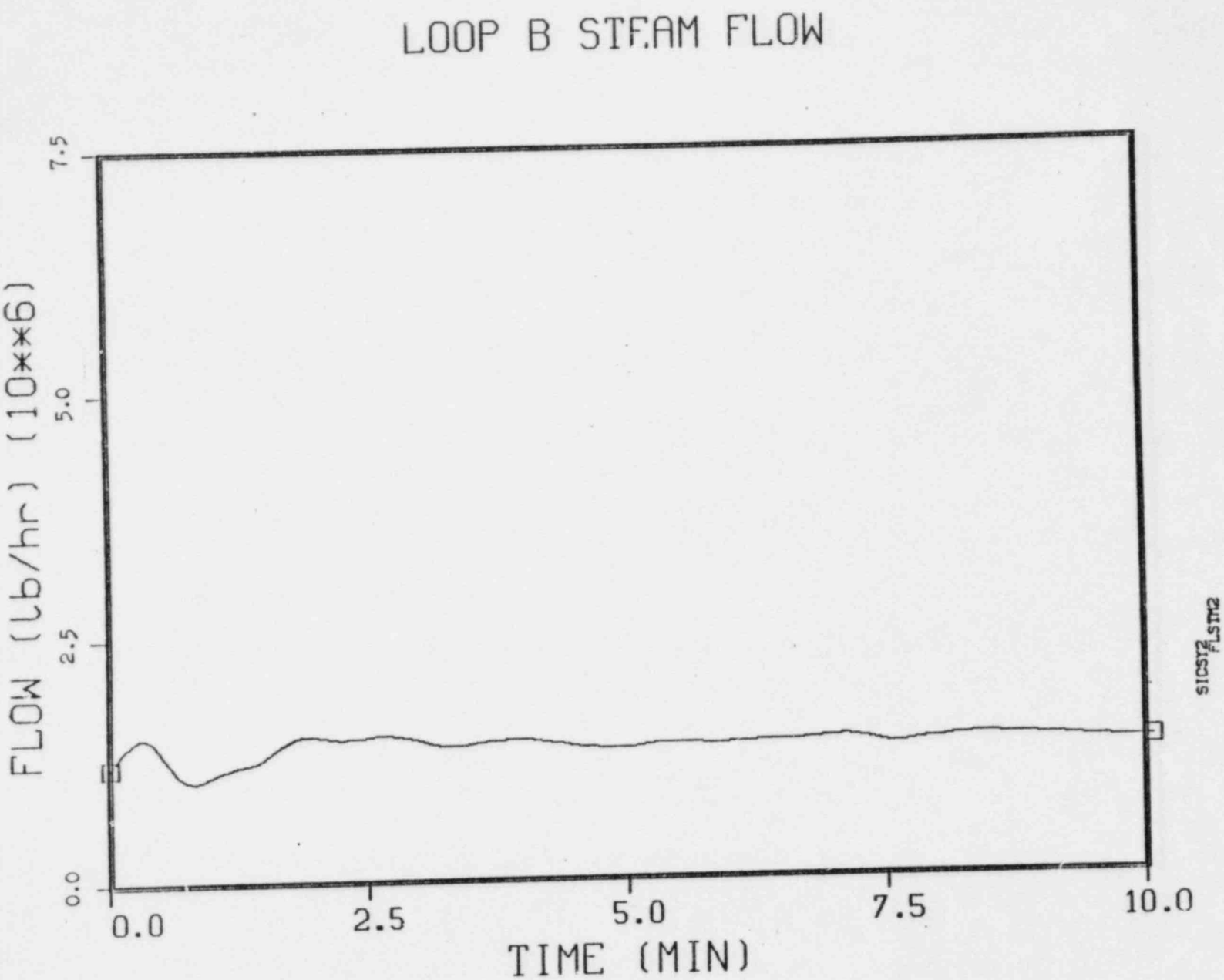


Fig. 4.2.14 Class 5 (20% power) steam generator B steam flow

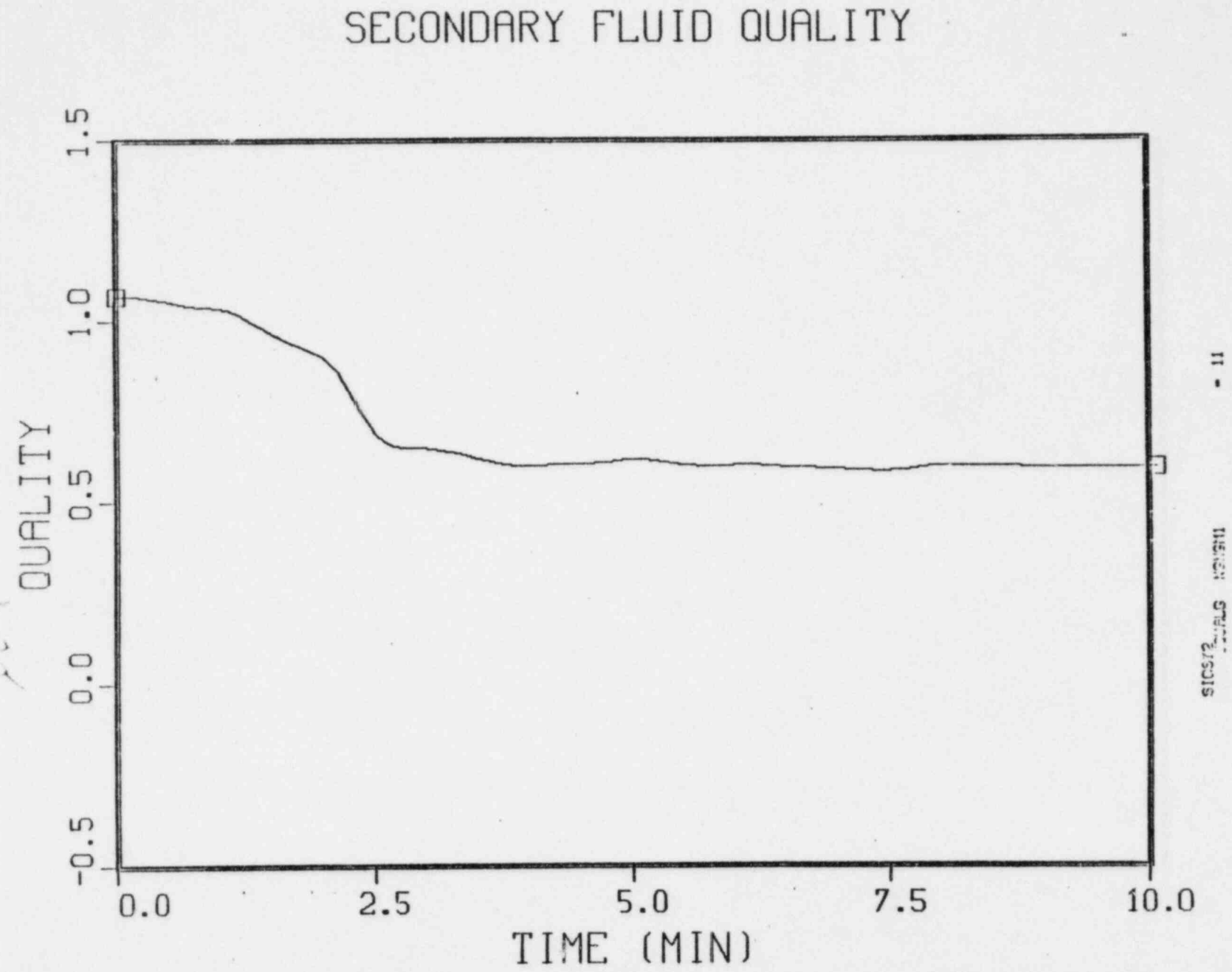


Fig. 4.2.15 Class 5 (20% power) steam generator A outlet quality

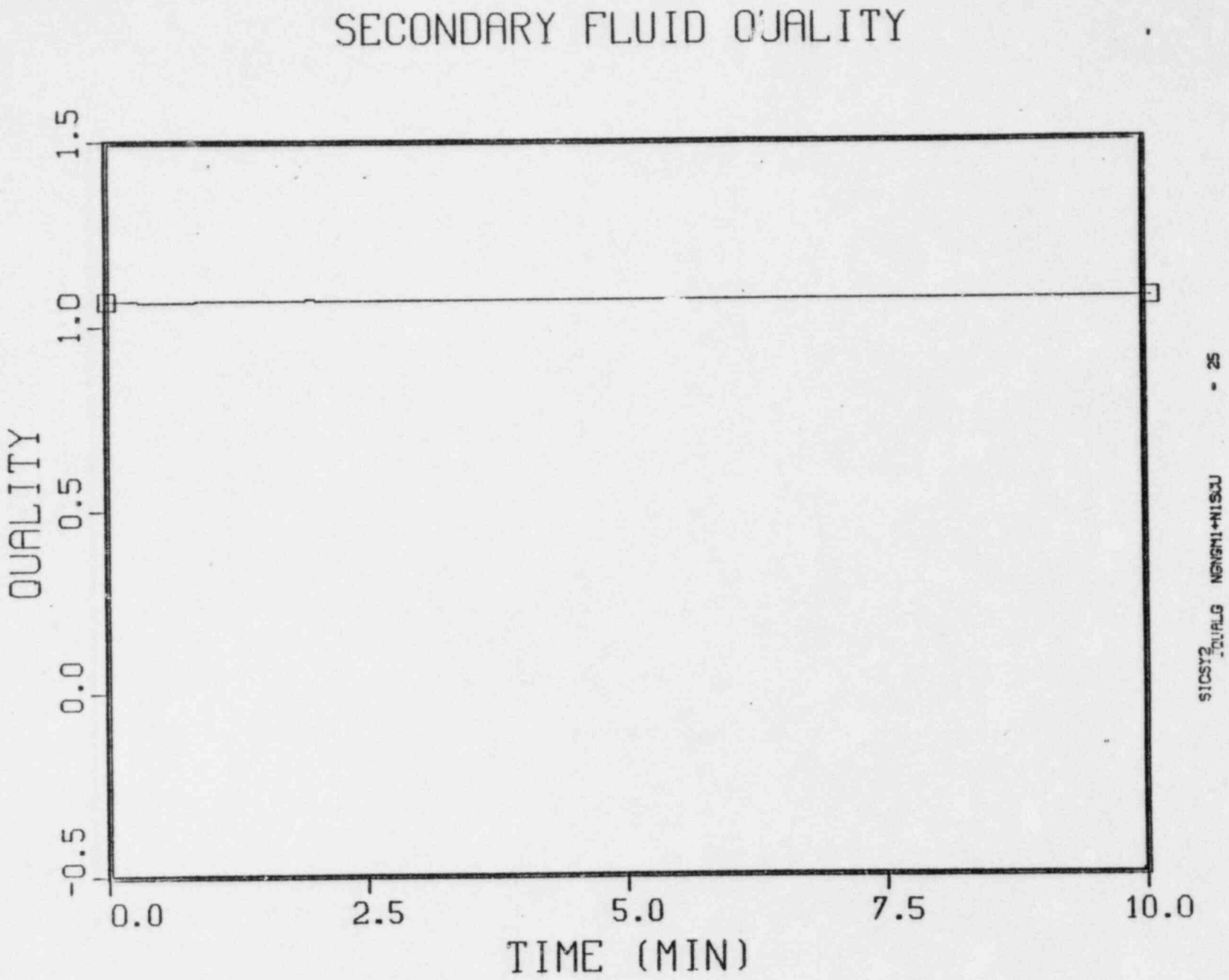


Fig. 4.2.16 Class 5 (20% power) steam generator B outlet quality

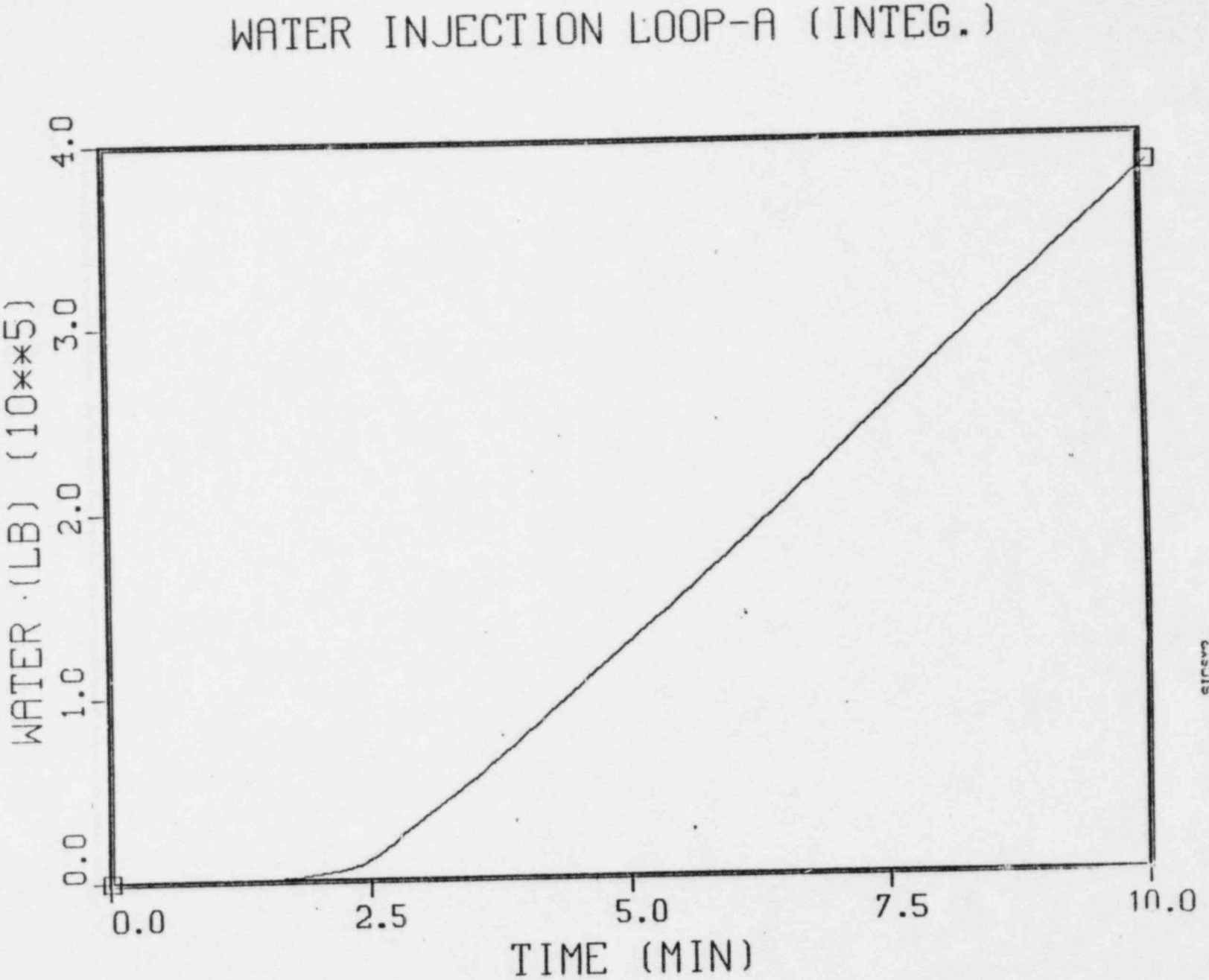


Fig 4.2.17 Class 5 (20% power) water injection into steam line A

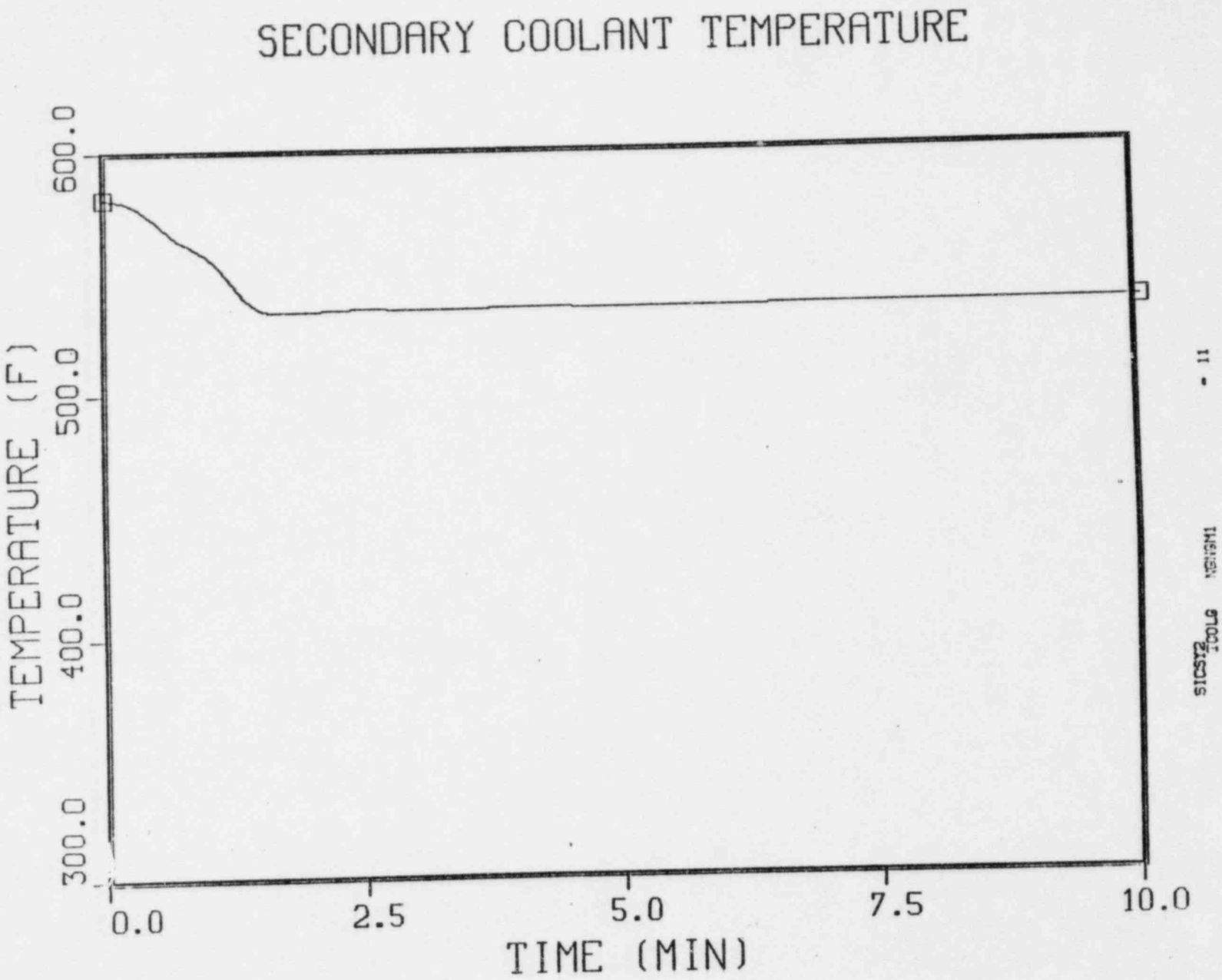


Fig 4.2.18 Class 5 (20% power) steam generator A outlet temperature

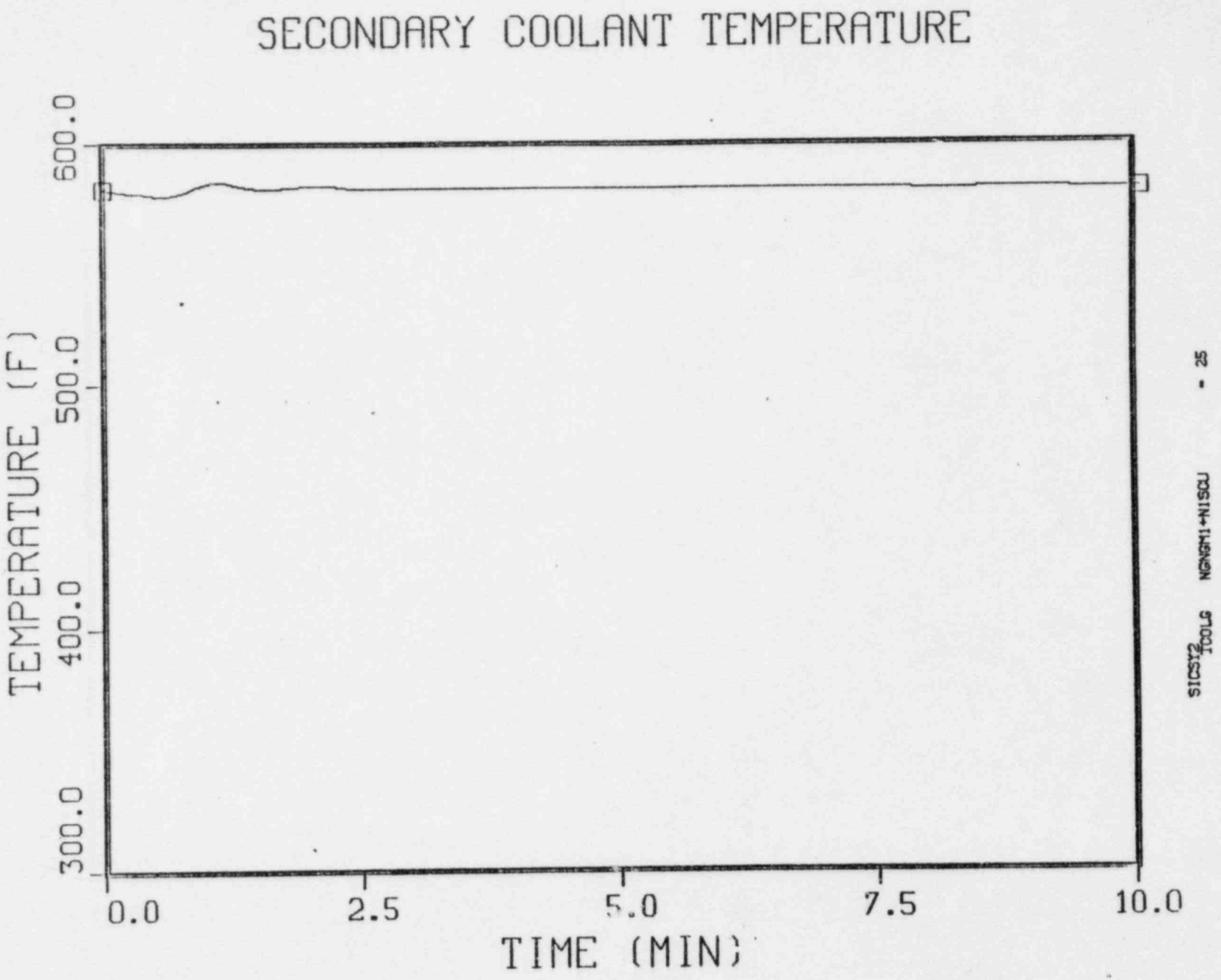


Fig. 4.2.19 Class 5 (20% power) steam generator B outlet temperature

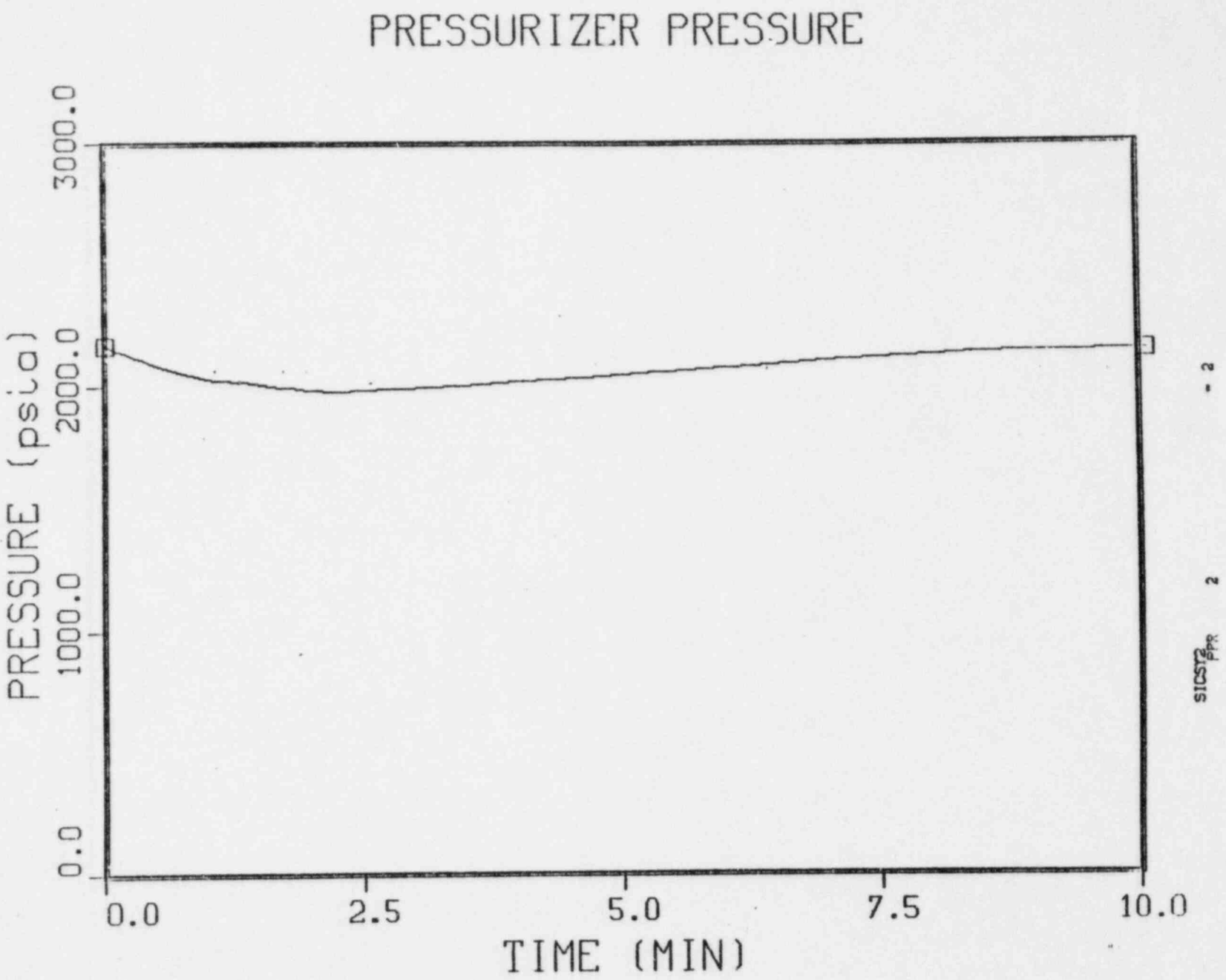


Fig. 4.2.20 Class 5 (20% power) pressurizer pressure

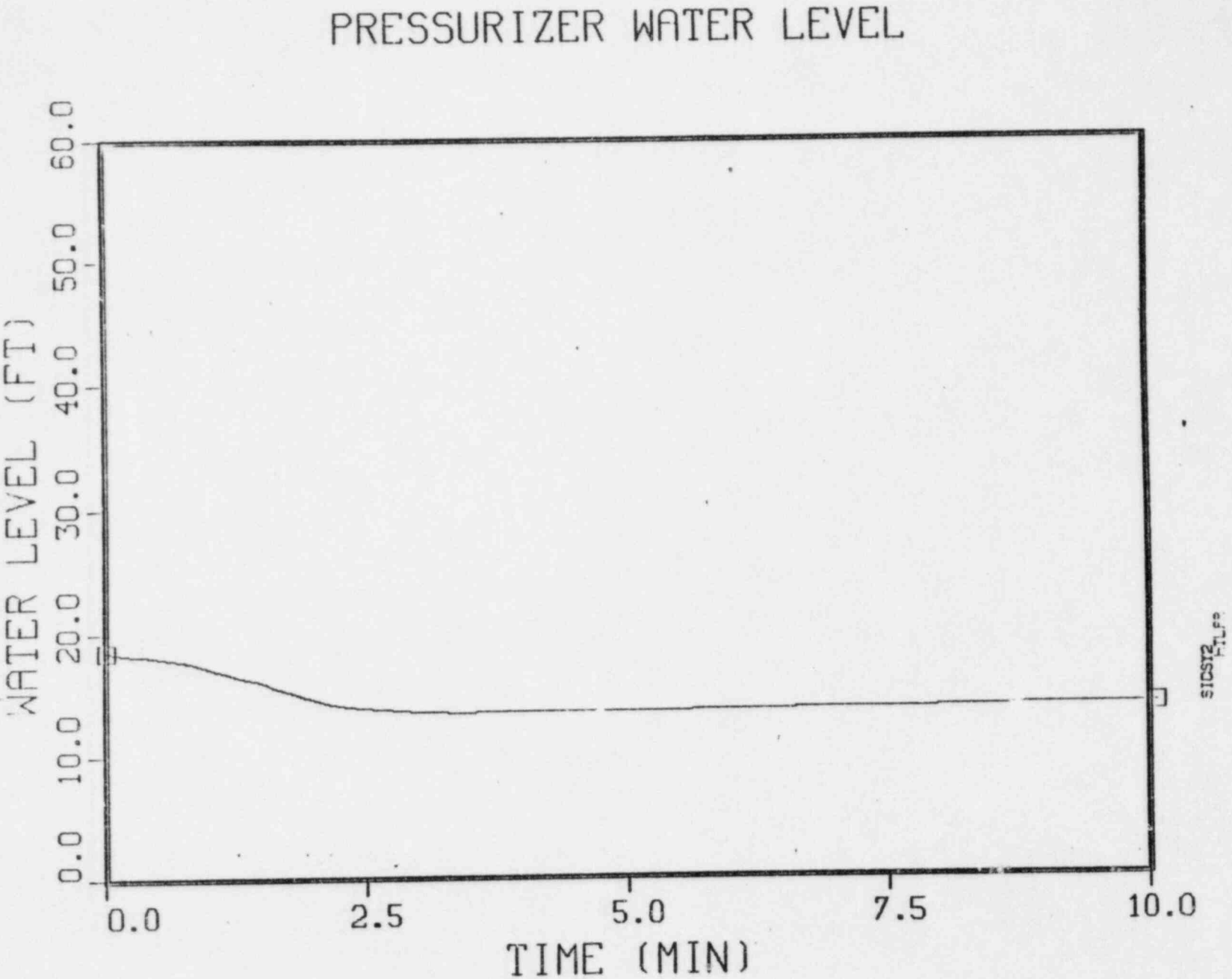


Fig. 4.2.21 Class 5 (20% power) pressurizer level

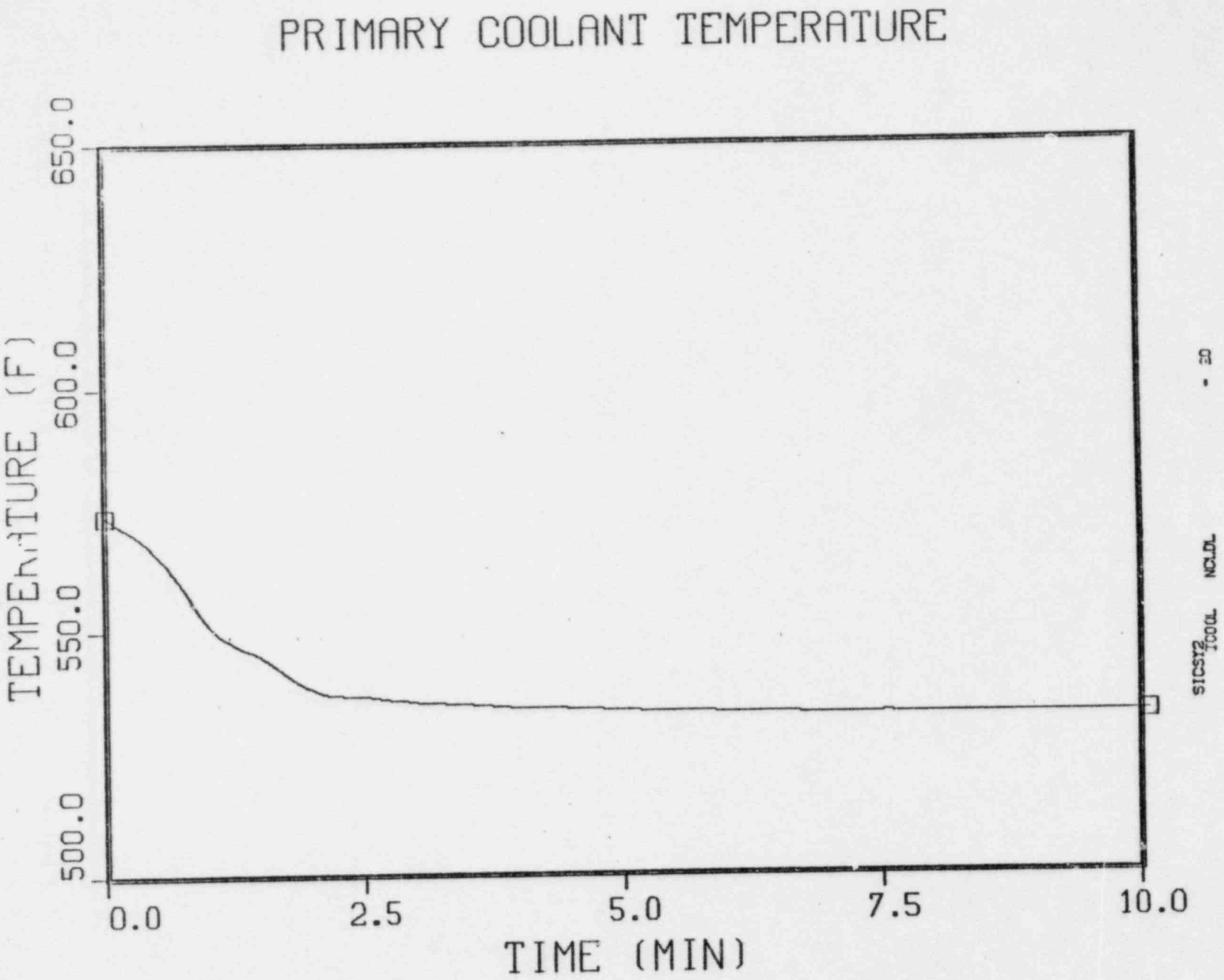


Fig. 4.2.22 Class 5 (20% power) loop A cold leg temperature

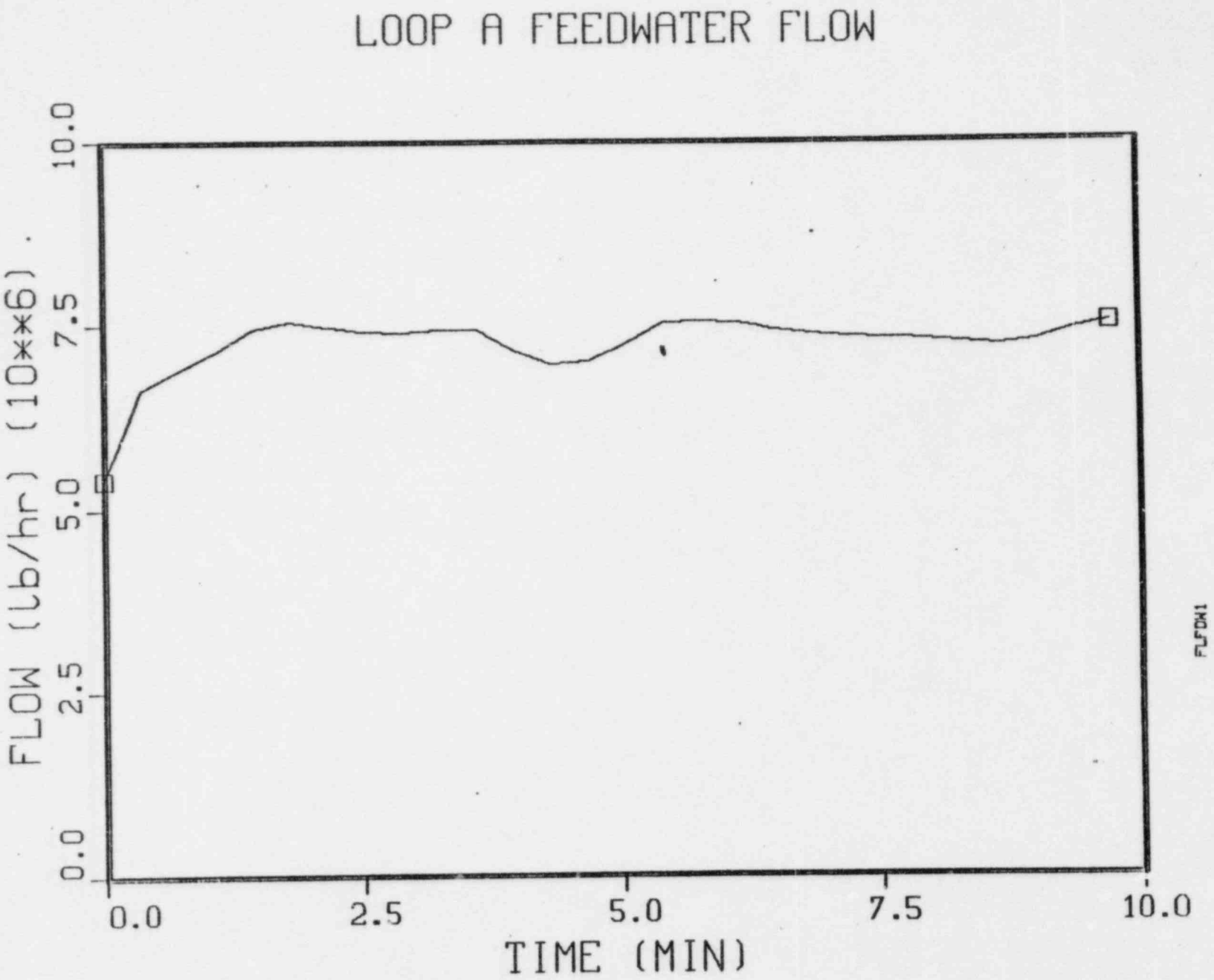


Fig. 4.2.23 Class 5 (100% power) steam generator A feedwater flow

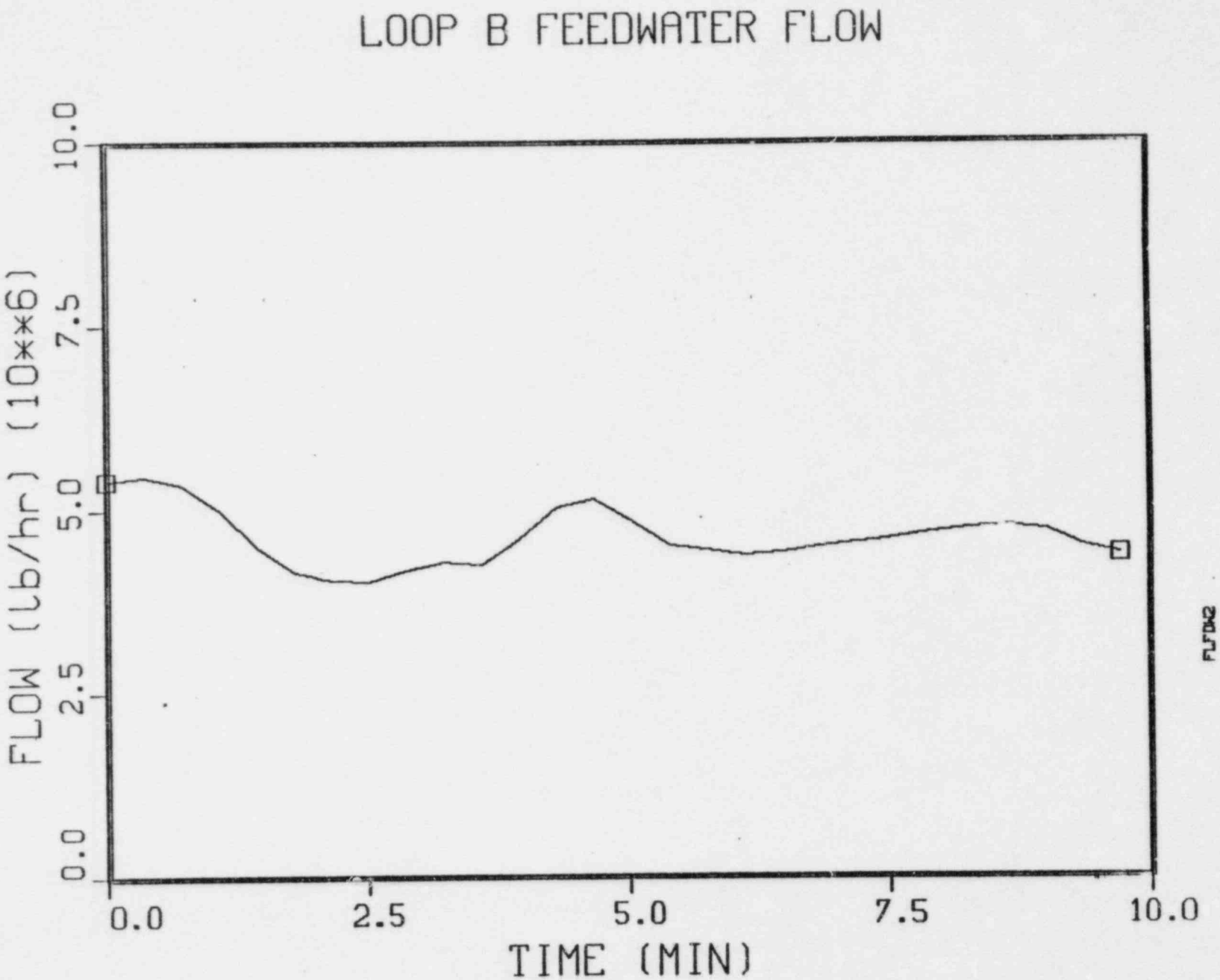


Fig. 4.2.24 Class 5 (100% power) steam generator B feedwater flow

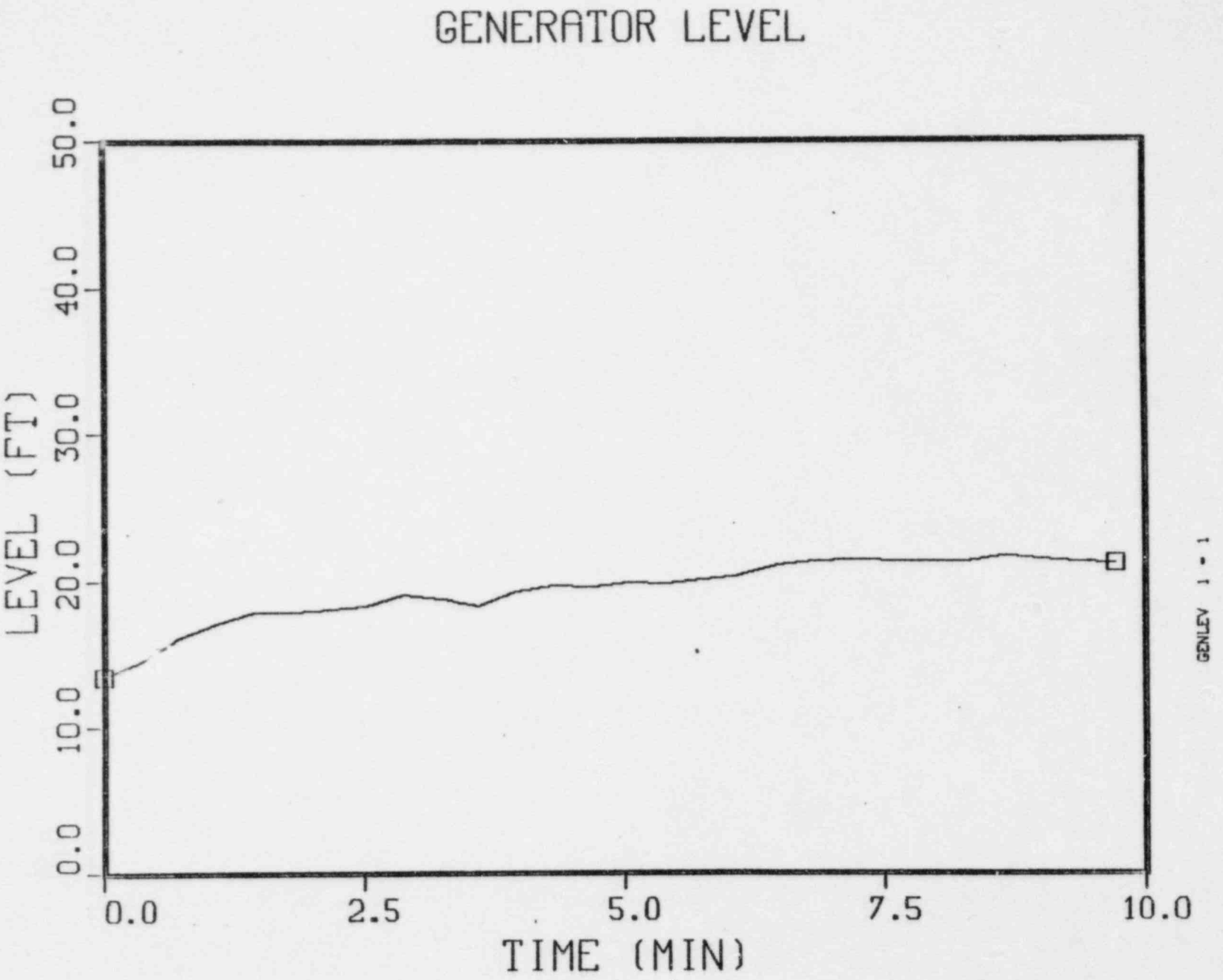


Fig 4.2.25 Class 5 (100% power) steam generator A water level

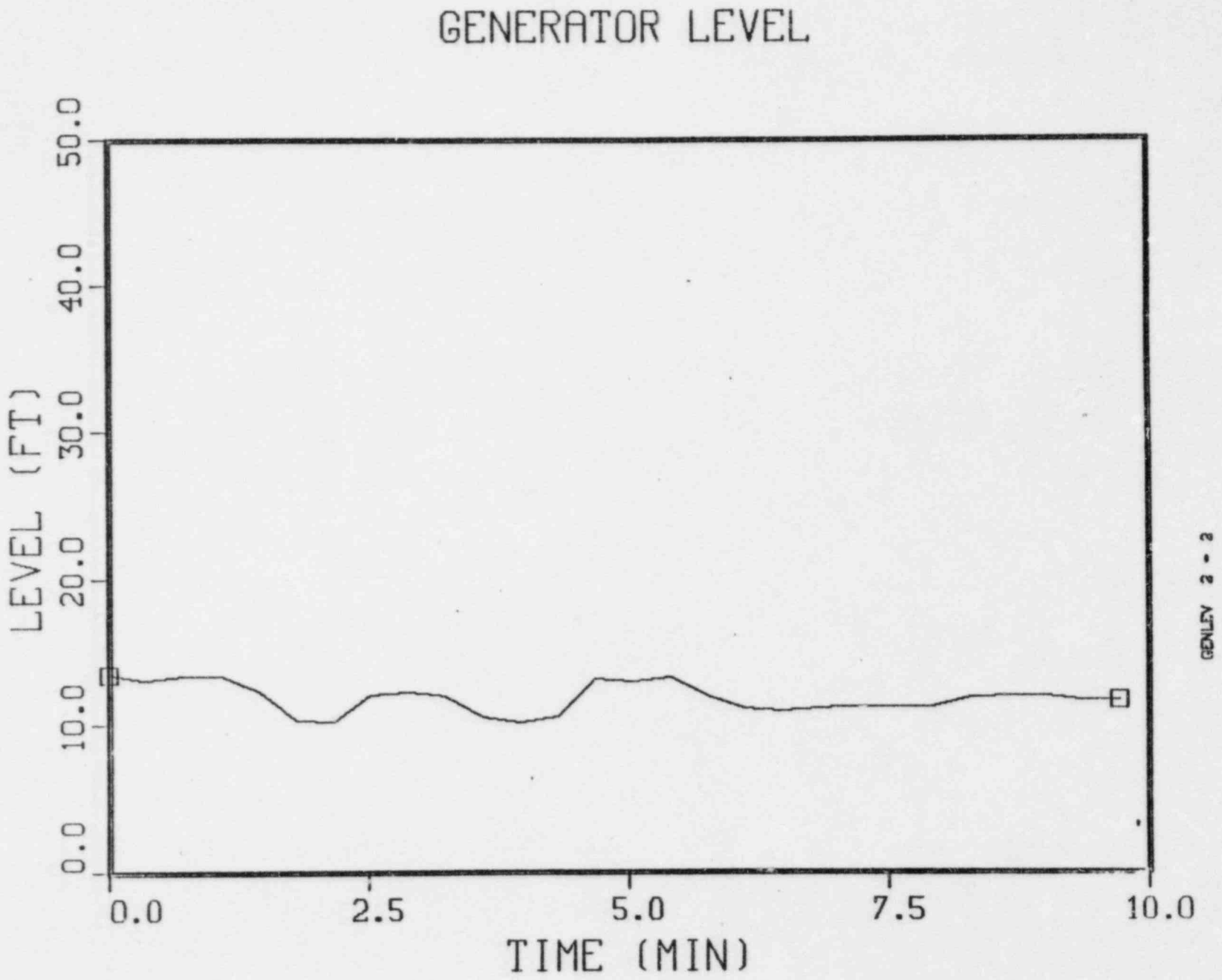


Fig. 4,2.26 Class 5 (100% power) steam generator B water level

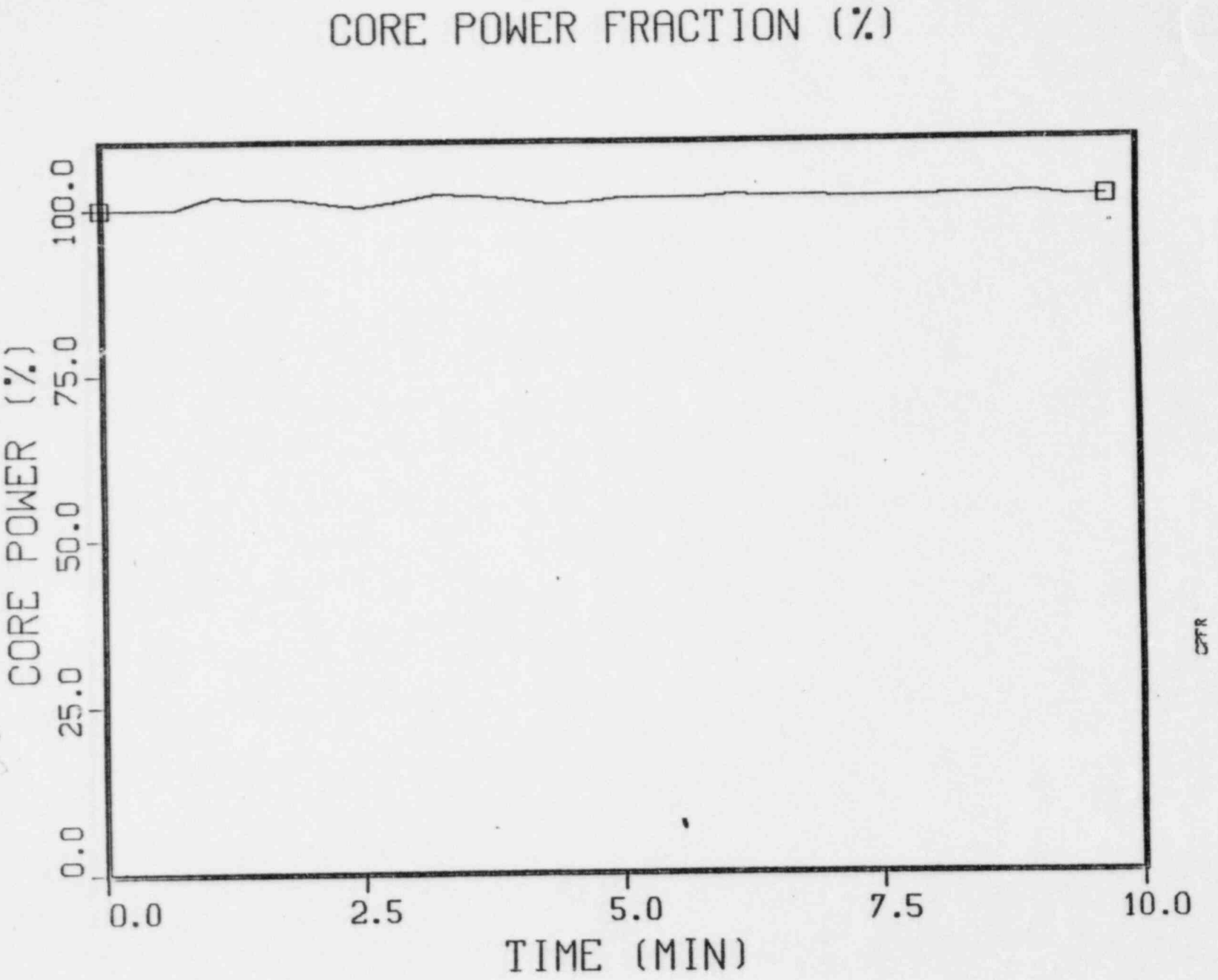


Fig. 4.2.27 Class 5 (100% power) core power

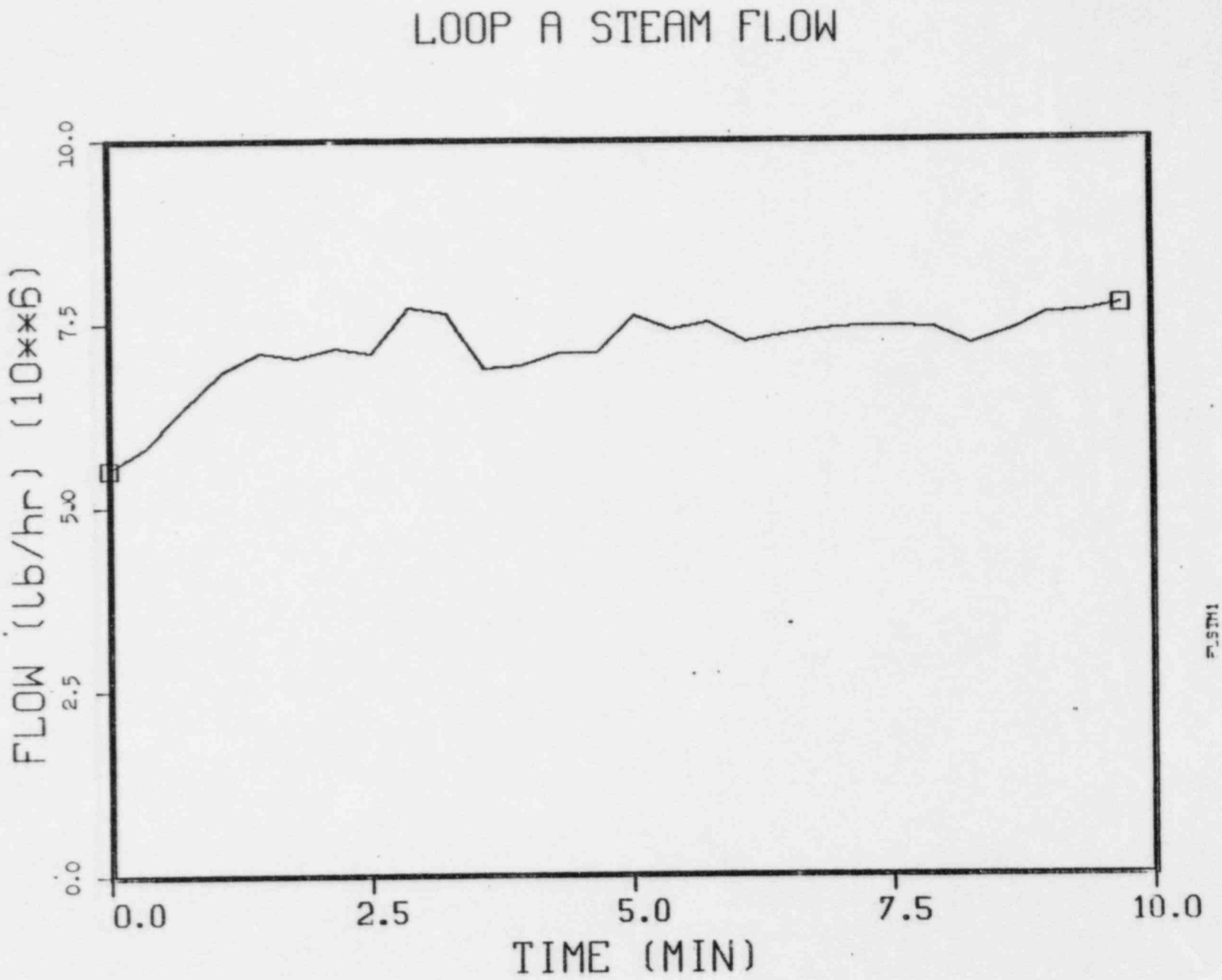


Fig. 4.2.28 Class 5 (100% power) steam generator A steam flow

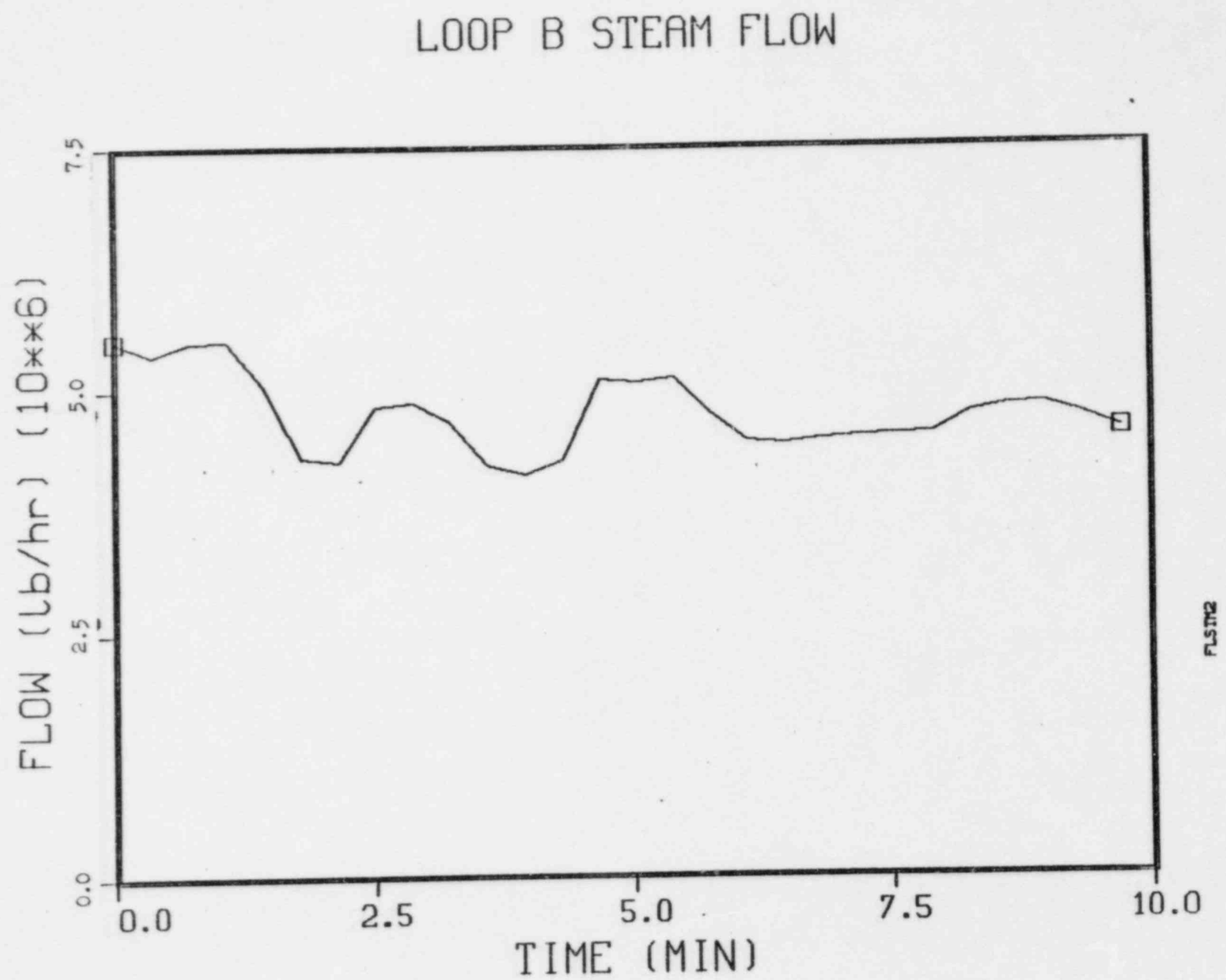


Fig. 4.2.29 Class 5 (100% power) steam generator B steam flow

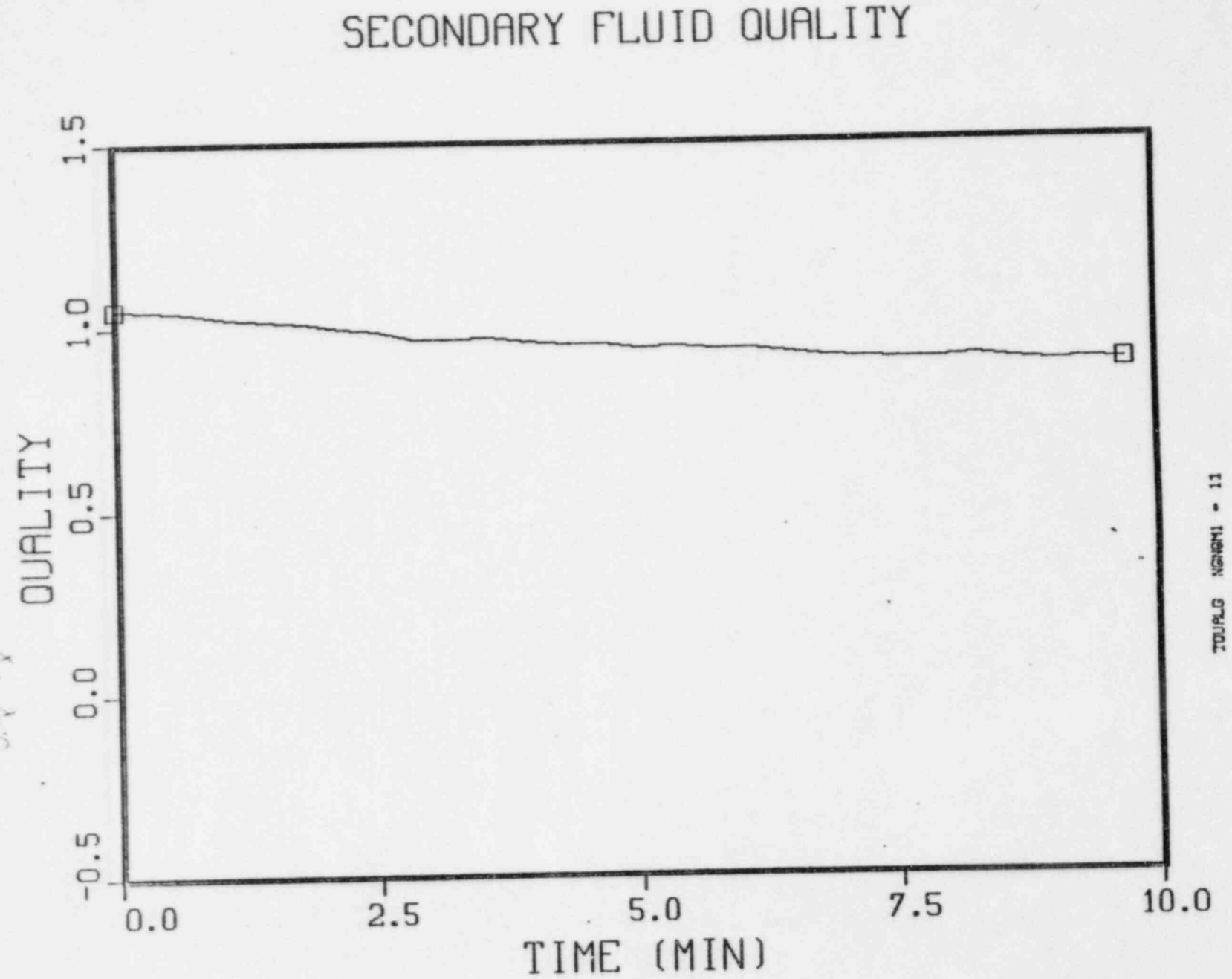


Fig. 4.2.30 Class 5 (100% power) steam generator A outlet quality

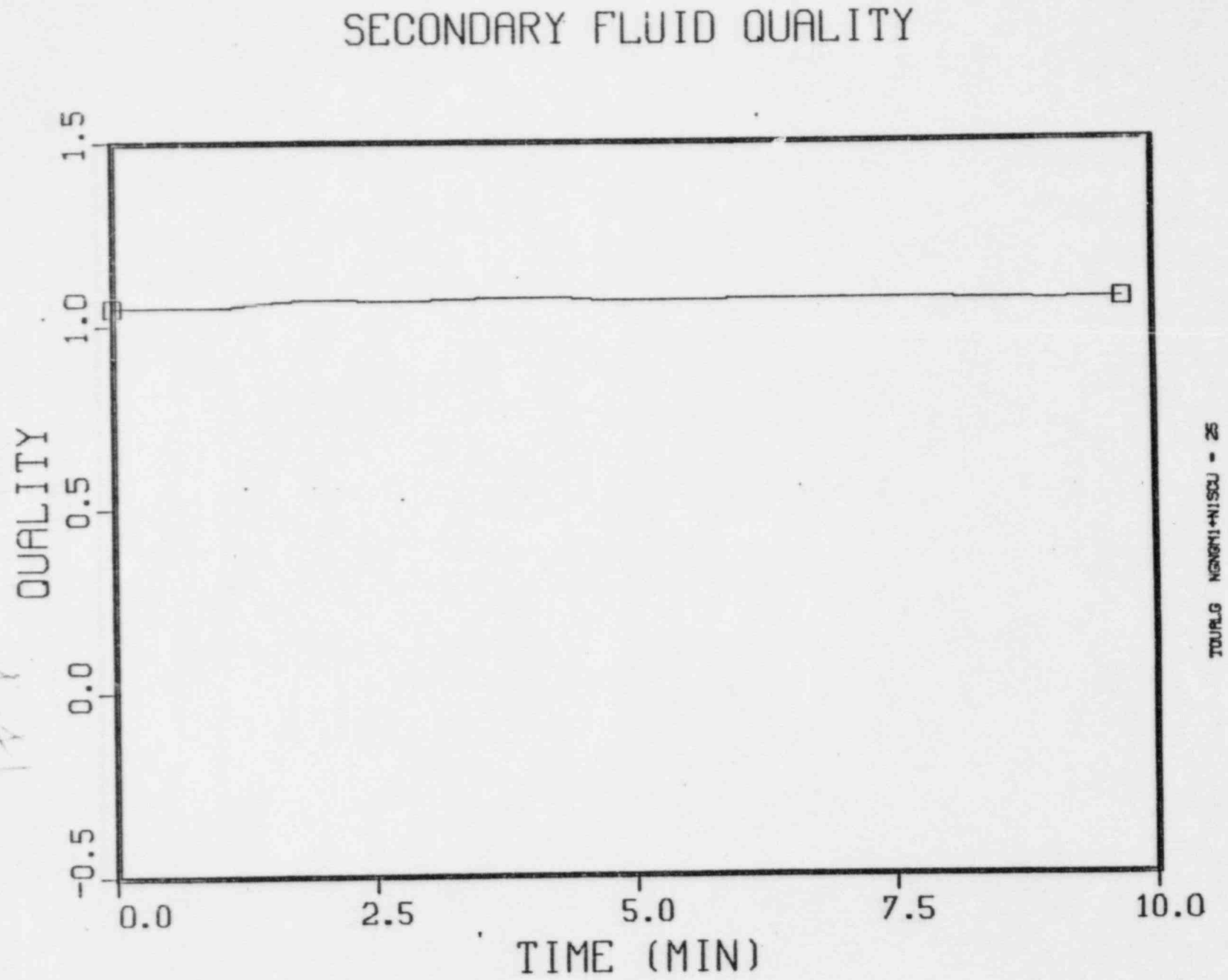


Fig. 4.2.31 Class 5 (100% power) steam generator B outlet quality

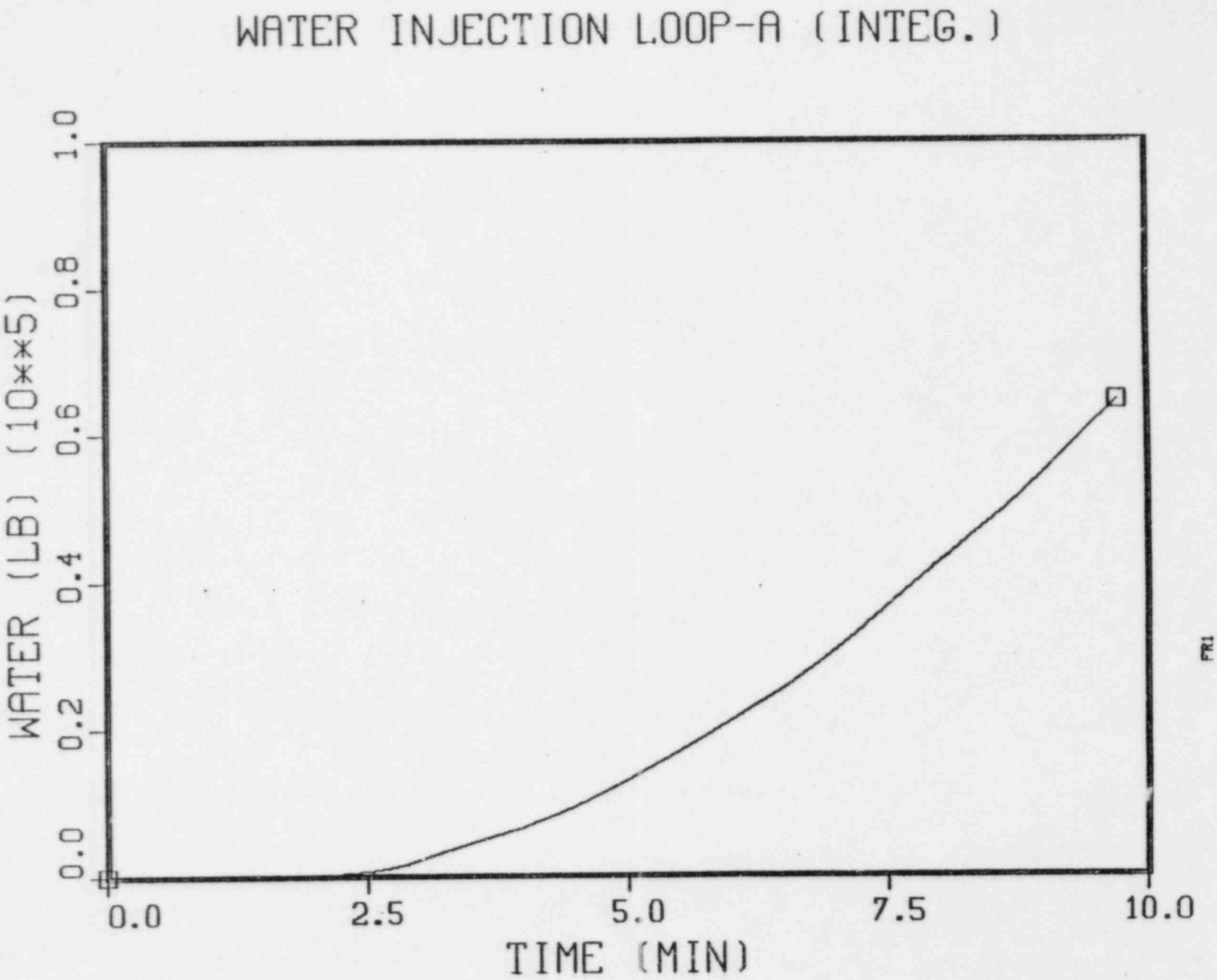


Fig. 4.2.32 Class 5 (100% power) water injection into steam line A

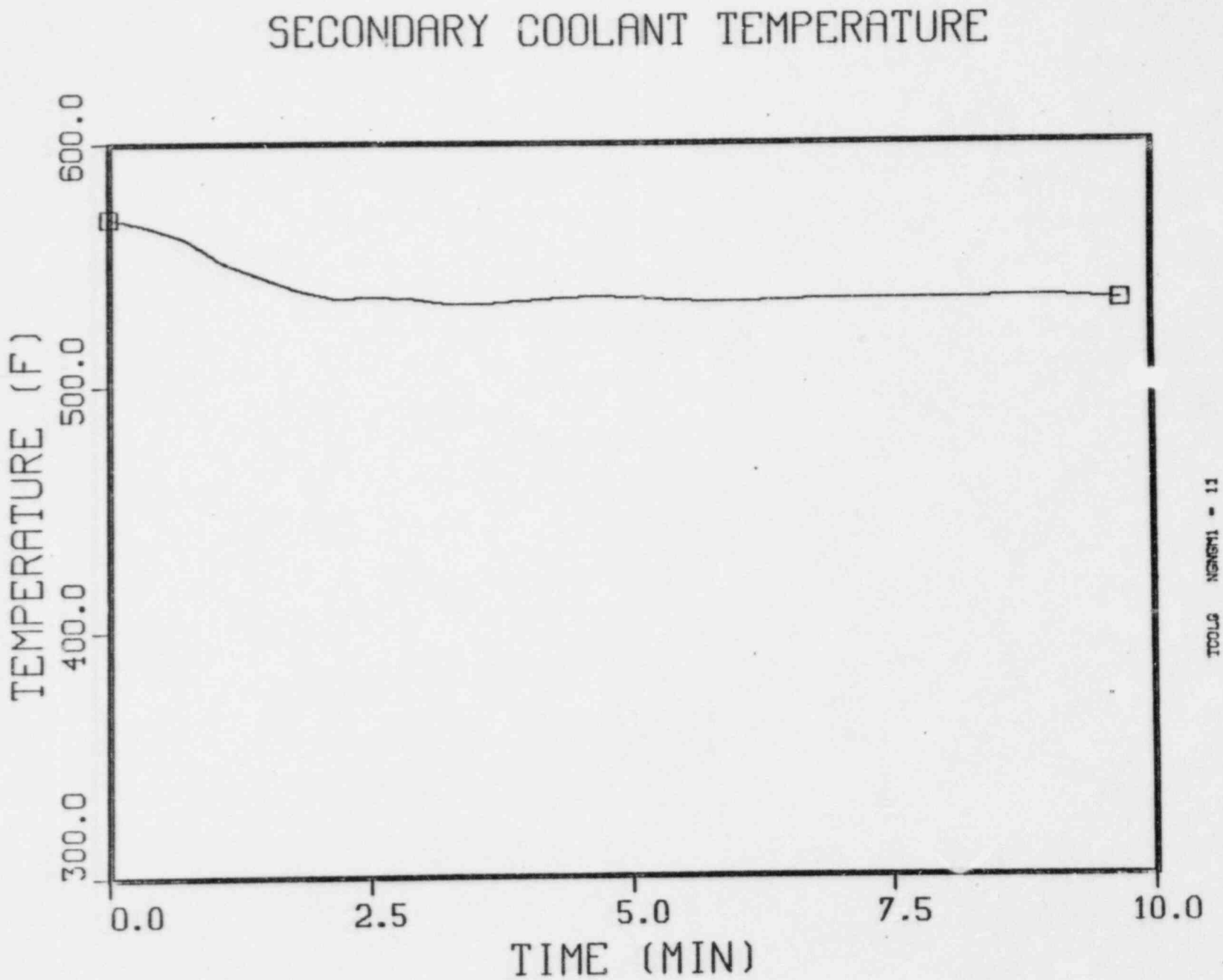


Fig 4.2.33 Class 5 (100% power) steam generator A outlet temperature

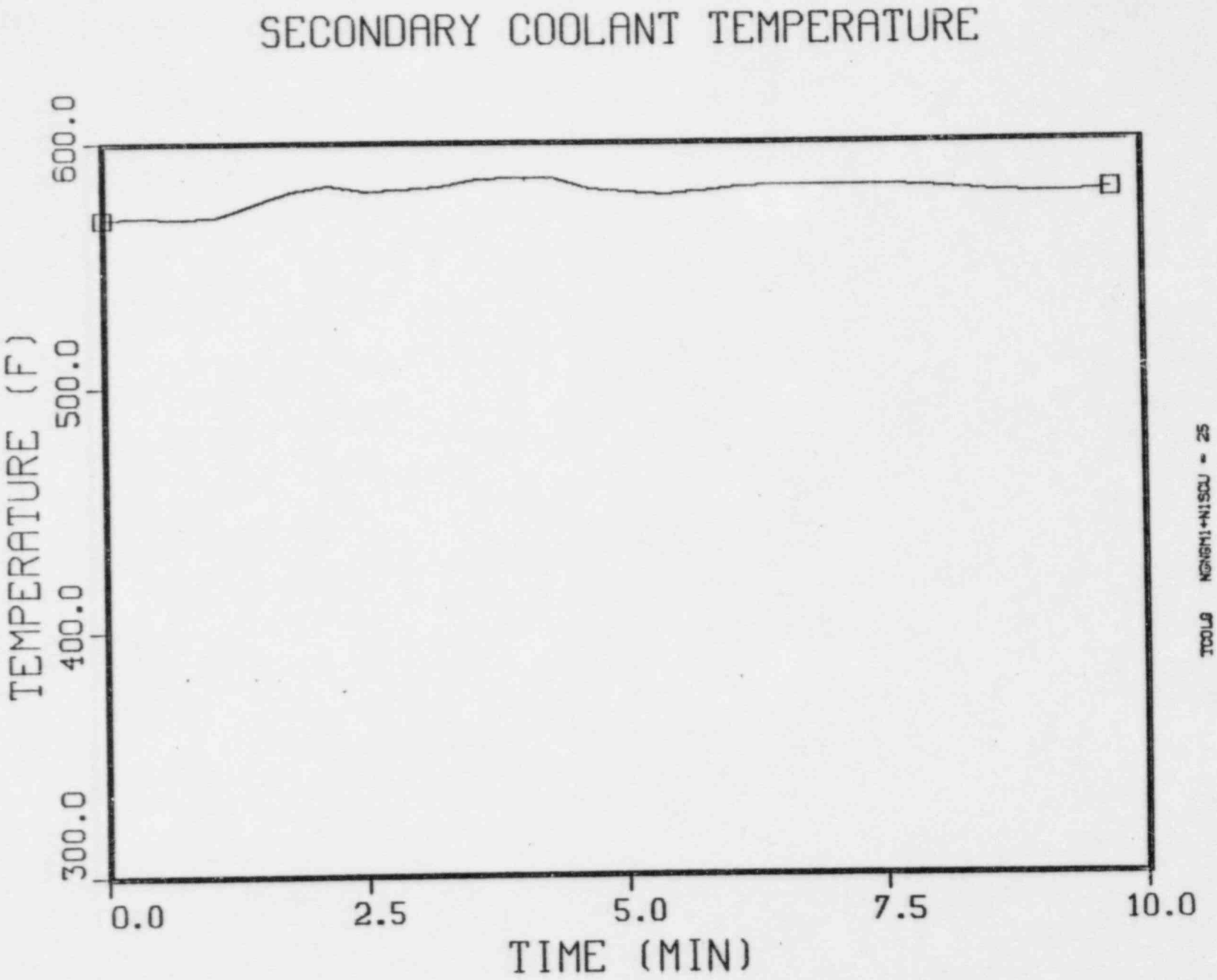


Fig. 4.2.34 Class 5 (100% power) steam generator B outlet temperature

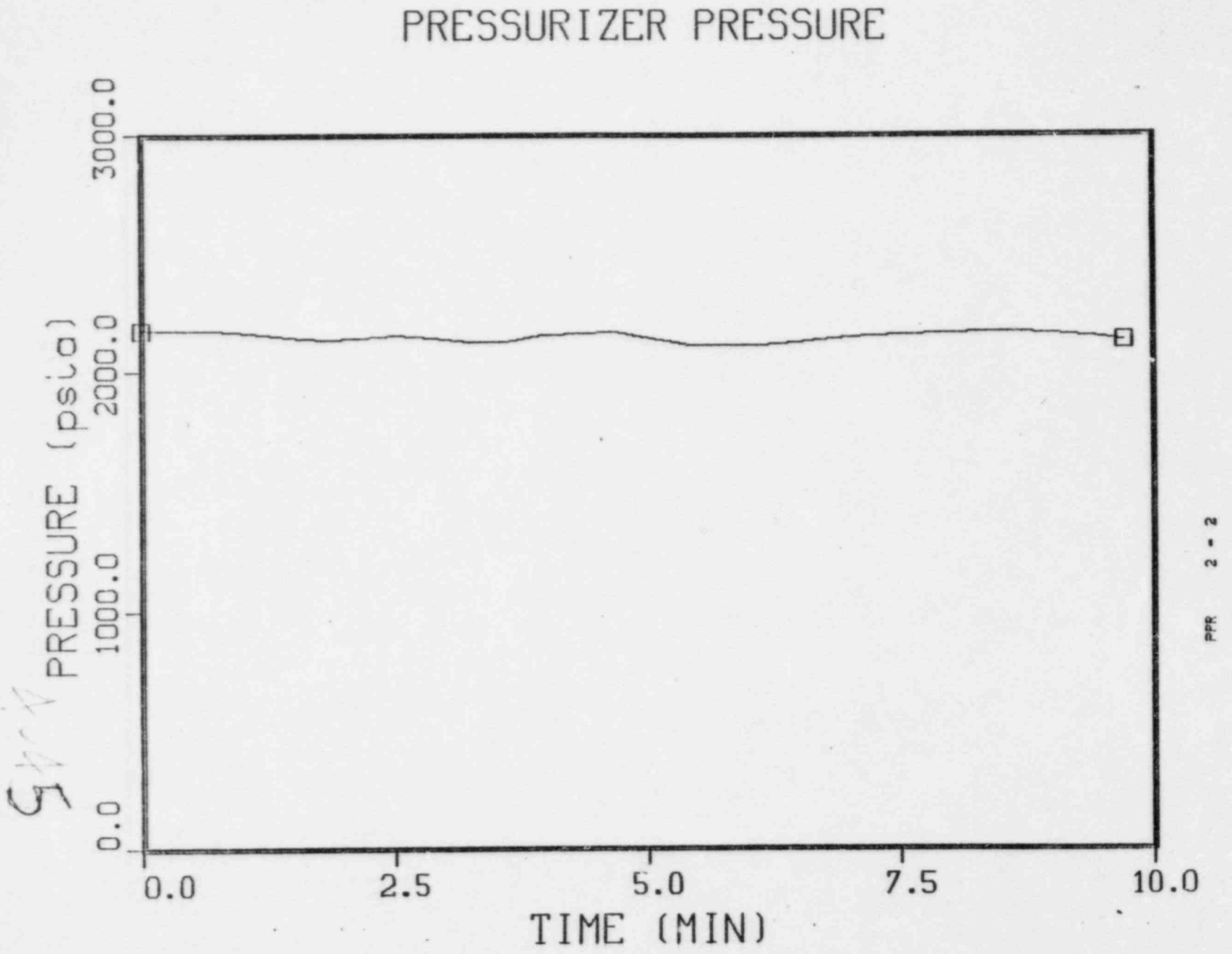


Fig. 4.2.35 Class 5 (100% power) pressurizer pressure

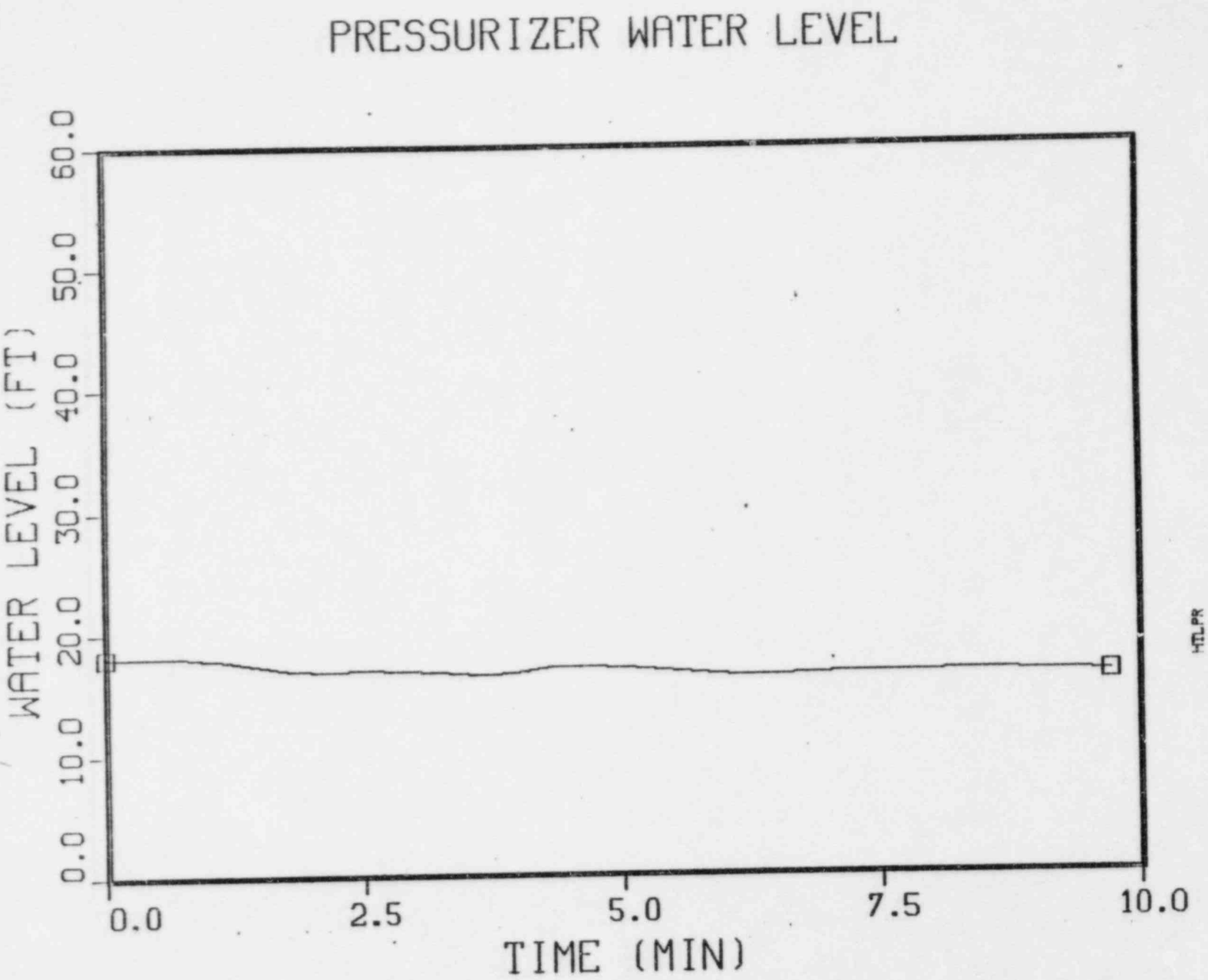


Fig. 4.2.36 Class 5 (100% power) pressurizer level

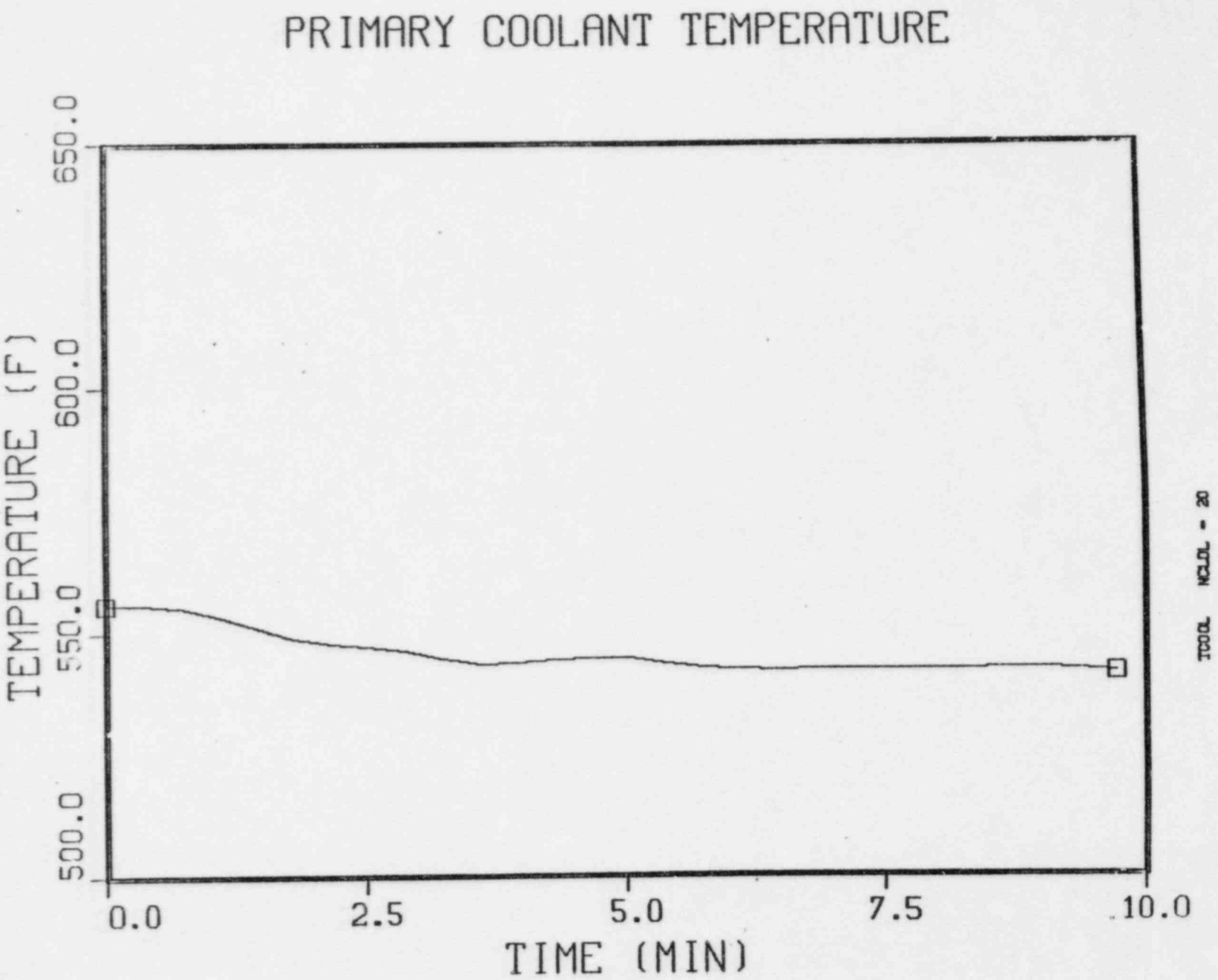


Fig. 4.2.37 Class 5 (100% power) loop A cold leg temperature

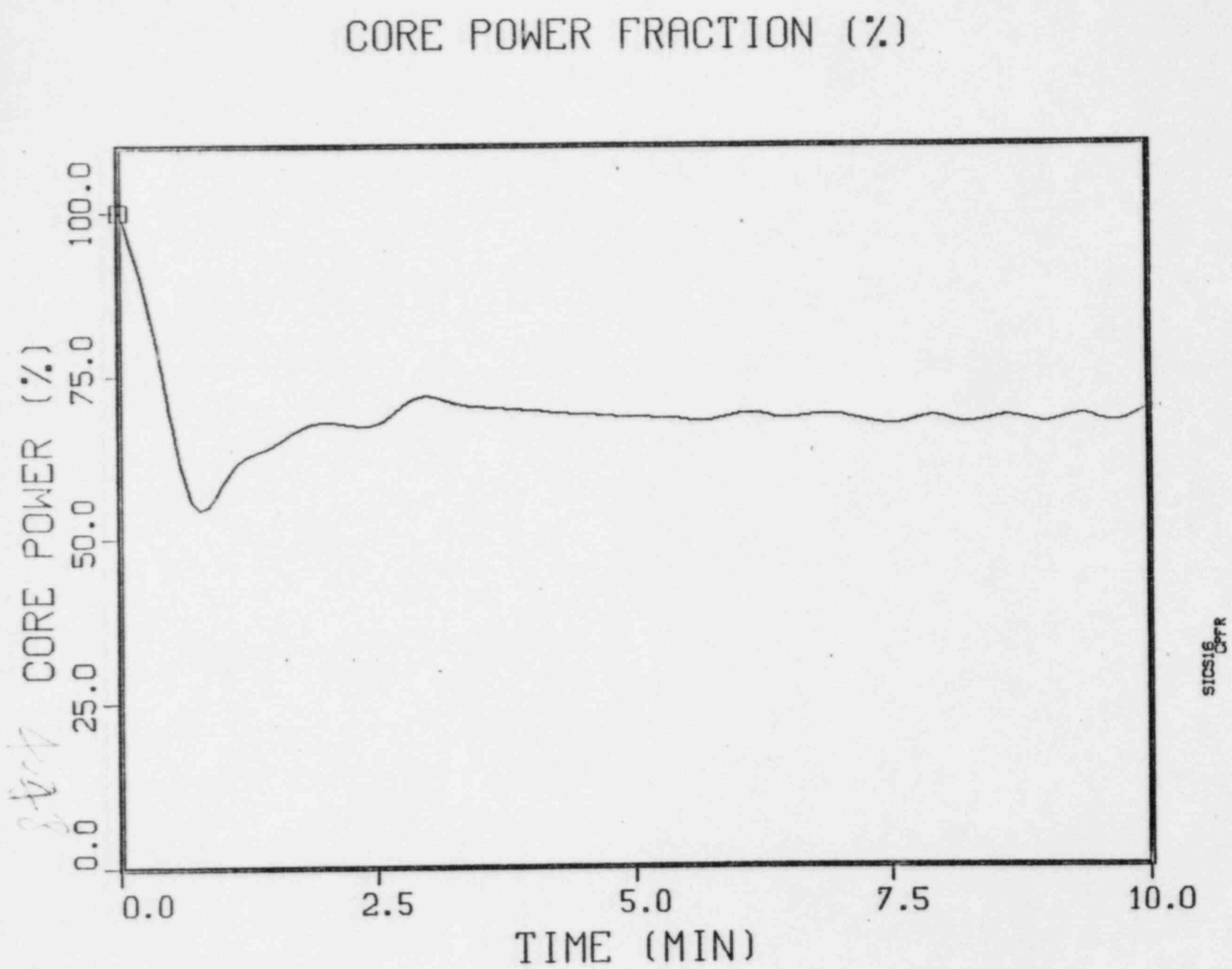


Fig. 4.2.38 Class 7 core power fraction

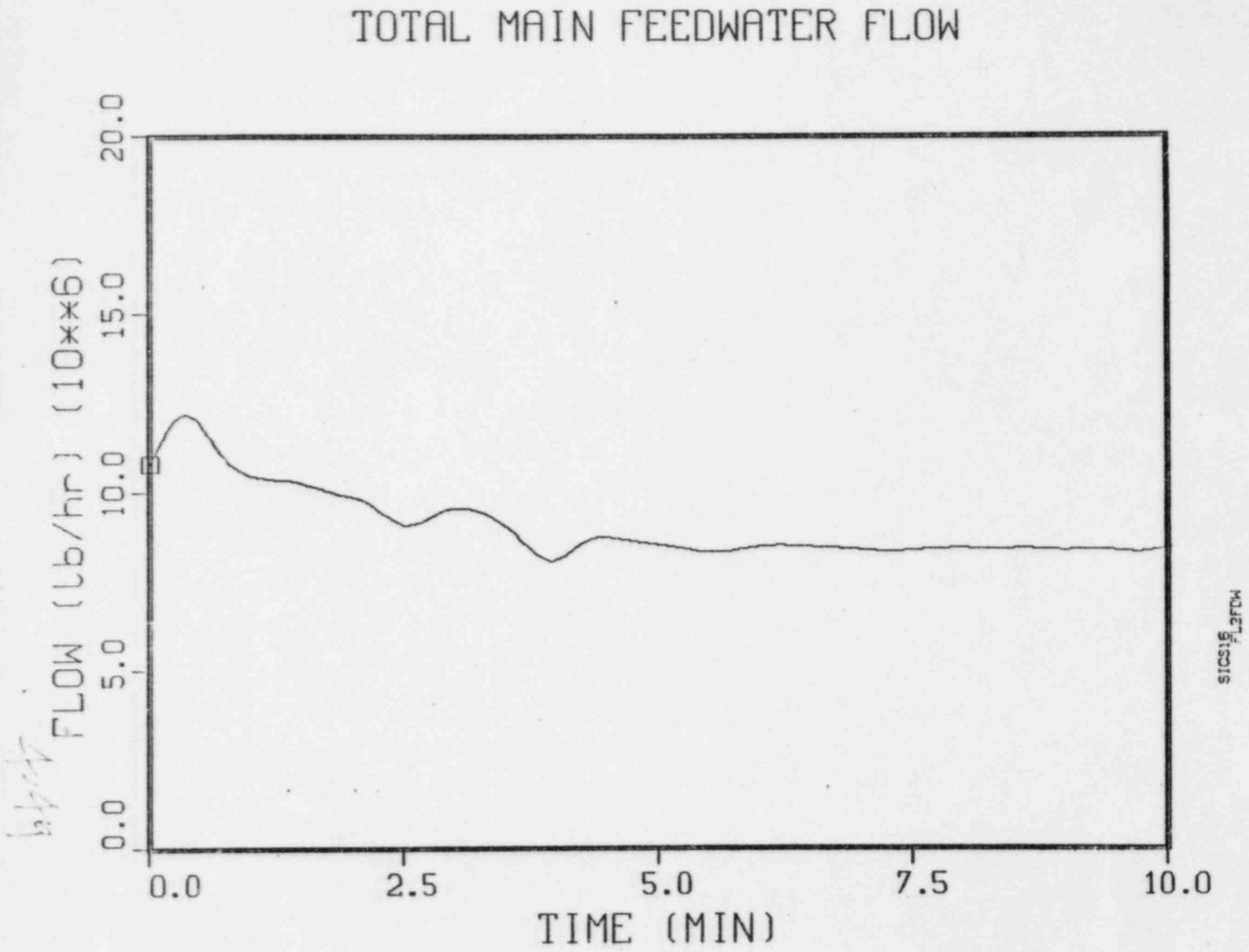


Fig. 4.2.39 Class 7 total feedwater flow

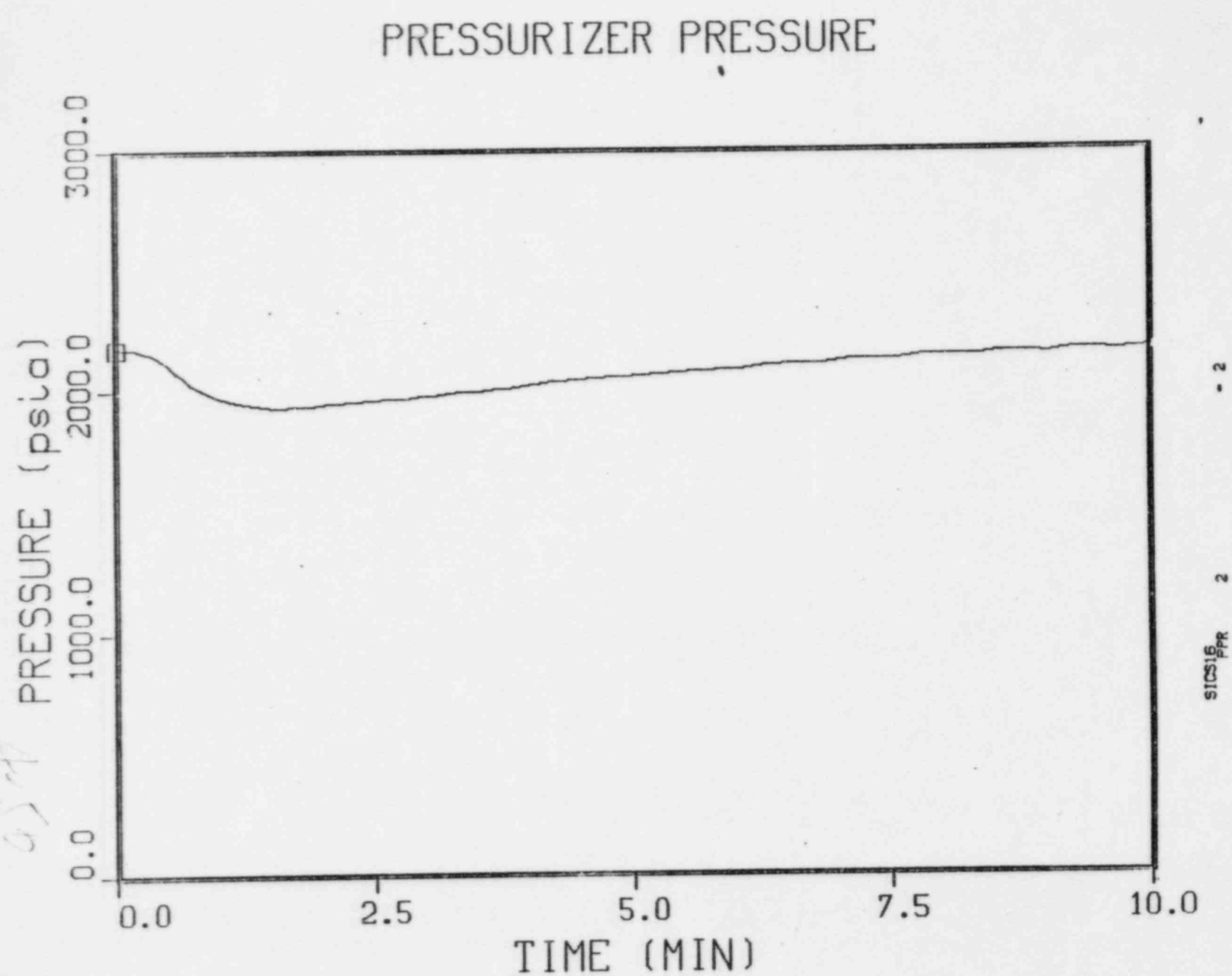


Fig. 4.2.40 Class 7 pressurizer pressure

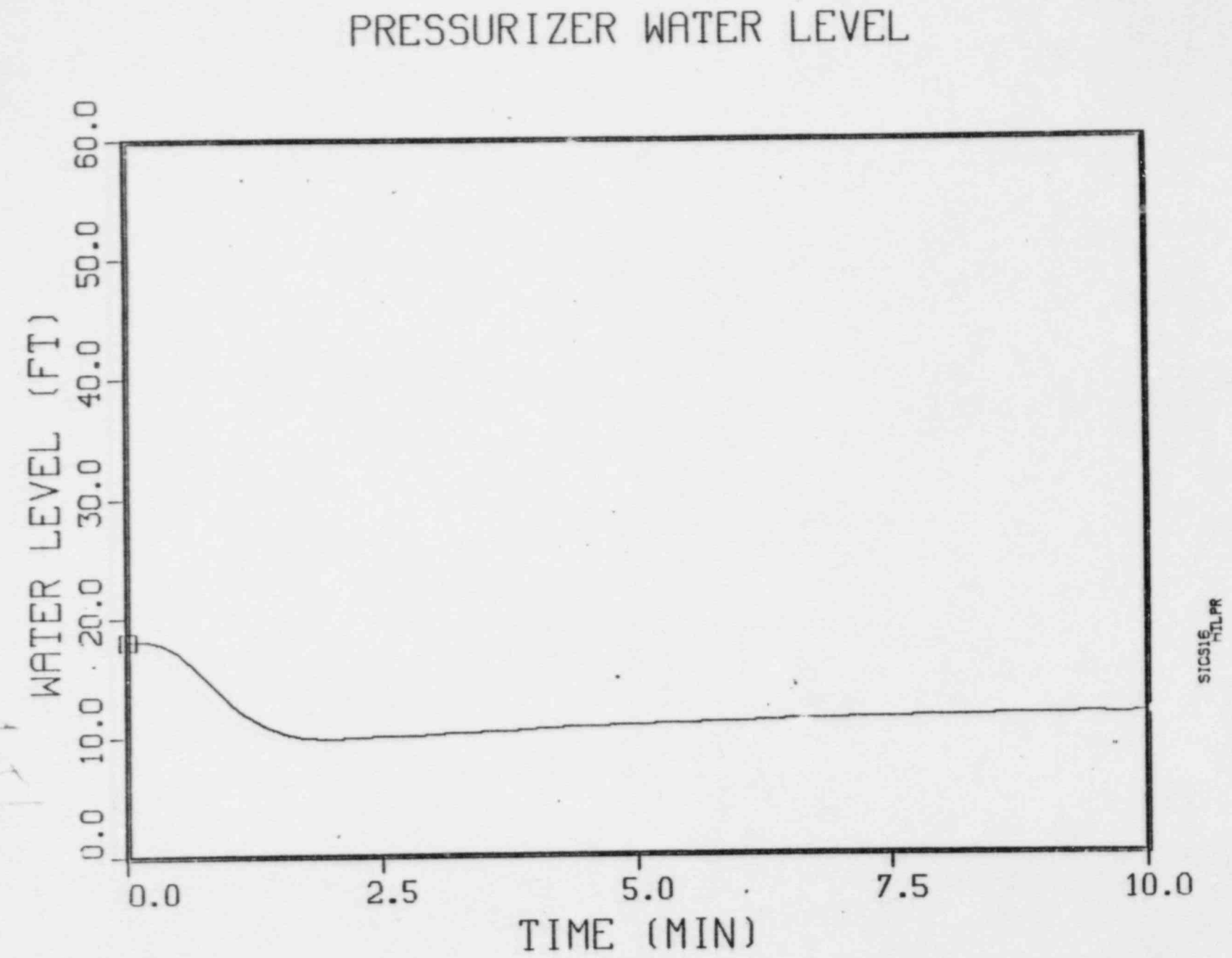


Fig. 4.2.41 Class 7 pressurizer water level

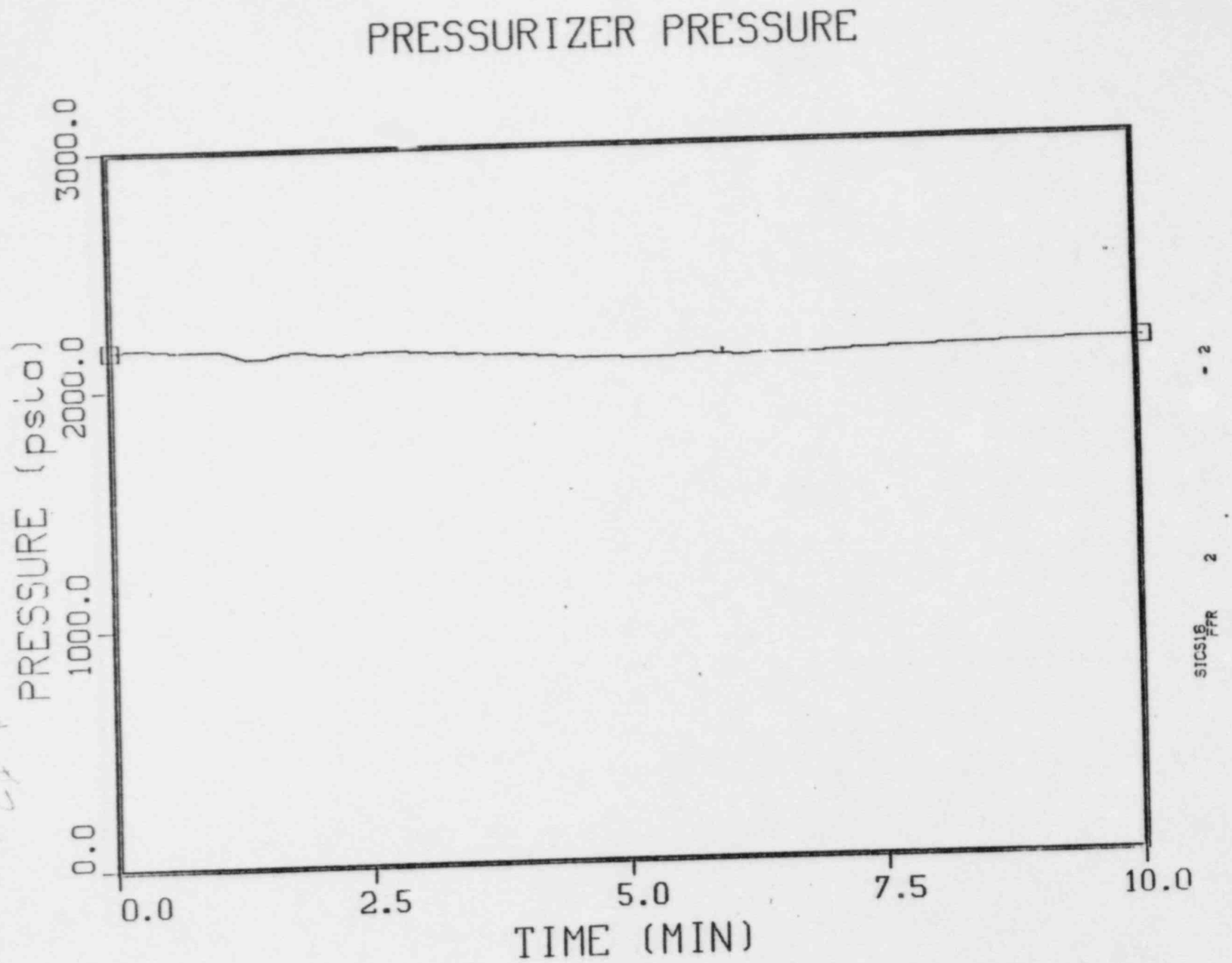


Fig. 4.2.42 Class 8 pressurizer pressure

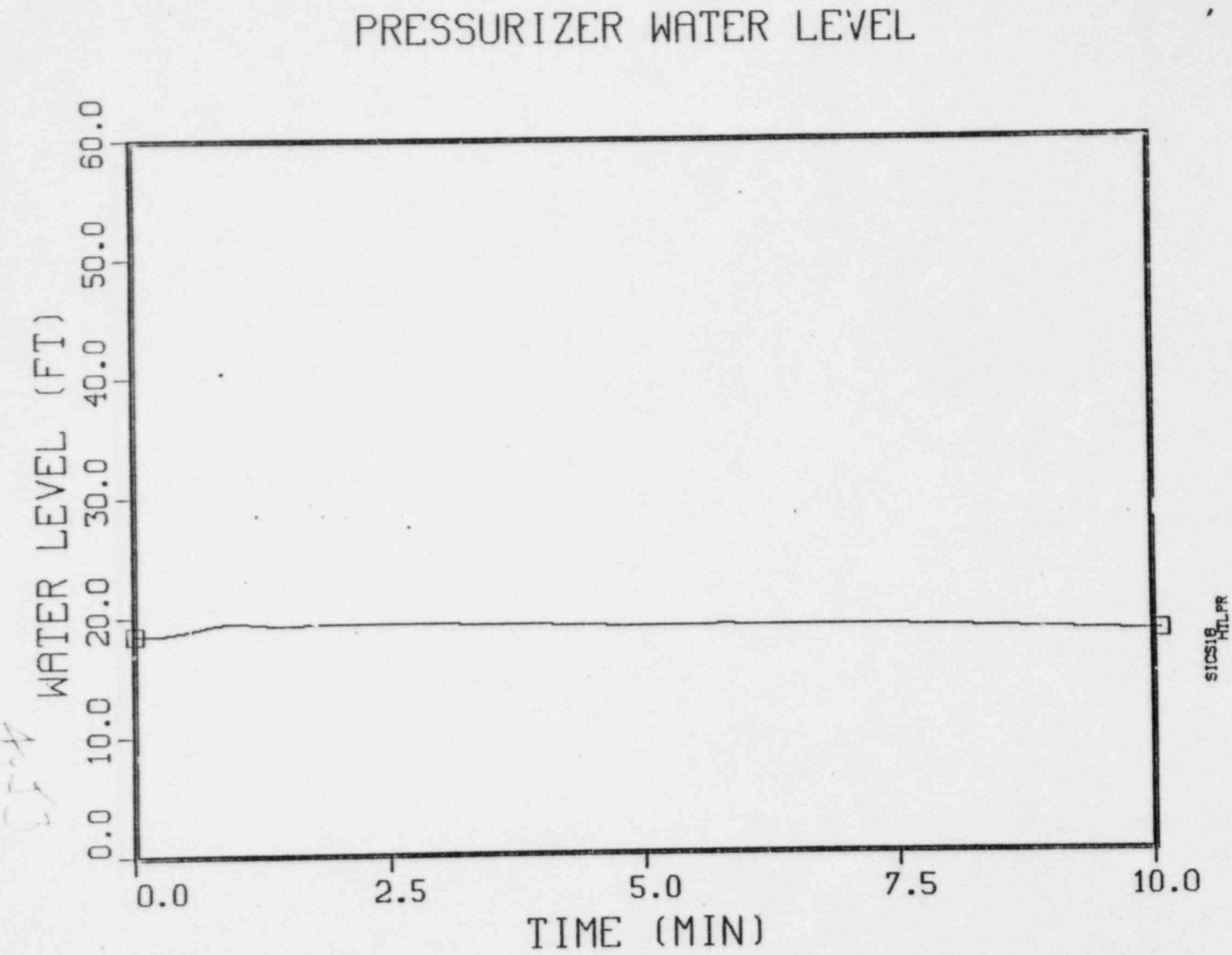


Fig. 4.2.43 Class 8 pressurizer water level

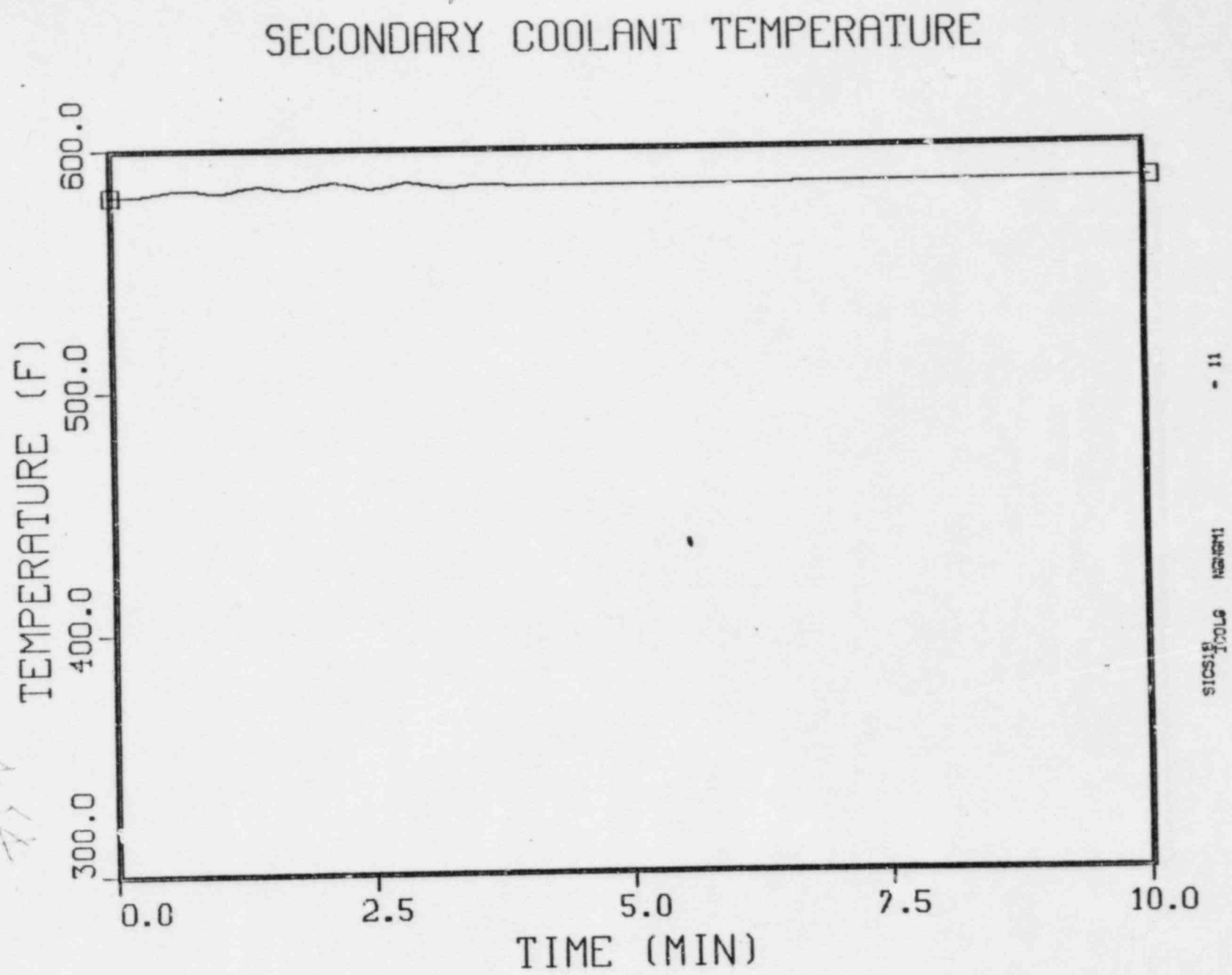


Fig. 4.2.44 Class 8 steam generator A outlet temperature

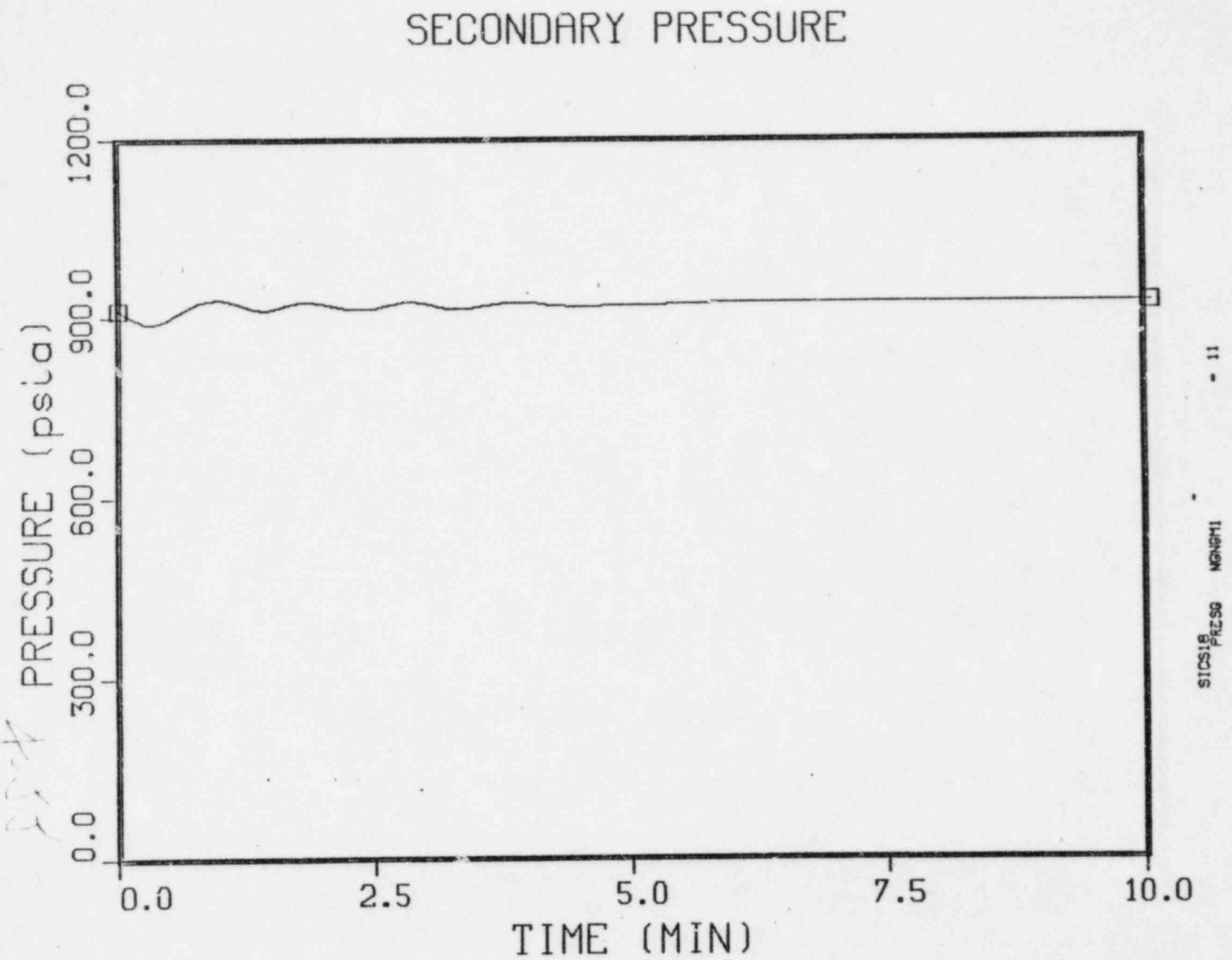


Fig. 4.2.45 Class 8 steam generator A outlet pressure

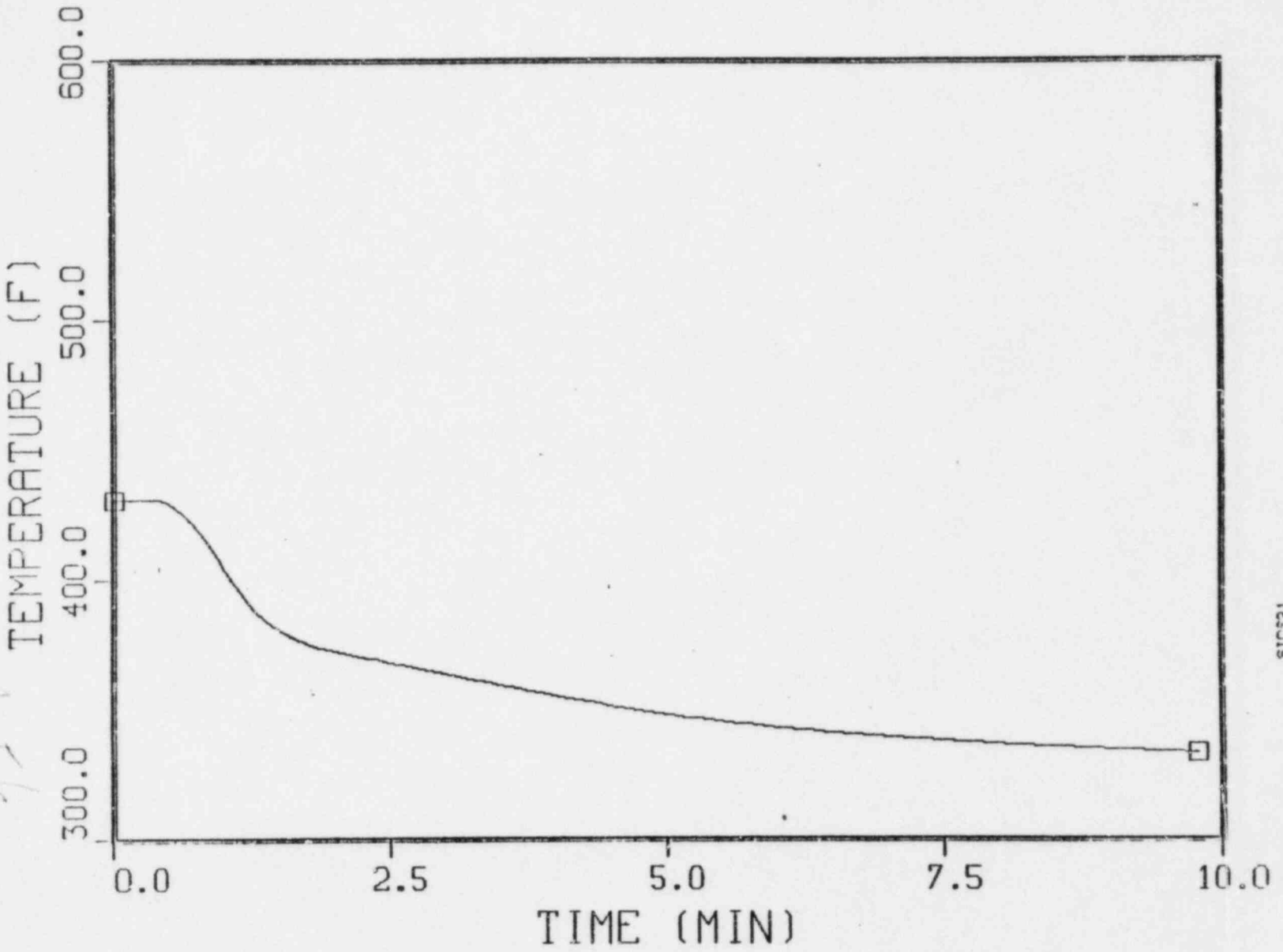


Fig. 4.2.46 Class 8 steam generator A feedwater temperature

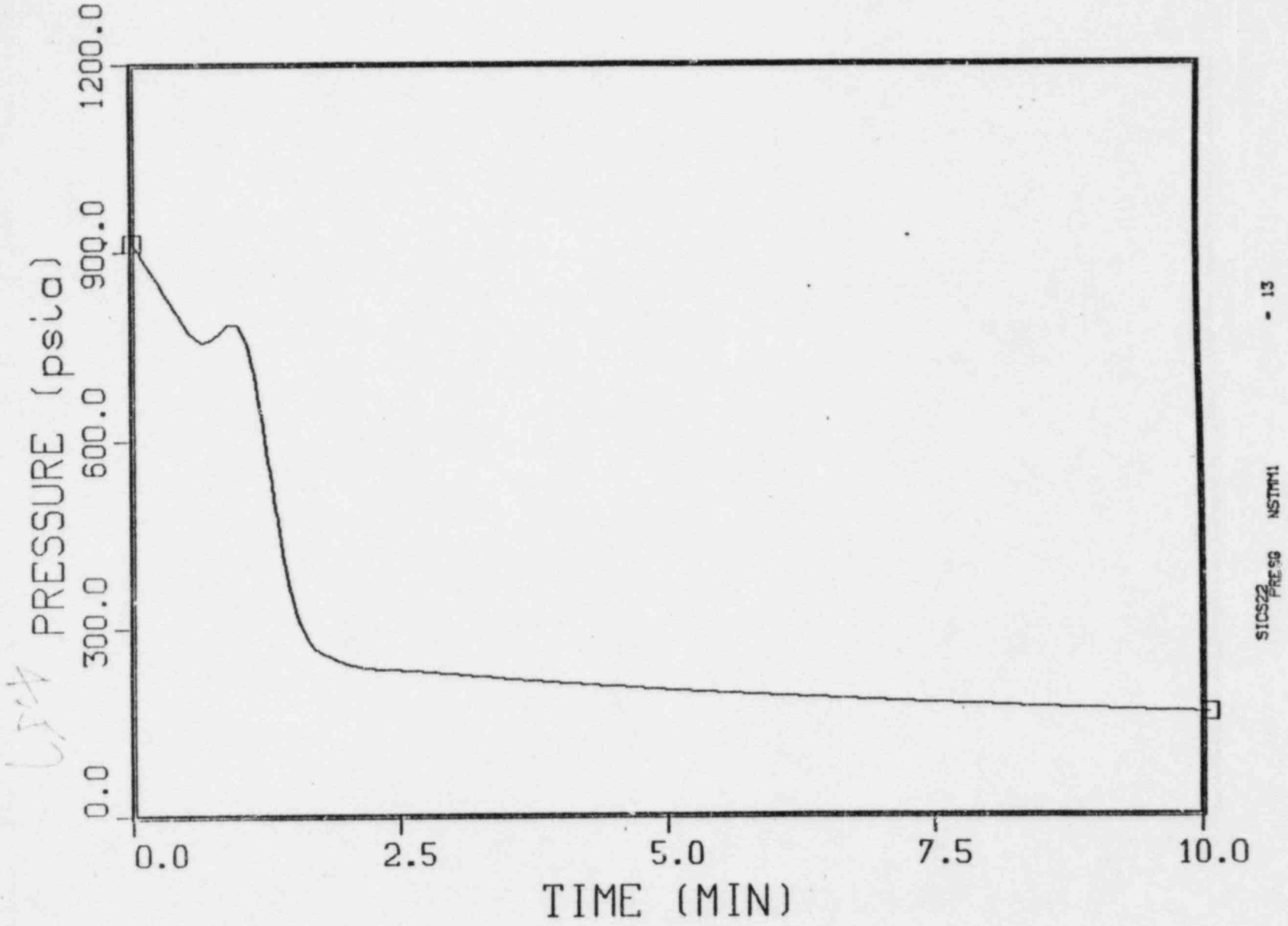


Fig. 4.2.47 Class 8 steam line A pressure

5.1 CONTROL FAILURES WITH SAFETY IMPLICATIONS

5.1.1 Steam Generator Overfill Control Failures

We have made a broad and inclusive survey of bounding cases of failures that induce steam generator overfeed or overfill (Sects. 3.2.5 and 4.2). The purpose of the survey was to determine whether unsafe conditions would be generated on either the primary or the secondary side as a result of the overfeed/overfill failure. We do not include in this group of failures steam line breaks or steam line valve failures except as they may be caused by an overfill failure.

The extreme cases to be considered are overfill of a single steam generator at 100% and 20% power with all SG high-level protection features failed. Examination of reactor coolant temperature, power, pressurizer level and pressure (Figs. 4.2.12, 20-22, 27, 35-37) shows that these variables are affected by the overfill, but they are soon brought to new steady-state values by the control system, and they do not appear at any time to enter a region of safety concern. We see no direct and immediate changes in the primary system which would give cause for alarm. However, as will be discussed below, significant safety concerns on the primary side arising from secondary system response to the overfill transient should be addressed.

On the secondary side we are concerned with the possible entry of liquid water into the steam lines and the amount and rate of such entry. In every bounding case of overfill simulated, the output from the overfilled steam generator dropped sufficiently in quality to cause some water injection into the steam line. Responding to the increased flow in the overfilling SG, the control system decreases flow in the other SG and adjusts power upward. The net effects are decreased quality, increased flow and inventory in the failed SG; increased quality, decreased flow and inventory in the other SG; increased power in the core; and decreased quality in the turbine header. These effects are relatively less severe at 100% power than at lower powers. Hence, safety concern at 100% power require similar concern at the lower powers that we have considered. See Figs. 4.2.8-37. In the following discussion of this scenario, we shall draw numerical results from the 100% power case.

5.1.1.1 Water in steam line

The most threatening failure scenario we have found that originates with control system failures causes the injection of water into the steam line. The scenario proceeds as follows.

We assume the MFW high-level pump trip is in an undetected failed state. (See Appendix A.2.2.3.) We next assume a failure that causes steam generator A control valve to fail fully open thus preventing the MFW A-blocking valve from closing. Failures of this kind would include all type C failures.

Both MFW pumps would increase to maximum speed (because the pressure drop across control valve A is low). The overfeed of SG-A causes the

