

7.0 INSTRUMENTATION AND CONTROL**TABLE OF CONTENTS**

7.1	INTRODUCTION.....	7.1-1
7.1.1	Identification of Safety-Related Systems.....	7.1-3
7.1.2	Identification of Safety Criteria.....	7.1-4
7.1.2.1	Design Bases.....	7.1-5
7.1.2.2	Independence of Redundant Safety-Related Systems.....	7.1-10
7.1.2.3	Physical Identification of Safety-Related Equipment	7.1-12
7.1.2.4	Conformance to IEEE 317-1971	7.1-12
7.1.2.5	Conformance to IEEE 323-1971	7.1-13
7.1.2.6	Conformance to IEEE 336-1971	7.1-13
7.1.2.7	Conformance to IEEE 338-1971	7.1-13
7.1.2.8	Conformance to Regulatory Guide 1.22	7.1-14
7.1.2.9	Conformance to IEEE 334-1971	7.1-15
7.1.2.10	Conformance to 10 CFR 50.62	7.1-15
7.1.2.11	Conformance to NUREG-0737	7.1-15
7.1.3	Detailed Electrical Instrumentation and Control Drawings	7.1-16
7.1.3.1	Identification and Purpose	7.1-16
7.2	REACTOR TRIP SYSTEM.....	7.2-1
7.2.1	Description	7.2-1
7.2.1.1	System Description	7.2-2
7.2.1.2	Design Bases: IEEE 279-1971	7.2-14
7.2.1.3	Final System Drawings	7.2-17
7.2.2	Analysis	7.2-18
7.2.2.1	Failure Mode and Effects Analysis.....	7.2-18
7.2.2.2	Evaluation of Compliance to Applicable Codes and Standards....	7.2-20
7.2.2.3	Specific Control and Protection Interactions	7.2-30
7.2.3	Tests and Inspections	7.2-34

TABLE OF CONTENTS

7.2.3.1	Inservice Tests and Inspections.....	7.2-34
7.2.3.2	Periodic Testing of the Nuclear Instrumentation System	7.2-36
7.2.3.3	Periodic Testing of the Process Analog Channels of the Protection Circuits	7.2-36
7.2.3.4	Regulatory Guide 1.22	7.2-37
7.3	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM.....	7.3-1
7.3.1	Description	7.3-1
7.3.1.1	System Description	7.3-1
7.3.1.2	Design Bases	7.3-6
7.3.1.3	Final System Drawings	7.3-9
7.3.2	Analysis	7.3-9
7.3.2.1	Evaluation of Compliance with IEEE 279-1971	7.3-10
7.3.2.2	Evaluation of Compliance with IEEE 308-1971	7.3-16
7.3.2.3	Evaluation of Compliance with IEEE 323-1971	7.3-16
7.3.2.4	Evaluation of Compliance with IEEE 334-1971	7.3-16
7.3.2.5	Evaluation of Compliance with IEEE 338-1971	7.3-17
7.3.2.6	Evaluation of Compliance with IEEE 344-1971	7.3-17
7.3.2.7	Response Time Testing	7.3-17
7.3.2.8	Further Considerations	7.3-18
7.3.2.9	Summary.....	7.3-18
7.4	SYSTEMS REQUIRED FOR SAFE SHUTDOWN.....	7.4-1
7.4.1	Description	7.4-1
7.4.1.1	Monitoring Indicators.....	7.4-2
7.4.1.2	Controls.....	7.4-2
7.4.1.3	Essential Services after Incident That Requires Hot Shutdown.....	7.4-5
7.4.1.4	Equipment and Systems Available for Cold Shutdown	7.4-6
7.4.2	Analysis	7.4-7

TABLE OF CONTENTS

7.5	POSTACCIDENT MONITORING DISPLAY INSTRUMENTATION	7.5-1
7.5.1	Description	7.5-1
7.5.2	Analysis	7.5-2
7.5.3	Deleted	7.5-3
7.5.4	Inadequate Core Cooling Monitoring System.....	7.5-3
7.5.4.1	Reactor Vessel Level	7.5-3
7.5.4.2	Subcooling Margin Monitor	7.5-4
7.5.4.3	Core Exit Temperature.....	7.5-4
7.5.5	Nuclear Instrumentation	7.5-4
7.6	ALL OTHER SYSTEMS REQUIRED FOR SAFETY.....	7.6-1
7.6.1	Instrumentation and Control Power Supply System	7.6-1
7.6.1.1	Description	7.6-1
7.6.1.2	Analysis.....	7.6-1
7.6.2	Residual Heat Removal Isolation Valves.....	7.6-3
7.6.2.1	Description	7.6-3
7.6.2.2	Analysis.....	7.6-4
7.6.3	Refueling Interlocks	7.6-4
7.6.4	Monitoring Combustible Gas in Containment.....	7.6-6
7.6.4.1	Description	7.6-6
7.6.4.2	Analysis.....	7.6-7
7.6.5	Semiautomatic Backup to Switchover from Injection to Recirculation.....	7.6-7
7.6.6	Accumulator Motor-Operated Isolation Valves	7.6-7
7.7	CONTROL SYSTEMS NOT REQUIRED FOR SAFETY	7.7-1
7.7.1	Description	7.7-1
7.7.1.1	Reactor Control System.....	7.7-3
7.7.1.2	Rod Control System.....	7.7-4

TABLE OF CONTENTS

7.7.1.3	Plant Control Signals for Monitoring and Indicating	7.7-5
7.7.1.4	Plant Control System Interlocks	7.7-9
7.7.1.5	Pressurizer Pressure Control	7.7-9
7.7.1.6	Pressurizer Water Level Control	7.7-10
7.7.1.7	Steam Generator Water Level Control	7.7-10
7.7.1.8	Steam Dump Control	7.7-11
7.7.1.9	Incore Instrumentation	7.7-12
7.7.1.10	Control Board	7.7-14
7.7.1.11	Boron Concentration Measurement System	7.7-15
7.7.2	Analysis	7.7-17
7.7.2.1	Separation of Protection and Control Systems	7.7-18
7.7.2.2	Response Considerations of Reactivity	7.7-19
7.7.2.3	Step Load Changes Without Steam Dump	7.7-21
7.7.2.4	Loading and Unloading	7.7-21
7.7.2.5	Load Rejection Furnished by Steam Dump System	7.7-22
7.7.2.6	Turbine-Generator Trip with Reactor Trip	7.7-22
7.8	ATWS MITIGATION SYSTEM ACTUATION CIRCUITRY (AMSAC).....	7.8-1
7.8.1	Description	7.8-1
7.8.1.1	System Description	7.8-1
7.8.1.2	Equipment Description	7.8-1
7.8.1.3	Functional Performance Requirements	7.8-3
7.8.1.4	AMSAC Interlocks	7.8-3
7.8.1.5	Trip System	7.8-3
7.8.1.6	Isolation Devices	7.8-4
7.8.1.7	AMSAC Diversity From the Reactor Protection Systems	7.8-4
7.8.1.8	Power Supply	7.8-4
7.8.1.9	Environmental Variations	7.8-4
7.8.1.10	Setpoints	7.8-4
7.8.2	Analysis	7.8-5
7.8.2.1	Safety Classification/Safety-Related Interface	7.8-5
7.8.2.2	Redundancy	7.8-5
7.8.2.3	Diversity From Existing Trip System	7.8-5

TABLE OF CONTENTS

7.8.2.4	Electrical Independence.....	7.8-5
7.8.2.5	Physical Separation From the RTS and ESFAS.....	7.8-6
7.8.2.6	Environmental Qualification	7.8-6
7.8.2.7	Seismic Qualification.....	7.8-6
7.8.2.8	Test, Maintenance, and Surveillance Quality Assurance.....	7.8-6
7.8.2.9	Power Supply.....	7.8-7
7.8.2.10	Testability at Power.....	7.8-7
7.8.2.11	Inadvertent Actuation	7.8-7
7.8.2.12	Bypass	7.8-7
7.8.2.13	Completion of Mitigative Actions Once Initiated.....	7.8-8
7.8.2.14	Manual Initiation.....	7.8-8
7.8.2.15	Information Readout	7.8-8
7.8.2.16	Compliance With Standards and Design Criteria.....	7.8-9

LIST OF TABLES

- 7.1-1 List of Schematic Diagrams and Location Drawings for Safety-Related Equipment
- 7.2-1 List of Reactor Trips
- 7.2-2 Protection System Interlocks
- 7.2-3 Reactor Trip System Instrument Accuracies
- 7.2-4 Trip Correlation
- 7.2-5 Reactor Trip System Instrumentation Response Times
- 7.3-1 Functions Initiated by Engineered Safety Features Actuation System
- 7.3-2 Instrumentation Operating Conditions for Engineered Safety Features
- 7.3-3 Instrumentation Operating Conditions for Isolation Functions
- 7.3-4 Interlocks for Engineered Safety Features Actuation System
- 7.3-5 (Deleted)
- 7.3-6 Failure Mode and Effects Analysis, Service Water System
- 7.3-7 Failure Mode and Effects Analysis, Component Cooling Water System
- 7.3-8 Failure Mode and Effects Analysis, Control Room and Air Conditioning and Filtration System
- 7.3-9 Failure Mode and Effects Analysis, Penetration Room Filtration System
- 7.3-10 Failure Mode and Effects Analysis, Auxiliary Feedwater System
- 7.3-11 Failure Mode and Effects Analysis, Emergency Safeguards Pump Room Cooling System
- 7.3-12 Failure Mode and Effects Analysis, Battery Room Ventilation System
- 7.3-13 Failure Mode and Effects Analysis, Battery Room Air Conditioning System

LIST OF TABLES

- 7.3-14 Failure Mode and Effects Analysis, Emergency Diesel Generator
- 7.3-15 Failure Mode and Effects Analysis, Engineered Safety Features Actuation System
- 7.3-16 Engineered Safety Features Response Times
- 7.5-1 Post Accident Instrumentation
- 7.5-2 (Deleted)
- 7.5-3 Control Room Indicators and/or Recorders Available to the Operator to Monitor Significant Plant Parameters During Normal Operation
- 7.7-1 Plant Control System Interlocks
- 7.7-2 Boron Concentration Measurement System Specifications

LIST OF FIGURES

- 7.2-1 Setpoint Reduction Function for Overpower and Overtemperature ΔT Trips
- 7.2-2 Pressurizer Sealed Reference Leg Level System
- 7.2-3 Design to Achieve Isolation Between Channels
- 7.3-1 Component Identification ESFAS
- 7.6-1 Logic Diagram for Residual Heat Removal System Isolation Valves
- 7.6-2 Logic Diagram for Residual Heat Removal System Isolation Valves
- 7.6-3 Logic Diagram for Backup to Semiautomatic Switchover Logic from Injection to Recirculation
- 7.6-4 Functional Block Diagram of Accumulator Isolation Valve
- 7.7-1 Simplified Block Diagram of Reactor Control System
- 7.7-2 Control Bank Rod Insertion Monitor
- 7.7-3 Rod Deviation Comparator
- 7.7-4 Block Diagram of Pressurizer Pressure Control System
- 7.7-5 Block Diagram of Pressurizer Level Control System
- 7.7-6 Block Diagram of Main Feedwater Pump Speed Control System
- 7.7-7 Block Diagram of Steam Generator Water Level Control System
- 7.7-8 Block Diagram of Steam Dump Control System
- 7.7-9 Basic Flux Mapping System
- 7.7-10 Source-Detector Assembly
- 7.7-11 Measurement Unit
- 7.7-12 Process Schematic for the Boron Concentration Measurement System
- 7.7-13 Boron Concentration Measurement System vs Normal Plant Operating Range of Boron Concentrations
- 7.8-1 Actuation Logic System Architecture

7.0 INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

This chapter presents the various plant instrumentation and control systems by relating the functional performance requirements, design bases, system descriptions, design evaluations, and tests and inspections for each. The information provided in this chapter emphasizes those instruments and associated equipment which constitute the protection system as defined in Institute of Electrical and Electronics Engineers (IEEE) 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations.

The primary purpose of the instrumentation and control systems is to provide automatic protection against unsafe and improper reactor operation during steady state and transient power operations, Conditions I, II, and III as defined in section 15.1, and to provide initiating signals to mitigate the consequences of faulted conditions, Condition IV as defined in chapter 15. Consequently, the information presented in this chapter emphasizes those instrumentation and control systems which are central to ensuring that the reactor can be operated to produce power in a manner that ensures no undue risk to the health and safety of the public.

It is shown that the applicable criteria and codes concerned with the safe generation of nuclear power, such as the Nuclear Regulatory Commission's (NRC) General Design Criteria (GDC) and the IEEE standards, are met by these systems.

Definitions

The definitions below establish the meaning of words in the context of their use in chapter 7.

Channel - An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single action signals are combined.

Module - Any assembly of interconnected components which constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Components - Items from which the system is assembled (e.g., resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

Single Failure - Any single event which results in a loss of function of a component or components of a system. Multiple failures resulting from a single event shall be treated as a single failure.

Protective Action - A protective action can be at the channel or the system level. A protective action at the channel level is the initiation of a signal by a single channel when the variable sensed exceeds a limit. A protective action at the system level is the initiation of the operation of a sufficient number of actuators to effect a protective function.

FNP-FSAR-7

Protective Function - A protective function is the sensing of one or more variables associated with a particular generating station condition signal processing and the initiation and completion of the protective action at values of the variable established in the design basis.

Type Tests - Tests made on one or more units to verify adequacy of design.

Cold Shutdown Condition - When the reactor is subcritical by at least 1 percent $\Delta k/k$ and T_{avg} is $\leq 200^\circ$.

Hot Shutdown Condition - When the reactor is subcritical by an amount greater than or equal to the margin as specified in the plant technical specifications and $350^\circ F > T_{avg} > 200^\circ F$.

Phase A Containment Isolation - Closure of all nonessential process lines which penetrate containment; initiated by the safety injection signal.

Phase B Containment Isolation - Closure of remaining process lines; initiated by containment high-high-high pressure signal (process lines which are isolated in phase B do not include required engineered safety features lines).

Trip Accuracy - The tolerance band containing the highest expected value of the difference between the desired trip point value of a process variable and the actual value at which a comparator trips (and thus actuates some desired result). This is the tolerance band within which a comparator must trip. It includes comparator accuracy, channel accuracy for each input, and environmental effects on the rack-mounted electronics. It comprises all instrumentation errors; however, it does not include any process effects such as fluid stratification.

Channel accuracy (a component of trip accuracy) includes accuracy of the primary element, transmitter, and rack-mounted electronics but does not include indication accuracy.

Actuation Accuracy - Synonymous with trip accuracy; used where the word "trip" may cause ambiguity.

Indication Accuracy - The tolerance band containing the highest expected value of the difference between the value of a process variable read on an indicator or recorder and the actual value of that process variable. An indication must fall within this tolerance band. It includes channel accuracy, accuracy of readout devices, and rack environmental effects but not process effects such as fluid stratification.

Reproducibility - This term may be substituted for "accuracy" in the above definitions for those cases where a trip value or indicated value need not be referenced to an actual process variable value but rather to a previously established trip or indication value; this value is determined by test.

Train - The term train, as applicable to protection systems using solid state logic, consists of an assembly of components that performs a protective function such as reactor trip or engineered safety features actuation system.

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

The instrumentation systems and supporting systems that are required to function to achieve the system responses assumed in the safety evaluations, and those needed to shut down the plant safely, are:

- Reactor trip system (section 7.2).
- Engineered safety features actuation system (section 7.3).
- Instrumentation and control power supply system (paragraph 8.3.1.1.4).

Detailed electrical-instrumentation and control (EI&C) drawings were provided to the NRC in a supplement as described in subsection 7.1.3 and table 7.1-1.

The reactor trip system and the engineered safety features actuation system are functionally defined systems. The functional descriptions of these systems are found in sections 7.2 and 7.3. For comparison of these systems with other plants, see tables 1.3-1 and 1.3-2. The equipment which provides the trip functions identified in section 7.2 is contained in the following:

- Process instrumentation and control system.⁽¹⁾
- Nuclear instrumentation system.⁽²⁾
- Solid state logic protection system.^(3, 15, 16, 17, 18, 19, 20, 21, 22, & 23)
- Reactor trip switchgear.⁽³⁾
- Manual actuation circuit.

The equipment which provides the actuation functions identified in section 7.3 is contained in the following:

- Process instrumentation and control system.⁽¹⁾
- Solid state logic protection system.^(3, 15, 16, 17, 18, 19, 20, 21, 22, & 23)
- Engineered safety features test cabinet.⁽⁴⁾
- Manual actuation circuits.

The above systems are designed by Westinghouse with the specific scope of supply as shown in drawings U-166231, U-166232, U-166233, U-166234, U-166235, U-166236, U-166237, U-166238, U-166239, U-166240, U-166241, U-166242, U-166243, U-166244, and U-166245.

In addition, several systems have been added to meet the Three Mile Island action plan requirements. These include a wide range containment pressure system, a wide range

containment water level system, a wide range stack effluent monitor, wide range secondary side effluent monitors, and containment narrow range sump level systems.

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

Paragraph 7.1.2.1 gives design bases for the systems given in subsection 7.1.1. Considerations for instrument errors are provided in the accident analyses. Functional requirements based on assumptions in the accident analyses are used in designing these systems, and preoperational testing verifies the adequacy of the design. Accuracies are given in sections 7.2, 7.3, and 7.5.

The documents listed below were considered in the design of the systems given in subsection 7.1.1. In general, the scope of these documents is given in the document itself. This determines the systems or parts of systems to which the document is applicable. A discussion of compliance with each document for systems within its scope is provided in the referenced sections. Because some documents were issued after design and testing had been completed, the equipment documentation may not meet the format requirements of some standards. The documents considered are:

- A. "General Design Criteria for Nuclear Power Plants," 10 CFR 50, Appendix A, July 7, 1971. (See sections 7.2, 7.3, 7.4, and 7.7.)
- B. Directorate of Regulatory Standards, U.S. Nuclear Regulatory Commission, "Instrument Lines Penetrating Primary Reactor Containment," Regulatory Guide 1.11.
- C. Directorate of Regulatory Standards, U.S. Nuclear Regulatory Commission, "Periodic Testing of Protection System Actuation Functions," Regulatory Guide 1.22.
- D. Institute of Electrical and Electronics Engineers, "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE 279-1971. (See sections 7.2, 7.3, and 7.6.)
- E. Institute of Electrical and Electronics Engineers, "Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations," IEEE 308-1971. (See subsection 8.3.1.2.)
- F. Institute of Electrical and Electronics Engineers, "Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations," IEEE 317-1971. (See subsection 7.1.2.4.)
- G. Institute of Electrical and Electronics Engineers, "Trial-Use Standard: General Guide for Qualifying Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 323-1971. (See subsection 7.1.2.5.)

- H. Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Type Tests of Continuous Duty Class 1 Motors Installed Inside the Containment of Nuclear Power Generating Stations," IEEE 334-1971. (See subsection 7.1.2.9.)
- I. Institute of Electrical and Electronics Engineers, "Installation, Inspection, and Testing Requirements for Instrumentation and Electrical Equipment During the Construction of Nuclear Power Generating Stations," IEEE 336-1971. (See subsection 7.1.2.6.)
- J. Institute of Electrical and Electronics Engineers, "Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE 338-1971. (See paragraph 7.1.2.7.)
- K. Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Seismic Qualification of Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 344-1971. (See section 3.10.)

7.1.2.1 Design Bases

7.1.2.1.1 Reactor Trip System

The reactor trip system acts to limit the consequences of Condition II events (faults of moderate frequency), such as loss of feedwater flow, by, at most, a shutdown of the reactor and turbine, with the plant capable of returning to operation after corrective action. The reactor trip system features impose a limiting boundary region to plant operation which ensures that the reactor safety limits are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions. Reactor trip setpoints are given in the plant technical specifications.

The design requirements for the reactor trip system are derived by analyses of plant operating and fault conditions where automatic rapid control rod insertion is necessary to prevent or limit core or reactor coolant boundary damage. The design bases required by IEEE 279-1971 are addressed in subsection 7.2.1. The design limits specified by Westinghouse for the reactor trip system are as follows:

- A. Minimum departure from nucleate boiling ratio (DNBR) will not be less than the safety analysis limit as a result of any anticipated transient or malfunction (Condition II faults).
- B. Power density will not exceed the rated linear power density for Condition II faults. (See chapter 4 for fuel design limits.)
- C. The stress limit of the reactor coolant system for the various conditions shall be as specified in chapter 5.

FNP-FSAR-7

- D. Release of radioactive material will not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius as a result of any Condition III fault.
- E. For any Condition IV fault, release of radioactive material will not result in an undue risk to public health and safety.

Functional performance requirements are as follows:

A. Reactor Trips

The reactor trip system automatically initiates a reactor trip:

1. Whenever necessary to prevent fuel damage for an anticipated malfunction (Condition II).
2. To limit core damage for infrequent faults (Condition III).
3. So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting faults (Condition IV).

B. Turbine Trips

The reactor trip system initiates a turbine trip signal whenever reactor trip is initiated to prevent the reactivity insertion that would otherwise result from excessive reactor system cooldown and to avoid unnecessary actuation of the engineered safety features actuation system.

C. Manual Trip

The reactor trip system provides for manual initiation of reactor trip by operator action.

7.1.2.1.2 Engineered Safety Features Actuation System

The engineered safety features actuation system (ESFAS) acts to limit the consequences of Condition III events (infrequent faults such as primary coolant spillage from a small rupture which exceeds normal charging system makeup and requires actuation of the safety injection system). The ESFAS acts to mitigate Condition IV events (limiting faults which include the potential for significant release of radioactive material).

The design bases for the engineered safety features are presented in chapter 6. Design bases requirements for the ESFAS, as required by IEEE 279-1971, are addressed in subsection 7.3.1.2.

Signals additional to those developed by the reactor trip system will be generated by the ESFAS to protect against the effects (and reduce the consequences) of more serious types of accidents

designated as Condition III and IV events. These are serious abnormal conditions in the reactor coolant system, main steam system, or containment vessel and include a loss-of-coolant accident (LOCA) or a steam break.

The general functions of the ESFAS are as follows:

A. Automatic Actuation

The primary functional requirement of the ESFAS is to receive input signals (information) from the various ongoing processes within the reactor plant and containment and to automatically provide, as output, timely and effective signals to actuate the various components and subsystems comprising the engineered safety features system. These output signals ensure that the engineered safety features system will meet its performance objectives as outlined in chapter 6. The functional diagrams presented in drawings U-166235, U-166236, U-166237, and U-166238 provide a graphic outline of the functional performance requirements of the ESFAS.

B. Manual Actuation Requirements

The ESFAS has provisions for manually initiating from the control room all of the functions of the engineered safety features system.

The following is a discussion of the requirements imposed on the ESFAS design by the design bases.

In addition to the requirements for a reactor trip for anticipated abnormal transients, the facility is provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary engineered safety features. The occurrence of a limiting fault, such as a LOCA or a steam break, requires a reactor trip plus actuation of one or more of the engineered safety features to prevent or mitigate damage to the core and reactor coolant system components and to ensure containment integrity.

To accomplish these design objectives the engineered safety features system has proper and timely initiating signals supplied by the sensors, transmitters, and logic components making up the various instrumentation channels of the ESFAS. The specific functions which rely on this system for initiation are listed in table 7.3-1.

7.1.2.1.3 Instrumentation and Control Power Supply System

The design bases for the instrumentation and control power supply system are as follows:

- A. The inverter has the capacity and regulation required for the ac output for proper operation of the equipment supplied.
- B. Redundant loads are assigned to different distribution panels which are supplied from different inverters.

FNP-FSAR-7

The functional performance requirements for the instrumentation and control power supply system are as follows:

- A. The system supplies regulated single phase ac power to all instrumentation and control equipment required for plant safety.
- B. The system supplies reliable and continuous power to all instrumentation and control equipment required for plant safety.
- C. Auxiliary devices within one channel required to operate dependent equipment are supplied from the same distribution panel to prevent the loss of electric power in one protection set from causing the loss of equipment in another protection set. No single failure within 120V instrumentation and control power supply system will cause a loss of power supply to more than one distribution panel.
- D. Each of the distribution panels is powered from its own inverter. Each inverter is supplied from a 125V DC system and is provided with an alternate regulated AC source.

7.1.2.1.4 Emergency Power

Design bases and system description for the emergency power supply are provided in subsection 8.3.1.

7.1.2.1.5 Interlocks

Interlocks are discussed in sections 7.2, 7.3, 7.6, and 7.7. The protection (P) interlocks are given in tables 7.2-2 and 7.3-4. These interlocks are designed to meet the requirements of paragraph 4.12 of IEEE 279-1971. Because of NRC requirements, the residual heat removal isolation valve interlocks are designed to meet the applicable requirements of IEEE 279-1971, as discussed in section 7.6. Control interlocks are identified in table 7.7-1. Because control interlocks (table 7.7-1) are not safety related, they have not been specifically designed to meet the requirements of any IEEE standards.

Testability of the interlocks associated with reactor trips for which credit is taken in the accident analysis is provided by the logic testing and semiautomatic testing capabilities of the solid state protection system. In the solid state protection system, the undervoltage coils (reactor trip) and master relays (engineered safety features actuation) are pulsed for all combinations of trip or actuation logic with and without the coincidence (interlock) signals. For example, reactor trip on low flow (two out of three loops showing two out of three low flow) is tested to verify operability of the trip above P-7 and nontrip below P-7. (Interlock testing as explained above may be performed at power.) Tables 7.2-2 and 7.3-4 specify the interlocks tested. Subsections 7.2.2.2.1 and 7.3.2.1.5 provide further details of testing capability.

7.1.2.1.6 Bypasses

Bypasses are designed to meet the requirements of IEEE 279-1971, paragraphs 4.11, 4.12, 4.13, and 4.14. A discussion of bypasses provided is given in sections 7.2 and 7.3.

7.1.2.1.7 Equipment Protection

Equipment related to the safe operation of the plant is designed, constructed, and installed to protect it from damage. This is accomplished by working to accepted standards and criteria aimed at providing reliable instrumentation which is available under varying conditions.

The criteria for equipment protection are given in chapter 3.

7.1.2.1.8 Diversity

Functional diversity has been designed into the system. Functional diversity is discussed in WCAP-7706, An Evaluation of Reactor Protection in Anticipated Operational Transients.⁽⁵⁾ The extent of diverse system variables has been evaluated for a wide variety of postulated accidents as discussed in WCAP-7306, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors.⁽⁶⁾ Generally, two or more diverse protection functions would automatically terminate an accident before unacceptable consequences could occur. For example, there are automatic reactor trips based upon nuclear flux measurements, reactor coolant loop temperature measurements, pressurizer pressure and level measurements, and reactor coolant pump underfrequency and undervoltage measurements, as well as manual and by initiation of a safety injection signal.

Regarding the ESFAS for a LOCA, a safety injection signal can be obtained manually or by automatic initiation from two diverse sets of signals:

- A. Low pressurizer pressure.
- B. High containment pressure.

For a steam break accident, diversity of safety injection signal actuation is provided by:

- A. Low steam line pressure.
- B. High steam line differential pressure.
- C. For a steam break inside containment, an additional parameter for generation of the signal, provided by high containment pressure.

All of the above sets of signals are redundant and physically separated and meet applicable requirements of GDC 22.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems in subsection 7.1.1 are designed to meet the independence and separation requirements of 1971 GDC 22 and paragraph 4.6 of IEEE 279-1971.

The electrical power supply, instrumentation, and control conductors for redundant circuits are physically separated to preserve redundancy and to ensure that no single credible event would prevent operation of the associated function due to electrical conductor damage. Critical circuits and functions include power, control, and analog instrumentation associated with the operation of the reactor trip system of the ESFAS. Credible events considered in the basic plant design include but are not limited to the effects of short circuits, pipe rupture, and missiles. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 279-1971 for circuits, which are located by necessity in non-category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E separation requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

7.1.2.2.1 General

- A. Cables of redundant circuits are run in separate cable trays, conduits, ducts, penetrations, etc.
- B. Circuits for nonredundant functions are run in cable trays or conduits separated from those used for redundant circuits. Where this cannot be accomplished, nonredundant circuits are run in a cable tray, conduit, etc., assigned to a redundant function. When so routed, the cable remains with that particular redundant circuit routing and does not cross over to other redundant groups.
- C. Horizontal or vertical separation is maintained between cable trays, conduit, or armored cables associated with redundant circuits.
- D. Where it is impractical for reasons of equipment arrangement to provide separate cable trays, cables of redundant circuits are isolated by physical barriers, installed in separate metallic conduit, or protected by suitable armored cables.
- E. Power and control conductors rated at 600 V or below are not placed in cable trays with conductors rated above 600 V.
- F. Analog or other low level type signal conductors are not routed in cable trays containing power or control cables.

