BAW-1743

July 1982

FAILURE MODE AND EFFECTS ANALYSIS OF THE MIDLAND NNI AND ICS

Babcock & Wilcox

a McDermott company

BAW-1743
July 1982

FAILURE MODE AND EFFECTS ANALYSIS OF THE MIDLAND NNI AND ICS

by

R. S. Enzinna
R. W. Winks
S. D. Swartzell
R. F. Broadwater
M. S. Kai
W. E. Wilson

Reviewed by: Luther D Jaynes Aug 19, 1982
Date

Approved by: Eric W Swanson 8/13/82
Date

BABCOCK & WILCOX
Nuclear Power Group
Nuclear Power Generation Division
P. O. Box 1260
Lynchburg, Virginia 24505

Babcock & Wilcox

EXECUTIVE SUMMARY

An analysis was undertaken to provide responses to NRC Questions 30.56 through 30.59 of the Midland Final Safety Analyses Report (FSAR). The NRC request was to (1) identify power sources, sensors, or sensor impulse lines that serve two or more non-safety grade control functions, (2) demonstrate that failures would not result in consequences outside the bounds of the existing FSAR safety analyses, and (3) ensure they were within the capability of operators and safety systems.

Potential transients, which could occur at the Midland plant for failures within the non-nuclear instrumentation (NNI) and integrated control system (ICS) were evaluated. It was shown that all failures evaluated resulted in plant responses that were bounded by analyses included in the Midland FSAR and were within operator and safety system capabilities.

Analysis of NNI and ICS failure modes and effects included the following events:

1. Single instrument failures.
2. Power supply failures.
3. Common sensor impulse line failures.

The analysis of single instruments consisted of postulating failures of control system inputs and outputs one at a time and evaluating their effects on the plant. All single instrument failures resulted in either plant responses that are bounded by the FSAR analyses or operating anomalies not severe enough to be analyzed in the FSAR and well within operator capabilities.

NNI and ICS power supplies were investigated to determine if a failure could cause more than one control function to fail and to determine if the resulting plant responses are bounded. The NNI and ICS designs incorporate redundant power supplied to each system with normal and backup a-c and d-c power auctioneered within the ICS, NNI-X, and NNI-Y cabinets. There are no

credible single failures of external or internal power supplies that will result in loss of any NNI or ICS functions. However, for the purpose of analyzing plant response, losses of a-c and d-c power were postulated for the NNI-X, NNI-Y, and ICS. This evaluation shows that complete losses of a-c and d-c power for the NNI-X, NNI-Y, or ICS are bounded by the FSAR analyses.

The evaluation of common impulse line failures consisted of identifying sensor impulse lines, which provide signals to more than one control function, and evaluating the failure effects. The only common impulse lines identified where failures could simultaneously affect more than one non-safety grade control function were pressurizer level and pressure taps. In addition, a common line is shared with the NNI and the safety-grade reactor protection system for the reactor coolant flow taps. The resultant plant responses to failures of these lines were evaluated and determined to be bounded by FSAR safety analyses.

CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

1.1. NRC Questions

This report documents the evaluation performed in reply to an NRC request for additional information regarding answers to FSAR questions 30.56 through 30.59, which concern the Midland instrumentation and control system.[1]

The request is as follows:

> Your responses to Questions 30.56 through 30.59 on control system failure concerns are incomplete. We requested that you identify any power sources, sensors, or sensor impulse lines which provide power or signals to two or more control (functions) and demonstrate that failures of the power sources, sensors, or sensor impulse lines will not result in consequences outside the bounds of the Chapter 15 analyses or beyond the capability of operators or safety systems.
>
> The evaluation required to answer the above concerns should consist of postulating failures which affect the major control systems (both in NSSS scope and BOP scope) and demonstrating that for each failure the resulting event is within the bounds of the accident analyses. The events considered should include but not necessarily be limited to the following:
>
> a. Loss of any single instrument
> b. Break of any common instrument line
> c. Loss of power to any systems or equipment such as to any inverter, to any control group, or to any process rack.
>
> The initial conditions for the analysis should be within the full operating power range of the plant (i.e., 0-100%).

- - - - -

[1] ICSB, Question 3 attached to NRC Meeting Notice, October 23, 1981.

The response to Questions 30.56 through 30.59 should be revised to specifically identify non-safety grade control systems and the impact of the failure with reference to Chapter 15 analyses that insure that these events are bounded by the plant safety analysis.

Questions 30.56 through 30.59 of the Midland FSAR are:

Question 30.56

Identify those control systems whose failure or malfunction could seriously impact plant safety.

Question 30.57

Indicate which, if any, of the control systems identified in the response to request 30.56 receive power from common power sources. The power sources considered should include all power sources whose failure or malfunction could lead to failure or malfunction of more than one control system and should extend to the effects of cascading power losses due to failure of higher level distribution panels and load centers.

Question 30.58

Indicate which, if any, of the control systems identified in the response to request 30.56 receive input signals from common sensors. The sensors considered should include, but should not necessarily be limited to, common hydraulic headers or impulse lines feeding pressure, temperature, level, or other signals to two or more control systems.

Question 30.59

Provide justification that any simultaneous malfunctions of the control systems identified in the responses to requests 30.57 and 30.58 resulting from failures or malfunctions of the applicable common power source or sensor are bounded by the analyses in Chapter 15 and would not require action or response beyond the capability of operators or safety systems.

1.2. Objective

The objective of this study is to respond to the NRC request identified in section 1.1. The remainder of this report documents the evaluation required to answer those questions.

2. CONCLUSIONS

The failure modes and effects analysis (FMEA) performed for the Midland non-nuclear instrumentation (NNI) and integrated control system (ICS) and their related power suppplies demonstrates that the potential failures identified that result in a reactor trip lead to events which are bounded by the safety analyses contained in Chapter 15 of the Midland FSAR. The postulated failures of the ICS and pressurizer controls are itemized and each is shown not to seriously impact plant safety, and none require action beyond the capability of safety systems or operators.

Not all failures will cause a reactor trip, and therefore, in the strictest sense, these failures result in plant conditions that are not bounded by the Chapter 15 Safety Analyses. Clearly these failures are much less severe than events presented by the SAR and are of a nature that do not require such analyses. These operational anomalies could be described or categorized by the resultant plant effects

Benign: No plant change results
Stable: A new and different steady-state operating point is reached
Quasi-equilibrium: A slow, gradual change results.

Single instrument failures were evaluated on a sensor-by-sensor basis. All single instrument failures evaluated resulted in either plant responses that are bounded by existing FSAR analyses or very mild and short duration transients, which are not severe enough to be addressed in the FSAR.

The NNI and ICS have normal and backup a-c and d-c power supplies that are auctioneered within the NNI-X, NNI-Y, and ICS cabinets. Because of this design, complete loss of a-c or d-c power to a cabinet is considered an unlikely event. However, for the purpose of this evaluation, the effects of hypothetical power supply failures were analyzed. The evaluation showed that the plant can withstand a complete loss of a-c or d-c power to the NNI-X, NNI-Y, or ICS with consequences within the bounds of the FSAR analyses.

The evaluation of common impulse lines identified common taps for pressurizer pressure and level. No other common line was identified whose failure could simultaneously affect more than one non-safety grade control function. It was also found that reactor coolant (RC) flow taps in the NNI are shared with the safety-grade reactor protection system (RPS), this is a protection rather than a control system. The evaluation shows that plant responses to failures of these common impulse lines are bounded by FSAR safety analyses.

3. SCOPE

A FMEA was performed on selected control systems. Failure modes were postulated for power sources, sensors, and sensor impulse lines whose failure may lead to simultaneous failure of control systems. Plant response was evaluated and a bounding FSAR safety analysis was identified for each applicable postulated failure.

3.1. Control Systems Included

The evaluation required to answer the NRC request consists of postulating failures that affect the major non-safety grade control systems and demonstrating that the resulting event for each failure is within the bounds of the Midland FSAR Chapter 15 accident analyses. This evaluation specifically addresses failure or malfunction of the major non-safety grade nuclear steam system (NSS) and balance-of-plant (BOP) control systems. The following control systems were included:

1. The ICS which includes the usual subsystems for reactor, turbine, and main feedwater (MFW) controls, in addition to the evaporator steam demand development system (ESDD).
2. Pressurizer controls, which include pressurizer heater, spray, and level (normal makeup) controls. These controls are supported by signals of the NNI.
3. Other miscellaneous plant controls (not given above) that have common power supplies, share common sensor inputs, or share common impulse lines are:
   a. Shared power supplies:
      (1) The RC pump seal injection control function of the makeup and purification system.
      (2) Boric acid addition tank interlocks of the chemical addition system.

   Note: Failures of power supplies for these functions produce no change of plant operation.

b. Shared sensor inputs:
   (1) None.

c. Shared sensor impulse lines (taps):
   (1) A common tap for RC flow instrumentation supplies input to the ICS and RPS.

No other control systems were identified that shared sensor inputs, sensor impulse lines, or power supplies.

3.2. Events Included

The failure events that have been postulated are:

1. Loss of any single instrument.
2. Power supply failures affecting more than one control function.
3. Loss of common sensor impulse lines.

Each of these failure events is described in detail in the following subsections.

3.2.1. Loss of a Single Instrument

Failures of sensor inputs and control signal outputs of the control systems were postulated one at a time and the effects on plant response were evaluated. Each input signal was postulated to fail instantaneously high (+10 volts), midscale (zero volts), and low (-10 volts) for analog signals, and high and low for contact inputs.

Figure 1 is a simplified schematic illustrating the ICS, NNI, and sources of sensor input. Table 1 lists the input signals to the NNI-X, NNI-Y, and ICS cabinets and outputs. The bulk of all the input signals originate in the NNI system located throughout the plant. In addition, there are two other sources of input signals to the ICS - the turbine-generator and other BOP equipment.

3.2.2. Power Supply Failures

Control functions that receive power from common power supplies were identified. Control system internal power supplies, in addition to inverters, higher level distribution panels, and load centers, were investigated to determine if failure or malfunction could cause failure or malfunction of multiple control functions.

The design of the external power supplies for the NNI and ICS incorporates redundant main and backup power sources from separate busses. The NNI-X, NNI-Y, and ICS each receive two redundant a-c power sources that are selected by an auto buss transfer logic and have two redundant d-c power supplies that are auctioneered within the NNI and ICS cabinets.

This configuration is very reliable and assures that there are no credible single failures of internal power supplies, inverters, higher level distribution panels, or load centers that will result in failure of the NNI or ICS. Because of the redundant nature of the NNI and ICS power supplies, single failure causes could not be postulated. However, for the purpose of analyzing plant response, complete losses of a-c and d-c power for the NNI-X, NNI-Y, and ICS were assumed. The specific power supply failures analyzed consist of the following

1. NNI-X 24 V dc failed to zero volts.
2. NNI-X 118 V ac failed to zero volts.
3. NNI-Y 24 V dc failed to zero volts.
4. NNI-Y 118 V ac failed to zero volts.
5. ICS 24 V dc failed to zero volts.
6. ICS 118 V ac failed to zero volts.

Figure 2 shows a simplified, single-line schematic of the power distribution system for the NNI-X. The power distributions for the NNI-Y and ICS are identical.

The effects of failures of individual fuses, although not explicitly included in the FMEA tables, are implicitly included in this evaluation. Sensors in the ICS and NNI are fused individually. The effects of single sensor fuse failures, therefore, are bounded by the evaluation of single instrument failures. In addition, the worst credible impact of a fuse failure (although the failure mechanism has not been postulated) is an individual power supply failure, which is bounded by the evaluation of the NNI-X, NNI-Y, or ICS power supply failures.

3.2.3. Loss of Common Sensor Impulse Lines

Failure of common sensor impulse lines, which could lead to failure or malfunction of multiple control system inputs, were identified. This investigation included the identification of common hydraulic headers, sensor taps,

and instrument lines feeding two or more control system inputs. The failure modes analyzed consisted of breaks for common level, pressure, or flow measurements, and open and short circuits for temperature measurements. In addition to common impulse lines in the major non-safety grade control systems, a unique condition for RC flow taps exists. RC flow is input to the ICS and the safety-grade RPS.

Plant response was evaluated for each failure mode; this evaluation is described below.