secondary flow and inventory in SG-A to increase while the outflowing steam temperature drops into the saturation region, and the quality drops below one. The ICS, responding to the increased flow, calls for less flow, causing MFW B control valve to begin closing, but this closure has no effect on A on account of the postulated failure. The net secondary flow increases, leading to a drop in core average temperature and to an increase in power by the ICS to attempt to compensate for this. These effects are demonstrated in Figs. 4.2.8-19, 23-34 which show the course of such an overfeed from 100% power in SG-A without a turbine trip.

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

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

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

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

This overfeed appears to require manual tripping of the MFW pumps to avoid further damage. Babcock & Wilcox Anticipated Transient Operating Guidelines instruct the operator to trip the MFW pumps manually on suspicion of MFW overfeed. An alert operator following procedures could

therefore terminate this event. Note, however, that the event does develop quite rapidly.

A type F failure in SG-A leads to a similar overfill. A type F failure is a leakage in the D-level pressure tap, sense line, or associated valve packings, causing erroneously low low-level signals to appear on both the MFW and the AFW A-D differential pressure indicators. The transient proceeds as above, but during the overfill that follows the turbine trip, the high-level MFW pump turbine trip signal is actuated (in this case we do not assume it fails); both MFW pumps trip; and the AFW is activated. Since the false low-level signal goes to the AFW also, the overfill of SG-A is continued by the AFW. The overfill continues until stopped by manual intervention or by damage.

The significant differences between the type F failure scenario and the preceding one are as follows. (a) In type F the MFW pumps are tripped, and the overfill is continued by the AFW. (b) The water ingress to the steam line from AFW feed is much slower than from MFW feed. (c) The water entering the SG and the steam line from the AFW is lower temperature than that from the MFW.

The overfill scenario leads to very substantial water ingress to the steam line. An event of this kind occurred at the Beznau (West Germany) PWR in July 1969, (Ref. Nuclear Power Experience, Vol PWR-2, VI Turb. Cycle Syst. E. Cond. & FW, p. 3), leading to conditions in the steam line so violent that they were characterized by some as a water hammer. Damage to equipment and line supports was extensive, although line rupture did not occur. Though steam lines differ in geometry, design, and materials, the Beznau event demonstrates that the postulated phenomenon can occur in a steam line with great force and cause great damage. Since steam lines are not qualified for this environment, prudence would suggest that given a massive, continuing water ingress, line rupture should be assumed to occur with a probability close to unity.

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

5.1.1.2 Possible steam generator tube rupture

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

We do not feel the FSAR conclusions can be applied to the scenario described in Sect. 5.1.1.1 for the following reasons.

a. The tube rupture calculations are based on empirical data taken from experimental conditions less stringent than those proposed in Sect. 5.1.1.1.

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

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

d. Section 5.1.1.1 proposes a scenario where several RC circulatory cycles may have elapsed between the reactor trip and a steam line break. In such time the evolution of core power and in the temperatures of the SG tubes would decrease considerably. These effects do not appear to be taken into account in the FSAR.

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

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

For the above reasons we do not believe there is sufficient information available to assess the effect of a steam line break (as described in Sect. 5.1.1.1) on possible SG tube rupture or multiple SG tube rupture.

5.2 ESTIMATED FREQUENCY OF OVERFILLING A STEAM GENERATOR AT THE OCONEE NUCLEAR STATION

The potential for overfilling a steam generator with feedwater has been identified as a transient of concern for the Oconee Nuclear Station. The estimated frequency of this transient has been estimated to be between 0.001 and 0.0001 overfill transients per steam generator per year. The methodology for this calculation is discussed in this report.

Steam generator (SG) overfill is defined for purposes of this calculation as an uncontrolled addition of main feedwater to either steam generator resulting in the addition of liquid to the steam lines. Although the emergency feedwater system could contribute to the frequency of SG overfill, the analysis of safety system response has been considered beyond the scope of the current effort and has not been included. It should be noted that, with the exception of manual initiation of emergency feedwater, the main and emergency feedwater systems are not expected to be operating concurrently.

In the Oconee design, SG overfill requires a failure in the main feedwater (MFW) control valves or instrumentation resulting in overfeeding one of the two steam generators (MFW overfeed), a concurrent failure of the MFW pump to trip on high SG ("operate range") level and failure of the operator to detect and manually trip the main feedwater pumps or isolate the feedwater line. These three contributors to SG overfill are shown in a fault tree format in Figure 5.2.1.

5.2.1 Manual Feedwater Pump Trip Failure

The conditional probability of the operator failing to terminate the MFW overfeed has been estimated to be 0.1 to 0.01 failures per demand for a main control valve induced feedwater overfeed. Under normal circumstances, this estimate would be considered high with respect to 0.01 to 0.001 failures per demand usually estimated for a simple task. However, two abnormal factors have been considered. First, the operators at Oconee are expected to rely on the automatic high level trip to some degree.

