WCAP-10272
Supplement 2

EVALUATION OF SURVEILLANCE FREQUENCIES AND OUT OF SERVICE TIMES FOR THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

G. R. Andre
R. C. Howard
R. L. Jansen
K. Leonelli

February, 1986

WESTINGHOUSE ELECTRIC CORPORATION
Nuclear Energy Systems
P. O. Box 355
Pittsburgh, Pennsylvania 15230

8989Q:1D/010886

ACKNOWLEDGEMENTS

The authors would like to thank Ms. N. L. Burns, Mr. K. J. Vavrek, and Mr. T. R. Haag for their contributions in performing the Risk Analysis and Ms. L. M. Matwijec and Ms. C. L. Smith for their contributions in performing the Fault Tree Analysis.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont)

TABLE OF CONTENTS (Cont)

LIST OF FIGURES

LIST OF FIGURES (continued)

LIST OF FIGURES (continued)

LIST OF FIGURES (continued)

LIST OF FIGURES (continued)

LIST OF FIGURES (continued)

LIST OF TABLES

LIST OF TABLES (continued)

1.0 INTRODUCTION

WCAP-10271, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System", and Supplement 1 document a methodology to be used to justify revisions to technical specifications and application of that methodology to the reactor protection system. The methodology consists of the deterministic and numerical evaluation of the effects of particular technical specification changes with consideration given to such things as safety, equipment requirements, human factors and operational impact. The objective of the methodology is to reach a balance in which safety and operability are ensured. The methodology was applied to reactor protection systems for two, three and four loop plants with either relay or solid state logic. The technical specification revisions evaluated were increased test and maintenance times, less frequent surveillance and testing in bypass.

Having evaluated reactor protection system instrumentation it is appropriate to extend the evaluation to engineered safety features instrumentation and actuation relays. This is particularly relevant since portions of the reactor protection system and engineered safety features actuation system are common. Therefore, this supplement documents an evaluation of the impact of increased test and maintenance times, increased surveillance intervals and testing in bypass for the engineered safety features actuation system.

Specifically this report addresses engineered safety features analog channels, logic and actuation relays for two, three and four loop plants with either relay or solid state logic.

The results of the evaluation documented in this report provide a justification for revisions to technical specifications for the engineered safety features actuation system. Proposed revisions to standard technical specifications are included as Appendix A of this report. Though the proposed technical specifications are based on the standard technical specifications, these or equivalent changes and their justifications are applicable to all Westinghouse plants regardless of the type of technical specification in use.

2.0 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM DESCRIPTION AND TESTING

The typical engineered safety features actuation system (ESFAS) consists of analog channels, combinational logic units and actuation relays. A typical analog channel is made up of a sensor, signal conditioning circuits and a comparator, of which the comparator is the output device, providing input to the combinational logic. Any particular protective feature will have either 2, 3 or 4 separate analog channels each providing input to two separate combinational logic trains. Each train of combinational logic will upon detection of 1 of 2, 2 of 3, or 2 of 4 (whichever is appropriate) inputs indicating that the monitored parameter is beyond the setpoint, actuate the actuation relays which cause appropriate plant systems to operate to mitigate design events.

Testing of the ESFAS is typically performed while at power. An overlapping test sequence is used, with each test within the testing scheme adequately testing a portion of the system. Satisfactory completion of all tests provides assurance that the system will perform as designed when a demand is placed upon it. Typical ESFAS testing involves verification of proper channel response to known inputs, proper comparator (bistable) settings and proper operation of the combinational logic and actuation relays.

This section of this report provides an overview of the ESFAS and system testing. Both solid state and relay logic designs are discussed. More detail can be obtained from the referenced documents.

2.1 SYSTEM DESCRIPTION

The evaluation documented in this report is largely based on a fault tree analysis. Fault trees are derived from hardware configurations which they model. Some knowledge of the design of the ESFAS then is necessary to understand the fault tree analysis. This section of this report provides an introduction to the design of the ESFAS. More detailed discussions can be found in documents referenced in Section 6.0 of this report.

2.1.1 ANALOG CHANNEL DESCRIPTION

The analog channels comprise the input portion of the ESFAS. A typical analog channel consists of: a sensor, loop power supplies, signal conditioning circuits and signal comparators. Separation of the redundant analog channels originates at the process sensors and continues through the field wiring and containment penetrations to the protection racks. At the protection racks, the components of the four channels are located in separate panels. Furthermore, power for each channel is supplied from separate buses. The major components are briefly described below.

1. The sensor measures physical parameters such as temperature, pressure, level or flow. The measurement is converted to an electrical signal and transmitted to the protection racks. The normal signal is a milliampere current proportional to the parameter being measured.

2. The loop power supply performs the following functions depending upon the specific hardware installed:

   a. It provides a constant voltage to the sensor/transmitter. This allows the sensor/transmitter to vary current flow in proportion to the magnitude of the monitored parameter.

   b. For more recent plant designs, the loop power supply converts the transmitter loop current to a proportional voltage signal which is supplied to the remainder of the circuit. The loop power supply provides isolated and non-isolated signals to control and indication functions and protective functions respectively. Early plant designs utilize a current loop with no conversion to a voltage signal.

3. The signal conditioning modules perform a number of functions such as amplification, square root derivation, lead/lag compensation, integration, summation, and isolation.

4. A signal comparator is usually a bistable device. The bistable compares the incoming signal to a predetermined setpoint and turns its output off or on if the input voltage exceeds the setpoint. Note that the setpoint can be exceeded in either direction to provide high and low alarms and trips. Each bistable will control two separate relays, one associated with logic train A and one associated with logic train B. The output relays may be either AC or DC powered, low voltage (~ 25) or high voltage (~ 120) depending on the plant specific application. The output relays operate contacts in the combinational logic which will actuate the actuation relays upon the appropriate input conditions.

Figure 2-1 shows a typical analog channel for recent plant designs. Figure 2-2 shows a typical analog channel for early plant designs. Additional details are available in documents referenced in Section 6.0.

2.1.2 SOLID STATE AND RELAY LOGIC DESCRIPTION

The solid state logic cabinet, or Solid State Protection System (SSPS), is a dual train redundant protection system receiving inputs from the analog channels. The interface between the analog channels and the SSPS is accomplished using relays in either an energized or deenergized state, as determined by the output of the comparators. The relays operate grounding contacts in the SSPS circuitry. When a comparator senses a trip condition the corresponding input relay will energize or deenergize as appropriate, applying a ground to a specific logic input. The logic inputs are applied to universal boards which are the basic circuits of the protection system. They contain 1 of 2, 2 of 3, 2 of 4, etc. logic circuits. Grounding of the appropriate number of universal board inputs will cause a trip signal to be generated.

16308-1

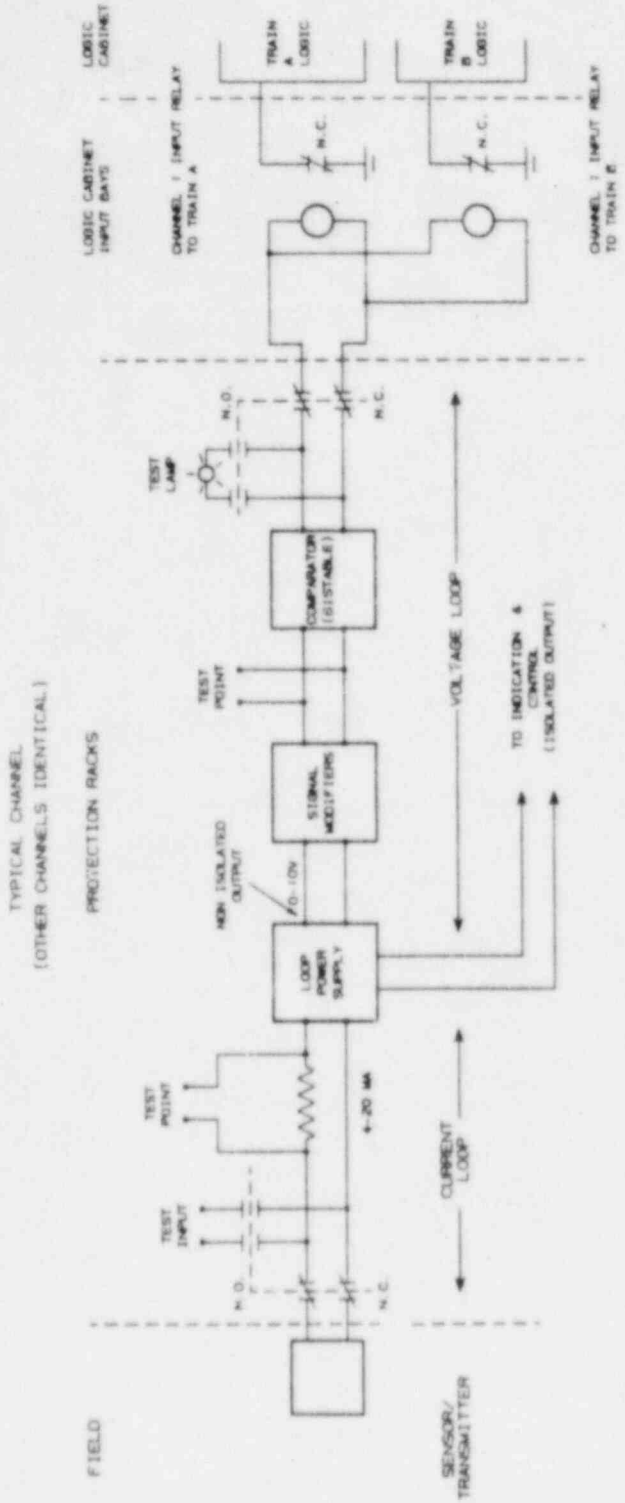


Figure 2-1. Solid State Protection System Analog Channel

16308-2

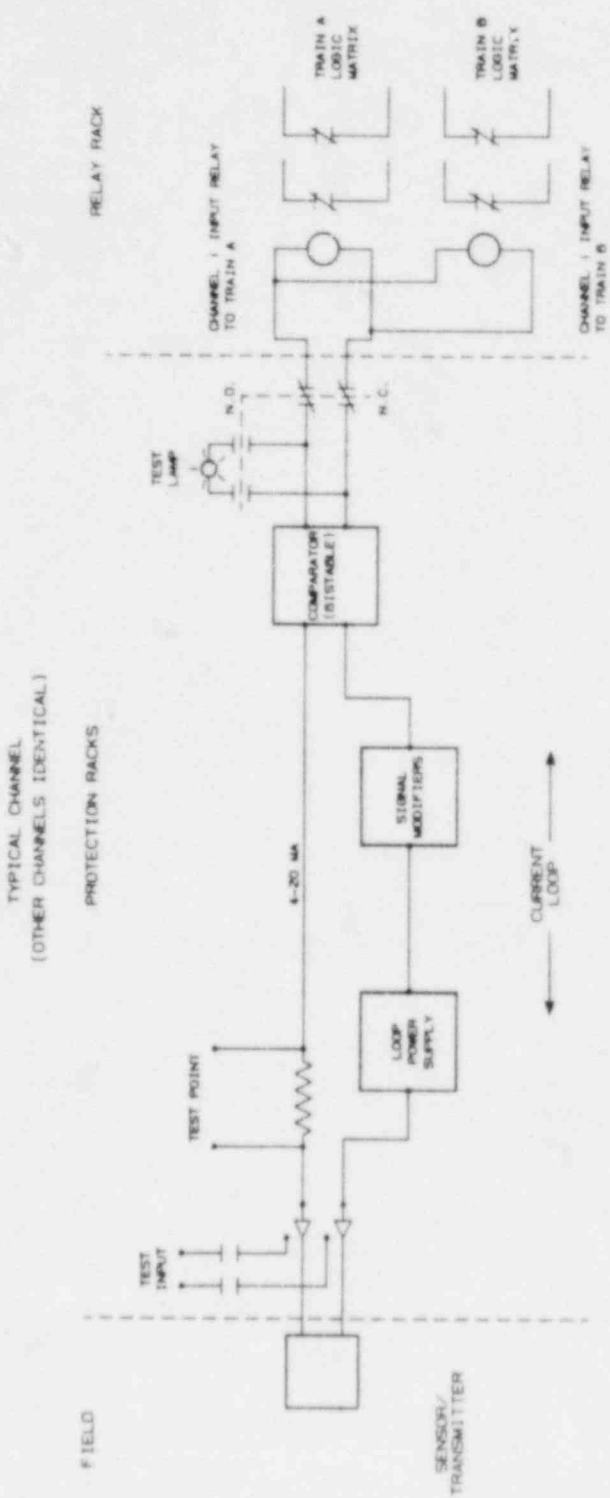


Figure 2-2. Relay Protection System Analog Channel

Outputs of the universal boards are connected to either other universal boards, undervoltage output boards or safeguard output boards. Connection to other universal boards allow additional logic combinations. For example, auxiliary feedwater may be started by low level in one steam generator as sensed by 2 of 3 channels. Each of the three steam generator level channels for one steam generator would input into a 2 of 3 universal board. For a three loop plant there would be 3 such circuits. The output of each of these universal boards would input into a 1 of 3 universal board to achieve the desired logic. Undervoltage output boards drive the undervoltage relays to trip the reactor trip breakers. Evaluation of reactor trip is documented in WCAP-10271 and Supplement 1. The safeguards output boards drive master relays. Upon deenergization of the input the safeguards output board will create a current path causing the master relays to energize. The master relay when energized closes contacts in slave relay circuits which in turn energize and operate contacts in motor starters, solenoid circuits, etc., to energize safeguards equipment.

The relay logic consists of contacts in series-parallel arrangements which energize a master relay when the appropriate combinations of contacts are closed, or deenergize a master relay when the appropriate combination of contacts are open, depending on the function. The series-parallel contacts are operated by the output relays of the analog channels. The series-parallel contacts are arranged to initiate the appropriate protective function when the required number of analog channels, eg. 1 of 2, 2 of 3, 2 of 4, sense an out of limit condition. The master relays in turn operate contacts to energize slave relays which operate contacts in motor starters, solenoid circuits, etc., to energize safeguards equipment.

Figure 2-3 shows a typical block diagram of SSPS.

Figure 2-4 shows a typical relay logic circuit diagram. Additional details are available in documents referenced in Section 6.0.

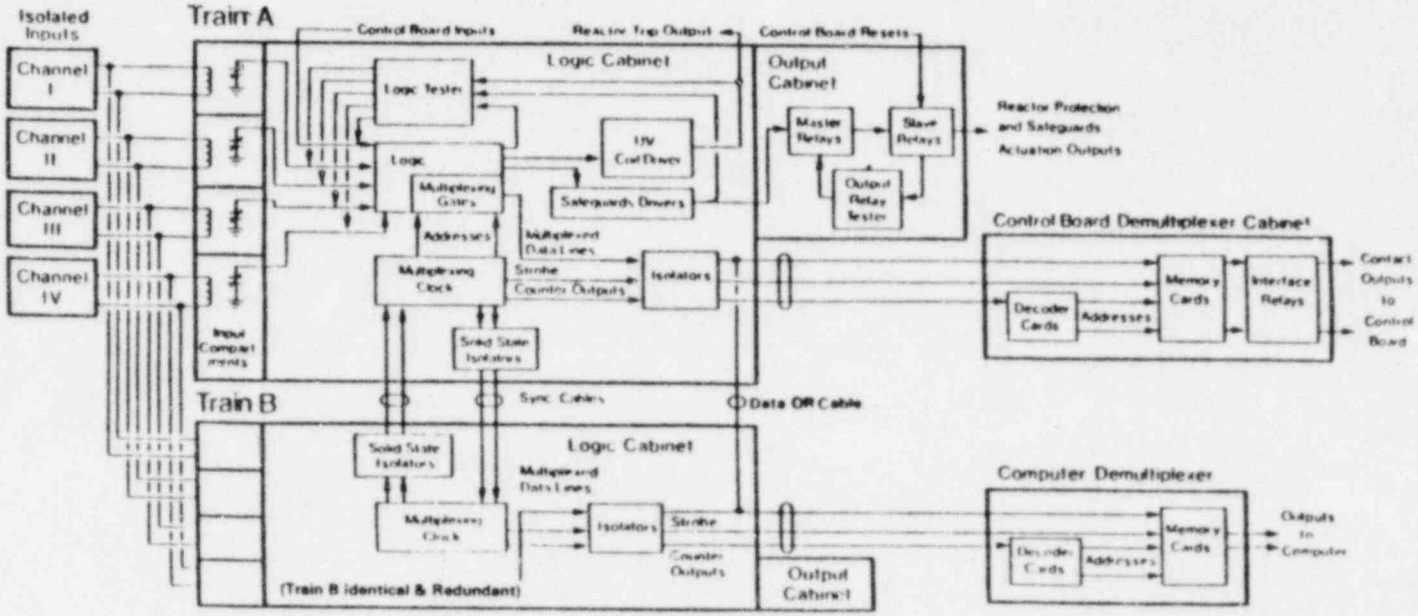


Figure 2-3. Solid State Protection System Block Diagram

16308-3

a,c

Figure 2-4. Relay Protection System Logic Circuit Diagram

2.1.3 ACTUATION RELAYS DESCRIPTION

The actuation relays function to start the safeguards equipment which is used to mitigate events. This is accomplished by a combination of relay operations initiated by the output of the logic circuit. As described above, for the SSPS, the safeguards output board is actuated upon removal of the input signal from the universal board logic. Deenergization of the input causes a transistor to trigger energizing a master relay. Each master relay energized in this fashion closes contacts which energize one or more slave relays. The number of master and slave relays energized is dependent upon the particular protective function. The more complex the function, the greater the number of relays energized. Each slave relay when energized closes contacts in the actuation circuits for one or more pieces of equipment. Typically each slave relay causes several components to operate.

The design of the actuation relays for the relay logic is similar in concept to that of the SSPS. The logic circuit contacts close energizing one, or more, master relay when the correct combination of analog channels sense the monitored parameter outside of limits. The master relays thus energized, close contacts energizing slave relays. As is the case with SSPS, the number of relays energized is dependent upon the particular protective function. The more complex function requires more relays. Each slave relay when energized closes contacts in the actuation circuits of one or more pieces of equipment. Typically, each slave relay causes several components to operate.

The actuation relays for both the SSPS and relay logic are train oriented. Train A logic energizes train A relays which energize train A equipment. Typically operation of either train is sufficient for mitigation purposes.

Figures 2-5 and 2-6 show typical circuit diagrams for SSPS and relay logic actuation relays respectively. Additional information may be obtained from references identified in Section 6.0.

16308-4

a,c

Figure 2-5. Solid State Protection System Actuation Relay Circuit Diagram

a,c

16308-5

Figure 2-6. Relay Protection System Actuation Relay Circuit Diagram

2.2 TESTING

Testing of the ESFAS is included in the fault tree model to allow an evaluation of test intervals and outage times. Testing of ESFAS components effects the availability of the ESFAS depending upon the component being tested. This section of this report provides an introduction to typical testing practices as an aid in understanding the fault tree model. Additional information may be obtained from the documents referenced in Section 6.0 and from plant technical manuals and test procedures.

2.2.1 ANALOG CHANNEL TESTING

Analog tests are performed to verify that the analog channel is functioning properly and that bistable settings in the signal comparator are at the desired setpoint. Analog channel testing has two levels of complexity, channel calibrations and channel functional tests. Calibrations include verification of proper operation of the sensor and the electronics. Although channel calibrations ensure proper channel operation they are typically performed with the plant shutdown and hence do not affect channel unavailability. For this reason channel calibrations are not included in the fault tree model. Channel functional tests are performed more frequently and typically at power. The functional test verifies proper operation of the entire analog channel excluding the sensor. Functional testing at power does impact ESFAS unavailability and hence is included in the fault tree model. Functional testing of ESFAS channels may be performed in either a trip or bypass mode depending on the function and/or circuit design. Each method is discussed. The following discussion of analog channel testing refers only to functional testing. Analog testing is performed as follows:

1. Channel test capability is typically provided in the process racks for each process channel. Test capability includes test jacks for inserting a test signal into the circuit, test connections to various locations in the circuit to verify performance, lamps or light emitting diodes (LED) for status indication, and switches and relays to align the system for the test to be performed.

2. The test switch for the function to be tested is put in the test position. This aligns the channel input to the test jacks. This or another similar switch realigns the bistable output for the function to be tested from the logic input relays to an indicator test lamp. The sensor/transmitter is disconnected and the circuit is now capable of receiving a test signal through the test jacks. For circuits tested in the trip condition with the bistable output disconnected from the logic input relays, the protection system receives a single channel actuation signal. Therefore, while analog testing in the trip condition only one additional signal is needed from the remaining redundant channels to activate ESFAS. For channels tested in the bypass condition the logic input relays receive a no-trip condition. Operation of a single additional channel therefore is not sufficient to cause an ESF actuation (unless a 1 of 2 logic is utilized). For either trip or bypass testing the input signal to the test jacks is adjusted and measurement made to ensure the channel and bistable performed as required. The bistable is adjustable by use of the indicator test lamp. Further verification is gained from the control board alarms and indications which remain in the circuit. When the test switches are restored to the normal position, the sensor/transmitter supplies its input to the circuit and the bistable output is realigned to the protection system logic.

Figure 2-1 and 2-2 include typical test circuits. Additional information may be obtained from documents referenced in Section 6.0.

2.2.2 SOLID STATE AND RELAY LOGIC TESTING

The SSPS can be tested either at power or during shutdown. Each train is tested separately with the tested train being maintained in the bypassed condition. While one train is in test the other train is capable of providing all protective functions. If an attempt is made to place both trains in test, the reactor will be automatically tripped.

Each train contains an identical semi-automatic test panel with the necessary controls for testing. Pulse testing fast enough to prevent operation of the master relay is used to avoid actuation. During testing of a train, all trips and safeguards actuations from that train are inhibited. In addition, all information transmitted to control board status lamps and annunciators and to the plant computer from the train under test is inhibited to avoid confusion to the operator. To test, the operator needs only to select the function to be tested on a rotary selector switch, press a "start test" pushbutton and wait for indication of the test result. All possible combinations of actuate and non actuate conditions are generated by the test system. Additionally, the logic testing is performed with and without the permissive function to ensure proper operation of ESFAS permissives for those channels affected by permissives.

The semi-automatic tester checks through the solid state logic to the master relay coils. Because some function may already be tripped when the plant is shutdown or when the plant is at power, a switch is provided to disconnect all input relay contacts from the circuit, thereby inhibiting the ability to trip or actuate ESF from one train. Position of this switch is monitored by the alarm system.

Various methods for testing relay logic exist and the method used at a particular plant is dependent upon the relay logic design. The method described here is the one most typical of all Westinghouse plants. The fault tree model for relay logic was based on a combination of the most conservative designs and hence is bounding for all Westinghouse plants with relay logic test capability.

The relay logic is tested by individually operating the logic input relay contacts while blocking master relay operation. The switch which places the analog channel in trip during analog channel testing or an equivalent switch is used to operate the logic input relays. Each logic combination, i.e., 1 of 2, 2 of 3, 2 of 4, which should result in ESF actuation is made up and verified by observation of a proving lamp or proper voltage indication. ESF actuation in the train being tested is prevented by blocking the master relays. Only one train of ESFAS is tested at a time, hence the remaining train is capable of performing all protective functions.

Figures 2-3 and 2-4 include typical test circuits. Additional information may be obtained in documents referenced in Section 6.0.

2.2.3 ACTUATION RELAYS TESTING

Testing of the actuation relays for plants with SSPS is accomplished by energizing the master and slave relays and verifying proper operation. The master relays are continuity tested as part of the logic test to demonstrate total circuit operation. The master relay test consists of energizing each master relay and verifying proper contact operation. Master relay contact operation is verified by observing continuity through each affected slave relay. The continuity check consists of energizing the slave relay through the master relay contact with a voltage which is insufficient to pick up the slave relay but which demonstrates continuity.

In addition to the continuity check described in the preceeding paragraph, each slave relay is tested individually by energizing the slave relay and verifying proper contact operation. Proper slave relay contact operation is verified in one of two ways. Actuated equipment which may be operated in the mitigation mode is either allowed to actuate or placed in a condition such that proper operation of the slave relay contacts can be verified without actuating the equipment when the slave relay is energized. Actuated equipment which must not be operated in the mitigation mode is prevented from operating by the slave relay test circuit. For these slave relays, proper contact operation is verified by a continuity check of the circuit containing the slave relay contact.

Plant specific designs for relay logic actuation relay test circuits vary. Testing capability covers a range from no designed online test capability to full designed online test capability. The typical plant has designed online master relay test capability but no designed online slave relay test capability. Offline testing does not effect ESFAS availability and hence is not modeled. The fault trees used for this evaluation model online testing since this is the most conservative design considering ESFAS availability and is bounding.

The master relay test consists of energizing the master relay, and verifying proper contact operation. Proper master relay contact operation is verified by performing a continuity check of the master relay contact in the slave relay circuit. The slave relay is prevented from operating by applying a voltage through the master relay contact which is insufficient to pick up the slave relay but which does check continuity.

Slave relay testing for relay logic design is accomplished similarly to slave relay testing for SSPS designs. Each slave relay is energized individually and proper contact operation verified. Proper slave relay contact operation is verified by observing either proper equipment response, proper circuit operation or by continuity.

Only one train of ESF actuation relays is tested at a time. Master relay testing inhibits the entire train. Slave relay testing affects only the relay being tested leaving the remainder of the slave relays unaffected. The opposite train would be functional and capable of providing any protective action required in either case.

Figures 2-5 and 2-6 include typical testing circuits for SSPS and relay logic actuation relays respectively. Additional information may be obtained in the documents referenced in Section 6.0.

3.0 EVALUATION OF IMPACT OF INCREASING SURVEILLANCE INTERVALS AND OUTAGE TIMES ON THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

This section of this report describes the unavailability and risk evaluation performed to assess the impact of increasing surveillance intervals and outage times on the ESFAS. The fault tree methodology described in Section 4.0 of WCAP-10271 was utilized for this evaluation. The discussions contained in Section 4.0 of WCAP-10271 are applicable to this evaluation and therefore are not repeated in this report. In general, only new or additional information pertinent to the ESFAS evaluation is included in this report. The risk evaluation discussed in detail in Section 3.4 is provided since WCAP-10271 does not contain a detailed discussion of risk assessment.

3.1 METHODOLOGY

Two methods were used to evaluate the impact of relaxing the testing and maintenance specifications for the Engineered Safety Features Actuation System (ESFAS). The first applied fault trees and risk analysis. The fault trees were used to model the ESF and determine the unavailability changes of the ESF signals due to the modified technical specifications. The unavailability values were applied in a risk analysis to estimate the effect on core melt frequency and exposure risk. The second method applied a Markovian unavailability analysis. This was used to estimate average reactor downtime and core damage probability for both sets of testing and maintenance conditions. The first method determined a time averaged unavailability for each ESF signal analyzed and applied an overall ESF signal unavailability to estimate core melt frequency and risk. The second method calculated time dependent and time averaged ESF signal unavailability and was used to confirm the results of the first method.

A general objective of this analysis is to determine the sensitivity of plant safety and operability variables (i.e. risk) to the ESF testing and maintenance parameters, thereby, giving guidelines to determine which

parameters may be relaxed. The results presented in the following sections should be viewed on a relative basis, not an absolute basis. If plant safety and operability variables are relatively insensitive to changes in testing and maintenance parameters then a change can be justified. Conversely, if the plant safety and operability variables are highly dependent (sensitive) on certain testing and maintenance parameters, then changes are less justifiable. It is not the intent of this analysis to restrict all plants to identical ESF testing and maintenance conditions, but to demonstrate that plants in general can justify relaxation of several of these ESF parameters.

Table 3.1-1 lists the testing and maintenance practices that were considered. The first case (Base Case) generally corresponds to the current conditions cited in the Standard Technical Specifications or plant specific technical specifications. The base case test intervals for the solid state systems are consistent with the surveillance intervals in STS - Rev. 4. The relay system base case test intervals are typical of several relay plants surveillance test intervals. However, it should be noted that most plants licensed prior to issuance of STS-Rev. 4 perform slave relay testing only during refueling outages. (12 to 18 months). The base case assumption of a these month slave relay test interval was made to be consistent with STS-Rev. 4 and not to be consistent with the typical plant. The second case (Case 1) corresponds to relaxed conditions which are based on past and current hardware performance, actual time required for testing and maintenance, and practical aspects of implementing current testing requirements. Both ESF designs, the relay protection system and the solid state protection system, were evaluated for both cases. The ESF signals and the logic associated with the signals that were evaluated for each design are listed in Tables 3.1-2 and 3.1-3.

Sensitivity studies were also performed on the ESF relay and solid state protection systems. The purpose of these studies was to determine the general response of signal unavailability to alternate testing and maintenance practices. These studies are based on the "Safety Injection on Low Steamline Pressure (2/3) Interlocked with P-12 (2/4)"signal for the relay system and "Safety Injection on Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3)" signal for the solid state system. The testing and maintenance conditions used are listed in Table 3.1-4 and Table 3.1-5 for the relay and solid state systems, respectively. Only the signal unavailability, based on fault tree techniques, was calculated.

TABLE 3.1-1

SURVEILLANCE REQUIREMENTS

COMPONENT	RELAY SYSTEM		SOLID STATE SYSTEM	
	BASE CASE	CASE 1	BASE CASE	CASE 1
Logic Cabinets				
Test interval (month)	1	6	2	6
Test time (hour)	3	8	1.5	4
Maintenance time (hour)	2	12	2	12
Master Relay				
Test interval (month)	1	6	2	6
Test time (hour)	3	8	1.5	4
Maintenance time (hour)	6	12	2	12
Slave Relay				
Test interval (month)	3	18	3	18
Test time (hour)	6	12	4	4
Maintenance time (hour)	6	12	2	12
Analog Channel				
Test interval (month)	1	3	1	3
Test time (hour)	2	4	2	4
Maintenance time (hour)	1	12	1	12

Note: Maintenance interval is one year for all cases.

The fault trees are constructed in accordance with the methods documented in NUREG/CR-2300, "The PRA Procedures Guide" (Ref. 1) and WCAP-10271 (Ref. 4) and Supplement 1. The Westinghouse GRAFTER computer code (Ref. 2) is used to edit and maintain the fault trees on file. The fault trees are quantified by use of the WAMCUT computer code (Ref. 3). WAMCUT performs the required Boolean algebra. Results from WAMCUT are in terms of point estimate probabilities and cutsets for specified events in each fault tree. The event of concern is the top level event; the unavailability of an ESF signal given a particular signal demand. A cutset is a group of elements whose simultaneous failure will cause a failure of the required ESF signal.

The five major contributors to ESF signal unavailability are:

1. Unavailability of components due to random failures.

2. Unavailability of components due to test.

3. Unavailability of components due to unscheduled maintenance.

4. Human error.

5. Common cause failure.

These are discussed in detail in Section 4.1 of WCAP-10271 (Ref. 4).

The Risk and Markov analyses are further discussed in Sections 3.4 and 3.5, respectively.

TABLE 3.1-2

ESF RELAY PROTECTION SYSTEM SIGNALS

SIGNAL		LOGIC	
SAFETY INJECTION			
1.	Pressurizer pressure - low	2/4	2/3
	interlocked with P11	2/3	
2.	Steamline pressure - low	2/4	2/3
	interlocked with P11	2/3	
3.	Steamline pressure - low	2/4	2/3
	interlocked with P12	2/4	2/3
4.	Containment pressure - high	2/3	
5A.	Differential steamline pressure - high	2/3	
5B.	Differential steamline pressure - high	2/3	
	interlocked with P11	2/3	
6.	Steam flow - high	1/2	
	coincident with T_{avg} - low-low	2/4	2/3
	or steamline pressure - low	2/4	2/3
	interlocked with P12	2/4	2/3
STEAMLINE ISOLATION			
1.	Steamline pressure - low	2/4	2/3
	interlocked with P11	2/3	
2.	Steamline pressure - low	2/4	2/3
	interlocked with P12	2/4	2/3

TABLE 3.1-2 (Continued)

ESF RELAY PROTECTION SYSTEM SIGNALS

	SIGNAL		LOGIC
3.	Steam flow - high	1/2	
	coincident with T_{avg} - low-low	2/4	2/3
	or steamline pressure - low	2/4	2/3
4.	Steam flow - high	1/2	
	coincident with T_{avg} - low-low	2/4	2/3
5.	Containment Pressure - high-high	2/3	2/4
6.	Steam flow - high-high	1/2	
	or steam flow - high	1/2	
	coincident with T_{avg} - low-low	2/4	
MAIN FEEDWATER ISOLATION			
1.	Steam generator level - high-high	2/4	2/3
AUXILIARY FEEDWATER PUMP START			
1.	Steam generator level - low-low	2/4	2/3
CONTAINMENT SPRAY AND PHASE B ISOLATION			
1.	Containment pressure - high-high	2/4	
2.	Containment pressure - high-high-high	2/4	

TABLE 3.1-3

ESF SOLID STATE PROTECTION SYSTEM SIGNALS

SIGNAL	LOGIC	
SAFETY INJECTION		
1. Pressurizer pressure - low	2/4	2/3
interlocked with P11	2/3	
2. Steamline pressure - low	2/4	2/3
interlocked with P11	2/3	
3. Steamline pressure - low	2/4	2/3
interlocked with P12	2/4	2/3
4. Containment pressure - high	2/3	
5. Differential steamline pressure - high	1 inst/stmline	
	3 inst/stmline	
6. T_{cold} - low-low	2/3	
coincident with steam pressure - low	2/3	
interlocked with P15	2/4	
7. Steam flow - high	1/2	
coincident with T_{avg} - low-low	2/4	2/3
or steamline pressure - low	2/4	2/3
interlocked with P12	2/4	2/3
STEAMLINE ISOLATION		
1. Steamline pressure - low	2/4	2/3
2. Steamline pressure - low	2/3	
or negative steamline pressure rate - high	2/3	
interlocked with P11	2/3	

TABLE 3.1-3 (Continued)

ESF SOLID STATE PROTECTION SYSTEM SIGNALS

	SIGNAL		LOGIC
3.	Containment pressure - high-high	2/4	2/3
4.	Steam flow - high	1/2	
	coincident with T_{avg} - low-low	2/4	2/3
	or steamline pressure - low	2/4	2/3
5.	Steamline pressure - low	2/3	
	and steam flow - high	1/2	
	coincident with T_{avg} - low-low	2/3	
	interlocked with P12	2/3	
6.	Steam flow - high-high	1/2	
	coincident with safety injection		
7.	Steam flow - high	1/2	
	interlocked with P12	2/4	
	coincident with safety injection		
MAIN FEEDWATER ISOLATION			
1.	Steam generator level - high-high	2/4	2/3
2.	T_{cold} low coincident with	2/3	
	Feedflow - High	2/3	
AUXILIARY FEEDWATER PUMP START			
1.	Steam generator level - low-low	2/4	2/3
2.	RCP bus undervoltage	2/4	2/3
3.	RCP bus undervoltage	1/2 twice	
CONTAINMENT SPRAY AND PHASE B ISOLATION			
1.	Containment pressure - high-high	2/4	
2.	Containment pressure - high-high-high	2/4	

TABLE 3.1-4

ESF RELAY PROTECTION SYSTEM SENSITIVITY STUDY PARAMETERS

CASE	MASTER RELAYS		SLAVE RELAYS	
	TEST INTERVAL (month)	TEST TIME (hour)	TEST INTERVAL (month)	TEST TIME (hour)
SS1	2	8	3	6
SS2	2	8	6	12
SS3	2	8	9	12
SS4	2	8	12	12
SS5	2	8	18	12
SS6	3	8	3	6
SS7	3	8	6	12
SS8	3	8	9	12
SS9	3	8	12	12
SS10	3	8	18	12
SS11	4	8	3	6
SS12	4	8	6	12
SS13	4	8	9	12
SS14	4	8	12	12
SS15	4	8	18	12
SS16	1	3	6	12
SS17	1	3	9	12
SS18	1	3	12	12
SS19	1	3	18	12

Note: All other parameters correspond to Case 1 conditions.

TABLE 3.1-5

ESF SOLID STATE PROTECTION SYSTEM SENSITIVITY STUDY PARAMETERS

CASE	MASTER RELAYS		SLAVE RELAYS	
	TEST INTERVAL (month)	TEST TIME (hour)	TEST INTERVAL (month)	TEST TIME (hour)
SS1	3	4	9	4
SS2	3	4	12	4
SS3	3	4	6	4
SS4	2	1.5	9	4
SS5	2	1.5	12	4
SS6	2	1.5	6	4
SS7	6	4	9	4
SS8	6	4	12	4
SS9	6	4	6	4

Note: All other parameters correspond to Case 1 conditions.

3.2 DATA

The majority of the data used in the fault tree analysis of the Engineered Safety Features is the same as that documented in WCAP-10271 and does not reappear in this document. Only failure rate estimates not previously provided in WCAP-10271 or Supplement 1 are included in this report. These additional failure rate estimates which are provided in Table 3.2-1 have been generated by reviewing a variety of data sources. The review of various data sources was necessary to supplement available nuclear power information for these components. Due to the differences in data sources, two methods for generation of failure rate estimates were necessary:

1. If sufficient raw data were available for a particular component, the failure rate estimate was calculated directly via the following equation:

   Failure Rate Estimate = Number of Failures/Total Operating Time

2. If sufficient raw data were not available, several data sources containing pre-calculated failure rates were reviewed in order to determine the most appropriate failure rate estimate.

All failure rate estimates provided are point estimates.

TABLE 3.2-1

FAILURE RATE ESTIMATE

Component Description	Failure Mode	Failure Rate Estimate
Relay	1. Mechanically bound	4.0×10^{-7}/hr
	2. Constant failure	8.5×10^{-6}/d*
	3. Shorted coil	1.0×10^{-7}/hr
	4. Open coil	1.0×10^{-8}/hr
Switch	1. All** (includes fails closed)	3.6×10^{-9}/hr

*Failure rates provided are hourly except where noted by /d which indicates a per demand failure rate. Per demand failure rates have been converted to hourly assuming 20 demands per year.

**The all failure mode is not dissected futher due to its magnitude.

3.3 FAULT TREE MODEL

Fault trees model the hardware configurations which lead to signal failure. Each fault tree specifically models and is unique to a particular ESF signal. Therefore, fault trees for each ESF signal, for both relay and solid state logic were developed. This section of the report discusses some of the more important aspects of the hardware designs which affect fault tree construction, particularly those associated with the actuation relays. Analog channel and logic modeling is discussed in more detail in WCAP-10271, Section 4.0. The fault trees used are provided in Appendix C of this report.

3.3.1 ANALOG CHANNELS

Discussions of the analog channels are applicable to both the relay and solid state logic due to the similarity of design. The more pertinent aspects of the analog channel fault tree model are testing and maintenance modeling. The fault tree is constructed utilizing the following assumptions:

1. Analog channel testing is performed in a bypass condition. Some ESFAS channels are tested in bypass and this constitutes the most limiting configuration from an unavailability aspect.

2. Testing of more than one analog channel at a time is assumed in the fault tree model. Although this is typically not true in practice it simplifies fault tree construction considerably and represents a more conservative case.

3. Maintenance of the analog channels is performed in the bypass condition. This represents actual practice. The maintenance times chosen for the Base Case are those allowed by current technical specifications.

3.3.2 SOLID STATE LOGIC

The pertinent assumptions relative to the solid state logic are as follows:

1. Testing of the logic prohibits actuation of the entire associated train. This is consistent with hardware design and is necessary to allow at power testing. The redundant train remains operational and capable of providing all ESF functions.

2. Maintenance of the logic is assumed to prohibit actuation of the entire associated train. This is consistent with actual practice or conservative.

3. Testing of the master relays prohibits actuation of the entire associated train. This is consistent with the test circuitry provided for the master relays and represents actual practice.

4. Maintenance of master relays makes the affected master relay and all associated slave relays inoperable. This is consistent with the design of the actuation relays.

5. The number of master and slave relays actuated by an ESF signal varies from signal to signal and is a function of the number of components to be operated. A review of several solid state plant specific designs was conducted to identify typical configurations. Based upon this review, two master relays each driving 3 slave relays, was modeled for each train of Safety Injection and Containment Spray functions. One master relay driving 2 slave relays was modeled for each train of a Steam or Feed Line Isolation function or an Auxiliary Feedwater Pump Start function. The ESF master/slave relay arrangements are summarized in Table 3.3-1.

6. Unavailability of an ESF function was assumed to occur if the equivalent relays, either master or slave, in the redundant trains were unavailable. That is, if the relays which actuate the high head safety injection pumps in each train are unavailable, the ESF function is assumed not to occur. This is a conservative assumption and considered to be bounding in that partial system failures are equated to total system failures. A less conservative approach, while not inappropriate, would have in all likelihood resulted in a significant increase in the complexity of fault tree modeling and was thus not used.

7. Testing and Maintenance of slave relays was modeled assuming that the affected relay only, is made inoperable. This is consistent with actual practice or conservative. In the case of testing, in many cases actuation of the slave relay is allowed to actuate the associated components and hence, no unavailability results. However, in some cases, actuation of the affected components is blocked rendering the components unavailable for automatic actuation. Since this represents the limiting case it was chosen for the model.

In the slave relay availability model, the consequences of human error are not explicitly modeled. A potential availability improvement does exist as a result of increasing the slave relay surveillance test interval when consideration is given to human error.

During slave relay testing it is sometimes necessary to block equipment actuation to prevent the creation of an adverse condition resulting from opertion of the affected equipment. For example, it may be desirable to block actuation of charging pump suction valves from the RWST to prevent inadvertently borating the reactor coolant system while at power. Considering the potential for human error, there is some probability that following slave relay testing the blocked equipment will not be properly realigned to the normal mode. Should this occur, the affected equipment would be unavailable. The result is an increase in the unavailability of the ESF equipment. Less frequent slave relay testing would minimize this contribution to ESF unavailability. Because the slave relay availability model does not include a human error component, this potential benefit from increasing the slave relay surveillance test interval is not included in the results.