3.3. Failure Modes and Effects Analysis

3.3.1. Component and Failure Mode Identification

The postulated failure events for the evaluated control systems were compiled into tables. Separate tables were prepared for loss of any single instrument, power supply failures, and loss of common sensor impulse lines. The failed components, failure modes, and control system input signals affected were itemized.

The FMEA tables also contain columns for description of the transient effects and the FSAR bounding event identification. The following sections describe how the effects and bounding events were determined and itemized for each failure mode.

3.3.2. Evaluation of Plant Response

The failure modes identified for loss of single instruments, power supply failures, and common sensor impulse line failures were the input for the effects analysis portion of the FMEA.

Plant response to each of the identified failure modes was evaluated and itemized. In some cases plant response to the failure could be determined by engineering judgment or from previous analysis[2]; in other cases the transient was run on a simulator for the Midland plant to predict or verify plant response. In each case the predicted plant response was reviewed and verified by an experienced engineer with a good working knowledge of the plant, control systems, and operational experience at other B&W plants.

- - - - -

[2]Integrated Control System Reliability Analysis, BAW-1564, Babcock & Wilcox, August 1979.

The simulator used to evaluate plant response was the digital nuclear steam supply simulator at Babcock & Wilcox's Advanced Controls Research Facility, which was modified to represent the Midland Unit 2 plant.

3.3.3. Assumptions for Plant Response Analysis

The following assumptions were made in the evaluation of plant response:

1. The ICS is operating in a full automatic mode.

2. The operators do not manually switch any sensor or take manual control of any parameter/device during the transient.

3. The transient was evaluated for a period from the time the signals fail until a sufficient time past reactor trip to ensure adequate post-trip response, or if the reactor did not trip, the evaluation was run until a new quasi-steady-state operating condition was achieved. (The evaluations usually were run for about 10 minutes if reactor trip did not occur.)

4. Midland Unit 2, which is designed to generate either 855 megawatts electric or 40% process steam load combined with a power generation of 510 megawatts electric, was modeled.

5. Two power levels were established as initial conditions for the response to selected failures - 100 and 30% power. The lower value was selected to represent a typical low power operating condition. Low power evaluations were made when it was clear that the plant response would be significantly different from the high power condition.

3.3.4. Identification of Bounding Events

The FMEA identifies, where appropriate, an FSAR transient that bounds the effect of each failure mode.

The failures can be divided into two categories: (1) those that cause a reactor trip and (2) those that do not cause a reactor trip. The failures that do not cause a reactor trip result in very mild transients of short duration. A slightly different final steady-state is reached from the pre-failure steady state. These transients are not severe enough to be addressed in a FSAR. Thus, no identification of bounding FSAR transients for these failures is made. For transients where a reactor trip is predicted, a bounding transient is identified.

3.3.5. Basis for Selecting Bounding Events

Because the FSAR Chapter 15 analyses are prescribed for the Standard Review Plants for very definite sets of events each with specific initial conditions and equipment failure assumptions, the SAR analyses will not always bear a "one-to-one" relationship with the failures evaluated by this study. Therefore, the following criteria were selected to permit the most appropriate alignment. For each condition the criteria for determining whether the event is bounded by the SAR analysis are given.

1. For events that did not result in trip, no bounding SAR analyses are applicable. (Note, however, that the analyses that were performed showed acceptable results.)

2. For secondary plant events that did result in a reactor trip, the most dominant characteristic of the event was used to determine the appropriate SAR analysis.

   a. For events characterized by total or partial loss of feedwater, the SAR total loss of feedwater event was selected. The event was considered to be bounding if the SAR peak RCS pressure was greater than the event evaluated for this report.

   b. For events characterized by excessive feedwater, the SAR analysis was considered to be bounding if the feed flow increase was greater (the reference SAR analysis is 15.1.2.).

   c. For events characterized by loss of steam pressure through the turbine bypass, the SAR turbine bypass failure case was considered to be bounding if the steam flow increase was greater.

3. For events that affected rod control or improper signals to the control rods, no bounding SAR analysis was selected. A reactor trip will occur, and the rod control system action is terminated by the insertion.

4. RESULTS

4.1. Plant Response to Loss of Single Instruments

Failures of the ICS and pressurizer control inputs were evaluated on a sensor-by-sensor basis. The effects of high, midscale, and low failures for each instrument are presented in Table 2. A brief description of each anticipated transient, whether or not the reactor tripped, and the bounding safety analysis is presented. The effects of failures of single ICS outputs are presented in Table 3.

Figure 3 gives an example of plant response to a single sensor failure. The plant response was evaluated using the B&W Advanced Controls Research Facility simulator. This example illustrates the expected response of the plant when the evaporator steam demand signal fails from 0% (off) to midscale or 50% of total steam demand. This transient does not lead to a reactor trip but achieves a new steady-state operating condition for the reactor and the turbine. This plant response is typical of many single input signal failures when no reactor trip is expected.

In general, failure of instruments in the high or low position (+10 or -10 V dc) is much less likely than a midscale failure (zero volts dc).

4.2. Plant Response to Power Supply Failures

This section presents the evaluation results of the transient response of the Midland plant to specific NNI and ICS power supply failures that would result in loss of power to groups of ICS and pressurizer instruments.

The specific instruments affected by each power supply failure are dependent on the position of hand selector switches in the NNI that allow the operator to select between redundant X or Y powered measurements of the same parameter. For the purpose of evaluating power failure effects, specific hand selector switch positions were assigned. For conservatism, it was assumed that upon an NNI power failure, the operator would not switch hand selectors to

the "good" sensors. Table 4 shows the specific position assumed for each selector switch in the NNI. In general, NNI-X powered sensors were selected for loop A measurements, NNI-Y powered sensors were selected for loop B measurements, and average measurements were selected where available.

Each postulated power supply failure affects the plant controls by causing groups of ICS or pressurizer instruments to suddenly change from normal to false indications. Plant response was evaluated by applying the false control signals to the Midland plant simulator while operating at full and 30% power levels.

Tables 5a through 5j present a list of the corresponding control system instruments affected by each power supply failure. For both the full and 30% plant power levels, the tables indicate the normal operating value of each instrument and the failed value, which was applied to the simulator.

The effects of the power supply failures on plant response are itemized in Table 6. The transient effects of each power supply failure are described and the FSAR analyses that bound the events are identified.

An example of plant response is illustrated in Figure 4. This figure represents the simulator model prediction of the transient effects of NNI-X 24 V dc power loss at 100% power.

Loss of NNI-X 24 V dc from full power results in a rapid overheating transient caused by loss of main feedwater to both steam generators. This transient is bounded by FSAR analysis 15.2.7,"Loss of Main Feedwater." This transient is described in more detail, along with the other power failures, in Table 6.

4.3. Plant Response to Loss of Common Sensor Impulse Lines

Table 7 identifies the control system inputs that share common taps, hydraulic headers, or instrument lines. Most of the common impulse lines identified are taps that supply two measurements of the same parameter. The operator selects one of the two measurements so that only one at a time is used for control. Thus, the failure has the same effect as loss of a single instrument, which is described in Table 2.

The only common impulse lines identified whose failure could affect more than one ICS or pressurizer control function were the pressurizer level and pressure taps. The transient resulting from break of these taps is described in Table 7 and is bounded by FSAR analysis 15.6.2, "Break in Instrument Lines or Lines From Primary System That Penetrate Containment."

One other commonality identified was the RC flow measurements shared between the ICS and the RPS. This is a special case because the RPS is a safety-grade protection system and not a control system. This failure is covered in section 4.4.

4.4. Break in RC Flow Tap

The RC flow rate taps on loops A and B of the Midland primary system are shared between the ICS and the safety-grade RPS. The transmitters are arranged on each loop so that two of four RPS channels and one of two ICS transmitters are on each tap.

The transient that results from a failure of the loop A (or B) RC flow rate signal to the ICS when the plant is operating at full power has been run on the Power Train V (177-fuel assembly plant) simulator. Figure 5 shows several parameters that were selected to indicate the nature of the transient. The initial effect of the loss of a valid RC flow rate signal is to cause the loop A Btu limits circuit to suddenly generate a 0 lb/second feedwater (FW) flow rate to match the demand. Since the total FW flow rate is now less than the total FW demand, the FW flow rate to the loop B steam generator increases. The loop B FW control valve will open fully, while the loop A control valve is being stroked fully closed.

The cross limits circuit in the ICS senses that the actual total FW flow rate is less than the total FW demand signal and will attempt to reduce reactor

power to match the total available FW flow. The rate of core power reduction is approximately 25% per minute for beginning-of-life (BOL) conditions and slightly higher for end-of-life (EOL) conditions.

The reduction of FW flow rate caused by the loop A Btu limits circuit is faster than the reduction in reactor power (which is limited by control rod insertion speed) and overheating of the RC system occurs. This will cause a reactor trip on the high RC pressure channel of the RPS less than 1 minute after the failure of the loop A RC flowrate signal. This transient is bounded by FSAR analysis 15.2.7, "Loss of Main Feedwater."

Table 1. Midland NNI and ICS Signals

Signal (transmitter)	NNI-X	NNI-Y	ICS_{in}	ICS_{out}
NR pressurizer pressure				
(2-1)	•			
(2-3)		•		
Pressurizer level				
(14-1)	•			
(14-2)	•			
(14-3)		•		
Pressurizer temperature				
(15-1)	•			
(15-2)		•		
Reactor coolant flow				
Loop A (1A5)	•		X or Y	
(1A6)		•		
Loop B (1B5)	•		X or Y	
(1B6)		•		
Total temperature comp. RC flow			X or Y	
T_{hot}				
Loop A (3A1)	•			
(3A2)		•		
Loop B (3B1)	•			
(3B2)		•		
T_{cold}				
Loop A (4A1)	•			
(4A3)		•		
Loop B (4B1)	•			
(4B3)		•		
Startup feedwater flow				
Loop A (3A)	•			
Loop B (3B)		•		
Feedwater temperature				
Loop A (1A1)	•		X or Y	
(1A2)		•		
Loop B (1B1)	•		X or Y	
(1B2)		•		
Main feedwater flow				
Loop A (2A1)	•		X or Y	
(2A2)		•		
Loop B (2B1)	•		X or Y	
(2B2)		•		

Table 1. (Cont'd)

Signal (transmitter)	NNI-X	NNI-Y	ICS_{in}	ICS_{out}
Steam pressure				
Loop A (12A1)	•		X or Y	
(12A2)		•		
Loop B (12B2)	•		X or Y	
(12B1)		•		
Turbine throttle pressure				
"A" (16A)	•		X or Y	
"B" (16B)		•		
Feedwater control valve ΔP				
Loop A (5A1)	•			
(5A2)		•		
Loop B (5B1)	•			
(5B2)		•		
Startup level				
Loop A (9A3)	•		X or Y	
(9A4)		•		
Loop B (9B4)	•		X or Y	
(9B3)		•		
Operate level				
Loop A (9A1)	•		X or Y	
(9A2)		•		
Loop B (9B1)	•		X or Y	
(9B2)		•		
Downcomer temperature				
Loop A (8A1)	•			
(8A2)		•		
Loop B (8B1)	•			
(8B2)		•		
T/C main feedwater flow				
Loop A			X	
Loop B			Y	
T/C startup feedwater flow				
Loop A			X	
Loop B			Y	
T/C reactor coolant flow				
Loop A			X	
Loop B			Y	
Main feedwater pump tripped				
Loop A				•
Loop B				•
Loops A and B T_{cold} difference			X or Y	

Table 1. (Cont'd)

Signal (transmitter)	NNI-X	NNI-Y	ICS_{in}	ICS_{out}
Selected T_{hot}			X or Y	
T_{ave}			X, Y, or both	
Reactor coolant pump running				
A1			•	
A2			•	
B1			•	
B2			•	
Reactor not tripped			•	
Both generator breakers tripped			•	
Turbine on high load limit			•	
Turbine on valve position limit			•	
Power/load unbalance			•	
Low condenser vacuum			•	
Condenser water not available			•	
Closed position of turbine valve 13-1			•	
13-2			•	
13-3			•	
13-4			•	
Turbine is tripped			•	
Turbine control on auto			•	
Generated megawatts			•	
Neutron power			•	
Asymmetric rod pattern exists			•	
Is turbine runback initiated			•	
ESDD			•	
Frequency deviation			•	
Startup feedwater valve >80% open				
Loop A			•	
Loop B			•	
Startup feedwater valve <50% open				
Loop A			•	
Loop B			•	
Main feedwater block valve open				
Loop A			•	
Loop B			•	