CHECKED _____ DATE _____

PROJECT NO. _____

SG OVERFILL FAULT TREE

Fig. 5.2.1

This may delay the rapid manual action required. Also, operator action has been assumed to be required only following failure of the automatic trip system. Since the automatic trip system may be failed due to a failed low steam generator measurement, an indicated low level may tend to confuse the operator and delay action. The conditional probability of the operator failing to trip the pumps following the much slower startup control valve overfeed has been estimated to lower by a factor of 10.

The available field data for this type of operator action is very limited. Although operators have succeeded in terminating feedwater flow for most known MFW overfeeds, at least one transient occurred in a foreign reactor which resulted in injection of liquid into the steam line.[1]

5.2.2 Automatic "High Level" Feedwater Pump Trip Failure

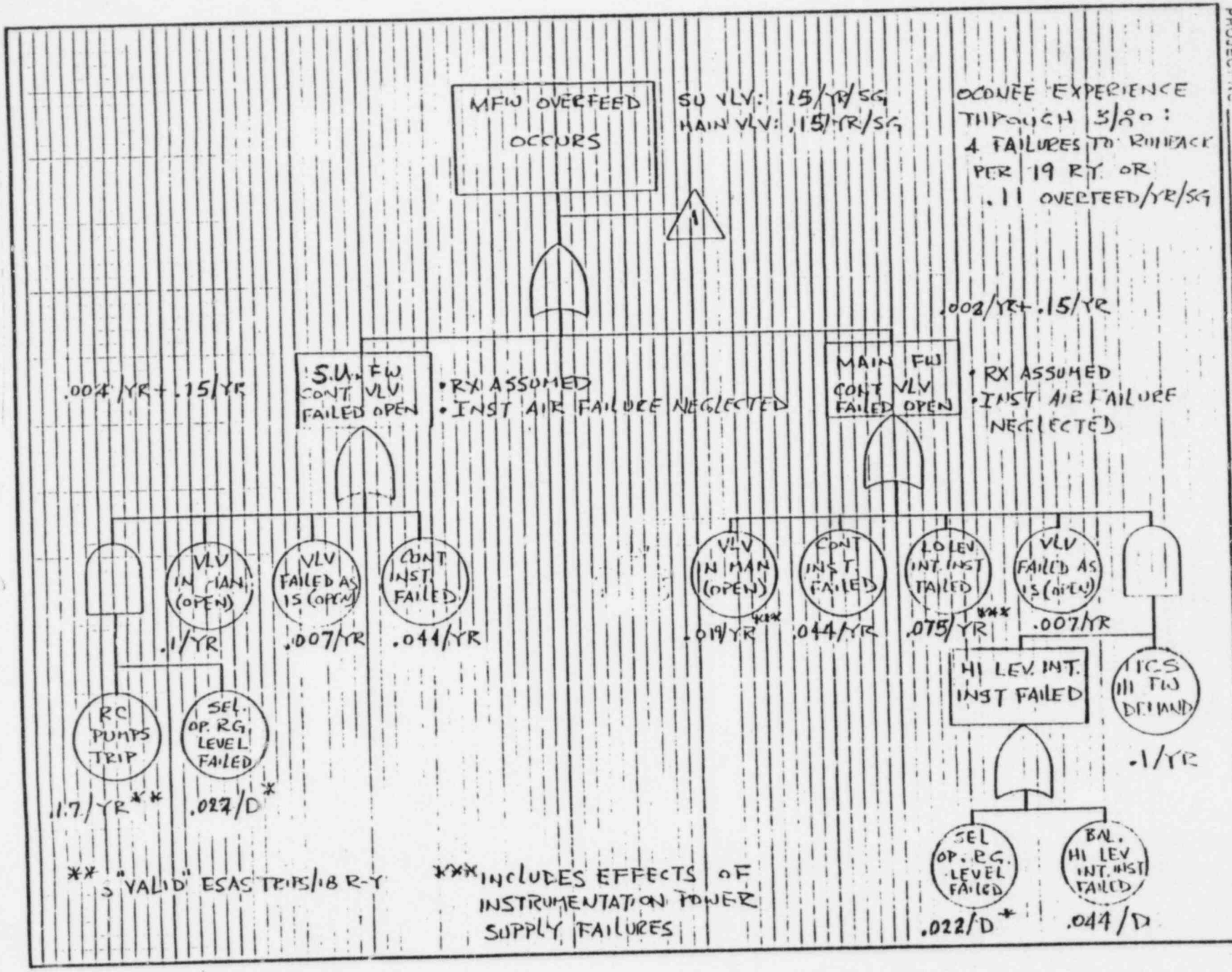
In the Oconee design, an indicated high SG level detected by both "operate range" level transmitters on either steam generator will initiate a trip of both main feedwater pumps. The pump trip circuitry modeled in the fault tree, Figure 5.2.1, has been obtained from available Bailey Meter Co. ICS circuit diagrams[2] and Oconee circuit diagrams.[3] The circuitry, for each steam generator, consists of two level (ΔP) transmitters each generating a signal proportional to the pressure difference between the steam generator operate range level taps. Each of these two signals are corrected based on the steam generator downcomer temperature in "multiplication modules" which generate temperature corrected signals to signal monitor modules. Each signal monitor closes one set of contacts to activate an alarm and another set which forms part of the feedwater pump trip logic on

---

[1] Nuclear Power Experience, Volume PWR-2, November 1976. (Beznav 1, July 1969)

[2] Schematic Diagram DB032344, Revision D, Bailey Meter Co.

[3] Elementary Design OEE-121-44, Revision 4, Duke Power Co.



PROJECT NO.

MFW OVERFEED
FAULT TREE
FIG. 5.2.2

indicated high level. The four pump trip contacts are arranged in a parallel-series array to energize a pump trip relay upon closure of both trip contacts on either steam generator. The trip relay activates trip contacts for each main feedwater pump to initiate pump trip (See Appendix A.2.2.3). The specific equipment activated by the pump trip relay is unknown.

Assuming an overfeed occurs and results in a high level in one of the two steam generators, the conditional probability that the pump trip circuitry fails to initiate a pump trip has been estimated. As shown on Figure 5.2.1, the pump trip failure occurs if either of the two transmitters, multiplication modules, signal monitor modules or the pump trip relay fail. In addition, the trip will fail if the unspecified circuitry or mechanical equipment associated with either pump fails to respond to the generated trip signal. The transmitter failure rates were estimated based on IEEE-500 data.[4] Module failure rates, however, were based on the number of operational amplifiers per module and the IEEE-500 operational amplifier failure rate.

The operational amplifier count was based on 820 series modules which, except for power supply, are believed to be similar in configuration to the Oconee 721 series modules. This methodology produced reasonable estimates when compared to available observed ICS component failure data. The module count for an 820 series ICS and the calculated module failure rates are shown in Table 5.2.1. The sum of these failure rates is 1.04 module failures per ICS per year. B&W Topical Report BAW-1564[5] lists 30 module failures per 19 calendar reactor years which corroborates the estimate well.

The failure rates of the transmitters and multiplication modules have been reduced by 50% to account for failure detection and repairs prior

---

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

[5] Integrated Control System Reliabilty Analyses, BAW-1564, August, 1979.

TABLE 5.2.1

CALCULATED MODULE TYPE FAILURE

RATES IN 820 SERIES ICS

Module Type	Number of Modules/ Type in ICS	Calculated Module Type Failures/Year[1]
Analog Memory	15	.032
Summer	53	.180
Signal Generator	17	.038
Summer and Integral	17	.077
Signal Limiter	6	.054
Signal Log	6	.014
Signal Monitor	13	.088
Tri-stable	16	.018
Function Generator	19	.301
Auctioneer	6	.041
Multiplier	4	.072
Miscellaneous	8	0.036
TOTAL	179	1.041

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

5.10

to an overfeed transient. (The failure of the pump trip circuit is of concern only if the circuit is failed when the overfeed transient occurs. Basing the conditional probability of failure on an assumed demand at one half the yearly test interval produces reasonable estimates). In addition to the failure probabilities listed for the known trip circuitry, a failure probability has been included to account for failure of the balance of equipment associated with the trip of the main feedwater pump's turbines. This failure probability was based on an additional relay-contact for each pump turbine.

Based on the model shown in Figure 5.2.1 and described above, an estimate of 0.065 failures of the pump trip circuit per demand has been obtained. The trip circuit modeled is unique to Oconee and limited operational data exists. The 0.065 failures per demand is not inconsistent with no known failures.

5.2.3 Main Feedwater Overfeed Frequency

The occurrence of a main feedwater (MFW) overfeed has been identified in Figure 5.2.1 as a necessary condition for SG overfill. The component failure combinations leading to MFW overfeed are identified in Figure 5.2.2. As shown, MFW overfeed may be caused by either startup (SU) feedwater control valve or either MFW control valve failing open. In either case it has been assumed that one of the control valves will fail to close following a reactor trip or fail open resulting in a reactor trip. This condition results in the supply of feedwater exceeding demand and an increasing steam generator level.

The failure rates are calculated on a single steam generator overfeed basis. Although overfeeding both steam generators is possible, the frequency is lower and the conditional probability of the SG high level instrumentation successfully tripping the pumps is higher.