7.1.2.2.2 Specific Systems

Channel independence is carried throughout the system, extending from the sensor through the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel set. Redundant analog

equipment is separated by locating modules in different protection rack sets. Each redundant channel set is energized from a separate ac power feed. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 384-1974 for separation of circuits, which are located by necessity in non-category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

There are four separate process analog rack protection sets. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and analog protection racks to the redundant trains in the logic racks. Redundant analog channels are separated by locating modules in different rack sets. Since all equipment within any rack is associated with a single protection channel set, there is no requirement for separation of wiring and components within the rack.

Independence of the logic trains is discussed in reference 3. Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full length control rod drive mechanisms, permitting the rods to free fall into the core.

A. Reactor Trip System

1. Separate routing is maintained for the four basic reactor trip system channel sets analog sensing signals, bistable output signals, and power supplies for such systems. The separation of these four channel sets is maintained from sensors to instrument racks to logic system cabinets.
2. Separate routing of the reactor trip signals from the redundant logic system cabinets is maintained, and, in addition, they are separated from the four analog channel sets. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 384-1974 for separation of circuits, which are located by necessity in non-category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

B. Engineered Safety Features Actuation System

1. Separate routing is maintained for the four basic sets of ESFAS analog sensing signals, bistable output signals, and power supplies for such systems. The separation of these four channel sets is maintained from sensors to instrument racks to logic system cabinets.
2. Separate routing of the ESFAS signals from the redundant logic system cabinets is maintained, and, in addition, they are separated from the four analog channel sets.

3. Separate routing of control and power circuits associated with the operation of engineered safety features equipment was required in order to retain redundancies provided in the system design and power supplies.

C. Instrumentation and Control Power Supply System

The separation criteria presented also apply to the power supplies for the load centers and busses distributing power to redundant components and to the control of these power supplies.

Reactor trip system and ESFAS analog circuits are routed, as necessary, in the same wireways, provided circuits have the same power supply and channel set identified (I, II, III, or IV).

7.1.2.3 Physical Identification of Safety-Related Equipment

Adequate information is provided to distinguish reactor trip engineered safety features and instrumentation and control power supply system as safety related. As previously stated, there are four protection channel set racks. A color-coded nameplate on each rack of each set is used to differentiate between protective and nonprotective sets. The color coding of the nameplates is as follows:

<u>Protection Set</u>	<u>Color Coding</u>
I	Yellow with black lettering
II	Green with white lettering
III	Orange with black lettering
IV	Silver with black lettering

Positive permanent identification of cables and/or conductors will be made at all terminal points. All nonrack-mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on the enclosure which houses them. All cables are numbered with identification tags.

For further details of the process analog system see sections 7.2, 7.3, and 7.7.

There are identification nameplates on the input panels of the solid state logic protection system. For details of the solid state protection system see sections 7.2 and 7.3.

7.1.2.4 Conformance to IEEE 317-1971

Electrical penetrations and degree of conformance with IEEE 317-1971, Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations,⁽⁷⁾ are discussed in section 6.1.

7.1.2.5 Conformance to IEEE 323-1971

Class 1 electrical equipment has been type tested to substantiate the adequacy of design. Most electrical devices and components are standard products and are type tested during the developmental stage. Documentation of type testing is in possession of the manufacturers and may not be in the form given in this IEEE standard.⁽⁸⁾ Successful operating experience of the electrical equipment is an important factor in determining the adequacy of the electrical equipment. Most of it is of standard design that has had widespread use in the industry.

7.1.2.6 Conformance to IEEE 336-1971

Degree of conformance with IEEE 336-1971, Installation, Inspection and Testing Requirements for Instrumentation and Electrical Equipment During the Construction of Nuclear Power Generating Stations,⁽⁹⁾ is discussed in paragraph 8.3.1.3.

7.1.2.7 Conformance to IEEE 338-1971

The periodic testing of the reactor trip system as described in section 7.2 conforms to the requirements of IEEE 338-1971⁽¹⁰⁾ with the following comments:

- A. Time response data on the protection systems are obtained during the startup test program, and appropriate sections are repeated when a component that affects time response is replaced. These procedures require that simulated signals be introduced as analog inputs for partial testing of protection channels, since a complete check, including the sensors, has not been developed by the industry. Validity of time response values assigned to sensors is considered to be established by channel comparison during normal plant operations on the basis that deterioration of time response characteristics of sensors will be observable by comparison of oscillations on associated readouts that will clearly indicate a "slow" transmitter. Response times for the solid-state protection system are routinely verified during periodic testing of the logic channels as required by the plant technical specifications.
- B. The reliability goals specified in paragraph 4.2 of IEEE 338-1971 are developed for FNP and described in the technical specifications.
- C. The periodic test frequency discussed in paragraph 4.3 of IEEE 338-1971 and specified in the plant technical specifications is conservatively selected to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the test frequency is accelerated to accommodate the situation until the marginal performance is resolved.
- D. The test interval discussed in paragraph 5.2 of IEEE 338-1971 is developed for FNP and described in the technical specifications.

FNP-FSAR-7

The periodic testing of the ESFAS conforms to the requirements of IEEE 338-1971 with the following comments:

- A. The response time specified in paragraph 4.1 of IEEE 338-1971 is verified for FNP periodically as described in the technical specifications. The response time is also required to be checked if a component affecting the time response had been replaced during maintenance.
- B. The reliability goals specified in paragraph 4.2 of IEEE 338-1971 are developed for FNP and described in the technical specifications.
- C. The periodic test frequency discussed in paragraph 4.3 of IEEE 338-1971 and specified in the plant technical specifications is conservatively selected to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the test frequency is accelerated to accommodate the situation until the marginal performance is resolved.
- D. The test interval discussed in paragraph 5.2 of IEEE 338-1971 is developed primarily on past operating experience and modified if necessary to ensure that system and subsystem protection is reliably provided. Analytical methods for determining reliability are not used to determine test interval.

Based on the scope definition given in IEEE 338-1971, no other systems described in chapter 7 are required to comply with this standard.

7.1.2.8 Conformance to Regulatory Guide 1.22

Periodic testing of the reactor trip system and the ESFAS, as described in subsections 7.2.2 and 7.3.2, complies with NRC Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions.⁽¹¹⁾

When the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the main control room by a separate annunciator for the train in test. Test circuitry does not allow two trains to be tested at the same time, so that extension of the bypass condition to a redundant system is prevented.

The actuation logic for the reactor trip system and the ESFAS is tested as described in sections 7.2 and 7.3. As required by Regulatory Guide 1.22, when actuated equipment is not tested during reactor operation, it has been determined that:

- A. There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant.

- B. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation.
- C. The equipment can routinely be tested when the reactor is shut down.

The list of equipment that cannot be tested at power is:

- A. Manual actuation switches.
- B. Turbine trip equipment that causes reactor trip.
- C. Main steam line stop valves (close).
- D. Feedwater pump discharge valves (close).
- E. Feedwater control valves (close).
- F. Main feedwater pump trip solenoids.
- G. Seal water isolation valves (close).
- H. Cooling water isolation valves (close).
- I. Instrument air into containment.

7.1.2.9 Conformance to IEEE 334-1971

The only motors discussed in chapter 7 that are within the scope of IEEE 334-1971⁽¹²⁾ are containment fan cooler motors (sections 6.2 and 7.3). These motors have been tested in the manner set forth in the standard.

7.1.2.10 Conformance to 10 CFR 50.62

The AMSAC conforms to the requirements of 10 CFR 50.62 as discussed in section 7.8.

7.1.2.11 Conformance to NUREG-0737

The detailed control room design review (DCRDR) and the safety parameter display system (SPDS) conform to the requirements of NUREG-0737, Supplement 1, as discussed in the NRC safety evaluation.⁽¹³⁾⁽¹⁴⁾

[HISTORICAL][7.1.3 DETAILED ELECTRICAL INSTRUMENTATION AND CONTROL DRAWINGS**7.1.3.1 Identification and Purpose**

A set of volumes containing nonproprietary detailed EI&C drawings has been prepared in accordance with the NRC interim guidelines, pending revisions of the Standard Format. It is entitled, "Joseph M. Farley Nuclear Plant, Safety-Related Schematic Diagrams and Location Drawings, November 1973," and is in four volumes, FNP-1001, FNP-1002, FNP-1003, and FNP-1004. The supplement furnished detailed information in response to paragraphs 7.2.1.3 and 7.3.1.3 and subsections 7.4.1 and 7.6.1 of the Standard Format. The purpose of the supplement was to facilitate tracing the safety-related signals from sensors to actuating devices. It was submitted with Amendment 27. A list of the submitted EI&C drawings and related FSAR figures is maintained in table 7.1-1 for historical purposes.]

REFERENCES

1. Reid, J. B., "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP-7913, January 1973.
2. Lipchak, J. B. and Stokes, R. A., "Nuclear Instrumentation System," WCAP-7669, April 1971.
3. Katz, D. N., "Solid State Logic Protection System Description," WCAP-7672, June 1971.
4. Haller, J. T., "Engineered Safeguards Final Device or Activator Testing," WCAP-7705, May 1972.
5. Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706, July 1971.
6. Burnett, T. W. T., "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," WCAP-7306, April 1969.
7. Institute of Electrical and Electronics Engineers, "Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations," IEEE 317-1971.
8. Institute of Electrical and Electronics Engineers, "Trial-Use Standard: General Guide for Qualifying Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 323-1971.
9. Institute of Electrical and Electronics Engineers, "Inspection and Testing Requirements for Instrumentation and Electrical Equipment During the Construction of Nuclear Power Generating Stations," IEEE 336-1971.
10. Institute of Electrical and Electronics Engineers, "Trail-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE 338-1971.
11. Division of Reactor Standards, Nuclear Regulatory Commission, "Periodic Testing of Protection Systems Actuation Functions," Regulatory Guide 1.22, February 17, 1972.
12. Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Type Tests of Continuous Duty Class 1 Motors Installed Inside the Containment of Nuclear Power Generating Stations," IEEE 334-1971.
13. NRC Safety Evaluation Related to Detailed Control Room Design Review, Joseph M. Farley Nuclear Plant, Units 1 and 2, October 3, 1990.
14. NRC Supplemental Safety Evaluation Report for the Safety Parameter Display System, Joseph M. Farley Nuclear Plant, Units 1 and 2, November 21, 1990.
15. WCAP-16769-P Revision 2, "Westinghouse SSPS Universal Logic Board Replacement Summary Report 6D30225G01/G02/G03/G04."

FNP-FSAR-7

16. WCAP-16770-P Revision 0, "Westinghouse SSPS Safeguards Driver Board Replacement Summary Report 6D30252G01/G02."
17. WCAP-16771-P Revision 1, "Westinghouse SSPS Undervoltage Driver Board Replacement Summary Report 6D30350G01/G02."
18. WCAP-16772-P Revision 1, "Westinghouse SSPS Semi-Automatic Tester Board Replacement Summary Report 6D30520G01/G02/G03/G04/G05."
19. WCAP -17867-P-A Revision 1, "Westinghouse SSPS Board Replacement Licensing Summary Report."
20. WCAP-16773-P Revision 0, "Westinghouse SSPS Clock Counter Board Replacement Summary Report 6D30687G01."
21. WCAP-16774-P Revision 0, "Westinghouse SSPS Decoder Board Replacement Summary Report 6D31031G01."
22. WCAP-16775-P Revision 0, "Westinghouse SSPS Isolation Board Replacement Summary Report 6D31033G01."
23. WCAP-16776-P Revision 1, "Westinghouse SSPS Memory Board Replacement Summary Report 6D31035G01."

[HISTORICAL]TABLE 7.1-1 (SHEET 1 OF 33)**LIST OF SCHEMATIC DIAGRAMS AND LOCATION DRAWINGS
FOR SAFETY-RELATED EQUIPMENT**

This table lists drawings which are presented in the FSAR by reference to project drawing numbers or were provided to the NRC in the supplement.

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
<i>Equipment Location Number Index</i>		
175070	11/01/73	Equipment numbers tabulation
<i>Nuclear Instrumentation System (NIS) Block Diagrams and Safeguards Test Cabinet</i>		
108D501	11/01/73	Process control block diagram
5655D37	11/01/73	Functional diagrams
5655D49	11/01/73	NIS source range functional block diagram
5655D50	11/01/73	NIS intermediate range functional block diagram
5655D51	11/01/73	NIS power range functional block diagram
5655D52	11/01/73	NIS auxiliary channels functional block diagram
724D17	11/01/73	Safeguards test cabinet (10 sheets)
<i>Elementary Diagrams, 177000 Series (Includes Related 207000 Series)</i>		
177000	11/01/73	Single line electrical auxiliary system (normal)
177001	11/01/73	Single line electrical auxiliary system (emergency)
177005	11/01/73	Single line protection and metering, 4160-V bus 1F
177006	11/01/73	Single line protection and metering, 4160-V bus 1G
177018	11/01/73	Single line protection and metering, 4160-V bus 1H
177027	11/01/73	Single line protection and metering, 4160-V bus 1J
177043	11/01/73	Single line protection and metering, 4160-V bus 1K
177044	11/01/73	Single line protection and metering, 4160-V bus 1L
177007	11/01/73	Single line protection and metering, 600-V load center 1A
177009	11/01/73	Single line protection and metering, 600-V load center 1C

TABLE 7.1-1 (SHEET 2 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177010	11/01/73	Single line protection and metering, 600-V load center 1D
177011	11/01/73	Single line protection and metering, 600-V load center 1E
177012	11/01/73	Single line protection and metering, 600-V load center 1F
177014	11/01/73	Single line protection and metering, 600-V load center 1H
177015	11/01/73	Single line protection and metering, 600-V load center 1J
177045	11/01/73	Single line protection and metering, 600-V load center 1K
177046	11/01/73	Single line protection and metering, 600-V load center 1L
177677	11/01/73	Single line protection and metering, 600-V load center 1R
177678	11/01/73	Single line protection and metering, 600-V load center 1S
177118	11/01/73	Interlock schematic station service transformer 1F
177122	11/01/73	Interlock schematic 600-V bus 1A
177024	11/01/73	Single line 120 V-ac vital and regulated system A
177025	11/01/73	Single line 120 V-ac vital and regulated system B
177754	11/01/73	Tray and conduit layout, cable spreading room
177033	11/01/73	Logic diagram diesel 1A auto start and loading
177032	11/01/73	Logic diagram diesel 1B auto start and loading
177036	11/01/73	Logic diagram diesel 1C auto start and loading

TABLE 7.1-1 (SHEET 3 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177037	11/01/73	Logic diagram diesel 2C auto start and loading
-	11/01/73	One-line diagram dc supply for diesel generators
207032	11/01/73	Logic diagram diesel 2B auto start and loading
177119	11/01/73	Interlock schematic component cooling water pump 2B
177120	11/01/73	Interlock schematic HHSI pump 2B
177121	11/01/73	Interlock schematic service water pump 1C
177082	11/01/73	Single line dc distribution system 1A
177083	11/01/73	Single line dc distribution system 1B
207000	11/01/73	Single line electrical auxiliary system (normal 4160 V and 600 V) Unit 2
207001	11/01/73	Single line electrical auxiliary system (emergency 4160 V and 600 V) Unit 2
207033	11/01/73	Logic diagram diesel 1A auto start and loading
207036	11/01/73	Logic diagram diesel 1C auto start and loading
207037	11/01/73	Logic diagram diesel 2C auto start and loading
177133	11/01/73	Interlock schematic battery charger 1C
177050	11/01/73	Elementary diagram 600-V LC bus 1A tie breaker from 600-V LC bus 1D
177051	01/10/75	Elementary diagram 575-V motor- operated valve
177052	11/15/74	Elementary diagram 575-V motor- operated valve
177053	11/15/74	Elementary diagram 575-V motor- operated valve
177058	11/01/73	Elementary diagram 600-V LC bus 1C tie breaker
177059	11/01/73	Elementary diagram 600-V LC bus 1C tie breaker from 600-V LC bus 1E

TABLE 7.1-1 (SHEET 4 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177064	11/01/73	Elementary diagram 600-V LC bus 1D tie breaker from 600-V LC bus 1A
177070	11/01/73	Elementary diagram 600-V LC bus 1E tie breaker from 600-V LC bus 1C
177072	11/01/73	Elementary diagram 600-V LC buses 1D and 1E, including breaker from bus 1F
177077	11/01/73	Elementary diagram 600-V LC breakers to battery chargers 1A and 1B
177078	11/01/78	Elementary diagram 600-V LC breakers to battery charger 1C
177080	11/01/73	Synchronizing diagram 4160-V emergency buses train A Units 1 and 2
177081	11/01/73	Synchronizing diagram 4160-V emergency buses train B Units 1 and 2
177087	11/01/73	Elementary diagram 600-V LC buses 1A, 1B, 1C, 1D, and 1E potential transformer
177089	11/01/73	Elementary diagram 600-V LC breakers to motor control centers 1A, 1B, 1F, 1G, 1S, 1U, and 1V
177091	11/01/73	Elementary diagram miscellaneous relay
177142	11/01/73	Elementary diagram 4160-V bus 1G incoming breaker from diesel generator 1B
177143	11/01/73	Elementary diagram 4160-V bus 1F incoming breaker from diesel generator 1A
177144	11/01/73	Elementary diagram 4160-V bus tie from 4160-V bus 1F to 1KC 1G101L
177145	11/01/73	Elementary diagram 4160-V bus tie breaker from 4160-V bus 1F to 1MC 1G101J
177155	11/01/73	Elementary diagram 4160-V bus 1F incoming startup transformer 1A

TABLE 7.1-1 (SHEET 5 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177157	11/01/73	Elementary diagram 4160-V bus 1F potential transformers
177159	11/01/73	Elementary diagram 4160-V bus 1F outgoing station service transformers 1D and 1G
177160	11/01/73	Elementary diagram 4160-V bus 1F outgoing station service transformer 1F
177161	11/01/73	Elementary diagram 4160-V bus 1F incoming startup transformer 1B
177163	11/01/73	Elementary diagram 4160-V bus 1G potential transformers
177166	11/01/73	Elementary diagram 4160-V bus 1G outgoing station service transformer 1F
177167	11/01/73	Elementary diagram 4160-V bus tie breaker 1G to 1J
177168	11/01/73	Elementary diagram 4160-V bus 1G incoming startup transformer 1A
177169	11/01/73	Elementary diagram 4160-V bus 1G incoming startup transformer 1B
177170	11/01/73	Elementary diagram 4160-V buses 1F and 1G diff. prot.
177173	11/01/73	Elementary diagram 4160-V bus 1G diff. prot.
177183	11/01/73	Elementary diagram component cooling water pump 4160-V bus 1C
177184	11/01/73	Elementary diagram component cooling water pump 4160-V bus 1A
177185	11/01/73	Elementary diagram component cooling water pump 4160-V bus 1B train A
177186	11/01/73	Elementary diagram auxiliary feedwater pump 4160-V buses 1A and 1
177187	11/01/73	Elementary diagram component cooling water pump 4160-V bus 1B train B

TABLE 7.1-1 (SHEET 6 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177188	11/01/73	Elementary diagram turbine-driven auxiliary feedwater pump-starter train A
177189	11/01/73	Elementary diagram turbine-driven auxiliary feedwater pump-starter train B
177199	11/01/73	Elementary diagram containment purge exhaust damper
177204	11/01/73	Elementary diagram containment purge system isolation dampers
177206	11/01/73	Elementary diagram containment post-LOCA air mixing fans
177221	11/01/73	Elementary diagram containment cooling high speed
177222	11/01/73	Elementary diagram containment cooling low speed
177224	11/01/73	Elementary diagram boric acid transfer pumps 1 and 2
177226	11/01/73	Elementary diagram charging/HHST pump 1B room cooler fan motor train A
177227	11/01/73	Elementary diagram RHR pump and containment spray pump from cooler fan motors
177229	11/01/73	Elementary diagram HHST and auxiliary feedwater pump room and common heat exchange cooler fan motor
177232	11/01/73	Elementary diagram containment cooler damper motor
177236	11/01/73	Elementary diagram containment purge supply fan high speed
177237	11/01/73	Elementary diagram containment purge exhaust fan low speed
177238	11/01/73	Elementary diagram penetration from exhaust fans 1 and 2
177239	11/01/73	Elementary diagram penetration room recirculation fans 1 and 2
177240	11/01/73	Elementary diagram boron injection tank recirculation pumps 1 and 2

TABLE 7.1-1 (SHEET 7 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177243	11/01/73	Elementary diagram component cooling water and pump room cooler fans
177246	11/01/73	Elementary diagram spent fuel pool air exhaust fans 1 and 2
177253	08/15/74	Elementary diagram phosphate injection pumps
177259	11/01/73	Elementary diagram radwaste air exhaust fan 1A motor
177262	11/01/73	Elementary diagram control rod drive mechanism cooler 1
177263	11/01/73	Elementary diagram control rod drive mechanism cooling fan dampers
177270	11/01/73	Elementary diagram control room filter fan motors
177275	11/01/73	Elementary diagram control room filter intake dampers
177277	11/01/73	Elementary diagram reactor cavity H2 dilution A/P compressors 1A and 1B
177278	11/01/73	Elementary diagram containment preaccess fan motors
177279	11/01/73	Elementary diagram control room filter exhaust dampers
177280	11/01/73	Elementary diagram control room outside air intake dampers
177281	11/01/73	Elementary diagram penetration room filter prefilter damper
177282	11/01/73	Elementary diagram refueling water surface supply and exhaust fan motors
177283	11/01/73	Elementary diagram penetration room filter recirculation damper
177284	11/01/73	Elementary diagram charging/ HHSI pump 1B room cooler fan train B
177291	11/01/73	Elementary diagram radwaste air exhaust fan 1B motor
177294	11/01/73	Elementary diagram miscellaneous auxiliary building sump pump motors

TABLE 7.1-1 (SHEET 8 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177371	11/01/73	Elementary diagram solenoid valves, sheet 75 Pressurizer liquid sample train A Pressurizer steam sample train A Reactor hot leg sample train A Accumulator sample train A
177372	11/01/73	Elementary diagram solenoid valves, sheet 76 Pressurizer liquid sample train B Pressurizer steam sample train B Reactor hot leg sample train B Accumulator sample train B
177399	11/01/73	Elementary diagram accumulator discharge valve closed alarm
177400	11/01/73	Elementary diagram accumulator discharge valve closed alarm
177569	11/01/73	Elementary diagram 575-V motor- operated valve
177570	11/01/73	Elementary diagram 575-V motor- operated valve
177572	11/01/73	Elementary diagram 575-V motor- operated valve
177583	11/01/73	Elementary diagram solenoid valve, sheet 32 Motor-driven auxiliary feedwater pump Auxiliary feedwater bypass
177584	11/01/73	Elementary diagram solenoid valves, sheet 31 Surge tank discharge to auxiliary building
177588	11/01/73	Elementary diagram solenoid valves, sheet 27 Spent fuel exhaust intake
177589	11/01/73	Elementary diagram solenoid valves, sheet 26 Fuel handling area vent system Penetration room dampers

TABLE 7.1-1 (SHEET 9 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177590	11/01/73	Elementary diagram solenoid valves, sheet 22 Turbine-driven auxiliary feedwater pump discharge
177591	11/01/73	Elementary diagram solenoid valves, sheet 23 Motor-driven auxiliary feedwater pump discharge
177592	11/01/73	Elementary diagram solenoid valves, sheet 24 Auxiliary steam condensate tank
177610	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 7 Reactor coolant pump component cooling water return from thermal barrier
177612	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 9
177613	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 10 Containment cooler service water return Containment cooler service water supply
177617	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 14 Service water to blowdown heat exchange Blowdown heat exchange, letdown chiller discharge
177618	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 15 Reactor coolant pump component cooling water return from oil coolers
177620	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 17 Auxiliary feedwater pump service water supply containment leak rate test
177622	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 19 Steam generator feedwater intake

TABLE 7.1-1 (SHEET 10 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177623	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 20 Service water from storage tank train A
177624	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 21 Service water from storage tank train B
177625	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 22 Component cooling water to reactor coolant pump
177628	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 25 Component cooling makeup water Component cooling water to spent fuel pool heat exchange Service water to component cooling water heat exchange Component cooling water to residual heat exchange
177627	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 24 Auxiliary feedwater to steam generators 1A, 1B, and 1C
177629	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 26 Containment cooler service water bypass Containment cooler service water discharge
177630	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 27 Component cooling water heat exchange
177632	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 29 RHR pumps 1 and 1B miniflow
177633	11/01/73	Elementary diagram 575-V motor-operated valves, sheet 30 Containment cooler discharge

TABLE 7.1-1 (SHEET 11 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177635	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 32 Service water to component cooling water heat exchange
177636	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 33 Reactor coolant pump motor cooler service water discharge
177644	11/01/73	Elementary diagram 575-V motor- operated valve
177645	11/01/73	Elementary diagram loading sequencer B1F essential sequencer
177646	11/01/73	Elementary diagram loading sequencer B1G essential sequencer
177647	11/01/73	Elementary diagram essential loading sequencer B1G breaker close failure indication
177648	11/01/73	Elementary diagram essential loading sequencer B1G breaker close failure indication
177649	11/01/73	Elementary diagram loading sequencer B1F LOSP sequencer
177650	11/01/73	Elementary diagram loading sequencer B1G LOSP sequencer
177653	11/01/73	Elementary diagram loading sequencer B1F load shedding scheme
177654	11/01/73	Elementary diagram loading sequencer B1G load shedding scheme
177659	11/01/73	Elementary diagram loading sequencer B2H load shedding scheme

TABLE 7.1-1 (SHEET 12 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177660	11/01/73	Elementary diagram loading sequencer B2J load shedding scheme
177688	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 47
177689	11/01/73	Elementary diagram 575-V motor- operated valves, sheet 48
177838	11/01/73	Elementary diagram 575-V motor- operated valve
177839	11/01/73	Elementary diagram 575-V motor- operated valve
177840	11/01/73	Elementary diagram 575-V motor- operated valve
177851	11/01/73	Elementary diagram solenoid valves, sheet 2 Excess letdown heat exchange inlet Excess letdown heat exchange discharge
177852	11/01/73	Elementary diagram solenoid valves, sheet 3 Surge tank discharge to auxiliary building
177853	11/01/73	Elementary diagram solenoid valves, sheet 4 Waste recycle evaporation discharge and inlet valves
177854	11/01/73	Elementary diagram solenoid valves, sheet 5 Reactor coolant pump component cooling
177855	11/01/73	Elementary diagram solenoid valves, sheet 6 Reactor coolant pump component cooling water thermal barrier return
177856	11/01/73	Elementary diagram solenoid valves, sheet 7 Component cooling heat exchange service water discharge
177857	11/01/73	Elementary diagram solenoid valves, sheet 8

TABLE 7.1-1 (SHEET 13 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177863	11/01/73	Steam to turbine-driven auxiliary feedwater pump Elementary diagram solenoid valves train A, sheet 14
177864	11/01/73	Main steam isolation valves Elementary diagram solenoid valves, sheet 15
177865	11/01/73	Main steam isolation bypass valve train A Elementary diagram solenoid valves, sheet 16
177866	11/01/73	Main steam isolation valve operator test Elementary diagram solenoid valves, sheet 17
177867	11/01/73	Main steam isolation bypass valve train B Elementary diagram solenoid valves, sheet 18
177205	11/01/73	Main steam isolation valves train B Elementary diagram spent fuel pool pumps 1A and 1B
177224	11/01/73	Elementary diagram boric acid transfer pumps 1A and 1B
177240	11/01/73	Elementary diagram boron injection tank recirculation pumps 1A and 1B
177174	11/01/73	Elementary diagram reactor coolant pumps 1, 2, and 3
177180	11/01/73	Elementary diagram charging/ HHSI pumps 1A and 1C
177181	11/01/73	Elementary diagram charging/ HHSI pump 1B train A
177182	11/01/73	Elementary diagram charging/ HHSI pump 1B train B
177193	11/01/73	Elementary diagram RHR/LHSI pumps 1A and 1B
177195	11/01/73	Elementary diagram containment spray pumps 1A and 1B
177107	11/01/73	Elementary diagram pressurizer heater backup group 1A (600-V LC emergency bus 1A)