3.3.3 RELAY LOGIC

The hardware design for relay logic plants varies over a considerable range as discussed in Section 2.1 of this report. For purposes of the fault tree model a review of several relay logic plant specific designs was conducted. Based upon this review a bounding relay logic design was identified. This bounding design was used to construct the fault tree model. The pertinent assumptions relative to the relay logic are as follows.

1. Items 1, 2, 3, 4, 6, and 7 of Section 3.3.2 are applicable to relay logic. Briefly, testing and maintenance of the logic prohibits actuation of the entire associated train. Testing of the master relays makes the entire associated train inoperable. Maintenance of a master relay makes the affected master and all associated slaves unavailable. Unavailability of an ESF function was assumed to occur if equivalent relays in the redundant trains are unavailable. Maintenance and testing of slave relays makes only the affected slave inoperable.

2. The fault tree model for the relay logic is based on the following assumptions. Safety Injection function assumed one master relay driving 6

slave relays for each train. The Steamline Isolation and Spray Actuation functions assumed 1 master relay driving 3 slave relays for each train. The Auxiliary Feedwater Pump Start and Feedwater Isolation functions assumed only 1 master relay driving no slave relays. These typical configurations were determined in conjunction with the aforementioned review. The ESF master/slave relay arrangements are summarized in Table 3.3-2.

TABLE 3.3-1

SOLID STATE LOGIC: MASTER/SLAVE RELAY ARRANGEMENTS

GSF	Master Relays[1]	Slave Relays[1]
1. Safety Injection	A	A1, A2, A3
	B	B1, B2, B3
2. Steam Line Isolation	A	A1, A2
3. Main Feedwater Isolation	A	A1, A2
4. Aux. Feedwater Pump Start	A	A1, A2
5. Containment Spray	A	A1, A2
6. Containment Isolation	A	A1, A2

(1) Relays per ESF train.

TABLE 3.3-2

RELAY LOGIC: MASTER/SLAVE RELAY ARRANGEMENTS

ESF	Master Relays[1]	Slave Relays[1]
1. Safety Injection	A	A1, A2, A3, A4, A5, A6
2. Steam Line Isolation	A	A1, A2, A3
3. Main Feedwater Isolation	A	None
4. Aux. Feedwater Pump Start	A	None
5. Containment Spray	A	A1, A2, A3
6. Containment Isolation	A	A1, A2, A3

(1) Relays per ESF train

3.4 RISK MODEL

A risk analysis was used to estimate the changes in core melt frequency and total Man-REM exposure due to the ESF unavailability changes. The analysis was based on the Millstone Unit 3 Probabilistic Safety Study (PSS) (Ref. 5), which includes a solid state ESF system, and considered only core melt frequencies and Man-REM exposure values related to internally initiated events. The primary objective of a PSS is to identify, analyze, and quantify the risk contribution associated with hypothetical accident sequences. A typical study consists of plant, containment, and site analyses. The plant analysis considers initiating events that have the potential of leading to core damage, analysis of plant systems used to mitigate the core damage potential, and construction of event trees that model the course of sequences leading to core damage. The chief measure for the plant analysis results is core melt frequency. The mitigating effects of the containment structure and radioactivity removal systems are subsequently modeled in the containment analysis using event tree techniques. This yields the frequency of occurrence for particular radiological releases. Finally, public health consequences are assessed based on site specific population density, evacuation speed, and anticipated meteorological conditions in the site analysis. One measure of success of the complete study is Man-REM exposure. This index is dependent on the plant, containment, and site analyses. While a plant specific risk study was used for this evaluation the results are considered to be typical of all Westinghouse plants.

The changes in the ESF unavailability (due to surveillance requirement relaxation) only affects the plant analysis, but the plant analysis changes must be propagated through the containment and site analyses to determine the effect of the ESF surveillance relaxation on the public health consequences. The Millstone study was the basis of the risk analysis due to the method of incorporating the ESF into the plant analysis. The ESF is incorporated into either the event trees that model the required sequence of events to mitigate the damage potential of initiating events, or into the support state model. The support state model includes systems that are highly depended on for the

successful operation of other systems, such as, electrical power and service water. The Millstone PSS also includes the ESF and emergency generator loading sequencer due to the high level of dependency between these systems and plant safety systems. The support systems are modeled in the PSS through eight simplified support states. Unavailability changes to the ESF impacts the probability of being in any particular support state. These probabilities are referred to as support state split fractions. This method precludes the ESF from the event trees and, therefore, simplifies the analysis.

Modeling of the ESF in the Millstone study was based on a safety injection signal considered representative of the ESF system. Values for both ESF trains unavailable, one ESF train unavailable, and both ESF trains available are input to the support state model in conjuction with unavailability values for the other three support state systems to yield support state split fractions. The unavailability of the ESF for this analysis is based on the solid state system "Safety Injection signal on Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3)". This signal is considered representative of the ESF signals in general, except for the relay protection system Main Feedwater Isolation and Auxiliary Feedwater Pump Start features (discussed in more detail in subsequent sections).

Support state split fractions were calculated from the support state model based on the ESF unavailabilities. The split fractions were then used in conjunction with the initiating event vector, plant matrix, containment matrix, and site matrix from the Millstone study to estimate revised core melt frequencies and the total Man-REM exposures. The ARBRE (Ref. 6) computer code is used to determine the support state split fractions. The PHIM (Ref. 7) and BORIS (Ref. 8) computer codes, which conduct matrix manipulations, use the split fractions in addition to the initiating event vector and the plant, containment, and site matrices to calculate core melt frequency and Man-REM exposure. These calculations were completed for the Base Case and Case 1 conditions and also two intermediate conditions. The intermediate conditions were included to evaluate the impact of alternate relaxed testing and maintenance conditions.

The changes in the test and maintenance times and intervals modify the core melt and Man-REM results through two effects. These are:

1. The ESF unavailability will increase/decrease depending on the increase/decrease in the test and maintenance parameters.

2. The initiating event frequency for spurious safety injection will also increase/decrease depending on the increase/decrease in test and maintenance parameters.

For this particular study the spurious safety injection frequency is expected to decrease with the relaxed parameters. However, contributions to core melt frequency and Man-REM from spurious safety injection are small. Therefore, reducing the spurious safety injection initiating event frequencies would have a negligible effect on these indices and was not considered in the risk analysis. None the less, the reduction in the spurious safety injection initiating event frequency as a result of increasing the surveillance test intervals should lead directly to utility cost savings. The benefits are provided by:

1. The reduction in manpower costs from reduced testing and associated administrative time required to follow the testing.

2. Reduction in costs related to recovering from spurious safety injections.

3.5 MARKOV MODEL

Markovian analysis can be used to evaluate alternate testing and maintenance schemes based on system unavailability, reactor downtime, and/or core melt frequency. The Markovian approach yields time dependent parameters, whereas, the previous approach (unavailability from fault tree analysis and core melt frequency from risk analysis based on a Probabilistic Safety Study) yields time averaged parameters. The Markov method can account for time and state dependencies which may be overlooked in the fault tree/risk analysis

methodology. The Markov approach indicates when a system's unavailability is at maximums and minimums based on the system's test and maintenance schedule and may easily account for staggered component/train testing schemes.

The Markovian methodology applied in this analysis follows the methodology applied by Brookhaven National Laboratory (BNL) in their evaluation of the Reactor Trip section of the Reactor Protection System Technical Specification Optimization Study [23]. The computer codes used in the analysis, STAGEN and MARELA, were also developed at BNL [22].

The Markov model requires analyzing the system in terms of a functional block diagram, comprised of supercomponents. The supercomponents model the subsystems and are composed of components with identical testing and maintenance schedules. State transition diagrams are developed for each supercomponent and for the complete system. These transition diagrams define the allowable operating states for the supercomponents (and system) and the allowable transition between the states. The functional block diagram, transition diagrams, and test and maintenance schedule in conjunction with the STAGEN and MARELA codes are used to evaluate the system. Depending on the transition diagram, the evaluation may be in terms of system unavailability, plant downtime, and/or core melt frequency.

The approach followed in this analysis consider only the system unavailability for evaluation of the various testing and maintenance schemes. Comparison between the two methods (fault tree and Markov) is based on system unavailability from the fault tree analysis and an overall time averaged value from the Markov method. Since this analysis is used essentially as a check on the results of the fault tree analysis, only one system, representative of the ESF, was evaluated. Steamline Isolation on Steamline Pressure Low (2/3) Interlock with P11 (2/3) in the solid state ESF design is considered to be representative with respect to overall configuration, i.e., all the basic components are modeled, 2 out of 3 logic on the analog channels and interlock is included, and master relays activate more than one slave relay.

Figure 3.1 shows the functional block diagram of the ESF Steamline Isolation where each block is considered a supercomponent. The model consists of three analog channels, and two trains each containing a logic cabinet, master relay, and two slave relays. Each master relay controls two slave relays. The master relay and logic cabinet in each train are combined into a single supercomponent since (1) they have identical test and maintenance times and intervals and (2) they both have the same impact on system operability.

Figure 3.2 shows the state transition diagram for an analog channel. The diagram consists of three states; (1) operating state, (2) failed state, and (3) tripped state. The analog channels are not modeled in the bypass state since the allowable outage time is small compared to mean time to failure and it is assumed that transition in and out of the bypass state occurs instantaneously. The diagram shows that the analog channel may pass from state 1 to state 2 when the component fails due to either random failure or common mode failure. The analog channel may also pass from state 1 to state 3 due to a spurious actuation. Scheduled testing may occur when the channel is in either state 1 or 2. When testing occurs in state 1, the channel may be (1) returned to the operating state, (2) returned to the failed state due to human error, or (3) be placed in the tripped state if the allowable outage time is exceeded. When testing occurs in state 2, the channel may be (1) returned to the failed state due to human error or (2) be placed in the tripped state when the fault is detected. Testing is assumed to be instantaneous. Transition from state 3 to state 1 occurs following any necessary maintenance and/or verification of the analog channel's operability.

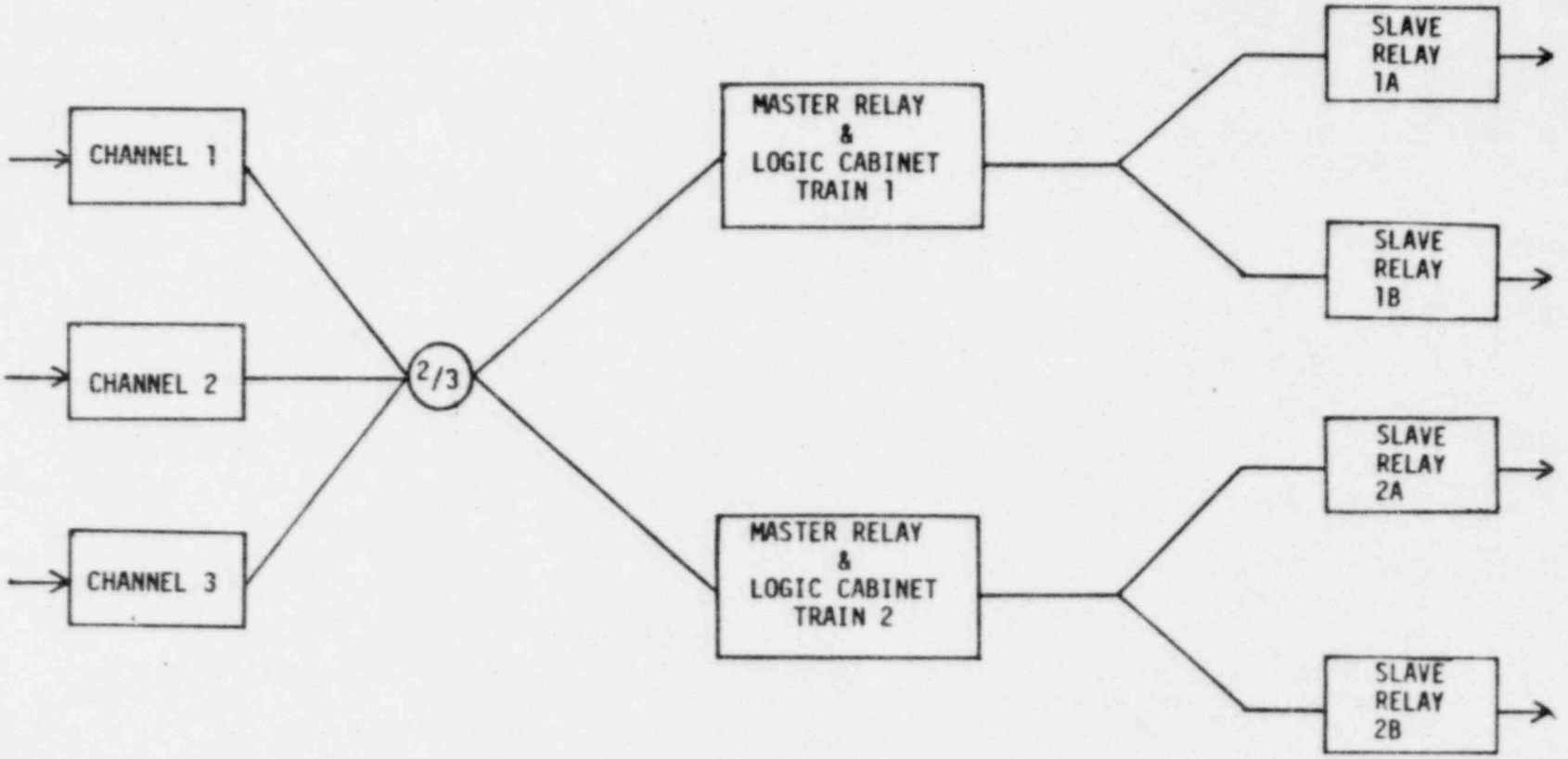
The transition diagram for the logic cabinet/master relay and slave relay supercomponents is similar to the analog channel diagram. The diagram consists of just two states, (1) operating state and (2) failed state. Again, the bypass state is not modeled for the same reasons given for the analog channels. Transition from state 1 to state 2 may occur due to either random failure or common mode failure. Following a test in state 1, the supercomponent may be (1) returned to the operating state or (2) returned to the failed state due to human error. Following a test in state 2, the

supercomponent may be (1) returned to the failed state due to human error or (2) returned to the operating state following the required repair. The required repair is assumed to be completed prior to plant shutdown. Repair is assumed to be instantaneous, as is testing. With this assumption, the steamline isolation logic train may be faced with a real demand at any time. The tripped state was not modeled for the logic cabinet/master relay or the slave relay supercomponents because spurious actuations were found not to be a primary contributor to overall core melt frequency as noted in the fault tree analysis.

The state transition diagram for the system is shown in Figure 3.3. The diagram consists of three states; (1) Steamline Isolation functional: all components up, (2) Steamline Isolation functional: one or more components failed, and (3) Steamline Isolation unavailable. The transition from state 1 to state 2 occurs following a single random failure of any component or a human error. The transition from state 1 to state 3 may only occur following a common mode failure. State 2 may transfer to state 1 after testing and maintenance on a failed component. State 2 may transfer to state 3 by either a single random failure, a common mode failure, or human error. The only transition state 3 can make is to state 2 after the test and maintenance has been performed on a failed component.

FIGURE 3.1

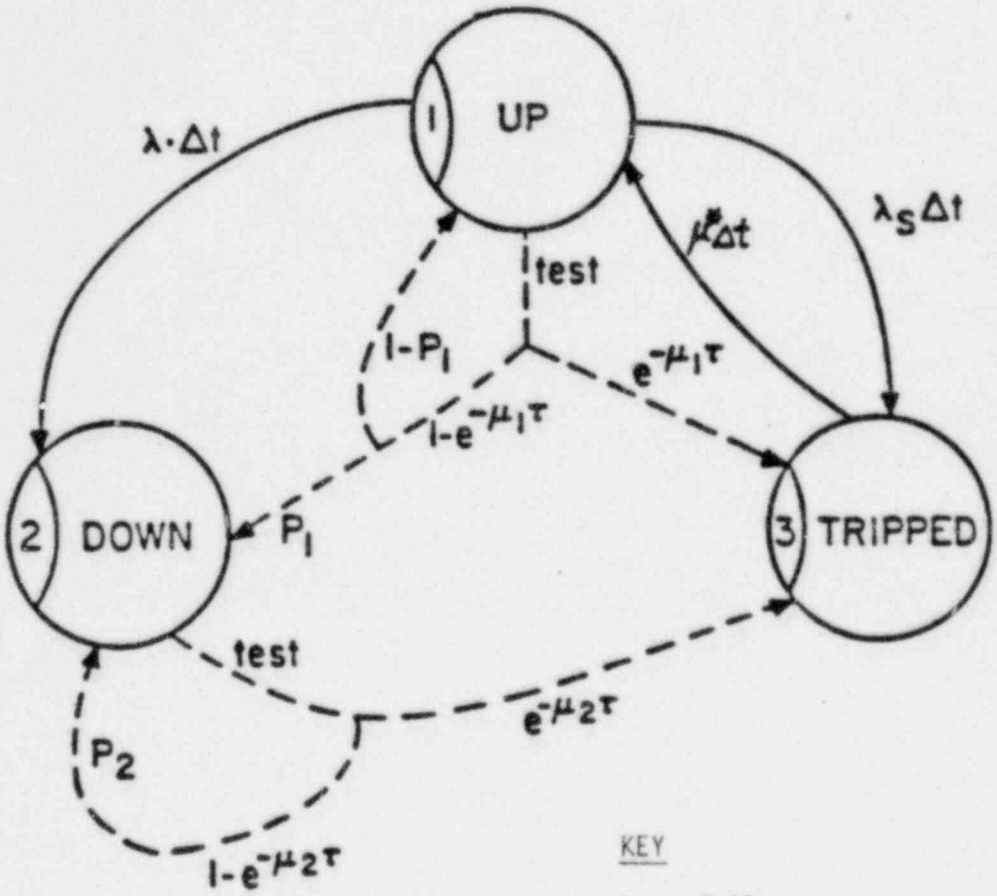
ESF LAYOUT FOR MARKOV MODEL



BASED ON STEAMLINE ISOLATION FEATURE

FIGURE 3.2

STATE TRANSITION DIAGRAM: ANALOG CHANNEL



KEY

λ = failure rate

λ_S = spurious trip rate

μ^* = 1/MTTR a tripped channel

μ_1 = 1/MTTT an operating channel

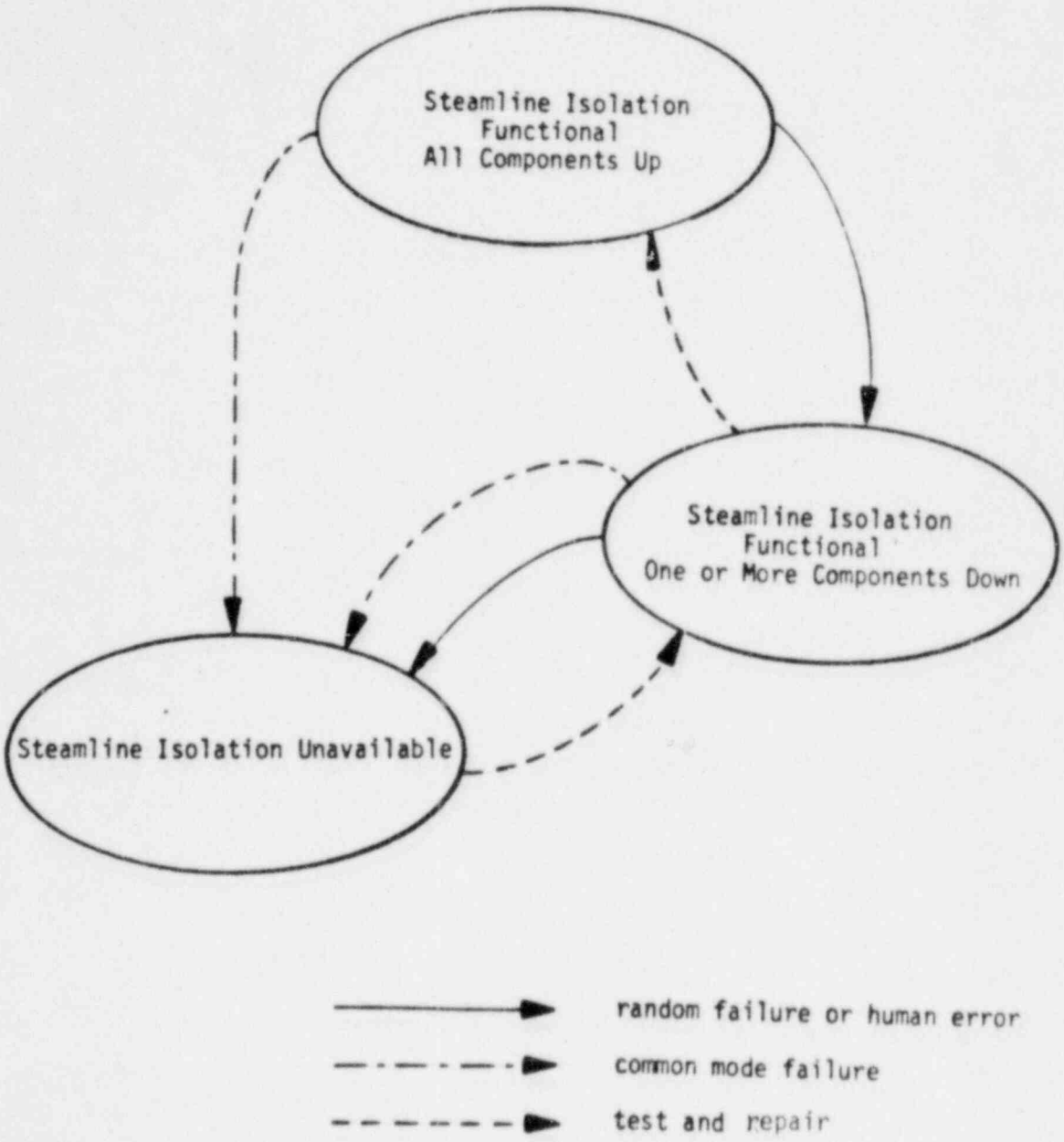
μ_2 = 1/MTTT a failed channel

P_1 = HEP when testing an operating channel

P_2 = HEP when testing a failed channel

FIGURE 3.3

STATE TRANSITION DIAGRAM: ESF



3.6 RESULTS

The results of the ESF signal unavailability analysis, risk analysis, and Markov analysis are presented in this section. General discussions involving the background of these analyses were presented in the preceding sections.

3.6.1 ESF SIGNAL UNAVAILABILITY

Table 3.1-1 indicates that all of the test times and intervals increased from the Base Case to Case 1 except for the solid state system slave relay test time which remained constant. Maintenance times also increased, however, maintenance intervals remained constant. Several opposing effects on the component and system unavailabilities are expected due to increasing these parameters. Increasing the test interval increases the component unavailability due to random failures, but decreases the component unavailability due to testing, provided the test time remains constant. Increasing the test time increases the component unavailability provided the test interval remains constant. Increasing the maintenance time also increases the component unavailability provided the maintenance interval does not change (note that the maintenance interval remains the same between the Base Case and Case 1). The unavailability related to common mode failure as calculated by the Beta factor method (master and slave relays and logic cabinet) increases with increasing test interval. Common mode failure calculated by the Atwood method (analog channels) is not affected by the time and interval changes since it is assumed that analog channel common cause failure is detectable within eight hours. The unavailability due to human factors is not affected by the time and interval changes.

The unavailability changes in the ESF are not expected to be directly proportional to the changes in test and maintenance times and intervals. This non-proportionality is due in part to the competing effects of increasing the times and intervals as previously discussed, and also due to redundancy of the ESF system design. That is, the design includes two trains of logic cabinets and master and slave relays, and multiple analog channels, i.e., 2 of 3 or 2 of 4 channel signals, required for relay actuation.

The unavailability results are shown in Tables 3.6-1 through 3.6-10 for the ESF relay and solid state protection systems. Unavailabilities are provided for each ESF system signal listed in Tables 3.1-2 and 3.1-3 for the Base Case and Case 1 conditions with and without the common mode failure contribution. In general, the unavailabilities without common mode failure increased by factors of 2 to 8 and with common mode failure increased by factors of 3 to 6.

Tables 3.6-11 through 3.6-15 give a breakdown of contributors to total unavailability for each of the ESF features; Safety Injection (SI), Steamline Isolation (SLI), Main Feedwater Isolation (MFWI), Auxiliary Feedwater Pump Start (AFWPS), and Containment Spray and Phase B Isolation (CS & PBI) for relay and solid state systems. The signals used for each feature are considered representative of that feature. In addition, 2 of 3 and 2 of 4 analog channel logic conditions were also included for each feature. The unavailability is divided into four categories. These are: 1) random failure, maintenance, and test for relays and logic cabinets, 2) random failure, maintenance, and test for analog channels, 3) common mode failure for relays and logic cabinets, and 4) common mode failure for analog channels. The following conclusions and observations apply to all the features of the relay and solid state systems except for the MFWI and AFWPS features of the relay system.

1. The main contributor to the unavailability is the common mode failure of the master and slave relays and logic cabinets. This generally accounts for 60% to 98% of the total.

2. The second largest contributor, for systems with 2 of 4 analog channel logic, is unavailability due to random failures, maintenance, and test of the relays and logic cabinets (2% to 18%). This is generally the third largest contributor (3% to 15%) for systems with 2 of 3 channel logic.

3. Unavailability due to analog channel failure is an insignificant contributor (less than 1%) for systems with 2 of 4 analog channel logic, but is generally the second largest contributor (6% to 25%) for systems with 2 of 3 channel logic.

4. Common mode failure of the analog channels is also a small contributor for both analog channel logics (less than 4%).

The following conclusions apply to the MFWI and AFWPS relay system features:

1. Common mode failure of the relays and logic cabinets is the largest contributor to total unavailability for 2 of 4 analog channel logic systems (60% to 90%), but it is the second largest contributor for 2 of 3 analog channel logic systems (20% to 40%).

2. Random failure, maintenance, and test of the relays and logic cabinets generally account for 2% to 13% of the unavailability.

3. The contribution from analog channel random failure, maintenance, and test is low (less than 2%) for 2 of 4 channel logic, but accounts for approximately 60% in 2 of 3 logic systems.

4. Depending on the case considered, the analog channel common mode failure contributes up to 25%.

Several other conclusions applicable to all the features are: 1) systems with 2 of 3 analog channel logic have higher unavailabilities than systems with 2 of 4 logic and 2) the unavailabilities of MFWI and AFWPS signals are lower than the other signal unavailabilities.

A third conclusion, which is not as evident, is that the majority of the unavailability due to random failure, maintenance, and test of the relays and logic cabinets is due to combinations of testing or maintenance with random failures of components associated with the top trees (master/slave relays). Typical dominant cutsets are:

1. One slave relay in Train A unavailable due to maintenance and the corresponding slave relay in Train B fails shorted.

2. Train B unavailable due to test and any one slave relay in Train A fails shorted.

3. Train A unavailable due to test and any one master relay in Train B mechanically bound.

It is important to note that failure of components in the logic cabinets do not contribute substantially to the ESF unavailability.,

Tables 3.6-11 through 3.6-15 also give a breakdown of the contribution of each of the categories to the change in unavailability due to relaxing the maintenance and test parameters. The analog channels (including common mode failure) with 2 of 4 channel logic generally account for less than 2% of the unavailability increase. Analog channels with 2 of 3 channel logic account for 5% to 15% of the increase (again including common mode failure) excluding the MFWI and AFWPS functions. For these functions, analog channels comprise over 50% of the increase. Note that analog channel common mode failure contribution to the signal unavailability increase is 0%.

The reason most ESF functions are insensitive to changes in analog channel testing and maintenance parameters is due to the large contributions to unavailability from master and slave relays and the low common mode failure contribution. The low analog channel common mode failure probability is a result of the assumption that analog channel common mode failures would be detectable within eight hours. That is, detectable independent of testing. The eight hour detection interval controls the common mode failure contribution which is the same for all cases considered. The common mode failure of the relays and logic cabinets is test interval dependent and these intervals are significantly longer than eight hours. The analog channels are large contributors to the MFWI and AFWPS functions. On an absolute basis the analog channel contributions are similar. However, for more complex functions the master and slave relay contributions are large with respect to the analog channel contribution masking the analog channel contribution. For these two particular functions which have no slave relays and only one master relay the analog channel contributions become proportionately larger relative to the lower overall function unavailability.

None of the unavailability values presented in Tables 3.6-1 to 3.6-15 consider analog channel diversity, that is, ESF actuation signals from more than one analog channel source. From the previous discussion concerning contributors to unavailability it is evident that in most cases the analog contribution is insignificant without considering diversity. Including diversity will further reduce the analog channel contribution. To estimate the effect of diversity, three cases were considered. These are summarized on Table 3.6-16. The only situation in which diversity has a substantial effect is for the MFWI and AFWPS features that use the relay design system with 2/3 analog channel logic. Otherwise, the diversity effect is small and the unavailabilities presented in Tables 3.6-1 to 3.6-10 (excluding 3.6-3 and 3.6-4) are indicative of signal unavailabilities with diversity. The values in Tables 3.6-3 and 3.6-4 are conservative.

TABLE 3.6-1

ESF RELAY PROTECTION SYSTEM UNAVAILABILITIES
SAFETY INJECTION FEATURE

	SIGNAL	BASE CASE		CASE 1	
		w/o CMF	w/CMF	w/o CMF	w/CMF
1A.	Pressurizer pressure - low - 2/4 interlocked with P11 - 2/3	7.1E-05	8.2E-04	1.0E-04	4.5E-03
1B.	Pressurizer pressure - low - 2/3 interlocked with P11 - 2/3	1.8E-04	9.3E-04	4.6E-04	4.9E-03
2A.	Steamline pressure - low - 2/4 interlocked with P11 - 2/3	7.1E-05	8.2E-04	1.0E-04	4.5E-03
2B.	Steamline pressure - low - 2/3 interlocked with P11 - 2/3	1.8E-04	9.3E-04	4.6E-04	4.9E-03
3A.	Steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	7.1E-05	8.2E-04	1.0E-04	4.5E-03
3B.	Steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	1.8E-04	9.3E-04	4.6E-04	4.9E-03
4.	Containment pressure - high - 2/3	1.5E-04	9.0E-04	2.8E-04	4.7E-03
5A.	Differential steamline pressure high - 2/3	1.5E-04	9.0E-04	2.8E-04	4.7E-03
5B.	Differential steamline pressure high - 2/3 interlocked with P11 - 2/3	1.5E-04	9.0E-04	2.8E-04	4.7E-03
6A.	Steamflow - high - 1/2 coincident with T_{avg} low-low - 2/3 or steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	1.1E-04	8.6E-04	2.2E-04	4.6E-03
6B.	Steamflow - high - 1/2 coincident with T_{avg} low-low - 2/3 or steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	1.1E-04	8.6E-04	2.2E-04	4.6E-03
6C.	Steamflow - high - 1/2 coincident with T_{avg} low-low - 2/4 or steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	1.1E-04	8.6E-04	2.2E-04	4.6E-03
6D.	Steamflow - high - 1/2 coincident with T_{avg} low-low - 2/4 or steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	1.1E-04	8.6E-04	2.2E-04	4.6E-03

TABLE 3.6-2

ESF RELAY PROTECTION SYSTEM UNAVAILABILITIES
STEAMLINE ISOLATION FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
1A.	Steamline pressure - low - 2/3 interlocked with P11 - 2/3	1.6E-04	5.6E-04	4.5E-04	2.8E-03
1B.	Steamline pressure - low - 2/4 interlocked with P11 - 2/3	4.5E-05	4.5E-04	8.8E-05	2.4E-03
2A.	Steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	1.6E-04	5.6E-04	4.5E-04	2.8E-03
2B.	Steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	4.5E-05	4.5E-04	8.8E-05	2.4E-03
3A.	Steamflow - high 1/2 coincident with T_{avg} - low-low - 2/3 or steamline pressure - low - 2/3	8.3E-05	4.9E-04	2.0E-04	2.5E-03
3B.	Steamflow high - 1/2 coincident with T_{avg} - low-low - 2/3 or steamline pressure - low - 2/4	8.3E-05	4.9E-04	2.0E-04	2.5E-03
3C.	Steamflow high - 1/2 coincident with T_{avg} - low-low - 2/4 or steamline pressure - low - 2/3	8.3E-05	4.9E-04	2.0E-04	2.5E-03
3D.	Steamflow high - 1/2 coincident with T_{avg} - low-low - 2/4 or steamline pressure - low - 2/4	8.3E-05	4.9E-04	2.0E-04	2.5E-03
4A.	Steamflow high - 1/2 coincident with T_{avg} - low-low - 2/4	8.4E-05	4.9E-04	2.1E-04	2.5E-03
4B.	Steamflow high - 1/2 coincident with T_{avg} - low-low - 2/3	2.1E-04	6.1E-04	6.4E-04	3.0E-03
5A.	Containment pressure - high-high - 2/3	1.2E-04	5.2E-04	2.7E-04	2.6E-03
5B.	Containment pressure - high-high - 2/4	4.5E-05	4.5E-04	8.5E-05	2.4E-03
6.	Steamflow - high-high - 1/2 or steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/4	4.5E-05	4.5E-04	8.4E-05	2.4E-03

TABLE 3.6-3

ESF RELAY PROTECTION SYSTEM UNAVAILABILITIES
MAIN FEEDWATER ISOLATION FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
1A.	Steam generator level - high-high - 2/3	1.2E-04	1.8E-04	3.8E-04	6.3E-04
1B.	Steam generator level - high-high - 2/4	9.0E-06	6.3E-05	2.2E-05	2.7E-04

TABLE 3.6-4

ESF RELAY PROTECTION SYSTEM UNAVAILABILITIES
AUXILIARY FEEDWATER PUMP START FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
1A.	Steam generator level - low-low - 2/3	1.2E-04	1.8E-04	3.8E-04	6.3E-04
1B.	Steam generator level - low-low - 2/4	9.0E-06	6.3E-05	2.2E-05	2.7E-04

TABLE 3.6-5

ESF RELAY PROTECTION SYSTEM UNAVAILABILITIES
CONTAINMENT SPRAY AND PHASE B ISOLATION FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
1.	Containment pressure - high-high - 2/4	4.5E-05	4.5E-04	8.5E-05	2.4E-03
2.	Containment pressure - high-high-high - 2/4	4.5E-05	4.5E-04	8.5E-05	2.4E-03

TABLE 3.6-6

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES
SAFETY INJECTION FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
1A.	Pressurizer pressure - low - 2/4 interlocked with P11 - 2/3	1.1E-04	9.7E-04	7.8E-04	5.4E-03
1B.	Pressurizer pressure - low - 2/3 interlocked with P11 - 2/3	2.2E-04	1.1E-03	1.1E-03	5.8E-03
2A.	Steamline pressure - low - 2/4 interlocked with P11 - 2/3	1.1E-04	9.7E-04	7.8E-04	5.4E-03
2B.	Steamline pressure - low - 2/3 interlocked with P11 - 2/3	2.2E-04	1.1E-03	1.1E-03	5.8E-03
3A.	Steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	1.1E-04	9.7E-04	7.8E-04	5.4E-03
3B.	Steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	2.2E-04	1.1E-03	1.1E-03	5.8E-03
4.	Containment pressure - high - 2/3	1.9E-04	1.1E-03	9.6E-04	5.6E-03
5A.	Differential steamline pressure - high - 1 instr./steamline	1.9E-04	1.1E-03	9.6E-04	5.6E-03
5B.	Differential steamline pressure - high - 3 instr./steamline	1.9E-04	1.1E-03	9.6E-04	5.6E-03
6A.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/4 or steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	1.5E-04	1.0E-03	9.0E-04	5.5E-03
6B.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/4 or steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	1.5E-04	1.0E-03	9.0E-04	5.5E-03
6C.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/3 or steamline pressure - low - 2/4 interlocked with P12 - 2/3 or 2/4	1.5E-04	1.0E-03	9.0E-04	5.5E-03

TABLE 3.6-6 (Continued)

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES
SAFETY INJECTION FEATURE

	SIGNAL	BASE CASE		CASE 1	
		W/o CMF	W/CMF	W/o CMF	W/CMF
6D.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/3 or steamline pressure - low - 2/3 interlocked with P12 - 2/3 or 2/4	1.5E-04	1.0E-03	9.0E-04	5.5E-03
7.	T_{cold} - low-low - 2/3 coincident with steam pressure low - 2/3 interlocked with P15 - 2/4	1.9E-04	1.1E-03	9.6E-04	5.6E-03

TABLE 3.6-7

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES
STEAMLINE ISOLATION FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
1A.	Steamline pressure - low - 2/4	4.3E-05	3.7E-04	3.5E-04	2.0E-03
1B.	Steamline pressure - low - 2/3	1.6E-04	4.8E-04	7.1E-04	2.4E-03
2.	Steamline pressure - low - 2/3 and negative steamline pressure rate-high - 2/3 interlocked with P12	4.5E-05	3.7E-04	3.6E-04	2.0E-03
3A.	Containment pressure - high-high - 2/4	4.3E-05	3.7E-03	3.5E-04	2.0E-03
3B	Containment pressure - high-high - 2/3	1.2E-04	4.4E-04	5.3E-04	2.2E-03
4A.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/4 or steamline pressure - low - 2/4	8.0E-05	4.0E-04	4.7E-04	2.1E-03
4B.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/4 or steamline pressure - low - 2/3	8.0E-05	4.0E-04	4.7E-04	2.1E-03
4C.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/3 or steamline pressure - low - 2/4	8.0E-05	4.0E-04	4.7E-04	2.1E-03
4D.	Steamflow - high - 1/2 coincident with T_{avg} - low-low - 2/3 or steamline pressure - low - 2/3	8.0E-05	4.0E-04	4.7E-04	2.1E-03
5A.	Steamline pressure - low - 2/4 and steamflow - high - 1/2 coincident with T_{avg}-low-low-2/4 interlocked with P12 - 2/3 or 2/4	4.3E-05	3.7E-04	3.6E-04	2.0E-03
5B.	Steamline pressure - low - 2/3 and steamflow - high - 1/2 coincident with T_{avg}-low-low-2/4 interlocked with P12 - 2/3 or 2/4	4.3E-05	3.7E-04	3.6E-04	2.0E-03
5C.	Steamline pressure - low - 2/4 and steamflow - high - 1/2 coincident with T_{avg}-low-low-2/3 interlocked with P12 - 2/3 or 2/4	4.3E-05	3.7E-04	3.6E-04	2.0E-03

TABLE 3.6-7 (Continued)

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES
STEAMLINE ISOLATION FEATURE

	SIGNAL	BASE CASE w/o CMF	BASE CASE w/CMF	CASE 1 w/o CMF	CASE 1 w/CMF
5D.	Steamline pressure - low - 2/3 and steamflow - high - 1/2 coincident with T_{avg}-low-low-2/3 interlocked with P12 - 2/3	4.3E-05	3.7E-04	3.6E-04	2.0E-03
6.	Steamflow - high-high - 1/2 coincident with SI	1.9E-04	1.4E-03	1.2E-03	7.5E-03
7.	Steamflow - high - 1/2 interlocked with P12 - 2/4 coincident with SI	1.9E-04	1.4E-03	1.2E-03	7.5E-03

TABLE 3.6-8

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES

MAIN FEEDWATER ISOLATION FEATURE

	SIGNAL	BASE CASE		CASE 1	
		w/o CMF	w/CMF	w/o CMF	w/CMF
1A.	Steam generator water level - high-high - 2/4 in one loop	4.3E-05	3.7E-04	3.5E-04	2.0E-03
1B.	Steam generator water level - high-high - 2/3 in one loop	1.2E-04	4.4E-04	5.3E-04	2.2E-03
2.	T_{cold} - low - 2/3 Feed flow - high - 2/3	4.2E-05	3.7E-04	3.5E-04	2.0E-03

TABLE 3.6-9

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES
AUXILIARY FEEDWATER PUMP START FEATURE

	SIGNAL	BASE CASE		CASE 1	
		w/o CMF	w/CMF	w/o CMF	w/CMF
1A.	Steam generator water level - low-low - 2/4 in one loop	4.3E-05	3.7E-04	3.5E-04	2.0E-03
1B.	Steam generator water level - low-low - 2/3 in one loop	1.2E-04	4.4E-04	5.3E-04	2.2E-03
2A.	RCP bus undervoltage - 2/3	1.6E-04	4.8E-04	7.1E-04	2.4E-03
2B.	RCP bus undervoltage - 2/4	4.3E-05	3.7E-04	3.5E-04	2.0E-03
3.	RCP bus undervoltage - 1/2 twice	1.2E-04	4.4E-04	5.9E-04	2.2E-03

TABLE 3.6-10

ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES
CONTAINMENT SPRAY AND PHASE B ISOLATION FEATURE

SIGNAL	BASE CASE		CASE 1	
	w/o CMF	w/CMF	w/o CMF	w/CMF
1A. Containment pressure - high-high-2/4	1.1E-04	9.7E-04	7.8E-04	5.4E-03
1B. Containment pressure - high-high-high-2/4	1.1E-04	9.7E-04	7.8E-04	5.4E-03

TABLE 3.6-11

SUMMARY OF UNAVAILABILITY CONTRIBUTIONS: RELAY SYSTEMS

Safety Injection

		UNAVAILABILITY CONTRIBUTIONS					
		2/3 ANALOG CHANNEL LOGIC			2/4 ANALOG CHANNEL LOGIC		
		BASE CASE	CASE 1	CHANGE* (percent)	BASE CASE	CASE 1	CHANGE* (percent)
1.	Total Random Failure, Maintenance, and Test	1.83E-04 (19.6%)	4.61E-04 (9.5%)	7.1	7.10E-05 (8.6%)	1.04E-04 (2.3%)	0.9
1A.	Relays and Logic Cabinets	7.01E-05 (7.5%)	9.87E-05 (2.0%)	0.7	7.01E-05 (8.5%)	9.87E-05 (2.2%)	0.8
1B.	Analog Channels	1.13E-04 (12.1%)	3.63E-04 (7.5%)	6.4	9.26E-07 (0.1%)	5.32E-06 (0.1%)	0.1
2.	Common Mode Failure: Relays and Logic	7.35E-04 (78.8%)	4.40E-03 (90.3%)	93.1	7.35E-04 (89.5%)	4.40E-03 (97.6%)	99.2
3.	Common Mode Failure: Analog Channels	1.50E-05 (1.6%)	1.50E-05 (0.3%)	0.0	1.5E-05 (1.8%)	1.5E-05 (0.3%)	0.0
4.	Total	9.33E-04	4.87E-03	100.0	8.21E-04	4.51E-03	100.0

Based on: Low Steamline Pressure interlocked with P12 (2/4).