Table 1. (Cont'd)

Signal (transmitter)	NNI-X	NNI-Y	ICS_{in}	ICS_{out}
AD valves position demand				
"A"				•
"B"				•
Open turbine valves				•
Close turbine valves				•
Open turbine valves 13-1, 2, 3, 4				•
Withdraw control rods				•
Insert control rods				•
Main feedwater valve demand				
Loop A				•
Loop B				•
Startup feedwater valve demand				
Loop A				•
Loop B				•
Open main feedwater block valve				
Loop A				•
Loop B				•
Close main feedwater block valve				
Loop A				•
Loop B				•
Request to trip turbine				•
Main feedwater pump speed demand				
Loop A				•
Loop B				•

Table 2. Plant Response to Failures of Single ICS and Pressurizer Control Inputs

Signals	Fails	Effect	Reactor trip	Transient bounded by
Loop A FW control valve ΔP	100 psi (high)	No effect. Auctioneer takes lower ΔP signal.	No	NA
	0 psi (low)	FW pumps go to high speed stop in attempt to maintain 50 psi across FW valves. FW flow to both SGs goes up, but FW control valves will close to bring FW flow back to setpoint; thus, overfeeding is only temporary. No change to post-trip control in the event that a reactor trip occurs, except that high pump speed causes higher pressure drop across FW valves (hence, control will not be as smooth as normal).	Unlikely	NA
	50 psi (midscale)	No effect if ΔP setpoint is less than 50 psid; same general effect as low failure above if ΔP setpoint is ≥50 psid.	No	NA
Loop B FW control valve ΔP		Same information as for loop A.		NA
Total temperature compensated RC flow	160 mpph (high)	No expected impact to power level.	No	NA
	0 mpph (low)	Loss of RC flow signal causes reactor runback to 15% at 20% per minute.	Unlikely	NA
	80 mpph (midscale)	Loss of RC flow signal causes reactor runback to approximately 50% at 20% per minute.	Unlikely due to sufficient RC flow rate during runback.	NA
Turbine header pressure	1200 psia (high)	Condenser dump and atmospheric dump valves go full open. Turbine throttle valves open for 5 seconds and then turbine transfers to manual and the ICS will go into tracking mode. Steam pressure decreases, MWe drops, and a reactor trip on low RC pressure normally results.	Yes	FSAR 15.1.3, "Steam Pressure Regulator Manfunction or Failure Resulting in Increasing Steam Flow"
	600 psia (low)	Turbine throttle valve closes for 5 seconds to try to maintain setpoint steam pressure. After 5 seconds, turbine transfers to manual and this causes actual steam pressure to increase, which causes trip of the reactor due to high RC pressure. Satisfactory secondary steam pressure control after reactor trip via the steam line safety valves.	Yes	FSAR 15.2.2, "Loss of External Electrical Load and/or Turbine Trip"
	900 psia (midscale)	This is a minor upset and no significant plant response will occur. Turbine will ramp open to reduce pressure to 885.	No	NA
SG outlet pressure, loop A	1200 psig (high)	SG-A Btu limits cause partial loss of feed flow to SG-A. Simultaneously, loop A bypass valves open. MW electric tracks down. Decrease in FW flow will cause reactor trip on high RC pressure. Loop A bypass remains open after reactor trip.	Yes	FSAR 15.2.7, "Loss of Main Feedwater"
	0 psig (low)	No effect on NSS.	No	NA
	600 psig (midscale)	No effect on NSS.	No	NA
SG outlet pressure, loop B		Results are the same as for loop A.		
FW temperature, loop A	500F (high)	If this failure occurs from 100% load, the expected result is an increase of FW flow to 110% times design flow. A momentary tracking condition will occur but normal T_{ave} and MWe control will bring unit back to steady state. While possible, a reactor trip is not expected. Final load may be slightly higher than initially. If failure occurs at low load, a greater percentage increase in MFW will occur, causing a higher probability of trip. The effect of a high FW temperature on Btu limits at low power is to raise the maximum FW flow allowed and adversely affect the 35F superheat protection to the turbine.	Not probable from high load.	

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
	0F (low)	Total FW demand would decrease approximately 40% due to Btu limits and each OTSG will be underfed leading to a reactor trip on high RC pressure.	Probable	FSAR 15.2.7
	250F (midscale)	For high power operation, reduction in MFW flow due to failed FW temperature on Btu limits will reduce MFW flow more than 10% and could cause a reactor trip on high RC pressure.	Probable	FSAR 15.2.7
FW temperature, loop B		Same as for loop A.		
Main FW flow, loop A	6.0 mpph (100%, high)	Loop A FW control valve closes to try to maintain constant indicated FW flow, which reduces actual flow. The partial loss of FW causes overheating of primary system and trips reactor on high RC pressure. Control after reactor trip is not changed. Startup level control prevents total loss of FW in affected loop.	Yes	FSAR 15.2.7
	0 mpph (0%, low)	Loop A FW valve will open fully. Loop A FW valve ΔP will decrease toward zero. Both MFW pumps will speed up. Loop B valve closes to reduce loop B flow. Loop A SG will be overfed and will cause a reactor trip on low RC pressure.	Yes	FSAR 15.1.2, "Feedwater System Malfunctions That Result in an Increase in Feedwater Flow"
	3.0 mpph (50%, midscale)	Depends on initial power level; a high power level resembles a "low" failure, only less severe. A low power level would resemble a "high" failure and would be less severe.	Probable, depending on reactor power level.	FSAR 15.1.2 or 15.2.7
Main FW flow, loop B		Same as for loop A.		
Startup FW flow, loop A	20% (high)	Above approximately 15% FW flow, startup measurement is not used for control; therefore, its failure has no effect. (Main FW block valve is open when flow is >15%.) Below approximately 15% flow high failure causes flow control valves to close until SG level drops to low level limit where flow will be restored by level controller.	Unlikely	NA
	0% (low)	No effect if MFWBV is open due to power >15%. If MFWBV is closed, loop A startup (SU) valve goes 80% open, causing the switch from SU to main for FW flow indication. Subsequently, the SU valve on loop A will cycle between 50 and 80% open, causing block valve to open and close. A reactor trip on high RC pressure less than 15% power.	Probable for power less than 15%	FSAR 15.2.7
	10% (midscale)	Either the SU valve will open or close depending on initial MFW flow rate (or power). Severity of these events is much smaller than high and low failures.	Unlikely	NA
Startup FW flow, loop B		Same as for loop A.		
Temperature compersated RC flow, loop A	80 mpph (100%, high)	This failure could cause an undesired re-ratioing of FW flow, decreasing loop B FW flow, and at high power levels very likely a reactor trip on high RC pressure. Control after reactor trip is not changed.	Yes	FSAR 15.2.7
	40 mpph (50%, midscale)	This will cause loop A Btu limits to reduce FW flow and lower loop A SG level. Overheating will lead to a reactor trip on high RC pressure.	Yes	FSAR 15.2.7
	0 mpph (0%, low)	FW flow will re-ratio with SG-A going on low level limit and SG-B feed flow limited only by Btu limits. For initial load of 100%, there is a net reduction in FW flow, and reactor will trip on high pressure. Control after reactor trip is not changed.	Yes	FSAR 15.2.7

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
Temperature compensated MC flow, loop B		Same as for loop A.		
SG-A operate level	100% (high)	Loop A feed flow will be reduced until SG-A level decreases below high level limit. Large reduction of FW flow causes overheating of primary and reactor trip on high pressure. Control after reactor trip is not changed.	Yes	FSAR 15.2.7
	0% (low)	No effect, except that SG-A loses protection of having a high level limit.	No	NA
	50% (midscale)	Same as 0% since normal setpoint is approximately 87.5%.		NA
SG-B operate level		Same as for SG-A.		
SU level, SG-A	250 in. (high)	No effect on operation above 20% power level. Below 20%, FW flow is on low level control. Prevents proper level control, and SG-A could boil dry.	No (at power levels above 20%)	FSAR 15.2.7
	0 in. (low)	FW control valves go full open and remain open after reactor trip. This would cause an overfill of SG-A, overcooling of the primary, and possible loss of pressurizer inventory and/or level indication.	Probable	FSAR 15.1.2
	125 in. (midscale)	Same as the high failure.		
SU level, SG-B		Same as for SG-A.		
Selected reactor outlet temperature, loop A, T_h	620F (high)	This failure causes T_{ave} to increase 15-20F, creating a large neutron error. The neutron error will cause rod insertion and will generate a cross limit to the FW controller that will increase total FW flow in an attempt to cool RCS. The combination of rod insertion and increased FW flow will overcool RCS and will likely cause a reactor trip, probably at low RC pressure. Control after reactor trip is unaffected.	Yes	FSAR 15.1.2
	520F (low)	Btu limits reduce feed flow to zero in loops A and B. Reactor trips on high RC pressure very quickly because of reduction of feed flow to both OTSGs. Control after reactor trip is not changed.	Yes	FSAR 15.2.7
	570F (midscale)	This will cause a low T_{ave} error, but ICS will probably adjust without causing a reactor trip.	Unlikely	NA
Selected reactor inlet temperature, loop A, T_c	620F (high)	This failure will cause T_{ave} to suddenly exceed the setpoint and ICS will insert rods and increase total FW demand to restore T_{ave}. Also, difference in cold leg temperatures will cause ICS to overfeed one SG and underfeed the other. Underfeeding will happen before rods are inserted and RCS will overheat. This will probably cause a reactor trip on high pressure.	Probable	FSAR 15.2.7
	520F	A low T_{ave} signal will develop from this failure and ICS will pull rods and lower total FW demand. Meanwhile, T_c will re-ratio FW flows, starving SG-A and overfeeding SG-B. Again, reactor would trip on high RC pressure due to overheating RCS.	Probable	FSAR 15.2.7
	570F (midscale)	This failure will cause T_{ave} to exceed its setpoint, rods will insert, and ΔT_c will re-adjust flows to both OTSGs. ICS and plant may adjust without a reactor trip or eventually the reactor will trip on high RC pressure.	Probable	FSAR 15.2.7

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
Reactor inlet temperature, loop A/B difference, ΔT_C	+10F (+ high, - low)	Feed flow to one SG goes up while flow goes down in other loop. If initial load is high enough, there will be a net reduction of total feed flow due to a Btu limit holding flow down in one SG, and a resultant reactor trip on high pressure. Control after reactor trip is not changed.	Probable	FSAR 15.2.7
	0F (midscale)	Normal operation, therefore, no effect.	No	NA
Reactor average temperature, T_{ave}	620F	Continuous control rod insertion. Cross limits will increase FW flow. Btu limits bring FW flow down as RC outlet temperature goes down, but overcooling is sufficient to cause reactor trip on low pressure. Control after reactor trip is not changed.	Probable	FSAR 15.1.2
	520F (low)	Reactor demand goes to 103%, causing rod pull. FW flow comes down due to cross limits. Reactor trips on high pressure due to overheating. Control after reactor trip is not changed.	Probable	FSAR 15.2.7
	570F (midscale)	Same as low T_{hot} or low T_{cold} failures above.	Probable	FSAR 15.2.7 or FSAR 15.1.2
RC pump running signal (any of four)	Falsely indicates pump not running	Initiates runback from 100 to 75% or from 75 to 45% power level at a runback rate = 50%/minute. Control after reactor trip is not changed.	No	NA
	Does not indicate pump not running	Fails to initiate reduction in power level at 50%/minute, but change in total RC flow will initiate a 20%/minute reduction. Reactor trip expected. Flux-to-flow trip on four pumps 100% power.	Probable	FSAR 15.3.1, "Single and Multiple Reactor Coolant Pump Trips"
Reactor not tripped	Not tripped	No effect until reactor trips. When reactor does trip, ICS cross limits will reduce MFW flow. Assume turbine is tripped by valid reactor signal; otherwise, throttle valves will close slowly to maintain steam pressure. Steam pressure controlled to 900 psi rather than 1015 psi after reactor trip.	No	NA
	Tripped (spuriously)	ICS action on MFW flow with reactor actually at power will not cause a real reactor trip. Turbine valves go to manual, ICS will track, and plant will run back to 15%.	No	NA
Both generator breakers tripped	Tripped	ICS goes into track and will not respond to changes in load demand. MW calibration integral is blocked so that generated MW may drift high or low. Poor control of MWe should not lead to a reactor trip. Control after reactor trip is not changed.	No	NA
	Not tripped	No impact until breakers actually trip. In the event a breaker trip occurs, the ICS will still perform adequately since high steam pressure will transfer turbine to manual, inducing a tracking condition.	No	NA
Generated MW	1000 MW (high)	Power level goes down by about 15%. Control after reactor trip is not changed.	No	NA
	0 MW (low)	Steam flow rate will try to increase reactor power and FW flow will be limited at about 103%, continued decrease is steam high flux setpoint. Reactor trip on high flux.	Yes	FSAR 15.1.2
	~50 MW (midscale)	Depending on initial power level, either high failure response, low failure response, or essentially no response (at midrange power levels).	Yes	FSAR 15.1.2
Low condenser vacuum or no condenser cooling water	Falsely indicates loss of water and vacuum	Either of these can cause turbine bypass valves not to open. However, atmospheric exhaust and safety valves are still available for pressure control after reactor trip.	No	NA