TABLE 7.1-1 (SHEET 14 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177111	11/01/73	Elementary diagram pressurizer heater backup group 1B (600-V LC emergency bus 1C)
177364	11/01/73	Elementary diagram solenoid valve, sheet 35 Letdown line isolation valve Accumulator fill line isolation valve Accumulator nitrogen supply header isolation valve Accumulator test line to refueling water
177365	11/01/73	Elementary diagram solenoid valve, sheet 36 Boron injection tank recirculation isolation valve Boron injection recirculation pump to boron injection tank isolation valve
177368	11/01/73	Elementary diagram solenoid valve, sheet 34 Accumulator test line isolation valve
177309	11/01/73	Elementary diagram boron injection tank heaters A and B
177313	11/01/73	Elementary diagram boron injection surge tank heater
177375	11/01/73	Elementary diagram solenoid valve, sheet 43 Letdown to demineralizer or volume control tank valve
177376	11/01/73	Elementary diagram solenoid valve, sheet 49 Letdown orifice isolation valve
177377	11/01/73	Elementary diagram solenoid valve, sheet 50 Letdown orifice isolation valve
177378	11/01/73	Elementary diagram solenoid valve, sheet 51

TABLE 7.1-1 (SHEET 15 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
		<i>Letdown orifice isolation valve</i>
177379	11/01/73	<i>Elementary diagram solenoid valve, sheet 42</i>
		<i>Boric acid filter to boric acid blender valve</i>
177381	11/01/73	<i>Elementary diagram solenoid valve, sheet 45</i>
		<i>Pressurizer power relief valve</i>
177382	11/01/73	<i>Elementary diagram solenoid valve, sheet 48</i>
		<i>Pressurizer relief tank to reactor</i>
		<i>Makeup water supply isolation valve</i>
		<i>Pressurizer relief tank vent to waste process system isolation valve</i>
177383	11/01/73	<i>Elementary diagram solenoid valve, sheet 46</i>
		<i>Reactor coolant drain tank pump discharge valve</i>
177384	11/01/73	<i>Elementary diagram solenoid valve, sheet 47</i>
		<i>Reactor coolant drain tank vent isolation valve</i>
177508	11/01/73	<i>Elementary diagram solenoid valve, sheet 53</i>
		<i>Waste gas discharge control valve</i>
177509	11/01/73	<i>Elementary diagram solenoid valve, sheet 54</i>
		<i>Boric acid makeup injection valve to charging pump heater</i>
177510	11/01/73	<i>Elementary diagram solenoid valve, sheet 55</i>
		<i>Boric acid dilution injection valve to volume control tank</i>
177511	11/01/73	<i>Elementary diagram solenoid valve, sheet 56</i>

TABLE 7.1-1 (SHEET 16 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177567	11/01/73	Reactor makeup water to boric acid blender valve Elementary diagram 575-V motor- operated valve, sheet 41
177568	11/01/73	Reactor coolant pump seal water return isolation valve Elementary diagram 575-V motor- operated valve, sheet 42
177569	11/01/73	Containment spray pump to spray nozzles isolation valve Elementary diagram 575-V motor- operated valve, sheet 43
177570	11/01/73	RHR system inlet isolation valve Elementary diagram 575-V motor- operated valve, sheet 44
177571	11/01/73	RHR system outlet isolation valve Elementary diagram 575-V motor- operated valve, sheet 45
177572	11/01/73	Low heat safety injection to reactor coolant system cross- over Elementary diagram 575-V motor- operated valve, sheet 40
177585	11/01/73	RHR system inlet isolation valve Elementary diagram solenoid valve, sheet 30
177586	11/01/73	Letdown line isolation valve Elementary diagram solenoid valve, sheet 29
177587	11/01/73	Letdown line isolation valve Elementary diagram solenoid valve, sheet 28
177593	11/01/73	Letdown to volume control tank Reactor coolant drain tank pump discharge Reactor coolant drain tank vent Pressurizer relief tank 2 supply isolation valve

TABLE 7.1-1 (SHEET 17 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
177602	11/01/73	Elementary diagram 575-V motor-operated valve, sheet 39 Volume control tank outlet isolation valve
177603	11/01/73	Elementary diagram 575-V motor-operated valve, sheet 38 Refueling water storage tank to charging pump valve
177604	11/01/73	Elementary diagram 575-V motor-operated valve, sheet 37 Volume control tank outlet isolation valve
177606	11/01/73	Elementary diagram 575-V motor-operated valve, sheet 3 Charging/safety injection pumps section heads isolation valve Charging/safety injection pumps discharge heater isolation valve Refueling water storage tank to RHR pumps 1A and 1B isolation valve
177607	11/01/73	Elementary diagram 575-V motor-operated valve, sheet 4 Containment sump to RHR pump 1B isolation valve Containment sump to RHR pump 1A isolation valve MMSI to reactor coolant system hot leg HHSI to reactor coolant system hot leg LHSI to reactor coolant system hot leg LHSI to reactor coolant system cold leg
177608	11/01/73	Elementary diagram 575-V motor-operated valve, sheet 5 Charging/safety injection pumps miniflow isolation valve

TABLE 7.1-1 (SHEET 18 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
		Charging/safety injection pumps to reactor coolant system isolation valve
177609	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 6 Accumulator 1A, 1B, and 1C discharge
177614	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 11 Boron injection tank outlet isolation valve Boron injection tank inlet isolation valve
177615	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 12 Pressurizer power relief isolation valve
177631	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 28 Refueling water storage tank to charging pump
177634	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 31 Reactor coolant pumps seal water return isolation valve
177637	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 34 Spray additive tank outlet isolation valve
177638	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 35 Containment spray pump inlet
177639	11/01/73	Elementary diagram 575-V motor- operated valve, sheet 36 Containment sump outlet valve
177858	11/01/73	Elementary diagram solenoid valve, sheet 9 Excess letdown isolation valve
177861	11/01/73	Elementary diagram solenoid valve, sheet 12 Reactor coolant system normal charging line

TABLE 7.1-1 (SHEET 19 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
		<i>Reactor coolant system alternate charging line</i>
177362	11/30/73	<i>Elementary diagram solenoid valve, sheet 77</i>
177373	11/30/73	<i>Elementary diagram solenoid valve, sheet 78</i>
177374	11/30/73	<i>Elementary diagram solenoid valve, sheet 79</i>
177523	11/30/73	<i>Elementary diagram solenoid valve, sheet 80</i>

Elementary Diagrams and Physical Drawings, 172000 Series

172062	02/01/74	<i>Conduit template 600-V switchgear buses 1H and 1J</i>
172100	02/01/74	<i>Outdoor duct runs general arrangement</i>
172101	02/01/74	<i>Outdoor electrical duct runs profile river duct 1A</i>
172102	02/01/74	<i>Outdoor electrical duct runs profile river duct 1B</i>
172103	02/01/74	<i>Outdoor electrical duct runs profile service water duct 1A</i>
172104	02/01/74	<i>Outdoor electrical duct runs profile service water duct 1E</i>
172239	02/01/74	<i>Details and assembly of service water undervoltage Detector cabinet service water battery</i>
172240	02/01/74	<i>Details and assembly of service water battery fuse boxes</i>
172270	02/01/74	<i>Electrical penetrations of river water and service water intake structure</i>
172285	02/01/74	<i>Class 1 cable tray support post</i>
172290	02/01/74	<i>Compression type cable transit river and service water intake structures</i>
172292	02/01/74	<i>Class 1 cable tray support bracket</i>
172328	02/01/73	<i>Bill of material service water intake structure</i>
172329	02/01/74	<i>Bill of material river water intake structure</i>

TABLE 7.1-1 (SHEET 20 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172338	02/01/74	Bill of material undervoltage detector cabinet
		Service water intake structure batteries
172366	02/01/74	125 V-dc distribution cabinet service water intake structure train A
172367	02/01/74	125 V-dc distribution cabinet service water intake structure train B
172369	02/01/74	120/208-V distribution cabinet river water intake structure train A
172370	02/01/74	120/208-V distribution cabinet river water intake structure train B
172371	02/01/74	120/208-V distribution cabinet service water intake structure train A
172372	02/01/74	120/208-V distribution cabinet service water structure train B
172373	02/01/74	Anchor bolt assembly for cable tray support post
172063	03/01/74	Conduit template 600-V switchgear buses 1R and 1S
172064	03/01/74	Conduit template 4160-V switchgear buses 1H and 2H
172065	03/01/74	Conduit template 4160-V switchgear buses 1J and 2J
172143	03/01/74	Outdoor ducts Class 1 diesel building to valve boxes and fuel oil tank
172155	05/15/74	Sections and details Class 1 ducts, diesel building area
172169	03/01/74	Diesel building lightning protection and roof grounding
172170	03/01/74	Grounding plan, diesel building to valve boxes
172171	03/01/74	Electrical equipment plan, diesel building
172172	03/01/74	Electrical sections and details, diesel building, sheet 1
172195	05/15/74	Diesel building slab

TABLE 7.1-1 (SHEET 21 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172196	05/15/74	Electrical section and details of conduit below slab, diesel building
172197	05/15/74	Embedded supports and conduits in wall
172211	05/15/74	Cable tray layout and exposed conduit, diesel building, sheet 1
172212	05/15/74	Cable tray layout and exposed conduit, diesel building, sheet 2
172213	05/15/74	Cable tray layout and exposed conduit, diesel building, sheet 3
172214	05/15/74	Cable tray layout and exposed conduit, diesel building, sheet 4
172230	05/15/74	Enlarged end and cable tray, partial plan, river intake structure, sheet 1
172231	05/15/74	Enlarged end and cable tray, partial plan, river intake structure, sheet 2
172232	05/15/74	Conduit plan for valve boxes
172233	05/15/74	Conduit plan valve box river water supply
172173	03/01/74	Electrical sections and details, diesel building, sheet 2
172174	03/01/74	Electrical sections and details, diesel building, sheet 3
172178	03/01/74	Electrical sections and details, diesel building, sheet 4
172195	03/01/74	Embedded conduit, diesel building slab
172196	03/01/74	Sections and details of conduit below slab, diesel building
172197	03/01/74	Embedded supports and conduit in walls, diesel building
172203	03/01/74	Diesel building cable tray and support plan, sheet 1
172211	03/01/74	Cable tray layout, diesel building, sheet 1

TABLE 7.1-1 (SHEET 22 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172212	03/01/74	Cable tray layout, diesel building, sheet 2
172213	03/01/74	Cable tray layout, diesel building, sheet 3
172214	03/01/74	Cable tray layout, diesel building, sheet 4
172243	03/01/74	Screen enclosure for diesel generator neutral resistor
172264	03/01/74	Details and assembly Class 1 emergency ventilation station
172265	03/01/74	Details and assembly Class 1 ventilation local control station
172266	03/01/74	Details and assembly Class 1 heater local control station
172204	02/01/74	General arrangement cable tunnel, sheet 1
172205	02/01/74	General arrangement cable tunnel, sheet 2
172206	02/01/74	General arrangement cable tunnel, sheet 3
172232	04/05/74	Conduit plan valve boxes, sheet 1
172233	04/05/74	Conduit plan valve boxes, sheet 2
172234	04/05/74	Conduit plan valve boxes, sheet 3
172311	03/01/74	Bill of material cable trays
172312	03/01/74	Bill of material cable tray supports
172313	03/01/74	Bill of material cable tunnel
172314	03/01/74	Bill of material diesel building
172340	02/01/74	Details and assembly of switchgear channels
172384	03/01/74	120/208-V distribution cabinet diesel 1C
172385	03/01/74	120/208-V distribution cabinet diesel 2C
172386	03/01/74	120/208-V distribution cabinet diesel 1-2A
172387	03/01/74	120/208-V distribution cabinet diesel 1B

TABLE 7.1-1 (SHEET 23 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172700	11/16/73	Main single line diagram generator and 4160-V transformer
172701	11/16/73	Single line 4160-V emergency station service
172202	11/16/73	Single line 4160-V emergency station service
172204	11/16/73	Single line 600-V emergency station service
172207	11/16/73	Single line and cable diagram dc distribution train E service water building
172708	11/16/73	Single line and cable diagram dc distribution train E service water building
172713	11/16/73	Bill of material relay panels 1 through 11
172714	11/16/73	Front view meter and relay panels 1 through 11
172723	12/21/73	Elementary diagram turbine auxiliary auto stop trips and emergency trip and vacuum reset
172732	11/16/73	Elementary diagram generator relaying
172741	11/16/73	Elementary diagram fire protection jockey pump
172744	11/16/73	Wiring diagram DEH valve test panel junction boxes 1 and 2
172745	11/16/73	Elementary diagram station service air compressor 1A
172747	01/04/74	Elementary diagram service water pump 1A
172748	01/04/74	Elementary diagram service water pump 1B
172749	01/04/74	Elementary diagram service water pump 1C (bus 1K)
172750	01/04/74	Elementary diagram service water pump 1C (bus 1L)
172751	01/04/74	Elementary diagram service water pump 1D
172752	01/04/74	Elementary diagram service water pump 1E

TABLE 7.1-1 (SHEET 24 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172761	01/04/74	Elementary diagram 4160-V bus 1H incoming breaker from diesel generator 1C
172762	11/30/73	Elementary diagram 4160-V bus 1H feeder breakers to station service transformers 1H and 1R
172763	01/18/74	Elementary diagram 4160-V bus 1J incoming breaker from diesel generator 2C
172764	11/30/73	Elementary diagram 4160-V bus 1J (emergency) feeder breaker to station service transformers 1J and 1S
172765	11/30/73	Elementary diagram 4160-V bus 1K feeder breaker station service transformer 1K
172766	11/30/73	Elementary diagram 4160-V bus 1E (emergency) feeder breaker to station service transformer 1L
172767	01/31/74	Elementary diagram 600-V buses 1G, 1P, and 1Q incoming breaker
172768	01/31/74	Elementary diagram feeder breaker 600-V buses 1G, 1P, and 1Q
172769	01/31/74	Elementary diagram 600-V buses 1G, 1P, and 1Q bus tie breaker from bus 1F
172770	11/16/73	Bill of material diesel generator relay panels
172771	11/16/73	Front view diesel generator relay panels typical for 1-2A, 1B, 2B, 1C, and 2C
172772	01/31/74	Elementary diagram diesel generator 1-2A relaying
172773	01/31/74	Elementary diagram diesel generator 1-2A metering
172774	02/28/74	Elementary diagram diesel generator 1-2A start, stop, and shutdown

TABLE 7.1-1 (SHEET 25 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172775	02/28/74	Elementary diagram diesel generator 1-2A exciter and miscellaneous controls
172776	01/31/74	Elementary diagram diesel generator 1B relaying
172777	01/31/74	Elementary diagram diesel generator 1B metering
172778	02/28/74	Elementary diagram diesel generator 1B start, stop, and shutdown
172779	02/28/74	Elementary diagram diesel generator 1B exciter and miscellaneous controls
172780	01/31/74	Elementary diagram diesel generator 1C relaying
172781	01/31/74	Elementary diagram diesel generator 1C metering
172782	02/15/74	Elementary diagram diesel generator 1C start, stop, and shutdown
172783	02/28/74	Elementary diagram diesel generator 1C exciter and miscellaneous controls
172784	11/16/73	Elementary diagram generator and transformer auxiliary relays
172787	11/16/73	Elementary diagram startup auxiliary transformers 1A and 1B protective relaying
172791	01/31/74	Elementary diagram diesel generator 2C relaying
172792	01/31/74	Elementary diagram diesel generator 2C metering
172793	02/28/74	Elementary diagram diesel generator 2C start, stop, and shutdown
172794	02/28/74	Elementary diagram diesel generator 2C exciter and miscellaneous controls
172795	11/30/73	Elementary diagram 4160-V bus 1H feeder breaker to station service transformer 1G

TABLE 7.1-1 (SHEET 26 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172796	11/30/73	Elementary diagram 4160-V bus 1H differential relaying
172797	11/30/73	Elementary diagram 4160-V bus 1J differential relaying
172798	11/30/73	Elementary diagram 4160-V bus 1K differential relaying
172799	11/30/73	Elementary diagram 4160-V bus 1L differential relaying
172818	01/04/74	Elementary diagram river and service water motor-operated and solenoid-operated valves
172825	01/31/74	Elementary diagram 600-V buses 1H, 1J, 1K, and 1L auxiliary breakers and potential transformers, sheet 1
172826	01/31/74	Elementary diagram 600-V buses 1H, 1J, 1K, and 1L feeder breakers and bus tie breakers, sheet 2
172827	01/31/74	Elementary diagram 600-V buses 1O, 1P, and 1Q potential transformers
172828	11/30/73	Elementary diagram 4160-V bus 1H potential transformer
172829	11/30/73	Elementary diagram 4160-V bus 1J potential transformer
172830	11/30/73	Elementary diagram 4160-V buses 1K and 1L potential transformer
172831	01/31/74	Elementary diagram 600-V buses 1R and 1S, sheet 1
172832	01/31/74	Elementary diagram 600-V buses 1R and 1S, sheet 2
172852	01/04/74	Elementary diagram startup auxiliary transformers 1A and 1B controls
172857	01/04/74	Elementary diagram motor control center 1K
172858	03/22/74	Elementary diagram motor control center 1L
172860	03/22/74	Elementary diagram motor control center 1N

TABLE 7.1-1 (SHEET 27 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172861	03/22/74	Elementary diagram motor control center 1P
172862	03/22/74	Elementary diagram motor control center 1S
172863	03/22/74	Elementary diagram motor control center 1T
172864	03/22/74	Elementary diagram motor control center 1X
172865	03/22/74	Elementary diagram motor control center 1Y
172868	11/16/73	Wiring diagram fire protection engine-driven fire pumps
172869	11/16/73	Elementary diagram motor-driven fire pump
172870	02/28/74	Single line and cable diagram fire protection 600-V and 120/208-V distribution cabinets
172875	01/04/74	Elementary diagram river water pump 4
172876	01/04/74	Elementary diagram river water pump 5
172877	01/04/74	Elementary diagram river water pump 8
172878	01/04/74	Elementary diagram river water pump 9
172879	01/04/74	Elementary diagram river water pump 10
172960	01/31/74	Elementary diagram motor-operated valves diesel generator cooling
172963	02/15/74	Elementary diagram diesel generator storage tank fuel pumps
172973	01/31/74	Elementary diagram diesel generator 2B relaying
172974	01/31/74	Elementary diagram diesel generator 2B metering
172975	02/28/74	Elementary diagram diesel generator 2B start, stop, and shutdown
172976	02/28/74	Elementary diagram diesel generator 2B exciter and miscellaneous controls

TABLE 7.1-1 (SHEET 28 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
6893D82	08/15/74	Elementary diagram reactor trip switchgear
172713	10/16/74	Bill of material for D-172714 front view meter and relay PNLS, sheet 7
172713	10/16/74	Bill of material for D-172714 front view meter and relay PNLS, sheet 8
172723	10/16/74	Elementary diagram river water pumps cooling and lube water strainers
172732	10/16/74	Elementary diagram generator relaying
172744	10/16/74	Wiring diagram DEH valve test panel junction boxes 1 and 2
172761	10/16/74	Elementary diagram 4160-V bus 1H incoming breaker from diesel generator 1C
172763	10/16/74	Elementary diagram 4160-V bus 1J incoming breaker from diesel generator 2C
172770	10/16/74	Bill of material for C-172771 front view diesel generator relay PNLS, sheet 4
172825	10/16/74	Elementary diagram 600-V buses 1H, 1J, 1K, and 1L incoming breaker and potential transformer, sheet 2
172857	10/16/74	Elementary diagram motor control center 1K (service water intake structure)
172858	10/16/74	Elementary diagram motor control center 1L (service water intake structure)
172860	10/16/74	Elementary diagram motor control center 1N (diesel building)
172861	10/16/74	Elementary diagram motor control center 1P (diesel building)

TABLE 7.1-1 (SHEET 29 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
172862	10/16/74	Elementary diagram motor control center 1S (diesel building)
172863	10/16/74	Elementary diagram motor control center 1T (diesel building)
172864	10/16/74	Elementary diagram motor control center 1X (river water intake structure)
172865	10/16/74	Elementary diagram motor control center 1Y (river water intake structure)
172963	10/16/74	Elementary diagram diesel generator storage tank fuel pumps, sheet 1
172963	10/16/74	Elementary diagram diesel generator storage tank fuel pumps, sheet 2

Location Drawings, 175000 Series

175055	11/01/73	Equipment location auxiliary building area plan at el 155 ft
175056	11/01/73	Equipment location auxiliary building area plan at el 139 ft
175057	11/01/73	Equipment location auxiliary building area plan at el 121 ft
175059	08/15/74	Equipment location auxiliary building roof plan at el 175 ft and above
175061	11/01/73	Equipment location auxiliary and control building area plan at el 139 ft
175062	11/01/73	Equipment location auxiliary and control building
175150	11/01/73	Instrumentation location containment and fuel handling area plan at el 105 ft 6 in.
175140	11/01/73	Instrumentation location auxiliary and control building area at el 155 ft

TABLE 7.1-1 (SHEET 30 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
175141	11/01/73	Instrumentation location auxiliary and control building area plan at el 139 ft
175142	11/01/73	Instrumentation location auxiliary and control building area at el 121 ft
175143	11/01/73	Instrumentation location auxiliary and control building area at el 100 ft and below
175144	11/01/73	Instrumentation location auxiliary building area at el 155 ft
175145	11/01/73	Instrumentation location auxiliary building area at el 139 ft
175146	11/01/73	Instrumentation location auxiliary building area at el 121 ft
175147	11/01/73	Instrumentation location auxiliary building area at el 100 ft and below
175148	11/01/73	Instrumentation location containment and fuel handling area at el 155 ft
175149	11/01/73	Instrumentation location containment and fuel handling area at el 129 ft

*Piping and Instrumentation Drawings, 170000 Series;
Instrument Installation Drawings, 170000 Series*

170119	11/30/73	P&ID river water system, sheet 1
170119	11/30/73	P&ID service water system, sheet 2
170060	08/29/73	P&ID diesel generator fuel oil supply system (deleted)

TABLE 7.1-1 (SHEET 31 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
170586	10/16/74	River water system automatic operations train A
170587	10/16/74	River water system automatic operations train B
170588	10/16/74	River water pump QSP25P004B
170589	10/16/74	River water pump QSP25P005B
170590	10/16/74	River water pump QSP25P008A
170591	10/16/74	River water pump QSP25P009A
170592	10/16/74	River water pump QSP25P010A
170593	10/16/74	River water motor-operated valve logic train A
170594	10/16/74	River water system valves train B
170623	10/16/74	River water lube water cyclone separator inlet motor-operated valves
170624	10/16/74	River water hand switch- operated motor-operated valves (typical)
170599	10/16/74	Service water pump 1A train A
170600	10/16/74	Service water pump 1B train A
170601	10/16/74	Service water pump 1C train A or B
170602	10/16/74	Service water pump 1D train B
170603	10/16/74	Service water pump 1E train B
170604	10/16/74	Service water diesel generator 2C Unit 1 train B isolation motor- operated valves
170605	10/16/74	Service water diesel generator 2C Unit 2 train B isolation motor- operated valves
170606	10/16/74	Service water diesel generator 1B Unit 1 train B isolation motor- operated valves

TABLE 7.1-1 (SHEET 32 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
170607	10/16/74	Service water diesel generator 1B Unit 2 train B isolation motor- operated valves
170608	10/16/74	Service water diesel generator 2B Unit 1 train B isolation motor- operated valves
170609	10/16/74	Service water diesel generator 1C Unit 1 train A isolation motor- operated valves
170610	10/16/74	Service water diesel generator 1C Unit 2 train B isolation motor- operated valves
170611	10/16/74	Service water diesel generator 1-2A Unit 1 train A isolation motor- operated valves
170612	10/16/74	Service water diesel generator 1-2A Unit 2 train B isolation motor- operated valves
170613	10/16/74	Service water diesel generator building train B isolation motor- operated valves
170614	10/16/74	Service water diesel generator building train A isolation motor- operated valves
170615	10/16/74	Service water to turbine building isolation motor- operated valves 514 and 516
170616	10/16/74	Service water to turbine building isolation motor- operated valves 515 and 517
170617	10/16/74	Service water trains A and B strainer isolation motor- operated valves

TABLE 7.1-1 (SHEET 33 OF 33)

<u>Drawing Number</u>	<u>Submittal to NRC (formerly AEC)</u>	<u>Title</u>
170618	10/16/74	Service water trains A and B emergency recirculation to pond motor-operated valves
170619	10/16/74	Service water push button- operated motor-operated valves (typical)
170622	10/16/74	Service water lube water cyclone separator inlet motor-operated valves
170625	10/16/74	Service water hand switch- operated motor-operated valves (typical)
170626	10/16/74	Service water system discharge backpressure control valves]

7.2 REACTOR TRIP SYSTEM

7.2.1 DESCRIPTION

The reactor trip system automatically keeps the reactor operating within a safe region by shutting down the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations such as mechanical hydraulic limitations on equipment and heat transfer phenomena. Therefore, the reactor trip system keeps surveillance on process variables which are directly related to equipment mechanical limitations, such as pressure and pressurizer water level to prevent water discharge through safety valves and uncovering heaters, and also on variables which directly affect the heat transfer capability of the reactor, e.g., flow and reactor coolant temperatures. Still other parameters utilized in the reactor trip system are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a setpoint, the reactor will be shut down in order to protect against either gross damage to fuel cladding or loss of system integrity which could lead to release of radioactive fission products into the containment.

The following systems make up the reactor trip system:

- Process instrumentation and control system.⁽¹⁾
- Nuclear instrumentation system.⁽²⁾
- Solid state logic protection system.^(3, 22, 23, 24, 25, 26, 27, 28, 29, & 30)
- Reactor trip switchgear.⁽³⁾
- Manual actuation circuit.

The reactor trip system consists of: sensors that feed analog circuitry comprised of two to four redundant channels that monitor various plant parameters; digital circuitry consisting of two redundant logic trains that receive inputs from the analog protection channels; and the logic necessary to automatically open the reactor trip breakers. (See drawings U-166231, U-166232, U-166233, U-166234, U-166235, U-166236, U-166237, U-166238, U-166239, U-166240, U-166241, U-166242, U-166243, U-166244, and U-166245 for symbology and functional logic diagrams.)

Each of the two trains A and B is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively. The two trip breakers in series connect three-phase ac power from the rod drive motor generator sets to the rod drive power cabinets, as shown in drawing U-166232. During plant power operation, a dc undervoltage coil and a shunt trip coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. The automatic shunt trip feature is provided for backup purposes of the undervoltage trip feature, and is fully capable of tripping the reactor trip breaker. However, the undervoltage trip feature provides the primary protective function of the reactor protection system. Thus, for reactor trip, a loss of dc voltage to the undervoltage coil releases the trip plunger and trips open the breaker. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall by gravity into the

core. The rods cannot be withdrawn until an operator resets the trip breakers. The trip breakers cannot be reset until the bistable which initiated the trip is reenergized. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers. Additionally, two test pushbuttons are used during testing to individually confirm the operability of the undervoltage and shunt trip functions. See paragraph 7.2.2.2.1 for further information on the testing of these breakers.

7.2.1.1 System Description

7.2.1.1.1 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the reactor trip system reaches a preset level. To ensure a reliable system, high quality design and components, manufacturing quality control, and testing are used. In addition to redundant channels and trains, the design provides a reactor trip system that monitors numerous system variables, i.e., provides protection system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in reference 4.

Table 7.2-1 provides a list of reactor trips which are described below.

A. Nuclear Overpower Trips

The specific trip functions generated are as follows:

1. Power Range High Neutron Flux Trip

The power range high neutron flux trip circuit trips the reactor when two of the four power range channels exceed the trip setpoint.

There are two independent bistables, each with its own trip setting, used for a high and a low setting. The high trip setting provides protection during normal power operation and is always active. The low trip setting, which provides protection during a startup, can be manually bypassed when two out of the four power range channels read above approximately 10-percent power (P-10). Three out of the four channels being below 10 percent automatically reinstates the trip function. Refer to table 7.2-2 for a listing of all protection system interlocks.