As shown, [redacted] failures resulting in a SU valve remaining open and affecting [redacted] pump trip circuit are separated from other failures affecting only the valve position. The SU valve is controlled by the operate range level transmitters following a trip of the four reactor

coolant (RC) pumps. Although an RC pump trip initiator, of itself, is expected to occur very infrequently without a loss of the external grid (which would trip the feedwater pumps), the operator is required to manually trip the RC pumps following an ESAS trip. Thus, failure of a SU valve resulting from a pre-existing operate range level transmitter failure is calculated based on the ESAS trip frequency (3 trips per 18 reactor years)[6] and transmitter/multiplier module failure rates. This yields a SU valve overfeed frequency of 0.004 per year for this failure mode. However, since this failure also disables the automatic pump trip circuit, its contribution to SG overfeed is greater than other overfeed initiators.

Other failures resulting in SU valve overfeed include control instrumentation module failures, failure of the valve and transfer of the valve to manual control. Module failure rates were estimated as discussed above. Overfeed transients resulting from SU valve failure was based on historical nuclear plant pneumatic valve experience[7] and the Oconee reactor trip frequency. The estimation of the frequency of the SU valve being placed in manual control, 0.1/year, is based on engineering judgement and specifically considers the fact that the transfer of the startup valve to manual cannot affect reactor performance until the reactor is tripped or shutdown. A combined frequency of 0.15 SU valve overfeeds per year was estimated for these failure modes.

Failure of the main FW control valve open, similar to the SU valve, can occur due to failures affecting the pump trip circuit or due to failures only affecting valve position. These failure modes are considered separately.

Placing the main control valve in manual is considered possible but less likely than leaving the SU valve in manual. The frequency of the operator

---

[6] Letter from W. Parker (Duke) to H. Denton (NRC), Attachment 1, July 12, 1980.

[7] In plant Reliability Data Program, NUREG-CR-3154, December 1983.

transferring the main control valve to the manual mode has been estimated to be 0.01 per year based on engineering judgement. One failure identified which would automatically place the main (and SU) control valves in the manual mode is a loss of ICS "auto" power (a branch circuit of ICS bus KI). The experience base, based on LER data for failure of non-1E buses at B&W plants, indicates a bus failure rate between .23 and .46 failures per bus per year.[8] However, at Oconee, failure of the bus supplying the ICS, bus KI, would automatically initiate main feedwater pump trip and not lead to overfeed. One failure of ICS auto power is known to have occurred at Oconee.[9] Assuming this one failure of one of the 5 major power supply branch circuits has occurred in the 23 R-Y experience at Oconee, the failure rate would be 0.009 failures per branch circuit per year. This failure rate has been included in the transfer of the main feedwater valve to manual failure mode.

Other failures which result in the main control valve remaining open are valve failures and control instrumentation module failures. The frequency of overfeed transient resulting from valve failure, as for the SU valve, was based on the historical nuclear plant pneumatic valve failure data (failures per demand) and the Oconee reactor trip frequency.

Two instrumentation failure initiators are shown: failure of the low steam generator level intercept circuit (minimum level control) and main feedwater valve control instrumentation module failure (downstream of the low level signal auctioneer module). The failure frequency of these circuits was based on the module failure rates of Table 5.2.1 and the IEEE-500 transmitter failure rates.

The last main control valve failure mode considered affects the feedwater pump trip circuit in addition to the control valve. The

---

[8] NUREG-0667.

[9] Letter from W. Parker to H. Denton, July 23, 1980.

feedwater control circuits are designed to limit (intercept) the maximum steam generator level signal based on operate range steam generator level signals. If the selected operate range level signal is failed when any of a number of ICS modules fail producing a high feedwater demand signal, an overfill transient not terminated by the automatic pump trip will occur. The frequency of the high level intercept circuit failure has been separated into the failures affecting the pump trip and the balance of the module failures which do not. (These failures contribute to main feedwater overfeed but not to the combined overfeed/pump trip failure. The ICS module failures (upstream of the high level intercept auctioneer module) which could cause high feedwater demand are numerous and no attempt has been made to individually quantify the individual module failure combinations. Based on engineering judgement, these failures have been estimated to occur with a frequency of approximately 0.1/year, which is not inconsistent with known operating experience. Combining these failure probabilities yields 0.002 failures per SG per year affecting both the valve position and high level pump trip and 0.004 failures per SG per year affecting only the valve position.

5.2.4 Summary of Results

The main feedwater overfeed transient has been estimated to occur with a frequency of 0.15 transients per SG per year for both the SU valve and main control valve failure transients. In addition, 0.004 and 0.002 transients per SG per year were estimated for those transients affecting both overfeed and the main feedwater pump trip.

Available Oconee operating experience indicates that four overfeed transients (failure to throttle main feedwater flow following reactor trip) have occurred through March, 1980.[10] This represents four overfeed transients over the elapsed operating time of the three units of 19 reactor years[11] or 38 steam generator years. The experience base

---

[10] Oconee Pressurized Thermal Shock Evaluation, DPC-RS-1001, January, 1982.