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
	Falsely indicates vacuum and water when really not available	Turbine bypass valves would pass steam to non-working condenser after turbine trip or a reactor trip and could cause damage to condenser.	No	NA
Turbine is tripped	Falsely indicates trip when turbine is running	Turbine will be transferred to manual. ICS goes into track mode and will follow actual generated MW. Turbine valves will control steam pressure to normal steam pressure setpoint. Would not lead to a reactor trip. If a reactor trip occurred, turbine would be tripped.	No	NA
	Falsely indicates no turbine tripped when there is	Without turbine usually going to manual and initiating tracking mode, loss of turbine could cause overheating of RCS and high RC pressure trip of reactor.	Yes	FSAR 15.2.2
Neutron power	125% (high)	Continuous control rod insertion and ICS cross limits causing an increase in FW flow (to the Btu limit) combine to create an overcooling and a reactor trip on low RC pressure. Control after reactor trip is not changed.	Yes	FSAR 15.1.2
	0% (low)	Continuous control rod withdrawal coupled with decreased FW flow will cause an overheating transient and a reactor trip on high RC pressure. Control after reactor trip is not changed.	Yes	FSAR 15.2.7
	62.5% (midscale)	Depending on initial power level, will cause either overcooling or overheating and probably reactor trips.	Probable	FSAR 15.2.7 or FSAR 15.1.2
Asymmetric rod pattern exists	Fault signal exists but pattern is okay	Runback to <60%. ULD at 30%/minute rate. Control after reactor trip not changed.	No	NA
	Asymmetric rod pattern exists but no signal is generated	No change in plant operating conditions until operator discovers it. He would initiate power runback to 60%.	Unlikely	NA
Loop A SU FW control valve >80% open	Falsely indicates >80% open	During low power startup, this failure would prematurely open MFW block valve. MFW control valve will be closed; however, some leakage through main valve is expected. Leakage should be small and can be compensated for by slight closure of SU valves. Excessive leakage may cause SU valve to close to 50%. At 50% a main block close signal will be generated and cycling of main block could occur.	No	NA
Loop A SU FW control valve <50% open	Falsely indicates <50% open	For any power level >15% with SU main block and main control valves all operating, this signal would close MFW block valve. This is a loss of MFW to OTSG-A at high power levels. Reactor will trip on high RC pressure.	Probable	FSAR 15.2.7
	Does not indicate <50% open	During power decrease when SU valve is <50% open this failure will not cause MFW block valve to fully close automatically.	Unlikely	NA
Loop B SU FW control valve <50% open		Same as for loop A.		
Main FW block valve open, loop A	Closed	Would transfer ICS FW flow input to SU flow. If at high load, the effect would be very similar to low failure of ICS FW flow signal. One SG is overfed and the other is underfed. Reactor trips on either high or low RC pressure depending on initial power level. Control after reactor trip is not changed.		FSAR 15.2.7 or FSAR 15.1.2

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
	Open	Would prevent transfer of FW flow indication from main to SU flow output. Would interfere with accurate FW control during orderly shutdown. Probably would not cause a reactor trip. Control after reactor trip not changed.	Not expected	NA
Main FW block valve open, loop B		Same as for loop A.		
Loop A MFW pump tripped	Falsely indicates FW pump trip	Would initiate a power runback to 55% power at 50%/minute. With both FW pumps actually running it should not lead to a reactor trip.	Unlikely	NA
	Falsely indicates FW pump is not tripped	For a real FW pump trip at high power, FW flow to both OTSGs will suddenly decrease then increase as FW pump speed increases to high speed stop. ICS will attempt to reduce power by cross limits but reactor will probably trip on high RC pressure due to overheating.	Probable	FSAR 15.2.7
Loop B MFW pump tripped		Same as for loop A.		
Pressurizer pressure (narrow range)	2500 psig (high)	Spray valve is opened. Primary system will depressurize very slowly and eventually a reactor trip on low RC pressure is expected. Control after reactor trip should be changed by operator action. To terminate this transient, operator should manually close spray block valve. This is a slow transient and operator has ample backup indication for diagnosis.	Yes	This is a mild transient, which does not have a specific evaluation in the FSAR. This event is similar to a very, very small LOCA and, therefore, is bounded by FSAR 15.6.2, "Break in Instrument Lines or Lines From Primary System That Penetrates Containment"
	1700 psig (low)	The spray valve will stay closed but all pressurizer heaters will come on. As pressurizer pressure increases, safety-grade PORV will open to control pressure. Control after reactor trip would not be changed. Reactor trip not expected. This is a slow transient and operator has ample backup indication for diagnosis.	No	NA
	2100 psig (midscale)	Same as low failure.		
Pressurizer level (selected)	400 in. (high)	Makeup valve will close and RCS pressure and pressurizer level will slowly decrease due to letdown flow greater than makeup flow. This is a slow transient and operator has ample backup indication for diagnosis.	Possible (low RC pressure)	This is a mild transient, which does not have a specific evaluation in the FSAR. This event is similar to but less severe than a letdown line break, and therefore is bounded by FSAR 15.6.2
	200 in. (midscale)	Makeup valve will open to try to raise level. Pressurizer level will increase and spray and PORV may operate to limit RC pressure. This is a cyclic pressure transient. This is a slow transient and operator has ample backup indication for diagnosis.	Possible (high or low RC pressure)	FSAR 15.5.1, "Inadvertent Operation of ECCS During Power Operation"
	0 in. (low)	Makeup valves will open. RC pressure will increase. Pressurizer interlock will be active but no heaters are required. Spray and PORV will open to control RC pressure. This may also be a cyclic pressure transient. This is a slow transient and operator has ample backup indication for diagnosis.	Possible (high or low RC pressure)	FSAR 15.5.1
Pressurizer temperature (selected)	750F (high)	This causes temperature compensated level to be high and makeup turned off, real pressurizer level decreases. This not being detected could cause heaters to go on with no water covering them and heaters may burn out. This is a slow transient and operator has ample backup indication for diagnosis.	Yes (low RC pressure)	This is a mild transient, which does not have a specific evaluation in the FSAR. This event is similar to but less severe than a letdown line break, and therefore is bounded by FSAR 15.6.2
	400F (midscale)	This causes temperature compensated level to be low. Makeup comes on to refill pressurizer. Spray controls pressure. Reactor will trip on high RC pressure after spray nozzle is submerged. This is a slow transient and operator has ample backup indication for diagnosis.	Yes (high RC pressure)	FSAR 15.5.1

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
	OF (low)	Same as midscale failure.	Yes (high RC pressure)	FSAR 15.5.1
Is turbine load limited?	Turbine is not load limited but signal says it is	Any further increase in turbine demand shall be ignored. It is the equivalent to turbine valves being in manual and at a setpoint. Control after reactor trip unchanged.	No	NA
	Turbine is really load limited but signal says it is not	Additional increases in load demand will be followed. Potential damage to turbine could occur if another protection signal does not take it off line. Control after reactor trip unchanged.	No	NA
Is turbine runback initiated?	Loss of stator coolant but no runback initiated on power	In a short time it would be harmful to turbine. Vibration levels could rise with a turbine trip to follow. Control after reactor trip unchanged.	No	NA
	No loss of stator coolant but a power runback initiated	This causes no problem but would be a nuisance and would need to be discovered and repaired before reloading turbine. Control after reactor trip unchanged.	No	NA
Is turbine back-end flow limited? (Unit 1)	Turbine is not back-end flow-limited but signal says it is	This should prevent turbine from increasing load even though turbine is really not back-end flow-limited and could accept more load. Control after reactor trip unchanged.	No	NA
	Turbine is back-end flow-limited but signal says it is not	The purpose of the signal is to prevent turbine from receiving any more load. Without this signal and being really back-end flow-limited, any increase in load could potentially damage turbine. Control after reactor trip unchanged.	No	NA
Frequency deviation	+3 Hz (high)	This is a power reduction or step down to ICS running back FW and reactor. The FW runs back faster than reactor power; however, with a limiter on frequency deviation, reactor should not trip.	Not expected	NA
	0 Hz (midscale)	No effect. ICS has no frequency deviation even when grid frequency is not 60 Hz and will adjust to whatever new operating condition turbine has changed to. Control after reactor trip unchanged.	No	NA
	-3 Hz (low)	This causes a step up in power limited by 105% reactor power. FW could run up faster than reactor power; however, with a limiter on frequency deviation, reactor should not trip. Control after reactor trip unchanged.	Not expected	NA
Turbine on valve position limited	Valve position is limited but signal fails to indicate limited	Additional load will go to turbine, but since valves will not open further, steam pressure may increase as much as 30 psi in both SGs. Control after reactor trip is unchanged.	No	NA
	Valve position is not limited but signal indicates it is	Any additional load request on turbine is ignored. Control after reactor trip is unchanged.	No	NA
Power/load unbalanced signal	Signal says power/load unbalance but is not power/load unbalance	Power/load unbalance signal is sent to ICS to switch into tracking mode. Meanwhile, power/load unbalance signal in turbine controls is also trying to lower turbine power to clear unbalance. It could run turbine back to 0% load. Control after reactor trip is unchanged.	No	NA

Table 2. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
	Signal says no power/load unbalance but there is	Power/load unbalance signal does not work when turbine is really unbalanced. Turbine may run unbalanced until another shutdown signal is created or turbine is runback on power/load unbalance; i.e., only the signal to ICS failed. ICS would try to make demanded megawatts and would not switch to track until after turbine tripped. Control after reactor trip is unchanged.	No	NA
Turbine bypass valve closed	Closed	Normally at power, all turbine bypass valves are closed, so if closed indication failed close it would have no effect. Control after reactor trip will be pressure regulated by main steam safety valves and atmospheric dump valves.	No	NA
	Open	It could also fail to indicate open and may not be detected immediately. Control after reactor trip is unchanged.	Unlikely	NA
ESDD (evaporator steam demand development signal)	40% of full power demand (high)	At 100% power, power plant is put into oscillations between high power and runback of electric load. Valves to evaporators do not open. The same at 30% power, but ULD walks up to 100% before oscillations start. No reactor trip is expected, but if oscillations continue, a low RC pressure trip is possible. Control after reactor trip is unchanged. (A high failure of ESDD is unlikely.)	Unlikely	NA
	20% of full power demand (midscale)	At 100% power, the effect is same as a high failure; but at low power, ICS levels out to 30% plus 20% or about 50% power level. No reactor trip except as before a possible low RC pressure trip. Control after reactor trip is unchanged.	Unlikely	NA
	0% of full power demand (low)	No effect because initially at 0% demand for ESDD.	No	NA