2. Intermediate Range High Neutron Flux Trip

The intermediate range high neutron flux trip circuit trips the reactor when one out of the two intermediate range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if two out of four power range channels are above approximately 10-percent power (P-10). Three out of the four power range channels being below this value automatically reinstates the

intermediate range high neutron flux trip. The intermediate range channels (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

3. Source Range High Neutron Flux Trip

The source range high neutron flux trip circuit trips the reactor when one of the two source range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup and plant shutdown, can be manually bypassed when one of the two intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when both intermediate range channels decrease below the P-6 value. This trip is also automatically bypassed by two out of four logic from the power range permissive (P-10). This trip function can also be reinstated below P-10 by an administrative action requiring manual actuation of two control board-mounted switches. Each switch will reinstate the trip function in one of the two protection logic trains. The source range trip point is set between the P-6 setpoint (source range cutoff flux level) and the maximum source range flux level. The channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

4. Power Range High Positive Neutron Flux Rate Trip

This circuit trips the reactor when an abnormal rate of increase in nuclear power occurs in two out of four power range channels. This trip provides protection against rod ejection accidents of low worth from mid-power and is always active.

Drawing U-166233 shows the logic for all of the nuclear overpower and rate trips. A detailed functional description of the equipment associated with this function is given in reference 2.

B. Core Thermal Overpower Trips

The specific trip functions generated are as follows:

1. Overtemperature ΔT Trip

This trip protects the core against low departure from nucleate boiling ratio (DNBR) and trips the reactor on coincidence as listed in table 7.2-1 with one set of temperature measurements per loop. The setpoint for this trip is continuously calculating by analog circuitry for each loop by solving the following equation:

FNP-FSAR-7

$$\Delta T \left(\frac{1 + \tau_4 s}{1 + \tau_5 s} \right) \leq \Delta T_0 \left[K_1 - K_2 \left(\frac{1 + \tau_1 s}{1 + \tau_2 s} \right) \left(T \frac{1}{1 + \tau_6 s} - T' \right) + K_3 (P - P') - f_1(\Delta I) \right]$$

where:

ΔT	=	Measured ΔT by RTD instrumentation.
ΔT_0	=	Indicated ΔT at Rated Thermal Power and Ref. T_{avg} .
T	=	Average reactor coolant temperature ($^{\circ}F$).
T'	=	Reference T_{avg} at Rated Thermal Power ($\leq 577.2^{\circ}F$).
P	=	Pressurizer pressure (psig).
P'	=	2235 psig (nominal pressurizer operating pressure).
K_1	=	Setpoint bias (percent of full power ΔT).
K_2	=	Constant based on the effect of temperature on the departure from nucleate boiling (DNB) limits (percent of full power $\Delta T/^{\circ}F$).
K_3	=	Constants based on the effect of pressure on the DNB limits (percent of full power ΔT) (psig).
$\tau_1, \tau_2, \tau_4, \tau_5, \tau_6$	=	Time constants (s).
s	=	Laplace transform variable (s^{-1}).
$f_1(\Delta I)$	=	A function of the neutron flux difference between upper and lower long ion chambers (percent of full power ΔT). Refer to figure 7.2-1.

One power range channel separately feeds each overtemperature ΔT trip channel.

Changes in $f(\Delta I)$ can only lead to a decrease in trip setpoint. Refer to figure 7.2-1.

The single pressurizer pressure parameter for the ΔT trips required per loop is obtained from separate sensors each connected to one of three pressure taps at the top of the pressurizer. This results in one pressure tap per loop. (Refer to paragraph 7.2.2.3.3.)

FNP-FSAR-7

Drawing U-166235 shows the logic for the overtemperature ΔT trip function. A detailed functional description of the process equipment associated with this function is contained in reference 1.

2. Overpower ΔT Trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in table 7.2-1, with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated using the following equation:

$$\Delta T \left(\frac{1 + \tau_4 s}{1 + \tau_5 s} \right) \leq \Delta T_0 \left[K_4 - K_5 \left(\frac{\tau_3 s}{1 + \tau_3 s} \right) \left(\frac{1}{1 + \tau_6 s} \right) T - K_6 \left(T \frac{1}{1 + \tau_6 s} - T'' \right) - f_2(\Delta I) \right]$$

where:

ΔT	=	Measured ΔT by RTD instrumentation
ΔT_0	=	Indicated ΔT at Rated Thermal Power and Ref. T_{avg} .
$f_2(\Delta I)$	=	A function of the neutron flux difference between upper and lower long ion chamber section (percent of full power ΔT).
K_4	=	A preset, manually adjustable bias (percent of full power ΔT).
K_5	=	A constant based on the effect of T_{avg} on overpower ΔT limit (percent of full power $\Delta T/^\circ F$).
K_6	=	A constant based on the effect of T_{avg} on overpower ΔT limit (percent of full power $\Delta T/^\circ F$).
T''	=	Reference T_{avg} at Rated Thermal Power ($\leq 577.2^\circ F$)
T	=	Average reactor coolant temperature ($^\circ F$).
$\tau_3, \tau_4, \tau_5, \tau_6$	=	Time constant (s).
s	=	Laplace transform variable (s^{-1}).

The source of temperature and flux information for overpower ΔT trip is identical to that of the overtemperature of ΔT trip, and the resultant ΔT setpoint is compared to the same ΔT . Drawing U-166235 shows the logic

for this trip function. The detailed functional description of the process equipment associated with this function is contained in reference 1.

C. Reactor Coolant System Pressurizer Pressure and Water Level Trips

The specific trip functions generated are as follows:

1. Pressurizer Low Pressure Trip

The purpose of this trip is to protect against low pressure which could lead to a DNBR of less than the safety analysis limit and to limit the necessary range of protection afforded by the overtemperature ΔT trip. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 (see table 7.2-2), the reactor is tripped when the compensated pressurizer pressure measurements fall below preset limits. This trip is blocked below P-7 to permit startup. The logic and interlocks are given in table 7.2-1.

The trip logic is shown in drawing U-166236. A detailed functional description of the process equipment associated with the function is contained in reference 1.

2. Pressurizer High Pressure Trip

The purpose of this trip is to protect the reactor coolant system against system overpressure.

The same sensors and transmitters used for the pressurizer low pressure trip are used for the high pressure trip, except that separate bistables are used for trip. These bistables trip when uncompensated pressurizer pressure signals exceed preset limits on coincidence as listed in table 7.2-1. There are no interlocks or permissives associated with this trip function.

The logic for this trip is shown in drawing U-166236. The detailed functional description of the process equipment associated with this trip is provided in reference 1.

3. Pressurizer High Water Level Trip

This trip serves to prevent water relief through the pressurizer safety valves. This trip is blocked below P-7 to permit startup. The coincidence logic and interlocks of pressurizer high water signals are given in table 7.2-1.

The trip logic for this function is shown in drawing U-166236. A detailed description of the process equipment associated with this function is contained in reference 1.

D. Reactor Coolant System Low Flow Trips

These trips protect against a DNBR of less than the safety analysis limit in the event of a loss of coolant flow situation. The means of sensing the loss of coolant flow are as follows:

1. Low Reactor Coolant Flow

This is the primary trip credited in the loss of flow accidents. The parameter sensed is reactor coolant flow. Three elbow taps in each coolant loop are used as a flow device that indicates the status of reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flowrate has occurred. An output signal from two out of the three bistables in a loop would indicate a low flow in that loop. The coincidence logic and interlocks are given in table 7.2-1.

The detailed functional description of the process equipment associated with the trip function is contained in reference 1.

2. Reactor Coolant Pump Bus Undervoltage Trip

This trip is an anticipatory trip which provides protection against low flow which can result from loss of voltage to more than one reactor coolant pump (e.g., from plant blackout or reactor coolant pump breaker opening). Primary protection for these postulated events is provided by RCS low flow.

Two undervoltage sensing relays are connected to each of the three reactor coolant pump buses. Two undervoltage sensing relays are connected to the motor side of each of the three reactor coolant pump breakers (Unit 1 only). These relays provide output signals when the bus voltage goes below approximately 70 percent of rated voltage. Signals from these relays are time delayed (as shown in drawing U-166235) to prevent spurious trips caused by short-term voltage perturbations. The coincidence logic and interlocks are given in table 7.2-1.

3. Reactor Coolant Pump Bus Underfrequency Trip

This trip is an anticipatory trip which provides protection against low flow resulting from bus underfrequency, for example, a major power grid frequency disturbance. Primary protection for this postulated event is provided by RCS low flow.

Two underfrequency sensing relays are connected to each of the three reactor coolant pump buses. Signals from relays connected to any two of the buses (time delayed to prevent spurious trips caused by short-term frequency perturbations) will trip the reactor if the power level is above P-7.

Drawing U-166235 shows the logic for the reactor coolant system low flow trips.

E. Steam Generator Trip

The specific trip function generated is as follows:

Low-Low Steam Generator Water Level Trip

This trip protects the reactor from loss of heat sink in the event of a loss of feedwater to one or more steam generators or a major feedwater line rupture. This trip is actuated on two-out-of-three low-low water level signals occurring in any steam generator.

The logic is shown in drawing U-166237. A detailed functional description of the process equipment associated with this trip is provided in reference 1.

F. Turbine Trip/Reactor Trip

The turbine trip/reactor trip is actuated by two-out-of-three logic from low auto stop oil pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above P-9. High-high steam generator water level signals in two out of three channels for any steam generator will actuate a turbine trip, trip the main feedwater pumps, and close the main and bypass feedwater control valves. The purpose is to protect the turbine and steam piping from excessive moisture carryover caused by the high-high steam generator water level. Other turbine trips are discussed in chapter 10.

The logic for this trip is shown in drawing U-166237.

The analog portion of the trip shown in drawing U-166245 is represented by dashed (---) lines. When the turbine is tripped, turbine auto stop oil pressure drops and the pressure is sensed by three pressure sensors. A digital output is provided from each sensor when the oil pressure drops below a preset level. These three outputs are transmitted to two redundant two-out-of-three logic matrices, either of which trips the reactor if above P-9.

The auto stop oil pressure signal also dumps the stop emergency trip fluid, closing all of the turbine steam stop valves. When all stop valves are closed, a reactor trip signal will be initiated if the reactor is above P-9. This trip signal is generated by redundant limit switches on the stop valves.

Components specified for use as sensors for input signals to the reactor protection system for auto stop oil pressure and throttle valve position conform to IEEE 279-1971 requirements; however, seismic criteria are not included in the qualification regarding sensor design, mounting, and location for that portion of the trip system located within non-Category 1 structures. In addition, these circuits share common terminal blocks which include circuits not related to the reactor trip system. Any loss of signal due to a high-energy line break (HELB) or

other credible event in the turbine building will result in a reactor trip input on the affected channel to the reactor trip system.

These exceptions are taken in the specific application of certain design requirements contained in IEEE 384-1974 for separation of circuits, which are located by necessity in non-Category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. Separation of circuits is maintained up to the terminal boxes on the turbine skid. From the terminal boxes to the sensor, 1E separation requirements are not met. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

G. Safety Injection Signal Actuation Trip

A reactor trip occurs when the safety injection system is actuated. The means of actuating the safety injection system are described in section 7.3. This trip protects the core in the event of a loss-of-coolant accident.

Drawing U-166238 shows the logic for this trip. A detailed functional description of the process equipment associated with this trip function is provided in reference 1.

H. Manual Trip

The manual trip consists of two switches with multiple outputs on each switch. One output is used to actuate the train A trip breaker, and another output actuates the train B trip breaker. Operating a manual trip switch removes the voltage from the undervoltage trip coil and energizes the shunt trip coil, either of which will cause a reactor trip.

There are no interlocks which can block this trip. Drawing U-166233 shows the manual trip logic.

I. System Accuracies and Response Times

The system accuracies and the system response times of the instrument trip signals are given in table 7.2-3 and paragraph 7.2.1.2, respectively.

7.2.1.1.2 Reactor Trip System Interlocks

A. Power Escalation Permissives

The overpower protection provided by the out of core nuclear instrumentation consists of three discrete, but overlapping, levels. Continuation startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

FNP-FSAR-7

A one of two intermediate range permissive signal (P-6) is required prior to source range level trip locking and detector high voltage cutoff.

Source range level trips are automatically reactivated and high voltage restored when both intermediate range channels are below the permissive (P-6) level. There is a manual reset switch for administratively reactivating the source range level trip and detector high voltage between the permissive P-6 and P-10 level, if required. Source range level trip block and high voltage cutoff are always maintained when above the permissive P-10 level.

The intermediate range level trip and power range (low setpoint) trip can be blocked only after satisfactory operation and permissive information are obtained from two of four power range channels. Individual blocking switches are provided so that the low range power range trip and intermediate range trip can be independently blocked. These trips are automatically reactivated when any three of the four power range channels are below the permissive (P-10) level, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown in drawing U-166234. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

See table 7.2-2 for the list of protection system interlocks.

B. Blocks of Reactor Trips at Lower Power

Interlock P-7 blocks a reactor trip at low power (below approximately 10 percent of full power) on a low reactor coolant flow or reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, or pressurizer high water level. See drawing U-166236 and table 7.2-2 for permissive applications. The low power signal is derived from three out of four power range neutron flux signals below the setpoint, in coincidence with two out of two turbine impulse chamber pressure signals below the setpoint (low plant load).

The P-8 interlock blocks a reactor trip on a low reactor coolant flow in any one loop when reactor power is below the P-8 setpoint (see table 7.2-2). The block action (absence of the P-8 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor will be allowed to operate with one inactive loop and trip will not occur until two loops are indicating low flow. See drawing U-166234 for derivation of P-8.

See table 7.2-2 for the list of protection system blocks.

7.2.1.1.3 Coolant Temperature Sensor Arrangement

The hot and cold leg temperature signals required for input to the protection and control functions are obtained using thermowell mounted resistance temperature detectors (RTDs) installed in each reactor coolant loop.

The hot leg temperature measurement in each loop is accomplished using three fast response, dual element, narrow range RTDs mounted in thermowells.

To account for temperature streaming, the sensors are located 120 degrees apart, and the temperatures measured by the three hot leg RTDs are electronically averaged to generate a hot leg average temperature. Provisions were made in the RTD electronics to allow for operation with only two RTDs in service. The two RTD measurements can be biased to correct for the difference compared with the three RTD average.

The cold leg temperature measurement in each loop is accomplished by one fast response, narrow range, dual element RTD. Temperature streaming in the cold leg is minimized by the mixing action of the reactor coolant pump.

The response time allocated in the safety analyses for measuring RCS hot and cold leg temperature for the thermowell and the fast response RTDs is 5 s. This response time does not include the process electronics.

7.2.1.1.4 Water Level Measurement Arrangement

Following a high energy line rupture in the vicinity of a water level measurement system that utilizes a water filled reference leg, the resulting adverse environment may cause heatup of the water in the reference leg. The heatup of the reference leg fluid results in additional channel uncertainty. The NRC issued IE Bulletin 79-21 which instructed each utility to investigate the impact of reference leg heatup at their nuclear power plants.

In response to IE Bulletin 79-21, Alabama Power Company submitted information concerning the potential impact on Plant Farley. The following systems were identified to be used for initiation of safety functions:

- Narrow range steam generator water level; and
- Pressurizer water level.

7.2.1.1.4a Steam Generator Water Level Measurement

The narrow range steam generator water level channels initiate reactor trip and auxiliary feedwater pumps on low-low steam generator water level which is the primary trip function following a loss of all ac power to station auxiliaries, loss of normal feedwater, and main feedline rupture. A loss of all ac power to station auxiliaries and loss of normal feedwater does not result in an adverse environment inside containment. However, a postulated main feedline rupture inside containment results in an adverse environment which may result in the heatup of the level measurement system reference legs. Increased reference leg temperature results in a

decrease in reference leg density and a subsequent increase in indicated water level. To minimize the heatup of the reference leg heatup following a high energy line rupture inside the containment prior to reactor trip, the narrow range steam generator water level reference legs were insulated to minimize the reference leg heatup such that the measured level is not significantly affected prior to reactor trip. The trip setpoint has been increased to account for the uncertainty due to reference leg heatup.

The narrow and wide range steam generator water level channels are also used for post-accident monitoring. The Farley Nuclear Plant Emergency Response Procedures (ERPs) have incorporated the uncertainties due to reference leg pressure and temperature effects into the appropriate operator action setpoints for steam generator water level.

7.2.1.1.4b Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation includes a slight modification of the usual tank level arrangement using differential pressure between an upper and a lower tap. The modification shown in figure 7.2-2 consists of the use of a sealed reference leg instead of the conventional open column of water. Refer to paragraph 7.2.2.3.4 for an analysis of this arrangement.

Pressurizer water level initiates reactor trip on high level. This trip function is not assumed to mitigate any initiating events that result in an adverse environment. Therefore, the pressurizer reference leg was not insulated.

Pressurizer water level is also used for post-accident monitoring. The Farley Nuclear Plant ERPs have incorporated the uncertainties due to reference leg pressure and temperature effects into the appropriate operator action setpoints for pressurizer water level.

7.2.1.1.5 Analog System

The process analog system is described in reference 1.

7.2.1.1.6 Digital Logic System

The solid state logic protection system takes binary inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light, and computer input signals which indicate the condition of bistable input signals, partial trip, and full trip functions and provides the status of the various blocking, permissive, and actuation functions. In addition, the system includes means for semiautomatic testing of the logic circuits. A detailed description of this system is given in references 3, 22, 23, 24, 25, 26, 27, 28, 29, and 30.

7.2.1.1.7 Isolation Amplifiers

In certain design applications, Westinghouse considers it advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel, as permitted by Institute of Electrical and Electronics Engineers (IEEE) 279.

In all of these cases, analog signals derived from protection channels for nonprotective functions are obtained through isolation amplifiers located in the analog protection racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring.

Isolation amplifier qualification type tests are described in references 5 and 6.

7.2.1.1.8 Energy Supply and Environmental Variations

The energy supply for the reactor trip system, including the voltage and frequency variations, is described in section 7.6. The environmental variations throughout which the system will perform are given in section 3.11.

7.2.1.1.9 Trip Setpoints

The setpoints that, when reached, will require trip action are given in the plant Technical Specifications.

7.2.1.1.10 Seismic Design

The seismic design considerations for the reactor trip system are given in section 3.10. The seismic design as discussed in section 3.10 meets the requirements of General Design Criterion (GDC) 2.

7.2.1.2 Design Bases: IEEE 279-1971

The following are the generating station conditions requiring reactor trip (paragraph 7.1.2.2.2):

- A. DNBR approaching the safety analysis limit.
- B. Power density (kW/ft) approaching rated value for Condition II faults. (See chapter 4 for fuel design limits.)
- C. Reactor coolant system overpressure creating stresses approaching the limits specified in chapter 5.

The following are the variables required to be monitored in order to provide reactor trips (paragraph 7.2.1.1 and table 7.2-1):

FNP-FSAR-7

- A. Neutron flux.
- B. Reactor coolant temperature.
- C. Reactor coolant system pressure (pressurizer pressure).
- D. Pressurizer water level.
- E. Reactor coolant flow.
- F. Reactor coolant pump operational status (bus voltage and frequency).
- G. Steam generator water level.
- H. Turbine-generator operational status (auto stop oil pressure and stop valve position).

The reactor coolant temperature variable is spatially dependent. See paragraph 7.3.1.2 for a discussion of the spatial dependence of this variable.

Table 7.2-4 provides a correlation between the chapter 15 accident analyses and the reactor protection system functions. This table also describes which reactor protection system functions the chapter 15 analyses credit for primary protection and those functions which may be regarded as backup functions. The nominal trip setpoint for each reactor trip function is listed in the plant Technical Specifications. The safety analysis limit (SAL) for each reactor trip credited for event mitigation is listed in table 15.1-3. Setpoint uncertainty calculations for each reactor trip system function demonstrate adequate margin between the safety analysis limit and the corresponding nominal trip setpoint.

The setpoints for the various functions in the reactor trip system have been analytically determined so that the safety analysis limits will prevent fuel rod clad damage and loss of integrity of the reactor coolant system as a result of any Condition II incident (anticipated malfunction). As such, the reactor trip system limits the following parameters to:

- A. Minimum DNBR = the reactor core safety limit.
- B. Fuel rod maximum linear power = 22.4 kW/ft.
- C. Maximum system pressure = 2735 psig.

The accident analyses described in chapter 15 demonstrate that the functional requirements as specified for the reactor trip system are adequate to meet the above limits. A discussion of the safety limits associated with the reactor core and reactor coolant system, and the reactor trip setpoints, is presented in the plant Technical Specifications.

For a discussion of energy supply and environmental variations, see paragraph 7.2.1.1.8.

The malfunctions, accidents, or other unusual events that could physically damage reactor trip system components or could cause environmental changes are as follows:

FNP-FSAR-7

- A. Earthquakes (chapter 3).
- B. Fire.
- C. Explosion (hydrogen buildup inside containment).
- D. Missiles (section 3.5).
- E. Flood.
- F. Wind and tornadoes (section 3.3).

The design requirements are as follows:

A. System Response Times

The total delay to trip is defined as the time delay from the time that a step change in the variable being monitored from 5 percent below to 5 percent above the trip setpoint is reached to the time that the rods are free and begin to fall. This is with transfer functions set to one. **[HISTORICAL]***[During preliminary startup tests, it will be demonstrated that actual instrument errors and time delays are equal to or less than the values assumed in the accident analyses.]*

Maximum allowable time delays in generating the reactor trip signal are as follows:

	<u>Time (s)</u>
1. Power range high nuclear power (high and low setpoint)	0.5
2. Neutron flux positive rate	0.5
3. Maximum overtemperature ΔT (OT ΔT)	(a), (b)
4. Maximum overpower ΔT (OP ΔT)	(a), (b)

FNP-FSAR-7

5a.	Pressurizer pressure (high)	1.0
5b.	Pressurizer pressure (low)	2.0
6.	Pressurizer high water level	2.0
7.	Low reactor coolant flow	1.0
8.	Reactor coolant pump bus underfrequency	0.6
9.	Reactor coolant pump bus undervoltage (Unit 2 only) Reactor coolant pump breaker motor side undervoltage (Unit 1 only)	1.5
10.	Low-low steam generator water level	2.0
11.	Turbine trip	1.0

B. The historical basis for reactor trip accuracies is given in table 7.2-3. The total channel statistical accuracy for reactor trip system actuation signals is provided in WCAP-13751.⁽¹³⁾

C. Protection system ranges are as follows:

	Range
1. Power range nuclear power	1- to 120-percent full power
2. Neutron flux positive rate	± 5 percent to ± 30 percent of full power

Notes:

(a)	RTD response time	≤ 5.0 s
(b)	Channel electronics/trip logic & breaker/gripper release	
	1. Overtemperature ΔT (OT ΔT), Tavg input:	≤ 2.0 s
	2. Overtemperature ΔT (OP ΔT), pressurizer pressure input (including sensor)	≤ 2.0 s
	3. Overtemperature ΔT , nuclear flux input:	≤ 2.0 s
	4. Overpower ΔT , Tavg input:	≤ 2.0 s
	5. ΔT input (to both OT ΔT and OP ΔT):	≤ 2.0 s

See table 7.2-5 for test acceptance criteria.

FNP-FSAR-7

3.	Overtemperature ΔT :	
	$T_{\text{hot leg}}$	530°F to 650°F
	$T_{\text{cold leg}}$	510°F to 630°F
	T_{avg}	530°F to 630°F
	Pressurizer pressure	1700 to 2500 psig
	$f(\Delta I)$	-50 to +50 percent
	ΔT setpoint	0 to 150 percent of full power
4.	Overpower ΔT	(See overtemperature ΔT)
5.	Pressurizer pressure	1700 to 2500 psig
6.	Pressurizer water level	Entire cylindrical portion of pressurizer
7.	Reactor coolant flow	ΔP equivalent to 0 to 120 percent of nominal full power flow
8.	Reactor coolant pump bus underfrequency	50 to 65 Hz
9.	Reactor coolant pump bus undervoltage (Unit 2 only)	0- to 100-percent rated voltage
	Reactor coolant pump breaker motor side undervoltage (Unit 1 only)	
10.	Deleted	
11.	Steam generator water level	+6.2 to -11.5 ft from normal full load water level

7.2.1.3 Final System Drawings

The functional diagrams for the reactor trip system for FNP Units 1 and 2 are shown in the functional logic diagrams in drawings U-166231, U-166232, U-166233, U-166234, U-166235, U-166236, U-166237, U-166238, U-166239, U-166240, U-166241, U-166242, U-166243, U-166244, and U-166245, with portions of the reactor trip system shown specifically in drawings U-166231, U-166232, U-166233, U-166234, U-166235, U-166236, U-166237, U-166238, and U-166245. See subsection 7.1.3 and table 8.2-1 for a list of supplemental drawings.

7.2.2 ANALYSIS

7.2.2.1 Failure Mode and Effects Analysis

A failure mode and effects analysis of the reactor trip system has been performed. Results of this study and a fault tree analysis are presented in WCAP-7706, An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients.⁽⁷⁾

7.2.2.1.1 General Discussion of Evaluation of Design

The reactor trip system automatically keeps the reactor operating within a safe region by tripping the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. Therefore, the reactor trip system keeps surveillance on process variables which are directly related to equipment mechanical limitations, such as pressure and pressurizer water level to prevent water discharge through safety valves and uncovering heaters, and also on variables which directly affect the heat transfer capability of the reactor, e.g., flow and reactor coolant temperatures. Still other parameters utilized in the reactor trip system are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a setpoint, the reactor will be shut down in order to protect against either gross loss of fuel cladding or system integrity that could lead to release of radioactive fission product into the containment.

While most setpoints used in the reactor protection systems are fixed, there are variable setpoints, e.g., the overtemperature ΔT and overpower ΔT setpoints. All setpoints in the reactor trip system have been selected either on the basis of applicable engineering code requirements or engineering design studies.

The capability of the reactor trip system to prevent loss of integrity of the fuel clad and/or reactor coolant system pressure boundary during Condition II and III transients is demonstrated in the safety analyses of chapter 15. These safety analyses are carried out using those setpoints determined from results of the engineering design studies. Setpoint limits are presented in the plant Technical Specifications. A discussion of the intent for each of the various reactor trips and the accident analyses (when appropriate) which utilize this trip is presented in paragraph 7.2.2.1.2. It should be noted that the selected trip setpoints all provide for margin before protective action is actually required to allow for uncertainties and instrument errors. The design meets the requirements of GDC 10 and 20.

7.2.2.1.2 Trip Setpoint Discussion

It has been pointed out previously that above a DNBR equal to the safety analysis limit there is no significant local fuel clad failure. The DNBR existing at any point in the core for a given core design can be determined as a function of the core inlet temperature, power output, operating pressure, and flow. Consequently, core safety limits in terms of a DNBR equal to the safety analysis limit value for the hot channel can be developed as a function of core ΔT , T_{avg} , and pressure for a specified flow as illustrated by the solid lines in figure 15.1-1A. Also shown as

solid lines in figure 15.1-1A are the loci of conditions equivalent to 118 percent of power as a function of ΔT and T_{avg} representing the overpower (kW/ft) limit on the fuel. The dashed lines indicate the maximum permissible setpoint (ΔT) as a function of T_{avg} and pressure for the overtemperature and overpower reactor trip. Actual setpoint constants in the equation representing the dashed lines are as given in the plant Technical Specifications. These values are conservative to allow for instrument errors. The design meets the requirements of GDC 10, 15, 20, and 29.

The DNB is not a directly measurable quantity; however, the process variables that determine DNB are sensed and evaluated. Small isolated changes in various process variables may not, when considered singly, result in violation of a core safety limit, whereas the individual variations, when operating together over sufficient time, may cause the overpower or overtemperature safety limit to be exceeded. The design concept of the reactor trip system takes cognizance of this situation by providing reactor trips associated with individual process variables, in addition to the overpower/overtemperature safety limit trips. The process variable trips prevent reactor operation whenever a change in the monitored value is such that a core or system safety limit is in danger of being exceeded should operation continue. Basically, the high pressure, low pressure, and overpower/overtemperature ΔT trips provide sufficient protection for slow transients, as opposed to such trips as low flow or high flux which will trip the reactor for rapid changes in flow or flux, respectively, that would result in fuel damage before actuation of the more slowly responding ΔT trips could be effected.