Note: First value of each set listed is unavailability.
Second value of each set listed is percent contribution to total unavailability.

* Percent change of total unavailability change from Base Case to Case 1.

TABLE 3.6-12

SUMMARY OF UNAVAILABILITY CONTRIBUTIONS: RELAY SYSTEMS

Steamline Isolation and Containment Spray and Phase B Isolation

		UNAVAILABILITY CONTRIBUTIONS					
		2/3 ANALOG CHANNEL LOGIC			2/4 ANALOG CHANNEL LOGIC		
		BASE CASE	CASE 1	CHANGE* (percent)	BASE CASE	CASE 1	CHANGE* (percent)
1.	Total Random Failure, Maintenance, and Test	1.58E-04 (28.1%)	4.48E-04 (16.1%)	13.1	4.52E-05 (10.1%)	8.83E-05 (3.7%)	2.2
1A.	Relays and Logic Cabinets	4.43E-05 (7.9%)	8.30E-05 (3.0%)	1.7	4.43E-05 (9.9%)	8.30E-05 (3.4%)	2.0
1B.	Analog Channels	1.14E-04 (20.2%)	3.65E-04 (13.2%)	11.4	9.26E-07 (0.2%)	5.32E-06 (0.2%)	0.2
2.	Common Mode Failure: Relays and Logic	3.87E-04 (69.2%)	2.32E-03 (83.8%)	87.4	3.87E-04 (86.6%)	2.32E-03 (96.3%)	98.5
3.	Common Mode Failure: Analog Channels	1.50E-05 (2.7%)	1.50E-05 (0.5%)	0.0	1.50E-05 (3.4%)	1.50E-05 (0.6%)	0.0
4.	Total	5.59E-04	2.77E-03	100.0	4.47E-04	2.41E-03	100.0

Based on: Steamline Pressure Low interlocked with P11 (2/3).

Note: First value of each set listed is unavailability.
Second value of each set listed is percent contribution to total unavailability.

* Percent change of total unavailability change from Base Case to Case 1.

TABLE 3.6-13

SUMMARY OF UNAVAILABILITY CONTRIBUTIONS: RELAY SYSTEMS

Main Feedwater Isolation and Auxiliary Feedwater Pump Start

		UNAVAILABILITY CONTRIBUTIONS					
		2/3 ANALOG CHANNEL LOGIC			2/4 ANALOG CHANNEL LOGIC		
		BASE CASE	CASE 1	CHANGE* (percent)	BASE CASE	CASE 1	CHANGE* (percent)
1.	Total Random Failure, Maintenance, and Test	1.21E-04 (69.1%)	3.80E-04 (60.7%)	57.4	8.95E-06 (14.3%)	2.21E-05 (8.2%)	6.4
1A.	Relays and Logic Cabinets	8.00E-06 (4.6%)	1.70E-05 (2.7%)	2.0	8.00E-06 (12.8%)	1.70E-05 (6.3%)	4.3
1B.	Analog Channels	1.13E-04 (64.5%)	3.63E-04 (58.0%)	55.4	9.24E-07 (1.5%)	5.32E-06 (1.9%)	2.1
2.	Common Mode Failure: Relays and Logic	3.85E-05 (22.0%)	2.31E-04 (36.9%)	42.7	3.85E-05 (61.6%)	2.31E-04 (86.2%)	93.7
3.	Common Mode Failure: Analog Channels	1.50E-05 (8.6%)	1.50E-05 (2.4%)	0.0	1.50E-05 (24.0%)	1.50E-05 (5.6%)	0.0
4.	Total	1.75E-04	6.26E-04	100.0	6.25E-05	2.68E-04	100.0

Based on: Steam Generator Level High-High.

Note: First value of each set listed is unavailability.
Second value of each set listed is percent contribution to total unavailability.

* Percent change of total unavailability change from Base Case to Case 1.

TABLE 3.6-14

SUMMARY OF UNAVAILABILITY CONTRIBUTIONS: SOLID STATE SYSTEMS

Safety Injection and Containment Spray and Phase B Isolation

		UNAVAILABILITY CONTRIBUTIONS					
		2/3 ANALOG CHANNEL LOGIC			2/4 ANALOG CHANNEL LOGIC		
		BASE CASE	CASE 1	CHANGE* (percent)	BASE CASE	CASE 1	CHANGE* (percent)
1.	Total Random Failure, Maintenance, and Test	2.21E-04 (20.3%)	1.14E-05 (19.7%)	19.6	1.09E-04 (11.2%)	7.80E-04 (14.4%)	15.1
1A.	Relays and Logic Cabinets	1.08E-04 (9.9%)	7.74E-04 (13.4%)	14.2	1.08E-04 (11.1%)	7.74E-04 (14.3%)	15.0
1B.	Analog Channels	1.13E-04 (10.4%)	3.63E-04 (6.3%)	5.3	9.26E-07 (0.1%)	5.32E-06 (0.1%)	0.1
2.	Common Mode Failure: Relays and Logic	8.50E-04 (78.0%)	4.63E-03 (80.1%)	80.6	8.50E-04 (87.3%)	4.63E-03 (85.4%)	85.0
3.	Common Mode Failure: Analog Channels	1.50E-05 (1.4%)	1.50E-05 (0.3%)	0.0	1.50E-05 (1.5%)	1.50E-05 (0.3%)	0.0
4.	Total	1.09E-03	5.78E-03	100.0	9.74E-04	5.42E-03	100.0

Based on: Pressurizer Pressure Low interlocked with P11 (2/3).

Note: First value of each set listed is unavailability.
Second value of each set listed is percent contribution to total unavailability.

* Percent change of total unavailability change from Base Case to Case 1.

TABLE 3.6-15

SUMMARY OF UNAVAILABILITY CONTRIBUTIONS: SOLID STATE SYSTEMS

Steamline Isolation, Main Feedwater Isolation, and Auxiliary Feedwater Pump Start

		UNAVAILABILITY CONTRIBUTIONS					
		2/3 ANALOG CHANNEL LOGIC			2/4 ANALOG CHANNEL LOGIC		
		BASE CASE	CASE 1	CHANGE* (percent)	BASE CASE	CASE 1	CHANGE* (percent)
1.	Total Random Failure, Maintenance, and Test	1.55E-04 (32.4%)	7.11E-04 (30.3%)	29.7	4.29E-05 (11.7%)	3.53E-04 (17.7%)	19.0
1A.	Relays and Logic Cabinets	4.20E-05 (8.8%)	3.48E-04 (14.8%)	16.4	4.20E-05 (11.4%)	3.48E-04 (17.4%)	18.7
1B.	Analog Channels	1.13E-04 (23.6%)	3.63E-04 (15.4%)	13.3	9.26E-07 (0.3%)	5.32E-06 (0.3%)	0.3
2.	Common Mode Failure: Relays and Logic	3.09E-04 (64.5%)	1.63E-03 (69.4%)	70.6	3.09E-04 (84.2%)	1.63E-03 (81.9%)	80.9
3.	Common Mode Failure: Analog Channels	1.50E-05 (3.1%)	1.50E-05 (0.6%)	0.0	1.50E-05 (4.1%)	1.50E-05 (0.8%)	0.0
4.	Total	4.79E-04	2.35E-03	100.0	3.67E-04	2.00E-03	100.0

Based on: Steamline Pressure Low.

Note: First value of each set listed is unavailability.
Second value of each set listed is percent contribution to total unavailability.

* Percent change of total unavailability change from Base Case to Case 1.

TABLE 3.6-16

EFFECT OF ANALOG CHANNEL DIVERSITY ON ESF FEATURE UNAVAILABILITY

CASE	WITHOUT DIVERSITY		WITH DIVERSITY		UNAVAILABILITY CHANGE
	ESF FEATURE UNAVAIL.	ANAL. CHAN. CONTRIBUTION	ESF FEATURE UNAVAIL.	ANAL. CHAN. CONTRIBUTION	
1. Relay and Solid State Systems with 2/4 Analog Channel Logic	2.68E-04	5.32E-06 2%	2.63E-04	Small Small	-2%
2A. Relay and Solid State Systems with 2/3 Analog Channel Logic except MFWI and AFWPS Features (channels high contributor)	2.35E-03	3.63E-04 15%	1.99E-03	Small Small	-15%
2B. Relay and Solid State Systems with 2/3 Analog Channel Logic except MFWI and AFWPS Features (channels low contributor)	5.78E-03	3.63E-04 6%	5.42E-03	Small Small	-6%
3. Relay Systems with 2/3 Analog Channel Logic - MFWI and AFWPS Features only	6.26E-04	3.63E-04 58%	2.63E-04	Small Small	-58%

Note: Values correspond to Case 1 conditions.

3.6.2 ESF SIGNAL UNAVAILABILITY SENSITIVITY STUDY

Tables 3.6-17 and 3.6-18 give the unavailabilities for the relay and solid state ESF protection systems, respectively, with and without common mode failure, for the sensitivity studies. The purpose of the sensitivity study is twofold. The first is to determine if any of the testing parameters are driving the system unavailability, and the second is to estimate unavailabilities for alternate conditions. Both studies considered changes to only the master and slave relay test intervals and times. It was previously indicated that these components dominate the system unavailabilities.

The relay protection system sensitivity study is based on Safety Injection signal from "Low Steamline Pressure (2/3) Interlocked with P-12 (2/4)". The results with common mode failure indicate:

1. Master relay test interval - negligible effect on ESF unavailability.

2. Master relay test time - negligible effect on ESF unavailability.

3. Slave relay test interval - significant effect on ESF unavailability. As the test interval increases the unavailability increases.

4. Slave relay test time - negligible effect on ESF unavailability.

As mentioned previously, the common mode failure dominates the ESF system unavailability. Since the common mode failure is strongly driven by the slave relay test interval this type of unavailability response to parameter changes is expected.

The unavailability trends for the results without common mode failure are not as obvious. The majority of the changes are small. In general, it appears that the master and slave relay test intervals are driving the ESF unavailability. Interestingly, they effect the unavailability in opposite

directions. That is, as the master relay test interval increases, the unavailability decreases, but as the slave relay test interval increases, the unavailability increases. As mentioned previously, the test interval effects the unavailability through component random failures and testing. In the cases analyzed, the system unavailability decrease, related to the master relay test interval increase, is driven by testing. Whereas, the system unavailability increase, related to slave relay test interval increase, is driven by random failures.

The solid state protection system study was based on a Safety Injection signal from "Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3)". In general, the solid state system unavailability responds similarly to the relay system. That is, increasing the slave relay test interval has the most significant effect on the ESF system unavailability with and without common mode failure. One difference is apparent. As the master relay test interval increases the unavailability, without common mode failure, does not decrease.

Based on these observations, the master relay test interval and test time and the slave relay test time may be increased without a significant effect on the ESF system unavailability. But, increasing the slave relay test interval significantly increases the ESF system unavailability. A factor of 2 increase in the slave test interval increases the ESF system unavailability by nearly a factor of 2. Note that these conclusions apply only to the parameter range analyzed in this study. Also note that the relay design Feedwater Isolation and Auxiliary Feedwater Pump Start systems contain only one relay (not a master/slave design). For the purposes of this discussion, this relay should be considered a slave.

TABLE 3.6-7

SENSITIVITY STUDY RESULTS
ESF RELAY PROTECTION SYSTEM UNAVAILABILITY

CASE	MASTER RELAY		SLAVE RELAY		UNAVAILABILITY	
	Interval (month)	Time (hour)	Interval (month)	Time (hour)	w/o CMF	w/CMF
SS1	2	8	3	6	5.2E-04	1.3E-03
SS2	2	8	6	12	5.4E-04	2.0E-03
SS3	2	8	9	12	5.4E-04	2.7E-03
SS4	2	8	12	12	5.5E-04	3.4E-03
SS5	2	8	18	12	5.7E-04	4.8E-03
SS6	3	8	3	6	4.8E-04	1.3E-03
SS7	3	8	6	12	5.0E-04	2.0E-03
SS8	3	8	9	12	4.9E-04	2.7E-03
SS9	3	8	12	12	5.0E-04	3.4E-03
SS10	3	8	18	12	5.2E-04	4.8E-03
SS11	4	8	3	6	4.7E-04	1.3E-03
SS12	4	8	6	12	4.8E-04	2.0E-03
SS13	4	8	9	12	4.8E-04	2.7E-03
SS14	4	8	12	12	4.8E-04	3.4E-03
SS15	4	8	18	12	5.0E-04	4.8E-03
SS16	1	3	6	12	5.1E-04	2.0E-03
SS17	1	3	9	12	5.1E-04	2.6E-03
SS18	1	3	12	12	5.2E-04	3.3E-03
SS19	1	3	18	12	5.4E-04	4.8E-03

Based on: Safety injection on Low Steamline Pressure (2/3) Interlocked with P-12 (2/4).

TABLE 3.6-18

SENSITIVITY STUDY RESULTS
ESF SOLID STATE PROTECTION SYSTEM UNAVAILABILITIES

CASE	MASTER RELAY		SLAVE RELAY		UNAVAILABILITIES	
	Interval (month)	Time (hour)	Interval (month)	Time (hour)	w/o CMF	w/CMF
SS1	3	4	9	4	6.4E-04	3.0E-03
SS2	3	4	12	4	7.1E-04	3.7E-03
SS3	3	4	6	4	5.6E-04	2.2E-03
SS4	2	1.5	9	4	6.0E-04	2.9E-03
SS5	2	1.5	12	4	6.5E-04	3.6E-03
SS6	2	1.5	6	4	5.2E-04	2.1E-03
SS7	6	4	9	4	6.5E-04	3.2E-03
SS8	6	4	12	4	7.1E-04	4.0E-03
SS9	6	4	6	4	5.7E-04	2.4E-03

Based on: Safety injection on Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3).

3.6.3 RISK ANALYSIS RESULTS

Figures 3-4 and 3-5 illustrate the core melt frequency and Man-REM exposure, respectively, as functions of the ESF unavailability. These values are based on the Millstone Unit 3 PSS and the Safety Injection signal on "Low Pressurizer Pressure (2/4) Interlocked with P-11 (2/3)" as discussed in Section 3.4. This signal is considered representative of signals from all features including the MFWI and AFWPS features of the relay protection system if the single relay is considered a slave. These curves are based on four different test and maintenance conditions. The ESF unavailabilities that correspond to these conditions are given in Table 3.6-19. Diversity of the analog channels, as previously discussed, does not have a significant effect on the majority of the ESF signal unavailabilities. Therefore, it is acceptable in the study to equate the unavailabilities calculated for the signals listed in Tables 3.1-2 and 3.1-3 (single source signal) with unavailabilities including diversity.

Increases in core melt frequency and Man-REM exposure of 15% and 70% are calculated due to changing the technical specification test and maintenance parameters to Case 1 conditions. The core melt frequency increase is relatively small due to modeling of recovery actions following an initiating event. The dominant contributors to the increase in core melt frequency are the Steam Generator Tube Rupture and the Steamline Break Outside Containment initiating events in conjunction with failure of both ESF trains. Neither of these states are amenable to ESF recovery actions. The third largest contributor is the Loss of Offsite Power event also in conjunction with failure of both ESF trains. Again, this state is not amenable to recovery actions. These three states account for approximately 70% of the core melt frequency increase. The increase in Man-REM exposure is related to transient and small LOCA early core melt plant damage states without containment cooling. Loss of containment cooling inhibits accident mitigation.

Several alternate cases for test and maintenance parameter relaxation were considered. They are:

A1. Relaxation of only analog channel parameters to Case 1 conditions.

A2. Relaxation of analog channel, logic cabinet, and master relay parameters to Case 1 conditions (i.e., relaxation of all parameters to Case 1 conditions except for leaving the slave relay test interval at the Base Case condition.)

A3. Relaxation of all parameters to Case 1 conditions except for increasing the slave relay test interval to 6 months.

A4. Relaxation of all parameters to Case 1 conditions except for increasing the slave relay test interval to 9 months.

A5. Relaxation of all parameters to Case 1 conditions except for increasing the slave relay test interval to 12 months.

These particular alternatives were chosen based on several factors: 1) the negligible contribution of analog channels to signal unavailability, 2) the relatively small contribution of master relay and logic cabinet test and maintenance parameters, and slave relay test and maintenance time to signal unavailability, and 3) the correlation between signal unavailability and slave relay test interval.

Table 3.6-20 summarizes the results for the alternate cases.

Previously it was shown that increasing only the analog channel test and maintenance parameters to Case 1 conditions (Case A1) increased the ESF signal unavailability by less than 0.5%. Figures 3-4 and 3-5 indicate that corresponding increases to the core melt frequency and Man-REM exposure are also negligible.

For Case A2, increasing all parameters to Case 1 values except for the slave relay test interval which is set at the Base Case value, the unavailability increases by 15%. This gives increases of 0.6% and 3 Man-REM for the core melt frequency and Man-REM exposure, respectively. Both increases are within the uncertainties of the PSS.

Cases A3, A4, and A5, and also Case 1 are all identical to Case A2 except for increased slave relay test intervals. Table 3.6-20 indicates that increases in unavailability, core melt frequency, and exposure of up to a factor of 5, 16%, and 84 Man-REM, respectively, were obtained when all testing and maintenance parameter were changed to Case 1.

As stated in Section 3.1 (Methodology) these results should be viewed on a relative basis and the sensitivity or dependence of the plant safety and operability to the testing and maintenance parameters is what should be considered. It has been demonstrated that plant safety and operability is insensitive to the testing and maintenance parameters of the analog channels, logic cabinets, and master relays in addition to the maintenance and testing time of the slave relays. Therefore, relaxation of these parameters can be justified.

TABLE 3.6-19

ESF UNAVAILABILITIES APPLIED IN THE RISK ANALYSIS

ESF STATE	BASE CASE*	CASE 1*	(2) CASE A**	(3) CASE B**
ESF trains A and B available***	9.78E-01	9.39E-01	9.52E-01	9.43E-01
ESF train A available and train B unavailable	1.04E-02	2.78E-02	2.27E-02	2.66E-02
ESF train B available and train A unavailable	1.04E-02	2.78E-02	2.27E-02	2.66E-02
ESF trains A and B unavailable	9.70E-04	5.41E-03	2.08E-03	3.68E-03

* - See Table 3.1-1 for associated testing and maintenance parameters.

** - No particular testing and maintenance parameters associated with these cases - see the Sensitivity Study for cases which match the unavailabilities.

*** - Availability = 1 - Total System Unavailability

TABLE 3.6-20

SUMMARY OF ANALYSIS FOR ALTERNATE TEST AND MAINTENANCE CONDITIONS

CASE*	ESF UNAVAILABILITY	ESF UNAVAILABILITY INCREASE (%)	CORE MELT FREQUENCY INCREASE (%)	MAN-REM EXPOSURE INCREASE
A1	9.7E-04	Negligible	Negligible	Negligible
A2	1.1E-03	15	0.6	3
A3	2.4E-03	150	5.1	27
A4	3.2E-03	230	8.1	42
A5	4.0E-03	310	10.8	57
Case 1	5.4E-03	460	16.0	84

* Case descriptions are defined in Section 3.6.3.

FIGURE 3-4

CORE MELT FREQUENCY INCREASES AS
A FUNCTION OF ESF UNAVAILABILITY

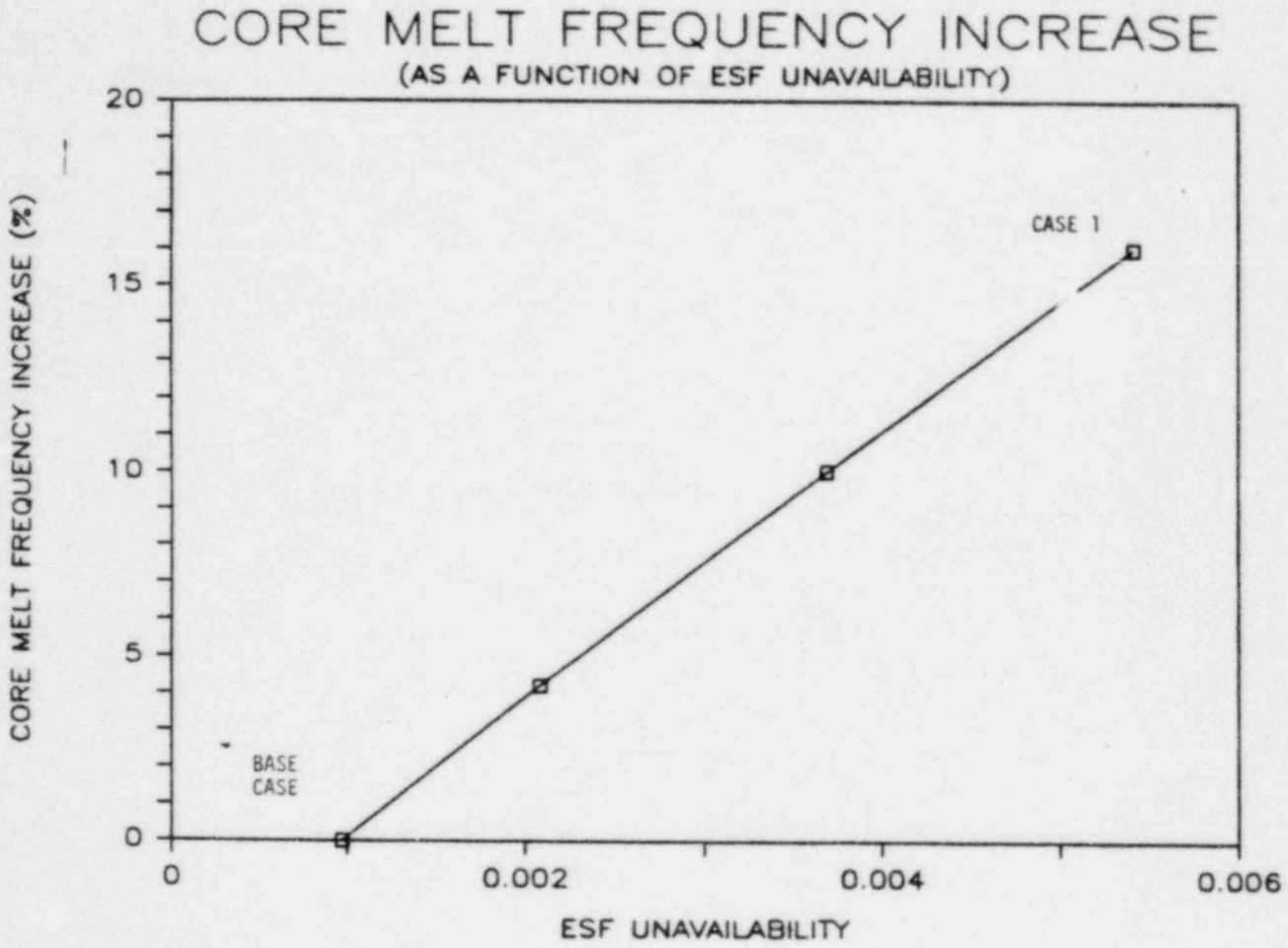
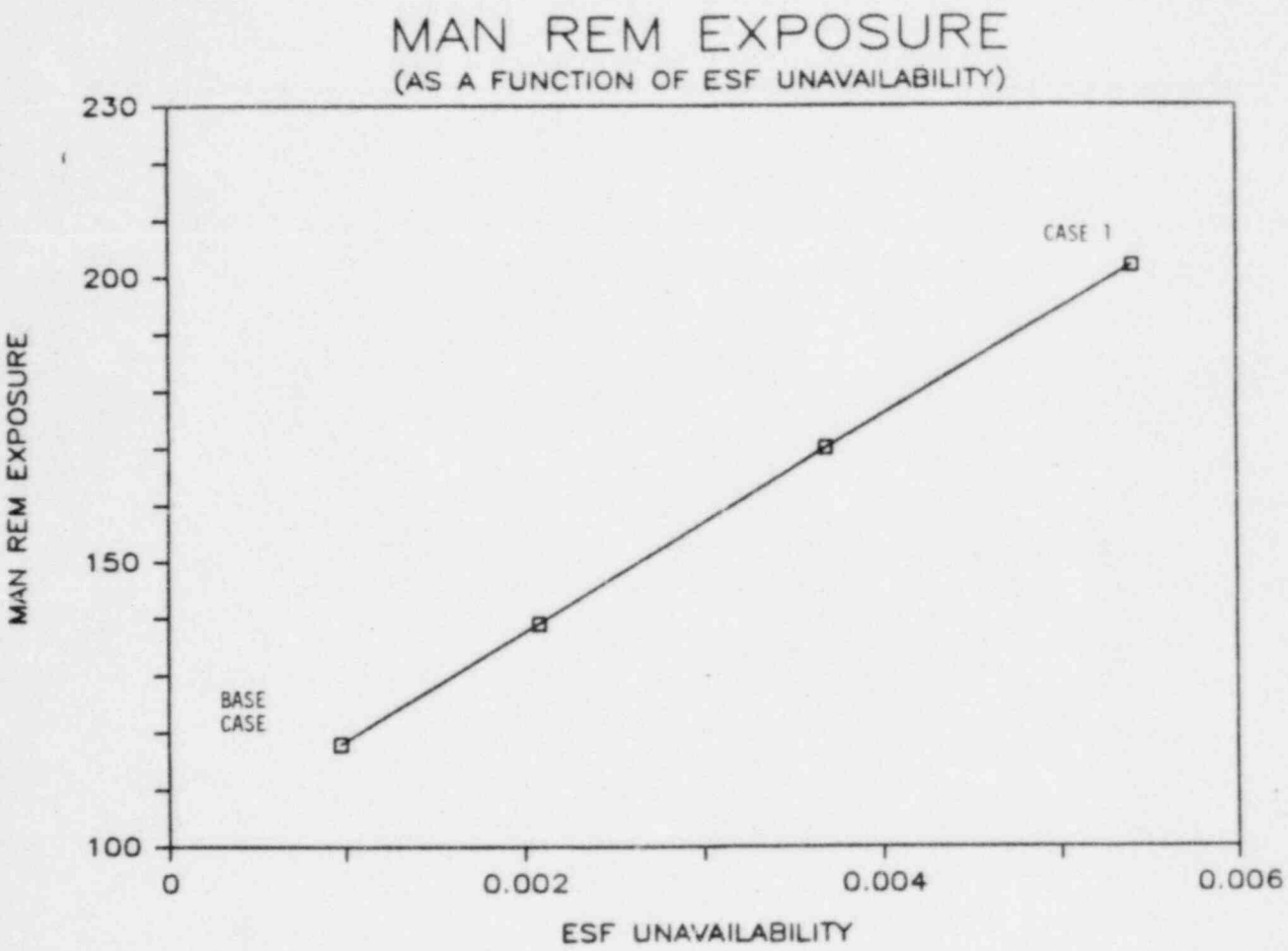


FIGURE 3-5

MAN-REM EXPOSURE AS A
FUNCTION OF ESF UNAVAILABILITY



3.6.4 MARKOV RESULTS

The Markov analysis was based on the Steamline Isolation on Steamline Pressure Low (2/3) Interlocked with P11 (2/3) feature of the solid state ESF. Unavailabilities were calculated for four testing schemes; 1) Base Case, 2) Case 1, 3) Case 1 with staggered testing, and 4) Case A2. The testing parameters for the Base Case and Case 1 are given on Table 3.1-1. Case A2 is described in Section 3.6.3. Case 1 with staggered testing applies the Case 1 testing parameters, but on a staggered basis. That is, the supercomponents that perform the same function in opposite trains are tested at the same intervals, but their test dates are staggered by the test interval divided by the number of supercomponents performing similar functions.

Table 3.6-21 summarizes the average unavailabilities for these cases as calculated by the Markov and fault tree methods. Also listed are the percent increases in unavailability from the Base Case to the other cases. The results from the two methods are in good agreement. The Markov results are lower since this method does not account for unavailabilities due to testing (testing is assumed to be instantaneous) and maintenance. Exponential failure rates as opposed to linear approximations also add to this difference. The increase in unavailability from the Base Case to Case 1 and Case A2 are also in agreement between the two methods. The increase in unavailability to Case A2 for the fault tree method is based on the Safety Injection feature (as presented in Section 3.6.3). This illustrates that the trends and magnitude of changes expected are in agreement by the two methods. Case 1 with staggered test is included to illustrate the potential effect of incorporating a staggered testing plan. The test intervals are identical to those used in Case 1. These results indicate a much smaller increase in unavailability for the staggered schedule.

Figure 3.6 shows the unavailability as a function of time for the Base Case, Case 1, and Case A2. The step changes (peak to valley transitions) are due to testing of a supercomponent or set of supercomponents. This figure shows three complete testing cycles for the Base Case and Case A2 and one complete testing cycle for Case 1. After each complete cycle the system unavailability is essentially zero. The Base Case, which has the largest amount of testing,

has the lowest unavailability and Case 1, with the least testing, has the highest unavailability. Again, this indicates that the trends and changes in unavailabilities for the various cases are in agreement with the fault tree analysis.

Figure 3.7 shows the unavailability as a function of time for Case 1 and Case 1 with staggered testing. Both cases have equal testing, but the staggered testing case does not attain unavailabilities equal to those in the standard testing case.

The following is concluded from the Markov analysis:

1. The average unavailabilities calculated by the Markov method are lower than the fault tree method primarily due to the treatment of testing and maintenance, and exponential as opposed to linear failure rate assumptions.

2. The Markov analysis results are in agreement with the fault tree results in terms of absolute value (considering conclusion #1) and in trends.

3. Staggered testing decreases the average unavailability of the system even though the amount of testing remains the same.

TABLE 3.6-21

MARKOV/FAULT TREE ESF UNAVAILABILITY COMPARISON

CASE*	FAULT TREE METHOD		MARKOV METHOD	
	UNAVAILABILITY	INCREASE (%)	UNAVAILABILITY	INCREASE (%)
Base Case	4.8E-04	-	2.9E-04	-
Case 1	2.4E-03	400	1.7E-03	490
Case A2	5.5E-04	15	3.7E-04	28
Case 1 with staggered testing	-	-	5.4E-04	86

* Case descriptions are defined in Section 3.6.3

Note: The comparison is based on the solid state ESF Steamline Isolation on Steamline Pressure Low (2/3) Interlocked with P11 (2/3).

FIGURE 3.6

ESF UNAVAILABILITY: STEAMLINE ISOLATION

BASE CASE, CASE 1, CASE A2

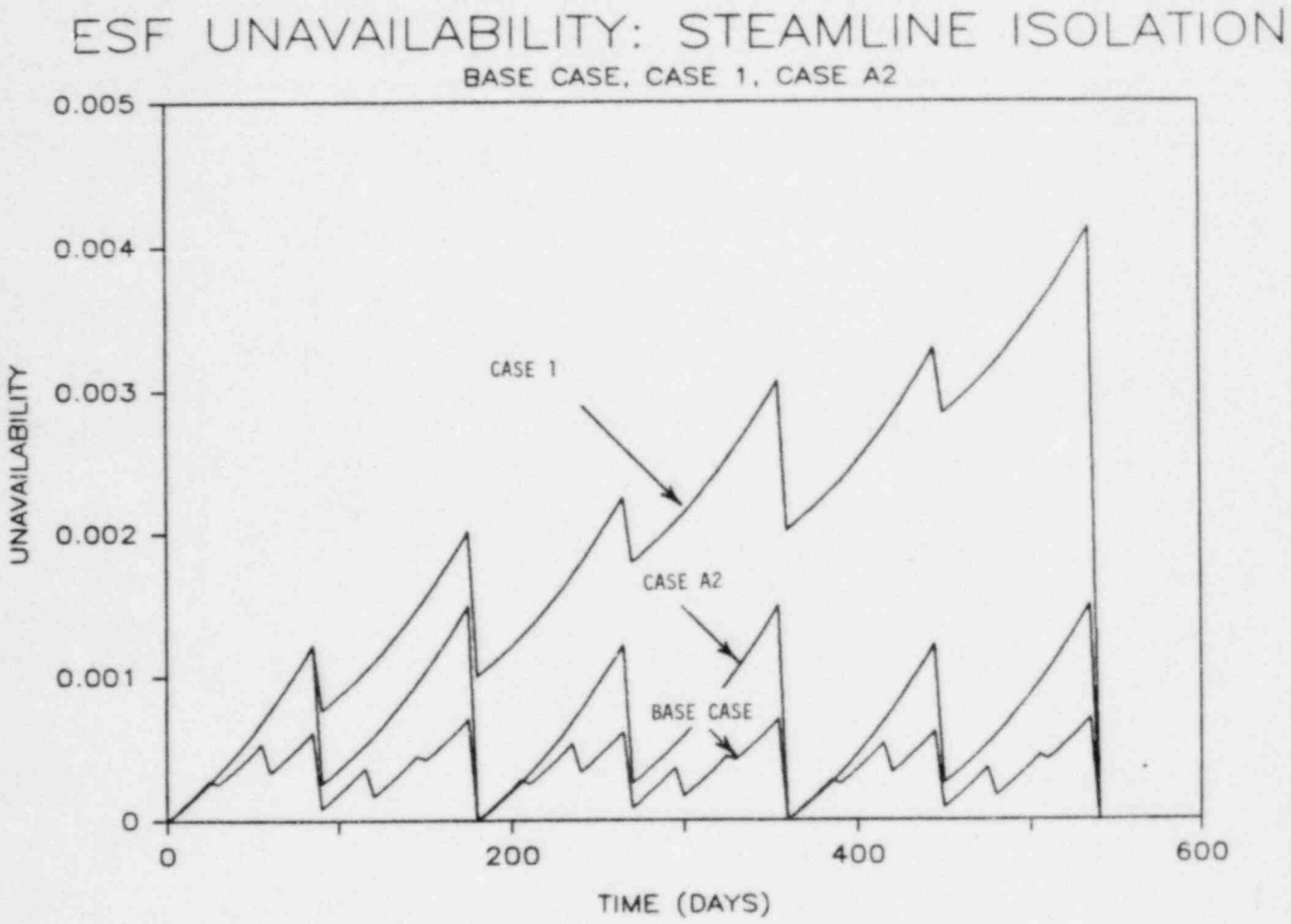
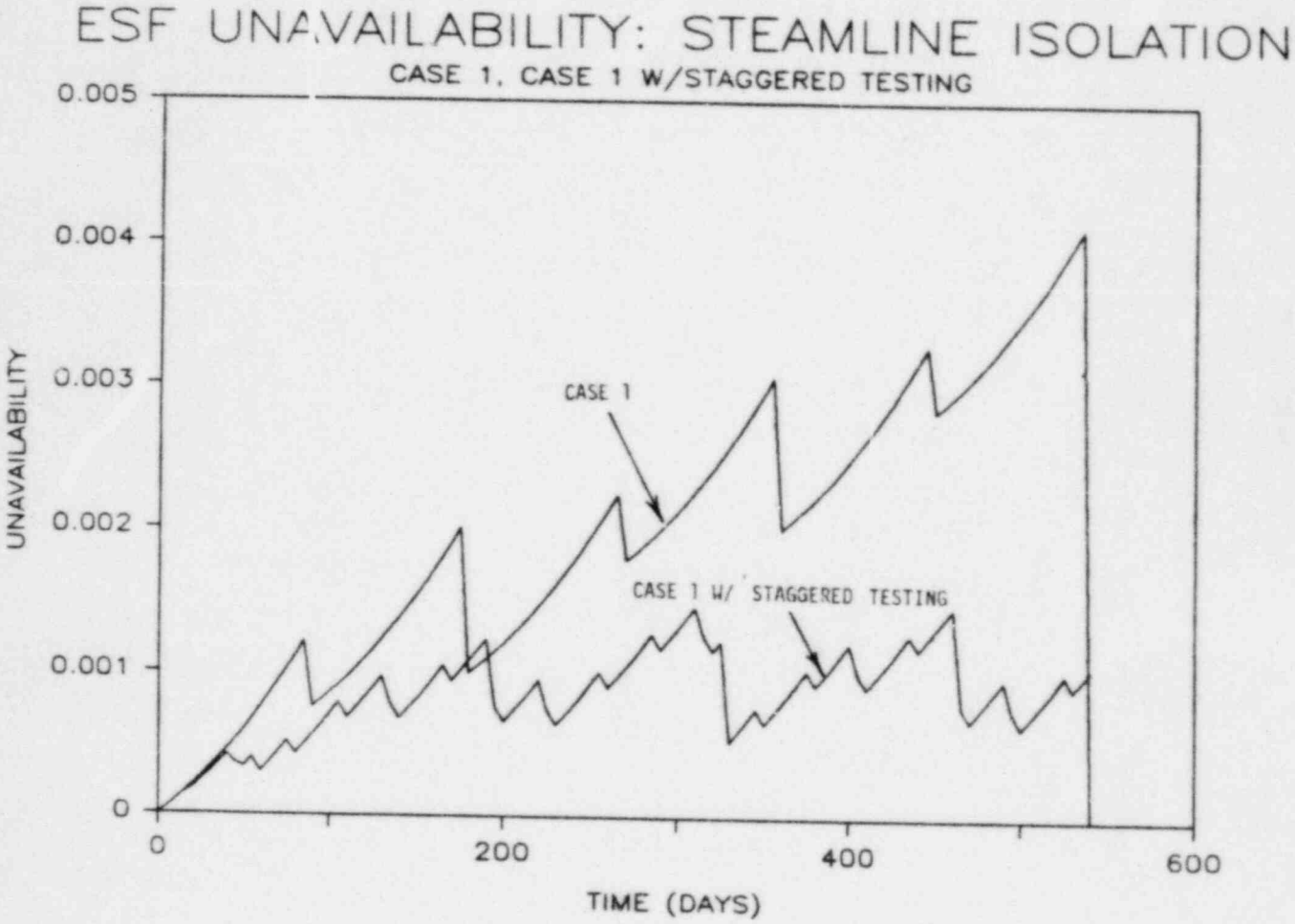


FIGURE 3.7

ESF UNAVAILABILITY: STEAMLINE ISOLATION
CASE 1, CASE 1 w/ STAGGERED TESTING



4.0 SUMMARIZATION OF IMPACT OF INCREASING SURVEILLANCE INTERVALS AND OUTAGE TIMES FOR THE ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

The foregoing sections of this report have documented an evaluation of increased surveillance intervals and outage times for the ESFAS. The purpose of this evaluation is to provide a justification for desired changes to test and maintenance practices considered to be beneficial to operating utilities. This section of the report summarizes the changes and the impact and benefits of implementing the changes.

4.1 INCREASED SURVEILLANCE INTERVALS

It is proposed that analog channel testing be conducted quarterly as opposed to the current monthly requirement, logic cabinets be tested semiannually on a staggered test bases as opposed to current monthly or once per two month intervals, and master relays be tested semiannually on a staggered test bases as opposed to current monthly or once per two month intervals. These changes are illustrated in standard technical specification format in Appendix A1. The basis for these changes are:

a. The general insensitivity of ESF feature unavailability to failures in the analog channels as shown in Section 3.6.1.

b. The general insensitivity of the ESF feature unavailability to failures in the actuation logic and master relay components as shown in Section 3.6.2.

c. The generally insignificant increase in the core melt frequency and man-rem exposure when the Case 1 relaxation for all ESF instrumentation except the slave relays are assumed in the risk analysis presented in Section 3.6.3. In Table 3.6-20 the predicted ESF unavailability increase is 15%, the core melt frequency increase is 0.6% and the man-rem exposure increase is 3 man-rem.

The summary of results presented in Table 3.6-20 indicates that the ESF unavailability is sensitive to the slave relay test interval. This result indicates that ESF unavailability may be lower for plants where slave relay testing occurs more frequently. This is not to be construed to imply that plants performing slave relay testing at an 18 month interval have an unacceptable ESF unavailability. Assessment of the acceptability of a specific value of ESF unavailability can only be made in conjunction with the application of some criteria such as the proposed safety goal. Such an assessment has not been made in connection with, nor included in this report. Until an absolute limit on safety system unavailability or a related parameter is quantified, the justification for surveillance test interval relaxations can only be based on the relative increase in unavailability from the base case. It is on this basis that the recommendations in this report are made.

As stated in Section 3.3.2, the reliability model of the slave relay does not include a human error contributor to unavailability. This contributor to ESF unavailability was not modeled due to the lack of data necessary to quantify the fault tree. Most plants licensed prior to 1951 test slave relays during refueling outages, not at power. The relatively few instances of testing slave relays at power from which a human error probability could be calculated are insufficient to constitute a statistically significant sample. Had sufficient data been available, it is expected that the sensitivity to slave relay test internal identified by the evaluation described in this report would have been measurably less, lending credence to the acceptability of increasing the slave relay test internal to 18 months for plants which currently test more frequently than that.