Table 3. Plant Response to Failures of Single ICS Outputs

Signals	Fails	Effect	Reactor trip	Transient bounded by
Increase turbine position	Max increase (high)	Causes turbine valve to open at approximately 10%/minute, decreasing steam pressure and increasing MWe. When a 50 psi pressure error exists for 5 seconds, turbine will transfer to manual and valve opening will stop. ICS will go into track and stabilize after a 5% load increase. A trip is unlikely. Control after a reactor trip is not changed by this failure.	Not expected	NA
Decrease turbine position	Max decrease (high)	Performance similar to an increase failure except pressure increases and load decreases approximately 5% (decrease rate is faster than increase rate) before the NSS stabilizes.	Not expected	NA
Turbine position	As is (midscale)	Will hold turbine valves to their last position. Plant cannot be maneuvered. No turbine trip expected.	No	NA
Turbine A and B bypass valves, atm "A" and "B" exhaust valves	100% (high)	If any one of these valves is driven open, it is not a significant problem unless reactor trips. If this happens, secondary steam pressure cannot be controlled to ≥1000 psig, primary overcools, and pressurizer level may be lost. Bypass or exhaust block valve can be closed to maintain pressure.	Possible at high load	FSAR 15.1.4, "Inadvertent Opening of Steam Generator Atmospheric Dump or Safety Valve" or FSAR 15.1.3, "Steam Pressure Regulator Malfunction or Failure Resulting in Increasing Steam Flow"
	0% (low)	If any one (or more) of these valves fails to open on demand, it is no problem because the steam line safety valves are available for secondary steam pressure control after reactor trip.	Not expected	NA
	50% (midscale)	If any one of these valves fail open, a similar result to the 100% fail open could result.	Possible at high load but not as probable as 100% case.	FSAR 15.1.4 or FSAR 15.1.3
Allow start of any RC pump	Yes/no	Failure can either prevent pumps from being started when they should or it can allow them to be started when they should not.	Not expected	NA
To CRD to permit rod withdrawal (runback limit)	Inhibit	No impact unless a power condition runback is present in CRD. If this occurs, rods cannot be withdrawn. The result is T_{ave} may drop low causing RC pressure to decrease.	Not expected	NA
	Not inhibit	This would allow rods to be withdrawn when an inhibit should exist.	Not expected	NA
Transfer turbine control to manual	Transfer requested	No effect except turbine goes to manual. ICS tracks generated MW, which is constant after transfer. No change to control after reactor trip.	Not expected	NA
	No transfer	Turbine will not transfer automatically to manual when demanded. If a subsequent upset did require turbine to transfer to manual, such as an increase or decrease turbine position failure, event would be terminated by a reactor trip. A double fault is required to cause a reactor trip. Control after trip is not affected.	Not expected	NA
SG-B on Btu limit SG-A on Btu limit		No effect on NSS. These outputs for operator information only.		

Table 3. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
SG-B on low level SG-A on low level FW limited by reactor Reactor limited by FW Neutron error	Yes/no	No effect on MSS. These outputs for operator information only.		
Withdraw control rods (two outputs)	Withdraw when not desired	No effect. The contacts for withdrawal are in series, therefore, two sets of contacts would have to fail before withdrawal would occur.	Not expected	NA
	Does not withdraw when withdrawal desired	Rods fail to respond to a withdrawal signal. Results in T_{ave} droop and possible RC pressure upsets.	Not expected	NA
Insert control rods (two outputs)	Insert when not desired	The two sets of contacts are in parallel, therefore, a failure will cause rod insertion. T_{ave} will decrease causing RC pressure upsets.	Not expected	NA
	Does not insert when desired	No impact since both contacts must fail to prevent rod insertion.	Not expected	NA
Loop B open main FW block valve	Open when opening not desired	Block valve is only closed at low loads when SGs are on level control. Will not interfere with effective SG level control unless leakage across main FW control valve is large. Could impact accuracy of FW flow measurement, but this is not needed for control.	Not expected	NA
	Not open when desired	Will prevent automatic opening of the main FW block valve during startup. Control after reactor trip not changed.	Not expected	NA
Loop A open main FW block valve		Same as loop B open main FW block valve.		
Loop B close main FW block valve	Close when closing not desired	Partial loss of FW to one SG, with reactor trip following soon after (high RC pressure). Control after reactor trip not changed.	Yes (high RC pressure)	FSAR 15.2.7
	Not closed when closing desired	Block valve will not close automatically when it should. However, this would not interfere with effective SG level control unless leakage across main FW control valve were large.	Not expected	NA
Loop A close main FW block valve		Same as loop B main FW block valve.		
Power to ICS exists (auto inhibit)	No	Transfers Diamond CRD to manual or does not let operator go to automatic.	Not expected	NA
	Yes	Auto inhibit not active.	Not expected	NA
Large neutron error does not exist (auto permit)	Large error	Does not let operator go to automatic with Diamond CRD.	Not expected	NA
	Not large error	Operator can transfer Diamond CRD to automatic when a large error exists.	Not expected	NA
FW pump B speed changer demand	High	Putting one feed pump on high speed stop would increase FW flow to both SGs. The effect would be partially or totally offset by an automatic speed decrease of unaffected pump. Reactor does not trip because FW valves automatically close to maintain FW flow at setpoint. No change to control after reactor trip.	Not expected	NA

Table 3. (Cont'd)

Signals	Fails	Effect	Reactor trip	Transient bounded by
	Low	Causes decrease of feed flow to both SGs. Unaffected pump speeds up and FW control valves open to partially or totally offset loss in flow. Reactor trip on high pressure likely due to undercooling. No change to control after reactor trip.	Yes, if total FW flow is less than can be accommodated by one MFW pump.	FSAR 15.2.7
	Midscale	With one pump on midscale speed at high power, other pump will pick up to maintain FW to SGs and FW valves will open to maintain flow to SG also. Once FW flow to SG and pressure drop across pumps is stabilized, a reactor trip is not probable unless at high power initially and FW flow demand to SG has not bee satisfied. Therefore, an undercooling event of SGs would occur and a high RC pressure trip is probable. No change after reactor trip. At low power levels only one FW pump is operating. One FW pump at midscale speed would require adjustment by both MFW control valves and reactor would not trip on low RC pressure.	Probable (at very high loads)	FSAR 15.2.7
FW pump A speed changer demand		Same as pump B FW speed changer demand.		
Loop B main FW valve	Closed (low)	At high power level, partial loss of FW flow to one SG with reactor trip on high pressure following shortly after valve closes. At low power, SU valve may be sufficient. No change to control after reactor trip.	Probable (high RC pressure)	FSAR 15.2.7
	Open (high)	Effect at full load is not great because feed valve is nearly open. If failure initiates at lower load, flow to one SG goes to above 100%. ICS reduces feed flow to other SG and partially compensates for extra feed flow in other SG. As extra feed flow cools the primary, control rods pull to try to bring T_{ave} back to setpoint. System may reach steady state at a higher load condition without reactor trip. This failure may cause reactor trip on low RC pressure if initiated from a very low power. No change to control after reactor trip.	Not expected	NA
	Half open (midscale)	Partial loss of FW to one SG [illegible] valve position is closing with respect to its last position before failure; otherwise, it will be an overfeed condition for the converse case. For an overfeed condition, pumps will speed up to maintain pressure drop across valve; rods will pull to maintain T_{ave} as long as cross limits are not initiated or Btu and high level limits are not exceeded causing a reactor trip. No change to control after reactor trip. For a partial loss of FW an undercooling of primary side is initiated with a high RC pressure reactor trip. No change to control after reactor trip.	Probable (high RC pressure)	FSAR 15.2.7
Loop A main FW valve		Same as for loop B main FW valve.		
Loop B startup FW valve	Open (high)	No effect if operating at power (i.e., SU valve is already open). If a SU valve remained open after reactor trip (or came open at very low power) one SG would be overfilled, resulting in excessive cooldown of the primary and possible loss of pressurizer level. Startup block valve can be closed and flow controlled using main valve.	Not expected	NA
	Closed (low)	When SU valve closes to 50%, main FW block valve is shut causing total loss of FW flow to one SG. Reactor trip on high pressure follows. Main block valve can be opened and affected SG fed with main FW valve.	Yes (high RC pressure)	FSAR 15.2.7
	Half open (midscale)	The same as a closed SU valve failure since midscale is 50% closed on SU valve, but a total loss of FW will not occur since valve remains half open. Reactor will still trip on high RC pressure. Main block valve can be opened and affected SG fed with main FW valve.	Yes (high RC pressure)	FSAR 15.2.7
Loop A startup FW valve		Same as for loop B startup FW valve.		

Table 3. (Cont'd)

Signal	Fails	Effect	Reactor trip	Transient bounded by
Total FW flow, loop A				
Total FW flow, loop B				
Unit load control panel indicating lights				
Unit load demand set				
RC flow runback in effect				
High load limit in effect				
Low load limit in effect		No effect on NSS. These outputs for operator information only.		
Loss of FW pump runback in effect				
Asymmetric rod runback in effect				
Loss of RC pump runback in effect				
Unit master in tracking				

Table 4. Assumed Hand Switch Positions

Parameter	Signals input to switch	Hand switch	Position selected
RC flow, loop A			
(X)	FT-1A5	FC-HS1A	X
(Y)	FT-1A6		
RC flow, loop B			
(X)	FT-1B5	RC-HS1B	
(Y)	FT-1B6		X
T_h, loop A			
(X)	TT-3A1	RC-HS3A	X
(Y)	TT-3A2		
T_h, loop B			
(X)	TT-3B1	RC-HS3B	
(Y)	TT-3B2		X
T_c, loop A			
(X)	TT-4A1	RC-HS4A1	
(Y)	TT-4A3		
Average	RC-TY4A		X
T_c, loop B			
(X)	TT-4B1	RC-H24B1	
(Y)	TT-4B3		
Average	RC-TY4B		X
T_h, loop A	RC-HS3A	RC-HS3	
loop B	RC-HS3B		
Average T_h	RC-TY3		X
T_{ave}, loop A	RC-TY7A	RC-HIS7	
loop B	RC-TY7B		
T_{ave}, both loops	RC-TY7		X
Pressurizer level			
(X)	LT-14-1	RC-HS14	X
(X)	LT-14-2		
(Y)	LT-14-3		
Pressurizer temperature			
(X)	TT-15-1	RC-HS15	X
(Y)	TT-15-2		
T_c loop A wide range			
(X)	TT-4A2	RC-HS4A2	X
(Y)	TT-4A4		

Table 4. (Cont'd)

Parameter	Signals input to switch	Hand switch	Position selected
T_c loop B wide range			
(X)	TT-4B2	RC-HS4B2	
(Y)	TT-4B4		X
Pressurizer pressure narrow range			
(X)	PT-2-1	RC-HS2-1	X
(Y)	PT-2-3		
Pressurizer pressure wide range			
(X)	PT-2-2	RC-HS2-2	
(Y)	PT-2-4		X
Main FW temp., loop A			
(X)	TT-1A1	SP-HS1A	X
(Y)	TT-1A2		
Temp. comp. MFW flow, loop A (X)	SP-FY2A1	SP-HS2A	X
MFW flow, loop A			
(X)	FT-2A1		
(Y)	FT-2A2		
Temp. comp. MFW flow, loop A (Y)	SP-FY2A2		
Main FW temp., loop B			
(X)	TT-1B1	SP-HS1B	
(Y)	TT-1B2		X
Temp. comp. MFW flow, loop B (X)	SP-FY2B1	SP-HS2B	
MFW flow, loop B			
(X)	FT-2B1		
(Y)	FT-2B2		
Temp. comp. MFW flow, loop B (Y)	SP-FY2B2		X
Main steam press., loop A			
(X)	PT-12A1	SP-HS12B	X
(Y)	PT-12A2		
Main steam press., loop B			
(Y)	PT-12B1		X
(X)	PT-12B2		

Table 4. (Cont'd)

Parameter	Signals input to switch	Hand switch	Position selected
Turbine header (throttle) pressure			
(X)	PT-16A	SP-HS16	X
(Y)	PT-16B		
MFW control valve ΔP, loop A			
(X)	PDT-5A1	SP-HS5A	X
(Y)	PDT-5A2		
MFW control valve ΔP, loop B			
(X)	PDT-5B1	SP-HS5B	
(Y)	PDT-5B2		X
SG startup level, loop A			
(X)	LT-9A3	SP-HS9A2	X
(Y)	LT-9A4		
SG startup level, loop B			
(Y)	LT-9B3	SP-HS9B2	X
(X)	LT-9B4		
SG downcomer temp., loop A			
(X)	TT-8A1	SP-HS8A	X
(Y)	TT-8A2		
SG downcomer temp., loop B			
(X)	TT-8B1	SP-HS8B	
(Y)	TT-8B2		X
Temp. comp. SG operate level, loop A			
(X)	SP-LY9A1	SP-HS9A1	X
(Y)	SP-LY9A2		
Temp. comp. SG operate level, loop B			
(X)	SP-LY9B1	SP-HS9B1	
(Y)	SP-LY9B2		X
Makeup tank level			
(X)	LT-25-1	MU-HS25	X
(Y)	LT-25-2		