Therefore, the reactor trip system has been designed to provide protection for fuel clad and reactor coolant system pressure boundary integrity where: a rapid change in a single variable or factor will quickly result in exceeding a core or a system safety limit, and a slow change in one or more variables will have an integrated effect which will cause safety limits to be exceeded. Overall, the reactor trip system offers diverse and comprehensive protection against fuel clad failure and/or loss of reactor coolant system integrity for Condition II and III accidents. This is demonstrated by table 7.2-4 which lists the various trips of the reactor trip system, the corresponding technical specification on safety limits and safety system settings, and the appropriate accident discussed in the safety analyses in which the trip could be utilized.

The nuclear power plant reactor trip system design employed by Westinghouse was evaluated in detail with respect to common mode failure and is presented in references 4 and 7. The design meets the requirements of GDC 21.

Preoperational testing is performed on reactor trip system components and systems to determine equipment readiness for startup. This testing serves as a very real evaluation of the system design.

Analyses of the results of Condition II, III, and IV events, including considerations of instrumentation installed to mitigate their consequences, are presented in chapter 15. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in section 7.4.

7.2.2.1.3 Reactor Coolant Flow Measurement

The elbow taps used on each loop in the primary coolant system are instrument devices that indicate the status of the reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. The correlation between flow and elbow tap signal is given by the following equation:

$$\frac{\Delta P}{\Delta P_O} = \left(\frac{w}{w_O} \right)^2$$

where ΔP_O is the pressure differential at the referenced flow w_O , and ΔP is the pressure differential at the corresponding flow w . The associated low flow reactor trip is a relative trip. As such, its setpoint is specified as a percentage of the reference flow and it is set at the corresponding ΔP . Uncertainties associated with the channel accuracy have been accounted for in the determination of the setpoint.

The full flow reference point is established during initial plant startup. The full flow reference point may be revised as necessary to reflect changes to actual plant conditions (e.g., tube plugging, fuel changes, pump degradation). At the beginning of each cycle of operation, a measurement must be performed to verify that the Minimum Measured Flow (MMF) listed in the Technical Specifications is met, thereby assuring that the safety analyses assumptions for flow have been satisfied. Appropriate uncertainties associated with the measurement of RCS flow have been accounted for in the determination of the MMF.

7.2.2.2 Evaluation of Compliance to Applicable Codes and Standards

7.2.2.2.1 Evaluation of Compliance with IEEE 279-1971

The reactor trip system meets the requirements of IEEE 279-1971⁽⁸⁾ as indicated below.

A. Single Failure Criterion

The protection system is designed to provide redundant (two, three, or four) instrumentation channels for each protective function and two logic train circuits. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required. This design meets the requirements of GDC 21. Loss of input power, the most likely mode of failure, to a channel or logic train will result in a signal calling for a trip. This design meets the requirements of GDC 23.

To prevent the occurrence of common mode failures, such additional measures as functional diversity, physical separation, and testing as well as administrative control during design, production, installation, and operation are employed, as discussed in reference 7. This design meets the requirements of GDC 21 and

22. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 279-1971 for separation of circuits, which are located by necessity in non-Category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

B. Quality of Components and Modules

For a discussion of the quality of the components and modules used in the reactor trip system, refer to chapter 17. The quality used meets the requirements of GDC 1.

C. Equipment Qualification

For a discussion of the type tests made to verify the performance requirements, refer to section 3.11. The test results demonstrate that the design meets the requirements of GDC 4.

D. Independence

Each individual channel is assigned to one of four channel designations, e.g., Channel I, II, III, or IV is shown in figure 7.2-3. Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in different protection cabinets. Each redundant channel is energized from a separate ac power feed. This design meets the requirements of GDC 21. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 279-1971 for separation of circuits, which are located by necessity in non-category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

Independence of the logic trains is discussed in reference 3. Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply, so that opening either breaker interrupts power to all full length control rod drive mechanisms, permitting the rods to free fall into the core.

The design philosophy is to make maximum use of a wide variety of measurements. The protection system continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in reference 4. Generally, two or

more diverse protective functions would terminate an accident before intolerable consequences could occur. This design meets the requirements of GDC 22.

E. Control and Protection System Interaction

The protection system is designed to be independent of the control system. In certain applications the control signals and other nonprotective functions are derived from individual protection channels through isolation amplifiers. The isolation amplifiers are classified as part of the protection system and are located in the analog protection racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring. The isolation amplifiers are designed such that a short circuit, an open circuit, or the application of 118 V-ac or 140 V-dc on the isolated output portion of the circuit (i.e., the nonprotective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation amplifiers are never returned to the protection racks. This design meets the requirements of GDC 24.

A detailed discussion of the design and testing of the isolation amplifiers is given in references 5 and 6. These reports include the results of applying various malfunction conditions on the output portion of the isolation amplifiers. The results show that no significant disturbance to the isolation amplifier input signal occurred. This design meets the requirements of GDC 24.

Where a single failure of a protection system component can cause a process perturbation which requires protective action, the protection system has been designed to withstand a second failure, without loss of protective action. This feature is normally achieved by providing two-out-of-four trip logic for each of the protective functions with the exception of steam generator protection, which relies on two-out-of-three trip logic, a control grade median signal selector (MSS) and the separation of previously shared protection set III narrow range level and steam flow instrument taps and associated instrument lines. The use of a control grade MSS will prevent any protection system failure from causing a control system action resulting in a need for subsequent protective action. This design meets the requirements of GDC 24.

Redundant control signal cables leaving the protection racks through isolation devices can come into close proximity elsewhere in the plant, such as the control board. It could be postulated that electrical faults or interference at these locations might be propagated into all redundant racks and degrade protection circuits because of the close proximity of protective and control wiring within each rack. Regulatory Guide 1.75, position C.4, and IEEE 384-1974, section 4.5(3), provide the option to demonstrate by tests that the absence of physical separation could not significantly reduce the availability of Class 1E circuits.

Therefore, Westinghouse conducted tests to demonstrate that Class 1E protection systems (nuclear instrumentation system, solid-state protection system, and 7300 process control system) could not be degraded by non-Class 1E circuits sharing the same enclosure. Conformance to the requirements of IEEE 279-1971 and Regulatory Guide 1.75 was established and accepted by the

FNP-FSAR-7

Nuclear Regulatory Commission (NRC); these requirements are applicable to these systems at the FNP units.

Tests conducted on the as-built designs of the nuclear instrumentation system and solid-state protection system were reported and accepted by the NRC in support of the Diablo Canyon application (dockets 51-275 and 50-323). Westinghouse considers these programs as applicable to all plants, including FNP. Westinghouse tests on the 7300 series process control system were covered in a report entitled, "Westinghouse 7300 Series Process Control System Noise Tests," subsequently reissued as reference 9. In a letter dated April 20, 1977,⁽¹⁰⁾ the NRC accepted the report in which the applicability of the FNP units is established (appendix G in reference 10).

F. Capability for Testing

The reactor trip system is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to ensure complete system operation. The protection system is designed to permit periodic testing of the analog channel portion of the reactor trip system during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. Note, however, that the source and intermediate range high neutron flux trips must be bypassed during testing.

The operability of the process sensors is ascertained by comparison with redundant channels monitoring the same process variables or those with a fixed known relationship to the parameter being checked. The process sensors within containment can be calibrated during plant shutdown.

Analog channel testing is performed at the analog instrumentation rack set by individually introducing simulated input signals into the instrumentation channels and observing the tripping of the appropriate output bistables. Process analog output to the logic circuitry is interrupted during individual channel test by a test switch which, when thrown, deenergizes the associated logic input and inserts a proving lamp in the bistable output. Interruption of the bistable output to the logic circuitry for any cause (test, maintenance purposes, or removed from service) will cause that portion of the logic to be actuated (partial trip), accompanied by a partial trip alarm and channel status light actuation in the control room. Each channel contains those switches, test points, etc., necessary to test the channel. See reference 1 for additional information.

The power range channels of the nuclear instrumentation system are tested by superimposing a test signal on the actual detector signal being received by the channel at the time of testing. The output of the bistable is not placed in a tripped condition prior to testing. Also, since the power range channel logic is two out of four, bypass of this reactor trip function is not required.

FNP-FSAR-7

To test a power range channel, a test-operate switch is provided to require deliberate operator action. Operation of the switch will initiate the channel test annunciator in the control room. Bistable operation is tested by increasing the test signal level up to its trip setpoint and verifying bistable relay operation by control board annunciator and trip status lights.

It should be noted that a valid trip signal would cause the channel under test to trip at a lower actual reactor power level. A reactor trip would occur when a second bistable trips. No installed provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the nuclear instrumentation system detector. If it is required to test a function with a setpoint below the signal being received from the detector, the detector input cables must be disconnected.

A nuclear instrumentation system channel which can cause a reactor trip through one-out-of-two protection logic (source or intermediate range) is provided with a bypass function that prevents the initiation of a reactor trip from that particular channel during the short period that it is undergoing testing. These bypasses initiate an alarm in the control room. For a detailed description of the nuclear instrumentation system, see reference 2.

The reactor logic trains of the reactor trip system are designed to be capable of complete testing at power. Annunciation is provided in the control room to indicate when a train is in test, when a reactor trip is bypassed, and when a reactor trip breaker is bypassed. Details of the logic system testing are given in reference 3. Applicability of the intervals for online functional testing of the reactor trip system is detailed in references 16, 20, and 21.

The reactor coolant pump breakers cannot be tripped at full power without causing a plant upset by loss of power to a coolant pump. However, the continuity test of the shunt trip coil can be tested at power. Manual trip cannot be tested at power without causing a reactor trip, since operation of either manual trip switch actuates both train A and train B. Turbine trip cannot be completely tested since a turbine trip/reactor trip would occur, thus interfering with normal operation. The logic for the safety injection reactor trip can be tested completely. However, actual safety injection cannot be initiated since this would interfere with normal plant operation.

The undervoltage and underfrequency sensing relays are tested during plant outage. The input to the solid-state protection system from these relays is tested during reactor operation, using the testing provisions of the system.

The logic associated with these trips is fully testable at power as discussed in paragraph 7.2.2.2.1.F.

Testing of the logic trains of the reactor trip system includes a check of the input relays and a logic matrix check. The following sequence is used to test the system:

1. Check of Input Relays

During testing of the process instrumentation system and nuclear instrumentation system channels, each channel bistable is placed in a trip mode causing one input relay in train A and one in train B to deenergize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. The contact that creates the reactor trip also causes a status lamp and an annunciator on the control board to operate. Either the train A or train B input relay operation will light the status lamp and annunciator.

Each train contains a multiplexer test switch. At the start of a process or nuclear instrumentation system test, this switch (in either train) is placed in the A + B position. The A + B position alternately allows information to be transmitted from the two trains to the control board. A steady status lamp and annunciator indicates that input relays in both trains have been deenergized. A flashing lamp means that one of the two trains is not operating properly. Contact inputs to the logic protection system, such as reactor coolant pump bus underfrequency relays, operate input relays which are tested by operating the remote contacts as described above and using the same type of indications as those provided for bistable input relays.

Actuation of the input relays provides the overlap between the testing of the logic protection system and the testing of those systems supplying the inputs to the logic protection system. Test indicators are status lamps and annunciators on the control board. Inputs to the logic protection system are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two out of four channels trip becomes a one-out-of-three trip when one channel is placed in the trip mode. Both trains of the logic protection system remain in service during this portion of the test.

2. Check of Logic Matrices

Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semiautomatic test panel in the train. Details of semiautomatic tester operation are given in reference 3. At the completion of the logic matrix and other associated tests, the return of the input error inhibit switch contacts to normal position is verified for each protection channel.

The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester.

The pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

Test indicators that are provided are an annunciator in the control room, indicating that reactor trips from the train have been blocked and that the train is being tested, and green and red lamps on the semiautomatic tester to indicate a good or bad logic matrix test. Protection capability provided during this portion of the test is from the train not being tested.

The general design features and details of the testability of the logic system are described in reference 3.

The testing capability meets the requirements of GDC 21.

G. Testing of Reactor Trip Breakers

Normally, reactor trip breakers A and B are in service, and bypass breakers A and B are racked in but open. In testing the protection logic, pulse techniques and the reactor trip bypass breakers are employed to prevent inadvertent reactor trip. The following procedure describes the method used for testing the trip breakers:

1. Close reactor trip bypass breaker A(B).
2. Depress and maintain Auto-Shunt Trip block pushbutton.
3. Manually trip reactor trip breaker A(B) through a protections system logic matrix.
4. Verify that reactor trip breaker A(B) trips open.
5. Release Auto-Shunt Trip block pushbutton.
6. Reclose reactor trip breaker A(B) from MCB.
7. Depress the Auto-Shunt Trip trip pushbutton momentarily.
8. Verify that reactor trip breaker A(B) trips open.
9. Reset reactor trip breaker A(B) at the MCB.
10. Open reactor trip bypass breaker A(B).

Auxiliary contacts of the bypass breakers are connected into the general warning alarm reactor trip alarm system of their respective trains such that, if either train is placed in test while the bypass breaker of the other train is closed, both reactor trip breakers and both bypass breakers will automatically trip.

Auxiliary contacts of the bypass breakers are also connected in such a way that, if an attempt is made to close the bypass breaker in one train while the bypass breaker of the other train is already closed, both bypass breakers will automatically trip.

The train A and train B alarm systems operate separate annunciators in the control room. The two bypass breakers also operate an annunciator in the control room. Bypassing of a protection train with either the bypass breaker or with the test switches will result in audible and visual indications.

The complete reactor trip system is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, a technical specification defining the minimum number of operable channels and the minimum degree of channel redundancy has been formulated. This technical specification also defines the required restrictions of operation in the event that the channel operability and degree of redundancy requirements cannot be met. Additionally, Technical Specifications will address the testing of the undervoltage and shunt trip functions and the manual reactor trip switch contact and wiring.

The reactor trip system is designed in such a way that response time tests can only be performed during shutdown. However, the safety analyses utilize conservative numbers for trip channel response time. The measured channel response times are compared with those used in the safety evaluations. On the basis of startup tests conducted on several plants, the actual response times measured are less than the times used in the safety analyses.

H. Bypasses

Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protection system and are designed in accordance with the criteria identified in paragraph 7.1.2.1.6. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

I. Multiple Setpoints

For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the protection system circuits are designed to provide positive means of administrative control (see paragraph 7.2.2.1.2) to ensure that the more restrictive trip setpoint is used. The devices used to prevent improper use of less restrictive trip settings are considered part of the protection system and are designed in accordance with the criteria of this section.

FNP-FSAR-7

J. Completion of Protective Action

The protection system is so designed that, once initiated, a protective action goes to completion. Return to normal operation requires action by the operator.

K. Manual Initiation

Switches (see drawings U-166233 and U-166235 for identification) are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment.

L. Access

The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, and test points and the means for manually bypassing channels or protective functions. For details refer to reference 1.

M. Information Readout

The protection system provides the operator with complete information pertinent to system status and safety. All transmitted signals (flow, pressure, temperature, etc.) which can cause a reactor trip are either indicated or recorded for every channel (see section 7.5), including all neutron flux power range currents (top detector, bottom detector, algebraic difference, and average of bottom and top detector currents).

Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified down to the channel level.

Alarms and annunciators are also used to alert the operator of deviations from normal operating conditions, so that he may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

N. Identification

The identification described in section 7.1 provides immediate and unambiguous identification of the protection equipment.

7.2.2.2.2 Evaluation of Compliance with IEEE 308

See paragraph 8.3.1.2 for a discussion of the power supply for the reactor trip system and compliance with IEEE 308.⁽¹¹⁾

7.2.2.2.3 Evaluation of Compliance with IEEE 323

Most electrical devices and components are standard products and were type tested during the developmental stage to substantiate the adequacy of design. This is the preferred method as indicated in IEEE 323.⁽¹²⁾ Documentation of type testing is in possession of the manufacturers and may not be in the form given in this IEEE standard. Successful operating experience was an important factor in determining the adequacy of the electrical equipment, because most of it is conventional type that has widespread use in the industry.

7.2.2.2.4 Evaluation of Compliance with IEEE 338

The periodic testing of the reactor trip system conforms to the requirements of IEEE 338⁽¹³⁾ with the following comments:

- A. The response time was checked during preoperational testing and is periodically tested as described in the Technical Specifications.
- B. The reliability goals specified in paragraph 4.2 of IEEE 338 are developed for FNP and described in the Technical Specifications.
- C. The periodic test frequency discussed in paragraph 4.3 of IEEE 338 and specified in the plant Technical Specifications is conservatively selected to ensure that equipment associated with protective functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the test frequency is accelerated to accommodate the situation until the marginal performance is resolved.
- D. The test interval discussed in paragraph 5.2 of IEEE 338 is developed primarily on past operating experience and modified, if necessary, to ensure that system and subsystem protection is reliably provided. Analytical methods for determining reliability are not used to determine test interval.

7.2.2.2.5 Evaluation of Compliance with IEEE 344

The seismic testing as discussed in section 3.10 and the references of section 3.10 conform to the guidelines set forth in IEEE 344⁽¹⁴⁾ with the exceptions noted in section 3.10.

7.2.2.2.6 Evaluation of Compliance with NRC General Design Criteria

The reactor trip system meets the requirements of the GDC⁽¹⁵⁾ as indicated throughout chapter 7.

7.2.2.3 Specific Control and Protection Interactions

7.2.2.3.1 Neutron Flux

The flux difference between the upper and lower long ion chambers from three of the four power range neutron detectors are used as inputs to the OT Δ T and OP Δ T setpoints. The isolated nuclear power output signal from the fourth channel is used for automatic rod control.

In addition, a deviation signal will give an alarm if any nuclear power channel deviates significantly from any of the other channels. Also, the control system will respond only to rapid changes in indicated nuclear power; slow changes or drifts are compensated by the temperature control signals. Finally, an overpower signal from any nuclear power channel will block manual and automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.2.3.2 Coolant Temperature

The accuracy of the narrow range resistance temperature detector (RTD) temperature measurements is demonstrated during plant startup tests by comparing temperature measurement from all RTDs with one another as well as with the wide range temperature measurements obtained from the RTDs located in separate wells in the hot leg and cold leg piping of each loop. The comparisons are done with the RCS in an isothermal condition. The linearity of the Δ T measurements obtained from the hot leg and cold leg RTDs as a function of plant power is also checked during plant startup tests. The absolute value of Δ T versus plant power is not important as far as reactor protection is concerned. Reactor trip system setpoints are based upon percentages of the indicated Δ T at nominal full power rather than on absolute values of Δ T. For this reason, the linearity of the Δ T signals as a function of power is of importance rather than the absolute values of the Δ T. As part of the plant startup tests, the loop RTD signals are compared with the core exit thermocouple signals.

The input signals (one per loop) to the reactor control system are obtained from electronically isolated protection T_{avg} and Δ T signals. An MSS is implemented in the reactor control system, one for T_{avg} and one for Δ T. The MSS receives three signals as inputs and selects the median signal for input to the appropriate control systems. Any single input failure, high or low, will not result in an adverse control system response since the failed high or low temperature signal will be rejected by the MSS. Hence, the implementation of an MSS in the reactor control system in conjunction with two-out-of-three protection logic satisfies the requirements of IEEE 279-1971, Section 4.7, "Control and Protection System Interaction."

In addition, channel deviation signals in the control system will give an alarm if any temperature channel deviates from a preset value of the median value by more than a preset amount. Automatic rod withdrawal blocks will also occur if any two of the temperature channels indicate an overtemperature or overpower condition.

7.2.2.3.3 Pressurizer Pressure

The pressurizer pressure protection channel signals are used for high and low pressure protection and as inputs to the overtemperature ΔT trip protective function. The FNP uses separate pressure channels for protection and control.

The pressurizer heaters are incapable of overpressurizing the reactor coolant system. Overpressure protection is based upon the positive surge of the reactor coolant produced as a result of turbine trip under full load, with a complete loss of feedwater, assuming the core continues to produce full power. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and an accumulation of 3 percent. Note that no credit is taken for the control system operation during this event.

In addition, operation of any one of the power-operated relief valves can maintain pressure below the high pressure trip point for most transients. The rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available to alert the operator of the need for appropriate action.

7.2.2.3.4 Pressurizer Water Level

Three pressurizer water level channels are used for reactor trip (2/3 high level). Isolated signals from these channels are used for pressurizer water level control. A failure in the water level control system could fill or empty the pressurizer at a slow rate (on the order of 1/2 h or more).

Experience has shown that hydrogen gas can accumulate in the upper part of the condensate pot on conventional open reference leg systems in pressurizer water level service. At reactor coolant system operating pressures, high concentrations of dissolved hydrogen in the reference leg water are possible. Upon sudden depressurization accidents, it has been hypothesized that rapid effervescence of the dissolved hydrogen could blow water out of the reference leg and cause a large level error, measuring higher than actual level.

Accurate calculations of this effect have been difficult to obtain. To eliminate the possibility of such effects, a bellows is used in a pot on the top of the reference leg to provide an interface seal and prevent dissolving of hydrogen gas into the reference leg water. Supplier tests were run which confirmed a time response of < 1.0 s.

The reference leg is uninsulated and will remain at local ambient temperature. This temperature will vary somewhat over the length of the reference leg piping under normal operating conditions but will not exceed 140°F. During a blowdown accident, any reference leg water flashing to steam will be confined to the condensate steam interface in the condensate pot at the top of the temperature barrier leg and will have only a small (about 1 in.) effect on the measured level. Some additional error may be expected due to effervescence of hydrogen in the temperature barrier water. However, even if complete loss of this water is assumed, the error will be less than 1 ft and can be tolerated.

The sealed reference leg design has been installed in various plants since early 1970, and operational accuracy was verified by use of the sealed reference leg system in parallel with an

open reference leg channel. No effects of operating pressure variations on either the accuracy or integrity of the channel have been observed.

Calibration of the sealed reference leg system is done in place after installation by application of known pressure to the low pressure side of the transmitter and by measurement of the height of the reference column. The effects of static pressure variations are predictable. The largest effect is due to the density change in the saturated fluid in the pressurizer itself. The effect is typical of level measurements in all tanks with two-phase fluid and is not peculiar to the sealed reference leg technique. In the sealed reference leg, there is a slight compression of the fill water with increasing pressure, but this is taken up by the flexible bellows. A leak of the fill water in the sealed reference leg can be detected by comparison of redundant channel readings on line and by physical inspection of the reference leg off line. Leaks of the reference leg to the atmosphere will be immediately detectable by off-scale indications and alarms on the control board. A closed pressurizer level instrument shutoff valve would be detected by comparing the level indications from the redundant level channels (three channels). In addition, there are alarms on one of the three channels to indicate an error between the measured pressurizer water level and the programmed pressurizer water level. There is no single instrument valve which could affect more than one of the three level channels.

The high water level trip setpoint provides sufficient margin such that the undesirable condition of discharging liquid coolant through the safety valves is avoided. Even at full power conditions, which would produce the worst thermal expansion rates, a failure of the water level control would not lead to any liquid discharge through the safety valves. This is due to the automatic high pressurizer pressure reactor trip actuating at a pressure sufficiently below the safety valve setpoint.

For control failures which tend to empty the pressurizer, two-out-of-three logic for safety injection action on low pressurizer pressure ensures that the protection system can withstand an independent failure in another channel. In addition, ample time and alarms exist to alert the operator of the need for appropriate action.

7.2.2.3.5 Steam Generator Water Level and Feedwater Flow

The basic function of the reactor protection circuit associated with low steam generator water level is to preserve the steam generator heat sink for removal of long-term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to maintain residual heat removal after trip, preventing eventual thermal expansion and discharge of the reactor coolant through the pressurizer relief valves into the relief tank even when main feedwater pumps are incapacitated. This reactor trip acts before the steam generators are dry to reduce the required capacity and starting time requirements of these auxiliary feedwater pumps and to minimize the thermal transient on the reactor coolant system and steam generators. Therefore, a low-low steam generator water level reactor trip is provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient. It is desirable to minimize thermal transients on a steam generator for a credible loss of feedwater accident. A protection system failure causing control system action is eliminated by providing separate taps for previously shared protection set III steam flow and steam generator narrow range level channels and physically separating

these instrument lines. In addition, a control grade MSS is installed in each steam generator water level control system. The prime objective of the MSS is to prevent a single failed protection system instrument channel from causing a perturbation to feedwater control system requiring subsequent protective action. All three narrow range water level channels for each steam generator provide input to the MSS. The MSS selects the median signal for use by the feedwater control system and determines control system action based on this signal. By rejecting the high and low signals, the MSS prevents unwarranted control system action based on a single, failed protection system instrument channel. Since no adverse control system action may now result from a single, failed protection instrument channel, a second random protection system failure (as would otherwise be required by IEEE-279-1971) need not be considered. A more detailed discussion of the MSS and its compliance with control and protection system single interaction criteria can be found in reference 17.

7.2.2.3.6 Environmental Control and Protection Interaction

Following a high energy line rupture, a potential exists that plant control systems which are not environmentally qualified to operate when subjected to adverse environmental conditions may be impacted. As a result of being subjected to adverse environmental conditions, a potential exists that the operation of one or more of these control systems may be degraded or exhibit spurious operating characteristics. Consequently, the initial conditions and assumptions associated with the Plant Farley accident analyses presented in chapter 15 may not be conservative due to the postulated control and protection system environmental interactions. The NRC issued IE Information Notice 79-22 requesting each utility to review their plant and determine the probability of such control and protection interactions occurring following a high energy line rupture.

In response to the Information Notice 79-22, issued September 14, 1979, Alabama Power Company reviewed several control systems for potential environmental interactions. The control systems investigated included reactor control, pressurizer pressure and level control, feedwater control, steam generator pressure control, steam dump control, and turbine control. Potential environmental interactions involving each of the above control systems were evaluated for the following high energy line breaks: small and large steamline rupture; small and large feedline rupture; small and large loss of coolant accident (LOCA); and rod ejection. The forty-nine possible environmental interactions investigated were determined to be bounded by the following four interactions identified in IE Information Notice 79-22 for Plant Farley:

- Main feedwater control system following a small feedline rupture outside containment;
- Steam generator PORV control system following a feedline rupture outside containment;
- Pressurizer PORV control system following a feedline rupture inside containment; and
- Rod control system following a small steamline rupture inside containment.

For the first three interactions identified, it was shown that the analyses presented in WCAP-9600, Report on Small Break Accidents for Westinghouse NSSS, bounded the consequences of the identified environmental interactions. A typical bounding analysis was performed to

demonstrate the consequences of the fourth interaction were within the results of those presented in the Plant Farley Safety Analysis Report.

7.2.3 TESTS AND INSPECTIONS

The reactor trip system meets the testing requirements of IEEE 338⁽¹³⁾ with the exceptions given in paragraph 7.2.2.2.4. The testability of the system is discussed in paragraph 7.2.2.1.F. The initial test intervals are specified in the plant Technical Specifications.

7.2.3.1 Inservice Tests and Inspections

Periodic surveillance of the reactor trip system is performed to ensure proper protective action. This surveillance consists of checks, calibrations, channel operational testing, response time testing, actuation logic testing, and trip actuating device operational testing which are summarized as follows:

A. Checks

A channel check shall be the qualitative assessment, by observation, of channel behavior during operation. This determination shall include, where possible, comparison of the channel indication and status to other indications or status derived from independent instrument channels measuring the same parameter. Failures such as blown instrument fuses, defective indicators, or faulted amplifiers are noticeable by simple observation of the functioning of the instrument or system. Furthermore, in many cases such failures are revealed by alarm or annunciator action, and a check supplements this type of surveillance.

B. Calibration

A channel calibration shall be the adjustment, as necessary, of the channel so that it responds within the required range and accuracy to known input. The channel calibration shall encompass the entire channel, including the required sensor, alarm, interlock, and trip functions. Calibration of instrument channels with resistance temperature detector (RTD) or thermocouple sensors may consist of an in-place qualitative assessment of sensor behavior and normal calibration of the remaining adjustable devices in the channel. Whenever a sensing element is replaced, the next required channel calibration shall include an in-place cross calibration that compares the other sensing elements with the recently installed sensing element. The channel calibration may be performed by means of any series of sequential, overlapping calibrations or total channel steps so that the entire channel is calibrated.

C. Channel Operational Testing

A channel operational test (COT) shall be the injection of a simulated or actual signal into the channel as close to the sensor as practicable to verify the

operability of required alarm, interlock, and trip functions. The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints so that the setpoints are within the required range and accuracy.