In Section 4.1.1 of Supplement 1 to WCAP-10271 (Ref. 4) expected benefits to the plant due to increasing the surveillance test interval are discussed. Human factors considerations and the impact of the increased surveillance test interval on hardware failure rates is also discussed. The discussion of the benefits of increasing the analog channel surveillance test interval in Ref. (4) is equally applicable to the ESF analog channels in this report.

4.2 INCREASED TEST AND MAINTENANCE TIMES

It is proposed that allowable test times specified for EFS instrumentation be extended from 2 hours to 4 or 8 hours for solid state and relay systems respectively and that maintenance times be extended up to 12 hours. For analog channels, the first 6 hours of maintenance would be accomplished with the channel in a bypass condition. Thereafter, the channel must be tripped.

Logic cabinets and the master and slave relays may be bypassed for 12 hours for maintenance. These changes are shown in the ACTION statements of Table 3.3-3 of Appendix A. The basis for these changes are:

a. The results of the fault tree reliability and risk analysis in which increased test and maintenance times were evaluated are considered to be acceptable. See paragraph 4.1 above.

b. Section 4.2.4 of WCAP-10271 points out that the times currently allowed by technical specifications for testing and maintenance are insufficient to accomplish the necessary work. The test and maintenance times proposed in Case 1 in Section 3.1 above have been identified as being more representative of actual conditions. Section 5.2 of WCAP-10271 discusses the impact of increasing test and maintenance times to more realistic values. If more time is allowed to test and maintain equipment a potential exists for reducing error and improving equipment reliability.

4.3 EQUIPMENT BYPASS

It is proposed that testing be accomplished in bypass and that the first 6 hours of analog channel maintenance be accomplished in bypass. These changes are shown in the ACTION statements of Table 3.3-3 of Appendix A. The basis for these changes are:

a. The results of the fault tree reliability and risk analysis in which testing and maintenance in bypass were evaluated are considered to be acceptable. See paragraph 4.1 above and Section 4.3.2 of WCAP-10271.

b. Section 3.3 and Section 5.1 of WCAP-10271 discuss the impact of performing test and maintenance in bypass. It was concluded that bypassing equipment during test and maintenance would minimize or eliminate partial trip operation which could result in 1 less inadvertent reactor trip per year at a two unit site. This constitutes a reduction in unnecessary transients and challenges to the protection systems and improves plant availability. Section 5.3 of WCAP-10271 discusses plant availability.

c. IEEE Standard 279 paragraph 4.11 recognizes the use of availability arguments for justifying equipment bypass. Though this paragraph deals with 1 of 2 systems, the same philosophy is equally applicable to 2 of 3 and 2 of 4 systems.

4.4 MODIFICATIONS AND DELETIONS OF ACTION STATEMENTS

ACTION statements in Table 3.3-3 of Appendix A have been modified or deleted in order to best implement the proposed technical specification changes. The time to place an analog channel in trip was changed from 1 to 6 hours to allow testing and maintenance in bypass. Test times specified in the technical specifications were changed from 2 hours to 4 to 8 hours to allow increased time for testing. These changes have been discussed in previous sections of this report. The change that has not been discussed is deletion of Action 15. This change is discussed in the following paragraph.

a. Action 15 - Action 15 is applicable to 2 of 3 logic combinations. It allows operation with a channel inoperable provided the channel is in trip until surveillance of a redundant channel is due. With the capability to perform surveillance tests in bypass, as justified by this analysis, the retrictions imposed by ACTION 15 are no longer required and ACTION #20 can be applied.

5.0 CONCLUSIONS

An evaluation of the impact of implementing the technical specification revisions proposed in Appendix A1 for ESF instrumentation has been completed. The results of these evaluations show that the impact on the ESF system is minimal, while the benefits to the operating utilities are large. The reliability of the ESF system remains high, plant safety is maintained, and the burden on the utility caused by technical specification compliance is significantly reduced. An improvement in plant availability would also be expected, due to less frequent surveillance testing. The acceptability of the proposed revisions has been demonstrated. WCAP-10271 and this supplement provide sufficient justification to allow revision of plant specific technical specification requirements on ESF instrumentation.

6.0 REFERENCES

1. "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", ANS and IEEE, NUREG/CR-2300, January, 1983.

2. "Graphic Fault Tree Editor (GRAFTER) User's Manual", Chismar, S. A. and Sharp, D. R., Westinghouse Nuclear Technology Division, December 31, 1981.

3. "WAMCUT, A Computer Code for Fault Tree Evaluation", Erdmann, R. C., Science Applications, Inc., NP-803, June 1978.

4. WCAP-10271, "Evaluation of Surveillance Frequencies and Out-of-Service Times for the Reactor Protection Instrumentation System", Jansen, R. L., Lijewski, L. M., and Masarik. R. J., January 1983. Westinghouse Proprietary Class 2. WCAP-10271 Supplement 1, "Evaluation of Surveillance Frequencies and Out-of-Service Times for the Reactor Protection Instrumentation System", Jansen, R. L., Lijewsku, L. M., Masarik, R. J., Moomau, W. H., July 1983. Westinghouse Proprietary Class 2.

5. "Millstone Unit 3 Probabilistic Safety Study", Westinghouse Electric Corporation, August 1983.

6. "ARBRE - An Event Tree Analysis Program", Chismar, S. A., WCAP-10010, Westinghouse Electric, Corporation, December 1981.

7. "Verification of Computer Code PHIM", Leonelli, K., Westinghouse Calculation Note, CN-PRA-83-114, January 2, 1985.

8. "BORIS - A Code to Document PRA Output in Matrix Format", Chismar, S. A. and Sancaktar, S., Westinghouse Electric Corporation, April 1982.

9. IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Generating Stations".

10. IEEE Standard 338-1977, "Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems".

11. IEEE Standard 352-1975, "Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems".

12. WCAP-7550, "Reactor Protection Logic System Design Review", W. C. Gangloff, August 1970. Westinghouse Proprietary Class 2.

13. WCAP-7672, "Solid State Logic Protection System Description", Katz, D. N., June 1971. Westinghouse Proprietary Class 3 (Non-Proprietary).

14. WCAP-7705, "Testing of Engineered Safety Features Actuation System", Swogger, J. W., May 1976. Westinghouse Proprietary Class 3 (Non-Proprietary).

15. WCAP-7706-L, "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients", Gangloff, W. C. and Loftus, W. D., July 1971. Westinghouse Proprietary Class 2.

16. WCAP-7913, "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems", Reid, J. B., January 1973. Westinghouse Proprietary Class 3 (Non-Proprietary).

17. WCAP-7488-L, "Solid State Protection System Description", Katz, D. N., January 1971. Westinghouse Proprietary Class 2.

18. Process Instrumentation and Control Equipment Reference Manuals for Various Westinghouse Plants.

19. Westinghouse Nuclear Energy System, Nuclear Technology Division, Solid State Protection System Technical Manual.

20. Engineered Safety Feature Cabinet Drawings for Various Westinghouse Plants.

21. Functional Logic Diagrams for Various Westinghouse Plants.

22. Papazoglou, I. A. and Gyftopoulos, E. P., "Markov Processes for Reliability Analyses of Large Systems", IEEE Trans. Reliability, R-26, 232, 1977.

23. Papazoglou, I. A. and Cho, N. Z., "Review and Assessment of Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System", BNL-NUREG-51780, Draft Copy, April 1984.

24. IEEE-500, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, 1983.

25. MIL-HDBK-217D, Military Handbook Reliability Prediction of Electronic Equipment, 1979.

26. Westinghouse Reliability Data Base (Proprietary)

27. WASH-1400: Reactor Safety Study

28. Green and Bourne, "Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors, Part 3,", AHSB(S) R117, UKAEA, 1966.

APPENDIX A1
PROPOSED CHANGES TO STANDARD TECHNICAL SPECIFICATIONS

INSTRUMENTATION

3/4.3.2 ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

LIMITING CONDITION FOR OPERATION

3.3.2 The Engineered Safety Feature Actuation System (ESFAS) instrumentation channels and interlocks shown in Table 3.3-3 shall be OPERABLE with their trip setpoints set consistent with the values shown in the Trip Setpoint column of Table 3.3-4 and with RESPONSE TIMES as shown in Table 3.3-5.

APPLICABILITY: As shown in Table 3.3-3.

ACTION:

a. With an ESFAS instrumentation channel or interlock trip setpoint less conservative than the value shown in the Allowable values column of Table 3.3-4, declare the channel inoperable and apply the applicable ACTION requirement of Table 3.3-3 until the channel is restored to OPERABLE status with the trip setpoint adjusted consistent with the Trip Setpoint value.

b. With an ESFAS instrumentation channel or interlock inoperable, take the ACTION shown in Table 3.3-3.

SURVEILLANCE REQUIREMENTS

4.3.2.1 Each ESFAS instrumentation channel and interlock and the automatic actuation logic and relays shall be demonstrated OPERABLE by the performance of the engineered safety feature actuation system instrumentation surveillance requirements specified in Table 4.3-2.

4.3.2.2 The ENGINEERED SAFETY FEATURES RESPONSE TIME of each ESFAS function shall be demonstrated to be within the limit at least once per 18 months. Each test shall include at least one train such that both trains are tested at least once per 36 months and one channel per function such that all channels are tested at least once per N times 18 months where N is the total number of redundant channels in a specific ESFAS function as shown in the "Total No. of Channels" Column of Table 3.3-3.

TABLE 3.3-3

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
1. SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER.					
a. Manual Initiation	2	1	2	1, 2, 3, 4	19
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
c. Containment Pressure-High	3	2	2	1, 2, 3	20*
d. Pressurizer Pressure-Low	4	2	3	1, 2, 3#	20*
e. Differential Pressure Between Steam Lines - High				1, 2, 3##	
1) Four Loop Plant					
Four Loops Operating	3/steam line	2/steam line any steam line	2/steam line		20*
Three Loops Operating	3/operating steam line	1###/steam line any operating steam line	2/operating steam line		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER. (Continued)					
ii) Three Loop Plant					
Three Loops Operating	3/steam line	2/steam line twice and 1/3 steam lines	2/steam line		20*
Two Loops Operating	3/operating steam line	2###/steam line twice in either operating steam line	2/operating steam line		16
f. Steam Flow in Two Steam Lines-High				1, 2, 3##	
i) Four Loop Plant					
Four Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Three Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER. (Continued)					
ii) Three Loop Plant					
Three Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Two Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16
Coincident With Either T_{avg}--Low-Low				1, 2, 3##	
i) Four Loop Plant					
Four Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 3 loops		20*
Three Loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in any two operating loops		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER. (Continued)					
ii) Three Loop Plant					
Three Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 2 loops		20*
Two Loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in operating loop		16
Or, Coincident With Steam Line Pressure-Low				1, 2, 3##	
i) Four Loop Plant					
Four Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 3 loops		20*
Three Loops Operating	1 pressure operating loop	1### pressure in any operating loop	1 pressure in any 2 operating loops		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER (Continued)					
ii) Three Loop Plant					
Three Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 2 loops		20*
Two Loops Operating	1 pressure/ loop	1### pressure in any operating loop	1 pressure any operating loop		16
2. CONTAINMENT SPRAY					
a. Manual	2	1 with 2 coincident switches	2	1, 2, 3, 4	19
b. Automatic Actuation Logic and actuation Relays	2	1	2	1, 2, 3, 4	14
c. Containment Pressure -- High-High	4	2	3	1, 2, 3	17
3. CONTAINMENT ISOLATION					
a. Phase "A" Isolation					
1) Manual	2	1	2	1, 2, 3, 4	19
2) Safety Injection	See 1 for above for all Safety Injection initiating functions and requirements.				

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
CONTAINMENT ISOLATION (continued)					
3) Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
b. Phase "B" Isolation					
1) Manual	2	1 with 2 coincident switches	2	1, 2, 3, 4	19
2) Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
3) Containment Pressure--High-High	4	2	3	1, 2, 3	17
c. Purge and Exhaust Isolation					
1) Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	18
2) Containment Radioactivity-High	4	2	3	1, 2, 3, 4	18
3) Safety Injection	See 1 above for all Safety Injection initiating functions and requirements.				

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION					
a. Manual	1/steam line	1/steam line	1/operating steam line	1, 2, 3	24
b. Automatic Actuation Logic and Actutation Relays	2	1	2	1, 2, 3	22
c. Containment Pressure--High-High	4	2	3	1, 2, 3	17
d. Steam Flow in Two Steam Lines--High				1, 2, 3	
i) Four Loop Plant					
Four Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Three Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16
ii) Three Loop Plant					
Three Loops Operating	2/steam line	1/steam line any 2 steam lines	1/steam line		20*
Two Loops Operating	2/operating steam line	1###/any operating steam line	1/operating steam line		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION (continued)					
Coincident With Either T_{avg}--Low-Low				1, 2, 3	
i) Four Loop Plant					
Four Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 3 loops		20*
Three Loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in any two operating loops		16
ii) Three Loop Plant					
Three Loops Operating	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 2 loops		20*
Two loops Operating	1 T_{avg}/ operating loop	1### T_{avg} in any operating loop	1 T_{avg} in any operating loop		16

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION (continued)					
Or, Coincident With					
Steam Line Pressure-Low				1, 2, 3	
i) Four Loop Plant					
Four Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 3 loops		20*
Three Loops Operating	1 pressure/ operating loop	1### pressure in any operating loop	1 pressure in any 2 operating loops		16
ii) Three Loop Plant					
Three Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 2 loops		20*
Two Loops Operating	1 pressure/ operating loop	1### pressure in any operating loop	1 pressure any operating loop		16
5. TURBINE TRIP & FEEDWATER ISOLATION					
a. Steam Generator Water Level--High-High	3/stm. gen.	2/stm. gen. in any operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2	20*
b. Automatic Actuation Logic and Actuation Relay	2	1	2	1, 2	22

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
6. AUXILIARY FEEDWATER					
a. Manual Initiation	2	1	2	1, 2, 3	23
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3	22
c. Stm. Gen. Water Level-Low-Low					
i. Start Motor-Driven Pumps	3/stm. gen.	2/stm. gen. in any operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2, 3	20*
ii. Start Turbine-Driven Pump	3/stm. gen.	2/stm. gen. in any 2 operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2, 3	20*
d. Undervoltage-RCP Start Turbine-Driven Pump	4-1/bus	2	3	1, 2	20*
e. Safety Injection Start Motor-Driven Pumps and Turbine-Driven Pump	See 1 above for all Safety Injection initiating functions and requirements				
f. Station Blackout Start Motor-Driven Pumps and Turbine-Driven Pump	2	1	2	1, 2, 3	19

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
AUXILIARY FEEDWATER (Continued)					
g. Trip of Main Feedwater Pumps Start Motor-Driven Pumps and Turbine-Driven Pump	2/pump	1/pump	1/pump	1, 2	19
7. AUTOMATIC SWITCHOVER TO CONTAINMENT SUMP					
a. RWST Level - Low	4	2	3	1, 2, 3, 4	17
Coincident With					
Containment Sump Level - High	4	2	3	1, 2, 3, 4	17
And					
Safety Injection	See 1 above for Safety Injection initiating functions and requirements				
b. Automatic Actuation Logic and Actuation Relays	2	1	2	1, 2, 3, 4	14
8. LOSS OF POWER					
a. 4 kv Bus Loss of Voltage	4/Bus	2/Bus	3/Bus	1, 2, 3, 4	20*
b. Grid Degraded Voltage	4/Bus	2/Bus	3/Bus	1, 2, 3, 4	20*

TABLE 3.3-3 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INTERLOCKS					
a. Pressurizer Pressure, P-11	3	2	2	1, 2, 3	21
b. Low-Low T_{avg}, P-12	4	2	3	1, 2, 3	21
c. Reactor Trip, P-4	2	2	2	1, 2, 3	23

TABLE 3.3-3 (Continued)

TABLE NOTATION

Trip function may be blocked in this MODE below the P-11 (Pressurizer Pressure Interlock) setpoint.

Trip function may be blocked in this MODE below the P-12 (Low-Low T_{avg} Interlock) setpoint.

The channel(s) associated with the protective functions derived from the out of service Reactor Coolant Loop shall be placed in the tripped mode.

* The provisions of Specification 3.0.4 are not applicable.

ACTION STATEMENTS

ACTION 14 With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 12 hours and in COLD SHUTDOWN within the following 30 hours; however, one channel may be bypassed for up to 4 (8)* hours for surveillance testing per Specification 4.3.2.1, provided the other channel is OPERABLE.

ACTION 15 Deleted

ACTION 16 With a channel associated with an operating loop inoperable, restore the inoperable channel to OPERABLE status within 6 hours or be in at least HOT STANDBY within the next 6 hours and in at least HOT SHUTDOWN within the following 6 hours. One channel associated with an operating loop may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1.

ACTION 17 With the number of OPERABLE channels one less than the Total Number of Channels, operation may proceed provided the inoperable channel is placed in the bypassed condition and the Minimum Channels OPERABLE requirement is met. One additional channel may be bypassed for up to 4 hours for surveillance testing per Specification 4.3.2.1.

ACTION 18 With less than the Minimum Channels OPERABLE requirement, operation may continue provided the containment purge supply and exhaust valves are maintained closed.

*Time outside parenthesis is SSPS plant, time inside parenthesis is relay logic plant logic cabinets and master relays. Relay logic plant slave relays may be bypassed for 12 hours.

TABLE 3.3-3 (Continued)

ACTION STATEMENTS (Continued)

ACTION 19 With the number of OPERABLE channels one less than the Minimum Channels OPERABLE requirement, restore the inoperable channel to OPERABLE status within 48 hours or be in at least HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours.

ACTION 20 With the number of OPERABLE channels one less than the Total Number of Channels, STARTUP and/or POWER OPERATION may proceed provided the following conditions are satisfied:

a. The inoperable channel is placed in the tripped condition within 6 hours.

b. The minimum channels OPERABLE requirement is met; however, the inoperable channel may be bypassed for up to 4 hours for surveillance testing of other channels per specification 4.3.2.1.

ACTION 21 With less than the Minimum Number of Channels OPERABLE, within one hour determine by observation of the associated permissive annunciator window(s) that the interlock is in its required state for the existing plant condition, or apply Specification 3.0.3.

ACTION 22 With the number of OPERABLE Channels one less than the Minimum Channels OPERABLE requirement, be in at least HOT STANDBY within 6 hours and in at least HOT SHUTDOWN within the following 6 hours; however, one channel may be bypassed for up to 4 (8)* hours for surveillance testing per Specification 4.3.2.1 provided the other channel is OPERABLE.

ACTION 23 With the number of OPERABLE channels one less than the Total Number of Channels, restore the inoperable channel to OPERABLE status within 48 hours or be in at least HOT STANDBY within 6 hours and in at least HOT SHUTDOWN within the following 6 hours.

ACTION 24 With the number of OPERABLE channels one less than the Total Number of Channels, restore the inoperable channel to OPERABLE status within 48 hours or declare the associated valve inoperable and take the ACTION required by Specification (3.7.1.5).

TABLE 4.3-2

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
1. SAFETY INJECTION, REACTOR TRIP FEEDWATER ISOLATION, CONTROL ROOM ISOLATION START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA (1)	SA (1)	Q	1, 2, 3, 4
c. Containment Pressure-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Pressurizer Pressure-Low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
e. Differential Pressure Between Steam Lines-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
f. Steam Flow in Two Steam Lines-High Coincident With Either	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
1. T_{avg} - Low-Low, or	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
2. Steam Line Pressure-Low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
2. CONTAINMENT SPRAY								
a. Manual Initiation	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2, 3, 4
c. Containment Pressure-High-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
3. CONTAINMENT ISOLATION								
a. Phase "A" Isolation								
1) Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
2) Safety Injection	See 1 above for all Safety Injection Surveillance Requirements							
3) Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2, 3, 4
b. Phase "B" Isolation								
1) Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
2) Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2, 3, 4
3) Containment Pressure-High-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
CONTAINMENT ISOLATION (Continued)								
c. Purge and Exhaust Isolation								
1) Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2, 3, 4
2) Containment Radiological-High	S	R	M	N.A.	N.A.	N.A.	N.A.	1, 2, 3, 4
3) Safety Injection	See 1 above for all Injection Surveillance Requirements							
4. STEAM LINE ISOLATION								
a. Manual	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2, 3
c. Containment Pressure-High-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Steam Flow in Two Steam Lines-High Coincident With Either	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
1. T_{avg}- Low-Low or	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
2. Steam Line Pressure-Low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
5. TURBINE TRIP AND FEEDWATER ISOLATION								
a. Steam Generator Water Level-High-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2
b. Automatic Actuation Logic and Actuation Relay	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2
6. AUXILIARY FEEDWATER								
a. Manual	N.A.	N.A	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	SA(1)	SA(1)	Q	1, 2, 3
c. Steam Generator Water Level-Low-Low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Undervoltage - RCP	N.A.	R	N.A.	R	N.A.	N.A.	N.A.	1
e. Safety Injection	See 1 above for all Safety Injection Surveillance Requirements							
f. Station Blackout	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3
g. Trip of Main Feedwater Pumps	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
AUTOMATIC SWITCHOVER TO CONTAINMENT SUMP								
a. RSWT Level-Low Coincident With Containment Sump Level - High and Safety Injection	S	R	M	N.A.	N.A.	N.A.	N.A.	1, 2, 3, 4
	S	R	M	N.A.	N.A.	N.A.	N.A.	1, 2, 3, 4
	See 1 above for all Safety Injection Surveillance Requirements							
b. Automatic Actuation Logic and Actuation Relays	N.A.	N.A.	N.A.	N.A.	M (3)	M (3)	Q	1, 2, 3, 4
8. LOSS OF POWER								
a. 4.16 kV Emergency Bus Undervoltage (Loss of Voltage)	N.A.	R	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4
b. 4.16 kV Emergency Bus Undervoltage (Degraded Voltage)	N.A.	R	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3, 4

TABLE 4.3-2 (Continued)

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
9. ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INTERLOCKS								
a. Pressurizer Pressure, P-11	N.A.	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
b. Low, Low T_{avg}, P-12	N.A.	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
c. Reactor Trip, P-4	N.A.	N.A.	N.A.	R	N.A.	N.A.	N.A.	1, 2, 3

TABLE 4.3-2 (Continued)

TABLE NOTATION

(1) Each train shall be tested at least every 180 days on a STAGGERED TEST BASIS.

(2) Each channel shall be tested at least every 92 days on a STAGGERED TEST BASIS.

(3) Each train shall be tested at least every 62 days on a STAGGERED TEST BASIS.

APPENDIX A2

This section of the appendix illustrates ESFAS functions for protection signals included in Table 3.1-2 and 3.1-3 but not included in the STS Table 3.3-3 or 4.3-2. ESFAS functions for the following signal and logics are presented.

	Signal	Logic	
1.	Safety Injection		
	a) Pressurizer Pressure - Low	2/3	
	b) Steamline Pressure - Low	2/3	2/4
	c) T-Cold Lo-Lo, coincident	2/3	
	with steam pressure-low	2/3	
2.	Steam Line Isolation		
	a) Steamline Pressure - Low	2/3	2/4
	b) Cont. Pres. Hi-Hi	2/3	
	c) Neg. Pres. Rate - Hi	2/3	
	d) Steam flow - Hi-Hi	1/2	
	e) Steam Pressure Low, coincident	2/3	
	with Steam flow Hi, and	1/2	
	T-avg Low-Low	2/3	
3.	Main Feedwater Isolation		
	a) Steam Generator Water Level Hi-Hi	2/4	
	b) T-Cold Low, coincident with	2/3	
	Feedwater flow Hi	2/3	
4.	Auxiliary Feedwater Pump Start		
	a) Steam Generator Water Level Low-Low	2/4	
	b) RCP Bus Undervoltage	2/3	
	c) RCP Bus Undervoltage	1/2, twice	

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION FUNCTIONS NOT INCLUDED IN STS TABLE 3.3-3

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
1. SAFETY INJECTION, REACTOR TRIP, FEEDWATER ISOLATION, CONTROL ROOM ISOLATION, START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER.					
a. Steam Line Pressure-Low	4	2	2	1, 2, 3#	20*
b. Steam Line Pressure-Low	3	2	2	1, 2, 3##	20*
c. Pressurizer Pressure-Low	3	2	2	1, 2, 3#	20*
d. T_{cold} Low-Low coincident with Steam Line Pressure-Low	3	2	2	1, 2, 3##	20*
	3	2	2	1, 2, 3##	20*

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION FUNCTIONS NOT INCLUDED IN STS TABLE 3.3-3

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION					
a. Steam Line Pressure-Low				1, 2, 3	
i) Four Loop Plant Four Loops Operating	4	2	3		20*
ii) Three Loop Plant Three Loops Operating	3	2	2		20*
b. Negative Steam Line Pressure Rate-High	3	2	2	1, 2, 3	20*
c. Containment Pressure--High-High	3	2	2	1, 2, 3	20*
d. Steam Flow High-High	2/Steam line	1/Steam line	1/Steam line	1, 2, 3	20*

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION FUNCTIONS NOT INCLUDED IN STS TABLE 3.3-3

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
4. STEAM LINE ISOLATION (continued)					
e. Steam Line Pressure-Low				1, 2, 3	
Three Loops Operating	1 pressure/ loop	1 pressure any 2 loops	1 pressure any 2 loops		20*
Coincident With T_{avg}--Low-Low	1 T_{avg}/loop	1 T_{avg} any 2 loops	1 T_{avg} any 2 loops		20*
and Steam Flow-High	2/Steam line	1/Steam line	1/Steam line		20*

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION FUNCTIONS NOT INCLUDED IN STS TABLE 3.3-3

FUNCTIONAL UNIT	TOTAL NO. OF CHANNELS	CHANNELS TO TRIP	MINIMUM CHANNELS OPERABLE	APPLICABLE MODES	ACTION
5. TURBINE TRIP & FEEDWATER ISOLATION					
a. Steam Generator Water Level - High-High	4/stm. gen.	2/stm. gen. in any operating stm. gen.	3/stm. gen. in each operating stm. gen.	1, 2	20*
b. T_{cold} Low coincident with	3	2	2	1,2	20*
Feedwater Flow Hi	3	2	2		20*
6. AUXILIARY FEEDWATER					
a. Stm. Gen. Water Level-Low-Low					
i. Start Motor-Driven Pumps	4/stm. gen.	2/stm. gen. in any operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2, 3	20*
ii. Start Turbine-Driven Pump	4/stm. gen.	2/stm. gen. in any 2 operating stm. gen.	2/stm. gen. in each operating stm. gen.	1, 2, 3	20*
b. Undervoltage-RCP Start Turbine-Driven Pump	3-1/bus	2	2	1, 2	20*
c. Undervoltage-Both RCP Busses	4-2/bus	2-1/bus	2-1/bus	1, 2	20*

ADDITIONAL ESFAS FUNCTIONS NOT INCLUDED IN STS TABLE 4.3-2

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
1. SAFETY INJECTION, REACTOR TRIP FEEDWATER ISOLATION, CONTROL ROOM ISOLATION START DIESEL GENERATORS, CONTAINMENT COOLING FANS AND ESSENTIAL SERVICE WATER								
a. Steamline Pressure-low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
b. T_{cold}-Low-low, Coincident	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
With Steam Line Pressure-low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
4. STEAM LINE ISOLATION								
a. Steam Line Pressure-Low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
b. Negative Steam Line Pressure Rate-High	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
c. Steam Line Pressure-Low Coincident With	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
1. Steam Flow-High, and	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
2. T_{ave}-Low-Low	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3
d. Steam Flow Hi-Hi	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2, 3

ADDITIONAL ESFAS FUNCTIONS NOT INCLUDED IN STS TABLE 4.3-2

ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION
SURVEILLANCE REQUIREMENTS

FUNCTIONAL UNIT	CHANNEL CHECK	CHANNEL CALIBRATION	ANALOG CHANNEL OPERATIONAL TEST	TRIP ACTUATING DEVICE OPERATIONAL TEST	ACTUATION LOGIC TEST	MASTER RELAY TEST	SLAVE RELAY TEST	MODES FOR WHICH SURVEILLANCE IS REQUIRED
5. TURBINE TRIP AND FEEDWATER ISOLATION								
a. T_{cold}- Low Coincident	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2
With Feed Flow-Hi	S	R	Q(2)	N.A.	N.A.	N.A.	N.A.	1, 2

APPENDIX B

FAULT TREE STRUCTURE

This appendix illustrates the structure of the fault trees applied in the study. The top trees, middle trees, and analog channel trees that were used to model each ESF signal are listed. The top trees essentially model the master and slave relays and the middle trees model the logic cabinets. The analog channel trees model the sensor, power supply, signal conditioning circuit, and signal comparators. The analog channel trees supply input to the middle trees which in turn supply input to the top trees. Several of the more complex signals (features) required several middle trees. The structure of these are also given. The fault tree identifiers used in this appendix correspond to the fault trees in Appendix C.

ESF RELAY PROTECTION SYSTEM - SAFETY INJECTION SIGNALS

1A. Pressurizer pressure - low - 2/4
interlocked with P11 - 2/3

- Top tree: SI1
- Middle tree: PP1A
- Analog Channel: B9

1B. Pressurizer pressure - low - 2/3
interlocked with P11 - 2/3

- Top tree: SI1
- Middle tree: PP1B
- Analog Channel: B9

2A. Steamline pressure - low - 2/4
interlocked with P11 - 2/3

- Top tree: SI1
- Middle tree: SP1A
- Analog Channel: B9

2B. Steamline pressure - low - 2/3
interlocked with P11 - 2/3

- Top tree: SI1
- Middle tree: SP1B
- Analog Channel: B9

ESF RELAY PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

3A. Steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree: SI1
Middle tree: SP1A (2/3), SP2A (2/4)
Analog Channel: B9

3B. Steamline pressure - low - 2/3
interlocked with P12 - 2/3 or 2/4

Top tree: SI1
Middle tree: SP1B (2/3), SP2B (2/4)
Analog Channel: B9

4. Containment pressure - high - 2/3

Top tree: SI1
Middle tree: CP1
Analog Channel: B10

5A. Differential steamline pressure - high - 2/3

Top tree: SI1
Middle tree: DSP1
Analog Channel: DSPC

ESF RELAY PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

5B. Differential steamline - pressure high - 2/3
interlocked with P11 - 2/3

Top tree: SI1
Middle tree: DSP2
Analog Channel: DSPC

6A. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/3
interlocked with P12 - 2/3 or 2/4

Top tree: SI1
Middle tree: SF1B + SF3B
Analog Channel: B9, TAVG, SFLOW

6B. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree: SI1
Middle tree: SF1B + SF3A
Analog Channel: B9, TAVG, SFLOW

ESF RELAY PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

6C. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/3
interlocked with P12 - 2/3 or 2/4

Top tree:	SI1
Middle tree:	SF1A ← SF2B
Analog Channel:	B9, TAVG, SFLOW

6D. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree:	SI1
Middle tree:	SF1A ← SF2A
Analog Channel:	B9, TAVG, SFLOW

ESF RELAY PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNAL

1A. Steamline pressure - low - 2/3
interlocked with P11 - 2/3
- Top tree: SLI1
- Middle tree: SP1B
- Analog Channel: B9

1B. Steamline pressure - low - 2/4
interlocked with P11 - 2/3
- Top tree: SLI1
- Middle tree: SP1A
- Analog Channel: B9

2A. Steamline pressure - low - 2/3
interlocked with P12 - 2/3 or 2/4
- Top tree: SLI1
- Middle tree: SP1B (2/3), SP2B (2/4)
- Analog Channel: B9

2B. Steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4
- Top tree: SLI1
- Middle tree: SP1A (2/3), SP2A (2/4)
- Analog Channel: B9

ESF RELAY PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNAL (Continued)

3A. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/3

Top tree:	SLI1
Middle tree:	SF4 ← SF3B
Analog Channel:	TAVG, SFLOW, B9

3B. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/4

Top tree:	SLI1
Middle tree:	SF4 ← SF3A
Analog Channel:	TAVG, SFLOW, B9

3C. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/3

Top tree:	SLI1
Middle tree:	SF4 ← SF2B
Analog Channel:	SFLOW, TAVG, B9

3D. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/4

Top tree:	SLI1
Middle tree:	SF4 ← SF2A
Analog Channel:	SFLOW, TAVG, B9

ESF RELAY PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNAL (Continued)

4A. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
Top tree: SLI1
Middle tree: SF4 ← TA1A
Analog Channel: SFLOW, TAVG

4B. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
Top tree: SLI1
Middle tree: SF4 ← TA1B
Analog Channel: SFLOW, TAVG

5A. Containment pressure - high-high - 2/3
Top tree: SLI1
Middle tree: CP1
Analog Channel: B10

5B. Containment pressure - high-high - 2/4
Top tree: SLI1
Middle tree: CP2
Analog Channel: B10

6. Steamflow - high-high - 1/2
or steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
Top tree: SLI1
Middle tree: HSF1 ← HSF2
Analog Channel: SFLOW, TAVG

ESF RELAY PROTECTION SYSTEM - MAIN FEEDWATER ISOLATION SIGNALS

1A. Steam generator level - high-high - 2/3
Top/Middle tree: FW1B
Analog Channel: B10

1B. Steam generator level - high-high - 2/4
Top/Middle tree: FW1A
Analog Channel: B10

ESF RELAY PROTECTION SYSTEM - AUXILIARY FEEDWATER PUMP START SIGNALS

1A. Steam generator level low-low - 2/3
Top/Middle tree: FW1B
Analog Channel: B10

1B. Steam generator level low-low - 2/4
Top/Middle tree: FW1A
Analog Channel: B10

ESF RELAY PROTECTION SYSTEM
CONTAINMENT SPRAY AND PHASE B ISOLATION SIGNALS

1. Containment pressure high-high - 2/4
   - Top tree: SLI1
   - Middle tree: CP2
   - Analog Channel: B10

2. Containment pressure high-high-high - 2/4
   - Top tree: SLI1
   - Middle tree: CP2
   - Analog Channel: B10

ESF SOLID STATE PROTECTION SYSTEM - SAFETY INJECTION SIGNALS

1A. Pressurizer pressure - low - 2/4
interlocked with P11 - 2/3
Top tree: SICPA
Middle tree: PP1 ← PP2A
↖ PB1 ← PB2
Analog Channel: B9

1B. Pressurizer pressure - low - 2/3
interlocked with P11 - 2/3
Top tree: SICPA
Middle tree: PP1 ← PP2B
↖ PB1 ← PB2
Analog Channel: B9

2A. Steamline pressure - low - 2/4
interlocked with P11 - 2/3
Top tree: SICPA
Middle tree: SP1 ← SP2A
↖ PB1 ← PB2
Analog Channel: B9

2B. Steamline pressure - low - 2/3
interlocked with P11 - 2/3
Top tree: SICPA
Middle tree: SP1 ← SP2B
↖ PB1 ← PB2
Analog Channel: B9

ESF SOLID STATE PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

3A. Steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree: SICPA
Middle tree: SP1 ← SP2A
↖ TB1 ← TB2A (2/4)
or
TB2B (2/3)
Analog Channel: B9

3B. Steamline pressure - low - 2/3
interlocked with P12 - 2/3 or 2/4

Top tree: SICPA
Middle tree: SP1 ← SP2B
↖ TB1 ← TB2A (2/4)
or
TB2B (2/3)
Analog Channel: B9

4. Containment pressure - high - 2/3

Top tree: SICPA
Middle tree: CP1
Analog Channel: B10

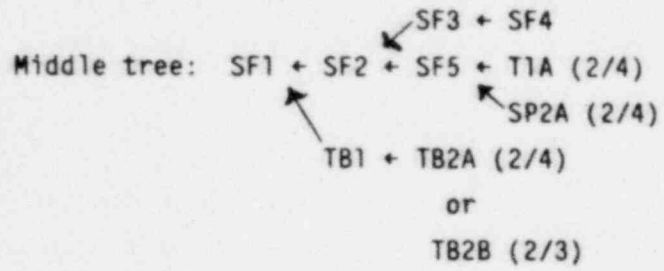
5A. Differential steamline pressure - high
1 instr./steamline

Top tree: SICPA
Middle tree: DP2A ← DP2B
Analog Channel: DSPC

ESF SOLID STATE PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

5B. Differential steamline pressure - high
3 instr./steamline
Top tree: SICPA
Middle tree: DP1 + DP2B
Analog Channel: DSPC

6A. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4
Top tree: SICPA



Analog Channel: SFLOW, TAVG, B9

ESF SOLID STATE PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

6B. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/3
interlocked with P12 - 2/3 or 2/4

Top tree: SICPA

Middle tree: SFI ← SF2 ← SF3 ← SF4
SF5 ← T1A (2/4)
SP2B (2/3)
TB1 ← TB2A (2/4)
or
TB2B (2/3)

Analog Channel: SFLOW, TAVG, B9

6C. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree: SICPA

Middle tree: SFI ← SF2 ← SF3 ← SF4
SF5 ← T1B (2/3)
SP2A (2/3)
TB1 ← TB2A (2/4)
or
TB2B (2/3)

Analog Channel: SFLOW, TAVG, B9

ESF SOLID STATE PROTECTION SYSTEM - SAFETY INJECTION SIGNALS (Continued)

6D. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree: SICPA

Middle tree: SF3 ← SF4
SFI ← SF2 ← SF5 ← T1B (2/3)
SP2B (2/3)
TB1 ← TB2A (2/4)
or
TB2B (2/3)

Analog Channel: SFLOW, TAVG, B9

7. T_{cold} - low-low - 2/3
coincident with steam pressure
low - 2/3
interlocked with P15 - 2/4

Top tree: SICPA

Middle tree: BLCK1 ← BLCK2
TCSP1 ← TCSP2
TCSP3 ← P151 ← P152

Analog Channel: B9, B10, TAVG

ESF SOLID STATE PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNALS

1A. Steamline pressure - low - 2/4

Top tree: AXFW

Middle tree: SL1 ← SP1 ← SP2A

Analog Channel: B9

1B. Steamline pressure - low - 2/3

Top tree: AXFW

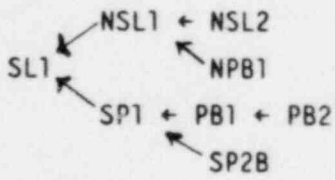
Middle tree: SL1 ← SP1 ← SP2B

Analog Channel: B9

2. Steamline pressure - low - 2/3
and negative steamline pressure
rate-high - 2/3
interlocked with P12

Top tree: AXFW

Middle tree:



Analog Channel: B9

3A. Containment pressure - high-high - 2/4

Top tree: AXFW

Middle tree: CP2

Analog Channel: B10

ESF SOLID STATE PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNALS (Continued)

3B. Containment pressure - high-high - 2/3

Top tree: AXFW

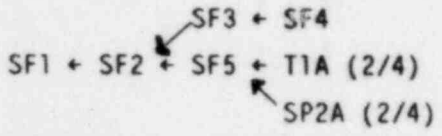
Middle tree: CP1

Analog Channel: B10

4A. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/4

Top tree: AXFW

Middle tree:

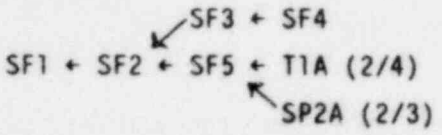


Analog Channel: SFLOW, TAVG, B9

4B. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
or steamline pressure - low - 2/3

Top tree: AXFW

Middle tree:



Analog Channel: SFLOW, TAVG, B9

ESF SOLID STATE PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNALS (Continued)

4C. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/4

Top tree: AXFW

Middle tree:

SF3 ← SF4
SF1 ← SF2 ← SF5 ← T1B (2/3)
SP2A (2/4)

Analog Channel: SFLOW, TAVG, B9

4D. Steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
or steamline pressure - low - 2/4

Top tree: AXFW

Middle tree:

SF3 ← SF4
SF1 ← SF2 ← SF5 ← T1B (2/3)
SP2B (2/3)

Analog Channel: SFLOW, TAVG, B9

5A. Steamline Pressure - low - 2/4
and steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
interlocked with P12 - 2/3 or 2/4

Top tree: AXFW

Middle tree:

SL1 ← ST1 ← SF3 ← SF4
T1A (2/4)
SP1 ← SP2A (2/4)
TB1 ← TB2B

Analog Channel: SFLOW, TAVG, B9

ESF SOLID STATE PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNALS (Continued)

5B. Steamline pressure - low - 2/3
and steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/4
interlocked with P12 - 2/4

Top tree: AXFW

Middle tree: SL1
- ST1 + SF3 + SF4
- T1A (2/4)
- SP1 + SP2B (2/3)
- TB1 + TB2B

Analog Channel: SFLOW, TAVG, B9

5C. Steamline pressure - low - 2/4
and steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
interlocked with P12 - 2/3

Top tree: AXFW

Middle tree: SL1
- ST1 + SF3 + SF4
- T1B (2/3)
- SP1 + SP2A (2/4)
- TB1 + TB2B

Analog Channel: SFLOW, TAVG, B9

ESF SOLID STATE PROTECTION SYSTEM - STEAMLINE ISOLATION SIGNALS (Continued)

5b. Steamline pressure - low - 2/3
and steamflow - high - 1/2
coincident with T_{avg} - low-low - 2/3
interlocked with P12 - 2/3

Top tree: AXFW

Middle tree: SL1
- ST1 + SF3 + SF4
- T18 (2/3)
- SP1 + SP28 (2/3)
- TB1 + TB2B

Analog Channel: SFLOW, TAVG, B9

6. Steamflow - high-high - 1/2
coincident with SI

Top tree: AXFW

Middle tree: S1 + SF4
- SI

Analog Channel: SFLOW

7. Steamflow - high - 1/2
interlocked with P12 - 2/4
coincident with SI

Top tree: AXFW

Middle tree: S1 + TB1 + T82A

Analog Channel: SFLOW

ESF SOLID STATE PROTECTION SYSTEM
MAIN FEEDWATER ISOLATION SIGNALS

1A. Steam generator water level -
high-high - 2/4 in one loop

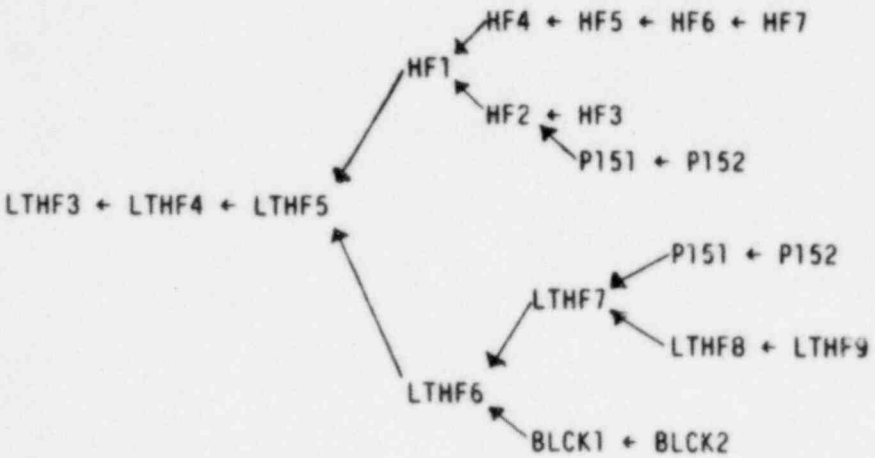
Top tree: AXFW
Middle tree: SGWL1 + SGWL2
Analog Channel: B10

1B. Steam generator water level -
high-high - 2/3 in one loop

Top tree: AXFW
Middle tree: SGWL1 + SGWL2
Analog Channel: B10

2. T_{cold} - low - 2/3
Feed flow - high - 2/3

Top tree: AXFW
Middle Tree:



Analog Channels: B9, B10

ESF SOLID STATE PROTECTION SYSTEM - AUXILIARY FEEDWATER PUMP START SIGNALS

1A. Steam generator water level - low-low - 2/4 in one loop

- Top tree: AXFW
- Middle tree: SGWL
- Analog Channel: B10

1B. Steam generator water level - low-low - 2/3 in one loop

- Top tree: AXFW
- Middle tree: SGWL
- Analog Channel: B10

2A. RCP bus undervoltage - 2/3

- Top tree: AXFW
- Middle tree: BUV
- Analog Channel: B9

2B. RCP bus undervoltage - 2/4

- Top tree: AXFW
- Middle tree: BUV
- Analog Channel: B9

3. RCP bus undervoltage - 1/2 twice

- Top tree: AXFW
- Middle tree: BUV
- Analog Channel: B9

ESF SOLID STATE PROTECTION SYSTEM - CONTAINMENT SPRAY AND PHASE B ISOLATION SIGNALS

1. Containment pressure - high-high - 2/4
   - Top tree: SICPA
   - Middle tree: CP2
   - Analog Channel: B9

2. Containment pressure - high-high-high - 2/4
   - Top tree: SICPA
   - Middle tree: CP2
   - Analog Channel: B9

APPENDIX C

FAULT TREES

This appendix contains the top, middle and analog/bistable channel trees used to evaluate the ESF signal unavailabilities. Figure numbers starting with "S" apply to the solid state protection system. Figure numbers starting with "R" apply to the relay protection system. Figure numbers starting with "B" apply to both systems and model the analog/bistable channels. The following is a general description of these figures.