[11] Letter from W. Parker to H. Denton, July 23, 1980.

results in an overfeed frequency of 0.11 overfeed transients per SG per year. This experience is in very good agreement with the 0.15 estimate for the rapid, main FW control valve failure induced overfeed transients obtained by combining the component failure probabilities. It should be noted that overfill transients quickly terminated by the operator, especially slow, SU valve failure induced transients, may not be documented.

As shown in Figure 5.2.1, combining the estimated overfeed frequency with the main feedwater pump trip failure frequency and the estimated frequency of the operator failing to manually trip the feedwater pumps yields a steam generator overfill frequency estimate of 0.001 to 0.0001 events per SG per year for rapid SG overfill transients.

5.3 APPLICABILITY OF RESULTS TO OTHER B&W INSTALLATIONS

Results to date are plant-specific for the Oconee-1 Nuclear Plant. Generic extensions to other B&W installations will primarily depend upon balance-of-plant configurations at the other facilities, and these in general will show more variation than will the primary systems.

The control characteristics which make possible the scenarios we describe are subtle and hard to track down. A great deal of effort has been spent in determining the fine details of feedwater delivery in the Oconee-1 plant, and even now there remain a number of uncertainties as to pump trips and operating characteristics.

If results are to be extended to other B&W installations, cooperation of the utilities involved will be required to determine details of control which are not presented or required to be presented in the safety analysis report.

5.4 RECOMMENDATIONS FOR MITIGATION OF CHALLENGES TO SAFETY THROUGH FAILURE OF CONTROLS

In the course of this study we have, we believe, uncovered some potential concerns, in particular, control system failures that might lead to the failure sequence discussed in Section 5.1. We have noted some places where improvements might be made and 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 Fig. A.2.4 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 Fig. A.2.4. 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 (Fig. A.2.3) 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, Fig. A.2.3 is the only sensor providing level information once the SG water level exceeds the high level pump trip height (level D,D' in Fig. A.2.3). 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.

5.5 RECOMMENDATIONS FOR FUTURE WORK

5.5.1 Consolidation of Present Investigation

The work described in this report is subject to a number of caveats as set forth in Sect. 1.3. Some unresolved issues involve data assumptions which can be confirmed or corrected when responses are received to outstanding requests for data. Also, additional code validation should be undertaken, including ongoing efforts to provide comparisons with RELAP-5 for identical scenarios.

5.5.2 Extension into Broader Concerns

The initial investigation restricted its scope to match the limited concerns of Unresolved Safety Issue A-47. This gave very limited attention to seismic and other harsh environmental challenges.

Once the concerns of A-47 are satisfied, we are scheduled to begin a program to examine the failure modes and effects of control systems when they are subjected to the multiple failures possible under harsh environmental conditions (earthquake, fire, and sabotage, in particular). The program will provide an in-depth investigation of the effects upon control systems of seismic and other harsh environments. The conclusions reached up to the present point in the program are in some respects incomplete because important contributions to control malfunctions were deliberately excluded from the initial examination. Specifically, these postponed areas include: (1) seismic and other environmental effects; (2) safeguards issues involving knowledgeable plant personnel in "nonvital" areas of the plant; (3) operator reaction to emergency conditions under circumstances wherein important instrument readings are unavailable or incorrect; and (4) control impact upon safety through frequent challenges to protection systems. Some of these concerns are referred to in the A-47 Task Action Plan, some are not. They were excluded from early consideration in this program in order to expedite the main thrust of the investigation. The neglected issues are large and complex and are partially addressed in other programs. In the 1986 schedule we intend to examine the effects of the four important areas listed above, using the augmented FMEA methods of the earlier investigation.

In the case of multiple failures, as from environmental effects or sabotage, control room indicators are apt to be included in the general malfunctioning when control systems fail. In the follow-on part of the program particular attention will be paid to assessing operator response to multiple alarms and failures, including failures of control room indicators.

We will consider the effects upon safety which control failures may produce through frequent challenges to the protection system. The function of the plant protection system is to guard against dangerous failures, including failures of control. Safety reliability is achieved through redundancy, diversity, testing, and standards, to the degree that the probability of protection system failure becomes a small percentage of the challenge rate. The ratio is not zero, however, and if the challenge rate becomes sufficiently high, the projected safety failure rate may be unacceptable. Control failures which have a historical record or presumptive capability for causing an excessive challenge rate to protective features will be examined.

Instrumentation and Controls Division

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

DRAFT FINAL REPORT

Volume 3
Appendix
Background Information

P. N. Austin
R. E. Battle
R. S. Booth
D. P. Bozarth[1]
R. Broadwater[2]
F. H. Clark
N. E. Clapp
R. A. Hedrick[1]
L. L. Joyner[3]
J. Lewin
C. L. Mason[1]
A. F. McBride[1]
O. L. Smith
R. S. Stone

Manuscript Completed: September 30, 1984

Date Issued:

[1]Science Applications, Inc., Oak Ridge, TN
[2]Tennessee Technological University, Cookeville, TN
[3]Joyner Engineers and Trainers, P.C., Forest, VA

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

NRC Fin Nos. B0467 and B0816

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

Table of Contents

Table of Contents (Continued)

C. HYBRID MODEL OF OCONEE- PLANT
(It will be incorporated to chapter 4.0 of the Main Report (Vol. 2))

APPENDIX A.1. GENERIC SYSTEMS LIST

A.1.1 BACKGROUND

Development of a generic systems list is possible because, with few exceptions, the same functions must be provided in a nuclear power plant regardless of plant design. The generic systems list presented here was developed by Science Applications, Inc. (SAI) as part of the Reliability Data Base Program.[1]

A.1.2 GENERIC SYSTEMS LIST DEVELOPMENT

The approach used to generate the generic systems list was to evaluate the standard safety analysis reports (SARs) for each of the major reactor vendors, for example, the CESSAR System 80,[2] RESAR 41,[3] BSAR-205[4] and GESSAR 238,[5] and the specific SARS for William H. Zimmer Unit 1,[6] Grand Units 1 and 2,[7] and Oconee.[8] In addition, the Stone and Webster PWR Reference Nuclear Power Plant SAR[9] was also used. Each of the SARs was examined, and from the information presented, a systems list for the specific vendor and balance of plant architect-engineer (A-E) was developed. The individual plant systems listings were then correlated by function, to generate the generic list.

For the generic systems list, several major systems groupings have been identified. Within each major grouping are various systems and their associated subsystems. The seven major groupings are:

Nuclear systems (N)
Engineered safety systems (S)
Containment systems (C)
Electrical systems (E)
Power conversion systems (P)
Process auxiliary systems (W)
Plant auxiliary systems (X)

For the nuclear systems, engineered safety systems, and containment systems groupings, there are significant differences between nuclear plants of the boiling water reactor (BWR) design and the pressurized water reactor (PWR) design. For the groupings, the lists apply only to PWRs; other lists apply to both designs. The generic systems list is presented in Table A.1. Descriptions for each system are provided in Sect. A.3.

Table A.1. Generic systems list for PWRs

Nuclear systems (N)	
N01	Reactor core
N02	Control rod drive system
N03	Reactor control system
N04	Reactor coolant system (including reactor vessel and internals)
N05	Emergency boration system[a]
N06	Reactor protection system
N07	Nuclear instrumentation system
N08	Residual heat removal/low-pressure injection system
N09	Chemical and volume control system (CVCS)

Table A.1. (continued)

Engineered safety systems (S)
S02 Engineered safety features actuation system
S03 Safety injection system
S03.A High-pressure safety injection subsystem[b]
S03.B Safety injection tank/core floor subsystem[b]
S03.C Low-pressure safety injection subsystem is a functional mode of the residual heat removal system[b]
S04 Remote shutdown system
S05 Auxiliary feedwater system

Table A.1. (continued)

Containment systems (C)	
C02	Reactor building/containment and penetrations
C03	Containment cooling system
C03.A	Ice condenser system[c]
C04	Containment isolation is a function of the engineered safety features actuation system (ESFA) and the various piping systems which penetrate containment
C05	Containment purge system
C07	Combustible gas control system
C08	Containment ventilation system
C10	Containment spray system
C11	Penetration room ventilation system

Table A.1. (continued)

Electrical systems (E)	
E01	Main power system
E01.A	Protective relaying and controls
E02	Plant ac distribution system
E02.A	Essential power system
E02.B	Nonessential power system
E02.C	HPCS power system
E02.D	Protective relaying and controls
E03	Instrumentation and control power systems
E03.A	DC Power system o Vital dc power subsystem o Plant dc power subsystem
E03.B	Instrument ac power system o Vital instrument ac power subsystem o Plant instrument ac power subsystem
E04	Emergency power system
E04.A	Diesel generator fuel oil subsystem
E04.B	Diesel generator cooling water subsystem
E04.C	Diesel generator air subsystem
E04.D	Diesel generator lubrication oil subsystem
E05	Plant lighting system
E05.A	Essential lighting
E05.B	Nonessential lighting
E06	Plant computer

Table A.1. (continued)

Electrical systems (E)	
E07	Switchyard
E07.A	DC control power system
E07.B	Protective relaying

Table A.1. (continued)

	Plant auxiliary systems (X)
X01	Potable and sanitary water system
X02	Fire protection system
X02.A	Water system
X02.B	Carbon dioxide system
X03	Communications system
X04	Security system
X05	Heating, ventilating, and air conditioning systems
X05.A	Control room habitability system
X05.B	Turbine building ventilation system
X05.C	Diesel building ventilation system
X05.D	Auxiliary building ventilation system
X05.E	Fuel building ventilation system
X06	Nonradioactive waste system
X06.A	Gaseous waste
X06.B	Liquid waste
X06.C	Solid waste

[a]Westinghouse units have emergency boration as a unique system. Babcock & Wilcox (B&W) and Combustion Engineering (CE) units provide emergency boration as a function of the CVCS.

[b]B&W units have these as separate, independent systems.

[c]Unique to one series of Westinghouse units.

A.1.3 GENERIC SYSTEM DESCRIPTIONS

A.1.3.1 Nuclear Systems

The nuclear system grouping is comprised of the reactor core and those systems and subsystems which monitor and control and core's reactivity, remove heat from the core, and otherwise directly support the safe operation of the reactor. The following description of systems are identified as applying to a BWR or PWR or both.

A.1.3.1.1 N01 Reactor Core (BWR and PWR)

The reactor core produces heat through nuclear fission. A reactor core contains about two to three hundred fuel assemblies that are arranged in a lattice fashion approximating an upright cylinder. The exact number of fuel assemblies varies with both the nuclear steam supply system (NSSS) vendor and the generation of the reactor design. Fuel assemblies are constructed of uranium dioxide (UO_2) pellets surrounded by a Zircaloy cladding tube. The lattice structure of the reactor core is a loose one that allows reactor coolant water to flow up and around the fuel assemblies. Empty spaces also are left in the lattice for the insertion of control rods.

Systems that interface with the PWR reactor core are the control rod drive system and the reactor coolant system. Also, some power- and temperature-measuring components may be inserted directly into the reactor core.

A.1.3.1.2 N02 Control Rod Drive System (BWR and PWR)

The control rod drive system is used for power shaping and reactivity control. The control rod drive system is made up of sixty to seventy control rod assemblies, each with its own drive mechanism. The neutron absorber in the control rods is boron carbide (B_4C) or silver-indium-cadmium alloys. As with the fuel assemblies, the exact number of control rod assemblies depends upon the NSSS vendor and the reactor design. Also included in the control rod drive system is an energy source for the drive mechanisms. For PWRs the energy source is electrical power. When fully inserted into the reactor core, the control rods provide sufficient negative reactivity to stop the core's chain reaction while at operating temperatures. Power shaping is accomplished by driving selected control rods to predetermined positions within the reactor core.

In PWRs control rods are suspended above the reactor core by electromechanical devices. When a trip signal is received, the electric current passing through the devices is interrupted causing them to release the control rods. The control rods then drop by gravity through their guide tubes into the reactor core. Control rod drive stators are typically cooled by the reactor building cooling water system.

Control rod drive systems in PWRs interface with the plant ac distribution system, the reactor building cooling water system, the dc power system, the reactor protection system, the reactor control system, and the reactor core. In BWRs the control rod drive system interfaces with the plant ac distribution system, the reactor protection system, the reactor control system, the control rod drive hydraulic subsystem, and the reactor core.

A.1.3.1.3 N03 Reactor Control System (BWR and PWR)

The reactor control system provides the means for monitoring and controlling control rod position during normal operating conditions. The objective of the reactor control system (RCS) is to match reactor power as closely as possible to unit demand while maintaining a controlled power level and balanced flux distribution in the reactor core. In BWRs this is accomplished by a manual control system in which an operator can selectively position a single control rod or a control rod group. The electric circuitry, switches, indicators, and alarms that are needed to provide input signals for the control rod drive system make up the reactor manual control system. In PWRs the control function may be either automatic or manual. While in the automatic mode, the input signal to the control rod mechanisms is produced by comparing the reactor power level with the unit demand as seen by the turbine. The relative difference between these signals controls the motion of the control rod drive mechanism. At low power conditions, the reactor is under manual control by an operator. The operator may also assume manual control at any time while the reactor is in a normal operating mode. The design and capabilities of the PWR reactor control systems vary depending upon the NSSS vendor. In Babcock and Wilcox (B&W) designed reactors, this system is called the integrated control system (ICS); in Combustion Engineering (CE) reactors, it is called the reactor regulating system. In B&W units, the ICS also controls the feedwater and turbine generator systems. The reactor control systems interface with the 120-Vac instrument power system, the control rod drive system, the nuclear instrumentation system, and the nonnuclear instrumentation systems of their respective units.

A.1.3.1.4 N04 Reactor Coolant System (PWR)

The reactor coolant system transports heat from the reactor core to the steam generators in which steam is produced for use in the unit's turbine. Depending upon the NSSS vendor and the generation of the design, two to four coolant loops are used. Loop design may involve one reactor coolant pump and one steam generator per loop or two reactor coolant pumps and one steam generator per loop. The reactor coolant system is a Safety Class 1 system. Electric power is provided by two or three separate buses depending on reactor design. The reactor coolant system is contained entirely within the containment building.

In PWRs reactor coolant pressure is maintained by a pressurizer that is connected to the piping between the reactor vessel and the steam generator (hot leg). Pressure is controlled by altering the saturation temperature and pressure of the steam and water that are inside the pressurizer. Condensing the steam volume by spraying cooler water into it reduces system pressure. Increasing the steam temperature by using electric heaters to heat the water volume increases system pressure. A system of pressure relief valves prevents overpressurizing the reactor coolant system.

The steam generators are vertical shell and tube (either straight or U-tube) heat exchangers in which hot reactor coolant water passes through the tubes heating secondary water on the shell side to the boiling point. Steam drying is accomplished inside the steam generators. Steam leaving the steam generators is transported to the unit's turbine by the main steam system.

The reactor vessel is an integral part of the RCS. The vessel makes up a part of the primary system pressure boundary, and it contains the reactor core, the core support structures, the in-core instruments, and the control rod guide tubes. In the Babcock and Wilcox NSSS, vent valves are placed between the upper plenum and the downcomer.

The reactor coolant system interfaces with the following systems:

- reactor core,
- control rod drive system,
- plant ac distribution system,
- dc power system (for pump-control circuitry),
- high-pressure safety injection system,
- residual heat removal system,
- chemical and volume control system,
- emergency boration system (Westinghouse reactors),
- main steam and feed water systems (through the steam generators),
- reactor building cooling water system (RC pump motor cooling),
- reactor vessel support system, and
- reactor cooling system piping.

A.1.3.1.5 N05 Emergency Boration System (PWR)

In the event of a steam line break or the spurious actuation of a main steam-pressure-relief valve in the presence of a stuck rod, PWRs require the rapid injection of a concentrated boron solution to control reactivity and to shutdown the reactor. In Westinghouse reactors, this function is provided by the emergency boration system. In CE and B&W reactors, boron injection is a function of the chemical and volume control system. The emergency boration system is a Safety Class 2 system which penetrates containment. Electric power is supplied by the essential ac distribution subsystem.

The emergency boration system is often a single-train system with redundant boron injection pumps. The pumps draw suction from a single tank and discharge into a header that connects to the suction side of each of the reactor coolant cold legs. Piping also connects the reactor coolant pump discharge to the boron injection tank. A recirculation loop which usually contains a pump and surge tank, is provided for testing and recirculating concentrated boric acid.

The emergency boration system interfaces with the following systems:

- essential ac distribution subsystem,
- reactor coolant system,
- chemical and volume control system,
- dc power system (for pump control circuitry), and
- emergency core cooling system (ECCS) actuation.

A.1.3.1.6 N06 Reactor Protection System (BWR and PWR)

The reactor protection system monitors the reactor, reactor coolant system, and other plant parameters important to safety. Upon an abnormal condition of any one or a combination of the various parameters, it instructs the control rod drive system to shut down the reactor to prevent fuel damage and in some instances to prevent the overpressurization of the reactor coolant system. The parameters which are typically monitored are

- reactor power and core power balance (axial and radial),
- reactor coolant temperature and pressure,
- operation of the reactor coolant or reactor recirculation pumps,
- reactor building pressure,
- feedwater flow, and

- turbine operation.

This list is not inclusive; thus, other parameters may be monitored depending upon the NSSS vendor and the design process.

Reactor protection systems are Class 1E systems and typically consist of four signal processing channels that are kept electrically independent and physically separate. The channel outputs are combined into a two-out-of-four (2/4) voting logic. The manner in which the 2/4 logic is developed depends upon the NSSS vendor. Each of the four signal processing channels monitors all of the plant parameters used by the particular design. When an abnormal condition of any of the parameters is sensed by a channel, the channel goes into a "trip" state. The coincidence of two signals on any of the four channels will cause the reactor protection system to initiate a reactor trip or shutdown.

Systems which interface with the reactor protection system are

- nuclear instrumentation or neutron monitoring system,
- nonnuclear instrumentation,
- ac instrument power system, and
- control rod drive system.

A.1.3.1.7 N07 Neutron Monitoring/Nuclear Instrumentation System (BWR and PWR)

The neutron monitoring or nuclear instrumentation system is used to monitor reactor performance and to provide this information to the plant operators, the reactor control system, and the reactor protection system. The neutron monitoring/nuclear instrumentation systems are typically made up of four to six subsystems depending upon the NSSS vendor. A source range monitor subsystem provides neutron flux indications during startup and low-power operation. The intermediate range monitor subsystem operates during low- and intermediate-power operations. In some designs, it may also input into the reactor protection system. The power range monitor subsystem provides flux indications during full-power operation. It is the prime source of neutron flux information for the reactor protection system. These three subsystems measure average reactor power and power imbalances. Some designs incorporate a local power range subsystem, which can provide detailed information about neutron flux throughout the reactor core and under any power level operation. In-core monitoring subsystems are also included and are usually used to calibrate the other subsystems. A rod block or rod withdrawal inhibit subsystem is also common and is used to prevent control rod withdrawals unless reactor coolant flow rates are within established boundaries.

The various sensors, with the exception of the in-core monitors, are mounted on the outside of the reactor vessel. All subsystems connected to the reactor protection system are Class 1E. In-core monitors are typically utilized for fuel management and are not classified 1E.

Systems which interface with the neutron monitoring/nuclear instrumentation system are

- o ac instrument power,
- o reactor protection system,
- o reactor control system, and
- o control rod drive system.

A.1.3.1.8 N08 Residual Heat Removal/Low Pressure Safety Injection System (BWR and PWRs)

The residual heat removal/low pressure safety injection system (RHR/LPSIS) is a versatile system which performs several functions during the various states of reactor operation. Its primary function is to remove heat from the reactor core during normal shutdowns, loss of coolant accidents (LOCAs), and post-LOCA conditions. It may also assist in containment heat removal and containment spray operations. The RHR/LPSIS is a Safety Class 2 system that is powered by the essential ac distribution subsystem. In some designs the RHR/LPSIS is called the decay heat removal/low pressure safety injection system or the shutdown cooling/low pressure safety injection system.

The RHR/LPSIS is a two- or three-train system depending upon the NSSS vendor and the design generation. Each train of the two-train designs has a 100% capacity and is redundant to the other train. Three-train designs require two of the three to operate in order to accomplish their function. Each train consists of a pump and a heat exchanger with their associated valves. In PWRs the pumps can be aligned to draw suction from the borated refueling water storage tank, the containment sump, or a hot leg (or legs) of the reactor coolant system.

During a normal shutdown, valve alignment directs flow from the reactor coolant system hot leg through the RHR pumps and heat exchangers into the reactor vessel (reactor recirculation system pump discharge in BWRs). Following a large LOCA, the LPSIS goes into a coolant injection mode when reactor vessel pressure lowers enough to permit operation. In this case, valve alignment directs suction from the borated or refueling water storage tank through the pumps and heat exchangers or piping to the reactor vessel. When the water level in the borated or refueling water storage tank falls to a predetermined height, suction in PWRs is changed to the containment sump and the storage tank is

usually valved out to prevent pump cavitation. This phase of operation is known as the recirculation mode.

The RHR/LPSIS interfaces with the following systems:

- o essential ac distribution subsystem,
- o dc power system (for pump- and valve-control circuitry),
- o reactor coolant/reactor recirculation system,
- o reactor building service water system, reactor building cooling water system or the chemical and volume control system (for secondary heat exchanger cooling),
- o refueling system (in PWRs), and
- o engineered safety features actuation system.

Other interfaces may include:

- o containment spray system, and
- o high-pressure safety injection system.

A.1.3.1.9 N09 Chemical and Volume Control System (PWR)

The chemical and volume control system controls the volume, purity, and boric acid content of the reactor coolant. The CVCS also provides seal injection water for the reactor coolant pumps. Coolant purity is controlled by continuously purifying a bypass stream of reactor coolant. Adjustments in coolant volume are made automatically to maintain a pre-determined level in the pressurizer. A "bleed and feed" technique is used to control the boric acid concentration in the reactor coolant. In B&W and CE units, the CVCS also supplies the emergency boration function.

Generally, the CVCS is a nonsafety system even though portions of it, such as the emergency boration piping and those sections of piping which form a part of the reactor coolant pressure boundary, are safety-grade piping. Electric power is supplied by the plant ac distribution system.

In B&W units, the chemical addition and boron recovery system, the letdown and purification system, and portions of the high-pressure injection system are the equivalent of the CVCS.

For coolant purification, a typical flow path through the CVCS is letdown from the RCS usually through a regenerative heat exchanger into a series of filters and demineralizers. Charging pumps draw suction from the volume-control tank and discharge, usually, back through the

regenerative heat exchanger into the RCS cold leg piping. The volume-control tank acts as a supply of coolant for increasing reactor coolant inventory and as a storage tank for inventory reduction.

The volume control tank is typically tied to the borated or refueling water storage tank or the boric acid mix tanks through boric acid transfer pumps and filters. Boric acid concentration in the reactor coolant is controlled by diverting the letdown stream to the boron recovery subsystem and sending either concentrated boric acid or demineralized water through the charging pumps.

Reactor coolant pump seal leakoff is collected in a header and usually is directed through a cooling heat exchanger to the volume-control tank. From there the charging pumps send a stream of flow through one of two redundant filters and a flow-control valve into a header that is connected to each reactor coolant pump seals.

Systems which interface with the CVCS are

- plant ac distribution system,
- dc power system (for pump- and valve-control circuitry),
- reactor coolant system,
- reactor building cooling water system (for nonregenerative heat exchanger secondary flow),
- demineralized water system,
- engineered safety features actuation system,
- refueling system,
- liquid radwaste system (for sluice from the filters and demineralizers),
- instrument air system (for flow-control valve), and
- gaseous radwaste (vents).

A.1.3.2 Engineered Safety Systems

The engineered safety systems grouping is made up of those systems, other than containment systems, that are used to mitigate the effects of a reactor accident such as a LOCA. The following systems descriptions are identified as relating to a BWR or a PWR or both.

A.1.3.2.1 S02 Engineered Safety Features Actuation System (PWR)

The engineered safety features actuation system monitors a number of plant parameters important to safety. An abnormal indication of any of these parameters will activate the ESFAS and the corresponding mitigation system to prevent excessive off-site radiation. Typical parameters which are monitored are

- reactor coolant or pressurizer pressure,
- reactor building pressure,
- refueling or borated water storage tank water level, and
- steam generator pressure (shell side).

The mitigating actions which are initiated by the ESFAS are

- high-pressure safety injection,
- low-pressure safety injection,
- containment isolation,
- low-pressure change to recirculation,
- containment cooling through ventilation,
- containment spray, and
- steam generator level control (in some systems).

The ESFAS is a Class 1E system that consists of three or four signal processing channels for each parameter which output typically into two, two-out-of-three (2/3) or two-out-of-four (2/4) voting logics. The exact combination of signal processing channels and voting logics for a particular reactor depends upon the NSSS vendor. An abnormal value for any of the monitored parameters will cause its signal processing channel to go into a "trip" state for each of the two voting logics. The coincidence of two tripped channels for the same parameter will cause the ESFAS to actuate the associated mitigation system or systems.

Systems which interface with the ESFAS are

- instrument ac power system,
- nonnuclear instrumentation,
- high-pressure safety injection system,
- residual heat removal/low pressure safety injection system,

- o containment cooling system,
- o containment spray system,
- o auxiliary feedwater system, and
- o any system which has valves that must be closed to isolate the containment.

A.1.3.2.2 S03 Safety Injection System (PWR)

The safety injection system is composed of three subsystems: the high-pressure safety injection subsystem, the safety injection tank/core flood subsystem, and the low-pressure safety injection subsystem. In B&W units, these subsystems are treated as individual systems. A discussion of each subsystem follows.

S03.A High-Pressure Safety Injection Subsystem (PWR)

The high-pressure safety injection subsystem (HPSIS) is designed to operate for small LOCAs when reactor coolant pressure has not been significantly reduced. In this circumstance, the HPSIS injects borated water into the RCS to provide cooling to limit core damage and fission product release and to ensure an adequate shutdown margin. The HPSIS is actuated by the ESFAS and is powered electrically by the essential ac distribution subsystem. The HPSIS is a Safety Class 2 system.

The HPSIS has two or three redundant trains depending upon the NSSS vendor. A typical train consists of a high-head pump which draws suction from the refueling water storage or volume-control tank, again depending upon the NSSS vendor. All pumps are started upon an initiation signal. The discharge from the pumps flows into the cold legs or hot legs of each reactor coolant loop. The particular connection point depends upon the NSSS vendor. Babcock and Wilcox and Combustion Engineering units have cold leg connections while Westinghouse units have cold leg and, in some plants, upper head connections.

The HPSIS interfaces with the following systems:

- o engineered safety features actuation system,
- o essential ac distribution subsystem,
- o dc power system (for pump- and valve-control circuitry),
- o chemical and volume control system or the refueling system, and
- o residual heat removal/low pressure safety injection system (for alternate suction).

S03.B Safety Injection Tank/Core Flood Subsystem (PWR)

The safety injection tank/core flood subsystem is a passive system that requires no external signal or power source to operate. It is designed to inject cooling water rapidly into the reactor vessel when vessel pressure falls below a predetermined level. The safety injection tank/core flood subsystem is a Safety Class 2 system.

In Westinghouse and CE designed reactors, the safety injection tank subsystem is a subsystem of the safety injection system. In B&W units the core flood system is a separate system which shares common reactor vessel inlet piping with the decay heat removal/low-pressure safety injection system.

Typically, there is one safety injection tank for each safety injection train. The tanks contain borated water and are pressurized to about 600 psig. Nitrogen is used to provide the charging pressure. The outlet of a safety injection tank is connected to a check valve which directs flow out of the tank. In series with the check valve is a motor-operated isolation valve. Under normal operating conditions, the motor-operated valves are open and reactor coolant pressure against the check valve outlets is enough to keep the valves closed. In the cold shutdown condition when reactor vessel pressure is not high enough to prevent the check valves' opening, the motor-operated valves are closed. In the event of a large LOCA, reactor vessel pressure will decrease. When the pressure has lowered below the charging pressure in the safety injection tanks the check valves will open, injecting cooling water into the vessel. The safety injection tanks contain enough borated water to cover the reactor core.

Systems which interface with the safety injection tank/core flood subsystem are

- reactor coolant,
- nitrogen subsystem of the plant gas system,
- borated or refueling water storage tank,
- other subsystems of the safety injection system or the RHR/LPSIS,
- plant ac distribution system (for motor-operated valve operation), and
- engineered safety features actuation system.

S03.C Low-Pressure Safety Injection Subsystem (PWR)

Low-pressure safety injection is a function of the RHR/LPSIS and is discussed in Sect. 1.3.1.11.

A.1.3.2.3 S04 Remote Shutdown System (BWR and PWR)

The remote shutdown system in both BWRs and PWRs usually consists of a remote control panel from which the systems necessary to bring the plant to a safe cold shutdown can be operated. The controls on the panelboard are redundant to their counterparts in the control room, and they are to be used in the event that the control room is damaged or becomes uninhabitable. The controls on the remote shutdown panel vary among NSSS designs. In some instances the remote shutdown system is a bunkered system. It is designated as a Class 1E system and interfaces with the following:

- o control rod drive system,
- o nuclear instrumentation system,
- o nonnuclear instrumentation system, and
- o essential ac power system.

A.1.3.2.4 S05 Auxiliary Feedwater System (PWR)

The auxiliary feedwater system is designed to provide an adequate supply of cooling water to the steam generators so that they can act as heat sinks for decay heat removal from the reactor core in the event of a loss of power, a feedwater line malfunction, a small LOCA, or a main steam line break. The system is a Safety Class 3 system with the exception of the piping between the isolation valves and the connections to the feedwater piping. These sections of piping are Safety Class 2. The auxiliary feedwater system generally penetrates containment. Electric power is provided by the essential ac distribution subsystem.

A turbine-driven pump is supplied steam from taps on the main steam lines. The auxiliary feedwater system is actuated by its own control system. Actuation may be initiated by a loss of ac power, a decrease in feedwater header pressure, a safety injection signal, low level in the steam generators, or a manual signal. During startup, the auxiliary feedwater system is used to increase steam generator pressure by drawing suction from the condensate storage tank. This provides enough steam to start the main feedwater pumps.

The auxiliary feedwater system may also be called the emergency feedwater system.

The auxiliary feedwater system typically consists of two motor-driven feedwater pumps and one steam turbine-driven feedwater pump. All three pumps are sized for 100% capacity; operation of only one pump is needed. All start on the actuation signal. The turbine-driven pump will operate as long as steam is available from the main steam lines

and dc control power is available. The pumps usually draw suction from two or more sources. Among the sources may be an auxiliary feedwater storage tank, the condensate storage tank, the service water system, and the condenser hotwell. The pumps' discharge typically passes through a common header before entering the piping connected to the main feedwater lines. There is at least one auxiliary feedwater line for each main feedwater line. Flow control in each auxiliary feedwater line is established by a flow-control valve.

The following systems interface with the auxiliary feedwater system:

- o main steam system,
- o feedwater system,
- o essential ac distribution system,
- o dc power system (for pump-control circuitry),
- o engineered safety features actuation system,
- o condensate system,
- o condenser storage system,
- o demineralized water system (makeup to the auxiliary feedwater storage tank), and
- o instrument air system (for pneumatic valves).

A.1.3.3 Containment Systems

The containment systems grouping is made up of the containment (primary and secondary, as applicable) and those systems needed to prevent containment overpressure, to prevent excessive leakage from the containment to the environment, and to provide a habitable atmosphere inside containment. The systems discussed in this section relate to a BWR or a PWR or both.

A.1.3.3.1 CO2 Reactor Building/Containment and Penetrations (PWR)

As in BWRs, the PWR containments are designed to mitigate the consequences of postulated accidents inside containment by containing the radioactive fluids and fission products that may be produced by the accidents. The containment is usually a cylindrical or hemispherical carbon steel lined, reinforced concrete structure which houses the reactor vessel, reactor coolant system, control rod drive mechanisms, emergency sump, various instrumentation, and other equipment. In some instances an air space, or annulus, separates the carbon steel liner and the concrete structure. Numerous electrical and piping penetrations pass through the containment structure. Two personnel

hatches, a fuel transfer tube, and one equipment hatch is typical. The electrical and piping penetrations are sealed by double O-ring or double gasket seals. All connecting cabling and piping pass through a penetrating room before attaching to the penetrations. The penetration room contains any gases that may leak through the penetrations during an accident situation. Equipment and personnel hatches are double-door air locks that are interlocked to prevent the simultaneous opening or both doors.

A.1.3.3.2 C03 Containment Cooling System (PWR)

The containment cooling system is designed to help reduce containment pressure following a pipe break inside containment by cooling and condensing the steam generated by the break. The containment cooling system typically works together with the containment spray system and the water in the emergency sump to reduce containment pressure. The containment cooling system is totally housed inside the reactor building. It is a Safety Class 2 system. Electrical power is provided by the essential ac distribution subsystem, and the actuation signal is generated by the engineered safety features actuation system on the occurrence of a 4-psig pressure inside containment.

The containment cooling system may also be known as the reactor building cooling system or a subsystem of the containment atmosphere recirculation system.

A typical system configuration has two to three fans which discharge through cooling coils into a common header. Fan suction is taken from air registers near the roof of the reactor building. After passing through the cooling coils and common header, the fan discharge is directed by ductwork into the lower portion of the reactor building structure. The air then flows upward through the reactor building and around the reactor vessel gaining heat as it rises. At the intake registers, the cycle starts again.

The containment cooling system interfaces with the reactor vessel, the reactor building, and the essential ac distribution subsystem.

A.1.3.3.3 C04 Containment Isolation (PWR)

Containment isolation is one of the functions provided by the ESFAS in PWRs. This system is discussed in Sect. 1.3.2.2.

A.1.3.3.4 C05 Containment Purge System (BWR and PWR)

The containment purge system is designed to provide a habitable working environment for personnel inside the containment structure by reducing airborne radioactivity and providing outside air during periods of extended occupancy. The containment purge system is a nonsafety system which is powered by the plant ac distribution system. The containment

purge system works essentially in the same fashion in both BWRs and PWRs.

In some designs, the containment purge system may be a subsystem in a containment atmosphere recirculation and cleanup system.

The containment purge system is usually divided into two subsystems: a supply subsystem and an exhaust subsystem. The supply subsystem uses a fan to draw in outside air. The air is filtered before entering the fan and heated after discharge. Then, the air is exhausted to the containment. The exhaust subsystem also uses two fans to draw air from the containment. Containment air passes through a multistage filtering system before it enters the fans. Fan exhaust discharges through the unit vent. The exhaust is usually monitored for radiation. On the occurrence of high radiation, selected dampers are closed, and the air flow goes into a recirculation mode. Some designs have a filtration system that can be connected to most or all of the containment air systems. The dual action of removing and filtering containment air and bringing in fresh air tends to lower the airborne radioactivity levels inside containment.

Systems which typically interface with the containment purge system are the plant ac distribution system, the containment, and in some instances, a glycol system for heating the fresh air.

A.1.3.3.5 C07 Combustible Gas Control System (BWR and PWR)

The combustible gas control system monitors the hydrogen content inside containment after a LOCA and maintains the concentration at a safe level. The system in newer designs is usually divided into two subsystems: the hydrogen recombiner subsystem is a Safety Class 2 system, and its backup, the dilution air subsystem, is nonsafety. Typically, older designs have a Safety Class 3 dilution air system. The recombiner subsystem is supplied electrical power by the essential ac distribution. The dilution air system is supplied by the nonessential portion of the ac distribution system in newer designs. Both BWR and PWR systems operate in essentially the same manner.

In older designs, this system may be referred to as a hydrogen purge system.

The recombiner subsystem design usually features two redundant recombiners with their associated fans, aftercoolers, and ductwork. The combiners may be either catalytic or electric. The dilution air subsystem has two piping trains, a supply train and an exhaust train, which operate in the same manner as the containment purge system (Sect. 1.3.3.9). The exhaust subsystem may also discharge into the gaseous radwaste system. A hydrogen analyzer continuously monitors containment air and actuates an alarm when the hydrogen concentration reaches a preset level, usually less than 4%. The combustible gas control system is manually initiated.

The plant ac distribution system is the primary interface for the combustible gas control system. The gaseous radwaste system may also interface.

A.1.3.3.6 C08 Containment Ventilation System (BWR and PWR)

The containment ventilation system circulates air within the containment to maintain the bulk air temperature suitable for personnel and equipment. The containment ventilation system is a nonsafety system and is supplied power from the plant ac distribution system. This system operates continuously under normal plant conditions but is shut off under accident conditions. Ventilation systems in both BWRs and PWRs work in the same fashion; each has ductwork branching to supply a flow of air to each of the rooms and compartments within the containment.

The containment ventilation system is also called the reactor building ventilation system, or it may be a subsystem of the containment atmosphere recirculation system. The containment ventilation system may be divided into various subsystems also. In BWRs the subsystems may include the drywell ventilation system. Those PWR containments that have an annulus (the air space between the steel liner and the reinforced concrete) typically have an annulus ventilation system as a subsystem.

The containment ventilation system typically consists of two or three fans and their associated ductwork and dampers. The fans generally discharge into a common header from which the ductwork branches into the various rooms and compartments. Some systems have a filtering unit installed in the ductwork. The system is manually operated from the control room.

The plant ac distribution system is the only system which directly interfaces with the containment ventilation system.