D. Response Time Testing

Response time testing consists of any series of sequential, overlapping, or total channel test measurements provided that such tests demonstrate the total channel response time as defined in the Technical Specifications. Sensor response time verification may be demonstrated by either 1) in place, onsite, or offsite test measurements or 2) utilizing replacement sensors with certified response times. The test results must be compared to properly defined acceptance criteria. In lieu of testing, bounding response time allocations may be used for selected protection system sensor and signal processing channel and actuation logic components. The technical basis and methodology for verifying RTS response time criteria using a combination of test data and bounding sensor and/or component response time allocations is provided in references 18 and 19. The measurement/verification of response time at the specified frequencies provides assurance that the reactor trip associated with each channel is completed within the time limit assumed in the accident analyses. The response time limits assumed in the safety analyses for the reactor trip system are provided in table 7.2-5.

E. Actuation Logic Testing

An actuation logic test shall be the application of various simulated or actual input combinations in conjunction with each possible interlock logic state and the verification of the required logic output. The actuation logic test, as a minimum, shall include a continuity check of output devices.

F. Trip Actuating Device Operational Test (TADOT)

A TADOT shall consist of operating the trip actuating device and verifying the OPERABILITY of required alarm, interlock, and trip functions. The TADOT shall include adjustment, as necessary, of the trip actuating device so that it actuates at the required setpoint within the required accuracy.

The minimum frequency for checks, calibration, channel operational testing, response time testing, actuation logic testing, and trip actuating device operational testing are defined in the plant's Technical Specifications.

7.2.3.2 Periodic Testing of the Nuclear Instrumentation System

The following periodic tests of the nuclear instrumentation system are performed:

- A. Testing at plant shutdown.
 - 1. Source range testing.
 - 2. Intermediate range testing.

3. Power range testing.
- B. Testing between P-6 and P-10 permissive power levels.
 1. Source range testing.
 2. Intermediate range testing.
 3. Power range testing.
- C. Testing above P-10 permissive power level.
 1. Source range testing
 2. Intermediate range testing.
 3. Power range testing.

Any deviations noted during the performance of these tests are investigated and corrected in accordance with the established calibration and troubleshooting procedures provided in the plant technical manual for the nuclear instrumentation system. Control and protection trip settings are indicated in the precautions, limitations, and setpoint documents for the nuclear steam supply system. The NIS reactor trip system setpoints are also provided in the plant Technical Specifications.

7.2.3.3 Periodic Testing of the Process Analog Channels of the Protection Circuits

The following periodic tests of the analog channels of the protection circuits are performed:

- A. T_{avg} and ΔT protection channel testing.
- B. Pressurizer pressure protection channel testing.
- C. Pressurizer water level protection channel testing.
- D. Steam generator water level protection channel testing.
- E. Reactor coolant flow protection channel testing.
- F. Impulse chamber pressure channel testing.

The following conditions are required for these tests:

- A. These tests may be performed at any plant power from cold shutdown to full power.
- B. Before starting any of these tests with the plant at power, all redundant reactor trip channels associated with the function to be tested must be in the normal (untripped) mode in order to avoid spurious trips.
- C. Control and protection setpoints are indicated in the precautions, limitations, and setpoint documents for the nuclear steam supply system. The process analog reactor trip system setpoints are also provided in the plant Technical Specifications.

- D. Reference is made to the supplier's systems manual(s) for systems description and static and dynamic testing (to be supplied with the equipment).
- E. Reference is made to the supplier's manual instrument documentation sheets, which provide information on available signal ranges and adjustments. In addition, the supplier's report of equipment test results provides equipment calibration data.
- F. Median Signal Selector Testing. The signal selector has been provided with the capability for online testing commensurate with periodic testing of the steam generator level channels. Signal selector testing consists of monitoring the three input signals and the one output signal via test points. Comparison of the output signal to the input signals permits determination of whether or not the median signal is being passed and, consequently, whether the signal selector is functioning properly. Any output signal at a value other than that corresponding to the median signal is indicative of a unit failure.

7.2.3.4 Regulatory Guide 1.22

Periodic testing of the reactor trip system actuation functions, as described, complies with NRC Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, February 1971. (See paragraph 7.1.2.8.)

REFERENCES

1. Reid, J. B., "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP-7913, January 1973.
2. Lipchak, J. B. and Stokes, R. A., "Nuclear Instrumentation System," WCAP-7669, April 1971.
3. Katz, D. N., "Solid State Logic Protection System Description," WCAP-7672, June 1971.
4. Burnett, T. W. T., "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," WCAP-7306, April 1969.
5. Garber, I., "Test Report of Isolation Amplifiers," WCAP-7862, August 1972.
6. Bartholomew, R. and Lipchak, J., "Test Report, Nuclear Instrumentation System Isolation Amplifier," WCAP-7819, Revision 1, January 1972.
7. Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706, July 1971.
8. Institute of Electrical and Electronics Engineers, "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE 279-1971.
9. Marasco, F. W. and Siroky, R. M., "Westinghouse 7300 Series Process Control System Noise Tests," WCAP-8892A, June 1977.
10. Letter dated April 20, 1977, from R. L. Tedesco (NRC) to C. Eicheldinger (Westinghouse).
11. Institute of Electrical and Electronics Engineers, "Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations," IEEE 308-1971.
12. Institute of Electrical and Electronics Engineers, "Trial-Use Standard: General Guide for Qualifying Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 323-1971.
13. Institute of Electrical and Electronics Engineers, "Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE 338-1971.
14. Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Seismic Qualification of Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 344-1971.
15. U.S. Nuclear Regulatory Commission, "General Design Criteria for Nuclear Power Plants," Appendix A to 10 CFR 50, July 7, 1971.

FNP-FSAR-7

16. Jansen, R. L., "Evaluation of Surveillance Frequencies and Out of Service Times for Reactor Protection Instrumentation System-Supplement 1," WCAP-10271, Supplement 1-P-A, May 1986.
17. "Elimination of the Low Feedwater Flow Reactor Trip via Implementation of the Median Signal Selector (MSS) at Farley Units 1 and 2," WCAP-13807 (Proprietary) and WCAP-13808 (Nonproprietary), August 1993.
18. Howard, R. C., "Elimination of Pressure Sensor Response Time Testing Requirements," WCAP-13632-P-A, Rev. 2, January 1996.
19. Morgan, C. E., "Elimination of Periodic Protection Channel Response Time Tests," WCAP-14036-P-A, Rev. 1, October 1998.
20. "Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times," WCAP-14333-P-A, Revision 1, October 1998.
21. "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test Completion Times," WCAP-15376-P-A, Revision 1, March 2003.
22. WCAP-16769-P Revision 2, "Westinghouse SSPS Universal Logic Board Replacement Summary Report 6D30225G01/G02/G03/G04."
23. WCAP-16670-P Revision 0, "Westinghouse SSPS Safeguards Driver Board Replacement Summary Report 6D30252G01/G02."
24. WCAP-16671-P Revision 1, "Westinghouse SSPS Undervoltage Driver Board Replacement Summary Report 6D30350G01/G02."
25. WCAP-16672-P Revision 1, "Westinghouse SSPS Semi-Automatic Tester Board Replacement Summary Report 6D30520G01/G02/G03/G04/G05."
26. WCAP-17867-P-A Revision 1, "Westinghouse SSPS Board Replacement Licensing Summary Report."
27. WCAP-16773-P Revision 0, "Westinghouse SSPS Clock Counter Board Replacement Summary Report 6D30687G01."
28. WCAP-16774-P Revision 0, "Westinghouse SSPS Decoder Board Replacement Summary Report 6D1031G01."
29. WCAP-16775-P Revision 0, "Westinghouse SSPS Isolation Board Replacement Summary Report 6D31033G01."
30. WCAP-16776-P Revision 1, "Westinghouse SSPS Memory Board Replacement Summary Report 6D31035G01."

BIBLIOGRAPHY

Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Type Tests of Continuous-Duty Class 1 Motors Installed Inside the Containment of Nuclear Power Generating Stations," IEEE 334-1971.

FNP-FSAR-7

TABLE 7.2-1 (SHEET 1 OF 2)

LIST OF REACTOR TRIPS

<u>Reactor Trip</u>	<u>Coincidence Logic</u>	<u>Interlocks</u>	<u>Comments</u>
High neutron flux (power range)	2/4	Manual block of low setting permitted by P-10	High and low settings; manual block and automatic reset of low setting by P-10
Intermediate range neutron flux	1/2	Manual block permitted by P-10	Manual block and automatic reset
Source range neutron flux	1/2	Manual block permitted by P-6; interlocked with P-10	Manual block and automatic reset; automatic block above P-10; manual reset available below P-10
Power range high positive neutron flux rate	2/4	No interlocks	
Overtemperature ΔT	2/3	No interlocks	
Overpower ΔT	2/3	No interlocks	
Pressurizer low pressure	2/3	Interlocked with P-7	Blocked below P-7
Pressurizer high pressure	2/3	No interlocks	
Pressurizer high water level	2/3	Interlocked with P-7	Blocked below P-7
Reactor coolant low flow	2/3 per loop	Interlocked with P-7 and P-8	Low flow in one loop will cause a reactor trip when above P-8; low flow in two loops will cause a reactor trip when above P-7; blocked below P-7

FNP-FSAR-7

TABLE 7.2-1 (SHEET 2 OF 2)

<u>Reactor Trip</u>	<u>Coincidence Logic</u>	<u>Interlocks</u>	<u>Comments</u>
Reactor coolant pump bus undervoltage	2/3	Interlocked with P-7	Blocked below P-7
Reactor coolant pump bus underfrequency	2/3	Interlocked with P-7	Underfrequency on two buses will trip all reactor coolant pump breakers and cause reactor trip; reactor trip blocked below P-7
Steam generator low-low water level	2/3 per SG	No interlocks	Low-low level in any steam generator will cause a reactor trip.
Safety injection signal	Coincident with actuation of safety injection	No interlocks	(See section 7.3 for engineered safety features actuation conditions)
Turbine-generator trip			
Low auto stop pressure oil	2/3	Interlocked with P-9	Blocked below P-9
Turbine stop valve close	4/4	Interlocked with P-9	Blocked below P-9
Train general warning alarm	2/2	No Interlocks	One general warning alarm per train
Manual safety injection	1/2	No interlocks	Two momentary controls: operating either control will actuate both trains
Manual	1/2	No interlocks	

TABLE 7.2-2 (SHEET 1 OF 2)
PROTECTION SYSTEM INTERLOCKS

<u>Designation</u>	<u>Derivation</u>	<u>Function</u>
Power Escalation Permissives		
P-6	1/2 neutron flux (intermediate range) above setpoint	Allows manual block of source range reactor trip
	2/2 neutron flux (intermediate range) below setpoint	Defeats the block of source range reactor trip
P-10	2/4 neutron flux (power range) above setpoint	Allows manual block of power range (low setpoint) reactor trip
		Allows manual block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Blocks source range reactor trip (backup for P-6)
	3/4 neutron flux (power range) below setpoint	Defeats the block of power range (low setpoint) reactor trip
		Defeats the block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Input to P-7

TABLE 7.2-2 (SHEET 2 OF 2)

<u>Designation</u>	<u>Derivation</u>	<u>Function</u>	
Blocks of Reactor Trips			
P-7	3/4 neutron flux (power range) below below setpoint (from P-10)	Blocks reactor trip on: low flow in more than one loop, undervoltage, underfrequency, pressurizer low pressure, and pressurizer high level	
	and		
	2/2 turbine impulse chamber pressure below setpoint (from P-13)		
P-8	3/4 neutron flux (power range) below setpoint	Blocks reactor trip on low flow in a single loop	
P-9	3/4 neutron flux (power range) below setpoint	Blocks reactor trip on turbine trip	
P-13	2/2 turbine impulse chamber pressure below setpoint	Input to P-7	

FNP-FSAR-7

[HISTORICAL] [TABLE 7.2-3 (SHEET 1 OF 2)]

REACTOR TRIP SYSTEM INSTRUMENT ACCURACIES

<u>Reactor Trip Signal</u>	<u>Accuracy</u>	<u>Note</u>
Power range high neutron flux	± 1 percent of full power	
Intermediate range high neutron flux	± 5 percent of full scale	(a)
	± 1 percent of full scale from 10^{-4} to 10^{-3} amperes	(a)
Source range high neutron flux	± 5 percent of full scale	(a)
Power range high positive nuclear power rate	± 5 percent	(a)
Power range high negative nuclear power rate	± 5 percent	
Overtemperature ΔT	± 3.2 °F	(a)
Overpower ΔT	± 2.7 °F	
Pressurizer low pressure	± 18 psi	
Pressurizer high pressure	± 14 psi	
Pressurizer high water level	± 2.3 percent of full range ΔP between taps at design temperature and pressure	
Low reactor coolant flow	± 2.5 percent of full flow within range of 70 percent of 100 percent of full flow	(a)
Reactor coolant pump bus undervoltage	± 1 percent of relay set voltage	

FNP-FSAR-7

TABLE 7.2-3 (SHEET 2 OF 2)

<u>Reactor Trip Signal</u>	<u>Accuracy</u>	<u>Note</u>
Reactor coolant pump bus underfrequency	± 0.1 Hz	
Low-low steam generator water level	± 2.9 percent of ΔP signal over pressure range of 600 to 1100 psig (this does not include EA and PMA allowances)	

a. Reproducibility.]

TABLE 7.2-4 (SHEET 1 OF 3)**TRIP CORRELATION**

<u>Reactor Trip</u>		<u>Accident^(a)</u>
Source range, high flux	15.2.1	- Uncontrolled RCCA bank withdrawal from a subcritical condition (B)
	15.2.4	- Boron dilution (B)
	15.4.6	- Rod ejection (B)
Intermediate range, high flux	15.2.1	- Uncontrolled RCCA bank withdrawal from a subcritical condition (B)
	15.2.4	- Boron dilution (B)
	15.4.6	- Rod ejection (B)
Power range, high flux (low setpoint)	15.2.1	- Uncontrolled RCCA bank withdrawal from a subcritical condition (P)
	15.2.4	- Boron dilution (P)
	15.2.6	- Startup of an inactive reactor coolant loop (B)
	15.2.10	- Excessive heat removal due to feedwater system malfunction (B)
	15.2.11	- Excessive load increase (B)
	15.4.6	- Rod ejection (P)
Power range, high flux (high setpoint)	15.2.2	- Uncontrolled RCCA bank withdrawal at power (P)
	15.2.4	- Boron dilution (B)
	15.2.6	- Startup of an inactive reactor coolant loop (B)
	15.2.10	- Excessive heat removal due to feed-water system malfunction (B)
	15.2.11	- Excessive load increase (B)
	15.4.6	- Rod ejection (P)
Positive neutron flux rate	15.2.1	- Uncontrolled RCCA bank withdrawal from a subcritical condition (B)
	15.2.2	- Uncontrolled RCCA bank withdrawal at power (P)
	15.4.6	- Rod ejection (B)

a. (B/P) - Backup/Primary trip designation based on FSAR Chapter 15 analysis.

TABLE 7.2-4 (SHEET 2 OF 3)

<u>Reactor Trip</u>	<u>Accident</u>
Overpower ΔT	15.2.2 - Uncontrolled RCCA bank withdrawal at power (B) 15.2.4 - Boron dilution (B) 15.2.5 - Partial loss of forced reactor coolant system flow (B) 15.2.10 - Excessive heat removal due to feedwater system malfunction (B) 15.2.11 - Excessive load increase (B) 15.4.2 - Main steam line break (P - at power)
Overtemperature ΔT	15.2.2 - Uncontrolled RCCA bank withdrawal at power (P) 15.2.4 - Boron dilution (P) 15.2.5 - Partial loss of forced reactor coolant system flow (B) 15.2.7 - Loss of external electric load and/or turbine trip (P) 15.2.10 - Excessive heat removal due to feedwater system malfunction (B) 15.2.11 - Excessive load increase (B) 15.2.12 - Accidental depressurization of the reactor coolant system (P) 15.3.6 - Single RCCA withdrawal at power (P) 15.4.2 - Feedline break (B) 15.4.3 - Steam generator tube rupture (B)
Low primary coolant flow	15.2.5 - Partial loss of forced reactor coolant system flow (P) 15.3.4 - Complete loss of forced reactor coolant system flow (P) 15.4.4 - Single reactor coolant pump locked rotor (P)
Reactor coolant pump, under-frequency or undervoltage	15.3.4 - Complete loss of forced reactor coolant system flow (B)
Pressurizer high pressure	15.2.2 - Uncontrolled RCCA bank withdrawal at power (B) 15.2.7 - Loss of external electrical load and/or turbine trip (P)

TABLE 7.2-4 (SHEET 3 OF 3)

<u>Reactor Trip</u>	<u>Accident</u>
Pressurizer high water level	15.4.2 - Feedline break (B)
	15.4.4 - Single reactor coolant pump locked rotor (B)
	15.2.2 - Uncontrolled RCCA bank withdrawal at power (B)
	15.2.4 - Boron dilution (B)
	15.2.7 - Loss of external electrical load and/or turbine trip (B)
	15.2.8 - Loss of normal feedwater (B)
	15.2.9 - Loss of offsite power to the station auxiliaries (station blackout) (B)
	15.2.14 - Inadvertent operation of ECCS during power operation (B)
Pressurizer low pressure	15.4.2 - Feedline break (B)
	15.2.3 - RCCA misalignment (one or more dropped RCCAs) (B)
	15.2.11 - Excessive load increase (B)
	15.2.12 - Accidental depressurization of the reactor coolant system (B)
	15.2.14 - Inadvertent operation of ECCS during power operation (P)
	15.3.1 - Loss of reactor coolant from small ruptured pipes or from cracks in large pipes which actuate emergency core cooling system (small break LOCA) (P)
	15.4.2 - Main steam line break (B)
Low-low steam generator water level	15.4.3 - Steam generator tube rupture (P)
	15.2.7 - Loss of external electrical load and/or turbine trip (B)
	15.2.8 - Loss of normal feedwater (P)
	15.2.9 - Loss of offsite power to the station auxiliaries (station blackout) (P)
	15.4.2 - Feedline break (P)
Reactor trip from safety injection signal (low steam line pressure)	15.4.2 - Main steam line break (P - at power)

TABLE 7.2-5 (SHEET 1 OF 2)

REACTOR TRIP SYSTEM INSTRUMENTATION RESPONSE TIMES

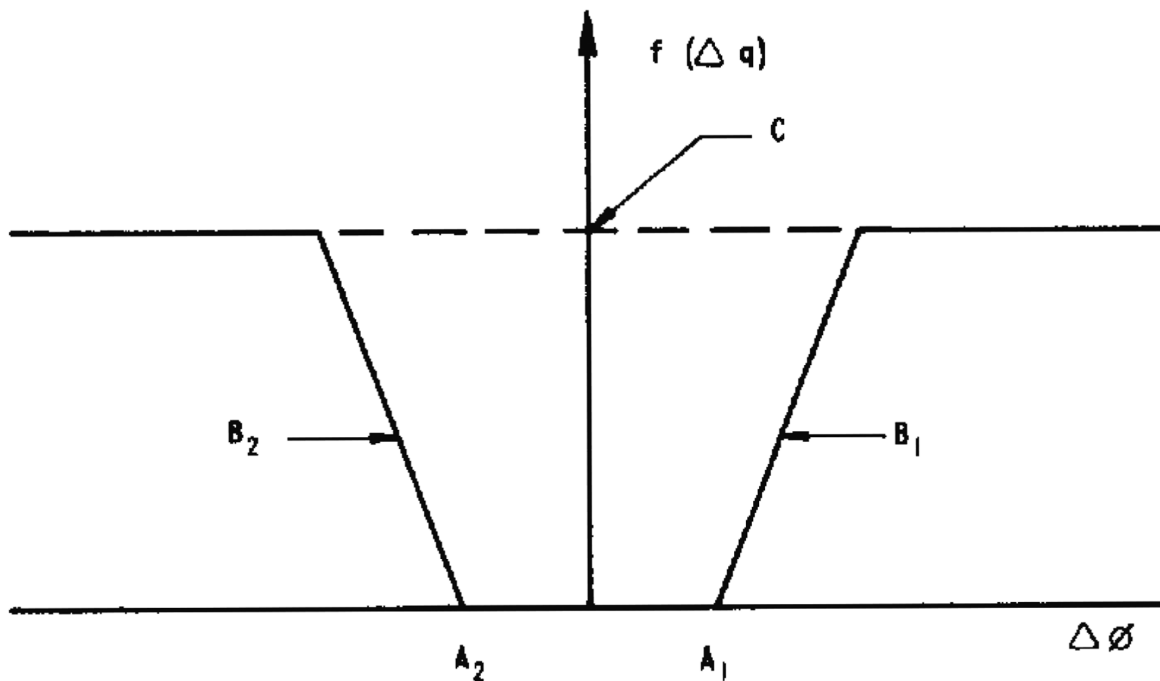
<u>Functional Unit</u>		<u>Response Time(s)</u>
1.	Manual reactor trip	NA
2.	Power range, neutron flux	
	a. High	$\leq 0.5^{(a)}$
	b. Low	$\leq 0.5^{(a)}$
3.	Power range, neutron flux, high positive rate	$\leq 0.65^{(a)}$
4.	Not used.	
5.	Intermediate range, neutron flux	NA
6.	Source range, neutron flux	NA
7.	Overtemperature ΔT	$\leq^{(a)(b)(c)}$
8.	Overpower ΔT	$\leq^{(b)(c)}$
9.	Pressurizer pressure-low	≤ 2.0
10.	Pressurizer pressure-high	≤ 1.0
11.	Pressurizer water level-high	NA
12A.	Loss of flow-single loop (above P-8)	≤ 1.0
12B.	Loss of flow-two loops (above P-7 and below P-8)	≤ 1.0
13.	Steam generator water level-low-low	≤ 2.0
14.	Undervoltage-reactor coolant pumps	NA
15.	Underfrequency-reactor coolant pumps	NA
16.	Turbine trip	
	a. Low auto stop oil pressure	NA
	b. Turbine throttle valve closure	NA
17.	Safety injection input from ESF	NA

TABLE 7.2-5 (SHEET 2 OF 2)

<u>Functional Unit</u>	<u>Response Time(s)</u>
18. Reactor trip system interlocks	NA
19. Reactor trip breakers	NA
20. Automatic trip logic	NA

- a. Neutron detectors are exempt from response time testing. Response time of the neutron flux signal portion of the channel shall be measured from detector output or input of first electronic component in channel.
- b. RTD response time ≤ 5.0 s
- The RTD response time cannot be summed with the channel response times listed in Note (c).
- c. The following are the required RTS channel response times (encompassing channel electronics/trip logic & breaker/gripper release) for an RTD response time of no greater than 5.0 seconds:
1. Overtemperature ΔT , T_{avg} input: ≤ 2.435 s
 2. Overtemperature ΔT , pressurizer pressure input (including sensor): ≤ 2.0 s
 3. Overtemperature ΔT , nuclear flux input: ≤ 2.0 s
 4. Overpower ΔT , T_{avg} input: ≤ 2.159 s
 5. ΔT input (to both OT ΔT and OP ΔT): ≤ 6.159 s

T_{avg} and ΔT response times include the effect of all transfer functions set to the recommended values.



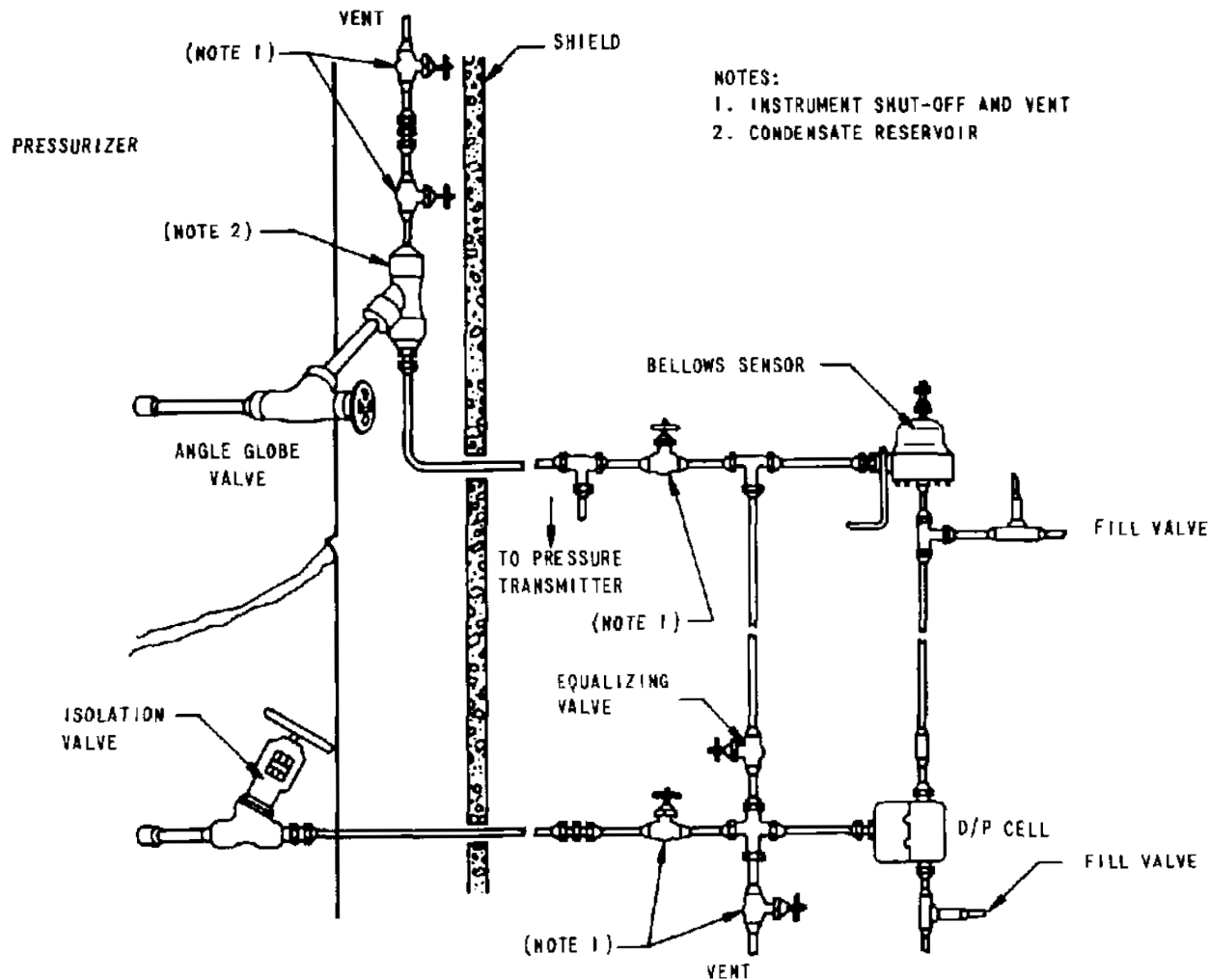
$\Delta \phi$ - NEUTRON FLUX DIFFERENCE BETWEEN UPPER AND LOWER LONG ION CHAMBERS

A_1, A_2 - LIMIT OF $f(\Delta \phi)$ DEADBAND

B_1, B_2 - SLOPE OF RAMP; DETERMINES RATE AT WHICH FUNCTION REACHES IT'S MAXIMUM VALUE ONCE DEADBAND IS EXCEEDED

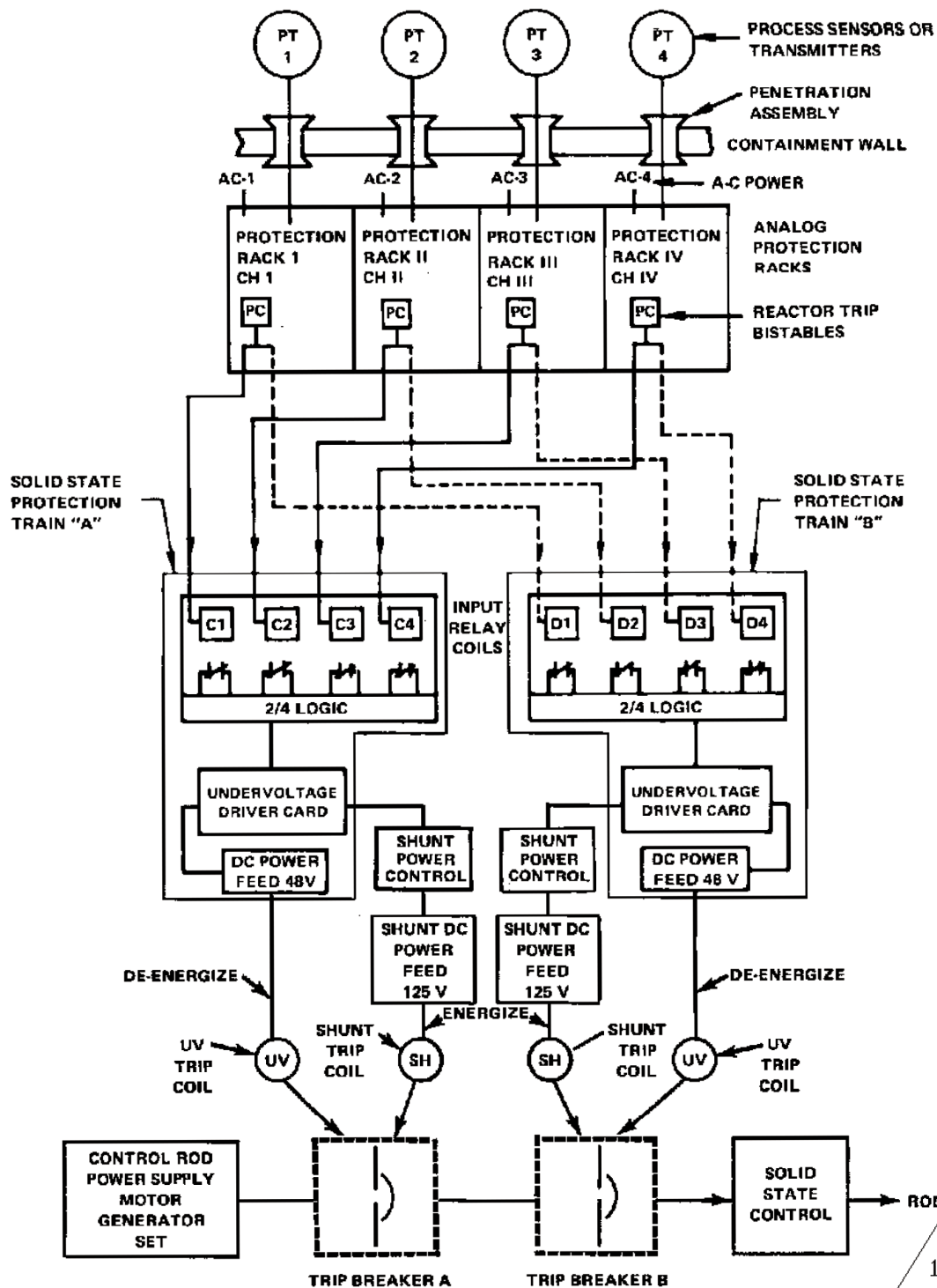
C - MAGNITUDE OF MAXIMUM VALUE THE FUNCTION MAY ATTAIN

REV 21 5/08



13

REV 21 5/08



REV 21 5/08

7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

7.3.1 DESCRIPTION

The engineered safety features actuation system (ESFAS) senses selected plant parameters, determines whether or not predetermined safety limits are being exceeded, and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Class III or IV faults). Once the required logic combination is completed, the system sends actuation signals to those engineered safety features (ESF) components whose aggregate function best serves the requirements of the accident. This design meets the requirements of General Design Criteria (GDC) 13 and 20.