Figures S1-S4: AXFW is a top tree used to model the master and slave relays for the Steamline Isolation, Main Feedwater Isolation, and Auxiliary Feedwater Pump start signals of the solid state protection system.

Figures S5-S13: SICPA is a top tree used to model the master and slave relays for the Safety Injection and Containment Spray and Phase B Isolation signals of the solid state protection system.

Figures S14-S67: These are the middle trees used to model the logic cabinets of the solid state protection system.

Figures R1-R7: SI1 is a top tree used to model the master and slave relays for the Safety Injection signal of the relay protection system.

Figures R8-R11: SLI1 is a top tree used to model the master and slave relays for the Steamline Isolation and Containment Spray and Phase B Isolation signals of the relay protection system.

Figures R12-R32: These are the middle trees used to model the logic cabinets of the relay protection system.

Figures R33-R34: These are the combined top/middle trees used to model the Main Feedwater Isolation and Auxiliary Feedwater Pump Start signals of the relay protection system.

Figures B1-B5: These are the trees used to model the analog/bistable channels.

The fault tree identifiers used on the figures in this appendix correspond to those used to describe the fault tree structure in Appendix B.

+a,c

FIGURE S1
AUXILIARY FEEDWATER, STEAMLINE ISOLATION, MAIN FEEDWATER ISOLATION DOES NOT INITIATE

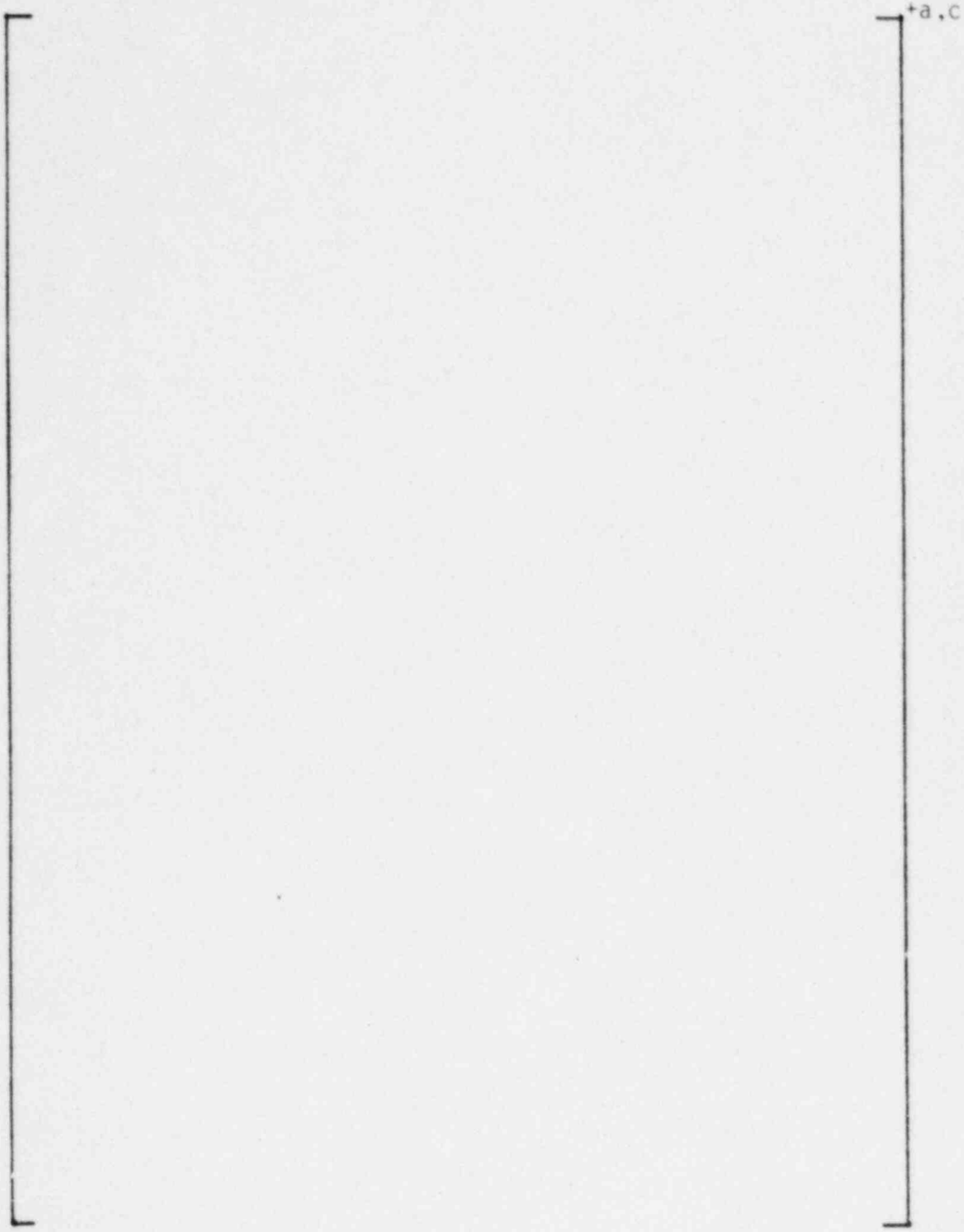


FIGURE S2
SLAVE RELAYS C1 AND D1 FAIL TO
PROVIDE START SIGNAL

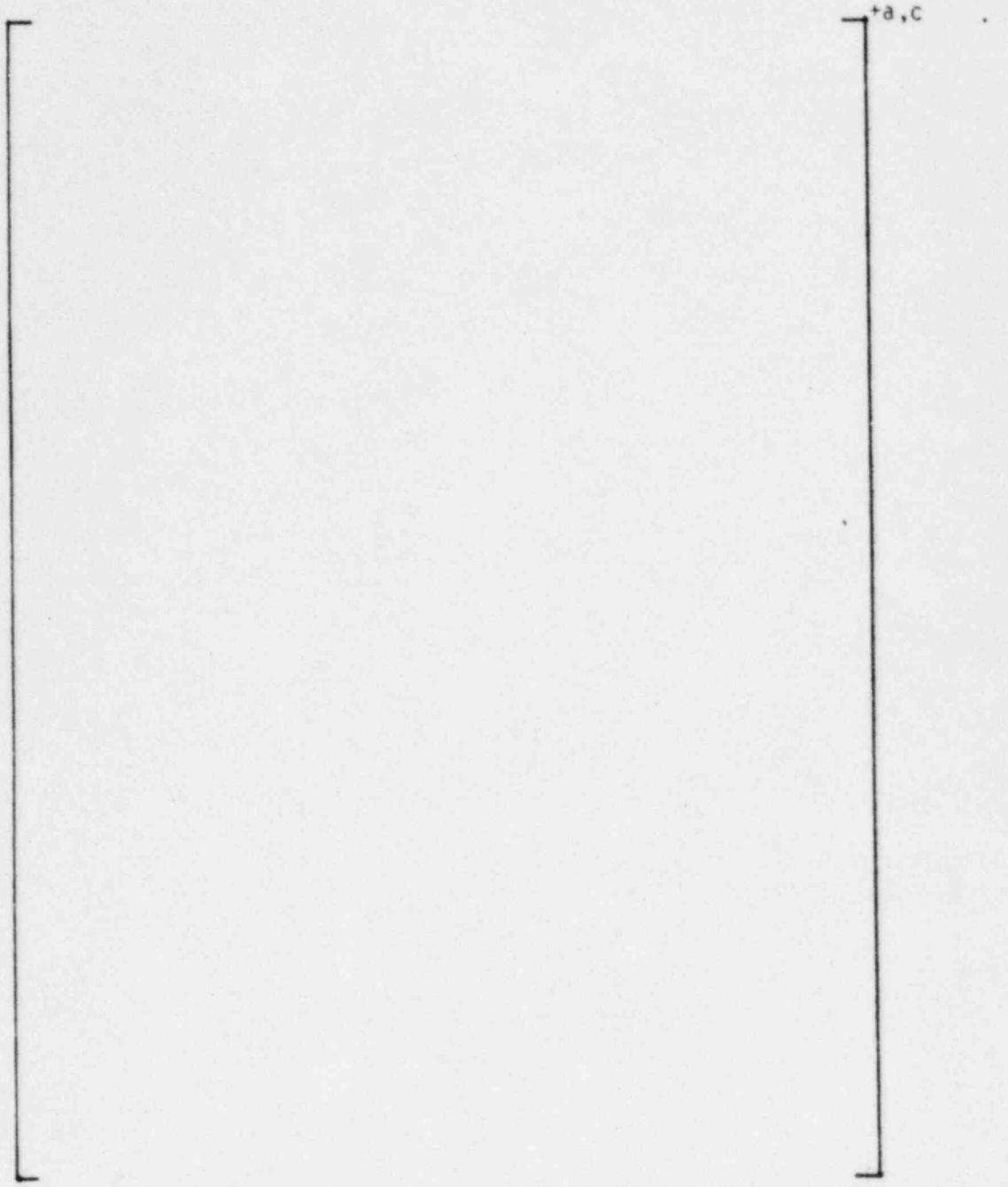


FIGURE S3
SLAVE RELAYS C2 AND D2 FAIL TO
PROVIDE START SIGNAL

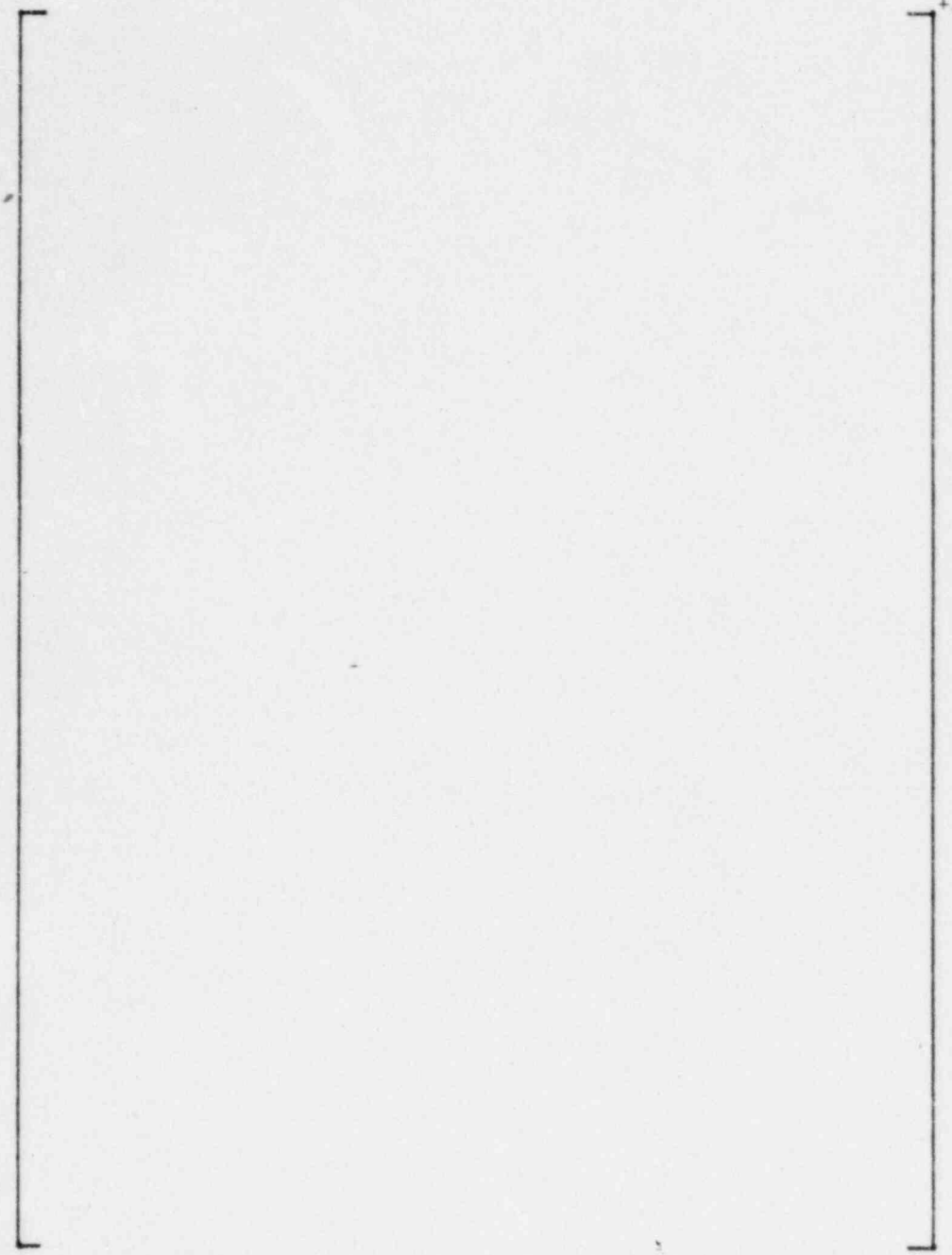


FIGURE S4
SAFEGUARDS DRIVER FAILS TO
PROVIDE SIGNAL

[+a,c]

FIGURE S5
SI, CONTAINMENT SPRAY DOES NOT INITIATE

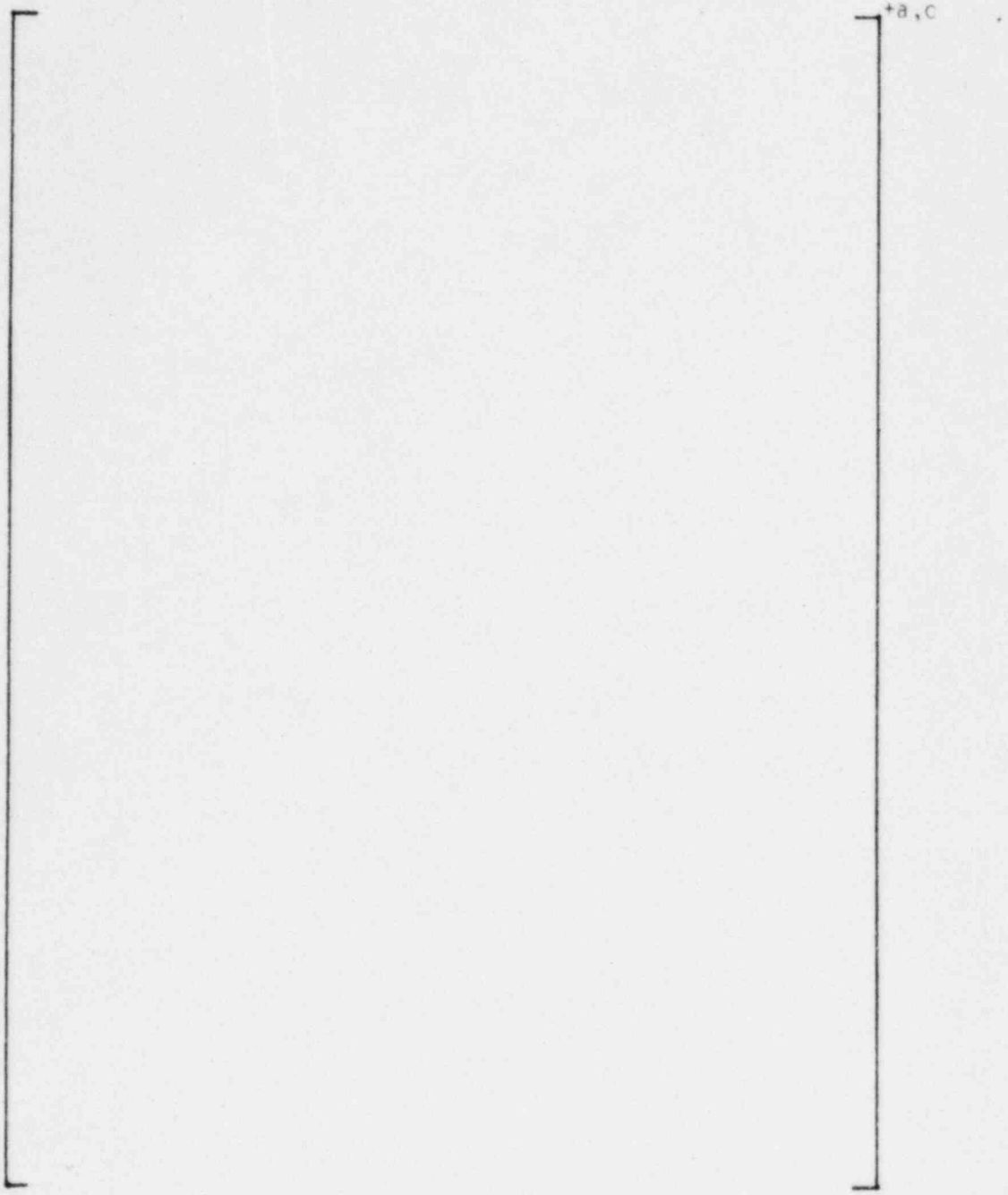


FIGURE S6
TRAIN A IN TEST, RANDOM
FAILURES IN TRAIN B

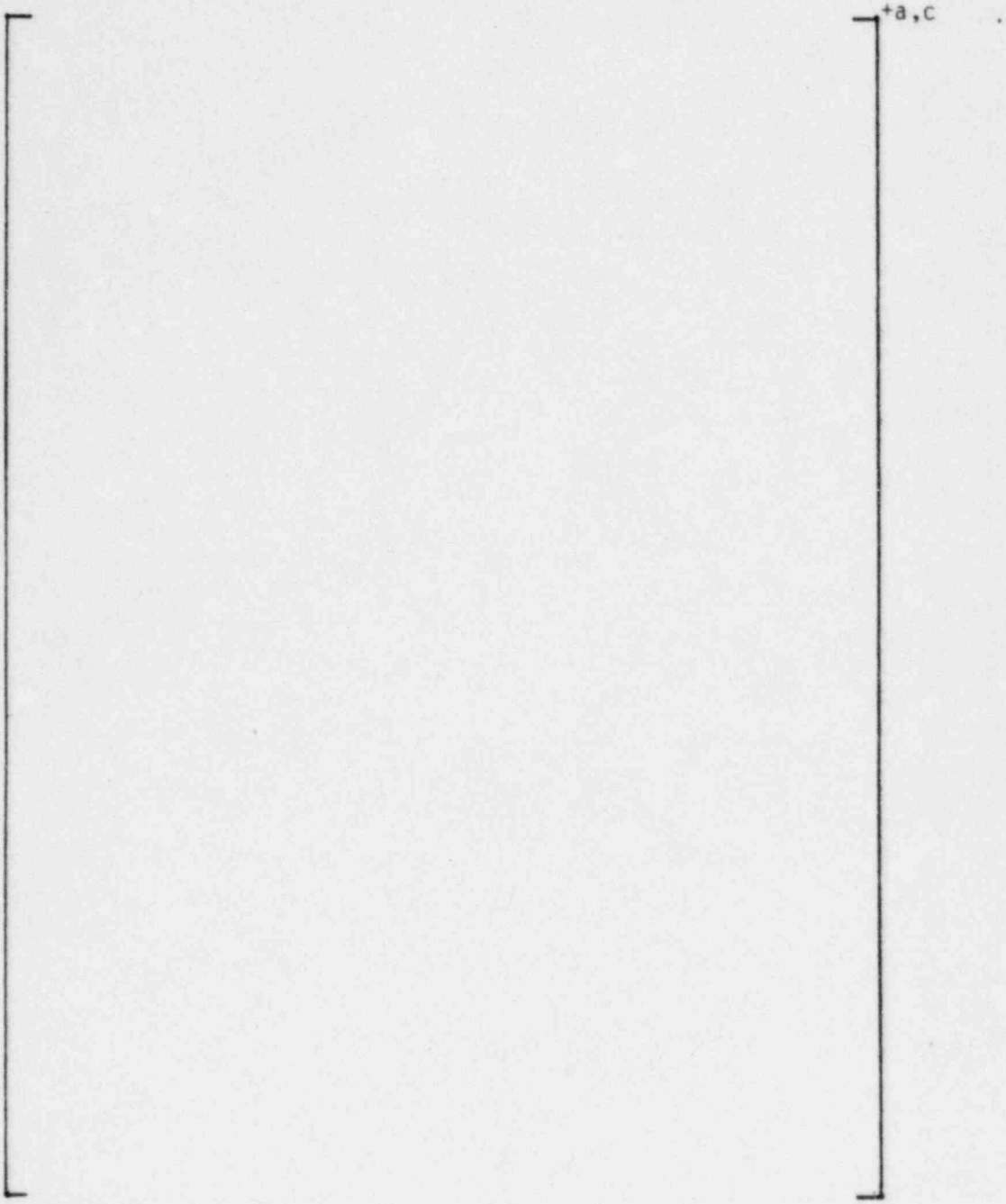


FIGURE S7
TRAIN B IN TEST, RANDOM
FAILURES IN TRAIN A

[+a,c]

FIGURE S8
SLAVE RELAYS C1 AND E1 FAIL TO
PROVIDE START SIGNAL

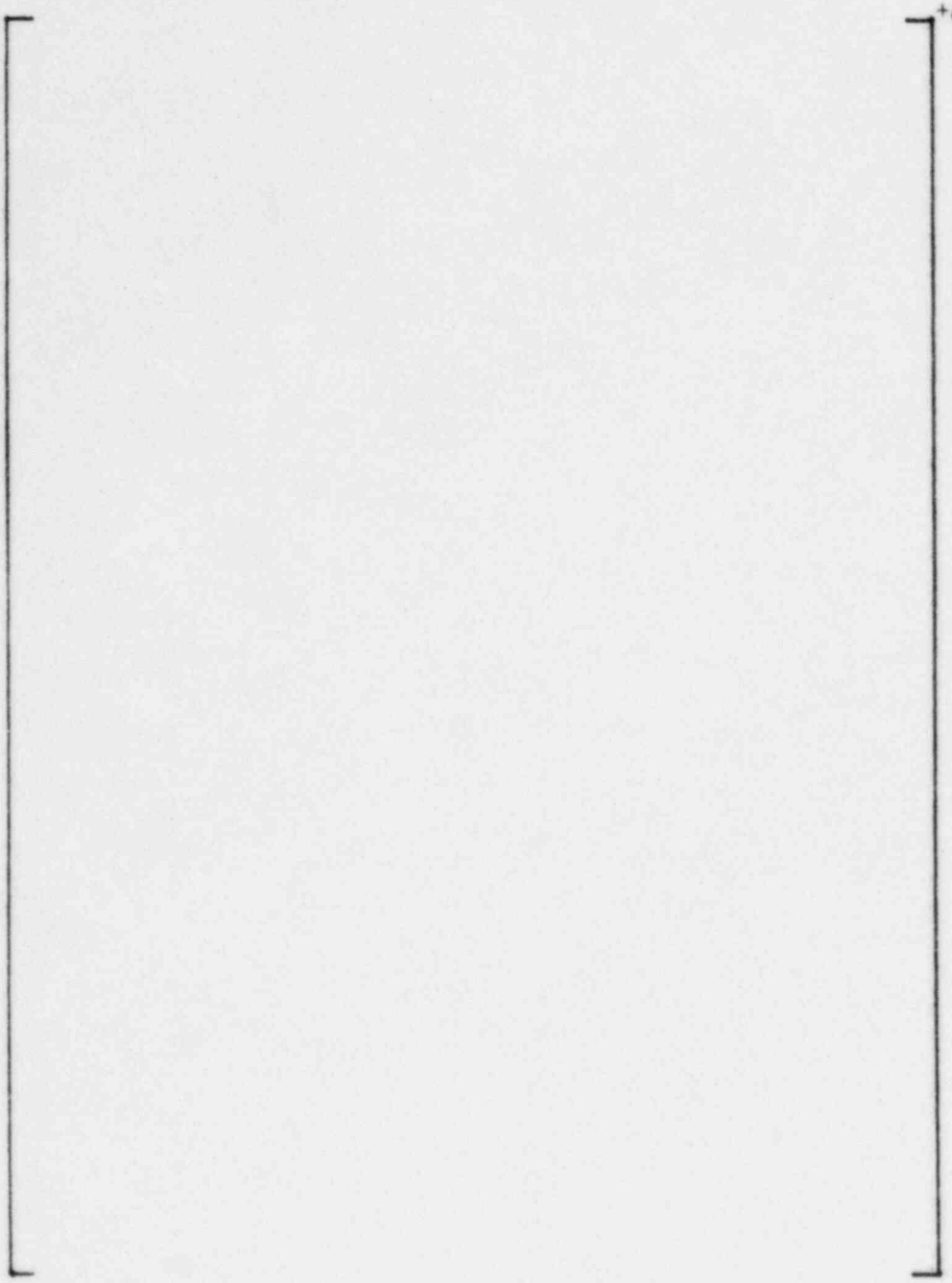


FIGURE S9
SLAVE RELAYS C2 AND E2 FAIL TO
PROVIDE START SIGNAL

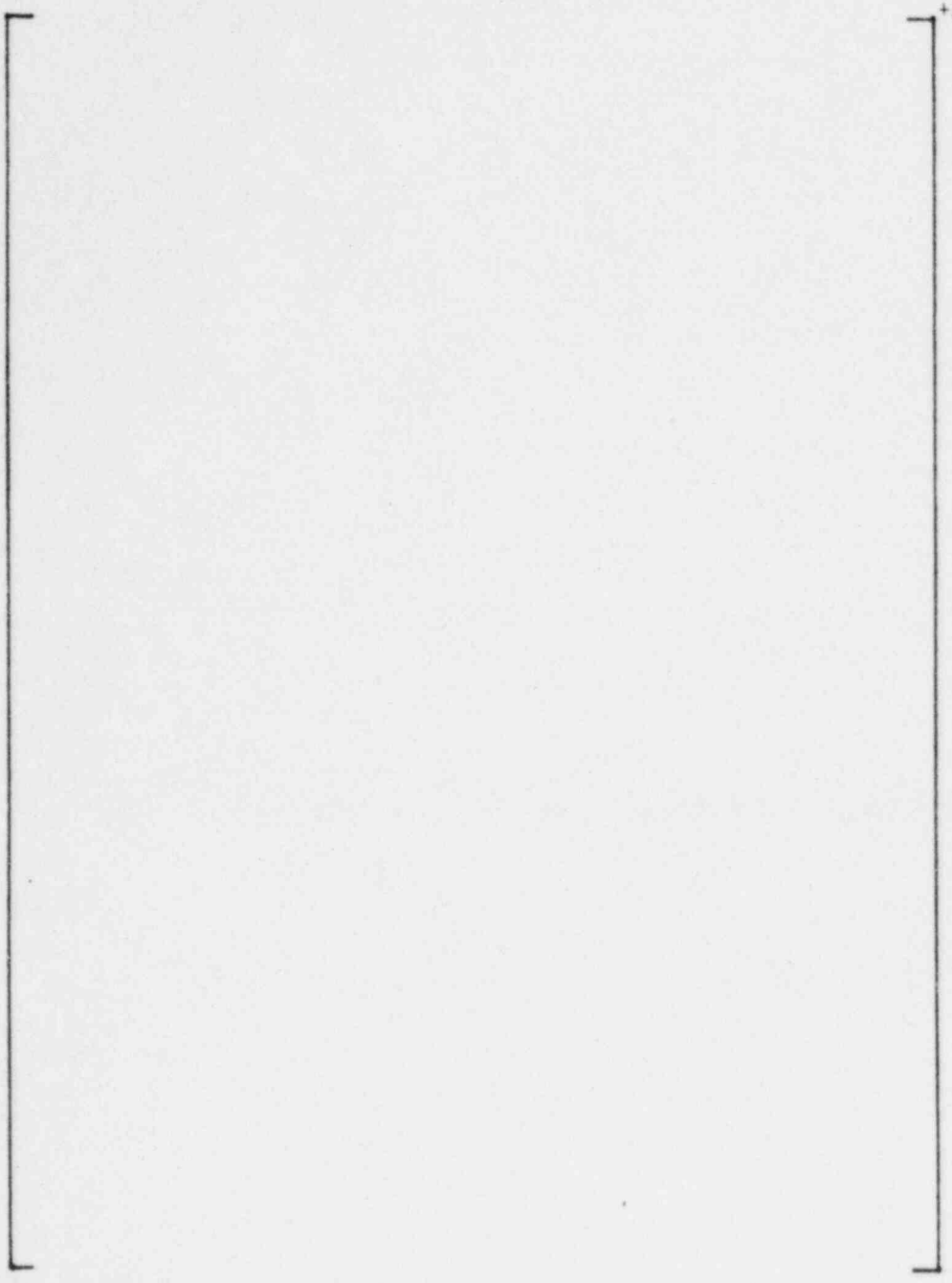


FIGURE S10
SLAVE RELAYS C3 AND E3 FAIL TO
PROVIDE START SIGNAL

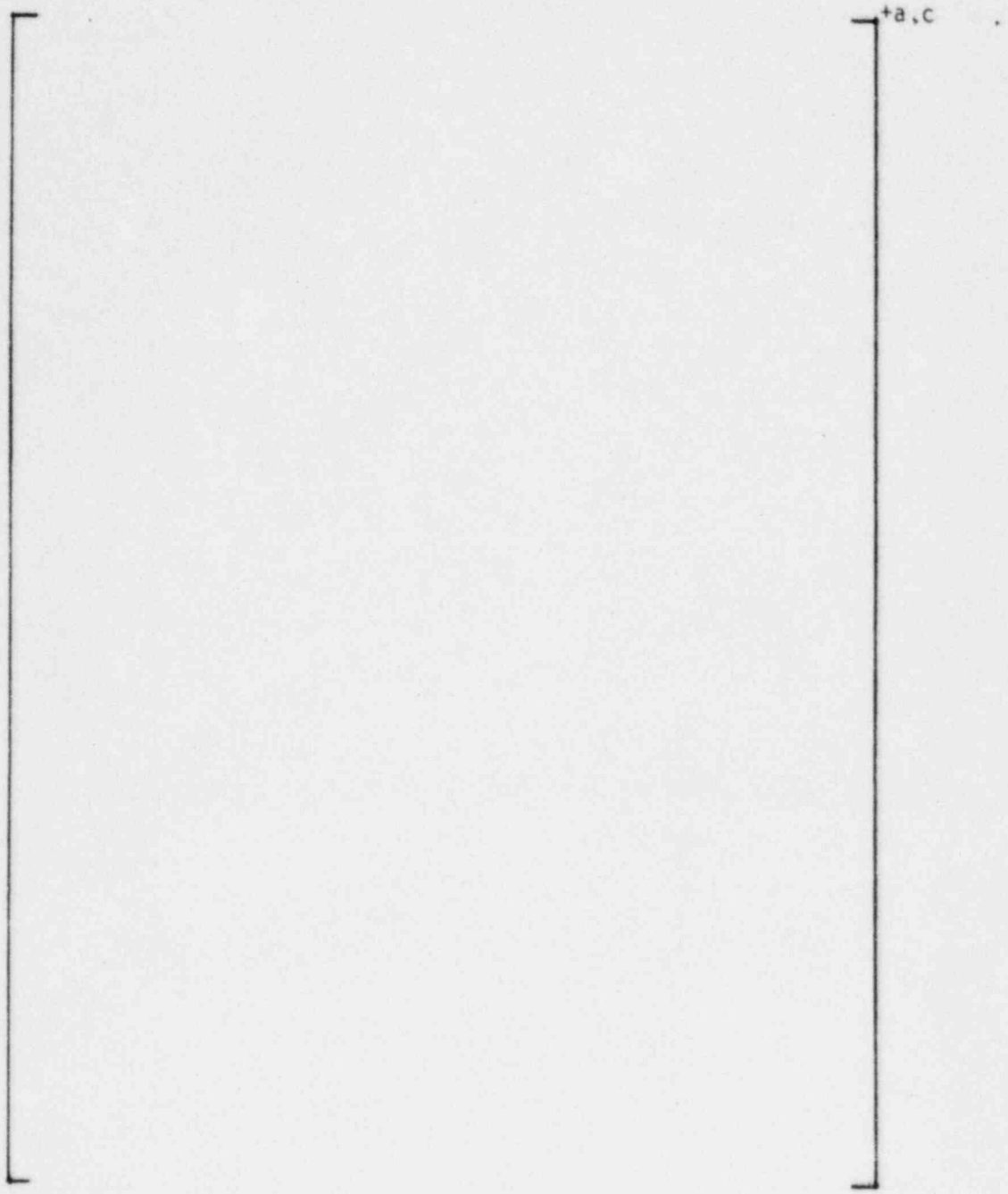


FIGURE S11
SLAVE RELAYS D1 AND F1 FAIL TO
PROVIDE START SIGNAL

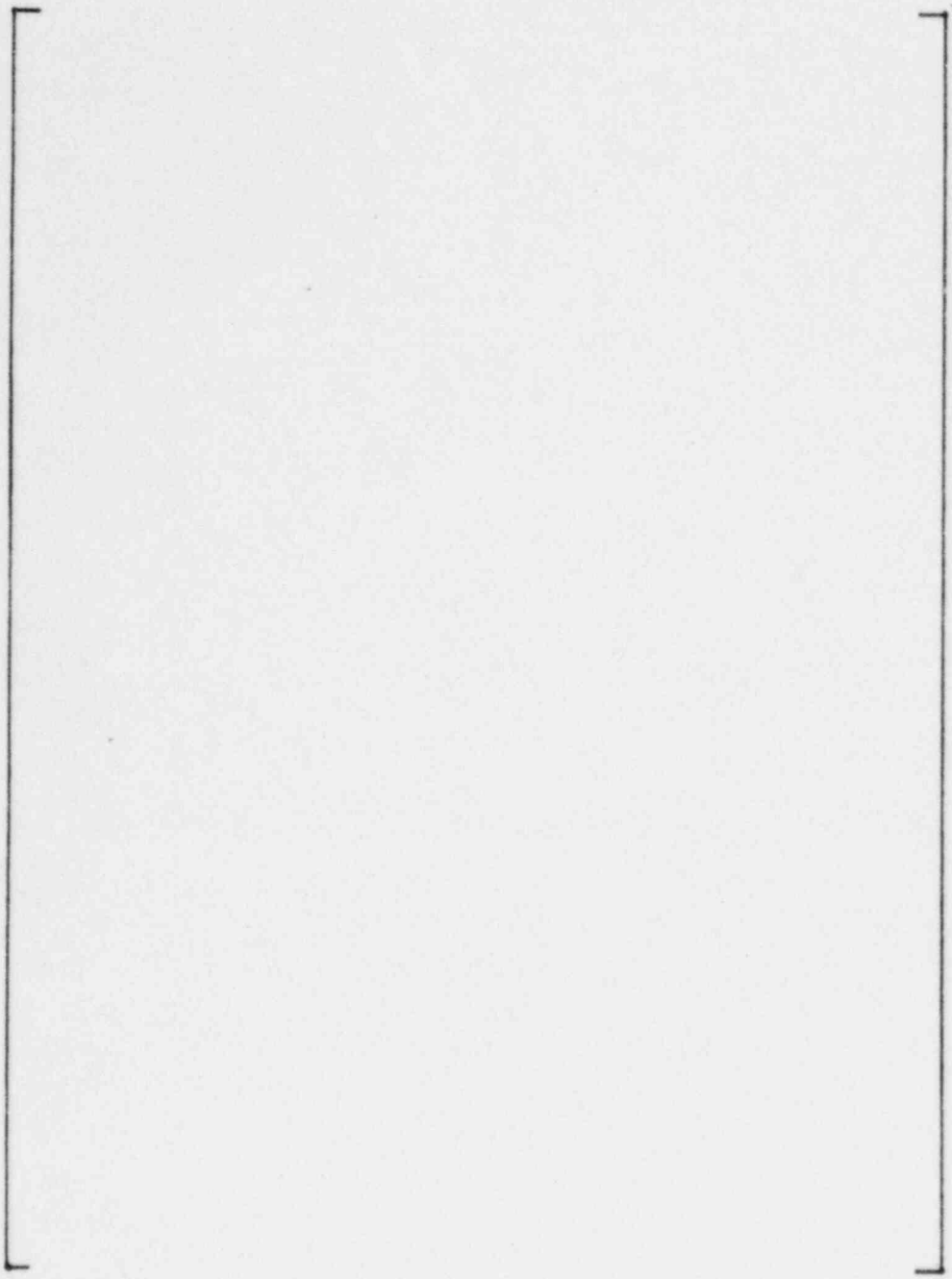


FIGURE S12
SLAVE RELAYS D2 AND F2 FAIL TO
PROVIDE START SIGNAL

[a,c]

FIGURE S13
SLAVE RELAYS D3 AND F3 FAIL TO
PROVIDE START SIGNAL

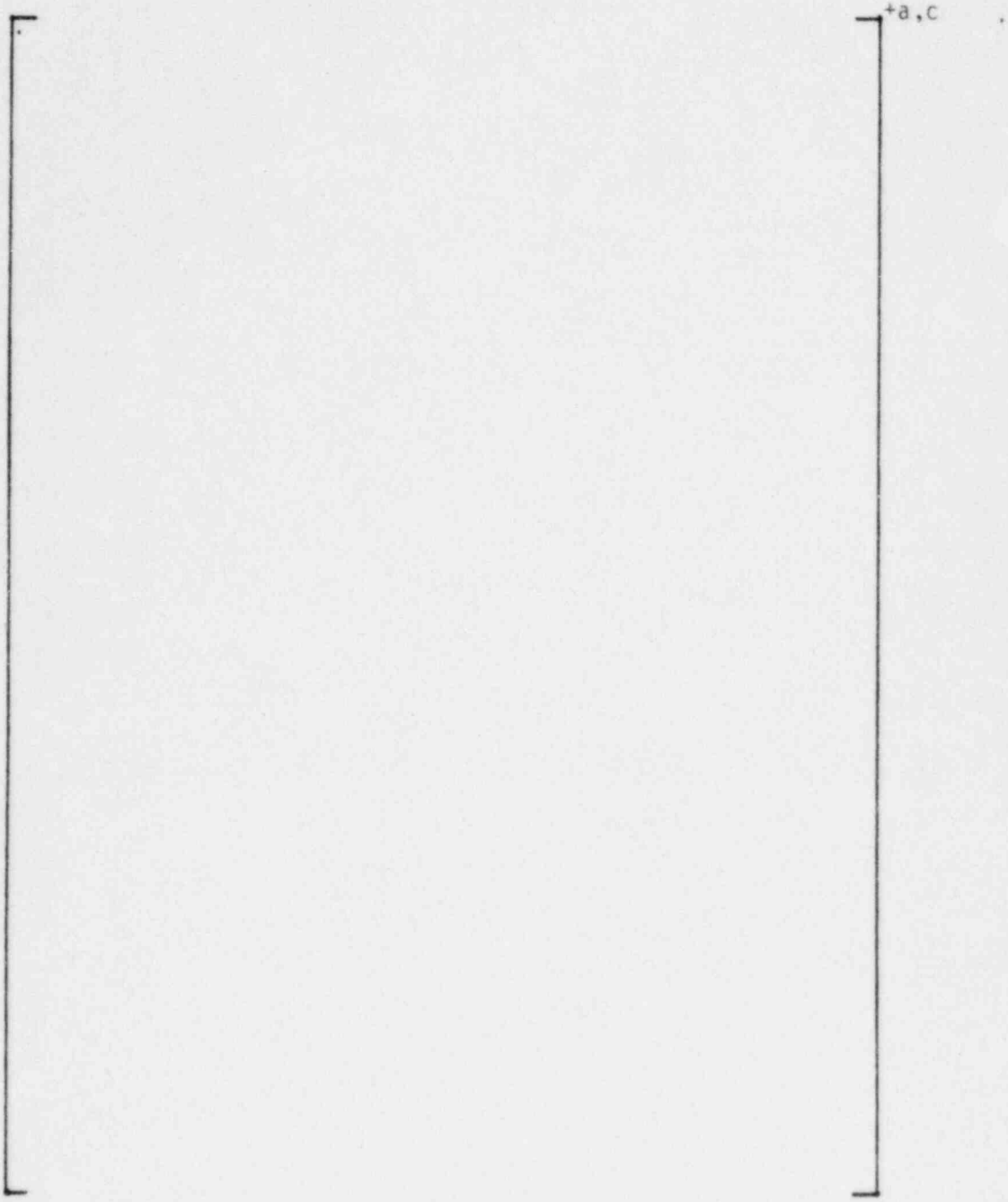


FIGURE S14
NO LOW PRESSURIZER PRESSURE SI
SIGNAL FROM SSPS

[+a,c]