Table 5a. ICS Input Signal Failures Due to NNI-X - 24 V dc Power Supply Failure at Full Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop A RC flow, mpph	70.0	40.0
2	Total RC flow, mpph	140.0	80.0
3	Loop A and B T_{hot}, F	600.0	570.0
4	ΔT_c (normal state), F	0.0 (T_{ca}=T_{cb}=556F)	0.0 (T_{ca}=T_{cb}=570F)
5	T_{ave}, F	579.0	570.0
6.	"A" S/U FW flow (no effect at high power), mpph	1.0	0.50
7	"A" FW temperature, F	455	250
8	"A" FW flow, mpph	5.3	3.0
9	"A" steam pressure, psig	910	600
10	Turbine header pressure, psig	885	900
11	"A" FW valve ΔP, psid	35	50
12	"A" S/U level, in.	160	125
13	"A" operate level, %	60	50
14	Non-safety-grade pressurizer heaters	Off	On[a]
15	Pressurizer spray valve	Off	Off[a]
16	Letdown flow control valve	Partially open	Closed[a]
17	Makeup flow control valve	Partially open	Open[a]

(a) For an overheating-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5b. ICS Input Signal Failures Due to NNI-X - 118 V ac Power Supply Failure at Full Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop A RC flow, mpph	70.0	40.0
2	Loop A and B T_{hot}, F	600.0	570.0
3	"A" FW temperature, F	455	250
4	"A" FW flow, mpph	5.3	3.0
5	"A" steam pressure, psig	910	600
6	Turbine header pressure, psig	885	900
7	"A" FW valve ΔP, psid	35	50
8	A" S/U level, in.	160	125
9	"A" operate level, %	60	50
10	Non-safety-grade pressurizer heaters	Off	On[a]
11	Pressurizer spray valve	Off	Off[a]
12	Letdown flow control valve	Partially open	Closed[a]
13	Makeup flow control valve	Partially open	Open[a]

[a]For an overheating-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5c. ICS Input Signal Failures Due to NNI-X - 24 V dc Power Supply Failure at 30% Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop A RC flow, mpph	70.0	40.0
2	Total RC flow, mpph	140.0	80.0
3	Loop A and B T_{hot}, F	586.0	570.0
4	ΔT_c (normal state), F	0.0 (T_{ca}=T_{cb}=581F)	0.0 (T_{ca}=T_{cb}=570F)
5	T_{ave}, F	579.0	570.0
6	"A" S/U FW flow (no effect at this low power), mpph	1.0	0.50
7	"A" FW temperature, F	330	250
8	"A" FW flow, mpph	1.5	3.0
9	"A" steam pressure, psig	890	600
10	Turbine header pressure, psig	885	900
11	"A" FW valve ΔP, psid	35	50
12	"A" S/U level, in.	40	125
13	"A" operate level, %	10	50
14	Non-safety-grade pressurizer heaters	Off	On[a]
15	Pressurizer spray valve	Off	Off[a]
16	Letdown flow control valve	Partially open	Closed[a]
17	Makeup flow control valve	Partially open	Open[a]

[a]For an overheating-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5d. ICS Input Signal Failures Due to NNI-X – 118 V ac Power Supply Failure at 30% Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop A RC flow, mpph	70.0	40.0
2	Loop A and B T_{hot}, F	586.0	570.0
3	"A" FW temperature, F	330	250
4	"A" MFW flow, mpph	1.5	3.0
5	"A" steam pressure, psig	890	600
6	Turbine header pressure, psig	885	900
7	"A" FW value ΔP, psid	35	50
8	"A" S/U level, in.	40	125
9	"A" operate level, %	10	50
10	Non-safety-grade pressurizer heaters	Off	Off[(a)]
11	Pressurizer spray valve	Off	On[(a)]
12	Letdown flow control valve	Partially open	Open[(a)]
13	Makeup flow control valve	Partially open	Closed[(a)]

(a)For an overheating-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5e. ICS Input Signal Failures Due to NNI-Y – 24 V dc Power Supply Failure at Full Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop B RC flow, mpph	70.0	40.0
2	ΔT_c (normal state), F	0.0 (T_{ca}=T_{cb}=556F)	14 (T_{cb}=570F)
3	"B" S/U FW flow (no effect at high power), mpph	1.0	0.50
4	"B" FW temperature, F	455	250
5	"B" MFW flow, mpph	5.3	3.0
6	"B" steam pressure, Psig	910	600
7	"B" FW valve ΔP, psid	35	50
8	"B" S/U level, in.	160	125
9	"B" operate level, %	60	50
10	Non-safety-grade pressurizer heaters	Off	On[a]
11	Pressurizer spray valve	Off	Off[a]
12	Letdown flow control valve	Partially open	Closed[a]
13	Makeup flow control valve	Partially open	Open[a]

[a]For an overheating-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5f. ICS Input Signal Failures Due to NNI-Y – 118 V ac Power Supply Failure at Full Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop B RC flow, mpph	70.0	[illegible]
2	ΔT_c (normal state), F	0.0 ($T_{ca}=T_{cb}=556F$)	14 ($T_{cb}=570F$)
3	"B" FW temperature, F	455	250
4	"B" MFW flow, mpph	5.3	3.0
5	"B" steam pressure, psig	910	600
6	"B" FW valve ΔP, psid	35	50
7	"B" S/U level, in.	160	125
8	"B" operate level, %	60	50
9	Non-safety-grade pressurizer heaters	Off	On[a]
10	Pressurizer spray valve	Off	Off[a]
11	Letdown flow control valve	Partially open	Closed[a]
12	Makeup flow control valve	Partially open	Open[a]

[a]For an overheating-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5g. ICS Input Signal Failures Due to NNI-Y - 24 V dc Power Supply Failure at 30% Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop B RC flow, mpph	70.0	40.0
2	ΔT_c (normal state), F	0.0 (T_{ca}=T_{cb}=571F)	5 (T_{cb}=566F)
3	"B" S/U FW flow (no effect at high power), mpph	1.0	0.50
4	"B" FW temperature, F	330	250
5	"B" FW flow, mpph	1.5	3.0
6	"B" steam pressure, psig	890	600
7	"B" FW valve ΔP, psid	35	50
8	"B" S/U level, in.	40	125
9	"B" operate level, %	10	50
10	Non-safety-grade pressurizer heaters	Off	Off[a]
11	Pressurizer spray valve	Off	On[a]
12	Letdown flow control valve	Partially open	Open[a]
13	Makeup flow control valve	Partially open	Closed[a]

[a]For an overcooling-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5h. ICS Input Signal Failures Due to NNI-Y - 118 V ac Power Supply Failure at 30% Power

Item	Parameter	Original value (normal)	Midscale value (0 volt)
1	Loop B RC flow, mpph	70.0	40.0
2	T_c (normal state), F	0.0 (T_{ca}=T_{cb}=571F)	5 (T_{cb}=566F)
3	"B" FW temperature, F	330	250
4	"B" FW flow, mpph	1.5	3.0
5	"B" steam pressure, psig	890	600
6	"B" FW valve P, psid	35	50
7	"B" S/U level, in.	40	125
8	"B" operate level, %	10	50
9	Non-safety-grade pressurizer heaters	Off	Off[a]
10	Pressurizer spray valve	Off	On[a]
11	Letdown flow control valve	Partially open	Open[a]
12	Makeup flow control valve	Partially open	Closed[a]

[a]For an overcooling-type transient, the controls for these functions were assumed to fail to the position that would aggravate the trend of the transient regardless of the actual operational mode of these control systems.

Table 5i. Output Signals of the ICS Due to 118 V ac Power Failure at 100% Power Level (and 30% Power Level)

Item	ICS output signal	Original value (normal)	Final value (abnormal)
1	Insert or withdraw rods	In auto	In manual
2	"A" and "B" MFW block valve	Open	Fails as is (open)
3	"Power to ICS exists" signal	Yes	No effect
4	"Large neutron error exists" signal	No	No effect[a]
5	"A" and "B" FW pump speed demand	In auto	(In auto)
6	"A" and "B" MFW control valve position	In auto	~50%
7	"A" and "B" S/U FW control valve position	In auto	~50%
8	Turbine throttle valve position	In auto	In manual
9	"A" and "B" turbine bypass valve position	Closed	50%

[a] With control rods and FW control valves in manual, a large neutron error will have no effect on the plant.

Note: For these transients pressurizer spray, makeup, and heater control actions were in automatic and normal.

Table 5j. Output Signals of the ICS Due to 24 V dc Power Failure at 100% Power Level (and 30% Power Level)

Item	ICS Output Signal	Original value (normal)	Final value (abnormal)
1	Insert or withdraw rods	In auto	In manual
2	"A" and "B" MFW block valve	Open	Closed
3	"Power to ICS exists" signal	Yes	No effect
4	"Large neutron error exists" signal	No	No effect[(a)]
5	"A" and "B" FW pump speed demand	In auto	∿60% (constant)
6	"A" and "B" MFW control valve position	In auto	∿50%
7	"A" and "B" S/U FW control valve position	In auto	∿50%
8	Turbine throttle valve position	In auto	In manual
9	"A" and "B" turbine bypass valve position	Closed	50%

(a) With control rods and FW control valves in manual, a large neutron error will have no effect on the plant.

Note: For these transients pressurizer spray, makeup, and heater control actions were in automatic and normal.

Table 6. Plant Response to NNI/ICS Power Supply Failures

Failure No.	Type of failure	Description of transient	Reactor tripped?	Transient bounded by FSAR analysis
1	Fail NNI-X 24 V dc at 100% power	This rapid overheating transient is caused by both loop A and B Btu limits reducing MFW flow to both OTSGs. The failure of loop A T_{hot} signal caused loops A and B Btu limits to generate a 0 lb/s FW demand signal. RC temperatures increased very rapidly, and the reactor tripped on high RC pressure. Emergency FW flow to both OTSGs maintained the 2-foot low water level, and the high RC temperatures decreased toward normal post-trip values.	Yes	FSAR 15.2.7, "Loss of Main Feedwater"
2	Fail NNI-X 118 V ac at 100% power	This is also a rapid overheating transient. Both loop A and B Btu limits reduced MFW flow to the OTSGs. The rapid reduction in MFW flow was due to loop A T_{hot} signal failing to 570F and causing a 0 lb/s FW demand signal in both loops. This transient is very similar to failure No. 1.	Yes	FSAR 15.2.7
3	Fail NNI-X 24 V dc at 30% power	This is a moderate overheating transient with loop A and B Btu limits reducing MFW flows to both OTSGs. The initial power level was only 30%, and the reactor tripped due to overheating of the RCS. EFW flow started automatically and maintained low water levels in both OTSGs.	Yes	FSAR 15.2.7
4	Fail NNI-X 118 V ac at 30% power	This is an upset transient with mild overheating followed by overcooling. The reactor trip does not occur during overheating of the RCS. Overheating was caused by loop A and B Btu limits reducing FW flows to zero when loop A T_{hot} signal failed to 570F. The turbine bypass valves opening to 50% depressurized both OTSGs and caused the overcooling of the RCS. EFW flow was started by low SG level, and the decreasing OTSG pressure caused an increase in EFW flow rate to the OTSGs. Reactor tripped on low RC pressure.	Yes	FSAR 15.1.2, "Feedwater System Malfunctions That Result in an Increase in Feedwater Flow"
5	Fail NNI-Y 24 V dc at 100% power	This is an overheating transient the trips the reactor on high RC pressure. Each Btu limit is partially reduced, but not to the same value. Initially, loop B FW flow decreased to 0 lb/s, whereas loop A FW flow only decreased momentarily. However, a short time later, loop A and B MFW flows had been reduced to 0 lb/s. During the same time, reactor power decreased before the reactor was tripped.	Yes	FSAR 15.2.7
6	Fail NNI-Y 118 V ac at 100% power	Same transient as above.	Yes	FSAR 15.2.7
7	Fail NNI-Y 24 V dc at 30% power	This is a mild overheating and sustained overcooling transient that would trip the reactor on low RC pressure. T_{ave} increased several degrees F before overcooling was initiated. Loop B Btu limits decreased about 25%, and while the loop B FW flow was dropping rapidly, loop A FW flow increased before dropping to zero. EFW flow restored water levels in both SGs and permitted both SGs to hold normal steam pressure.	Yes	FSAR 15.1.2

Table 5j. Output Signals of the ICS Due to 24 V dc Power Failure at 100% Power Level (and 30% Power Level)

Item	ICS Output Signal	Original value (normal)	Final value (abnormal)
1	Insert or withdraw rods	In auto	In manual
2	"A" and "B" MFW block valve	Open	Closed
3	"Power to ICS exists" signal	Yes	No effect
4	"Large neutron error exists" signal	No	No effect[(a)]
5	"A" and "B" FW pump speed demand	In auto	∿60% (constant)
6	"A" and "B" MFW control valve position	In auto	∿50%
7	"A" and "B" S/U FW control valve position	In auto	∿50%
8	Turbine throttle valve position	In auto	In manual
9	"A" and "B" turbine bypass valve position	Closed	50%

[(a)] With control rods and FW control valves in manual, a large neutron error will have no effect on the plant.