7.3.1.1 System Description

The ESFAS is a functionally defined system described in this section. The equipment which provides the actuation functions identified in table 7.3-1 is listed below and discussed in this section and the referenced WCAPs:

- A. Process instrumentation and control system.⁽¹⁾
- B. Solid-state logic protection system.^(2, 16, 17, 18, 19, 20, 21, 22, 23, & 24)
- C. ESF test cabinet.⁽³⁾
- D. Manual actuation circuit.

The following is a summary of those generating station conditions requiring protective action. (See appropriate sections of chapter 15 for discussion.)

- A. Primary system:
 - 1. Rupture in small pipes or cracks in large pipes.
 - 2. Rupture of a reactor coolant pipe (loss-of-coolant accident (LOCA)).
 - 3. Steam generator tube rupture.
- B. Secondary system:
 - 1. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief, or safety valve.
 - 2. Rupture of a major steam pipe.

The following summarizes the generating station variables required to be monitored for each accident:

FNP-FSAR-7

- A. Ruptures in small pipes or cracks in large primary system pipes:
 - 1. Pressurizer pressure.
 - 2. Pressurizer water level.
 - 3. Containment pressure.
- B. Rupture of a reactor coolant pipe (LOCA):
 - 1. Pressurizer pressure.
 - 2. Pressurizer water level.
 - 3. Containment pressure.
- C. Steam generator tube rupture:
 - 1. Pressurizer pressure.
 - 2. Pressurizer water level.
- D. Minor secondary system pipe breaks:
 - 1. Pressurizer pressure.
 - 2. Pressurizer water level.
 - 3. Steam line pressures.
 - 4. Steam line differential pressures.
 - 5. Steam flows.
 - 6. Reactor coolant average temperatures (T_{avg}).
 - 7. Containment pressure.
- E. Rupture of a major steam pipe (same as D above).

7.3.1.1.1 Signal Computation

The ESFAS consists of two discrete portions of circuitry: an analog portion consisting of redundant channels which monitor various plant parameters such as the reactor coolant system and steam system pressures, temperatures and flows, and containment pressures; and a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and perform the needed logic to actuate the ESF. Each digital train is capable of

actuating the ESF equipment required. The intent is that any single failure within the ESFAS shall not prevent system action when required.

The redundant concept is applied to both the analog and logic portions of the system. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment vessel penetration, and analog protection cabinets, terminating at the redundant groups of safeguards logic racks. This design meets the requirements of 1971 GDC 21.

Section 7.2 provides further details on protective instrumentation. The same design philosophy applies to both systems and meets the requirements of 1971 GDC 20, 21, 22, 23, and 24.

The variables are sensed by the analog circuitry as discussed in reference 1 and in section 7.2. The outputs from the analog channels are combined into actuation logic as shown in drawings U-166235, U-166236, U-166237, and U-166238. Tables 7.3-2 and 7.3-3 give additional information pertaining to logic and function.

The interlocks associated with the ESFAS are outlined in table 7.3-4. These interlocks satisfy the functional requirements discussed in subsection 7.1.2. The control functions of the interlocks are outlined in table 7.7-1.

Manual controls are also provided to switch from the injection to the recirculation phase after a LOCA.

Actions which the ESFAS initiates when it is called on to perform its function are listed in table 7.3-1.

7.3.1.1.2 Implementation of Functional Design

A. Analog Circuitry

The process analog sensors and racks for the ESFAS are covered in reference 1. Discussed in reference 1 are the parameters to be measured including pressures, flows, tank and vessel water levels, and temperatures, as well as the measurement and signal transmission considerations. These latter considerations include the basic current transmission system, transmitters, orifices and flow elements, and resistance temperature detectors. Other considerations covered are automatic calculations, signal conditioning, and location and mounting of the devices.

The sensors monitoring the primary system are located as shown in the piping flow diagrams in chapter 5. The secondary system sensor locations are shown in the steam system flow diagrams given in chapter 10.

Containment pressure is sensed by four physically separated pressure transmitters mounted by strong supports outside of the containment, which are connected to containment atmosphere by a filled and sealed hydraulic transmission system similar to the sealed pressurizer water level reference leg. The distance from

penetration to transmitter is kept to a minimum, and separation is maintained. This arrangement, together with the pressure sensors external to the containment, forms a double barrier and conforms to 1971 GDC 56 and Regulatory Guide 1.11.

The following is a description of those process channels not included in the reactor trip system or ESFAS which enable additional monitoring of in-containment conditions in the post-LOCA recovery period. These channels are located outside of the containment (with the exception of sump instrumentation) and will not be affected by the accidents.

1. Refueling Water Storage Tank Level

Level instrumentation on the refueling water storage tank consists of two channels. One channel indicates in the main control room and alarms on high, Technical Specification minimum, low, and low-low water levels. The other channel indicates in the main control room and alarms on low and low-low water levels.

2. High-Head Safety Injection Pumps Discharge Pressure

These channels clearly show that the safety injection pumps are operating. The high-head safety injection pump motor power feed breakers indicate that they have closed by energizing indicating lights on the control board. The transmitters of the high-head safety injection pumps discharge pressure are outside containment.

3. Valve Position

All ESF remote-operated valves have position indication on the control board in two places to show proper positioning of the valves. Red and green indicator lights are located next to the manual control station showing open and closed positions. For automatically actuated valves, monitor lights are provided for verification of valve position following the initiation of ESF actuation signals including safety injection, phase A or B isolation, or loss of offsite power. These monitor lights thus enable the operator to assess quickly the status of the automatic actuation. These indications are derived from contacts integral to the valve operators. In the cases of the accumulator isolation valves, redundancy of position indication is provided by valve stem-mounted limit switches which actuate annunciators on the control board when the valves are not correctly positioned for ESF actuation. The stem-mounted switches are independent of the limit switches in the motor operators. See section 7.6 for additional information.

4. Containment Air Coolers

The exit temperature of the containment air coolers cooling water discharge is indicated in the control room. Additionally, the radiation level of the

FNP-FSAR-7

cooling water from the containment air coolers is monitored by two radiation monitor units. One unit is installed in each of two independent flow trains.

In addition to the above containment coolers instrumentation, the following local instrumentation is available:

- a. Residual heat exchanger exit temperatures (indication also provided in the control room). The indication of the residual heat removal pumps discharge pressure is provided in the control room.
- b. Safety injection test line pressure and flow.

5. Sump Instrumentation

The containment level indicator consists of two displacement type level transmitters with indication in the control room. The transmitter for each unit will be located above possible flood level and is designed to operate for 3 h in a postaccident environment.

B. Digital Circuitry

The ESF logic racks are discussed in detail in references 2, 16, 17, 18, 19, 20, 21, 22, 23, and 24. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 2 also covers certain aspects of online test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separation, and provisions for ensuring instrument qualification. The outputs from the analog channels are combined into actuation logic as shown in drawing U-166235 (T_{avg}), drawing U-166236 (pressurizer pressure and water level), drawing U-166237 (steam flow, pressure, and differential pressure), and drawing U-166238 (ESF actuation).

To facilitate ESF actuation testing, two cabinets (one per train) are provided which enable operation to the maximum practical extent of safety features loads on a group-by-group basis until actuation of all devices has been checked. Final actuation testing is discussed in detail in subsection 7.3.2.

7.3.1.1.3 Final Actuation Circuitry

The outputs of the solid-state logic protection system, i.e., the slave relays, are energized to actuate. The functions that are initiated by the ESFAS are listed in table 7.3-1.

If an accident is assumed to occur coincident with a loss of offsite electrical power (blackout), the ESF loads are sequenced onto the diesel generators to prevent overloading them. This sequence is discussed in paragraph 8.3.1.1.7. The design meets the requirements of 1971 GDC 35.

7.3.1.2 Design Bases

Refer to Institute of Electrical and Electronics Engineers (IEEE) 279-1971.⁽⁴⁾

The generating station conditions which require protective action are given in paragraph 7.3.1.1. The generating station variables that are required to be monitored in order to provide protective actions are also summarized in paragraph 7.3.1.1.

The only variable sensed by the ESFAS which has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by using three narrow range fast response resistance temperature detectors (RTDs) installed radially 120 degrees apart in the RCS hot leg piping. These RTDs extend into the RCS fluid, sensing the temperature in three distinct locations within the hot leg. The signal from these RTDs is electronically averaged by the process instrumentation and control system to provide a representative T_{hot} indication. Fast response RTDs, one each, are also installed in the three RCS cold legs. The measurements from the hot and cold leg RTDs provide the required inputs to the process instrumentation and controls system for delta T and T average signals.

The parameter values that will require protective action are given in the plant Technical Specifications.

The malfunctions, accidents, or other unusual events which could physically damage protection system components or could cause environmental changes are LOCA, steam breaks, earthquakes, fire, explosion (hydrogen buildup inside containment), missiles, and flood.

The design requirements are as follows:

A. System Response Times

The time delays are defined as the time required for the desired action (such as ESF sequence actuation) to be initiated following a step change in the variable being monitored from 5 percent below to 5 percent above the trip setpoint. The times typically include sensor delay, and include analog and logic delay (with all externally adjustable transfer functions and all externally adjustable time delays set to the value to be used for operation), and final actuator delay (e.g., breaker opening or closing) but do not include the time required for the actuated device to operate (e.g., pump starting time).

Time response data on the protection systems are obtained during the startup test program, and appropriate sections are repeated as required by Technical Specifications. These procedures require that simulated signals be introduced as analog inputs for partial testing of protection channels, since a complete check, including the sensors, is not practical. Validity of time response values assigned to sensors is considered to be established by channel comparison during normal plant operation, on the basis that deterioration of time response characteristics of sensors will be observable by comparison of oscillations on associated readouts that will clearly indicate a "slow" transmitter. Response times for the solid-state protection system are routinely verified during periodic testing of the logic channels as required by the Technical Specifications.

FNP-FSAR-7

Maximum allowable time delays in generating the engineered safety feature signals are as follows:

	<u>Time (s)</u>
1. Pressurizer pressure – low	2.0
2. Steam line differential pressure - high	2.0
3. Steam line flow – high (assume other signals present)	2.0
4. Steam line pressure low	2.0
5. RCS T_{avg} - low-low (assume other signals present)	(a), (b)
6. Steam generator water level - high-high	2.0
7. Containment pressure - high	2.0
8. Containment pressure - high-high	2.0
9. Containment pressure - high-high-high	2.0
10. Actuation signals for auxiliary feedwater pumps	2.0

Notes:

- (a) RTD response time ≤ 5.0 s

The RTD response time cannot be summed with the channel response times listed in Note (b).

- (b) The following are the required ESFAS channel response times (encompassing channel electronics from input to instrumentation racks until signal reaches the isolation valves) for an RTD response time of no greater than 5.0 s:

Steamline Isolation T_{avg} input: ≤ 6.159 s

FNP-FSAR-7

B. Accuracies

Historical basis for ESF accuracies is given below. The total channel statistical accuracy for ESF actuation signals is provided in WCAP⁽¹³⁾.

<u>ESF Signals</u>	<u>Accuracy</u>
Pressurizer pressure	± 14 psi
Steam line differential pressure	± 3 percent of span
Steam flow	± 4.5 percent of maximum guarantee flow over pressure range (600 to 1100 psig)
Steam line pressure	± 4 percent of span
RCS T_{avg}	$\pm 2^{\circ}F$
Steam generator water level	± 2.25 percent of narrow range span over pressure range (600 to 1100 psig)
Containment pressure	± 1.8 percent of full scale

***[HISTORICAL]** Actuation signal accuracies required for generating the required actuation signals for loss of coolant protection are as follows:*

<i>Pressurizer pressure (uncompensated)</i>	<i>± 14 psi</i>
---	--------------------------------

Actuation signal accuracies required in generating the required actuation signals for steam break protection are given:

- | | |
|--------------------------------|---|
| <i>1. Steam line pressure</i> | <i>± 4 percent</i> |
| <i>2. Steam flow signals</i> | <i>4.5 percent of maximum guarantee flow over pressure range (600 to 1100 psig)</i> |
| <i>3. T_{avg}</i> | <i>$\pm 2^{\circ}F$</i> |

FNP-FSAR-7

4. *Containment pressure* *±1.8 percent signal of full scale]*

C. Ranges

Ranges of sensed variables to be accommodated until conclusion of protective action is ensured.

Instrument ranges required in generating the ESF actuation signals are:

- | | |
|-------------------------------------|---|
| 1. Pressurizer pressure | 1700 to 2500 psig |
| 2. Steam line differential pressure | 0 to differential pressure for 122.7 percent rated steam flow |
| 3. Steam line pressure | 0 to 1200 psig |
| 4. Steam line flow | 0 to 122.7 percent rated steam flow |
| 5. RCS T _{avg} | 530°F to 630°F |
| 6. Steam generator water level | 0 to 100 percent narrow range span |
| 7. Containment pressure | -5 to 65 psig |

7.3.1.3 Final System Drawings

The functional diagrams for the ESFAS for Units 1 and 2 are shown in functional logic diagrams U-166236 through U-166238 and U-166243 through U-166245. See subsection 7.1.3 and table 7.1-1 for a list of supplemental drawings.

7.3.2 ANALYSIS

A failure mode and effects analysis (see tables 7.3-6 through 7.3-15) for the ESFAS, train A, is presented in table 7.3-15 with listed components identified in figure 7.3-1. Any single failure in train A will not prevent ESF actuation by train B.

Failure analysis of pumps, valves, and heat exchangers of ESF systems is presented in the following sections:

FNP-FSAR-7

- A. Service water system - table 9.2-3.
- B. Component cooling water system - table 9.2-11.
- C. Control room air conditioning and filtration system - table 9.4-3.
- D. Penetration room filtration system - table 6.2-18.
- E. Auxiliary feedwater system - table 6.5-2.
- F. Emergency safety features pump room cooling system - table 9.4-7.
- G. Battery room ventilation system - table 9.4-7.
- H. Battery charging room air conditioning system – table 9.4-7.
- I. Emergency diesel generator systems - table 7.3-14.
- J. Emergency core cooling system (ECCS) - tables 6.3-6 and 6.3-8.

Failure mode and effects analysis for active failures of the actuating circuits of the above listed systems are found in tables 7.3-6 through 7.3-14. All drawings, except elementary drawings, that are referenced in the various tables are found in the indicated sections of the FSAR. Elementary drawings were provided to the NRC in a supplement entitled, "Safety Related Schematic Diagrams and Location Drawings, November 1973," as discussed in subsection 7.1.3.

7.3.2.1 Evaluation of Compliance with IEEE 279-1971

7.3.2.1.1 Single Failure Criteria

The discussion presented in paragraph 7.2.2.2.1 is applicable to the ESFAS, with the following exception.

In the ESF, a loss of instrument power will call for actuation of ESF equipment controlled by the specific bistable that lost power (containment spray and RWST low-low level excepted). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in chapter 8. For containment spray, the final bistables are energized to trip to avoid spurious actuation. In addition, manual containment spray requires simultaneous actuation of both manual controls. This is considered acceptable because spray actuation on high-high-high containment pressure signal provides automatic initiation of the system via protection channels meeting the criteria of IEEE 279-1971.⁽⁴⁾ Moreover, all containment spray safety-related equipment (valve and pumps) can be individually, manually actuated from the control board. Hence, a secondary mode of containment spray initiation is available. Likewise, the RWST low-low level signal is an energize-to-actuate function whose protection channels meet the criteria of IEEE 279-1971. This design reduces the chance of a spurious alignment of the containment sump to the RHR pump suction when this function is not desired to occur, thus preventing RHR pump

damage due to less than adequate water level in the containment sump. Additionally, the recirculation mode can be aligned from the main control board which is the primary method for switchover from injection mode to recirculation mode. The design meets the requirements of GDC 21 and 23. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 279-1971 for separation of circuits, which are located by necessity in non-category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

7.3.2.1.2 Equipment Qualification

The ability of ESF equipment inside containment which is required for post-LOCA operation to function in the adverse environment associated with the LOCA or in-containment steam break has been evaluated in reference 5 and section 3.11.

7.3.2.1.3 Channel Independence

The discussion presented in paragraph 7.2.2.2.1 is applicable. The ESF outputs from the solid-state logic protection cabinets are redundant, and the actuations associated with each train are energized up to and including the final actuators by the separate ac power supplies which power the logic trains. Some exceptions are taken in the specific application of certain design requirements contained in IEEE 279-1971 for separation of circuits, which are located by necessity in non-category 1 structures. The auto stop oil pressure and throttle valve position inputs are designed as close as reasonably achievable to the 1E requirements. The intent of the design requirements is met in that the system functional requirements are not impaired by these circuits.

7.3.2.1.4 Control and Protection System Interaction

The discussions presented in paragraph 7.2.2.2.1 are applicable.

7.3.2.1.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in paragraph 7.2.2.2.1 are applicable to the sensors, analog circuitry, and logic trains of the ESFAS.

The following discussions cover those areas in which the testing provisions differ from those for the reactor trip system.

7.3.2.1.5.1 Testing of Engineered Safety Features Systems. The ESF systems are tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident. ESF test cabinets are discussed in WCAP-7705.⁽³⁾ The testing program, which meets the requirements of 1971 GDC 21, 37, 40, and 43 of Regulatory Guide 1.22, is as follows:

- A. Prior to initial plant operations, ESF system tests were conducted.
- B. Subsequent to initial startup, the minimum frequency and type of surveillance for ESF system tests will be as specified in Technical Specifications.
- C. During refueling or online operation of the reactor, the ESF analog and logic circuitry will be fully tested. In addition, most of the ESF final actuators will be fully tested, with some of the tests performed while on line and others performed during Integrated Safeguards testing. The remaining few final actuators whose operation is not compatible with continued online plant operation will be checked by means of continuity testing.
- D. During normal operation, the operability of testable final actuation devices of the ESF systems will be tested by manual initiation from the control room.

7.3.2.1.5.2 Performance Test Acceptability Standard for the "S" and "T" (Safety Injection and Phase A Isolation) and for the "P" (Automatic Demand Signal for Containment Spray and Phase B Isolation) Actuation Signals Generation. During reactor operation and/or refueling the basis for ESFAS acceptability will be the successful completion of the overlapping tests performed on the initiating system and the ESFAS. Checks of process indications verify operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits through the logic input relays and including the input of the logic cards. Solid-state logic testing checks the digital signal path from the logic card inputs through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays. Final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation. Most can be tested at power without causing plant upset. However, to minimize the potential for plant upset and unnecessary challenges to plant equipment, most slave relays are tested during refueling. A continuity check can be performed on the actuators of the untestable devices at power as discussed later. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves have completed their travel.

The basis for acceptability for the ESF interlocks will be control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint.

Maintenance checks, such as resistance to ground of signal cables in radiation environments, are based on qualification test data which identify what constitutes acceptable radiation (thermal, etc.) degradation. The maintenance requirements and implementation schedule will be incorporated into the environmental qualification administrative program.

7.3.2.1.5.3 Frequency of Performance of Engineered Safety Features Actuation Tests.

During reactor operation, complete system testing (excluding sensors and slave relays or those devices whose operation would cause plant upset) is performed as described in Technical Specifications. Testing, including the sensors and slave relays, is also performed during scheduled plant shutdown for refueling.

7.3.2.1.5.4 Engineered Safety Features Actuation Test Description. The following sections describe the testing circuitry and procedures for the online portion of the testing program. The guidelines used in developing the circuitry and procedures are:

- A. The test procedures must not involve the potential for damage to any plant equipment.
- B. The test procedures must minimize the potential for accidental tripping.
- C. The provisions for online testing must minimize complication of ESF actuation circuits so that their reliability is not degraded.

7.3.2.1.5.5 Description of Initiation Circuitry. Since several fluid systems comprise the total ESF, each of which may be initiated by different process conditions and reset independently of each other, separate initiating circuits exist in each of the two trains of the ESF actuation circuitry. The specific functions which rely on the ESFAS are listed in table 7.3-1.

The output of each of the initiation circuits consists of a master relay which drives slave relays for contact multiplication as required. The logic, master, and slave relays are mounted in the solid-state logic protection cabinets designated train A and train B, respectively, for the redundant counterparts. The master and slave relay circuits operate various pump and fan circuit breakers or starters, motor-operated valve starters, solenoid-operated valves, emergency generator starting, etc.

7.3.2.1.5.6 Analog Testing. Analog testing is identical to that used for reactor trip circuitry and is described in paragraphs 7.2.2.2.1.F and 7.2.3.3. Briefly, in the analog racks, proving lamps and analog test switches are provided. Administrative control requires, during bistable testing, that the bistable output be put in a trip condition by placing the test switch in the test position. This action connects the proving lamp to the bistable output and disconnects the output of the bistable to the solid-state protection cabinets, thus deenergizing (operating) the input relays in train A and train B cabinets, and allows injection of a test signal to the channel. Relay logic in the process cabinets automatically blocks the test signal. This, of necessity, is done on one channel at a time. Status lights and single-channel trip alarms in the main control room confirm that the bistable relays have been deenergized and that the bistable outputs are in the trip mode. An exception to this is containment spray, which is energized to actuate two-out-of-four coincidence logic and reverts to two-out-of-three when one channel is in test. A signal is then inserted through a test jack. Verification of the bistable trip setting is now confirmed by the proving lamp.

7.3.2.1.5.7 Solid-State Logic Testing. After the individual channel analog testing is complete, the logic matrices are tested from the train A and train B logic rack test panels. This step provides overlap between the analog and logic portions of the test program. During this test, each of the logic inputs are actuated automatically in all combinations of trip and nontrip logic. Trip logic is not maintained sufficiently long enough to permit master relay actuation; master relays are "pulsed" in order to check continuity.

Following the logic testing, the individual master relays are actuated electrically to test their mechanical operation. Actuation of the master relays during this test will apply low voltage to the slave relay coil circuits to allow continuity checking but not slave relay actuation. During logic testing of one train, the other train can initiate the required ESF function. For additional details, see reference 2.

7.3.2.1.5.8 Actuator Testing. At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. Slave relays do not operate because of reduced voltage.

In the next step, operation of the slave relays and the devices controlled by their contacts will be checked. For this procedure, control switches mounted on a safeguards test cabinet panel in the logic rack area are provided for each slave relay. These controls are of the type that require two deliberate actions on the part of the operator to actuate a slave relay. By operation of these relays one at a time through the control switches, all devices that can be operated on line are tested. Devices are assigned to the slave relays such that no undesired effect on plant operation occurs. This procedure minimizes upset to the plant and again ensures that overlap in the testing is continuous, since the normal power supply for the slave relays is utilized.

During this last procedure, close communication between the main control room operator and the man at the test panel is required. Prior to the energizing of a slave relay, the operator in the main control room ensures that plant conditions will permit operation of the equipment that will be actuated by the relay. After the tester has energized the slave relay, the main control room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps, and annunciators in the control board and, using a prepared checklist, records all operations. He then resets all devices and prepares for operation of the next slave relay actuated equipment.

Exceptions to online testability and a discussion of Regulatory Guide 1.22 are given in paragraph 7.1.2.8. While the FNP ESFAS hardware (SSPS and STC) is designed to accommodate online testing, slave relay testing will normally be conducted during refueling. The surveillance period for slave relays is based on reference 12.

7.3.2.1.5.9 Actuator Blocking and Continuity Test Circuits. The limited number of components that cannot be operated online are discussed above. For these components, additional blocking relays are provided which allow operation of the slave relays without actuation of the associated ESF devices. Interlocking prevents blocking the output of more than one slave relay at a time. The circuits provide for monitoring of the slave relay contacts, the devices' control circuit cabling, control voltage, and the devices' actuating solenoids. The slave relays associated with these final ESF devices may be tested online utilizing the STC circuitry or during refueling.

7.3.2.1.5.10 Time Required for Testing. It is estimated that analog testing can be performed at a rate of several channels per hour. Logic testing can be performed in < 30 min. Testing of actuated components (including those which can only be partially tested) will be a function of control room operator availability. When performed online, it is expected to require several shifts to accomplish these tests. During this procedure automatic actuation circuitry will override testing, except for

those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time the redundant devices in the other trains would be functional. When slave relay testing is performed during shutdown, fewer constraints are imposed on plant operators.

7.3.2.1.5.11 Summary. The procedures described provide capability for checking completely from the process signal to the logic cabinets and from there to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc., including all field cabling actually used in the circuitry called upon to operate for an accident condition. For those few devices whose operation could seriously affect plant or equipment operation, the same procedure provides for checking from the process signal to the logic rack. To check the final actuation device, a continuity test of the individual control circuits is performed.

The procedures require testing at various locations.

- A. Analog testing and verification of bistable setpoint are accomplished at process analog racks. Verification of bistable relay operation is done at the main control room status lights.
- B. Logic testing through operation of the master relays and low voltage application to slave relays is done at the logic rack test panel.
- C. Testing of pumps, fans, and valves is done at a test panel located in the vicinity of the logic racks in combination with the control room operator.
- D. Continuity testing for those circuits that cannot be operated is done at the same test panel mentioned in item C above.

7.3.2.1.5.12 Testing During Shutdown. ECCS tests will be performed at each major fuel reloading. With the reactor coolant system pressure ≤ 350 psig and temperature $\leq 350^\circ\text{F}$, a test safety injection signal will be applied to initiate operation of the system. This safety injection and residual heat removal pumps are made inoperable for this test. The test will be performed on an 18 month staggered test basis on one train each outage.