A.1.3.3.7 C10 Containment Spray System (PWR and BWR)

The containment spray system provides a water spray to the containment following a LOCA or steam line break to limit containment pressure and to minimize the release of radioactive iodine and particulates to the environment. The containment spray system is a Safety Class 2 system which is found in all PWR designs. Newer BWR designs have a containment spray which is a subsystem of the RHR/LPSI (Sect. 1.3.1.11). Electric power for the containment spray pumps is provided by separate essential ac distribution subsystem buses. The containment spray system is normally housed in the auxiliary building with the exception of the spray headers and nozzles, which are in the containment.

The containment spray system may also be called the reactor building spray system.

There are a number of possible configurations for the containment spray system. It is normally a two- or three-train system which draws suction either directly from the refueling water storage tank and the emergency sump, or indirectly from these sources through the RHR/LPSIS or the safety injection system. Most systems have chemical addition tanks from which sodium hydroxide (NaOH) or hydrazine is added to the spray water. These chemicals have the dual effect of improving iodine removal from the containment atmosphere and of neutralizing much of the corrosive effects of the boric acid in the refueling storage tank water. Each of the two or three piping trains has a containment spray pump which discharges into a spray header or headers inside the containment. In some designs, the pumps discharge through containment spray heat exchangers. The containment spray system may be manually actuated, or it may be automatically actuated by the ESFAS. High containment pressure (~10 psig) causes the ESFAS to actuate containment spray.

The following systems typically interface with the containment spray system:

- o essential ac distribution subsystem,
- o dc power system,
- o refueling water system (condensate storage system for BWRs),
- o emergency sump,
- o residual heat removal/low pressure safety injection system,
- o reactor building cooling water system (when heat exchangers are included), and
- o chemical and volume control system (for the addition of NaOH or hydrazine).

A.1.3.3.8 C11 Penetration Room Ventilation System (PWR)

Those reactor buildings that do not have a steel liner usually have a penetration room through which all connections to electrical or piping penetrations must pass. The penetration room is outside of an adjacent to the reactor building. After an accident, some leakage will occur around the electrical and piping penetrations. The penetration room ventilation system is designed to prevent this leakage from escaping into the environment. It is a Safety Class 3 system and is powered by the essential ac distribution subsystem.

The penetration room ventilation system is a two-train system. The two redundant fans draw suction from the penetration room and discharge through a multistage filter unit into the unit vent. When high radiation occurs at the vent, the system goes into a recirculation mode, or the flow is routed to the gaseous radwaste system. The suction from the penetration room keeps it at a slightly lower pressure than the outside so that any leakage is into the room rather than from the room. The penetration room ventilation system is manually actuated from the control room.

Systems which may interface with the penetration room ventilation system are the essential ac distribution subsystem and, possibly, the gaseous radwaste system.

A.1.3.4 Electrical System

The electrical system is made up of plant systems that supply electric power to either the utility grid or to other plant systems that are purely electrical.

A.1.3.4.1 E01 Main Power System

The non-Class 1E main power system receives electric power from the unit generator and directs it to the main stepup transformer where the voltage is raised to a level compatible with the utility transmission system.

There are two basic arrangements of the main power system. In the first, an isolated phase bus is used to connect the unit generator to the main stepup transformer. The second arrangement has a split isolated phase bus and two "half size" main stepup transformers. In both bases taps are provided on the isolated phase bus for connections to a unit auxiliary transformer that supplies the plant ac distribution system. Some newer designs also incorporate generator breakers which are connected to the unit generator terminals. These breakers are used to isolate the unit generator such that power can be backfed from the switchyard through the main transformer to the plant ac distribution system. The isolated phase buses normally are provided with a cooling system.

Protective relaying for the main power system is designed to protect and isolate the equipment should a fault occur. If a fault occurs, the relays will initiate the opening of the appropriate circuit breakers to isolate the faulted equipment and limit equipment damage. Relays that provide instantaneous overcurrent or time overcurrent protection and differential zone protection are typical.

Systems which interface with the main power system are:

- turbine generator,

- o switchyard, and
- o plant ac distribution system (through the unit auxiliary transformer).

A.1.3.4.2 E02 Plant AC Distribution System

The plant ac distribution system receives power from the unit auxiliary transformer, the standby or reserve auxiliary transformer (preferred for unit shutdown), or the emergency ac power system. The Class 1E essential ac distribution subsystem provides electric power to systems that bring the plant to a safe shutdown following an accident. The essential ac distribution subsystem is further divided into two or three redundant independent trains. These trains are kept electrically separate and are separated physically as much as possible. Separation is used to reduce the probability of common-cause failure of redundant systems. The non-Class 1E nonessential ac distribution subsystem supplies electric power to the remainder of the plant's systems.

The plant ac distribution system is a hierarchical arrangement of switchgear at three or four voltage levels. Both essential and nonessential subsystems are constructed in this manner. The highest voltage levels are fed from the unit generator through a unit auxiliary transformer when the unit is operating. When the unit is shut down, plant loads are fed from the switchyard through a reserve or transformer or, in the case of a generator breaker design, from the switchyard through the main transformers to the unit auxiliary transformers. The highest voltage level is either 13,800- or 6,900-V (for a few it is 4160-V) which supplies the reactor coolant pumps (RCP). Power distributed through the plant is normally supplied from the 4160-V buses. It is at the 4160-V lines that the essential-M-nonessential distinctions are first made. Other than the RCPs, most large pump motors in the plant are supplied from these switchgear. Also the lower voltage switchgear are supplied from the 4160-V switchgear. Some designs have essential and nonessential switchgear at this level. Other designs have one set of switchgear with both essential and nonessential loads. In the event of an accident, all loads are shed from the switchgear, with only the essential loads picked up again as the emergency diesels come to speed. (In the Oconee plant, emergency power is from a hydro plant, which can start under load. Here only, nonessential loads are ever shed.) When normal power is not available, the emergency power system generally is connected at the 4160-V level.

The next voltage level is either 600- or 480-V. Switchgear at this level are fed from 4160-V switchgear through auxiliary transformers. This voltage level is used to supply power to medium-to-small pump and fan motors and large valve-operator motors. Plants also have switchgear at the 208- or 120-V level supplied from 600- or 480-V through auxiliary transformers. Small valve-operator, pump, and fan motors are powered from these switchgear. Some instrumentation may

also be included on these switchgear. The separation between the nonessential and the various trains of the essential subsystems are maintained at these voltage levels.

Switchgear above the 120-V level typically have two breakers through which they may be supplied power. Only one of the supply breakers is closed at any one time. Relays are supplied to coordinate the operation of the normally closed and normally open supply breakers.

Relays are installed to protect loads, buses, and cables and to isolate faults at the lowest possible level. The protection scheme is coordinated using instantaneous and time overcurrent relays, differential relays, thermal overload, lock-out relays and other protective device to limit equipment damage for fault current or other abnormal conditions.

The following systems interface with the plant ac distribution system:

- o main power system,
- o switchyard,
- o emergency power system,
- o dc power system,
- o plant safety related systems (essential ac distribution subsystem), and
- o plant nonsafety related subsystems (nonessential ac distribution subsystem).

A.1.3.4.3 E03 Instrumentation and Control Power Systems

The instrumentation and control power systems provide dc or ac power to the instruments and control circuits for the plant. The dc power system is designed to supply either 125- or 150-V dc to its designated loads. The instrument ac power system supplies 120-V ac to its designated loads. The distinction between safety and nonsafety power supplies is kept in these systems. Each system is discussed in the following sections.

E03.A DC Power System

The dc power system supplies an uninterruptable source of dc electrical power to some instrumentation and numerous control circuits in the plant. Safety related dc loads are supplied from a Class 1E vital dc power subsystem. Other dc loads are supplied from the plant dc power system. However, many plants supply non-Class 1E loads from a Class 1E

dc power system. The Class 1E system is protected by a Class 1E breaker that can isolate the nonsafety load.

The Class 1E vital dc power subsystem may be composed of four separate panelboards which are supplied electric power by a battery charger connected in parallel with a 125-V battery. The battery chargers are connected to the 600/480-V switchgear in the essential ac distribution subsystem (Sect. 1.3.4.2). In the event of a loss of ac power, the batteries maintain uninterrupted power to their loads. Control circuits for ac circuit breakers and the inverters for the instrument ac power system (Section A.1.3.4.5) are important Class 1E loads on the dc panelboards.

The non-Class 1E plant dc power subsystem is constructed similar to the vital dc power subsystem except that sometimes it is two 125-V sources to supply 250-V as well as 125-V dc power. The 250-V plant dc power subsystem supplies loads such as emergency lighting and emergency lube oil sumps for nonsafety loads.

The dc power system interfaces with the following systems:

- o plant ac distribution system,
- o instrument ac power system,
- o most of the safety related plant systems (vital subsystem for control circuitry), and
- o most of the nonsafety plant systems (plant subsystem for control circuitry).

E03.B Instrument AC Power System

The instrument ac power system provides an uninterruptible source of 120-V single phase ac power to the plant's non-Class 1E instrumentation and to the plant computer. Safety related instrumentation is supplied from the vital instrument ac power subsystem.

The Class 1E vital instrument ac power subsystem normally has four separate panelboards. Each panelboard is supplied power from an inverter which is connected to a vital dc power panelboard or, for short times such as during maintenance, from a nonsafety, regulated power supply that can be corrected by a manual selector switch. Loads on the vital instrument ac power panelboards are reactor protection system (RPS) channel cabinets and the ESFAS channel cabinets and other safety related instruments.

The non-Class 1E plant instrument ac power subsystem is supplied by inverters or by a regulated, 120-V, single-phase supply. Nonsafety instrumentation, the plant computer, and the turbine-generator electro-

hydraulic control (EHC) system are supplied by the plant instrument ac power system.

Systems interfacing with the instrument ac power system are

- dc power system,
- plant computer,
- reactor protection system,
- engineered safety features actuation system,
- turbine-generator electro-hydraulic control system,
- other safety related instrumentation (vital subsystem), and
- other nonsafety related instrumentation.

A.1.3.4.4 E04 Emergency Power System

The emergency power system is designed to supply an adequate amount of electrical power to safely shut down the plant when the normal ac power supply has been lost. The system has two distinct portions: an electrical system and a supporting group of mechanical systems. The electrical portion is Class 1E and the mechanical systems are Safety Class 3.

The electrical portion of the emergency power system typically consists of a diesel-powered generator, a circuit breaker to connect the generator to a 4160-V switchgear, undervoltage relays on the 4160-V switchgear to actuate the emergency power system, and the load-shedding and load-sequencing circuitry. There are typically two emergency power trains. The supporting mechanical subsystems are discussed in the following sections.

The Oconee Nuclear Power Plant does not use diesels to power its emergency ac power system; it is the only plant in the U.S. that has two hydro generators that serve the functions normally performed by the diesels. To make the discussion generic, a description of diesel powered ESF was included.

The plant ac distribution system and the dc power system are the only plant systems that interface with the electrical portion of the emergency power system.

E04.A Diesel Generator Fuel Oil Subsystem

The diesel generator fuel oil subsystem supplies the fuel to run the generators in the emergency power system. There is a fuel system for each diesel. Most nuclear units have fuel systems sized to operate the

diesels for 7-d when the diesel is operating under maximum loading conditions. The diesel generator fuel oil subsystem is a Safety Class 3 system.

The fuel system consists of one or two large storage tanks and a smaller day tank for each diesel. Redundant pumps transfer fuel oil from the storage tank to the day tank. The pumps can be manually actuated, or they can be actuated by the level in the day tank. Depending upon the design, the day tank may supply fuel to the diesel via a fuel pump or gravity feed.

The diesel generator fuel oil subsystem interfaces with the essential ac distribution subsystem and the dc power system.

E04.B Diesel Generator Cooling Water Subsystem

The diesel generator cooling water subsystem provides cooling for the diesel generators. The system may also have heaters in the diesel jacket-water for warning the diesel when it is shut down. The diesel jacket-water may be cooled by plant service water or by air. The diesel generator cooling water system is a Safety Class 3 system.

Typical system configuration features redundant pumps that discharge into the diesel jacket. Pump suction draws from the diesel jacket through a radiator or heat exchanger and a lubrication oil cooler. A surge tank regulates water inventory. A recirculation loop with a heater and a small pump warms the jacket when the diesel is not operating. The temperature of the water leaving the diesel jacket is monitored and trips the diesel if an excessive temperature is reached. In some plants, this trip is bypassed when an ESF actuation signal occurs.

Systems which interface with the diesel generator cooling water subsystem are

- essential ac distribution subsystem,
- dc power system (for control circuitry),
- station service water system (heat exchanger cooling), and
- diesel generator lubrication oil subsystem.

E04.C Diesel Generator Starting Air Subsystem

The diesel generator starting air subsystem supplies compressed air to starting motors on the diesel generators to provide for a rapid start of the diesel. Each diesel has a separate starting air system except for some older diesels that are started by electric motors. The diesel generator starting air system is a Safety Class 3 system.

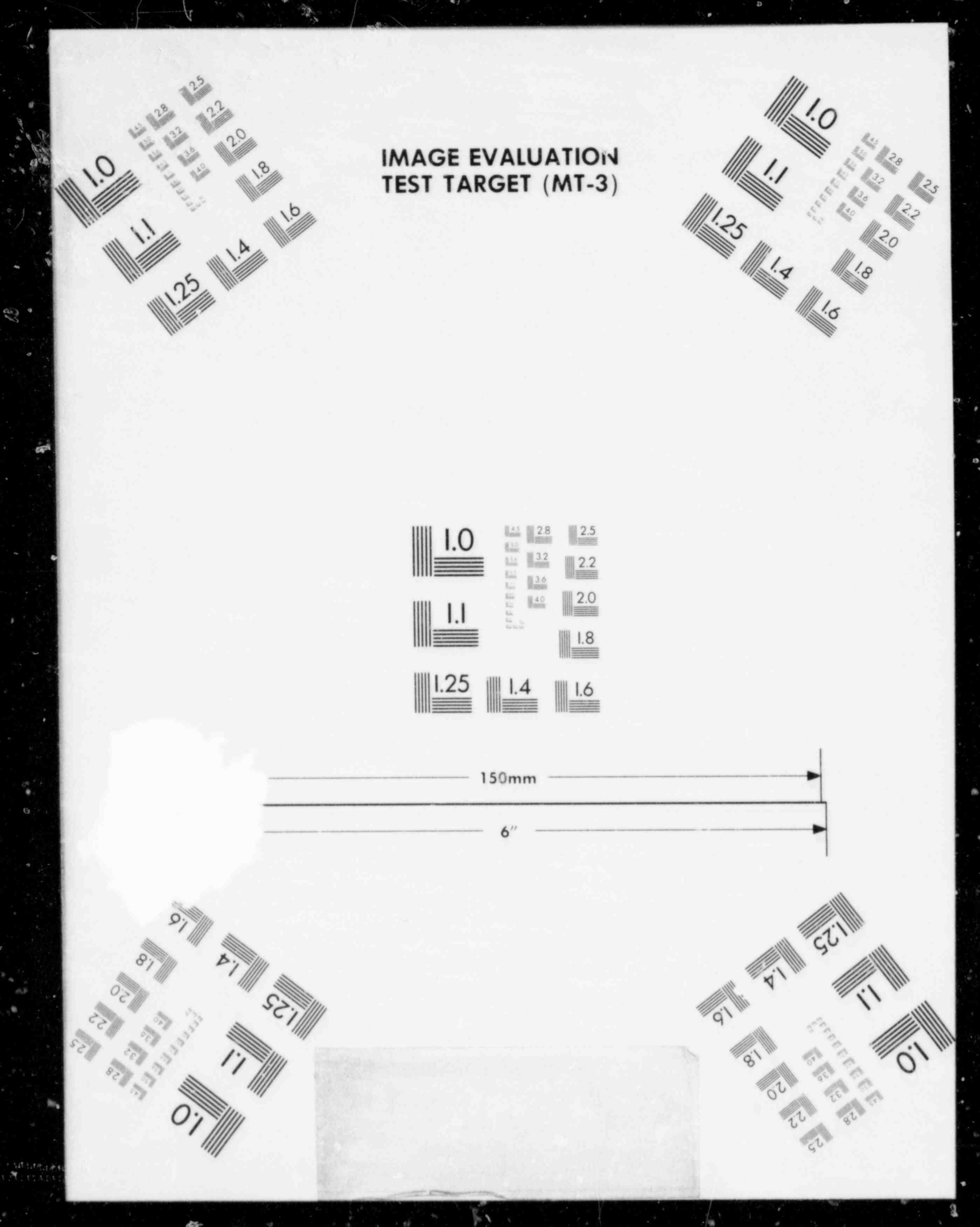


IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

This system is typically a two-train system. Each train has an air compressor which exhausts into compressed air storage tanks. Compressor suction is taken from the atmosphere and filtered before it enters the compressor. A cross tie is typically provided between the two trains. An air dryer has been found to be important because of the number of failures caused by moisture (usually corrosion) in the starting air.

The essential ac distribution subsystem and the dc power system interface with the diesel generator starting air subsystem.

E04.D Diesel Generator Lubrication Oil Subsystem

The diesel generator lubrication oil subsystem supplies oil to lubricate the moving parts of the diesel generator. Each diesel has a lube oil system. The system is designated as Safety Class 3.

The system features a loop with a motor-driven pump, which increases oil pressure enough to permit starting the diesel. This loop is sometimes filtered and heated. After the diesel has started, lube oil pumps circulate oil through the engine. The recirculation loop usually has a filter and a lube oil cooler.

The systems which interface with the diesel generator lubrication oil system are the essential ac distribution subsystem, the dc power system, and the diesel generator cooling water subsystem.

A.1.3.4.5 E05 Plant Lighting System

The plant lighting system provides illumination in the plant for personnel to perform their required tasks. The system is typically divided into essential and nonessential subsystems. The essential subsystem is Class 1E and provides lighting for those areas in the plant in which personnel activity will be required after an accident. The nonessential subsystem is a nonsafety system. Outdoor lighting may also be provided.

The plant lighting panelboards are usually loads on the vital instrument ac power subsystem, the plant ac power subsystem, and/or the 120-V level of the nonessential ac distribution system, depending upon the safety designation of the lighting system.

A.1.3.4.6 E06 Plant Computer

The plant computer functions vary among plants. Typical among the functions are

- monitoring and printout of plant parameters,
- performance of calculations based on plant parameters,

- o various information displays through either a printer or a cathode ray tube (CRT), and

- o in some designs, control of selected balance-of-plant systems.

The plant computer is a nonsafety component. Its power is supplied by an inverter or other regulated, 120-V, single-phase power supply.

A.1.3.4.7 E07 Switchyard

The switchyard links the unit and the utility's transmission grid. Transmission lines distribute the power produced by the unit to transmission substations, which further distribute the power. The switchyard is connected to the generator through the main transformer. It also provides power through a startup transformer when the unit is shutdown. The switchyard is not safety related and is under control of the transmission system dispatch center.

There are many switchyard designs. Important factors considered in the design are capital costs and equipment availability.

The switchyard interfaces with the main power system and sometimes with the plant ac distribution system.

A.1.3.5 Power Conversion System

The power conversion system grouping is made up of the systems and components that are used to transform, or support the transformation of, heat energy produced by the reactor core into electrical energy.

A.1.3.5.1 P01 Main Steam System

The main steam system is used to transport the steam generated in the steam generators to the turbine generator. The interface with the turbine generator is at the turbine stop valves. Depending upon the design, from two to four steam lines may be used. The main steam system is a nonsafety system which penetrates containment although portions of the system are safety related.

After leaving containment, several pressure-relief valves are connected, in parallel, to the main steam lines. Groups of these are normally set to open at three succeedingly higher pressure levels. Next in the steam lines are the main steam-isolation valves (MSIVs). These valves usually are pneumatically actuated and require two coincident signals from the ESFA system to actuate a closure. The MSIVs are Safety Class 3 components. Between the MSIVs and the turbine stop valves are a number of steam taps. One tap is in each leg for the turbine-bypass-to-condenser lines and the atmospheric dump valves. Taps also supply steam for the main feedwater pump turbines, the auxiliary or emergency feedwater pump turbines, and the moisture

separator reheaters. A connecting line for the auxiliary steam system is also provided.

The main steam system interfaces with the following systems:

- dc power system (for MSIV control circuitry),
- instrument air system,
- reactor coolant system (through steam generators in PWRs),
- turbine generator,
- turbine bypass system,
- feedwater system,
- auxiliary feedwater system, and
- auxiliary steam system.

A.1.3.5.2 P02 Turbine Generator System

The turbine generator is the device used to transform mechanical (steam) energy to electrical energy. The turbine generator is a nonsafety system that is supported by subsystems. The turbine is normally a three-stage device with the stages mounted axially along the turbine shaft. The first stage is a high-pressure turbine; the last two stages are low-pressure turbines. The high-pressure turbine is driven by the main steam system. From the exhaust of the high-pressure turbine, the steam is directed through the moisture separator reheaters and then to the low-pressure turbines. The low-pressure turbines exhaust into the condenser. Taps are provided on the high- and low-pressure turbines to supply steam to the condensate and feedwater heaters. Generator output is connected to the main stepup transformer through an isolated phase bus.

The turbine is controlled by an electro-hydraulic control (EHC) subsystem. The turbine is controlled by regulating the flow of steam through it. The EHC subsystem accomplishes this by throttling the turbine-control and intercept valves. To trip the turbine, the turbine-stop valves are closed shutting off the steam supply. Generator voltage is controlled by an exciter system.

Systems which interface with the turbine generator system are

- main steam system,
- electro-hydraulic control subsystem,
- turbine gland seal subsystem,

- o turbine lubrication subsystem,
- o stator (hydrogen) cooling subsystem,
- o hydrogen seal oil subsystem,
- o main power system,
- o feedwater and condensate systems (through steam supply to the water heaters), and
- o condenser.

Turbine Generator Subsystems

The EHC subsystem controls the turbine by regulating the steam flow through the turbine. The EHC subsystem is capable of remote, manual, or automatic starting of the turbine, loading the turbine at a preset rate, and holding load and speed at a preset level. The EHC subsystem typically has three distinct sections: a speed-control unit, a load-control unit, and a valve-positioning unit. Steam flow through the turbine is accomplished by throttling the pneumatically operated turbine-control valves and intercept valves. Trips are accomplished by closing the turbine-stop valves. Turbines designed by Allis-Chalmers provide a backup mechanical-hydraulic control system.

The turbine gland seal subsystem seals the turbine shaft between both turbine casings and between the exhaust hoods and the atmosphere. This prevents air from leaking into the turbine building. The shaft seals are labyrinth or pressure-packing glands through which steam is passed outward away from the turbine. The seals exhaust into a gland steam condenser.

The turbine lubricating subsystem supplies oil to lubricate the moving parts of the turbine generator. The subsystem is divided into two parts: a lubricating oil section and an oil conditioning system. The lubricating oil section consists of bearing oil pumps, an oil reservoir, and oil coolers in series. The oil conditioning section is made up of a clean oil storage tank, a used oil storage tank, a filtering unit, and an oil transfer pump. Water from the turbine building cooling water system is used to cool the oil in the heat exchangers.

The stator (hydrogen) cooling subsystem is used to remove heat from the coils of the generator stator. The hydrogen fills the stator housing and keeps the stator windings in a moisture-free condition. When replacement of the hydrogen is necessary, it is displaced by carbon dioxide (CO_2), and then a fresh supply of hydrogen is added. This system consists of pressure regulators and controls for the hydrogen gas and a CO_2 circuit for purging operations.

The hydrogen seal oil subsystem is used to prevent hydrogen leakage through the generator shaft seals. This system circulates oil through the shaft seals entraining any hydrogen that leaks into them. The system consists of pumps, storage tanks, and the controls necessary to degasify the oil before returning it to the shaft seals.

A.1.3.5.3 P03 Turbine Bypass System

The turbine bypass system allows the NSSS to follow approximately a 50% step load reduction to the turbine generator without causing a reactor trip or lifting the main steam pressure-relief valves. The turbine bypass system is a nonsafety system.

The turbine bypass system consists of a pneumatically or electrically operated turbine-bypass valve and controls, one or two isolation valves and controls, and associated piping for each main steam line. On the occurrence of a large reduction in electrical load, the turbine-bypass valves open relieving main steam directly to the condenser. Some designs use a group of small turbine-bypass valves in parallel rather than a single large valve for each steam line. This helps prevent an uncontrollable cooldown if a valve sticks open. The turbine-bypass valves are opened automatically by the turbine EHC subsystem following a large load reduction. During a normal shutdown of the reactor, the turbine-bypass valves are opened manually to release steam generated by decay heat in the reactor. As cooldown continues, the turbine-bypass valve is throttled closed eventually transferring the decay heat removed to the RHR/LPSIS.

The turbine bypass system interfaces with the following systems:

- Main steam system,
- Condenser,
- EHC subsystem,
- Instrument air system, and,
- Plant ac distribution system (for motor-operated isolation valves).

A.1.3.5.4 P04 Condenser and Condensate System

The function of the condenser is to condense steam from the low-pressure turbine exhausts, the feedwater pump turbines, and the turbine bypass system. The condensate system takes condensed steam from the condenser and heater drains and delivers it to the feedwater system. Along the way the condensate is purified and heated. The condenser and condensate system is a nonsafety system.

The condenser is a triple-shell, single-pass water box in which circulating cooling water is used to condense steam from the turbine. As the steam condenses into a liquid, it is collected in the hotwell sections of the condenser. In the event that one train of the circulating cooling water is lost, a condenser circulating water pump is activated to provide water to both sides of the condenser shell.

The condensate system draws the condensed steam from the hotwells through two or three condensate pumps. The pumps discharge through the steam jet air ejectors and gland steam condensers before passing to the condensate cleanup/polishing system. This system may be bypassed. The exact order of these components and systems varies with design. From the condensate cleanup/polishing system, the system water pressure is raised by two or three condensate booster pumps. The discharge from these pumps is passed through a string of condensate heaters. From the condensate heaters, the water enters the feedwater system. A condensate storage tank is a subsystem provided at the discharge of the booster pumps to act as a surge tank and help regulate the system water inventory. A number of flow-control and isolation valves are scattered throughout the system. Their operation generally requires instrument air or electrical power. Condensate makeup is provided by the demineralized water system.

The condenser and condensate system interfaces with the following systems:

- turbine generator,
- turbine bypass system,
- feedwater system,
- turbine gland seal subsystem,
- condenser evacuation subsystem,
- condensate cleanup/polishing system,
- auxiliary feedwater system,
- auxiliary steam system,
- demineralized water system,
- instrument air system,
- dc power system, and
- plant ac distribution system.

P04.A Condenser Evacuation System

The condenser evacuation system is designed to provide initial vacuum in the condenser shells during startup, to maintain the vacuum during condenser operation, and to dispose of noncondensable gases collected from the condenser. The loss of condenser vacuum allows buildup of noncondensable gases, which inhibit the heat transfer capability of the condenser. The condenser evacuation system is a nonsafety system.

Steam jet air ejectors are used to remove noncondensable gases from the condenser and to maintain the vacuum in the condenser shells. This is done by passing a jet of steam through the condenser shells. The passage of the steam creates a vacuum which draws the noncondensable gases into the jet stream. The air ejectors exhaust into the gaseous radwaste system. The steam jet air ejectors function by using auxiliary steam. Motor drive air removal pumps remove initial condenser shell side air.

The condenser evacuation system may also be known as the condenser vacuum system or the vacuum system.

Systems interfacing with the condenser evacuation system are

- condensate system,
- auxiliary steam system,
- gaseous radwaste system, and,
- plant ac distribution system.

P04.B Condensate Cleanup/Polishing System

The condensate cleanup/polishing system removes impurities which result from the condensate water. This results in a high purity effluent capable of meeting feedwater and steam generator chemistry standards. This is a nonsafety system.

The condensate cleanup/polishing system consists of several mixed-bed demineralizers. The exact number depends upon design; however, sufficient capacity usually is provided for operation at full condensate flow while one of the demineralizers is being regenerated. Differential pressure around the demineralizers is monitored to detect impaired flow. At a preset pressure level, a bypass valve is opened to prevent demineralizer damage.

The condenser cleanup/polishing system interfaces with the following systems:

- condensate system and

- plant ac distribution system.

P04.C Condensate Heater Drain Subsystem

The condensate heater drain subsystem collects the steam condensed in the condensate heaters and returns it to the main condenser. The condensate heater drain system is a nonsafety system.

The steam passing through the shell side of the condensate heaters is collected in a common header. Depending upon design, either gravity-flow or motor-operated pumps return the water to the condenser.

The condenser, the main steam system (extraction steam), the condensate system, and the plant ac distribution system interface with the condensate heater drain system.

A.1.3.5.5 P05 Feedwater System

The feedwater system takes condensate from the condensate system, heats it, raises its pressure, and delivers it to the steam generators in PWRs or the reactor vessel in BWRs to be boiled off as steam. The feedwater system is a nonsafety system that penetrates containment.

In general, two steam turbine-driven main feedwater pumps draw suction from the condensate system. Some plants (particularly Westinghouse designed) have electric powered main feedwater pumps. Both pumps are needed for full operation. The pumps discharge through a string of feedwater heaters into a common header. From the header, one feedwater line goes to each steam generator in PWRs. The BWRs generally have two lines which lead to the reactor vessel. These lines each contain a feedwater-regulation valve which is used to throttle feedwater flow to match unit demand. A parallel loop bypasses the feedwater-regulation valves and contains the startup valves. These valves are used to throttle feedwater flow during startup. Both the feedwater-regulation valves and the startup valves are pneumatically operated. Control is provided by the feedwater control system except in B&W reactors which use the integrated control system. In PWRs the connections to the auxiliary feedwater system are made in this section of piping. The flow-control valves and check valves isolate the containment.

The systems which interface with the feedwater system are

- condensate system,
- main steam system (including extraction steam),
- reactor coolant system (PWRs),
- auxiliary feedwater system (PWRs),
- integrated control system (B&W),

- o feedwater heater drain subsystem,
- o instrument air system, and
- o plant ac distribution system.

P05.A Feedwater Heater Drain System

The feedwater heater drain system collects the steam condensed in the feedwater heaters and returns it to the main condenser. In some designs, this system is combined with the condensate heater drain system to form a single heater drain system. All of these are nonsafety systems.

The condensed steam is collected in a common header. It then may be either gravity fed or pumped back to the main condenser.

The condenser, the main steam system (extraction steam), the feedwater system, and the plant ac distribution system interface with the feedwater heater drain system.

A.1.3.5.6 P06 Circulating Water System

The circulating water system provides cooling water to the condenser to condense the steam exhausted from the turbine. The circulating water system is the ultimate heat sink for the plant. Two designs are prevalent: an open system and a closed system. The open system draws raw water from outside the plant, passes it through the condenser, and discharges it back into the water source at another location. The closed system recirculates cooling water through the condenser to cooling towers and back. The cooling towers transfer heat to the surrounding air. Makeup water is provided by a raw water source. The circulating water system is a nonsafety system.

The circulating water system may also be called the condenser circulating water system.

The system consists of several pumps, depending upon the particular design, flowcontrol, and isolation valves. For open systems, a system of moving screens on the intake valves strains out debris in the raw water. Other water systems may take suction from the circulating water system depending on design.

The circulating water system interfaces with the following:

- o condensate system,
- o environment,
- o plant ac distribution system, and

- dc power system (for isolation valves).

A.1.3.5.7 P07 Steam Generator Blowdown System (PWR)

In CE and Westinghouse designs, the steam generator blowdown system is used in addition to the chemical feed section of the feedwater system and the condensate cleanup/polishing system to control the chemical composition and solids concentration of the feedwater in the steam generators. Babcock and Wilcox designs, because of their steam generator design and their water chemistry, do not require this system. This is a nonsafety system.

Each steam generator has a blowdown line containing a flow-control valve and a containment-isolation valve. The lines join in a common header. From the header, blowdown steam enters a system of blowdown concentrator reboilers. Main steam is used to evaporate the blowdown. Main steam condensate flows from the reboilers into reboiler receivers (tanks) where it is directed back to first-stage reheaters. Bottom liquid represents the difference between the blowdown feed rate and the evaporation rate. This flows into the base of a separator where it is drawn off. Bottom liquid is normally discharged from the plant; however, if radioactivity is detected in the liquid, it is diverted to the liquid radwaste system. Any residual liquids in the separators are periodically blown down to a sludge pot and sent to the solid radwaste system.

Systems interfacing with the steam generator blowdown system are

- main steam system,
- liquid radwaste system,
- solid radwaste system,
- instrument air system, and
- dc power system (for valve-control circuitry).

A.1.3.5.8 P08 Auxiliary Steam System

The auxiliary steam system supplies heating steam through the plant and recovers the condensed steam from the equipment served. At multiunit plants, this system is often shared by the units. It is a nonsafety system.

Steam for the system may be obtained from taps on the main steam lines when the unit is operating or from a fossil-fired auxiliary boiler when the unit is shutdown. Steam flows from these sources through a common header to the various pieces of equipment served in the plant.

Condensate is collected and pumped back to the boilers. Surge tanks holdup extra fluid.

The auxiliary steam system interfaces with the following:

- o boron recovery subsystem of the CVCS,
- o domestic hot water tank,
- o various evaporators in waste systems,
- o demineralized water storage tank heaters,
- o condensate storage tank heaters,
- o steam jet air ejectors, and
- o turbine gland seal subsystem.

A.1.3.6 Process Auxiliary Systems

The process auxiliary systems grouping is made up of those systems and subsystems that support the plant systems directly involved in the safely producing electrical power. The systems and subsystems of the process auxiliary systems groupings are essentially the same for both BWRs and PWRs.

A.1.3.6.1 W01 Radioactive Waste System

The radioactive waste system collects radioactive wastes from the plant and reduces the concentration of the radionuclides to as low a level as is practicable so that the wastes can be safely released or stored. Three subsystems handle each of the three states in which waste is produced: gaseous, liquid, and solid. Each of these subsystems is discussed in this section.

W01.A Gaseous Radwaste System

The gaseous radwaste system is usually made up of two portions: the process gas (hydrogenated) and low-activity process vent (aerated) streams. The process gas (hydrogenated) portion of the system is designed to remove fission product gases from the reactor coolant letdown stream and from the liquids collected in the reactor coolant drain tank in PWRs. The process gas portion of the gaseous radwaste system is a Safety Class 3 system. Radioactive gases collected from reactor building vents, the steam jet air ejectors (in PWRs), and from the process gas adsorption bed gas drain are collected by the low-activity process vent portion of the system. These gases are filtered, monitored, and, if the concentration of radioactive nuclides is low enough, discharged to the environment. The low-activity process vent

portion of the gaseous radwaste system is a nonsafety system. Both portions may penetrate containment.

Other names used to identify the gaseous radwaste system are

- radioactive gaseous waste system,
- gaseous waste disposal system, and
- gaseous radioactive waste system.

There are numerous designs of this system. Almost all are unique in some manner; however, a large number of them involve gas compressors along with a filtration and monitoring section. Those designs which remove dissolved gases from liquids use a degasifier for this purpose. Some designs feature hydrogen control using a recombiner. Almost all of the major components have installed spares. After collecting the waste gases, most systems run the gases through a system of filters, dryers, and air compressors. When hydrogen is a concern, a recombiner normally is used early in the process. After processing, the gases are monitored, and if their level of radioactivity is low enough, they are released to the atmosphere. If the level is too high, the gases may be either recycled or sent to a holdup storage tank until the level of radioactivity falls to a predetermined level. The specific arrangement of the equipment in the gaseous radwaste system is highly dependent upon the architect-engineer and the utility involved with the design of the plant.

Systems interfacing with the Gaseous Radwaste System are

- plant ac distribution system,
- chemical and volume control system (PWRs),
- combustible gas control system,
- boron recovery subsystem (of CVCS),
- various vents and drains,
- engineered safety features actuation system (PWRs),
- condenser evacuation subsystem,
- liquid waste subsystem,
- refueling system, and
- instrument air system.

W01.B Liquid Radwaste System

The liquid radwaste system collects potentially radioactive liquids from the plant and treats them to reduce their concentration of radioactive nuclides. The liquid radwaste system penetrates containment. The system may be designated a Safety Class 3 system or a nonsafety system depending on design.

Other names which may be used for the liquid radwaste system are

- o radioactive liquid waste system,
- o liquid radioactive waste system, and
- o liquid waste disposal system.

System design usually includes two piping systems which connect at several points. One section of piping is used for high-level radioactive liquids; the other is used for low-level radioactive liquids. Liquids from the process gas section of the gaseous radwaste system, the boron recovery subsystem (PWRs), the steam generator blowdown system (Westinghouse and CE units), or the solid radwaste system enter the high-level section. The low-level section collects from the low-level process vent section of the gaseous radwaste system, the laundry and showers, and the boron recovery subsystem (PWRs). Drain tanks are the first components in either section of piping. One of two parallel pumps draws suction from its associated set of tanks. The high-level pumps discharge into a waste evaporator and then a condenser. This combination removes impurities from the liquid. Periodically the sludge in the bottom of the evaporator is drained, cooled, and sent to the solid radwaste system. The condensed liquid is pumped through a cooler into a series of demineralizers and filters. Upon exiting, the liquid is transferred to a storage tank for reuse in the plant if its radioactivity level is reduced enough. If the level is still high, it is transferred to the low-level section. From the initial tanks, the low-level pumps discharge through a set of filters into a waste evaporator where laundry and shower waste liquid is added. Again suspended solids are separated and sent to the solid radwaste subsection. The low-level distillate is released to the environment if the level of radioactivity is low enough. If the level is above the release value, it is recycled or stored in a tank until the amount of radioactivity has been reduced.