Note: For these transients pressurizer spray, makeup, and heater control actions were in automatic and normal.

Table 6. Plant Response to NNI/ICS Power Supply Failures

Failure No.	Type of failure	Description of transient	Reactor tripped?	Transient bounded by FSAR analysis
1	Fail NNI-X 24 V dc at 100% power	This rapid overheating transient is caused by both loop A and B Btu limits reducing MFW flow to both OTSGs. The failure of loop A T_{hot} signal caused loops A and B Btu limits to generate a 0 lb/s FW demand signal. RC temperatures increased very rapidly, and the reactor tripped on high RC pressure. Emergency FW flow to both OTSGs maintained the 2-foot low water level, and the high RC temperatures decreased toward normal post-trip values.	Yes	FSAR 15.2.7, "Loss of Main Feedwater"
2	Fail NNI-X 118 V ac at 100% power	This is also a rapid overheating transient. Both loop A and B Btu limits reduced MFW flow to the OTSGs. The rapid reduction in MFW flow was due to loop A T_{hot} signal failing to 570F and causing a 0 lb/s FW demand signal in both loops. This transient is very similar to failure No. 1.	Yes	FSAR 15.2.7
3	Fail NNI-X 24 V dc at 30% power	This is a moderate overheating transient with loop A and B Btu limits reducing MFW flows to both OTSGs. The initial power level was only 30%, and the reactor tripped due to overheating of the RCS. EFW flow started automatically and maintained low water levels in both OTSGs.	Yes	FSAR 15.2.7
4	Fail NNI-X 118 V ac at 30% power	This is an upset transient with mild overheating followed by overcooling. The reactor trip does not occur during overheating of the RCS. Overheating was caused by loop A and B Btu limits reducing FW flows to zero when loop A T_{hot} signal failed to 570F. The turbine bypass valves opening to 50% depressurized both OTSGs and caused the overcooling of the RCS. EFW flow was started by low SG level, and the decreasing OTSG pressure caused an increase in EFW flow rate to the OTSGs. Reactor tripped on low RC pressure.	Yes	FSAR 15.1.2, "Feedwater System Malfunctions That Result in an Increase in Feedwater Flow"
5	Fail NNI-Y 24 V dc at 100% power	This is an overheating transient the trips the reactor on high RC pressure. Each Btu limit is partially reduced, but not to the same value. Initially, loop B FW flow decreased to 0 lb/s, whereas loop A FW flow only decreased momentarily. However, a short time later, loop A and B MFW flows had been reduced to 0 lb/s. During the same time, reactor power decreased before the reactor was tripped.	Yes	FSAR 15.2.7
6	Fail NNI-Y 118 V ac at 100% power	Same transient as above.	Yes	FSAR 15.2.7
7	Fail NNI-Y 24 V dc at 30% power	This is a mild overheating and sustained overcooling transient that would trip the reactor on low RC pressure. T_{ave} increased several degrees F before overcooling was initiated. Loop B Btu limits decreased about 25%, and while the loop B FW flow was dropping rapidly, loop A FW flow increased before dropping to zero. EFW flow restored water levels in both SGs and permitted both SGs to hold normal steam pressure.	Yes	FSAR 15.1.2

Table 6. (Cont'd)

Failure No.	Type of failure	Description of transient	Reactor tripped?	Transient bounded by FSAR analysis
8	Fail NNI-Y 118 V ac at 30% power	Same transient as failure No. 7.	Yes	FSAR 15.1.2
9	Fail ICS 118 V ac at 100% power	An overheating transient caused by MFW system closing to 50% capacity leads to a reactor trip on high RC pressure. T_{ave} increased significantly, and RC pressure reached a peak of 2410 psia before post-trip cooling was initiated by the 50% open failure of the turbine bypass valves, which caused steam pressure to vent down to 600 psig.	Yes	FSAR 15.2.7
10	Fail ICS 24 V dc at 100% power	This is an overheating transient with the MFW valves closing to 50% and MFW block valves closing completely. The reactor tripped on high RC pressure. The turbine bypass valves also failed to 50% open, and both SGs vented down to 600 psi.	Yes	FSAR 15.2.7
11	Fail ICS 118 V ac at 30% power	This is a long sustained overcooling transient that will lead to a reactor trip on low RC pressure. The turbine bypass valves failed 50% open and depressurized both OTSGs. The MFW valves opened to 50%, but SG levels dropped to the low level setpoint because the FW pumps were approximately on the low speed stop.	Yes	FSAR 15.1.3, "Steam Pressure Regulation Malfunction or Failure Resulting in Increasing Steam Flow"
12	Fail ICS 24 V dc at 30% power	This transient is similar to No. 11. Turbine bypass valves failed to 50% open and MFW block valves closed. The reactor will trip on low RC pressure.		

Table 7. Common Instrument Line Failures

Failure No.	Signals	Failure	Effects	Reactor tripped?	Transient bounded by
1	PT-2-1, narrow-range pressurizer pressure (X) PT-2-2, wide-range pressurizer pressure (X) LT-14-3, pressurizer level (Y)	Break in low tap fails outputs low	This failure will try to energize all heaters. Assuming that this level was selected, the Pzr level indication fails low so heaters are turned off by low level interlock. Makeup flow will increase and try to "refill" the Pzr. It will actually decrease in pressure and level will fall due to the LOCA effect of the tap break. Reactor could trip on low RC pressure. Control after reactor trip needs operator attention due to tap break.	Possible (low RC pressure)	FSAR 15.6.2, "Break in Instrument Lines or Lines From Primary System That Penetrate Containment"
2	PT-2-3, narrow-range pressurizer pressure (Y) PT-2-4, wide-range pressurizer pressure (Y) LT-14-2, pressurizer level (X)	Break in low tap fails outputs low	Same as above.	Possible (low RC pressure)	FSAR 15.6.2
3	TE-15-1, pressurizer temperature (X) TE-15-2, pressurizer temperature (Y)	Open or short circuit fails outputs low or high	Only one Pzr temperature is used for temperature-compensating the Pzr level ΔP signal. The other thermocouple is not used at all when not selected. Thus, this failure is equivalent to a single input signal failure.	See Table 2	See Table 2
4	LT-9A3, SG startup level, loop A (X) LT-9A1, SG operate level, loop A (X)	Break in high tap fails outputs high	Same as failure of single input signal. Operate level will fail high, and startup level will fail high, but only the operate level high setpoint will take a controlled action and close FW control valves as previously described under operate level measurement failure.	See Table 2	See Table 2
5	LT-9A4, SG startup level, loop A (Y) LT-9A2, SG operate level, loop A (Y)	Same as above	Same as above.	See Table 2	See Table 2
6	Loop B operate and startup level measurements	Same as above	Same as for loop A level measurements.		
7	TE-8A1, SG downcomer temp, loop A (X) TE-8A2, SG downcomer temp, loop A (Y)	Open or short circuit	Same as a single input signal failure since downcomer temperatures have no control system action. Control after reactor trip unchanged.	See Table 2	See Table 2

Table 7. (Cont'd)

Failure No.	Signals	Failure	Effects	Reactor tripped?	Transient bounded by
8	TE-8B1 & TE-8B2, SG downcomer temp, loop B	Open or short circuit	Same as above.	See Table 2	See Table 2
9	TE-1A1, FW temp, loop A (X) TE-1A2, FW temp, loop A (Y)	Open or short circuit	Since only one loop A FW temperature is selected, this failure is equivalent to a single input failure. High and low failures of loop A (or B) FW temperatures are described in Table 2.	See Table 2	See Table 2
10	TE-1B1 & TE-1B2, FW temp, loop B	Open or short circuit	Same as above.	See Table 2	See Table 2
11	TE-4A1, T_c loop A (X) TE-4A2, T_c loop A wide range (X)	Open or short circuit	This failure is equivalent to a single input signal failure since the wide-range T_{cold} is not used for a control system input. Refer to Table 2 for high and low failures of the T_{cold} signal.	See Table 2	See Table 2
12	TE-4B1 & TE-4B2, T_{cold} loop B	Open or short circuit	Same as above.	See Table 2	See Table 2
13	TE-4A3 & TE-4A4, T_{cold} loop A	Open or short circuit	Same as above.		
14	TE-4B3 & TE-4B4, T_{cold} loop B	Open or short circuit	Same as above.		
15	TE-3A1, T_H loop A (X) TE-3A2, T_H loop A (Y)	Open or short circuit	Only one T_{hot} in a loop is used for control. The other is used for display. Thus, this failure is equivalent to a single input signal failure. See Table 2 for both high and low failures of T_{hot}	See Table 2	See Table 2
16	TE-3B1 & TE-3B2, T_H loop B	Open or short circuit	Same as above.	See Table 2	See Table 2