FIGURE S15
2 OF 4 PRESSURIZER PRESSURE
CHANNELS FAIL

[+a,c]

FIGURE S16
2 OF 3 PRESSURIZER PRESSURE
CHANNELS FAIL

[+a,c]

FIGURE S17
P-11 FAILS AND BLOCKS SI

[+a,c]

FIGURE S18
PRESSURIZER PRESSURE CHANNELS TO
P-11 FAIL LOW

+a,c

FIGURE S19
NO SECONDARY SIDE STEAMLINE
ISOLATION SIGNAL FROM SSPS

[+a,c]

FIGURE S20
NO STEAMLINE PRESSURE SIGNAL
FROM SSPS

[+a,c]

FIGURE S21
2 OF 4 STEAM PRESSURE SIGNALS FAIL

[+a,c]

FIGURE S22
2 OF 3 STEAM PRESSURE SIGNALS FAIL

+a,c

FIGURE S23
NO HIGH STEAM FLOW WITH LOW Tavg
OR LOW STEAM PRESSURE SIGNAL

[+a,c]

FIGURE S24
HIGH STEAM FLOW AND LOW-LOW
Tavg SIGNALS FAIL

+a,c

FIGURE S25
HIGH STEAM FLOW SIGNAL FAILS

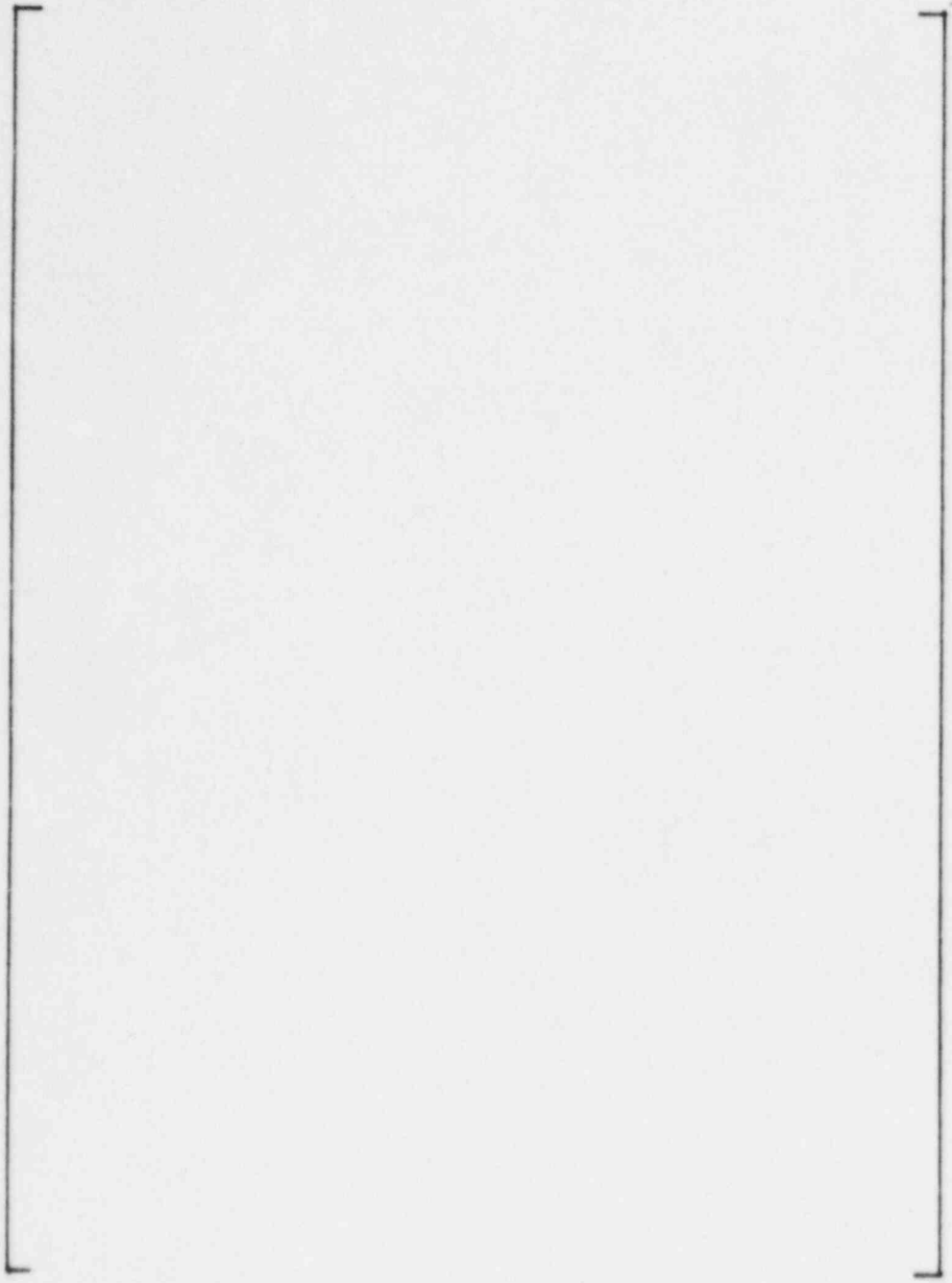


FIGURE S26
1 OF 2 STEAM FLOW CHANNELS FAIL

+a,c

FIGURE S27
LOW STEAM PRESSURE AND LOW-LOW Tavg SIGNALS FAIL

[+a,c]

FIGURE S28
HIGH STEAM FLOW AND LOW Tavg
SIGNALS FAIL

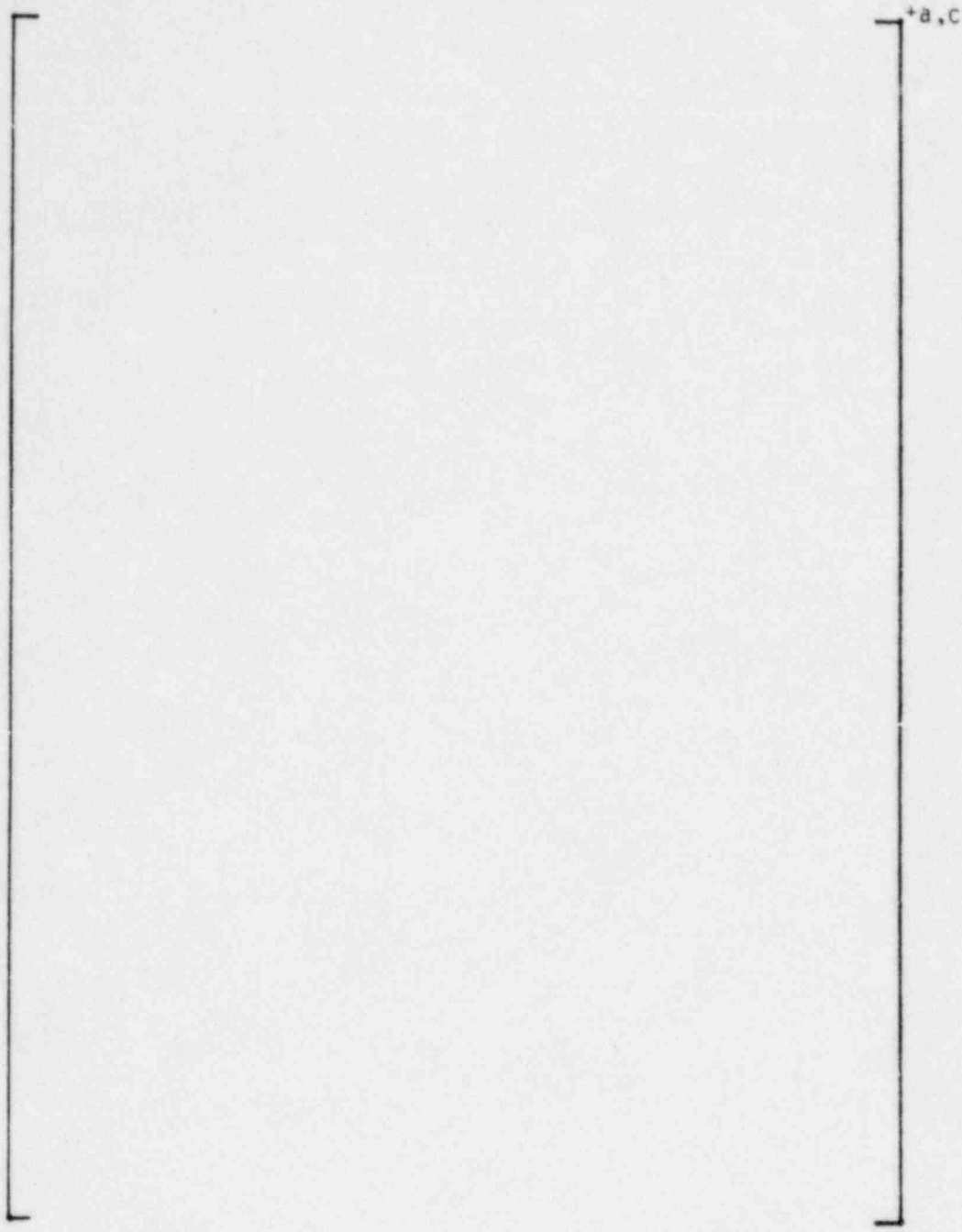


FIGURE S29
LOW-LOW Tavg SIGNAL FAILS

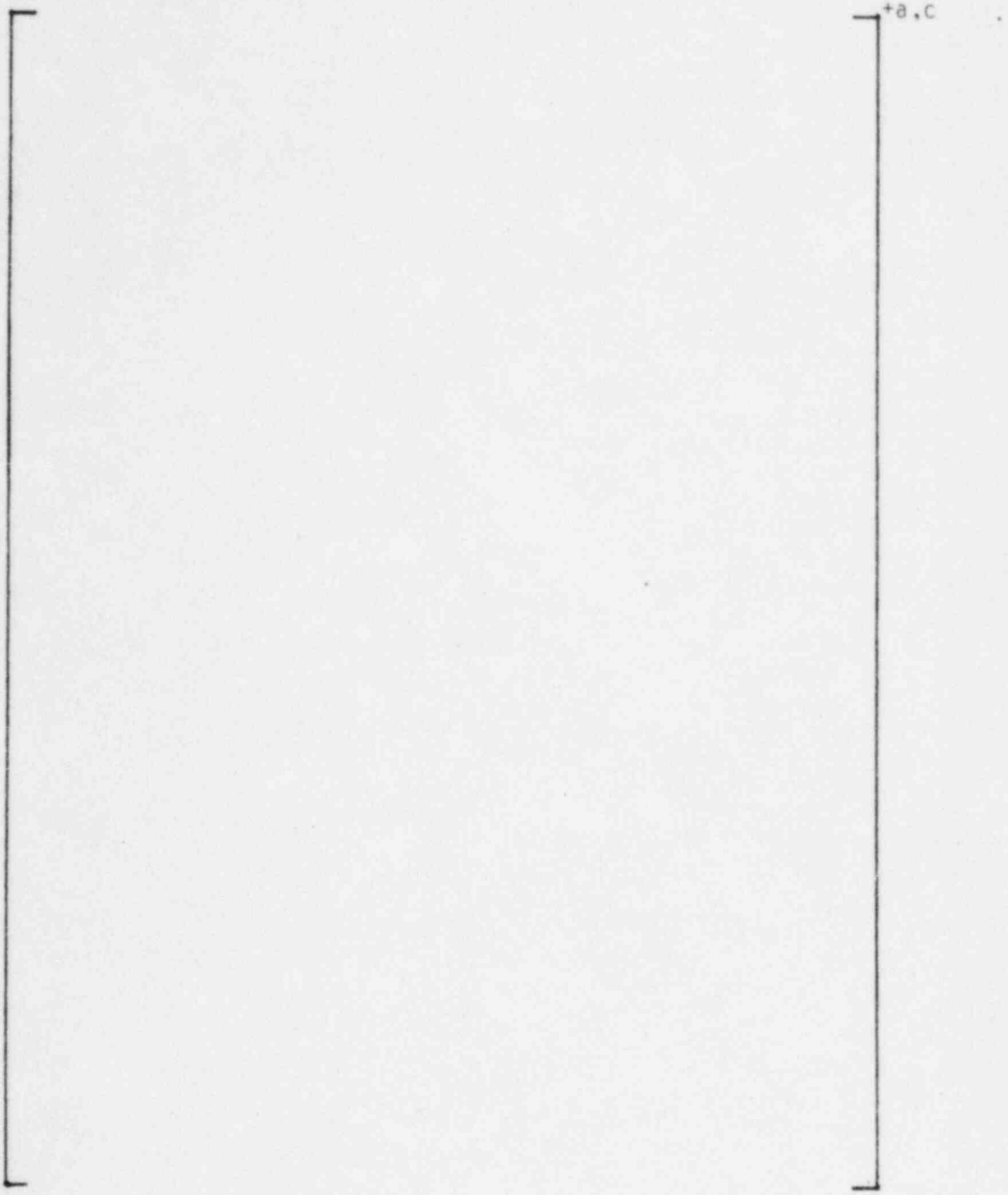


FIGURE S30
2 OF 3 LOW-LOW T_{avg} SIGNALS FAIL

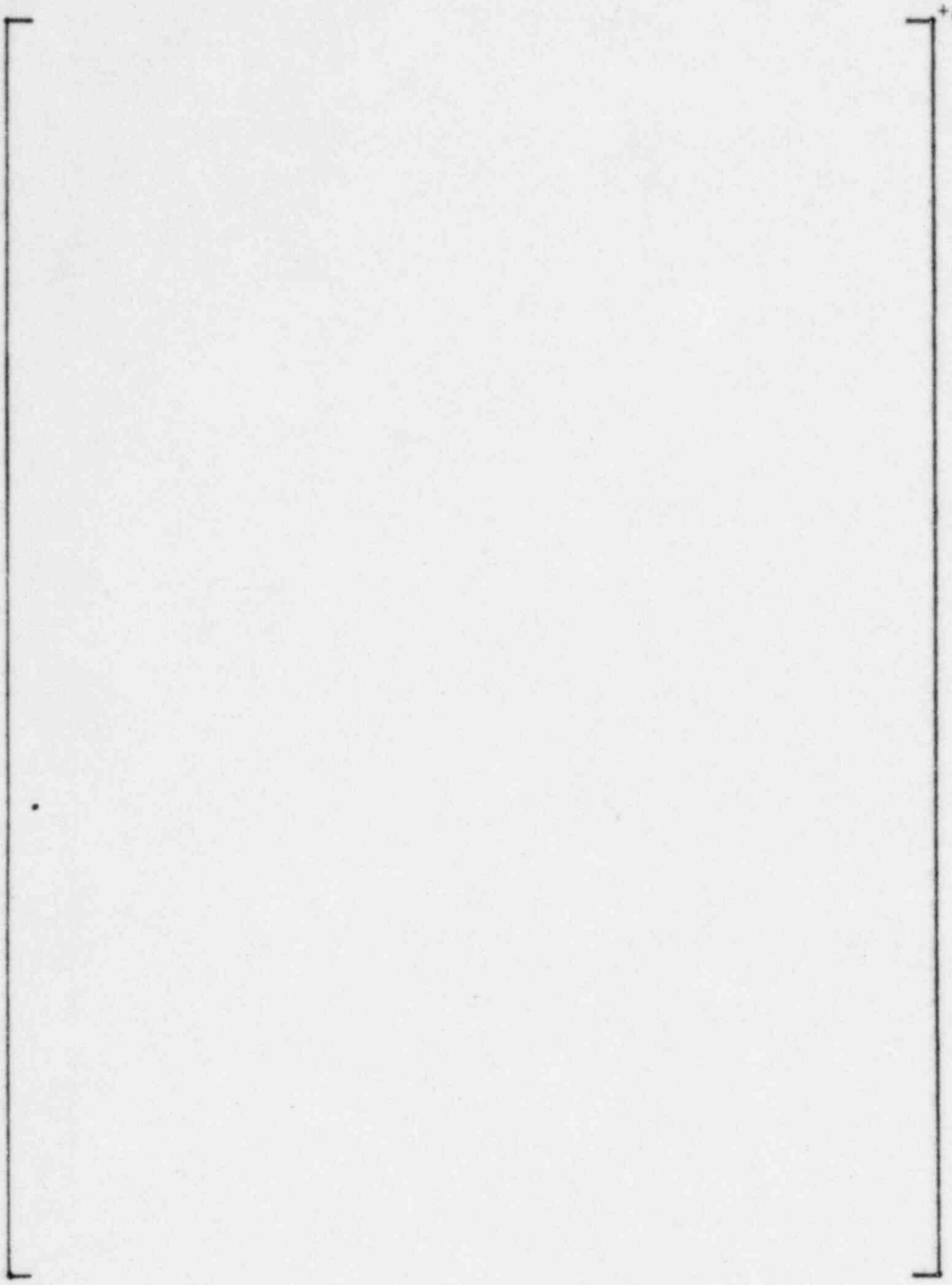


FIGURE S31
NO HIGH DIFFERENTIAL STEAMLINE
PRESSURE SIGNAL FROM SSPS

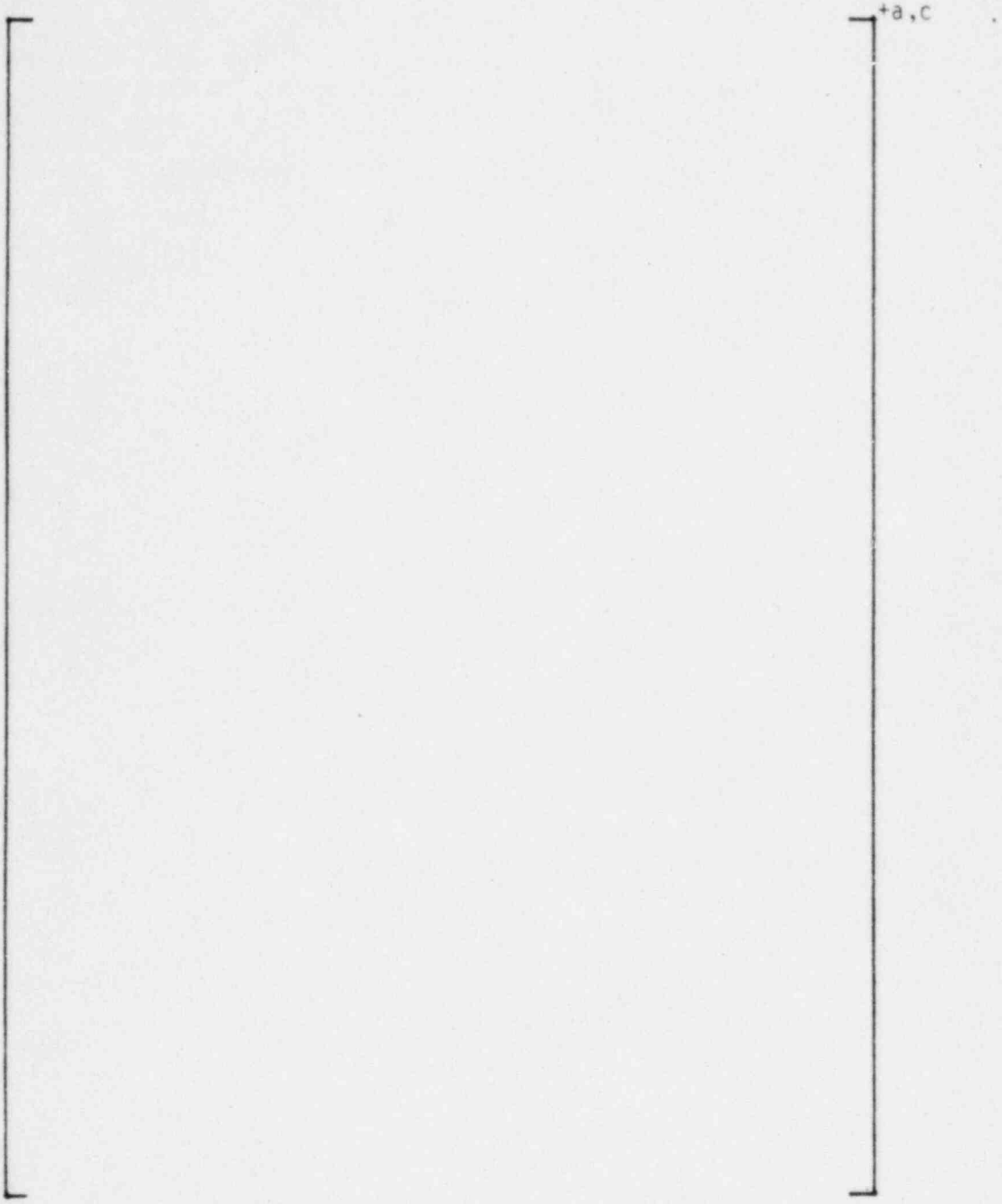


FIGURE S32
1 OF 1 HIGH DIFFERENTIAL STEAMLINE
PRESSURE CHANNELS FAIL

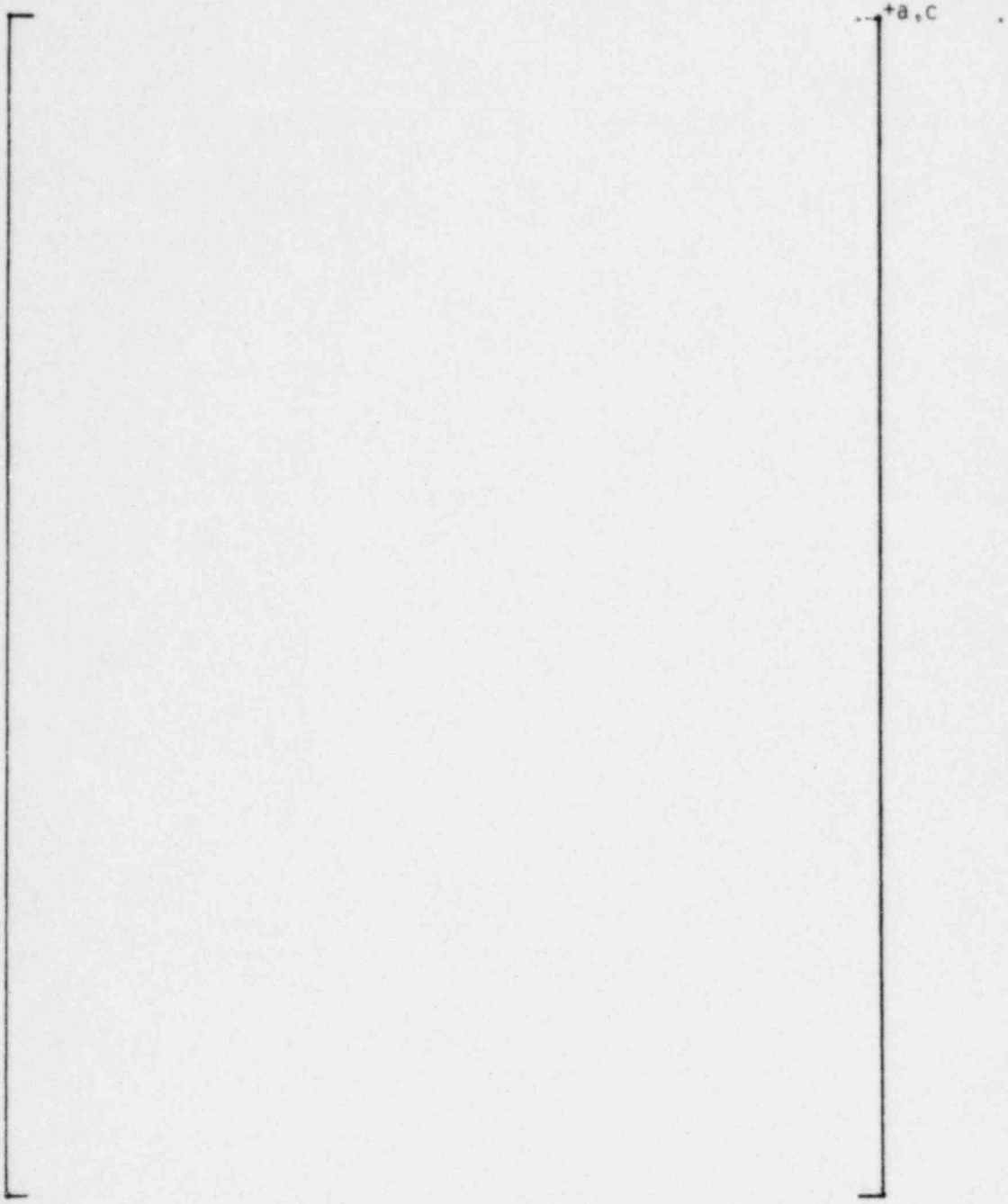


FIGURE S33
2 OF 3 HIGH DIFFERENTIAL STEAMLINE
PRESSURE CHANNELS FAIL

+a,c

FIGURE S34
P-12 FAILS AND BLOCKS SI

+a,c

FIGURE S35
2 OF 4 Tavg CHANNELS TO P-12
FAIL LOW

[+a,c]

FIGURE S36
2 OF 3 Tavg CHANNELS TO P-12
FAIL LOW

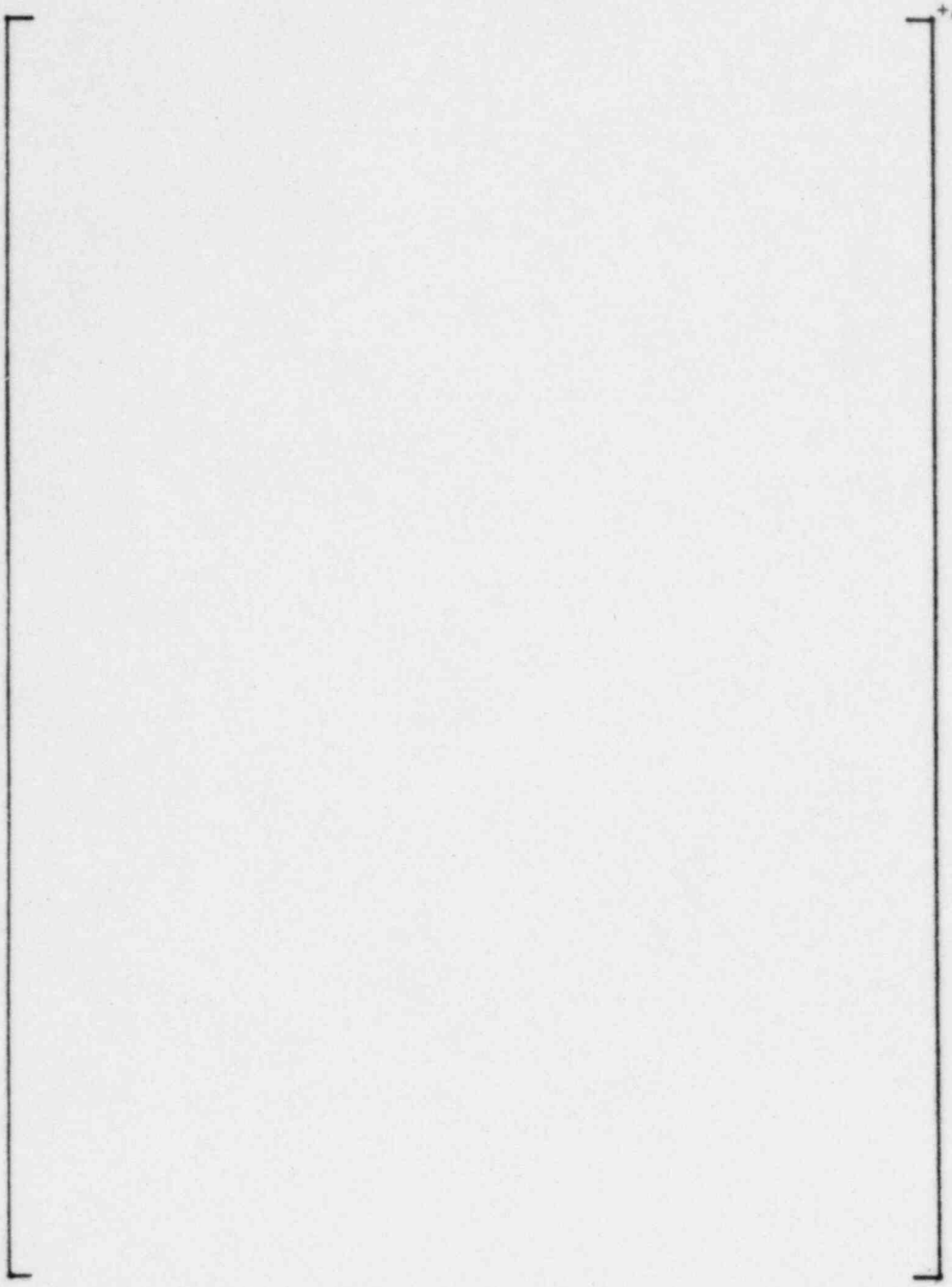


FIGURE S37
NO HIGH NEGATIVE STEAMLINE
PRESSURE RATE SIGNAL

[ ]+a,c

FIGURE S38
2 OF 3 HIGH NEGATIVE STEAMLINE
PRESSURE RATE CHANNELS FAIL

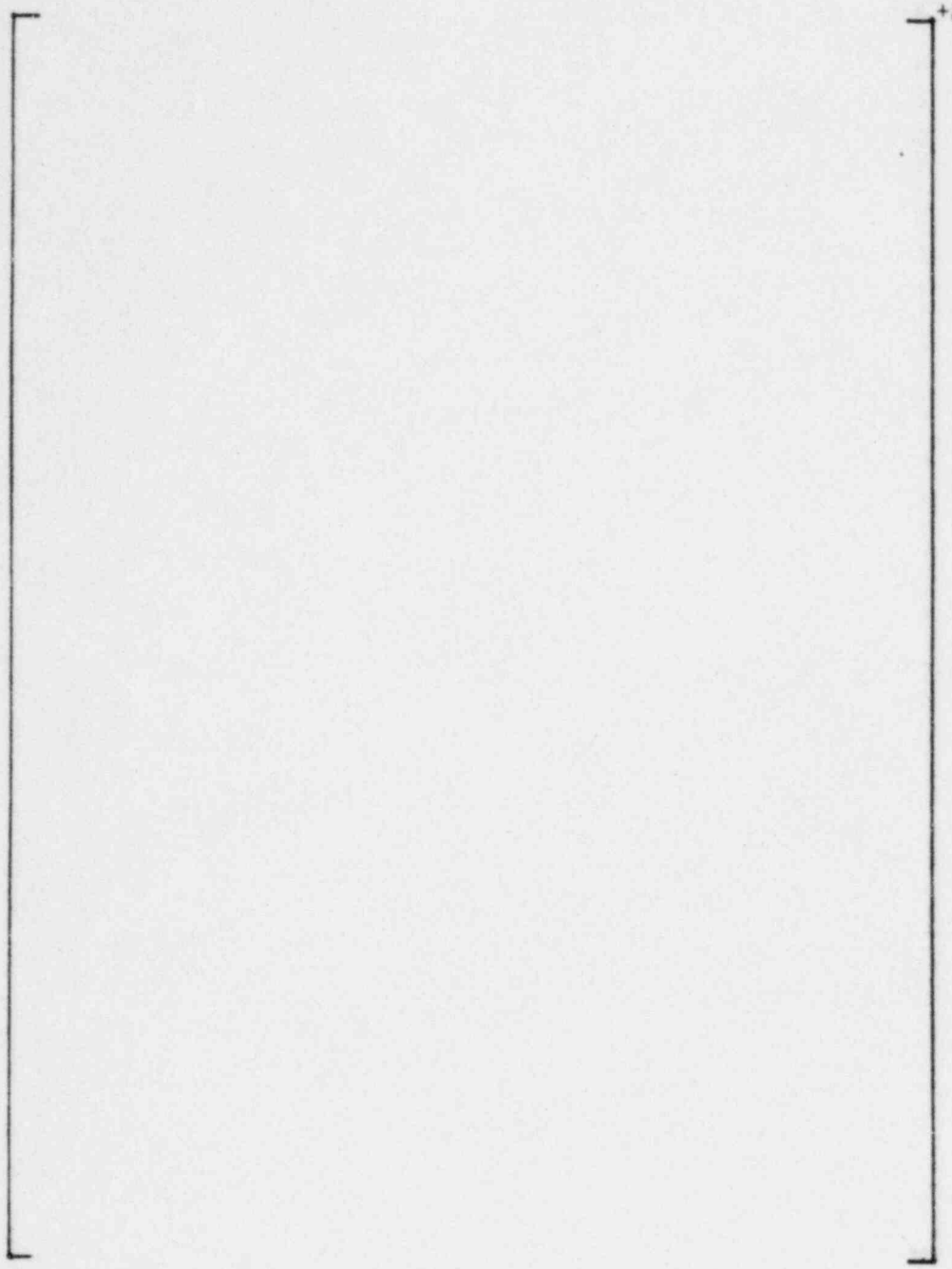


FIGURE 839
P-11 FAILS HIGH

+a,c

FIGURE S40
2 OF 3 CONTAINMENT PRESSURE
CHANNELS FAIL

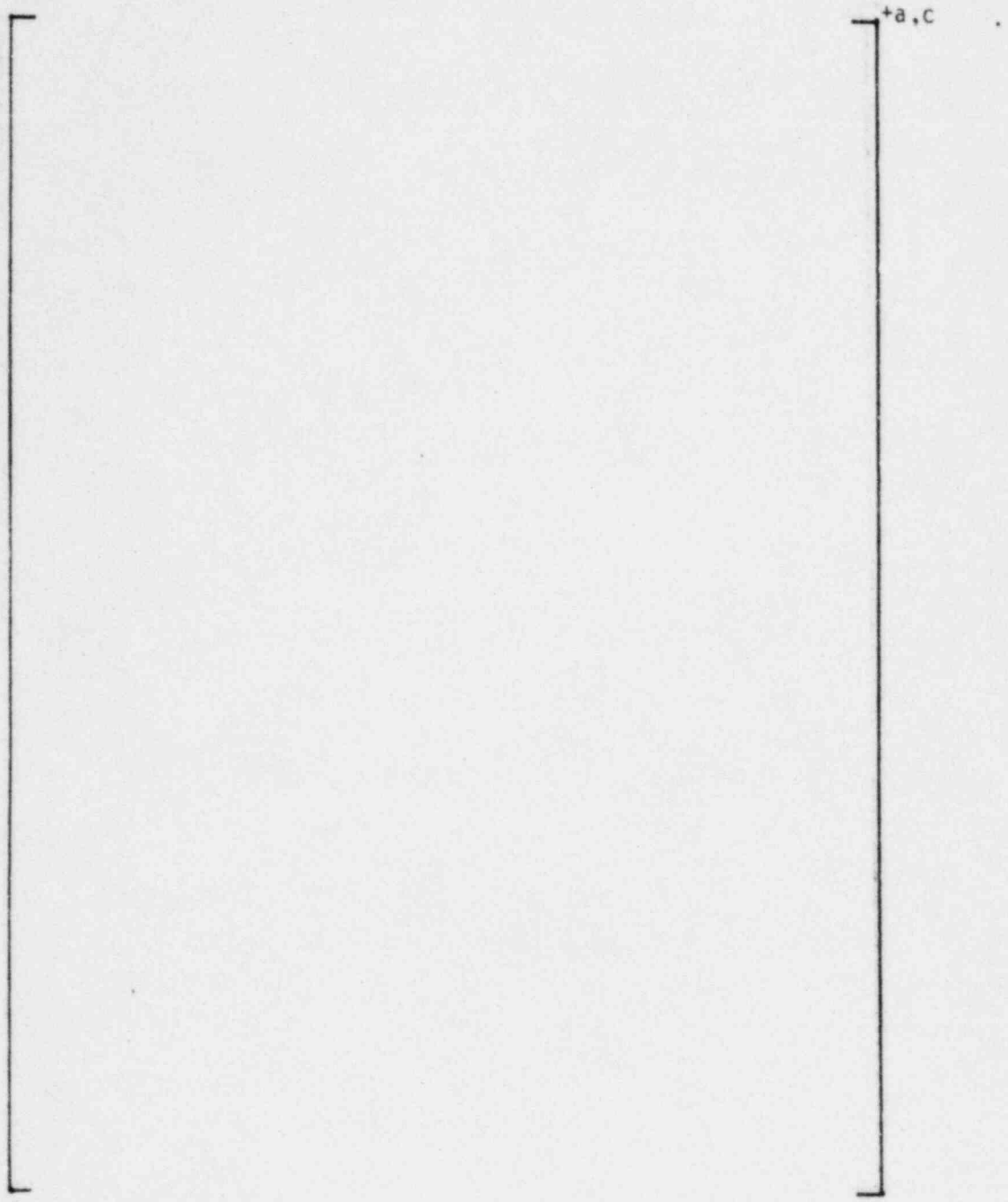


FIGURE S41
2 OF 4 CONTAINMENT PRESSURE
CHANNELS FAIL

[+a,c]

FIGURE S42
NO HIGH STEAM FLOW OR HIGH-HIGH
STEAM FLOW SIGNAL FROM SSPS

[+a,c]

FIGURE S43
NO HIGH STEAM FLOW FROM 1 LOOP

+a,c

FIGURE S44
NO LOW STEAM GENERATOR WATER
LEVEL SIGNAL

+a,c

FIGURE S45
3 OF 4 LOW STEAM GENERATOR WATER LEVEL CHANNELS FAIL

[+a,c]

FIGURE S46
HIGH FEEDFLOW SIGNAL FAILS

[+a,c]