The following systems interface with the liquid radwaste system:

- o plant ac distribution system,
- o gaseous radwaste system,
- o solid radwaste system,

- o engineered safety features actuation system (PWRs),
- o chemical and volume control system (PWRs),
- o steam generator blowdown system (Westinghouse and CE units), and
- o laundry and showers.

W01.C Solid Radwaste Subsystem

The solid radwaste system is used to collect, holdup, solidify, package, and store radioactive materials prior to their shipment off-site to a disposal facility. This system may be classified as non-safety or Safety Class 3 depending upon design. It does not penetrate containment. Wastes such as sludge, spent resins from demineralizers, spent filter cartridges, and miscellaneous solid materials that have become contaminated with use are treated in the solid radwaste system.

Other names used to identify this system are

- o Radioactive solid waste system,
- o Solid waste disposal system, and
- o Solid radioactive waste system.

The sludge and resins entering the system go to a holdup tank. When it is sufficiently filled for processing, it is transferred to an evaporation cycle, which further solidifies the wastes. Next, a solidifying material is added and the combination is placed into a container. After solidification is complete, the container is capped, labeled, and stored awaiting removal from the site. Compressible solid wastes are compressed into a container before a mixture of sludge and solidifier are added to immobilize them. Noncompressible materials are handled in the same manner except that they are not compressed. After solidifying, these containers are capped, labeled, and stored also.

Systems interfacing with the solid radwaste system are

- o plant ac distribution system,
- o liquid radwaste system,
- o chemical and volume control system (PWRs),
- o boron recovery subsystem (of CVCS),
- o condensate cleanup/polishing subsystem,
- o steam generator blowdown system (Westinghouse and CE units)

- o demineralized makeup water system,
- o filters from many systems, and
- o contaminated tools, clothing, cloths, etc.

A.1.3.6.2 W02 Radiation Monitoring System

The radiation monitoring system is provided to ensure that any substantial abnormal radioactivity that is released can be detected within a reasonable amount of time. A level of protection philosophy is employed in that various points in the process systems are monitored; the plant itself is monitored, and the environment surrounding the plant is monitored. Limits are established by Section 10CFR20 of the NRC General Design Criteria.

All points where potentially radioactive materials may enter the environment are monitored and alarmed. Usually the monitors' output is tied into control circuits to shut off equipment to stop the release. Selected areas inside the plant are monitored and alarmed. The plant is divided into zones with increasingly stringent levels used to generate alarms as potential contact with the environment is increased. Areas where plant personnel are expected to spend large amounts of time are also monitored. All monitors have independent power supplies to prevent losing monitors because of a single failure. Areas outside the plant are monitored to ensure that no radioactivity exceeding established levels is released without detection. These environmental monitors may be either fixed or mobile.

A.1.3.6.3 W03 Cooling Water Systems

Numerous water systems are used in a nuclear plant. Some, which are directly involved in the power generation process and in safeguards protection, have already been discussed. Other auxiliary systems, which support these systems' operation, are listed below. The design of these systems varies greatly from plant to plant as well as from NSSS vendor to NSSS vendor; however, they all provide the same basic functions. Among these are cooling water systems, demineralized makeup water systems, service water systems, and chilled water systems.

W03.A Reactor Building Cooling Water System

The reactor building cooling water system provides an intermediate cooling loop for removing heat from the engineered safety systems and transferring it to the essential service water system. The reactor building cooling water system is designated as Safety Class 3 and is typically subdivided into two or three distinct trains. The number of trains is dependent upon the number of engineered safety systems provided by each reactor vendor. Electric power for each train is provided through separate emergency buses. The reactor building

cooling water system penetrates containment in PWRs and secondary containment in BWRs.

The reactor building cooling water system may be called by several names. Among these are

- component cooling water system,
- reactor plant component cooling water system, and
- reactor building closed cooling water system.

A typical train of the reactor building cooling water system will consist of one or more (redundant) pumps and their associated motors connected in series with a heat exchanger for transferring heat to the essential service water system and several parallel piping legs, which connect to the various engineered safety systems.

Systems which typically interface with the reactor building cooling water system are

- essential ac power system,
- essential service water system,
- containment spray system,
- residual heat removal/low-pressure safety injection system,
- high-pressure safety injection system (PWRs),
- containment cooling/heat removal system, and
- spent fuel cooling and cleanup system.

Other interfacing systems are

- reactor coolant/recirculation system,
- chemical and volume control system (PWRs)
- spent fuel storage and cooling system,
- liquid and gaseous radwaste systems, and
- engineered safety features actuation system (PWRs).

W03.B Turbine Building Cooling Water System

The turbine building cooling water system provides an intermediate cooling loop for removing heat from components located inside the

turbine and auxiliary buildings and transferring it to the nonessential service water system. Coolers in such systems as the chemical and volume control system, the chilled water system, the reactor water cleanup system, and the steam generator blowdown system are cooled by the turbine building cooling water system. This system does not penetrate containment and is designated as a nonsafety system. Electric power is supplied by the nonessential ac distribution system.

The turbine building cooling water system also may be called:

- recirculating water system,
- turbine plant component cooling water system, and
- turbine building closed cooling water system.

System design involves a single-train with redundant pumps. Pump discharge flows through the tube side of a turbine building cooling water heat exchanger before entering a common header. Several parallel piping legs leave the header and pass through the shell side of various heat exchangers.

Systems which interface with the turbine building cooling water system are

- nonessential ac distribution subsystem,
- Chemical and volume control system (PWRs),
- Chilled water system, and
- Steam generator blowdown system (Westinghouse and CE units)

A.1.3.6.4 W04 Service Water Systems

W04.A Demineralized Makeup Water System

The demineralized makeup water system is the source of high purity water for use as primary grade water in the primary auxiliary systems such as condensate in the secondary auxiliary systems and for general use wherever demineralized water is needed inside the plant. The demineralized water system is a nonsafety system that penetrates containment. Electric power is provided by the nonessential ac distribution subsystem.

The demineralized water system is normally divided into two sections: a water treatment section and a storage and transfer section. The water treatment section is supplied water by a tap on the circulating water system. This water enters a settling tank; then it is passed through a series of filters and demineralizers until it reaches a high level of purity. It is then sent to the demineralized water storage

tank for use in the various water systems in the plant. One of two redundant pumps is used to transfer the water. The storage tank, transfer pumps, and associated piping make up the transfer section of the system.

In PWRs the following systems interface with the demineralized makeup water system:

- o nonessential ac distribution system,
- o chemical and volume control system,
- o auxiliary feedwater system,
- o condenser and condensate system,
- o circulating water system,
- o auxiliary steam system,
- o solid radwaste system,
- o potable and sanitary water system,
- o chilled water system,
- o spent fuel cooling and cleanup system,
- o reactor and turbine building cooling water systems, and
- o service water system.

W04.B Station Service Water System

The station service water system is used to transfer heat from the cooling water systems and various other plant components to the ultimate heat sink (usually the circulating water system). In most designs there is one service water system, but it is broken into essential and nonessential subsystems. The essential service water subsystem is designated a Safety Class 3 system and is powered by the essential ac distribution subsystem. The nonessential service water system is a nonsafety system and is usually isolated from the essential subsystem by a safeguards signal.

The station service water system is a two-train system. Redundant pumps draw suction from taps on the circulating water system piping. Some designs have a third pump as an installed spare. The pumps usually discharge into a common header (for nonessential use) and two parallel, redundant headers (for essential use). The common header can be isolated by a motor-operated valve.

From the common header, legs branch off to provide cooling water flow from the turbine building cooling water cooler, for cooling jackets and large motors in the turbine and auxiliary building, and for the non-safety heating, ventilating and air conditioning (HVAC) water chillers. Each leg of the essential portion branches into parallel legs that connect to redundant components such as the reactor building cooling water heat exchanger, the fuel pool makeup (emergency), safety HVAC water chillers, cooling jackets of large motors inside containment, and the diesel generator cooling water heat exchangers. Flow from all the parallel legs join together at a common discharge header and flow back into the circulating water.

Systems interfacing with the station service water system are

- plant ac distribution system (both subsystems),
- circulating water system,
- reactor and turbine building cooling water systems,
- chilled water system,
- compressed air system,
- reactor coolant and reactor recirculation systems (motor cooling), and
- diesel generator cooling water system.

W04.C Chilled Water System

The chilled water system provides cold water to various HVAC air cooling coils and generator leads coolers. The chilled water system is normally divided into two parts. Safety Class 3 portion of the system provides cooling water to the safety related air cooling systems inside containment. A nonsafety portion supplies cooling water to generator leads coolers and to HVAC cooling units throughout the plant but outside containment. The nonsafety portion can be isolated on receipt of a safeguards signal.

The chilled water system is a closed-loop system. Two or three pumps, depending on design, draw water from mechanical refrigeration units, which are serviced by the station service water system. The pumps discharge into a common header which branches to go to each of the associated coolers. Isolation valves ensure flow to the safety related coolers during accident conditions. Flow from the various coolers returns to the refrigeration units. Usually a surge tank provides control system water inventory.

Systems interfacing with the chilled water system are

- o essential ac distribution subsystem,
- o containment cooling system (PWRs),
- o HVAC systems
- o turbine generator,
- o station service water system, and
- o engineered safety features actuation system (PWRs).

A.1.3.6.5 W05 Refueling System

The refueling system is used to exchange new fuel assemblies for used ones at the end of each fuel cycle. The refueling system is designed to meet Seismic Category I requirements. The system is also designed such that all refueling activities take place under water to take advantage of water's shielding and cooling capabilities.

A typical system consists of equipment in three places: in the reactor building, in the spent fuel building, and in the fuel transfer tube connecting the reactor building and spent fuel building. Equipment in the reactor building typically consists of one or two fuel-handling bridges (depending on design), a control rod assembly handling tool (in PWRs), various cranes and hoists, and an underwater closed circuit TV system to aid in control. The spent fuel building houses such items as a fuel-handling bridge, fuel storage racks, and a new fuel handling tool. The transfer tube is, itself, a part of the system. It may actually be two tubes: one used for fuel entering the reactor building and one used for fuel leaving the reactor building. The transfer tube, or tubes, can be isolated through the use of valves at the entrance to the reactor building. A carriage or a boom, depending on design, is used to move fuel assemblies through the transfer tube. The transfer tube and the containment in PWRs are flooded with borated water from the refueling, or borated, water storage tank.

The refueling system interfaces with the plant ac distribution system, the spent fuel storage and cooling system, the condensate system (PWRs), the reactor core, and the control rod drive system (PWRs).

A.1.3.6.6 W06 Spent Fuel Storage System

The spent fuel storage system is used to store spent fuel assemblies that have been taken from the reactor core. The spent fuel storage system is designed for Seismic Category I loads and for tornadoes and external missiles. The atmosphere in the spent fuel building is confined and filtered.

The spent fuel pool is the major component of the spent fuel storage system. It is normally filled with primary-grade demineralized water.

In PWRs, borated water is added from the refueling or borated water storage tank. Storage racks in the bottom of the pool hold the spent fuel assemblies and maintain an adequate separation to prevent the fuel from reaching criticality.

The spent fuel storage system interfaces with the refueling system, the demineralized water system, and the fuel pool cooling and cleanup system.

W06.A Fuel Pool Cooling and Cleanup System

The fuel pool cooling and cleanup system removes decay heat from the spent fuel and provides clarification and purification for the water in the fuel pool and refueling, or borated, water storage tank. The fuel pool cooling and cleanup system is a Safety Class 3 system. Electric power is supplied from the essential ac distribution subsystems.

The cooling and purification sections of the system may be completely separate or the purification section may divert a portion of the cooling stream through the filters and demineralizers. The cooling portion typically uses two independent, redundant piping trains each with a pump and cooler. If the cooling and purification sections are combined, taps in each line divert flow through the filters and demineralizers. The purification section is also a two-train system with taps on the cooling piping lines or with pumps and suction points in the spent fuel pool and refueling cavity. Pump discharge passes through a filter and into a demineralizer. The number of filters and demineralizers depends upon the system's design. From the demineralizer, the flow returns to the spent fuel pool. A loop also recirculates water in the refueling, or borated, water storage tank through the filtration system.

The fuel pool cooling and cleanup system interfaces with the essential ac distribution system, the spent fuel storage system, the demineralized water system, and the reactor building cooling water system (for secondary cooler flow).

A.1.3.6.7 W07 Compressed Air System

The compressed air system supplies compressed air throughout the plant for pneumatic valve operation, instrumentation (where pneumatic systems are used), and for use with pneumatic tools. The system has two major subsystems: the instrument air subsystem and the service air subsystem. The instrument air subsystem is frequently divided into a Safety Class 3 portion with supply loads inside containment and a nonsafety portion for the remainder of the plant.

The service and nonsafety instrument air portion are sometimes combined. This system normally has two 100%-capacity or three 50%-capacity air compressors. Each compressor has an intake filter and aftercoolers loading into a common header. Air receivers are provided

to store compressed air. A service air leg branches from the common header in addition to the instrument air legs. Each instrument air leg contains an air filter and a 100%-capacity air dryer. In designs featuring a separate containment instrument air system, air is drawn from and discharged to the containment creating no pressure increase inside containment. As with the nonsafety portion, two compressors with filters, aftercoolers, and air dryers make up two redundant trains. Each train also has air receivers to store the compressed air.

Systems interfacing with the compressed air system are

- o plant ac distribution system,
- o station service water system (for aftercooler secondary flow), and
- o various systems having pneumatically operated valves and instruments.

A.1.3.6.8 W08 Process Sampling System

The process sampling system provides a means of drawing samples from various process systems and the facilities for analyzing the samples. Samples drawn from inside the containment have remotely operated valves for isolation purposes. Typical of the analysis performed on the samples are boron concentration (PWRs), fission product radioactivity level, hydrogen and oxygen gas content, pH, corrosion product concentration, and conductivity. The system is designed to be manually operated on an intermittent or continuous basis under all plant conditions.

The process sampling system features numerous lines connecting process piping to sample sinks. Hot lines have sample coolers with secondary flow provided by the station service water system. Those samples, on which conductivity analysis are performed, have a constant temperature bath to minimize errors in measurement caused by temperature differences. Demineralized water at the sample sinks is for rinsing purposes. All sample sinks drain into the liquid radwaste system.

The Process Sampling System interfaces with:

- o various systems requiring chemical analysis,
- o station service water system,
- o demineralized water system,
- o liquid radwaste system, and
- o engineered safety features actuation system (PWRs).

A.1.3.6.9 W09 Plant Gas System

The plant gas system is used to supply compressed gases to the various places it is needed in the plant. It is a nonsafety system. The plant gas system normally features a nitrogen and a hydrogen subsystem.

Both the compressed nitrogen and hydrogen are provided in gas bottles. Each of the bottles discharges through a pressure-control valve into a header with parallel piping legs to distribute the gas.

Nitrogen bottles connect to:

- safety injection accumulators,
- volume control tank (in some designs),
- refrigerant dryers,
- charcoal bed gas adsorbers,
- gas compressors, and
- gaseous vents and drains (for purging).

Hydrogen bottles connect to the volume control tank (in some designs) and the generator stator cooling subsystem.

A.1.3.7 Plant Auxiliary System

Plant auxiliary systems are provided to support plant activities and personnel. They are typically nonsafety systems. Design of these systems varies greatly since almost all are plant specific. The systems and subsystems of the plant auxiliary system grouping are discussed in this section.

A.1.3.7.1 X01 Potable and Sanitary Water System

The potable and sanitary water system provides water throughout the plant (except in containment) for drinking water, showers, laundries, and restroom facilities. It is a nonsafety system. The source of water may be a local water system, or in remote locations, the circulating water system. If circulating water is used, stations for filtration and chemical addition insure the water is safe for consumption. A common header distributes the water, and another collects discharge. Discharge returns to a local sewage system when available, or through a sewage-processing station before release to the plant water supply (downstream of intakes).

A.1.3.7.2 X02 Fire Protection System

The fire protection system is designed to detect, annunciate, and extinguish any fires which may occur and to provide some mitigation for the effects of the fires. Fire protection is generally a nonsafety system. It is typically divided into two subsystems: a water system and a carbon dioxide system.

The water system is used in all areas of the plant except those which contain electric equipment. Two water pumps are usually provided, one of which may be steam turbine driven. The pumps discharge into a header that supplies various fire hoses and overhead sprinklers throughout applicable areas of the plant. The water supply is taken from the circulating water system in most cases. Heat actuated detection devices activate the systems and annunciate its operation.

The carbon dioxide system is used to protect areas such as the cable spreading room, switchgear rooms, and electrical penetrations and tunnels. This system is supplied CO_2 from a storage tank. Piping connects the storage tank with valved distribution points in electrical areas. Heat actuated sensors operate the system. Rooms that require occupancy during normal operation, such as the control room, use portable CO_2 extinguishers.

A.1.3.7.3 X03 Communications System

The communications system is designed to provide reliable communications among essential areas of the station and to essential locations remote from the plant during all plant conditions. A diverse communications system insures this capability. Intraplant communications are provided by:

- page/party public address and evacuation alarm system,
- sound-powered telephone system,
- hand-held portable radio system, and
- private branch telephone exchange.

Off-site communications systems include local telephone service and microwave link through the utility's system-wide communications system.

A.1.3.7.4 X04 Security System

The security system is designed to protect vital areas of the plant from intrusion by nonauthorized personnel. The system's many levels of protection includes the fence around the exclusion area, security procedures, microwave detection systems, and card-keyed locks on doors within the plant. Since these designs are considered proprietary, little information is available about them.

A.1.3.7.5 X05 Heating, Ventilating and Air Conditioning System (HVAC)

The HVAC group of conditioning systems removes heat, ventilates, and maintains a comfortable environment for personnel in the various buildings and rooms of the power plant. (Containment cooling and ventilating systems are excluded from this group.) Each of the major equipment and personnel areas normally has its own system. Some designs, however, have a central system. The HVAC systems are non-safety systems with the exception of the control room HVAC. The HVAC systems for safety related equipment are safety related if they are required for equipment operability.

All HVAC systems feature one or two trains, each with a fan, a filtration system, and an air cooler. Most are closed systems with return and discharge registers in appropriate positions to maximize air flow through the rooms.

Typical HVAC systems are provided for:

- control room,
- switchgear rooms,
- cable spreading room,
- electrical tunnels,
- diesel generator room (usually ventilation only),
- battery rooms,
- solid waste and decontamination building,
- turbine building (usually ventilation only),
- fuel building, and
- administrative building.

A.1.3.7.6 X06 Nonradioactive Waste System

The nonradioactive waste system is used to process all gaseous, liquid, and solid wastes that do not contain radionuclides and that are not handled by the radioactive waste system (Sect. 1.3.6.1), which is discussed earlier in this document. It is not a safety system. This system is divided into three subsystems by waste category: gaseous, liquid, and solid. Each of these subsystems are discussed in this section.

X06.A Gaseous Waste Subsystem

Very few nonradioactive or uncontaminated gases are generated and those that are present are usually handled by the radioactive waste system.

X06.B Liquid Nonradioactive Waste Subsystem

The liquid waste system collects liquid wastes that are not contaminated with radionuclides and therefore may be handled more simply and much less expensively than contaminated wastes. A large amount of this type of waste is generated in both BWR and PWR power plants.

X06.C Solid Waste Subsystem

The solid waste system handles routine nonradioactive wastes similar to any large chemical plant and is separated from the radioactive waste system for economic reasons. In most power plants the solid wastes generated are combustible and therefore are incinerated for volume reduction, and the resultant ash is disposed of in sanitary landfills.

The nonradioactive waste system interfaces with virtually every other system in the plant.

A.2. DESCRIPTION OF ONCE-THROUGH STEAM GENERATOR

This section describes the functional design and the controls of the steam generator.

A.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.-I 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 overfill. 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 A.2.1 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.

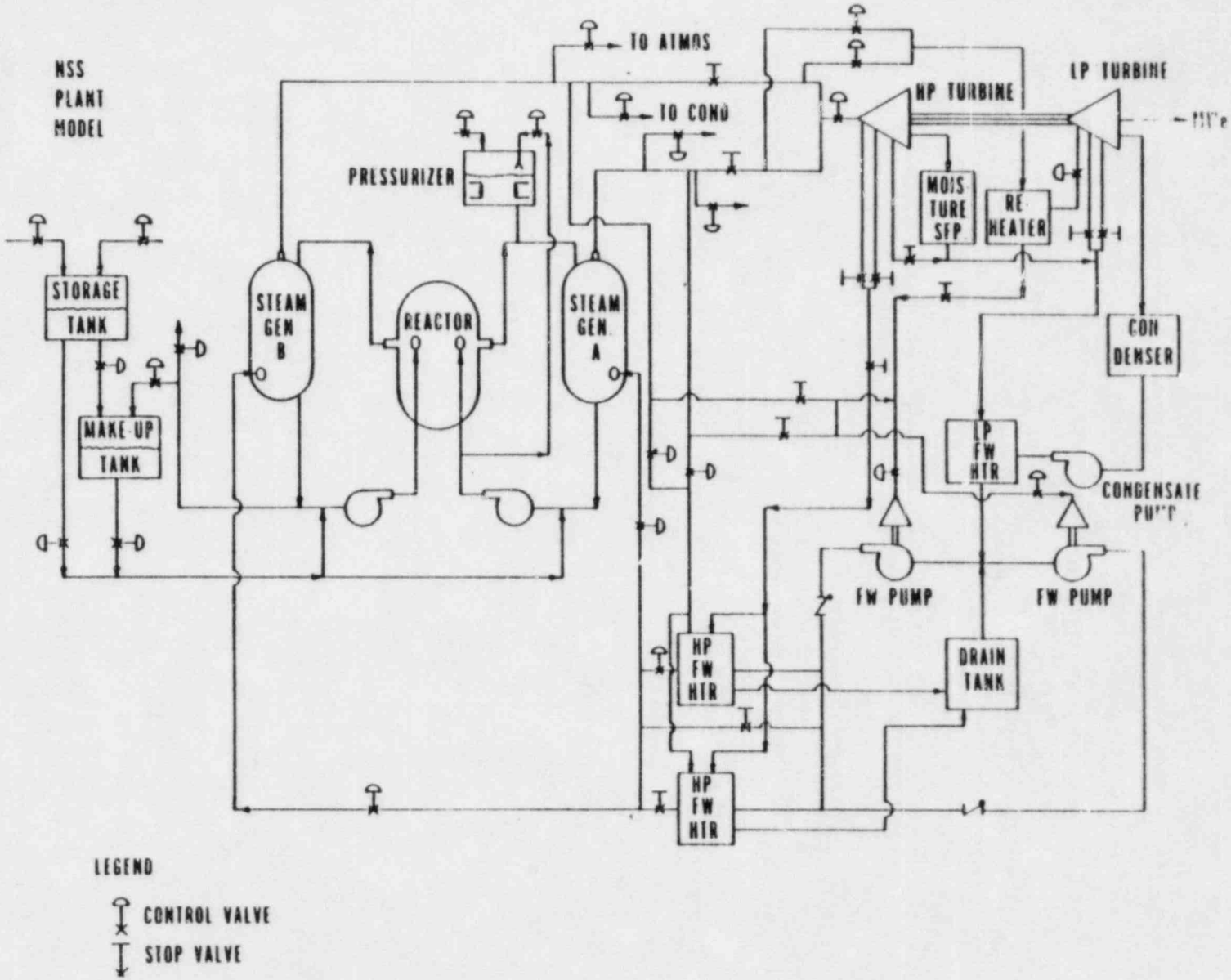


Fig. A.2.1 Simplified schematic diagram of a nuclear power plant.

A.2.2 STEAM GENERATOR CONTROLS

A.2.2.1 Operating Controls

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

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

In maintaining total feedwater flow equal to total feedwater demand, the feedwater control subsystem manipulates two start-up valves, two main valves, and two pumps. The feedwater control includes the following considerations, each of which will be discussed below (see Fig. A.2.2 - all references to Points and Blocks are on Fig. A.2.2:

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

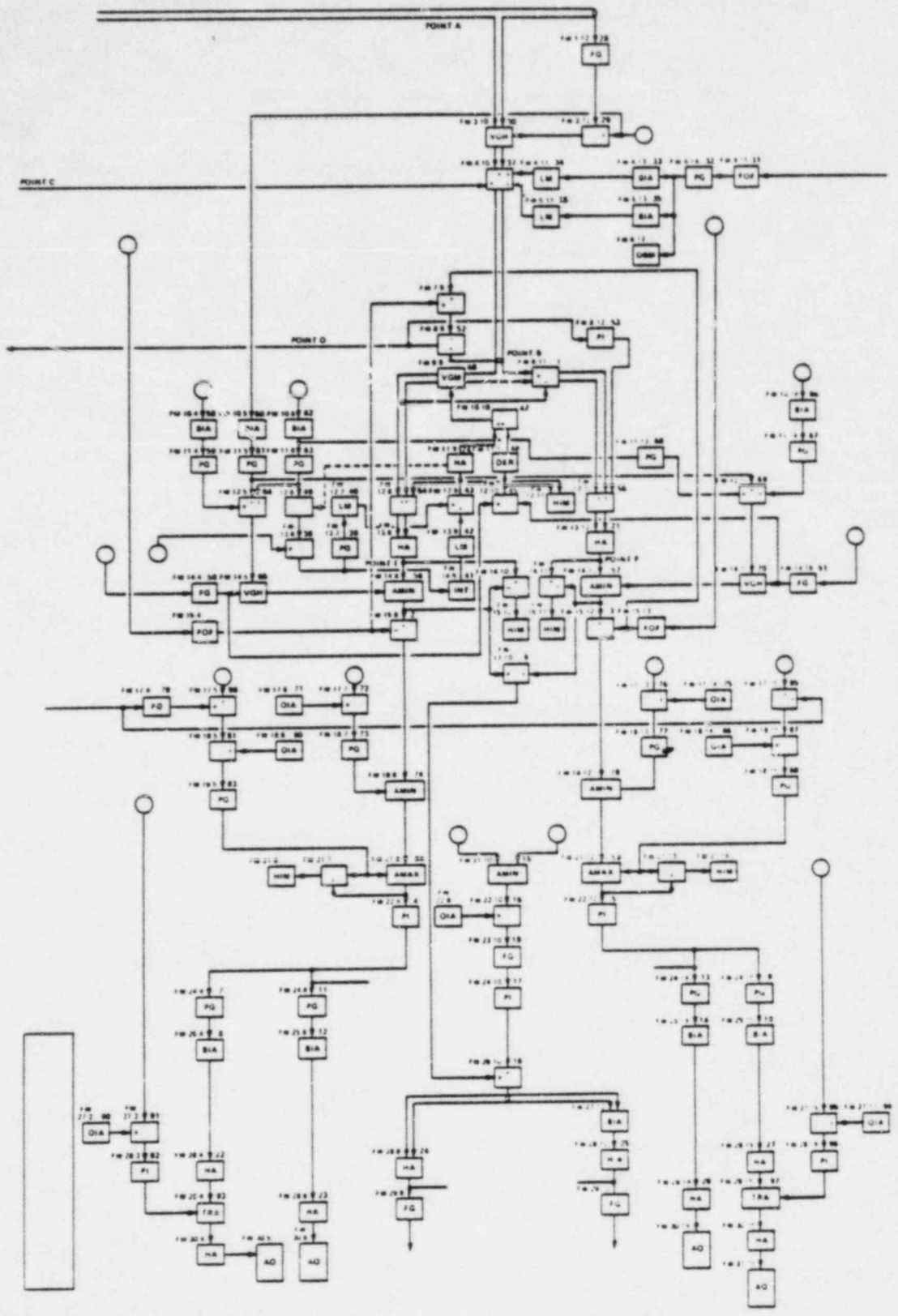


Fig. A.2.2. Schematic diagram of Oconee-1 steam generator control system.

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 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 delta-T_c Hand/Automatic station (Block 44) may be used to replace the demand created by delta-T_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 delta-T_c will deviate from zero unless the feedwater flows are ratioed properly. To aid in maintaining delta-T_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 delta-T_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°C=35°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.

A.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 A.2.3 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.

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.

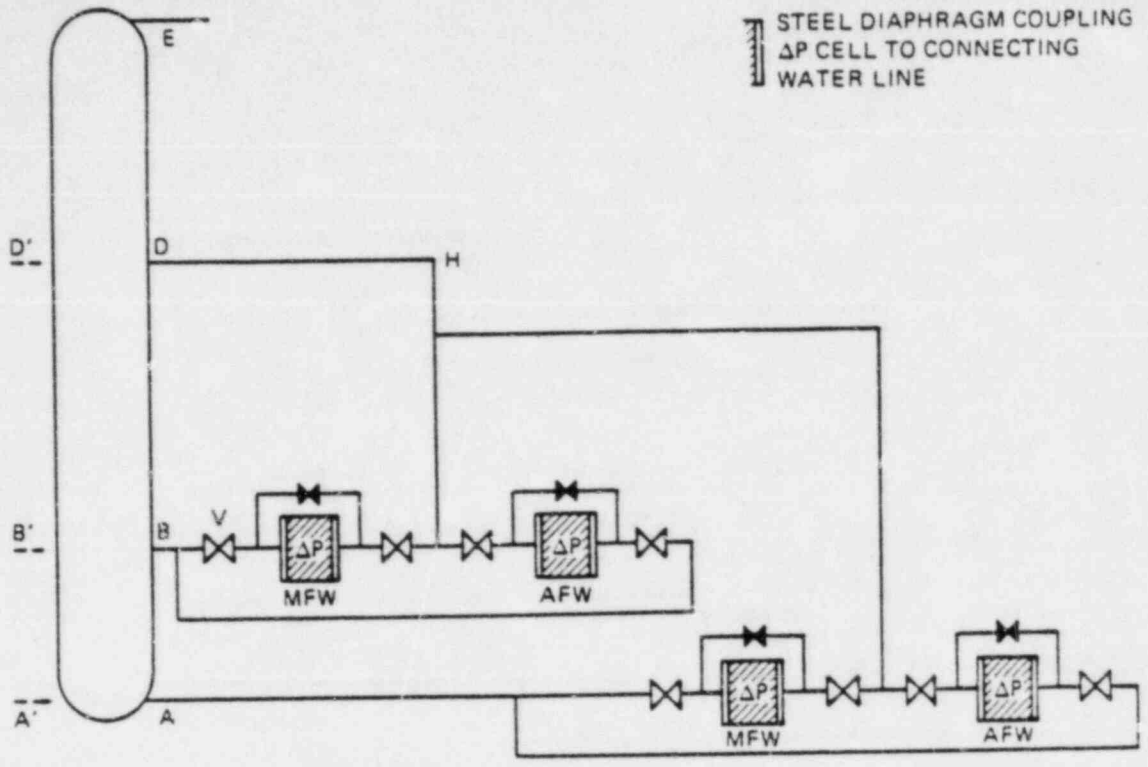


Fig. A.2.3 Schematic diagram of steam generator pressure taps and ΔP cells.

The path from each pressure tap to the (normally open) blocking valves (Fig. A.2.3) 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).

A.2.2.3 High Level Main Feedwater Pump Trip Circuitry

Figure 4 is a schematic of the circuit transmitting SG high level sensed signals to the high level MFW pump trip and alarm. The following failures can place this system in an undetected failed state.

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

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

The circuitry of 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.

This circuitry is tested during refueling.

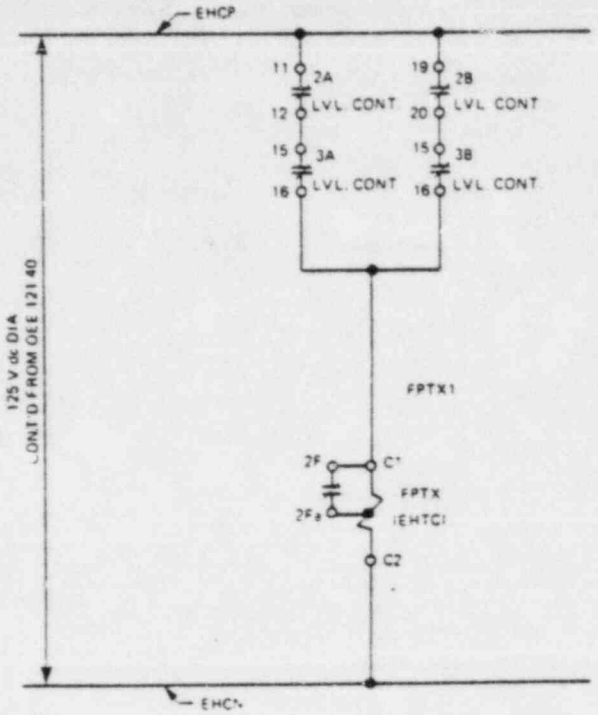


Fig. A.2.4 Main feedwater pump high-level trip circuit.

A.2.2.4 Further Details of System Description

In order to follow the scenario descriptions we present, some further understanding of system detail is necessary.

1. The detectors on the steam generators which are considered to be level detectors are, in fact, not. They are detectors of differential pressure. The confusion is somewhat compounded because the low-level instrumentation, at least, is calibrated to read differentia pressure in units of inches of water. The use of differential pressure as a level indicator is straightforward when the gravitational term is dominant. In an active flow region like the steam generators, which are two-phase flow devices, the flow terms are not only important — they dominate. The relation between level (if, indeed, a level can be defined) and differential pressure is heavily flow dependent. Hence, even if a differential pressure detector were calibrated to some arbitrarily defined equivalent level during normal operations, the strong flow variations that accompany many transients would cause the calibration to be of no value during the transient or other off-normal condition.

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

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

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

APPENDIX B. SELECTION OF PRESSURIZED WATER REACTORS PLANT EQUIPMENT INVOLVED IN PRESSURIZED THERMAL SHOCK EVENTS

In Appendix A, the systems of pressurized water reactors (PWRs) have been listed and described. The impact of most PWR plant systems on the course of a pressurized thermal shock (PTS) transient is minor. The purpose of Appendix B is to select for additional study those PWR systems which may have a significant impact on PTS.

Pressurized thermal shock transients are defined to be the simultaneous occurrence of high reactor coolant system (RCS) pressure and low vessel wall temperature in high-irradiation sections of the reactor vessel (belt line region). Typically, RCS pressures >2000 psi and RCS temperatures <300°F are thought to be of significant concern.

In Section B.1, those PWR systems whose operation or mis-operation could reduce the RCS temperatures significantly are discussed. Systems whose operation or mis-operation could produce or maintain high RCS pressures are discussed in Section B.2. In Section B.3, the potential sequential or concurrent operations of systems necessary to produce PTS transients are discussed.

The systems considered are typical of B&W designed nuclear steam supply systems (NSSS). Specific differences with other NSSS designs are noted.

B.1 REACTOR COOLANT SYSTEM TEMPERATURE REDUCTION

The temperature of the high-irradiation section of the reactor vessel is of particular concern in pressurized thermal shock transients. As shown in Fig. B.1, three heat transport modes exist which could reduce the temperature of this section: external heat transport, heat transport to fluids in the vessel downcomer and conduction to low-temperature metal sections. In Fig. B.2, the systems that are involved in these heat transport modes are diagrammatically shown.

B.1.1 External Heat Transport

The RCS in a B&W 177 FA PWR operates at ~550°F in the reactor inlet piping, ~600°F in the reactor outlet piping, and ~650°F in the pressurizer. To maximize NSSS thermal efficiency and minimize heat loads on containment cooling systems, the RCS surfaces are insulated, usually with metallic, thermal radiation shield insulation. When properly installed, RCS insulation will result in nearly uniform temperatures in the pressure boundary walls.

There appears to be little potential for overcooling the high-irradiation sections of vessel under most conditions. Two abnormal

conditions can be postulated that could increase the surface heat transfer rate and decrease the vessel surface temperature.

If a section of the insulation in the area of the high-irradiation section were to be removed exposing the vessel surface to the reactor cavity air flow, the surface temperature could be lowered. Based on a simple one-dimensional (normal to surface) calculation, the surface temperature could reach ~460°F. The 90°F reduction is not thought to be significant to PTS.

The potential for flooding the reactor cavity with water could increase the potential for significant external heat removal. If the insulation were intact, preventing direct contact of the water and vessel surface, no significant surface temperature reduction is expected. (The possible effects of leakage through the insulation have not been investigated.) However, if a section of insulation were removed and the reactor cavity flooded, a reduction of the vessel surface temperature to below 300°F is credible.

Potential sources of water in the containment include the containment spray system, plant water lines, and feedwater lines. The potential for rupturing one of these lines or inadvertently actuating the spray system and subsequently flooding the reactor cavity should be investigated to assess the feasibility and time scale of these postulated events.

B.1.2 Heat Transport to Fluids in the Downcomer

B.1.2.1 Depressurization of the RCS

Loss of coolant accidents (LOCAs), depending on break size, produce RCS fluid temperature temporal derivatives from 2,200°F/h to 36,000°F/h. This phenomenon happens rapidly and the primary fluid temperature reaches ~350°F. With this base temperature, depressurization by itself does not produce PTS conditions. It is the injection of cold fluids, resulting from the depressurization, that lead to PTS.

B.1.2.2 Injection of Cold Water Into Reactor Vessel Downcomer

The temperature of the high-irradiation vessel section is principally controlled by the temperature of reactor coolant in the vessel downcomer. Coolant is injected into the downcomer during all modes of reactor operation, and the vessel wall temperature will be determined by the flow rates and temperatures of these injected fluids. The fluid flows of concern are those from the four inlet (cold leg) pipes and the two core flood/low-pressure injection (CF/LPI) nozzles.* Under certain conditions, reactor coolant also may enter the downcomer either from

---

*The CF/LPI vessel nozzles are unique to B&W plants. In other NSSS designs the CF and LPI systems inject into the inlet piping.

the core region (because of back flow) or through the internal vent valves,* which will increase the downcomer fluid temperatures. Heat also may be added to the downcomer by conduction through the core barrel, but this effect is expected to be minor.