Figure 1. Sources of Sensor Input for the NNI and ICS

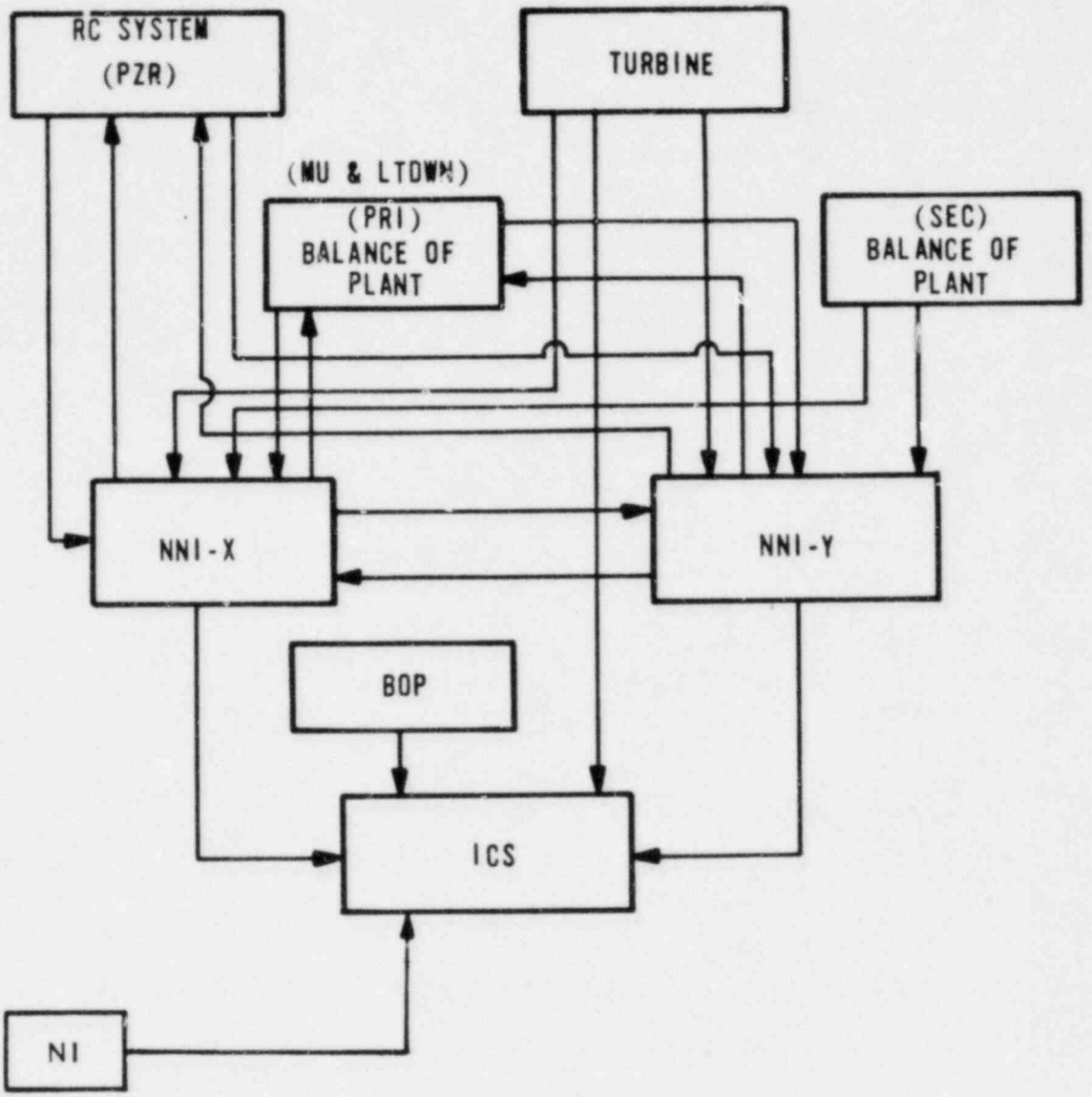


Figure 2. NNI-X Power Distribution System, Schematic Diagram

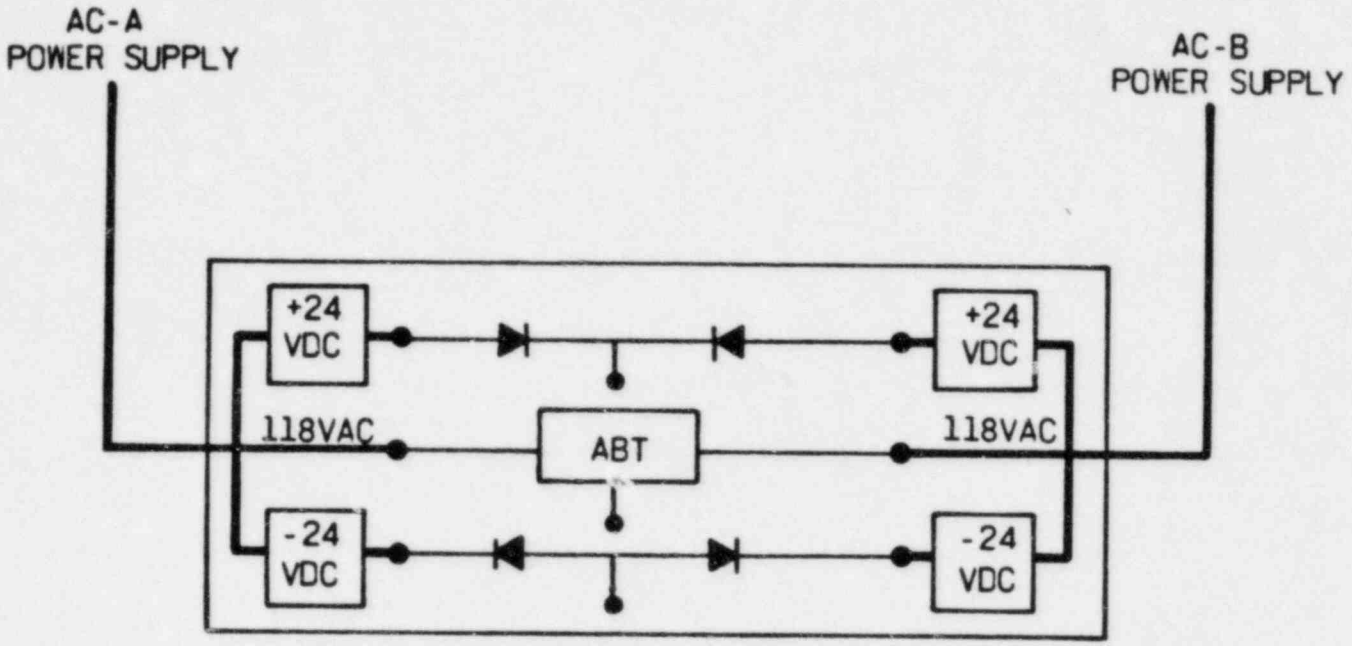
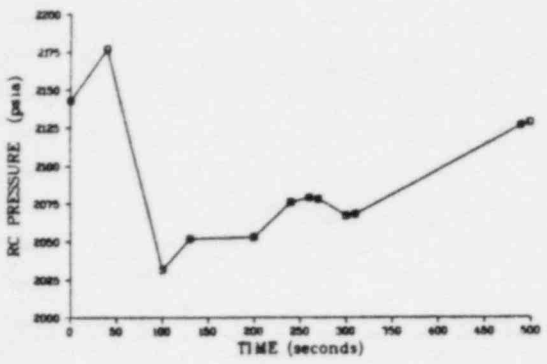
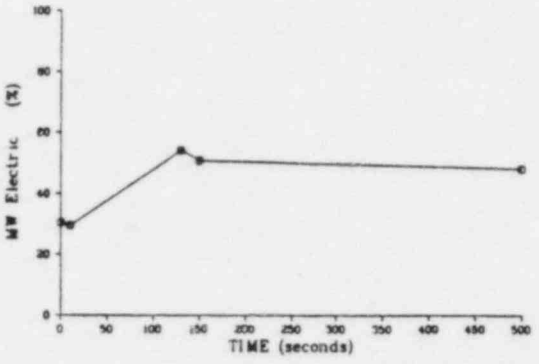
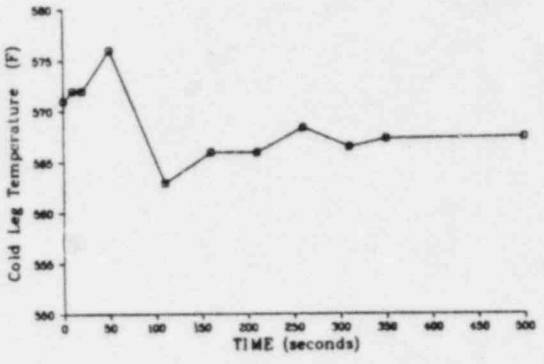
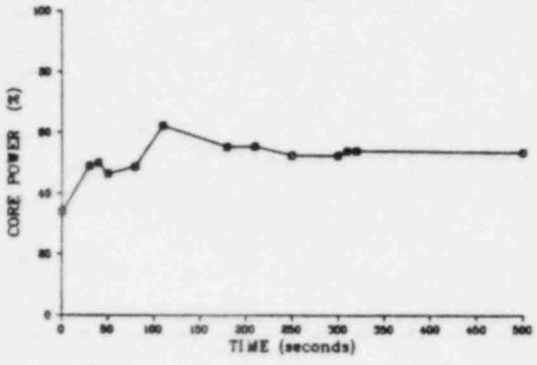


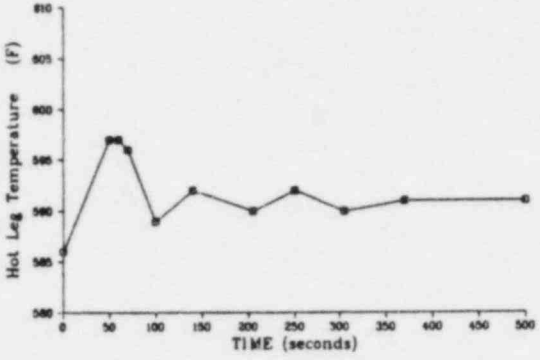
Figure 3. Response to Mid-Scale ESOD Failure at 30% Power

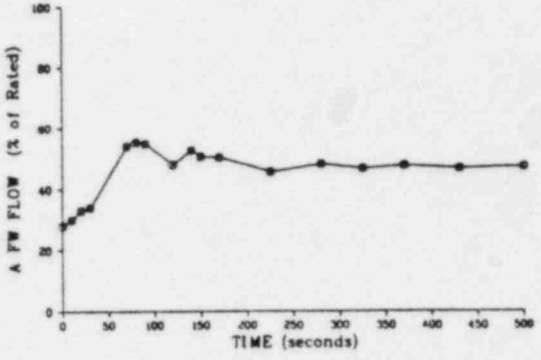


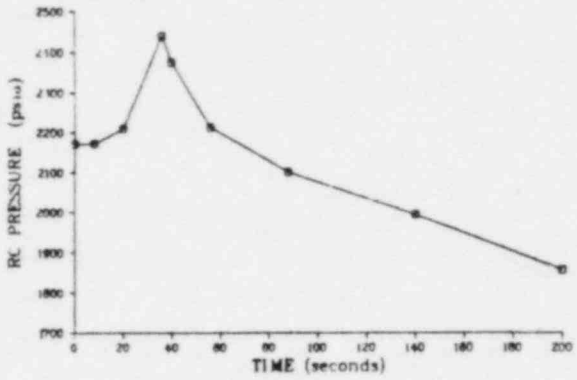


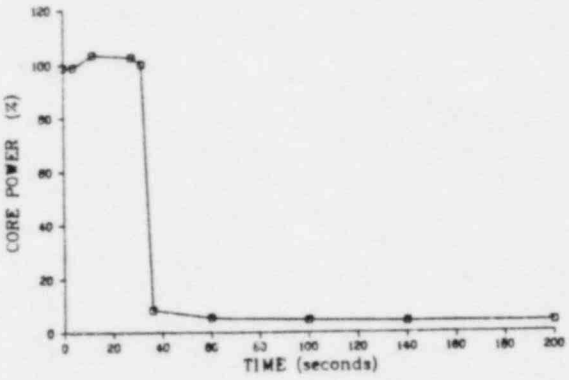


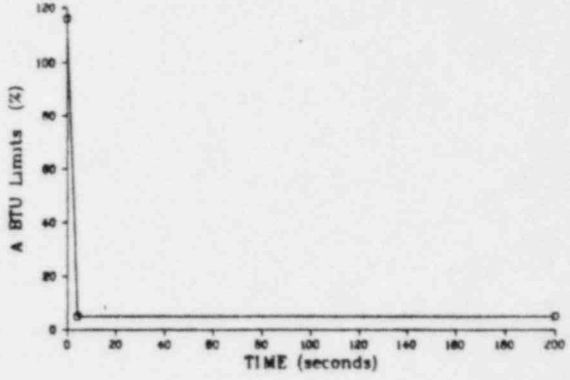


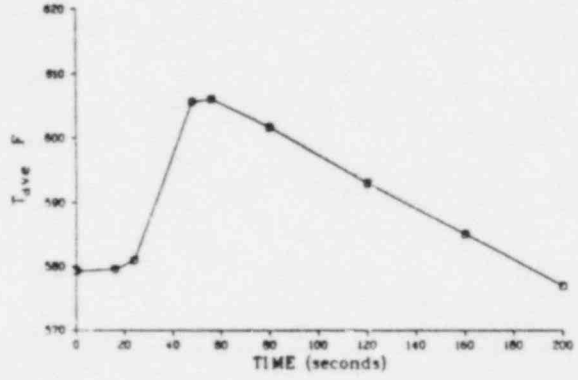


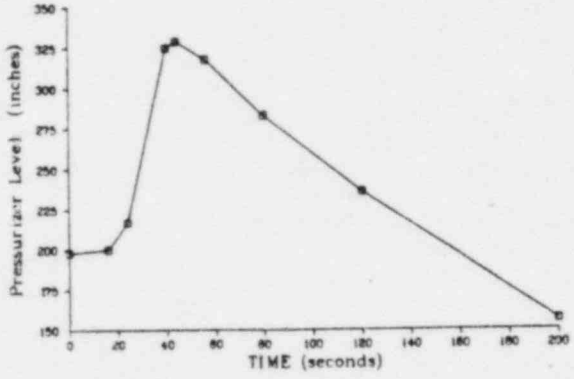












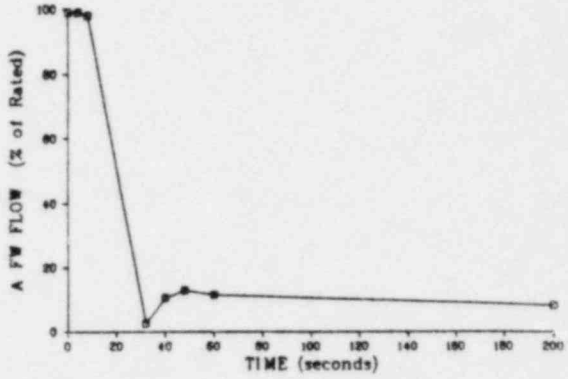


Figure 4. Response to NNI-X 24 V dc Power Supply Failure at 100% Power

Figure 5. Predicted Response to Loss of Loop A RC Flow Input Signal to ICS