FIGURE S47
HIGH FEEDWATER LOGIC FAILS

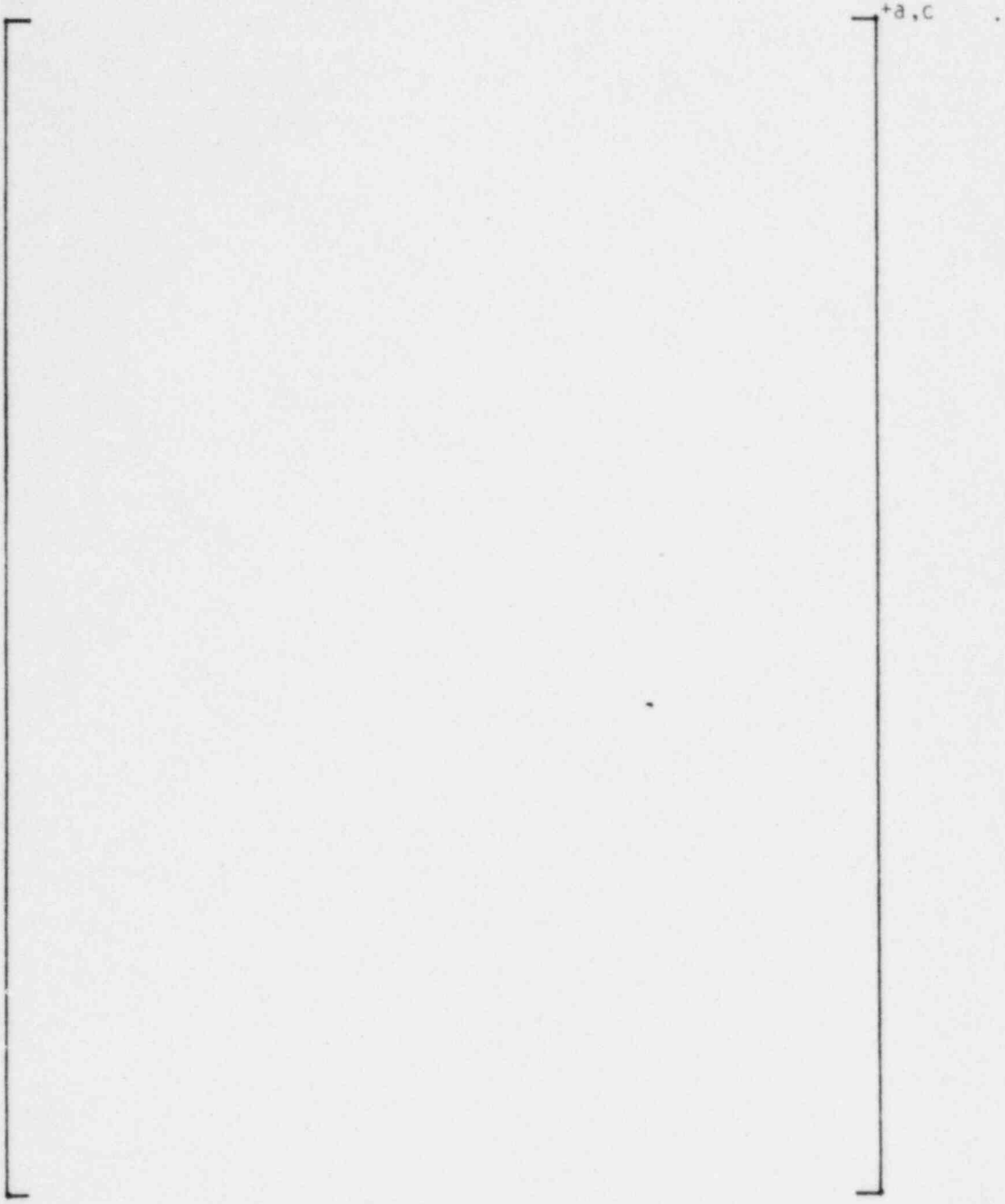


FIGURE S48
2 OF 3 HIGH FEED FLOW CHANNELS FAIL

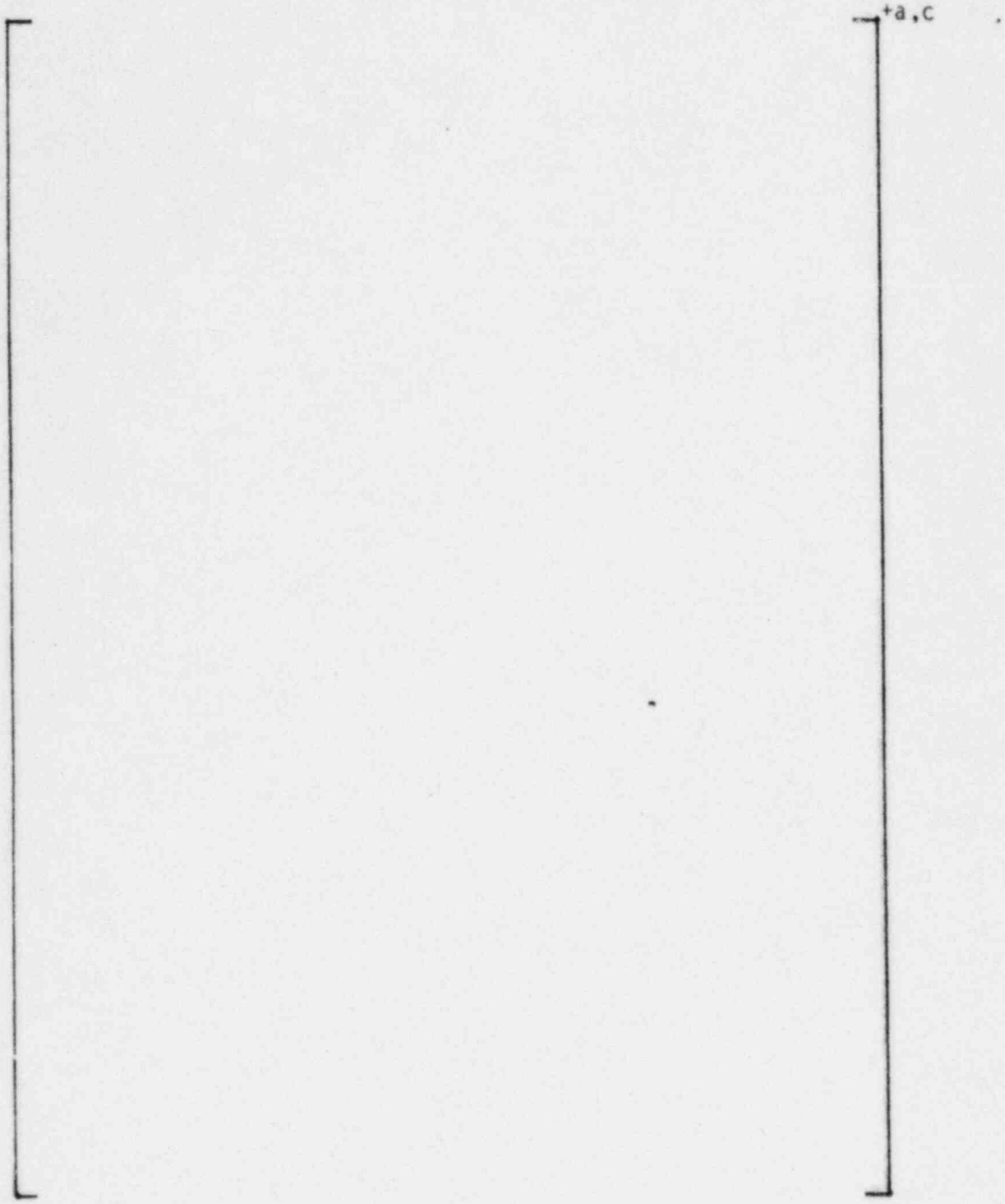


FIGURE S49
TIME DELAY CIRCUIT FAILS

[+a,c]

FIGURE S50
3 OF 4 LOW RCS FLOW AND LOW RCS TEMPERATURE CHANNELS FAIL

+a,c

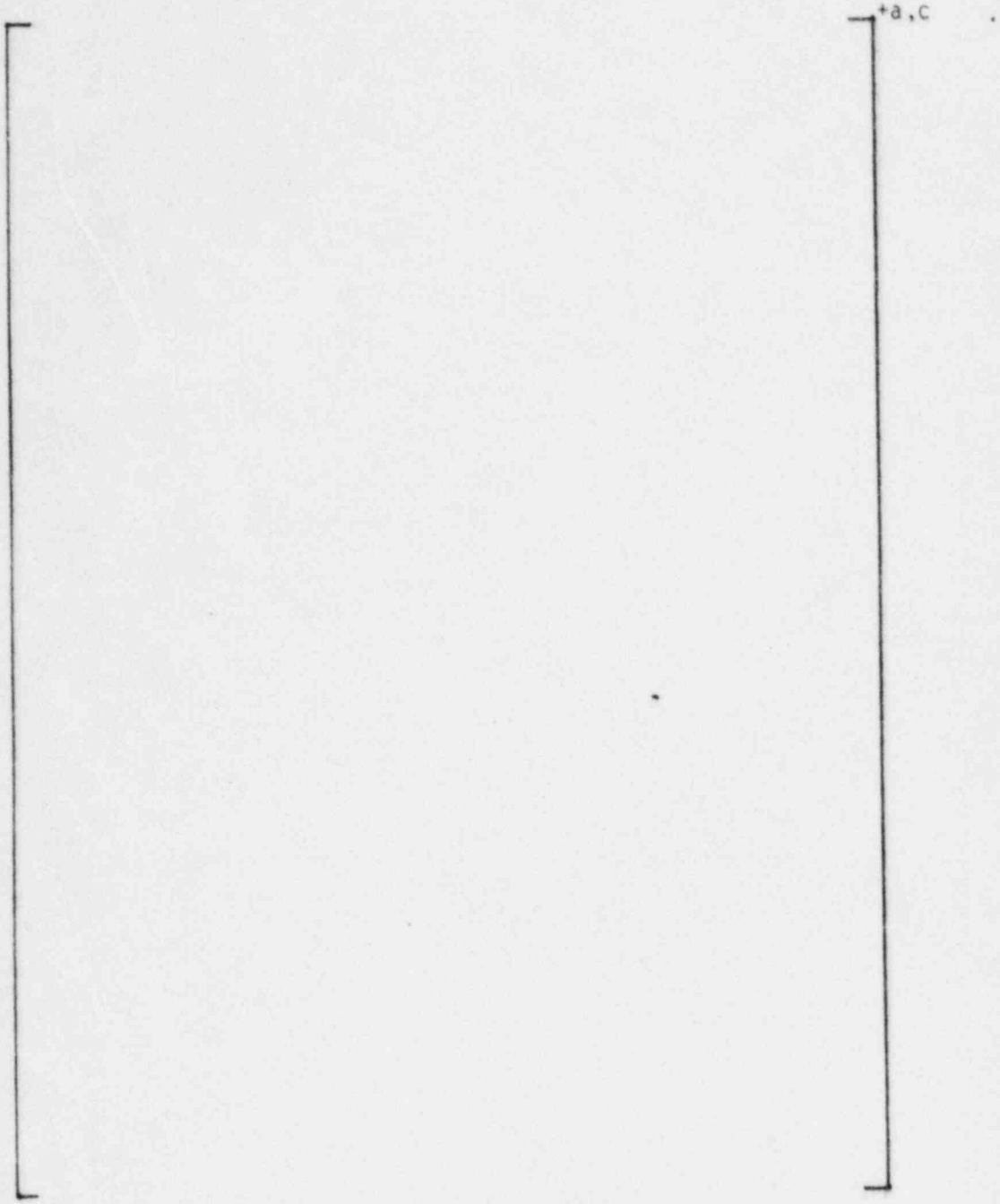


FIGURE S51
2 OF 3 LOW RCS FLOW CHANNELS FAIL

[+a,c]

FIGURE S52
LOW RCS FLOW AND LOW RCS
TEMPERATURE SIGNALS FROM 1-LOOP
FAILS

+a,c

FIGURE S53
RCP BUS UNDERVOLTAGE SIGNAL FAILS

+a,c

FIGURE S54
2 OF 3 BUS UNDERVOLTAGE
CHANNELS FAIL

+a,c

FIGURE S55
LOW Tcold FEEDWATER ISOLATION
SIGNAL FAILS

+a,c

FIGURE S56
LOW Tcold AND HIGH FEED FLOW
SIGNALS FAIL

[+a,c]

FIGURE S57
LOW Tcold BLOCKING CIRCUITS FAIL

[+a,c]

FIGURE S58
LOW Tcold CIRCUIT
PERMISSIVES FAIL

+a,c

FIGURE S59
LOW Tcold LOGIC FAILS

+a,c

FIGURE S60
2 OF 3 LOW Tcold CHANNELS FAIL

[+a,c]

FIGURE S61
P-11 TO LOW Tcold CIRCUIT FAILS

[+a,c]

FIGURE S62
2 OF 3 PRESSURIZER PRESSURE
CHANNELS TO P-11 TO LOW Tcold
CIRCUIT FAIL

[+a,c]