The principal mode of injecting cold water into the downcomer is direct injection of cold water from external tanks. Coolant may be injected into the downcomer from two types of external tanks: the two** CF (or accumulator) tanks and the borated (refueling) water storage tank (BWST).

These tanks provide a source of borated water to be injected into the RCS following accidents.***

Each of the two CF tanks is connected to a separate CF/LPI vessel nozzle. Each tank contains ~1000 ft^3 of borated water at ambient containment temperatures (~100°F) and is pressurized with nitrogen to ~600 psi. During normal reactor operation the tanks are isolated from the 2200-psi RCS by two series check valves per line. The tanks thus automatically discharge into the downcomer following depressurization transients, as the RCS pressure decreases below 600 psi. During normal plant shutdowns, the normally open isolation valve in each line is closed, and the tanks are depressurized to prevent CF tank discharge during refueling.

Two credible events can be postulated that would result in CF tank injection: operator failure to isolate and depressurize the tank during a controlled RCS shutdown and an uncontrolled depressurization caused by a transient. Although possible, deliberate repressurizing of the CF tanks and opening the isolation valves during shutdown are not considered credible.

Failure to isolate the CF tanks during a controlled shutdown will result in a slow injection of water from the tanks. The condition would be indicated by CF tank level and/or pressure alarms and increased pressurizer and/or makeup tank levels. The potential for decreasing vessel wall temperatures will be a function of fluid mixing in the CF/LPI nozzle area, the number of reactor coolant pumps in operation, the rate of injection, and the heat conduction from surrounding areas. Although unanalyzed, it is not thought that the temperature reduction of the vessel wall would be significant.

---

*Unique to B&W NSSS designs.

**NSSS designs other than B&W have additional accumulator tanks injecting into the inlet piping.

***The BWST also provides a source of water for flooding the refueling the canal prior to refueling operations.

Reactor coolant system pressures to more than 500 gal/min per pump at RCS pressures of 600 psi or less. The effect of HPI on vessel wall temperature will vary with HPI flow rate, the reactor coolant flow rate in the inlet lines, and the degree of mixing and heat conduction in the vessel wall.

B.1.2.3 Heat Removal From Recirculated Reactor Coolant

Three systems cool the reactor coolant in the heat exchangers and reinjected the coolant into the vessel downcomer. These systems are the primary reactor coolant loops, used for power production; the letdown and makeup loops, used for reactor coolant purification and the boric acid concentration control; and the decay heat removal loops, used for residual heat removal during shutdown.

Steam Generator and Power Conversion System

During normal power operation reactor coolant, which passes through the core and reaches a temperature of ~600°F is reduced to ~550°F in the two steam generators, and is pumped into the reactor vessel downcomer through the four inlet lines.

The reactor coolant inlet temperature, which will control the vessel wall temperature, depends on the balance of the heat added to the coolant in the core and the heat removed from the coolant in the steam generators. Because of the high rates at which heat can be transferred in these components, there is a large potential for inlet temperature decreases.

During power operations the integrated control system* (ICS) monitors and controls many variables that may affect vessel inlet temperature. However, since there are no credible operating states in which the reactor is critical and the inlet temperature approaches 300°F, the reactor may be assumed tripped** (subcritical) for purposes of PTS analysis. With this assumption, two controlled parameters will affect reactor inlet temperature significantly: steam generator feedwater level and steam pressure.

Following a reactor trip, reactor power will rapidly decrease to residual heat levels (<6% full power) and slowly decrease thereafter. Reactor coolant temperatures will equilibrate at ~550°F*** with the reactor coolant (RC) pumps running. If the RC pumps are tripped, the

---

*Unique to B&W plants.

**Scram failure will tend to increase inlet temperature.

***Saturation temperature at the 1000 psi steam generator steam pressure set point.

reactor inlet temperature will equilibrate below 550°F and the outlet above 550°F to provide a driving head for natural circulation flow.

The steam generator steam pressure normally would be controlled to ~1000 psi by ICS control of the condenser steam dump valves. (This function is performed by the atmospheric dump valves or steam safety valves if the condenser dump valves fail closed.) The steam generator feedwater level normally would be controlled to one of two set points by ICS control of the startup feedwater-control valves. If the RC pumps are operating, the level is controlled to ~2 ft. A 20-ft level is maintained to provide the heat sink for natural circulation of reactor coolant if the RC pumps are tripped.

In the B&W once through steam generator (OTSG), feedwater is sprayed into the feedwater annulus where it is mixed with steam from the tube region. This creates a saturated feedwater mixture which flows into the tube region and is vaporized by heat transferred from the reactor coolant flowing on the inside of the steam generator tubes. Part of the steam produced is drawn into the feedwater annulus, and the remainder is rejected to the condenser or the atmosphere in the shutdown mode.

The rate of heat transfer from the primary fluid to the secondary is controlled by the amount of feedwater in the tube bundle region (heat transfer surface area) and the temperature difference between the saturated liquid and the reactor coolant temperature.

During power operation, the liquid inventory in the steam generator is greater than that required for residual heat removal. Following a reactor trip (and consequential turbine trip), the ICS will begin to control steam pressure with the condenser dump valves and throttle back the main feedwater flow rate to the shutdown condition. Failure of either of these functions could lead to reduced reactor coolant vessel inlet temperature.

Failures of the steam generator level instruments, ICS processing modules, or actuators on the feedwater-control and block valves could lead to excessive main feedwater injection. The heat transfer rate from the primary system will be limited by the high steam generator pressure, which terminates the production of steam, and the decreasing reactor coolant temperature, which also limits the heat transfer driving potential. The transient will be terminated by manual intervention, automatically by isolation of the feedwater on low RCS pressure, or when insufficient steam is available to drive the main feedwater pump turbines. This transient is expected to result in significant vessel inlet temperature reduction. However, the additional loads placed on the steam lines when flooded, including the potential for water hammer, would increase the probability for steam line failure and a far more significant overcooling problem.

Failure of the main feedwater system to deliver sufficient flow will automatically actuate the auxiliary feedwater system upon the detection of low steam generator level or other signals. Once actuated the auxiliary feedwater system will continue to inject feedwater into the steam generators in excess of residual heat removal requirements until throttled by the operator.* However, since manual intervention is a well-defined operator action, the probability for continued cooldown is not expected to be significant.

Transients that depressurize the steam generators will result in significant reductions in the vessel inlet temperature. Transients that produce depressurization include normal cooldown, failure of the steam relief valves or, in the worst case, a steam line failure.

Depressurization will occur when the flow rate of steam dumped to the atmosphere or condenser exceeds the production rate of steam in the steam generators. This will result in a lower saturation pressure and temperature in the steam generators and, consequently, an increased thermal potential for primary to secondary heat transfer. The increased boil-off rate will be accompanied by the automatically increased feedwater flow rate required to maintain steam generator level.

During a normal plant shutdown, this process is followed in a controlled manner until the RCS temperatures reach ~300°F** and the residual heat removal (RHR) system is placed in operation. The cooldown would also result from a failure of the steam dump valves or their controls. Under these conditions, the cooldown would proceed at a higher initial rate and probably result in automatic main feedwater and main steam line isolation*** and automatic initiation of auxiliary feedwater and high-pressure injection (HPI).

The limiting depressurization transient is the steam line rupture. In contrast to the failed-open valve case, a line rupture may occur upstream of the isolation valves, and the depressurization may not be automatically terminated. As before, the main feedwater will be automatically isolated, and the HPI and auxiliary feedwater systems will be automatically initiated. Major, unisolated steam line ruptures

---

*Some B&W plant designs have automatic control systems which automatically throttle flow.

**The potential for further cooldown in this mode is extremely limited because of the low RCS temperatures and high specific volume of the steam produced at this temperature.

***Some B&W plants do not have main steam line isolation valves. For these plants, a cooldown to ~300°F can be expected unless the steam dump valves can be closed.

occurring at high reactor power (maximum steam generator liquid inventory) will result in RCS temperatures <300°F.

Chemical and Volume Control and Residual Heat Removal Systems

In addition to heat removal from recirculated reactor coolant in the steam generators, reactor coolant is recirculated through the CVC and RHR systems.

During normal power operation, 50 gal/min of reactor coolant is continuously cooled to ~120°F and purified and reinjected into the RCS inlet pipes. The letdown and makeup rate may be increased occasionally to 200 gal/min during dilution or boration operations for rapid power changes. In both cases, the flow rates are too small to significantly affect the temperature of the reactor coolant because of the far higher RCS inlet pipe flow rates.

The RHR system is manually placed in operation to cool the RCS from ~300°F to 140°F during normal plant shutdowns. After the RCS is depressurized to below 300 psi, the RHR isolation valves are opened and reactor coolant recirculated through the RHR system. The rate of RCS cooldown is controlled by the number of RHR loops in operation (one or two) and the fraction of flow which bypasses the RHR heat exchangers.

B.1.3 Conduction of Heat to Low-Temperature Metal Sections

The high-irradiation vessel section and the vessel inlet lines are the lowest temperature parts of the RCS. The major effect of conduction will be to increase the temperature of localized low-temperature regions during transients.

B.1.4 Summary of Reactor Coolant Systems Temperature Reduction Process

Several processes that could result in a temperature reduction in the high-irradiation section of the reactor vessel have been discussed in Sect. B.1. The response of the vessel wall to these processes ranged from insignificant to potentially large. The processes and qualitative estimates of their potential vessel wall temperature reduction are summarized in Table B.1. Notice, however, that in neither Sect. B.1 nor Table B.1 have multiple failure modes been considered.

B.2 PRESSURIZATION OF THE RCS

As previously stated, PTS transients are caused by low vessel wall temperatures in combination with high RCS pressures. Mechanisms for achieving low temperatures have been discussed in Sect. 2.1. In this section, mechanisms which maintain or produce high RCS pressures are discussed.

In general, there are two ways of achieving RCS pressures in excess of 2000 psi: achieve or maintain a saturation temperature in some part of

Table B.1. Summary of reactor coolant system temperature reduction processes

Process	Potential for reactor vessel wall temperature reduction			
	Large	Moderate	Small	Insignificant
External heat transport				
o Normal operation				X
o Removed insulation in region			X	
o Flooded reactor cavity			X[a]	
o Flooded cavity and removed insulation	X			
Heat transport to fluids in downcomer				
o Depressurization of RCS	X			
o Injection of cold water into downcomer				
o CF tank				
(Large to medium LOCA)	X			
(Small LOCA or large SLB)		X		
(Failure to isolate during shutdown)			X	
o HPI (Interrupted RC flow)	X			
(Natural or forced RC circulation)			X	
o LPI (Large to moderate LOCA)	X			
(RCS pressure >200 psi)				X

Table B.1. (continued)

Process	Potential for reactor vessel wall temperature reduction			
	Large	Moderate	Small	Insignificant
o Heat removal from recirculated reactor coolant				
o Excessive feedwater flow to S.G.		X		
o S.G. depressurization and cooldown during shutdown	X			
o Failed open steam relief valves		X[b]		
o Steam line rupture	X			
o CVC				X
o RHR	X			
Conduction of heat				X

[a]Will depend on integrity of vessel insulation.

[b]With main steam line isolation; if valves not isolated, the cooldown potential is considered large.

the RCS in excess of 650°F or pressurize the RCS using the HPI/CVC pumps.

B.2.1 Maintenance of a 650°F Saturation Temperature

Under normal operating conditions, the 2200 psi pressure in the RCS is achieved and maintained by controlling the saturation temperature of the pressurizer. The temperature of the liquid in the pressurizer is heated to ~650°F using electric resistance heaters. Since the balance of the RCS is operated below 600°F, the reactor coolant is maintained in a subcooled state.

Two other heat sources are capable of heating and pressurizing the RCS: the core, which generates residual heat even when subcritical, and the RC pumps, which recirculate reactor coolant and "generate" heat through viscous shear in the fluid. To the extent that heat generated in the RCS is not removed through the RHR system or steam generators, the heat will be added to the reactor coolant raising its temperature. The RCS pressure will increase to the saturation pressure of the highest temperature liquid in the system. Unless otherwise removed, the energy generated in the system would be removed by reactor coolant release through relief and safety valves.

During most operating conditions, the pressurizer power operated relief valve (PORV) and the two code safety valves open at pressures >2400 psi. When the reactor is being shutdown, the PORV may be reset to ~500 psi and if the RHR system is in operation; the RHR system relief valve is set to open at ~350 psi. It is thought that the reset PORV and/or RHR system relief valves can limit system pressure to <2000 psi. The capacities of these valves should be investigated further.

Although the core and/or RC pumps are capable of repressurizing the system, the process is expected to be very slow. During the heatup of the fluid, heat transfer to the vessel wall must be taken into account.

B.2.2 Pressurization of the Reactor Coolant System with the High-Pressure Injection/Chemical and Volume Control System Pumps

In addition to raising the reactor coolant temperature, the RCS may be pressurized by injecting fluid into the system. The three HPI/CVCS pumps are capable of injecting fluid into the RCS at pressures >2000 psi. These pumps have a shutoff head of over >3000 psi and each is capable of pumping at ~300 gal/min at RCS pressures >2000 psi.

The rate at which the HPI/CVCS pumps can pressurize the system will depend on the flow rate and the thermodynamic state of the RCS. Normally, 700 ft^3 of saturated steam is maintained in the pressurizer. As liquid is injected, the steam will compress and begin to condense because of higher than saturation pressure and lower injected water temperatures. After the steam is entirely condensed (solid water RCS),

the pressure rise to the relief valve set point would occur rapidly. During shutdown, nitrogen is injected into the pressurizer to control pressure. The nitrogen would compress, similar to steam, but would not condense.

One or two HPI/CVCS pumps are normally in operation during power operation and shutdown modes. For reactor coolant purification, ~50 gal/min of reactor coolant is "letdown" from the RCS to the makeup tank. The fluid in the makeup tank is then pumped into the RCS at a rate controlled by the makeup control valve sufficient to maintain pressurizer level. A failure of the makeup control valve could inject the contents of the makeup tank into the RCS. However, since the RCS and CVCS form a closed system, the RCS pressure rise is limited.

During shutdown and cooldown of the RCS, a net injection of fluid to accommodate reactor coolant contraction is required. Since the boric acid concentration of the reactor coolant must be increased in this shutdown mode, the makeup volume is supplied by the concentrated boric acid tanks. In this mode, a failure of the makeup valve controls could drive the RCS to pressures >2000 psi unless the PORV or the RHR safety valve was available to limit the pressure increase.

The HPI/CVCS pumps also are used to perform the high-pressure injection safety function. Two of the pumps are automatically started by the ESFAS upon detected low RCS pressure, high containment pressure or low steam pressure. Inadvertent actuation of HPI can also occur. When initiated, water in the BWST is pumped by the HPI pumps directly into the RCS at the maximum (unthrottled) flow rate. During shutdown operation, the automatic initiation functions are manually bypassed. In the HPI mode, pressurization of the RCS could occur as described for the CVCS mode.

B.2.3 Other Pressurization Modes

Although the mechanisms described in Sects. 2.2.1 and 2.2.2 are the only identified means of reaching 2000 psi, coreflood tank (CFT) injection must also be considered. The CFT can only inject at RCS pressures <600 psi. However, the introduction of this mass into the RCS may increase the rate of repressurization in the other modes described.

B.3 PRESSURIZED THERMAL SHOCK SEQUENCES

Mechanisms which individually may result in vessel wall temperatures <300°F or RCS pressures >2000 psi have been identified and discussed in Sects. 2.1 and 2.2. With some significant exceptions, the pressurization and cooldown transients must occur sequentially to produce the simultaneous occurrence of low wall temperatures and high RCS pressures. The sequential occurrence of these mechanisms is discussed in Sect. 2.3.

Sixteen PTS sequences involving "large" or "moderate" cooldown mechanisms (see Table B.1) and potential pressurization mechanisms are listed and evaluated in Table B.2. These transients fall into four types:

- o planned events--hydrotest,
- o maintenance of normal operating pressure and a vessel wall cooldown transient,
- o maintenance of planned shutdown temperatures and a repressurization transient, and
- o transients which couple cooldown and repressurization mechanisms.

In Table B.2, the vessel wall cooldown and pressurization mechanisms are listed for each sequence together with interactions that may affect the course of the transient. Interactions include control room operator intervention and the operation of relief valves. A qualitative evaluation of the "potential significance" of the transients also has been made for each sequence. This evaluation considered the potential for the physical process to result in the low temperature, high pressure PTS condition (i.e., a large LOCA is judged "insignificant" with respect to PTS since RCS pressures >2000 psi could not be maintained).

B.3.1 Planned Events

Hydrotests of the RCS typically are required following RCS pressure boundary repair. The conditions existing during a hydrotest are specified by regulation. However, inadvertent violation of these regulations could result in a PTS transient. It should be noted that these are performed with the core shutdown.

B.3.2 Maintenance of Normal Operating Pressure and Vessel Wall Cooldown

One sequence has been identified which would reduce the vessel wall temperature without affecting RCS pressure--external heat transfer to a flooded vessel cavity. Although of large potential significance, this transient is expected to be a relatively low frequency event. To achieve high wall heat transfer, removal or displacement of a section of insulation in the high-irradiation region is necessary. Because of the large volume, a significant period of time will be required to flood the vessel cavity to the level of the high-irradiation zone. During this time the control room operator would probably be capable of isolating the source of water. Under conditions of an in-containment steam line break (SLB), however, the automatically actuated containment sprays may be allowed to operate for a long period of time.

Table B.2. Pressurized thermal shock mechanisms

Principal cooldown mechanism	Principal pressurization mechanism	Other interactions	Potential significance
Planned events			
Planned cold shutdown	Planned hydrotest of RCS	Violation of technical specifications (Maintenance of RCS temperatures in excess of RT_{NDT})	Large
Maintenance of normal operating pressure and vessel wall cooldown			
Flooded reactor cavity with water	None required-M-normal operation	Operator intervention insulation removal or degradation required	Large
Maintenance of planned shutdown temperature and a repressurization transient			
Normal shutdown	Makeup valve failure prior to RHR	Pressure limited by PORV if reset or operator intervention	Large if PORV not reset or PORV fails
Normal shutdown	Spurrious HPI initiation	Pressure limited by PORV if reset or operator intervention	Large if PORV not reset or PORV fails
Normal shutdown	Pressurizer heater control failure	Pressure limited by PORV if reset or operator intervention	Large if PORV not reset or PORV fails
Normal shutdown	Feedwater failure	Pressure limited by PORV if reset or operator intervention operation of RC pumps or internals vent valves will result in vessel wall heat up	Insignificant RCS temperature rises

Table B.2. (continued)

Principal cooldown mechanism	Principal pressurization mechanism	Other interactions	Potential significance
RHR-normal shutdown	HPI/CVC failure	Pressure limited by RHR relief valve and/or reset PORV	Insignificant
RHR-normal shutdown	Feedwater failure	Pressure probably limited by RHR relief valve and/or reset PORV. Temperature of vessel wall will increase caused by operation of RC pumps or internal vent valves	Insignificant RCS temperature rises
Transients which couple cooldown and repressurization mechanisms			
Steam line break (SLB) automatic HPI and CFT injection will increase cooldown of vessel wall	HPI (automatic actuation) automatic CFT injection will increase repressurization rate	Cooldown may be limited if break can be isolated	Large
Failed open steam relief valves	HPI (automatic actuation)	Cooldown limited by automatic SG isolation-pressurizer heaters in operations when pressurizer liquid level is sufficiently high.	Small-if no SG isolation (see SLB)
HPI (interrupted RC flow)	HPI (probable automatic actuation). Net increase in reactor coolant mass required.	SG may be manually depressurized to limit RCS pressure. Flow through internals vent valves may limit vessel wall cooldown.	Large-M-however effect of internals vent valves must be investigated

Table B.2. (continued)

Principal cooldown mechanism	Principal pressurization mechanism	Other interactions	Potential significance
CFT injection (small LOCA)	Not credible-M-LOCAs sufficiently large to depressurized RCS to 600 psi will effectively limit repressurization. For the case of isolation of a failed open PORV see (interrupted RC flow)		Insignificant
CFT injection (large to medium LOCA)	Not credible		Insignificant
LPI (large to medium LOCA)	Not credible		Insignificant
CFT injection (SLB)	See SLB sequence 9		
Excessive feedwater flow to SG	HPI (probable automatic actuation)	Possible automatic isolation of main feedwater on low RCS pressure.	Small-unless SG depressurized (see SLB sequence 9). Large if not terminated.

The inspection procedures and design of the vessel insulation would have to be reviewed, and the conditions required for significant vessel cavity flooding would have to be analyzed to further evaluate this PTS sequence.

B.3.3 Maintenance of Planned Shutdown Temperature and a Repressurization Transient

Reductions in RCS temperature to 120°F for planned plant shutdown occur more than once per year. Should a repressurization transient occur during this time, the PTS conditions would result. These sequences are identified in Table B.2.

Should the HPI/CVC systems fail in the injection mode or the pressurizer heaters fail "on" prior to RHR operation, the repressurization could be limited by the PORV or by operator intervention. Typically, the PORV is reset to ~500 psi specifically to limit pressurization in a cold RCS condition. Thus, failure of the operator to reset the PORV or PORV failure are integral items in these PTS sequences. In addition, even if the PORV were to be closed, the existence of the pressurizer steam volume would delay repressurization and possibly allow the operator to terminate the repressurization manually. It is recommended that the operating procedures, including the resetting of the PORV, be further investigated to evaluate these sequences.

With the RHR system in operation during RHR-normal shutdown the RCS would be further protected from repressurization by the RHR safety valves set at ~350 psi. The capacity of these valves could be investigated.

B.3.4 Transients Which Couple Cooldown and Repressurization Mechanisms

Transients may be postulated which would simultaneously initiate cooldown and repressurization mechanisms. The initiating transient may, itself, be a relatively low-frequency event. However, after it occurred, the PTS conditions may be likely. These transients are identified in Table B.2.

A large SLB occurring upstream of the main steam isolation valves (MSIV) will result in a rapid cooldown and depressurization of the RCS. A break downstream of the MSIV or a failure (open) of the steam dump valves would be isolated automatically and the transient terminated. RCS temperatures <300°F are predicted for a major SLB.

Following the cooldown, the low RCS pressures will result in automatic injection from the CFT and the HPI. This will augment the cooldown and repressurize the RCS. Repressurization times of <20 min are possible.

During the repressurization, heat transfer to the steam generators is expected to be minimal (the affected steam generator will be isolated

and the other will be pressurized to 1000 psi and 500°F). The heat generated in the core will raise the temperature of the reactor coolant. With the RC pumps in operation, significant reheating of the vessel wall is possible. If the RC pumps are not in operation, reactor coolant heated in the core may flow directly to the downcomer through the internal vent valves and mix with the inlet fluid, heating the vessel walls.

The potential for a SLB to produce PTS conditions is considered significant. It is recommended that the temperature response of the RCS to this transient during the cooldown and repressurization/heatup modes be investigated in detail.

A LOCA will depressurize the RCS and result in the initiation of the HPI. Under certain conditions the HPI may produce a vessel wall cooldown and RCS repressurization. In general, LOCAs which result in CFT injection or LPI are too large to allow repressurization by the HPI. Two cases remain: a PORV failure subsequently isolated or a small break LOCA.

Following a small LOCA, RCS pressure will decrease because of heat removal to the steam generators and the mass/energy removal through the break. Assuming the RC pumps are tripped per procedure (this should be checked), the reactor coolant lost in excess of the HPI capacity through the break will eventually cause loss of circulation of reactor coolant, resulting in a loss of heat transfer to the steam generators.

In this condition, the energy produced in the core will be stored in the reactor coolant (as saturated steam or water) or released through the break. The mass inventory will vary with the HPI flow rate and mass loss rate. Under some conditions of break size and location, core heat production and HPI flow rate, RCS repressurization could result.

The cold HPI fluid injected into RCS inlet pipes can eventually decrease the inlet reactor coolant temperature below 300°F. However, under these conditions, the pressure at the core exit will be slightly higher than the downcomer because of the density differences in the downcomer and core fluids. This will result in a flow of reactor coolant from the core exit into the downcomer through the internal vent valves.

The downcomer fluid in contact with the vessel wall will be a mixture of the hot fluid from the core and the core fluid from the inlet piping. If the mixture temperature falls below 300°F, PTS conditions can occur. It is recommended that the fluid and wall temperature distributions be investigated in detail.

The last sequence considered is a main feedwater flow control malfunction resulting in excessive flow to one or both steam generators. Typically this will result in a reactor trip. Following reactor trip or the detection of high steam generator level, the

control system may be capable of interminating feedwater. If the RCS pressure decreases below 1600 psi the feedwater flow will be terminated automatically by the ESFAS. If the pressure does not increase, RCS temperatures will be maintained.

Unless multiple failure modes are assumed, excessive feedwater flow to the steam generators cannot, of itself, lead to PTS. This condition may, however, jeopardize the integrity of the steam lines. If the feedwater flow is not terminated manually by the operator or automatically by the ICS or ESFAS, the steam lines will begin to fill with water. In addition to the increased deadweight, the interaction of the steam in the lines and the liquid could result in kinetic effects significantly, increasing the mechanical loads on the steam lines and their supports. The integrity of the steam lines under these conditions is jeopardized. The effects of a SLB have been previously discussed; however, a SLB under these conditions would be more severe because of the large steam generator inventory.

Based on the previous discussions, the generic systems potentially involved in overcooling events are listed in Table B.3.

Table B.3. Generic systems involved in overcooling events

N03[a]	Reactor coolant system
N04	Reactor coolant system
N07	Nuclear instrumentation system
N08	Residual heat removal/low-pressure safety injection system
S02	Engineered safety features actuation system
S03	Safety injection system
S05	Auxiliary feedwater system
C10	Containment spray system
E03	Instrumentation and control power system
P01	Main steam system
P02	Turbine generator system
P02.A[a]	Electro-hydraulic turbine control subsystem
P03	Turbine bypass system
P04	Condenser and condensate system
P05[a]	Feedwater system
W03	Cooling water systems
W04	Service water systems
W05	Refueling system

[a]Interfaces with B&W's Integrated Control System.

B.4 REFERENCES

1. Science Applications, Inc., Interim Report, In-Plant Reliability Data Base Development, SAI #1-245-08-036-00, November, 12, 1980.

2. Combustion Engineering Standard Safety Analysis Report (CESSAR).

3. Westinghouse Standard Safety Analysis Report (RESAR-41).

4. Babcock & Wilcox Standard Safety Analysis Report (BSAR-205).

5. General Electric Standard Safety Analysis Report (GESSAR-238).

6. W. H. Zimmer Nuclear Plant Final Safety Analysis Report.

7. Grand Gulf Nuclear Station, Final Safety Analysis Report.

8. Oconee Nuclear Station, Final Safety Analysis Report.

9. Stone and Webster PWR Reference Nuclear Power Plant Safety Analysis Report.

APPENDIX C

HYBRID MODEL OF OCONEE-1 PLANT

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

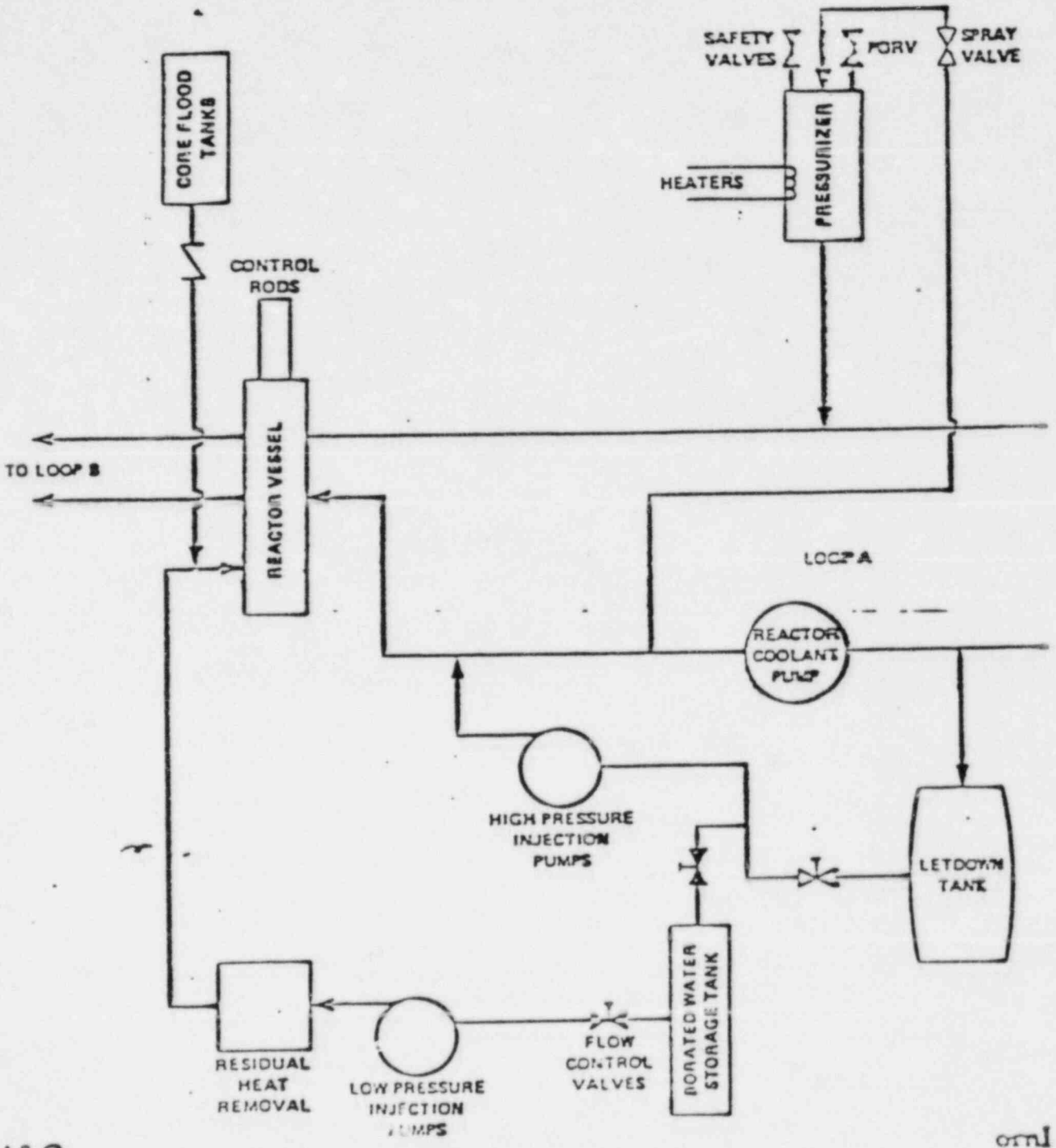
The simulations undertaken require various sets of model components, depending on the problem under consideration; for example, a problem in reactivity might not require consideration of the turbine. The range of problems to be considered is extremely broad. For example, some specific control-related safety issues that have occurred in the past are:

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

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

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

ORNL MODEL LAYOUT OF OCONEE 1
PRIMARY/SYSTEM



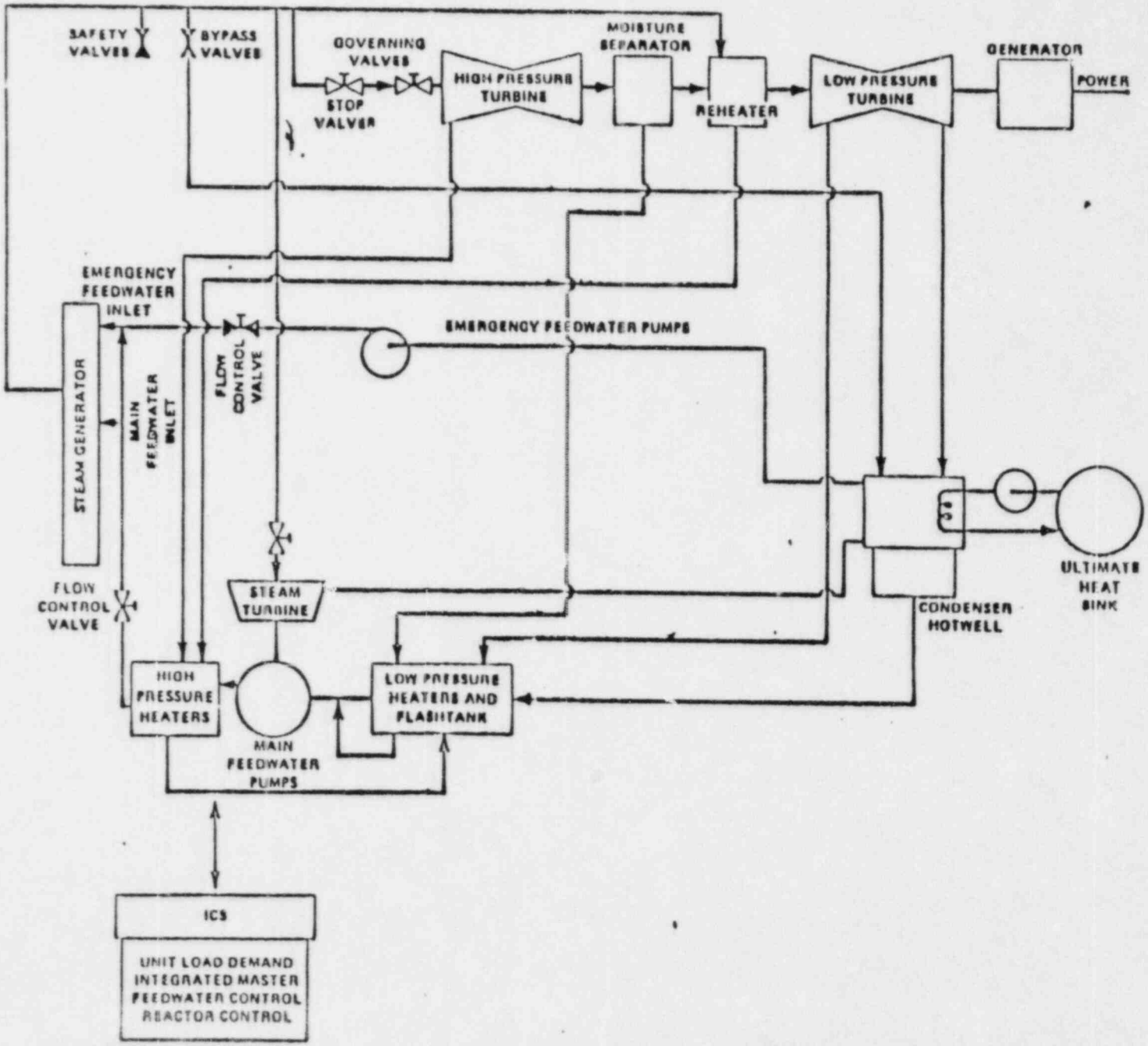
I&C

ornl

Figure 1b

ORNL-DWG 83-8948

ORNL MODEL LAYOUT OF OCONEE 1
SECONDARY SYSTEM



IAC

Details of the handling of the various plant systems are as follows.

I. Core

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

1. Zero-order kinetics, the simplest, is useful in afterheat and comparable fixed- or zero-flux studies.
2. Point kinetics, the next level of complexity, is useful in fixed flux-shape cases. Three to six neutron groups are appropriate.
3. One-dimensional (1-D) flux distribution is useful where axial spatial neutronics is important, for example when treating details of the interaction among rods and/or coolant temperature and/or boron poison in maintaining reactivity and axial offset. Here the computationally fastest appropriate 1-D code is used. The two-group diffusion approximation is employed. Control rod action can be simulated by suitably modifying neutron cross sections with a preprogrammed correlation between cross sections and rod location.
4. Though not used to this point, higher-order geometries (e.g., X-Y, R-θ, 3-D) could ultimately be included in the neutronics for a more complete mapping of core detail.

B. Thermal-hydraulics. In choosing a formalism for the core thermal-hydraulics we reviewed theories and codes developed in the United States and abroad that treat single- and two-phase flow, including RELAP-4, RELAP-5/Mod 1 (EG&G), TRAC PD2 and PF1 (LASL), RAMONA-3B (BNL), THOR (BNL), RETRAN-02 and FAST (EPRI), FLASH-5 (Bettis), COBRA-3 (Battelle), MATTEO (European Atomic Energy Community), BRUCH-DL (West Germany), HUBBLE-BUBBLE-1 (UKAEA), THIRST (Atomic Energy of Canada), SINOD (Yugoslavia), UTSG (West Germany), and STUDS 1,2 (Sweden). The methodology chosen most closely follows the formalism of RELAP-4.

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

II. Steam Generator

The PWR steam generator varies from vendor to vendor in ways that do not invite a single generic representation. B&W design characteristics were used for the initial model. Primary and secondary coolant were one pass systems. Coolant regimes having suitable correlations include: subcooling, nucleate boiling, transition boiling, film boiling, and superheating.

III. Pressurizer

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

IV. Reactor coolant pumps

The RETRAN-02, TRAC, and other codes include pump models; we have adapted this work to ours. Multiple pumps and loops are treated to allow studies of failures of fewer than all pumps, and thus asymmetries in the loops can be studied.

V. Turbine generator and feedwater heaters

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

VI. Feedwater pumps

RETRAN-02, TRAC, or other sources provide the formalism adapted to our model. Multiple pumps and loops were simulated and thus failure of fewer than all pumps can be studied. The auxiliary feedwater system was included.

VII. Condensate pumps

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

VIII. Emergency core cooling system (ECCS)

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

IX. Control system

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

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