FIGURE S63
LOW Tcold AND LOW STEAM PRESSURE
SIGNALS FAIL

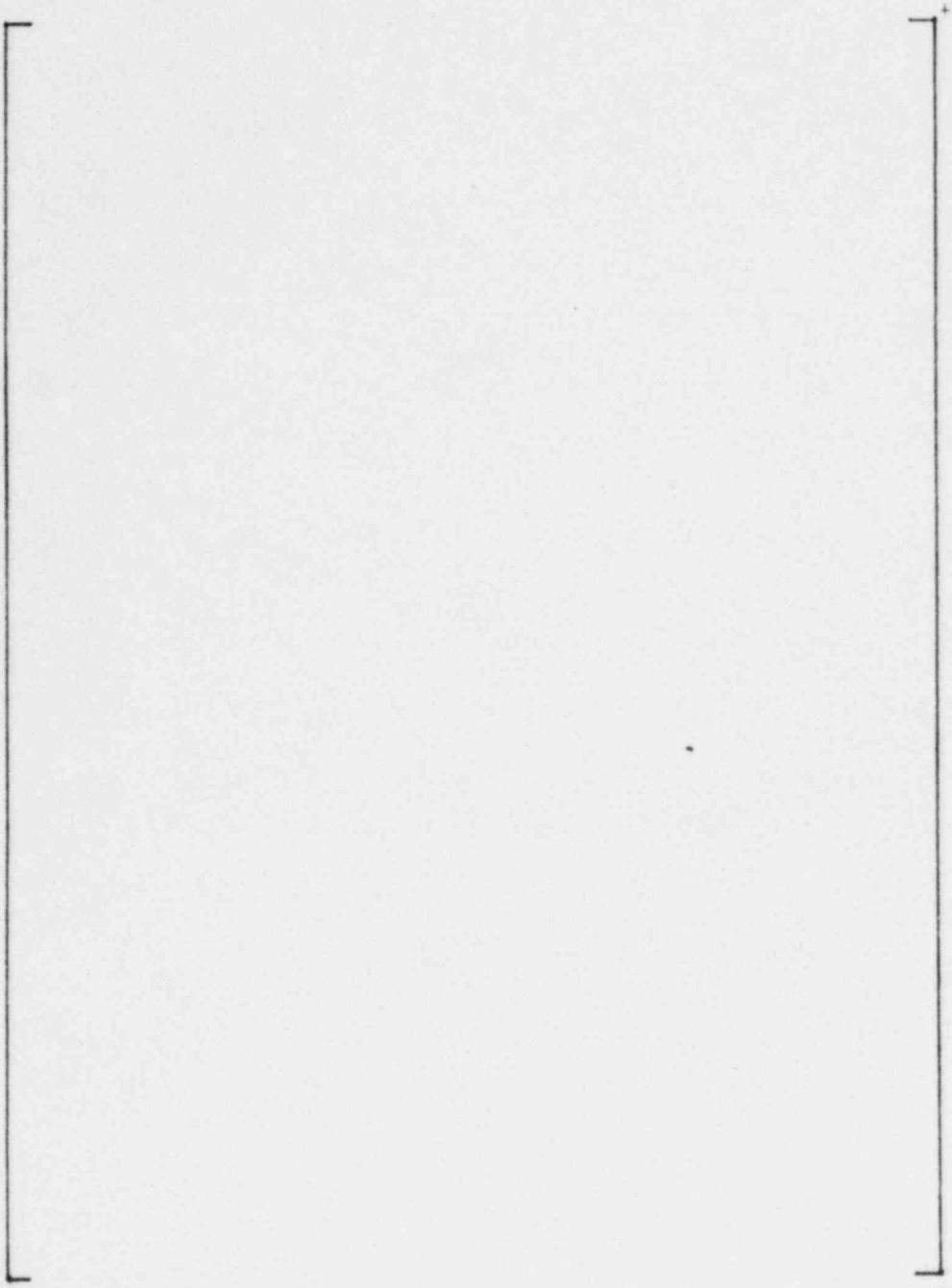


FIGURE S64
2 OF 3 LOW STEAM PRESSURE CHANNELS
TO LOW Tcold CIRCUIT FAIL

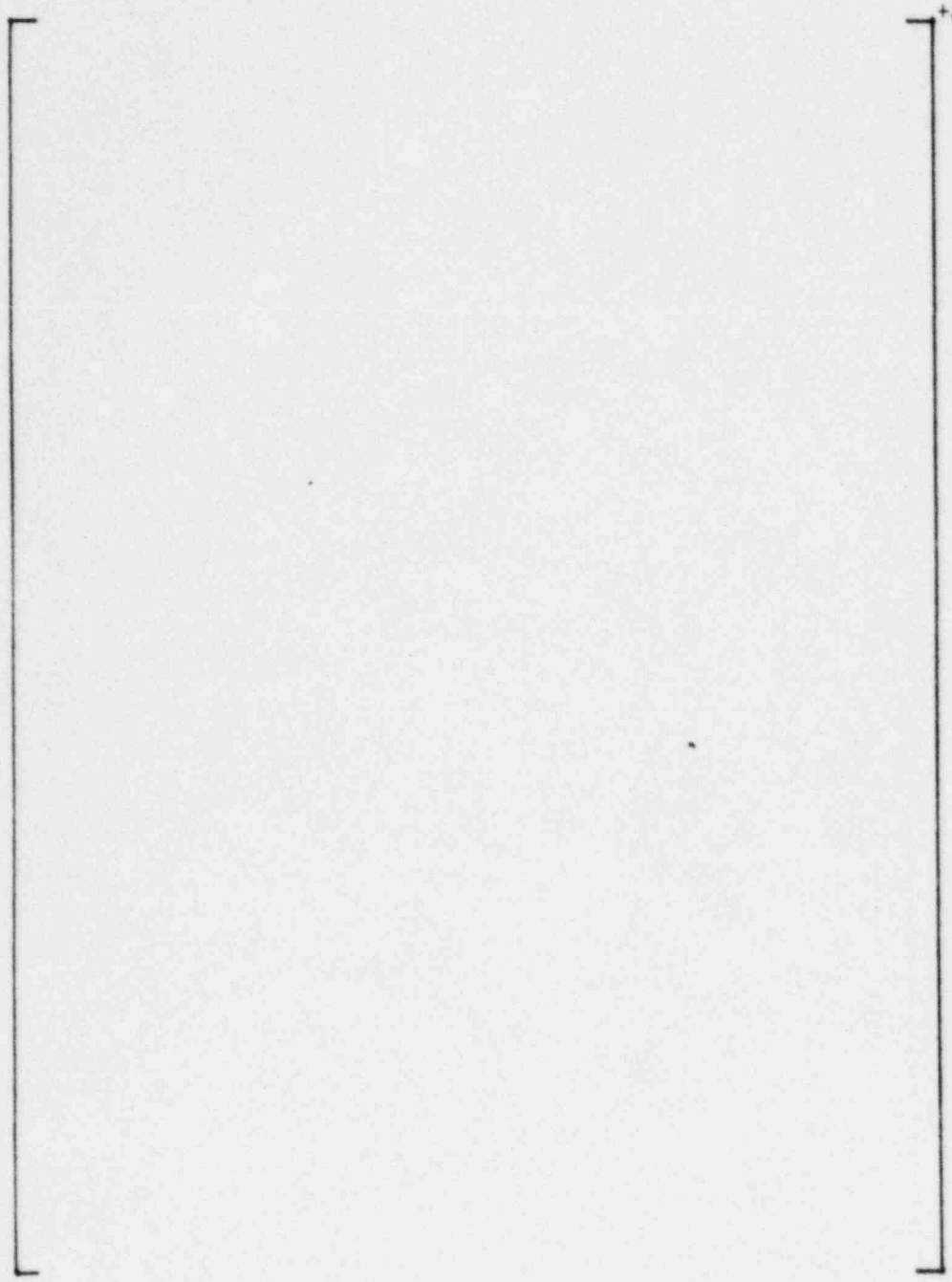


FIGURE S65
LOW Tcold CHANNELS OR P-15
PERMISSIVES FAIL

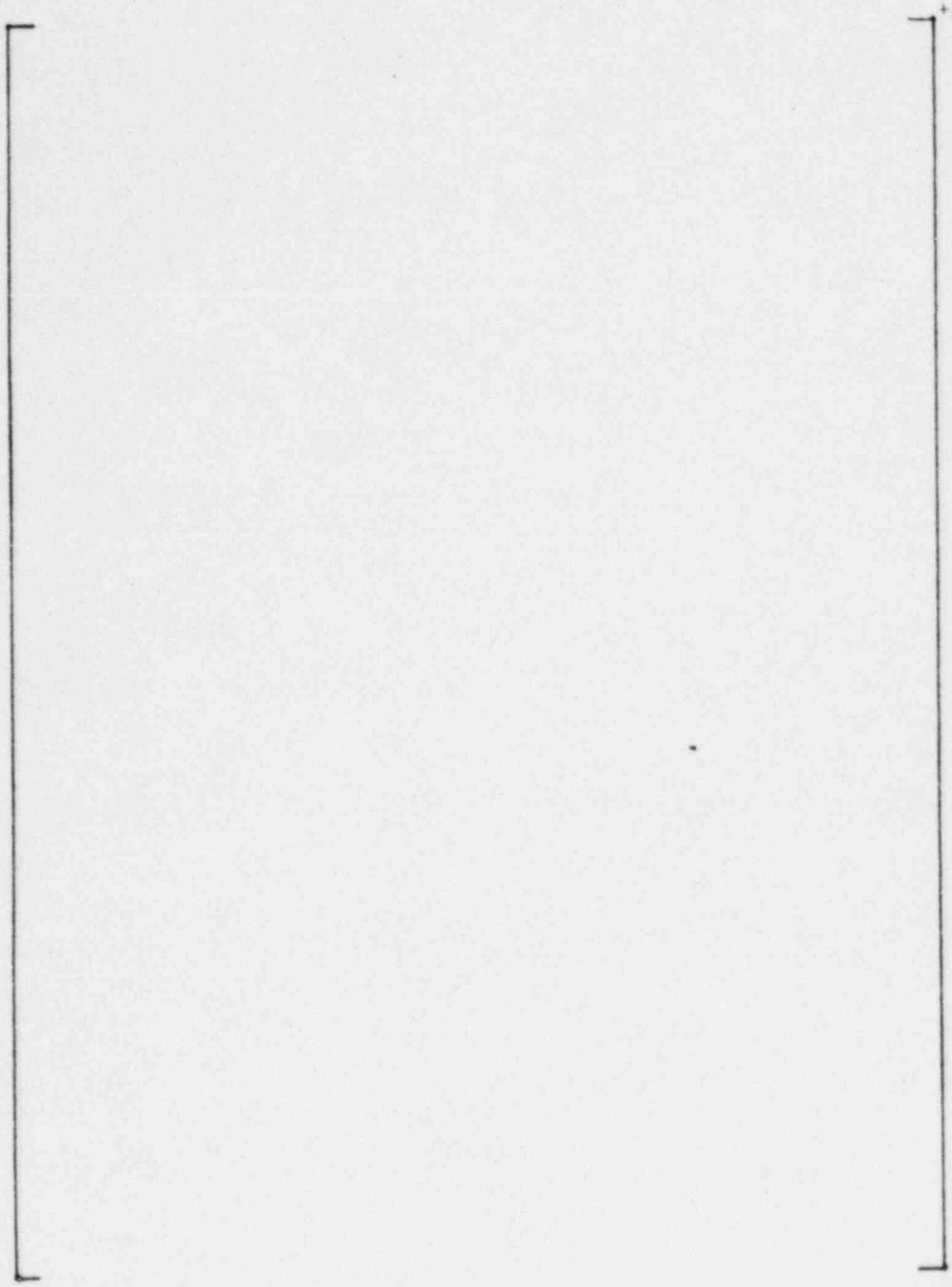


FIGURE S66
PERMISSIVE P-15 FAILS HIGH

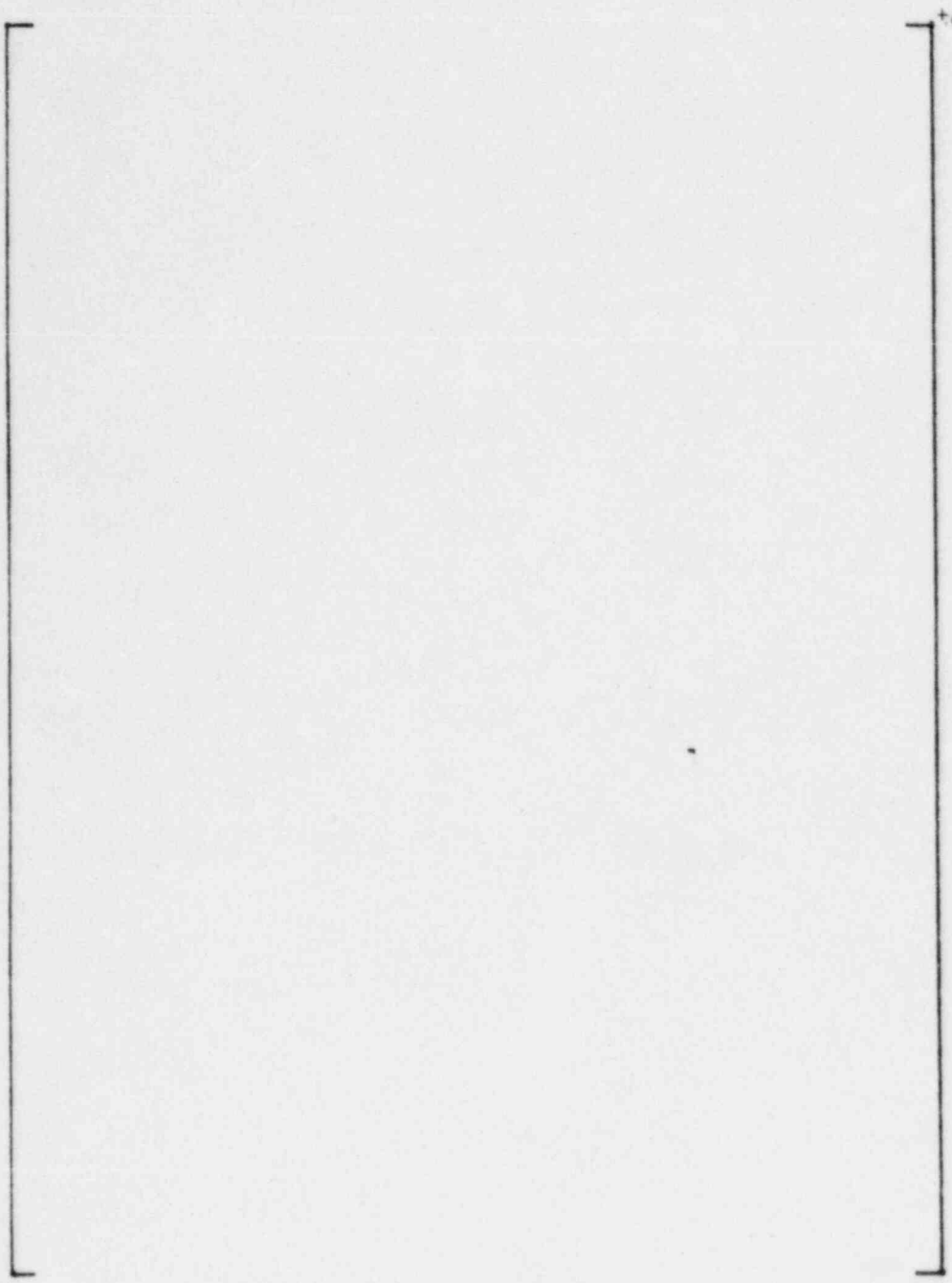


FIGURE S67
3 OF 4 POWER RANGE CHANNELS
TO P-15 FAIL

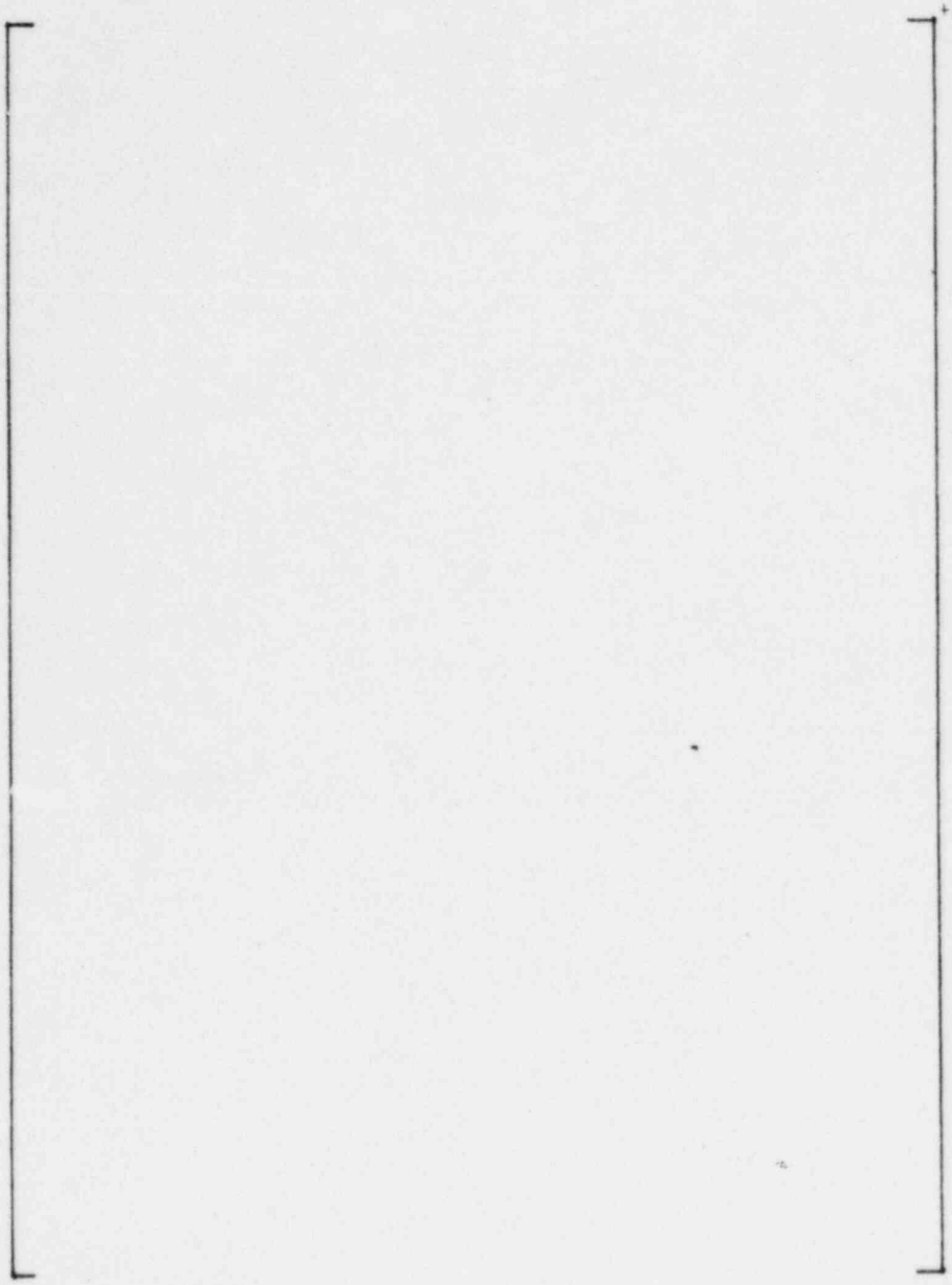


FIGURE R1
SAFETY INJECTION FAILS

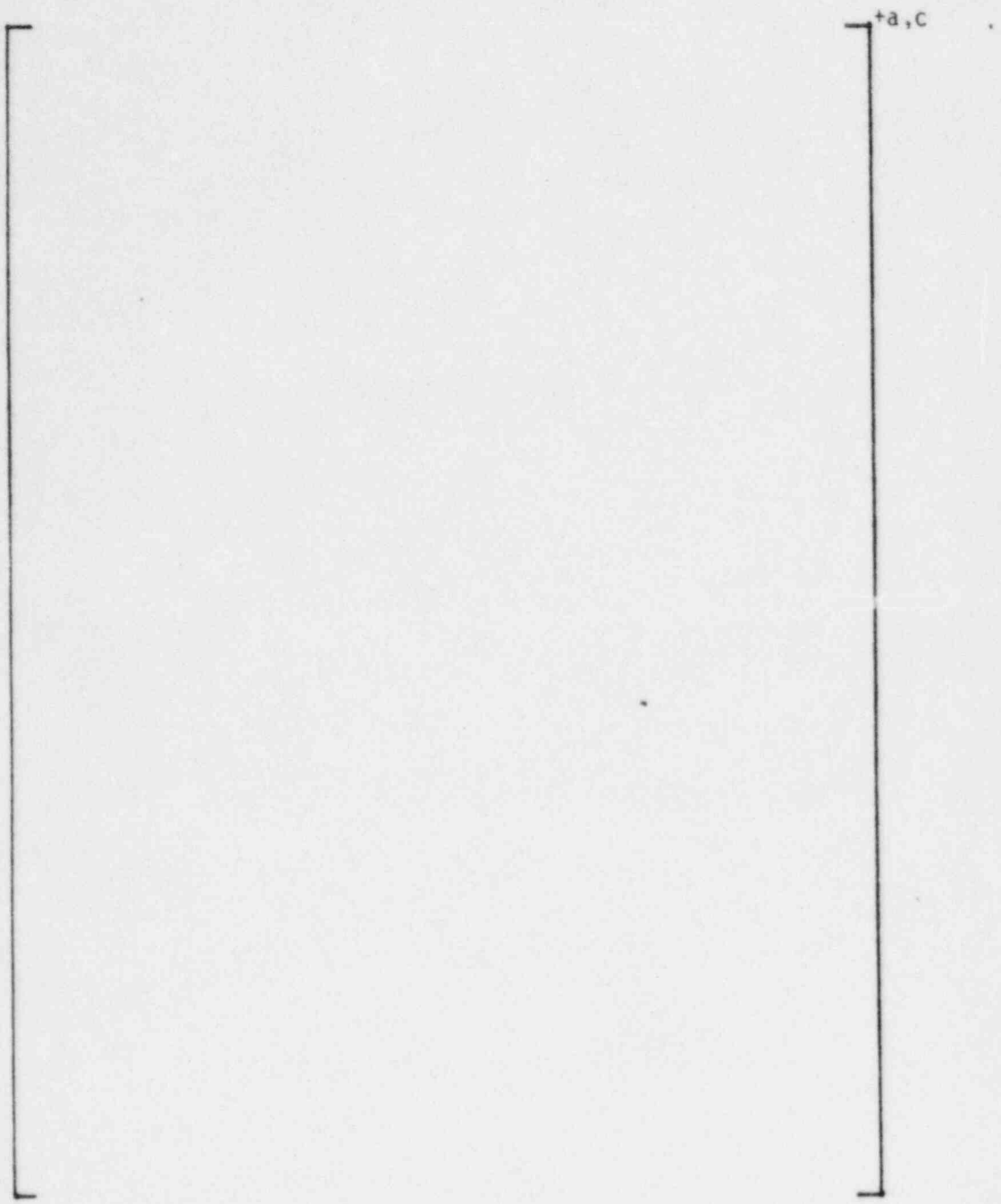


FIGURE R2
SLAVE RELAYS A1 AND C1 TO SI FAIL

+a,c

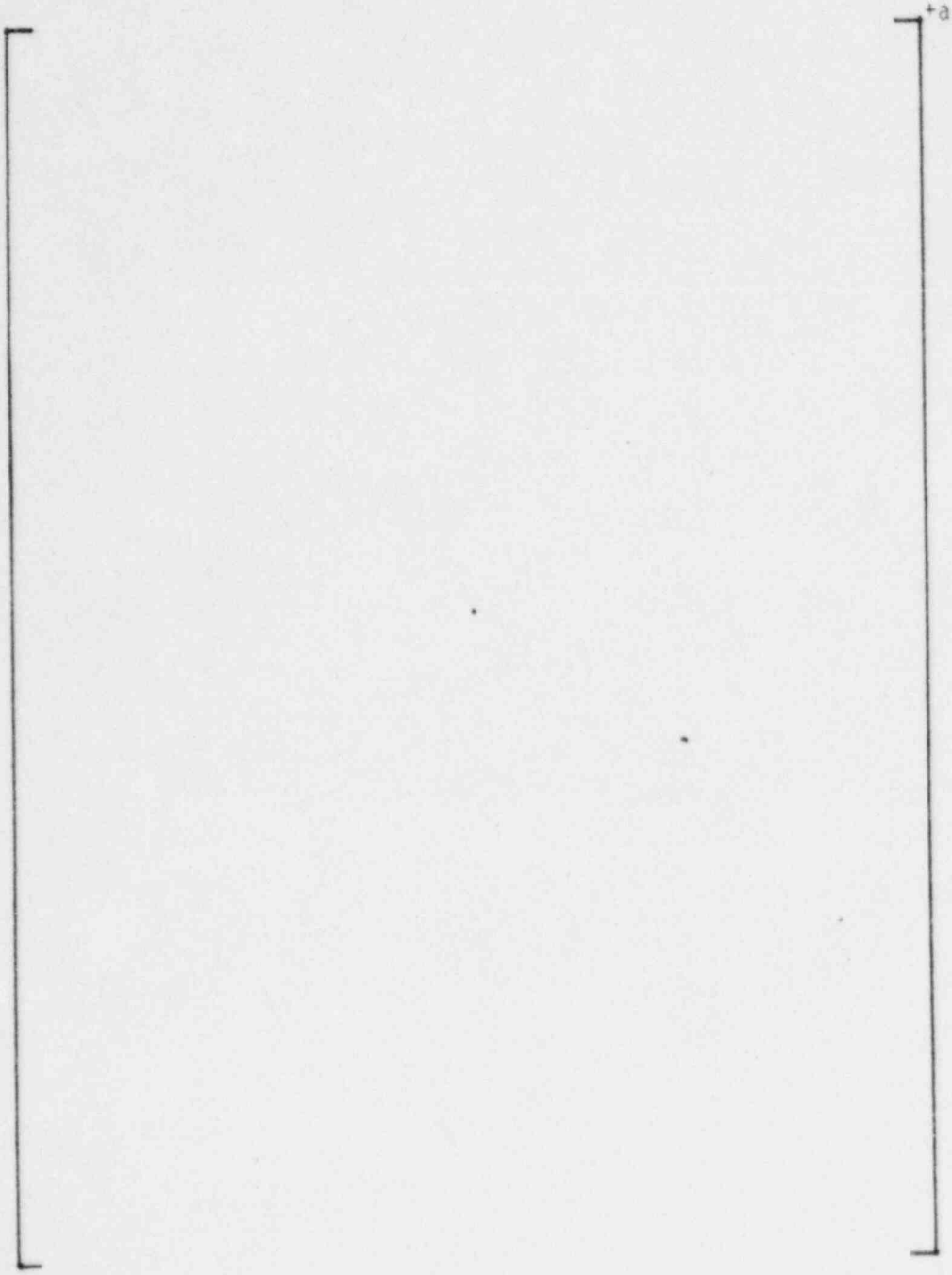


FIGURE R3
SLAVE RELAYS A2 AND C2 TO SI FAIL

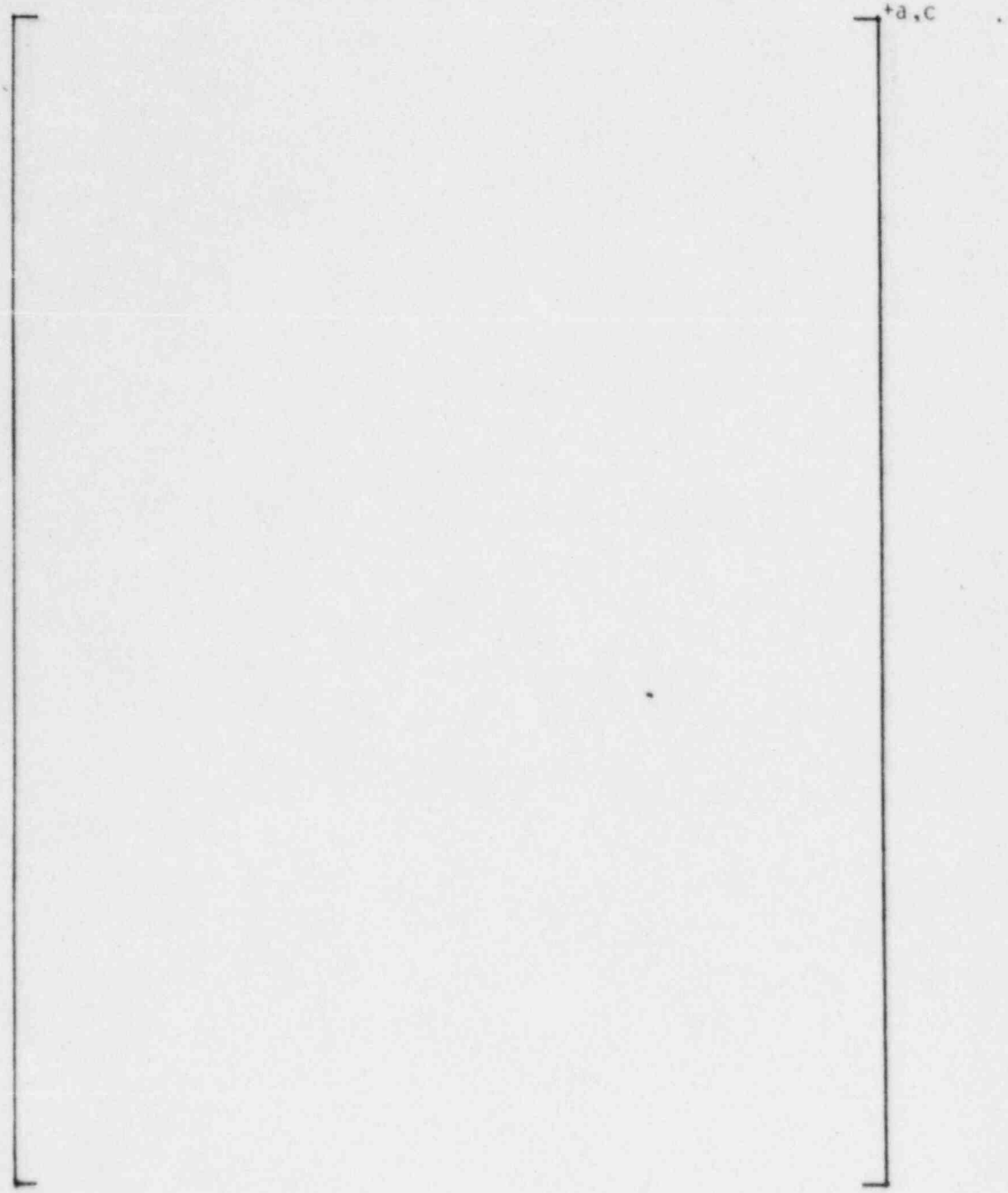


FIGURE R4
SLAVE RELAYS A3 AND C3 TO SI FAIL

+a,c

FIGURE R5
SLAVE RELAYS B1 AND D1 TO SI FAIL

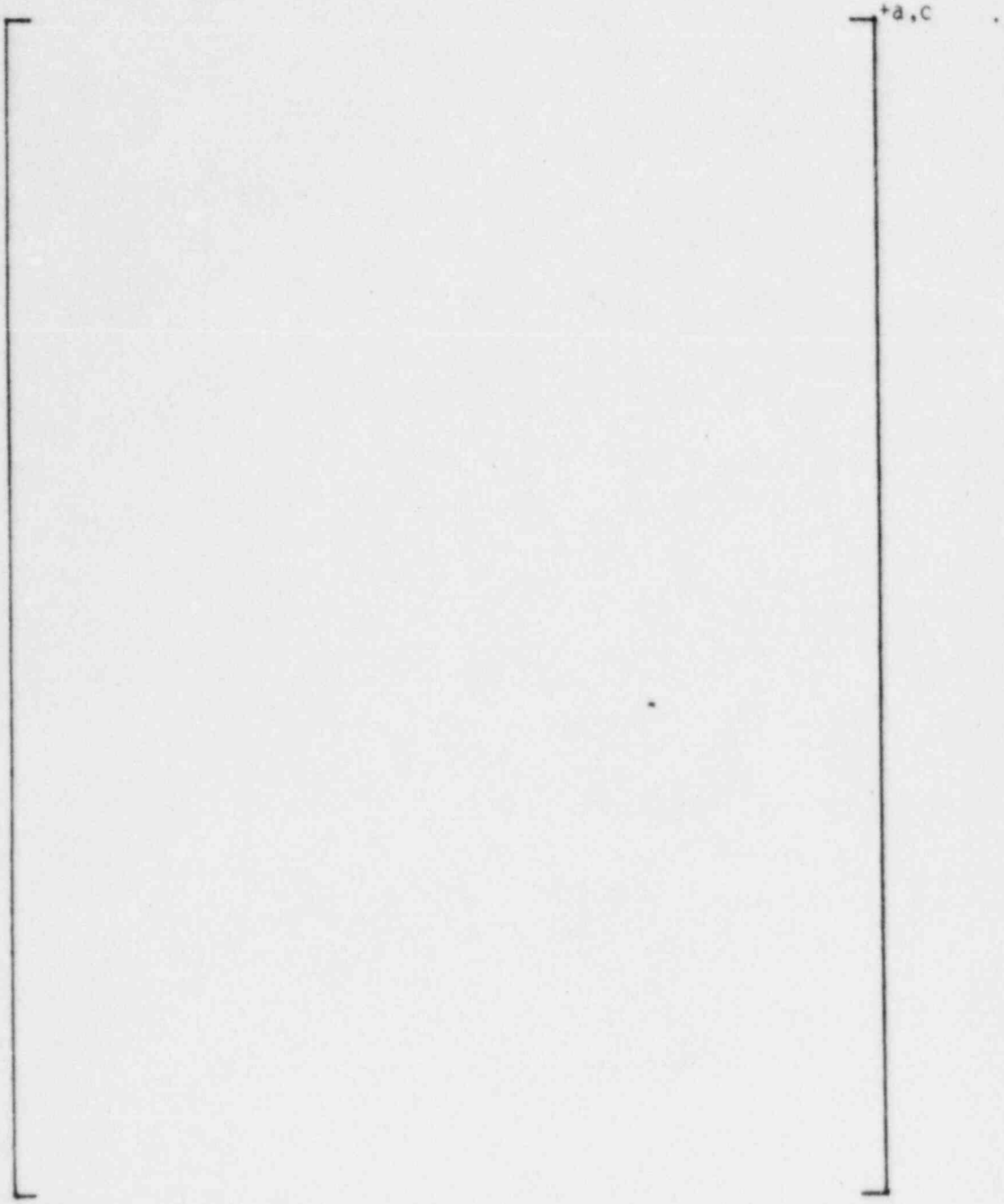


FIGURE R6
SLAVE RELAYS B2 AND D2 TO SI FAIL

+a,c

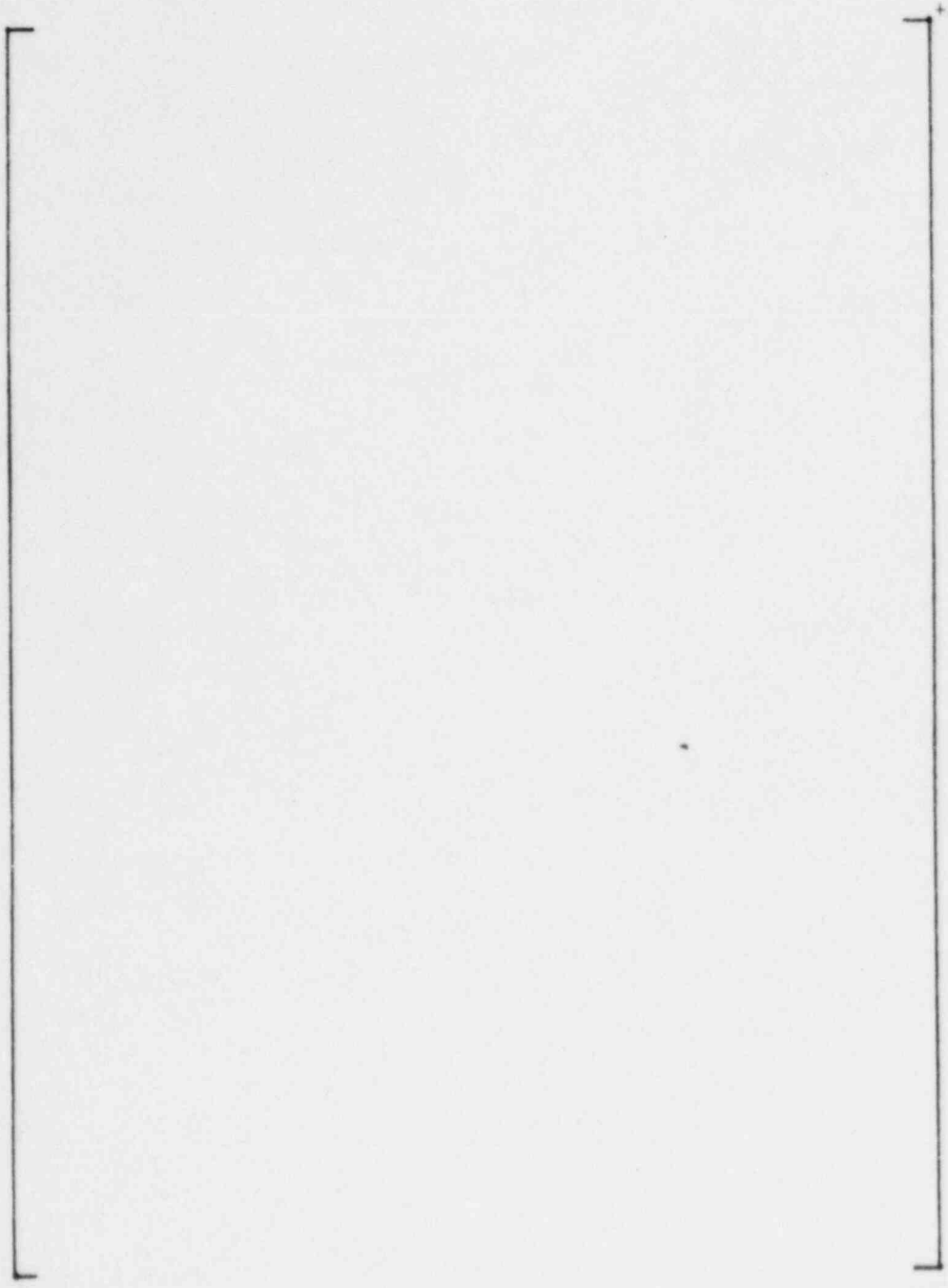


FIGURE R7
SLAVE RELAYS B3 AND D3 TO SI FAIL

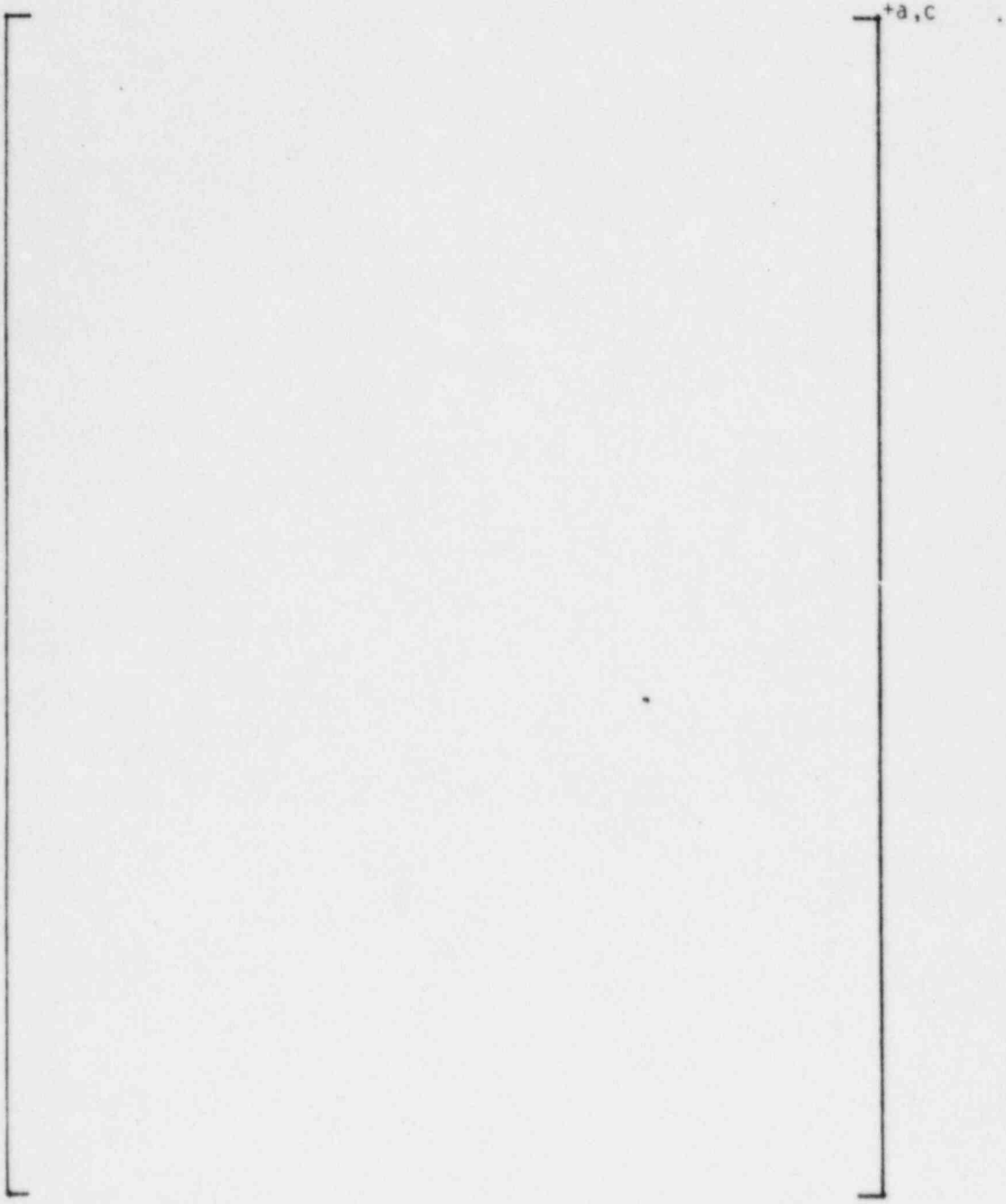


FIGURE R8
STEAMLINE ISOLATION FAILS

+a,c

FIGURE R9
SLAVE RELAYS A1 AND B1 TO
STEAMLINE ISOLATION FAIL

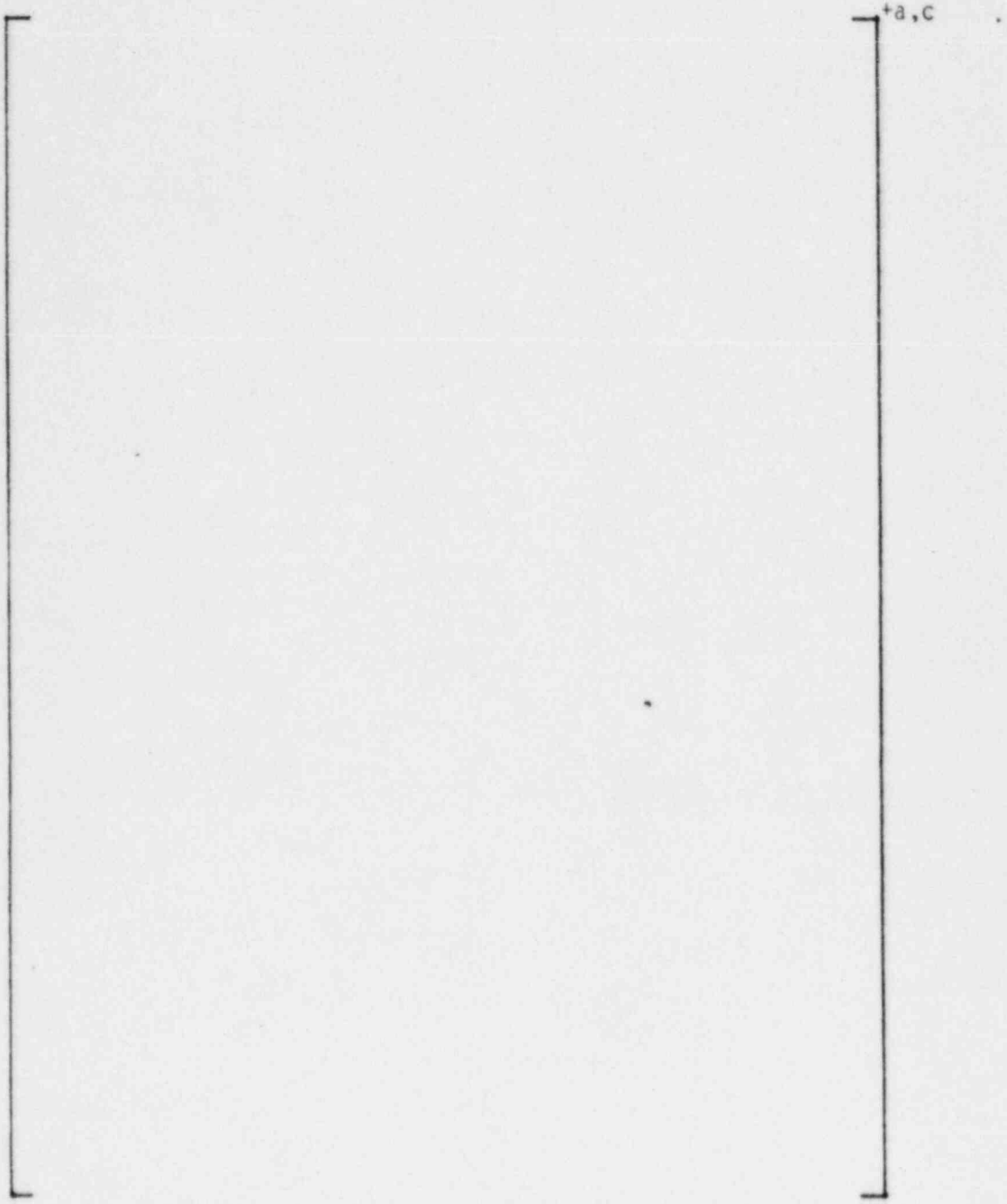


FIGURE R10
SLAVE RELAYS A2 AND B2 TO
STEAMLINE ISOLATION FAIL

+a,c

FIGURE R11
SLAVE RELAYS A3 AND B3 TO
STEAMLINE ISOLATION FAIL

[+a,c .

]

FIGURE R12
PRESSURIZER PRESSURE SIGNAL FAILS

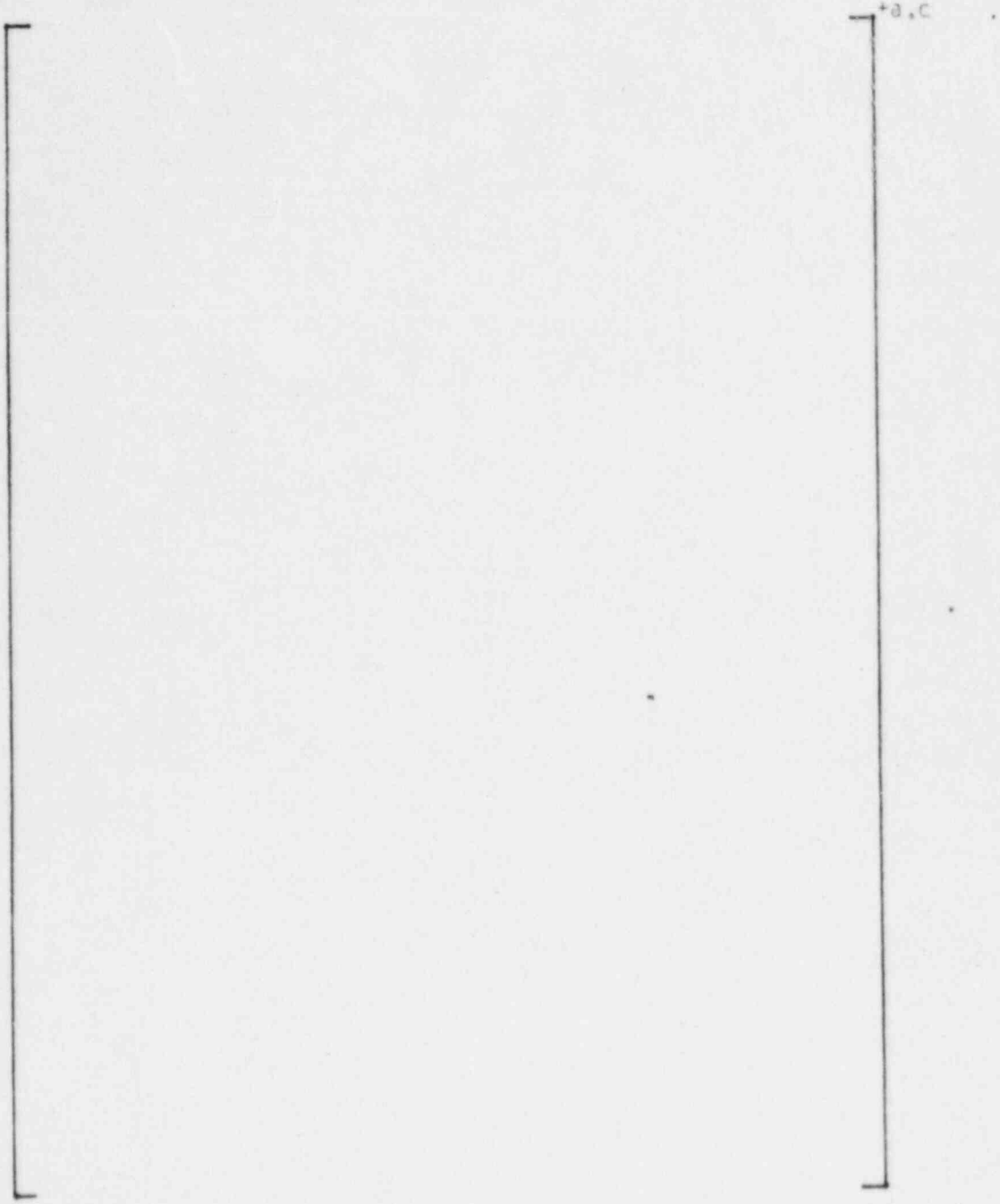


FIGURE R13
2 OF 3 PRESSURIZER PRESSURE
CHANNELS AND P-11 FAIL

[+a,c]

FIGURE R14
LOW STEAMLINE PRESSURE (3 OF 4)
SIGNALS FAIL

[+a,c]

FIGURE R15
LOW STEAMLINE PRESSURE (2 OF 3)
SIGNALS FAIL

[+a,c]

FIGURE R16
LOW STEAMLINE PRESSURE (2 OF 4)
AND P-12 (2 OF 4) SIGNAL FAILS

[+a,c]

FIGURE R17
LOW STEAMLINE PRESSURE (2 OF 3)
AND P-12 (2 OF 4) SIGNAL FAILS

[+a,c]

FIGURE R18
HIGH CONTAINMENT PRESSURE (2 OF 3)
SIGNAL FAILS

[+a,c]

FIGURE R19
HIGH-HIGH CONTAINMENT PRESSURE
(3 OF 4) SIGNAL FAILS

[+a,c]

FIGURE R20
HIGH STEAM FLOW (2 OF 4)
SIGNAL FAILS

+a,c

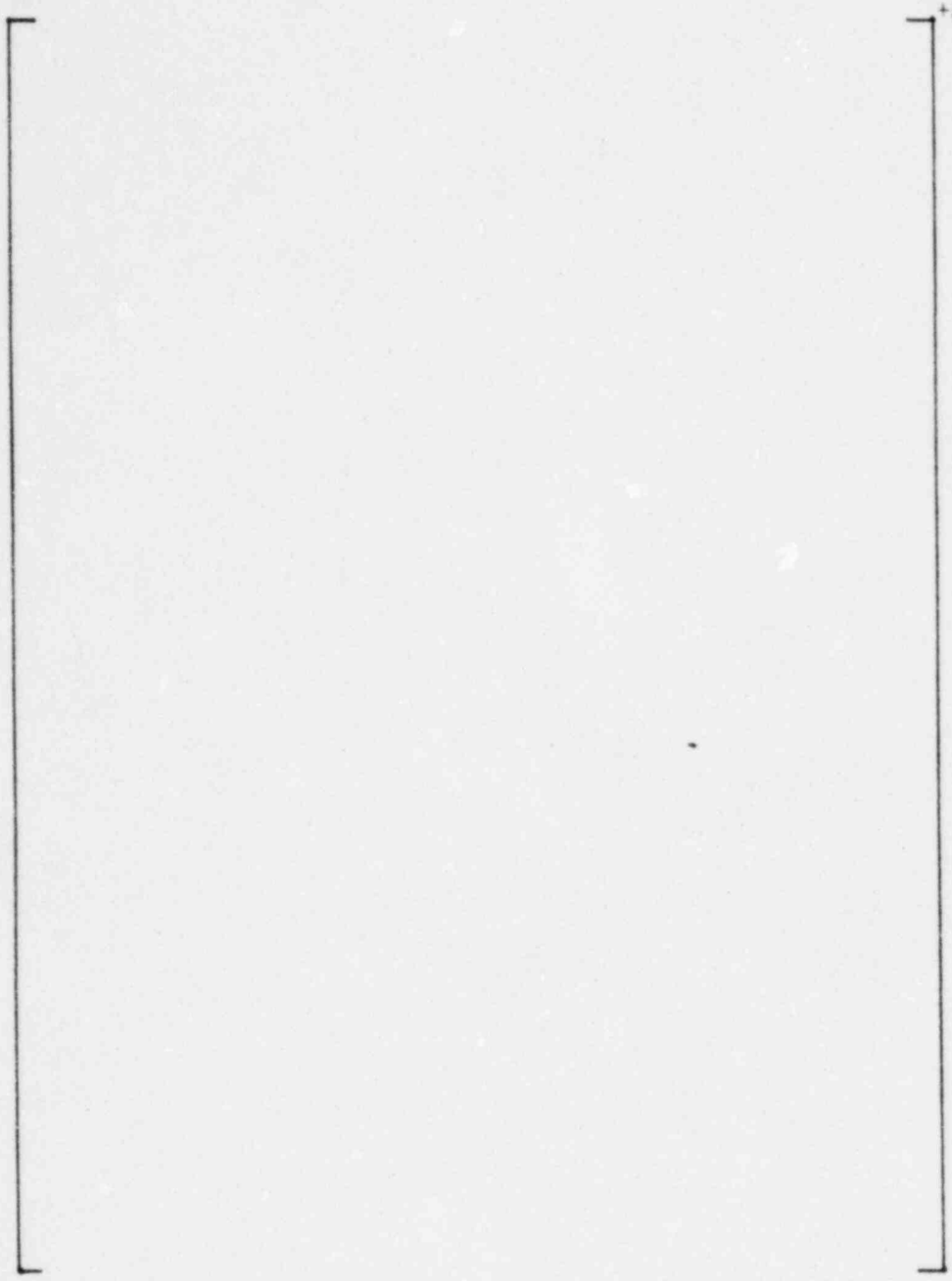


FIGURE R21
LOW-LOW Tavg (3 OF 4) AND LOW
STEAM PRESSURE (3 OF 4)
CHANNELS FAIL

[+a,c]

FIGURE R22
LOW-LOW Tavg (3 OF 4) AND LOW
STEAM PRESSURE (2 OF 3)
CHANNELS FAIL

+a,c

FIGURE R23
HIGH STEAM FLOW (2 OF 3)
SIGNAL FAILS

[+a,c]

FIGURE R24
LOW-LOW Tavg (2 OF 3) AND LOW
STEAM PRESSURE (3 OF 4)
CHANNELS FAIL

[[+a,c]

FIGURE R25
LOW-LOW Tavg (2 OF 3) AND LOW
STEAM PRESSURE (2 OF 3)
CHANNELS FAIL

[+a,c]

FIGURE R26
HIGH DIFFERENTIAL STEAMLINE
PRESSURE SIGNAL FAILS

+a,c

FIGURE R27
HIGH DIFFERENTIAL STEAMLINE
PRESSURE AND P-11 FAIL

+a,c

FIGURE R28
HIGH STEAM FLOW AND LOW-LOW Tavg
AND LOW STEAM PRESSURE
SIGNAL FAILS

+a,c

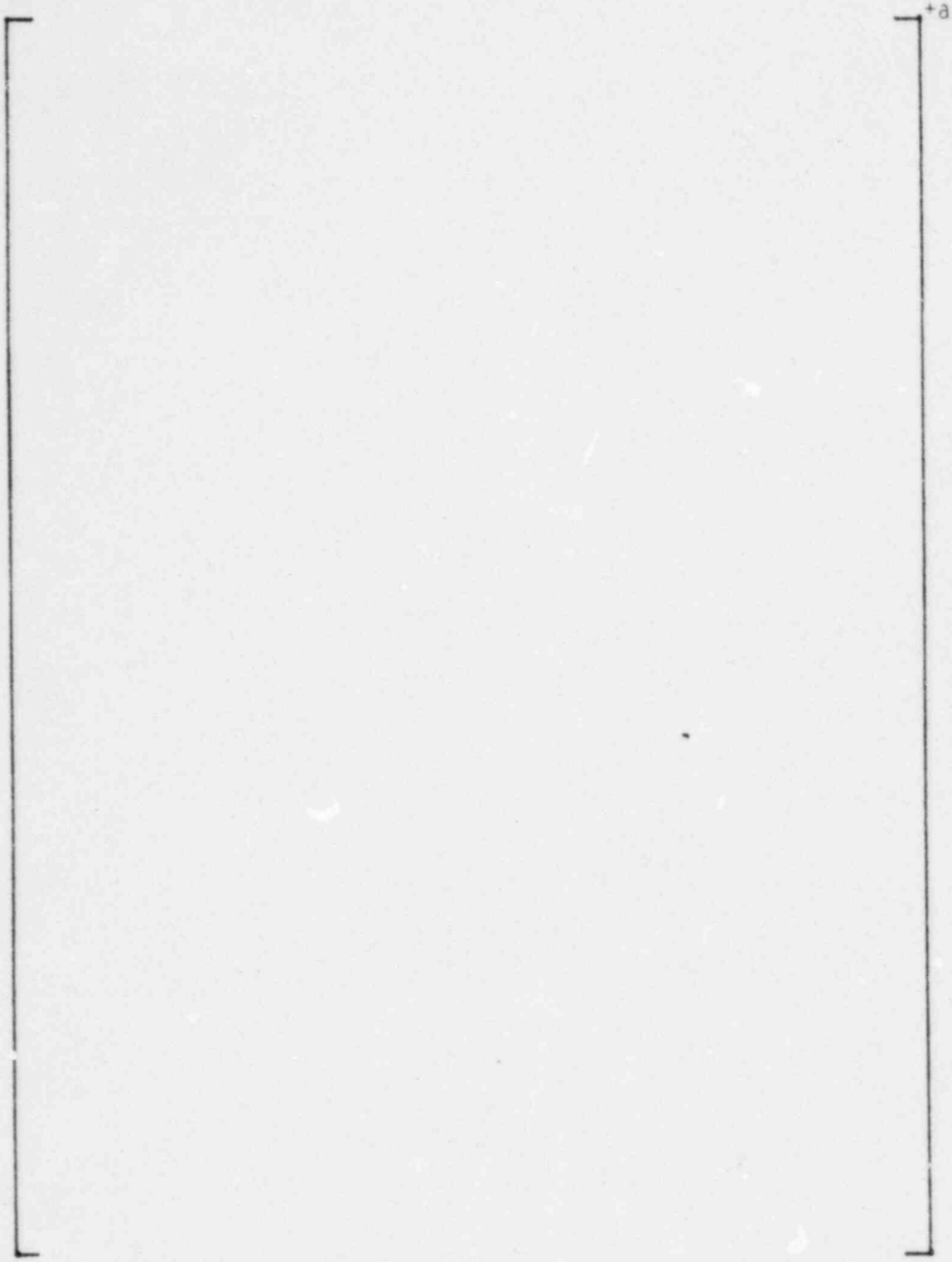


FIGURE R29
3 OUT OF 4 BISTABLES
DO NOT REMOVE POWER

+a,c

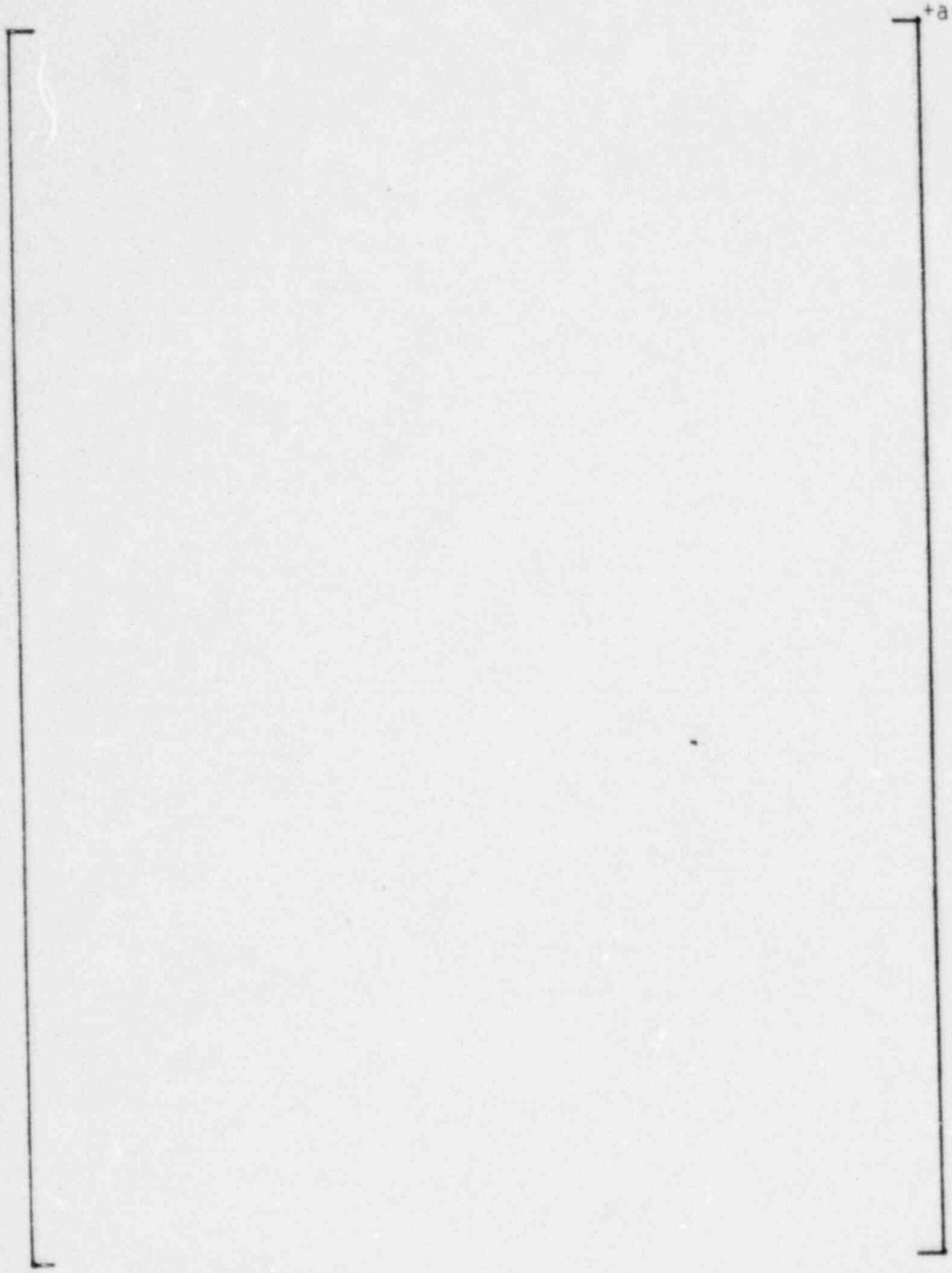


FIGURE R30
2 OUT OF 3 BISTABLES
DO NOT REMOVE POWER

+a,c

FIGURE R31
HIGH-HIGH STEAM FLOW OR HIGH
STEAM FLOW AND LOW Tavg
SIGNAL FAILS

+a,c

FIGURE R32
LOW Tavg (3 OF 4) OR LOW STEAM
PRESSURE (2 OF 2) CHANNELS FAIL
SIGNAL FAILS

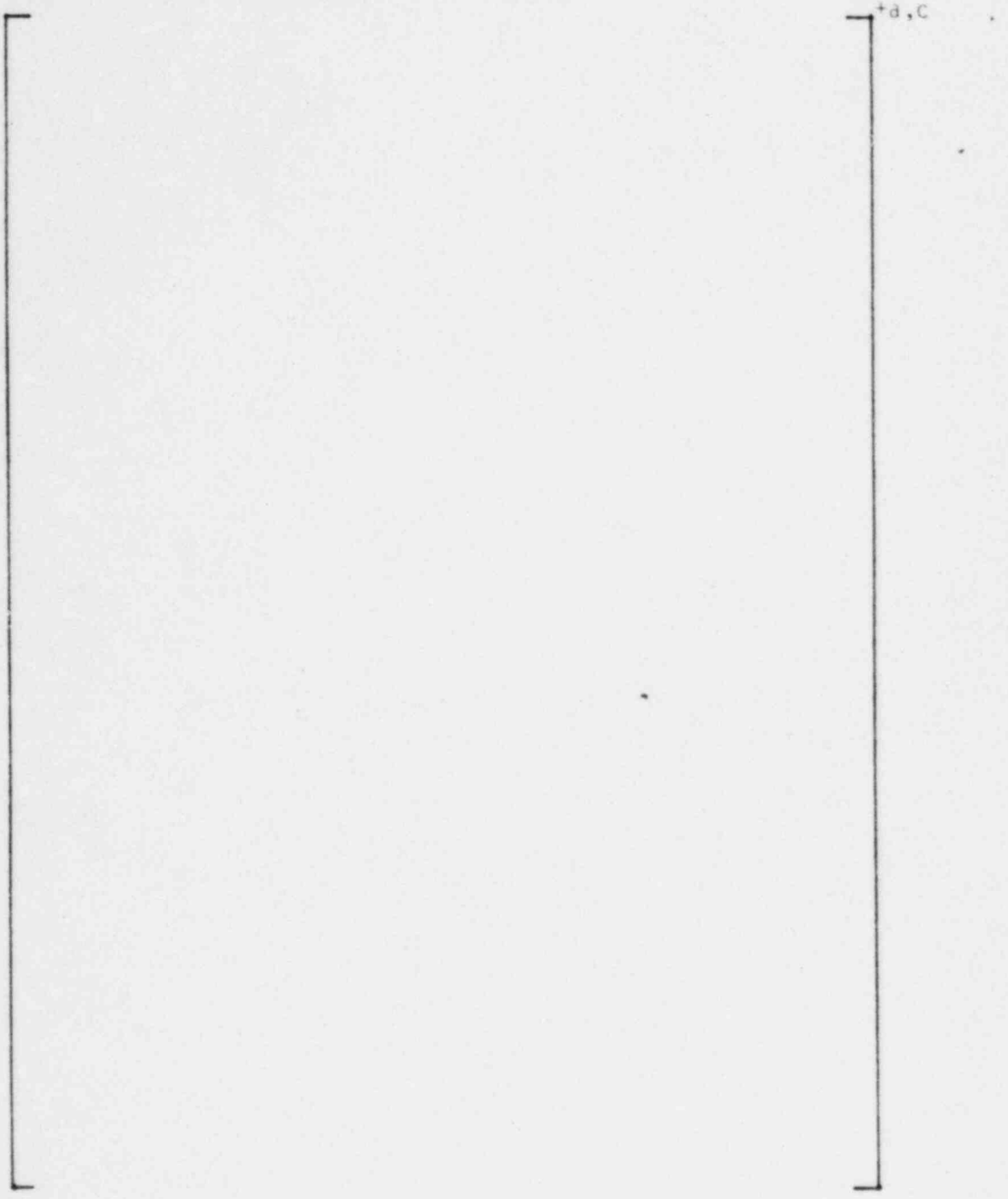


FIGURE R33
3 OF 4 STEAM GENERATOR WATER LEVEL
CHANNELS FAIL TO PROVIDE SIGNAL

[+a,c

]

FIGURE R34
2 OF 3 STEAM GENERATOR WATER LEVEL
CHANNELS FAIL TO PROVIDE SIGNAL

[+a,c]

FIGURE B1
DIFFERENTIAL STEAM PRESSURE
BISTABLE CHANNEL FAILS

+a,c

FIGURE B2
PRESSURIZER PRESSURE BISTABLE
CHANNEL FAILS

[+a,c

]

FIGURE B3
STEAM FLOW BISTABLE
CHANNEL FAILS

+a,c

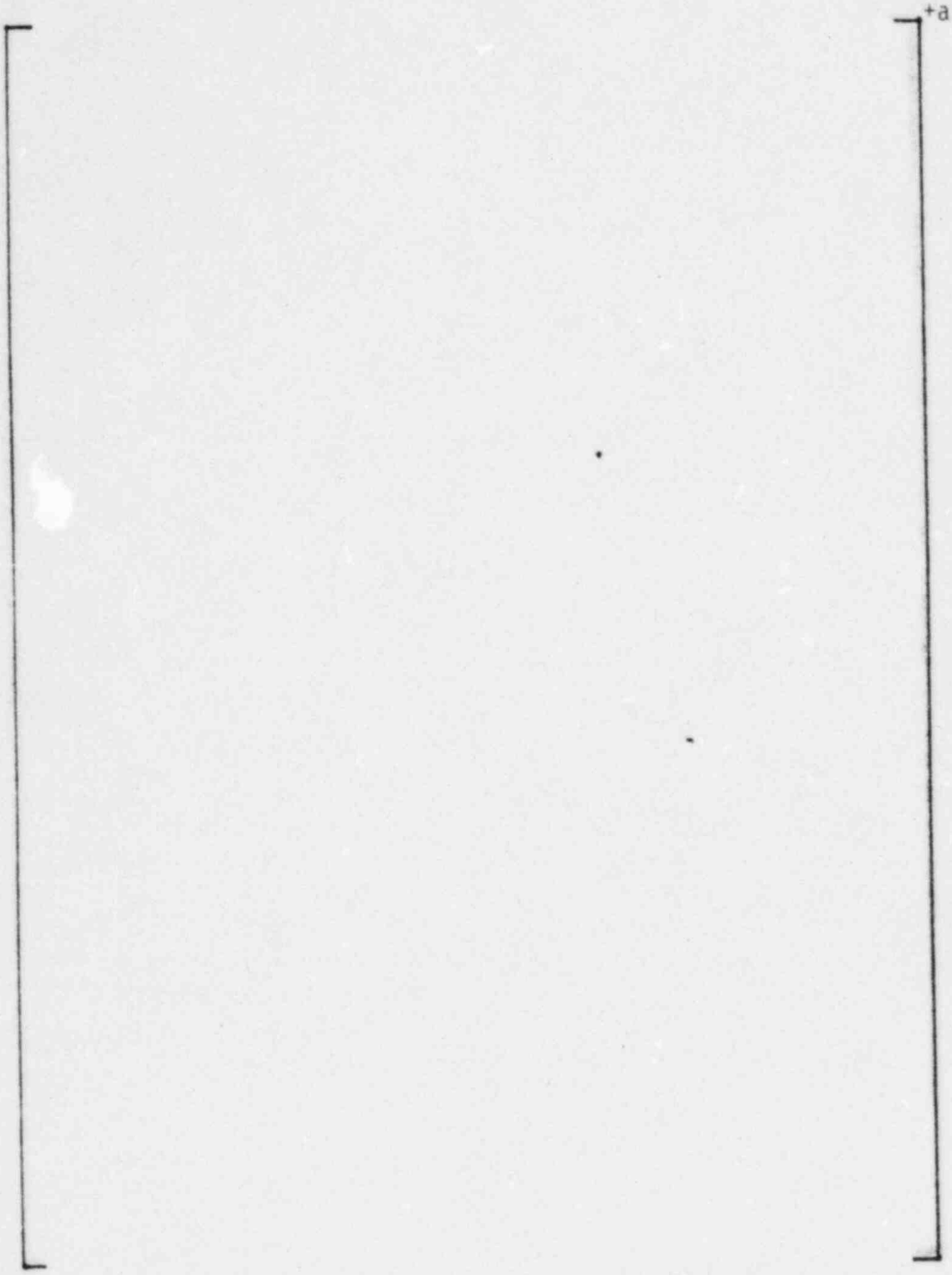


FIGURE B4
TYPE 1 BISTABLE CHANNEL FAILS

+a,c

FIGURE B5
Tavg BISTABLE CHANNEL FAILS