Containment spray system tests will be performed at each major fuel reloading. The tests will be performed with the flow directed through the containment spray system test line into the refueling canal and the spray additive tank blocked closed. The tests will be initiated by tripping the normal actuation instrumentation.

7.3.2.1.5.13 Periodic Maintenance Inspections. The maintenance procedures that follow may be accomplished in any order. The frequency will depend on the operating conditions and requirements of the reactor power plant. If any degradation of equipment operation is noted, either mechanically or electrically, remedial action is taken to repair, replace, or readjust the equipment.

Typical maintenance procedures include the following:

- A. Check cleanliness of all exterior and interior surfaces.
- B. Check all fuses for corrosion.
- C. Inspect for loose or broken control knobs and burned out indicator lamps.
- D. Inspect for rust, moisture, and condition of cables and wiring.
- E. Mechanically check all connectors and terminal boards for looseness, poor connection, or corrosion.
- F. Inspect the components of each assembly for signs of overheating or component deterioration.
- G. Perform complete system operating check.

The balance of the requirements listed in reference 4, IEEE-279, paragraphs 4.11 through 4.22, are discussed in paragraph 7.2.2.2.1. Paragraph 4.20 receives special attention in section 7.5.

7.3.2.2 Evaluation of Compliance with IEEE 308-1971

See section 7.6 and chapter 8, which discuss the power supply for the protection systems, for discussions on compliance with IEEE 308-1971.⁽⁶⁾

7.3.2.3 Evaluation of Compliance with IEEE 323-1971

The instrumentation associated with ESF equipment is type tested to substantiate the adequacy of design. This is the preferred method as indicated in IEEE 323-1971.⁽⁷⁾ Documentation of type testing is in possession of the manufacturers and may not be in the form given in this standard.

7.3.2.4 Evaluation of Compliance with IEEE 334-1971

The only continuous duty, in-containment Class 1 motors are containment fan coolers, which have been tested in the manner set forth in IEEE 334-1971.⁽⁸⁾

7.3.2.5 Evaluation of Compliance with IEEE 338-1971

The periodic testing of the ESFAS conforms to the requirements of IEEE 338-1971⁽⁹⁾ with the following comments:

- A. The response time was checked during preoperational testing and is periodically tested as described in the Technical Specifications.

- B. The reliability goals specified in paragraph 4.2 of IEEE 338-1971 are developed for FNP and described in the Technical Specifications.
- C. The periodic test frequency discussed in paragraph 4.3 of IEEE 338-1971 and specified in the plant Technical Specifications is conservatively selected to ensure that equipment associated with protective functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the test frequency is accelerated to accommodate the situation until the marginal performance is resolved.
- D. The test interval discussed in paragraph 5.2 of IEEE 338-1971 is developed primarily on past operating experience and modified, if necessary, to ensure that system and subsystem protection is reliably provided. Analytical methods for determining reliability are not used to determine test interval.

7.3.2.6 Evaluation of Compliance with IEEE 344-1971

The seismic testing, as set forth in paragraph 7.2.1.10, IEEE 338-1971,⁽⁹⁾ IEEE 344-1971,⁽¹⁰⁾ WCAP-7706,⁽¹¹⁾ and WCAP-7705,⁽³⁾ conforms to the guidelines set forth in IEEE 344-1971.⁽¹⁰⁾

7.3.2.7 Response Time Testing

Response time testing consists of any series of sequential, overlapping, or total channel test measurements provided that such tests demonstrate the total channel response time as defined in the Technical Specifications. Sensor response time verification may be demonstrated by either 1) in-place, onsite, or offsite test measurements or 2) utilizing replacement sensors with certified response times. The test results must be compared to properly defined acceptance criteria. In lieu of testing, bounding response time allocations may be used for selected protection system sensor and signal processing channel and actuation logic components. The technical basis and methodology for verifying ESF response time criteria using a combination of test data and bounding sensor and/or component response time allocations is provided in references 14 and 15. The measurement/verification of response time at the specified frequencies provides assurance that the reactor trip associated with each channel is completed within the time limit assumed in the accident analyses. The response time limits assumed in the safety analyses for the ESFAS are provided in table 7.3-16.

7.3.2.8 Further Considerations

In addition to the considerations given above, a loss of instrument air or loss of component cooling water to vital equipment has been considered. Assuming no other accident conditions, neither cause safety limits, as given in the Technical Specifications, to be exceeded. Likewise, loss of either one of the two will not adversely affect the core or the reactor coolant system, nor will it prevent an orderly shutdown if this is necessary. Furthermore, all pneumatically operated valves and controls will assume a preferred operating position upon loss of instrument air. It is also noted that, for conservatism during the accident analyses (chapter 15), credit is not taken for the instrument air systems nor any control system benefit.

7.3.2.9 Summary

The effectiveness of the ESFAS is evaluated in chapter 15, based upon the ability of the system to contain the effects of Condition III and IV faults, including LOCAs and steam break accidents. The ESFAS parameters are based upon the component performance specifications which are given by the manufacturer or verified by test for each component. Appropriate factors to account for uncertainties in the data are factored into the constants characterizing the system.

The ESFAS must detect Condition III and IV faults and generate signals which actuate the ESF. The system must sense the accident condition and generate the signal actuating the protective function reliably and within a time determined by and consistent with the accident analyses in chapter 15.

Much longer times are associated with the actuation of the mechanical and fluid system equipment associated with ESF. This includes the time required for switching and bringing pumps and other equipment to speed and the time required for them to take load.

Operating procedures require that the complete ESFAS normally be operable. However, redundancy of system components is such that the system operability assumed for the safety analyses can still be met with certain instrumentation channels out of service. Channels that are out of service are to be placed in the tripped mode or bypass mode in the case of containment spray.

7.3.2.9.1 Loss of Coolant Protection

By analysis of a LOCA, it has been verified that except for very small coolant system breaks which can be protected against by the charging pumps followed by an orderly shutdown, the effects of various LOCAs are reliably detected by the low pressurizer pressure signal; the ECCS is actuated in time to prevent or limit core damage.

For large coolant system breaks the passive accumulators inject first, because of the rapid pressure drop. This protects the reactor during the unavoidable delay associated with actuating the active ECCS phase.

High containment pressure also actuates the ECCS. Therefore, emergency core cooling actuation can be brought about upon sensing this other direct consequence of a primary system break; i.e.,

FNP-FSAR-7

the ESFAS detects the leakage of the coolant into the containment. The generation time of the actuation signal of about 2.0 s, after detection of the consequences of the accident, is adequate.

Containment spray will provide additional emergency cooling of containment and also limit fission product release upon sensing elevated containment pressure (high-high-high) to mitigate the effects of a LOCA.

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is assumed to be about 2.0 s, well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the fluid systems.

The analyses in chapter 15 show that the diverse methods of detecting the accident condition and the time for generation of the signals by the protection systems are adequate to provide reliable and timely protection against the effects of loss of coolant.

The nominal setpoint for the initiation of the containment spray is set at 50 percent of design pressure. The corresponding high-high-high safety analysis limit (SAL) modeled in the containment analysis includes allowances for instrument uncertainty. Following a LOCA, the SAL pressure setpoint will be reached in approximately 8 s.

The containment pressure instrumentation that generates the containment spray signal has the same time delay as the instrumentation that generates the signal on high-high containment pressure for closing the main steam stop valves, as presented in paragraph 7.3.1.2. The maximum allowable time delay in generating this actuation signal is 2.0 s.

To yield the maximum containment spray delay time, a LOCA/LOSP is postulated. At $t = 0$, an LOSP is assumed. Subsequently, the diesel is signaled to start by the Class 1E BUS UV signal. At $t = 8$ s, the containment spray actuation signal is generated separately from the LOSP. The MOVs begin to stroke open once the diesels re-energize the Class 1E BUS. The spray pumps are started on diesel loading Step 2. At $T = 62$ s, the system begins spraying into the containment atmosphere.

This maximum containment spray delay time of 62 s includes 15 s for LOSP signal generation and diesel starting time (the High-3 signal is generated prior to Step 2 sequencing for LOCA), a 12 s MOV stroke time (which bounds the concurrent delays associated with Step 2 sequencing and spray pump startup), and a 35-s spray header fill time.

During normal plant operation, up to four units will be operating. Service water is flowing through all four containment coolers during normal operation. Following a LOCA, at least two coolers will be operated in low speed.

If offsite power is available, the four containment coolers (2 per train) that were operating at high speed during normal operation will switch to low speed upon receipt of a safety injection signal. Two coolers (1 per train) may be shut down by the plant operator, and two coolers will continue to operate. There is no time delay in starting the containment coolers, if offsite power is available.

If offsite power is lost, power will not be available for the high speed windings of the containment air cooler motors.

However, the diesel generators will automatically be started, and at least two coolers will be started in low speed by the loss-of-power shutdown sequencer. This will occur regardless of whether a LOCA has occurred. The time between the loss of offsite power and the restarting of the containment coolers is 27.4 s. The service water pumps are restarted by the diesels 5 s before the containment coolers.

7.3.2.9.2 Steam Break Protection

The ECCS is also actuated in order to protect against a steam line break. About 2.0 s elapse between sensing high steam line differential pressure or low steam line pressure and generation of the actuation signal. Analysis of steam break accidents, assuming this delay for signal generation, shows that the ECCS is actuated for a steam break in time to limit or prevent damage in the core. There is a reactor trip, but the core reactivity is further reduced by the highly borated water injected by the ECCS.

Additional protection against the effects of steam break is provided by feedwater isolation which occurs upon actuation of the ECCS. Feedwater line isolation is initiated to prevent excessive cooldown of the reactor.

Additional protection against a steam break accident is provided by closure of all steam line isolation valves to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (about 2.0 s) is again short compared to the time to trip the fast acting steam line isolation valves which are capable of closure in < 7 s after receipt of a signal.

In addition to actuation of the ESF, the effect of a steam break accident also generates a signal resulting in a reactor trip on overpower or following ECCS actuation. However, the core reactivity is further reduced by the borated water (2000 ppm)^(a) injected by the ECCS.

The analysis in chapter 15 of the steam break accidents and an evaluation of the protection system instrumentation and channel design show that the ESFAS is effective in preventing or mitigating the effects of a steam break accident.

7.3.2.9.3 Feedline Break Protection

The ESFAS is actuated to protect against a feedline break. Following reactor trip due to a low-low steam generator water level trip setpoint, pressure in the steam line falls below a given setpoint. When the setpoint is reached, all main steam isolation valves are closed, which guarantees a steam supply for the turbine-driven auxiliary feedwater pump.

Assurance that adequate feedwater is available for the feedline break is provided by the auxiliary feedwater system, which includes two motor-driven pumps and one turbine-driven pump. The motor-driven pumps are initiated automatically by one of the following signals:

- A. Safety injection or safeguards sequence (derived from the solid-state protection system output cabinets).

FNP-FSAR-7

- B. Two out of three low-low level in any steam generator (derived from the solid-state protection system output cabinets).
- C. Manual start.
- D. Trip of all main feed pumps.
- E. Blackout signal.

The turbine-driven pumps, as well as the closing of blowdown and sample valves, are initiated automatically by one of the following signals:

- A. Two out of three low-low level in two out of three steam generators (derived from the solid-state protection system output cabinets).
- B. Manual start.
- C. Loss of voltage signal.

Evaluation of the protection system instrumentation and channel design shows that minimum auxiliary feedwater capacity is adequate to remove decay heat to prevent overpressurization of the reactor coolant system and to prevent uncovering the reactor core. Minimum auxiliary feedwater capacity is that capacity available following a feedline break event, assuming the worst single failure. The analysis in chapter 15 of the feedline break accident shows that the ESFAS is effective in mitigating the effects of a feedline break accident.

a. The minimum RWST boron concentration was increased to 2300 ppm in Unit 1 License Amendment 68 and Unit 2 license Amendment 60. The purpose of the safety injection during this event is to control the return to criticality by inserting negative reactivity into the core. The injection of 2300 ppm boron concentration from the RWST would insert more negative reactivity into the core than the 2000 ppm boron concentration, which would cause the event to be terminated sooner. Therefore, the injection of 2300 ppm boron concentration from the RWST is bounded by the analysis presented.

REFERENCES

1. Reid, J. B., "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP-913, January 1973.
2. Katz, D. N., "Solid State Logic Protection System Description," WCAP-7672, June 1971.
3. Haller, J. T., "Engineered Safeguards Final Device or Actuator Testing," WCAP-7705, May 1972.
4. Institute of Electrical and Electronics Engineers, "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE 279-1971.
5. Locante, J. and Igne, E. G., "Environmental Testing of Engineered Safety Features Related Equipment (NSSS -Standard Scope)," WCAP-7744, Volume I, August 1971.
6. Institute of Electrical and Electronics Engineers, "Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations," IEEE 308-1971.
7. Institute of Electrical and Electronics Engineers, "Trial-Use Standard: General Guide for Qualifying Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 323-1971.
8. Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Type Tests of Continuous Duty Class 1 Motors Installed Inside the Containment of Nuclear Power Generating Stations," IEEE 334-1971.
9. Institute of Electrical and Electronics Engineers, "Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protective Systems," IEEE 338-1971.
10. Institute of Electrical and Electronics Engineers, "Trial-Use Guide for Seismic Qualification of Class 1 Electrical Equipment for Nuclear Power Generating Stations," IEEE 344-1971, dated August 11, 1971.
11. Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706, July 1971.
12. Metro, B. J., "Reliability Assessment of Westinghouse Type AR Relays used as SSPS Slave Relays," WCAP-13877, January 1994.
13. Andre, S. V., "Westinghouse Setpoint Methodology for Protection Systems for Southern Nuclear Operating Company Farley Nuclear Plant Units 1 and 2," WCAP-13751, June 1993.
14. Howard, R. C., "Elimination of Pressure Sensor Response Time Testing Requirements," WCAP-13632-P-A, Rev. 2, January 1996.
15. Morgan, C. E., "Elimination of Periodic Protection Channel Response Time Tests," WCAP-14036-P-A, Rev. 1, October 1998.

FNP-FSAR-7

16. WCAP-16769-P Revision 2, "Westinghouse SSPS Universal Logic Board Replacement Summary Report 6D30225G01/G02/G03/G04."
17. WCAP-16670-P Revision 0, "Westinghouse SSPS Safeguards Driver Board Replacement Summary Report 6D30252G01/G02."
18. WCAP-16671-P Revision 1, "Westinghouse SSPS Undervoltage Driver Board Replacement Summary Report 6D30350G01/G02."
19. WCAP-16672-P Revision 1, "Westinghouse SSPS Semi-Automatic Tester Board Replacement Summary Report 6D30520G01/G02/G03/G04/G05."
20. WCAP-17867-P-A Revision 1, "Westinghouse SSPS Board Replacement Licensing Summary Report."
21. WCAP-16773-P Revision 0, "Westinghouse SSPS Clock Counter Board Replacement Summary Report 6D30687G01."
22. WCAP-16774-P Revision 0, "Westinghouse SSPS Decoder Board Replacement Summary Report 6D31031G01."
23. WCAP-16775-P Revision 0, "Westinghouse SSPS Isolation Board Replacement Summary Report 6D31033G01."
24. WCAP-16776-P Revision 1, "Westinghouse SSPS Memory Board Replacement Summary Report 6D31035G01."

TABLE 7.3-1 (SHEET 1 OF 2)**FUNCTIONS INITIATED BY ENGINEERED
SAFETY FEATURES ACTUATION SYSTEM**

<u>Item</u>	<u>Function</u>
1	Reactor trip, provided one has not already been generated by the reactor trip system
2	Engineered safety features actuation system sequence, which actuates equipment that includes items 2a through 2g and ensures the proper sequencing of engineered safety features power demands on the engineered safety features buses supplied by either preferred or standby power supply
2a	Cold leg injection isolation valves, which are opened for injection of borated water by safety injection pumps into the cold legs of the reactor coolant system. The receipt of a safety injection signal by the accumulator motor-operated valves is discussed in paragraph 6.3.2.2.7.
2b	Charging pumps, residual heat removal pumps, and associated valving, which provide emergency makeup water to the cold leg of the reactor coolant system following a loss-of-coolant accident
2c	Containment air recirculation fans and coolers, which serve to cool the containment and limit the potential for release of fission products from the containment by reducing the pressure following an accident
2d	Component cooling pumps and valves
2e	Service water pump and valves, which provide cooling water to the component cooling system heat exchangers and is thus the heat sink for containment cooling
2f	Motor-driven auxiliary feedwater pumps and control valves
2g	Penetration room filtration system
3	Phase A containment isolation, "T" signal, whose function is to prevent fission product release by isolating all nonessential process lines on receipt of the safety injection signal
4	Steam line isolation, to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled reactor coolant system cooldown
5	Main feedwater line isolation, to limit the energy release for a steam line break and to limit the extent of the reactor coolant system cooldown
6	Emergency diesel start, to ensure backup supply of power to emergency and supporting systems components
7	Control room intake duct isolation, to meet control room occupancy requirements following a loss-of-coolant accident

TABLE 7.3-1 (SHEET 2 OF 2)

<u>Item</u>	<u>Function</u>
8	Containment spray actuation, "P" signal, which performs the following functions listed as items 8a and 8b
8a	Containment spray initiation, which serves to reduce containment pressure and temperature following a loss-of-coolant or a steam break accident
8b	Phase B containment isolation initiation, other than safety injection lines which are not closed. The remaining process lines into containment are isolated following a loss of reactor coolant accident or a steam or feedwater line break within containment.

TABLE 7.3-2 (SHEET 1 OF 2)
INSTRUMENTATION OPERATING CONDITIONS
FOR ENGINEERED SAFETY FEATURES

<u>Number</u>	<u>Functional Unit</u>	<u>Number of Channels</u> ^(a)	<u>Number of Channels to trip</u>
1.	Safety Injection		
1a.	Manual ^(a)	2 switches	1 switch
1b.	Containment pressure high	3	2
1c.	Differential pressure high between steam lines	9 (3 per steam line)	2 per steam line and 1/3 comparison between steam lines
1d.	Pressurizer low pressure ^(b)	3	2
1e.	Steam line low pressure ^(c)	3 pressure signals	2
2.	Containment Spray		
2a.	Manual ^(a)	2 pairs of switches	2 switches per pair
2b.	Containment pressure high-high-high	4	2
3.	Auxiliary feedwater		
3a.	Motor driven pumps		
3a1	Manual ^(d)	2 switches (1 switch per pump)	2 switches (1 switch per pump)
3a2	Steam generator water level low-low	3 per steam generator	2/3 in any steam generator
3a3	Safety injection	See item 1	
3a4	Trip of main feedwater pumps	4 (2 per pump)	2 (1 per pump)

FNP-FSAR-7

TABLE 7.3-2 (SHEET 2 OF 2)

<u>Number</u>	<u>Functional Unit</u>	<u>Number of Channels</u> ^(a)	<u>Number of Channels to trip</u>
3a5	AMSAC actuation	1	1
3b	Turbine driven pump		
3b1	Manual ^(e)	1 switch	1 switch
3b2	Steam generator water level low-low	3 per steam generator	2/3 in 2/3 steam generators
3b3	RCP bus undervoltage	3 bus	2 bus
3b4	AMSAC actuation	1	1

a. Each switch actuates both Train A & B.

b. Permissible bypass if reactor coolant pressure is less than P-11.

c. Permissible bypass if reactor coolant temperature is less than P-12.

d. Motor driven AFW pump 1 switch actuates Train A and motor driven AFW pump 2 switch actuates Train B.

e. Turbine driven AFW pump switch opens steam admission valves.

TABLE 7.3-3 (SHEET 1 OF 2)
INSTRUMENTATION OPERATING CONDITIONS
FOR ISOLATION FUNCTIONS

<u>Number</u>	<u>Functional Unit</u>	<u>Number of Channels</u>	<u>Number of Channels to Trip</u>
1.	Containment Isolation		
1a.	Safety injection - Phase A	See item 1 of table 7.3-2.	
1b.	Containment pressure high-high-high - Phase B	See item 2b of table 7.3-2.	
1c.	Manual		
	Phase A ^(a)	2	1
	Phase B	See item 2a of table 7.3-2.	
2.	Steam Line Isolation		
2a.	Steam flow high coincident with low-low T _{avg}		
	Steam flow high	2 per steam line	1 high flow per steam line on 2/3 steam lines
	Low-low T _{avg}	1 per loop	2/3 low-low T _{avg}
2b.	Steam line low pressure	1 per steam line	2/3 steam lines
2c.	Containment pressure high-high	3	2
2d.	Manual ^(a)	1 per loop	1 per loop

a. Each switch actuates both Train A & B.

FNP-FSAR-7

TABLE 7.3-3 (SHEET 2 OF 2)

<u>Number</u>	<u>Functional Unit</u>	<u>Number of Channels</u>	<u>Number of Channels to Trip</u>
3.	Feedwater line isolation		
3a.	Safety injection	See item 1 of table 7.3.2	
3b.	Steam generator water level high-high	3 per steam generator	2/3 in any steam generator
3c.	Low T_{avg} coincident with reactor trip		
	Low T_{avg}	1 per loop	2/3 low T_{avg}
	Reactor trip	2	1
4.	Turbine Trip		
4a.	Safety injection	See item 1 of table 7.3-2	
4b.	Steam generator water level high-high	See item 3b	See item 3b
4c.	Reactor Trip	2	1
5.	Steam generator feedwater pump trip ^(a)		
5a.	Safety injection	See item 1 of table 7.3-2	
5b.	Steam generator water level high-high	See item 3b	See item 3b

a. Train A trips both feedwater pumps.

TABLE 7.3-4 (SHEET 1 OF 2)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

<u>Designation</u>	<u>Input</u>	<u>Function Performed</u>
P-4 ^(a)	Reactor trip	Actuates turbine trip
		Prevents opening of main feedwater valves which were closed by safety injection or high steam generator water level
		Allows manual block of the automatic reactivation of safety injection
		Blocks steam dump control via load rejection T_{avg} controller
	Makes steam dump valves available for either tripping or modulation	
P-11	Reactor not tripped	Defeats the manual block preventing automatic reactivation of safety injection
		Block steam dump control via plant trip T_{avg}
	2/3 pressurizer pressure below setpoint	Allows manual block of safety injection actuation on low pressurizer pressure signal
	2/3 pressurizer pressure above setpoint	Blocks automatic opening of the power relief valves
		Defeats manual block of safety injection actuation
		Opens accumulator motor-operated isolation valves

a. See table 7.7-1 for control functions

TABLE 7.3-4 (SHEET 2 OF 2)

<u>Designation</u>	<u>Input</u>	<u>Function Performed</u>
P-12	2/3 T _{avg} below setpoint ^(a)	Allows manual block of safety injection actuation on low steam line pressure
		Blocks steam dump Allows manual bypass of steam dump block for the cooldown dump valves only
	2/3 T _{avg} above setpoint	Defeats the manual block of safety injection actuation on low steam line pressure
P-14	2/3 steam generator water level above setpoint on any steam generator	Defeats the manual bypass of steam dump block
		Closes all feedwater control valves
		Trips all main feedwater pumps which closes the pump discharge valves
		Actuates turbine trip

a. This signal, in coincidence with high steam line flow in 2/3 steam lines, actuates steam line isolation.

FNP-FSAR-7

TABLE 7.3-5

(THIS TABLE INTENTIONALLY DELETED)

TABLE 7.3-6 (SHEET 1 OF 15)
FAILURE MODE AND EFFECTS ANALYSIS,
SERVICE WATER SYSTEM

Component Identification Service Water PumpsLogic Diagram Number NAElementary Number D-172747 through D-172752,
D-202747 through D-202752Engineering Flow Diagram Number:
D-170119 Sh. 1 & D-200013 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 4.16-kV bus power	Failure of pump to start when required or automatic stoppage when pump is running	4.16-kV bus U/V or bus breaker auto trip alarm on emergency power board	Redundant train pumps can be started
Loss of 4.16-kV power to motor due to automatic breaker trip	Interruption of service water supply to one train	Breaker automatic trip alarm on main control board	Two pumps are provided per train; the standby pump will be started from the main control board
Loss of 125 V-dc breaker control power to one pump	Inability of pump to start on manual or automatic signal, or trip the breaker when required	During testing or observation of control switch indicating lights	Two pumps are provided per train; the standby pump will be started from the main control board; a failure to trip a breaker may cause loss of bus on one train, redundant train pumps can be started manually
Failure of loss of power sequencer or ESS sequencer start signal to both pumps in one train	Inability of both pumps in a train to start automatically	ESFAS malfunction alarm on main control board or periodic testing	Both redundant pumps in other train start automatically on loss of offsite power; pumps can be started manually from control switches on the main control board

TABLE 7.3-6 (SHEET 2 OF 15)

Component Identification 3019A,B,C,D and 3024A,B,C,DLogic Diagram Number NAElementary Number C-177613/D-207613Engineering Flow Diagram Number:
D-175003 Sh. 1, D-205003 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-610 fails to operate on receipt of safety injection signal	Two valves in the following grouping would not operate: MOV 3019 A/B and 3024 A/B or MOV 3019 C/D and 3024 C/D a. If valve initially open, no effect on system b. If valve initially closed, system reduced to 2/4 (minimum requirements)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication lights at main control board	Valves fail as is; normal position is open; post-LOCA position is open; operator can open valves
Loss of power to motor control center U or V	Two valves in the following grouping would not operate: MOV 3019 A/B and 3024 A/B or MOV 3019 C/D and 3024 C/D a. If valve initially open, no effect on system b. If valve initially closed, system reduced to 2/4 (minimum requirements) c. Loss of ability to close valve	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position at main control board	Position indication lights of main control board will be out
Contacts of relay K-610 fail to close on receipt of safety injection signal or failure of open/close relay to operate	Valve fails as is; if valve initially closed, system reduced to 3/4	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication lights at main control board	Operator can open valves

TABLE 7.3-6 (SHEET 3 OF 15)

Component Identification 3019A,B,C,D and 3024A,B,C,D (cont.)Logic Diagram Number NAElementary Number C-177613/D-207613Engineering Flow Diagram Number:
D-175003 Sh. 1, D-205003 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Thermal overload relay contacts open	Valve fails as is; if valve initially closed, system reduced to 3/4; loss of ability to close valve	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication lights at main control board	
Loss of 120 V-ac control power	Valve fails as is; if valve initially closed, system reduced to 3/4	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication at main control board	Position indication lights or main control board will be out

TABLE 7.3-6 (SHEET 4 OF 15)

Component Identification 3131Logic Diagram Number NAElementary Number C-177612/D-207612Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-604 fails to operate on safety injection signal	Valve fails as is; alternate valve (3134) operates to effect isolation; operator can close if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed; two containment isolation valves in series, one required to operate
Contacts of ESF relay K-604 fail to close on safety injection signal	Valve fails as is; alternate valve (3134) operates to effect isolation; operator can close if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center U	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

TABLE 7.3-6 (SHEET 5 OF 15)

Component Identification 3131 (cont.)Logic Diagram Number NAElementary Number C-177612/D-207612Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open (By-passed for Unit 1 per SNC1086636)	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter to operate	Valve fails as is; operator can close/open valve depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

TABLE 7.3-6 (SHEET 6 OF 15)

Component Identification 3134Logic Diagram Number NAElementary Number D-177636/D-207636Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-604 fails to operate on safety injection signal	Valve fails as is; alternate valve (3131) operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed; two containment isolation valves in series, one required to operate
Contacts of ESF relay K-604 fail to close on safety injection signal	Valve fails as is; alternate valve (3131) operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center V	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

TABLE 7.3-6 (SHEET 7 OF 15)

Component Identification 3134 (cont.)Logic Diagram Number NAElementary Number D-177636/D-207636Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter relay to operate	Valve fails as is; operator can close/open valve depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

TABLE 7.3-6 (SHEET 8 OF 15)Component Identification 3135Logic Diagram Number NAElementary Number D-177636/D-207636Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-604 fails to operate on safety injection signal	Valve fails as is; alternate valve (QV075) is a check valve which operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed; two containment isolation valves in series, one required to operate
Contacts of ESF relay K-604 fail to close on safety injection signal	Valve fails as is; alternate valve (QV075) is a check valve which operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center V	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

TABLE 7.3-6 (SHEET 9 OF 15)

Component Identification 3135 (cont.)Logic Diagram Number NAElementary Number D-177636/D-207636Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter relay to operate	Valve fails as is; operator can close/open valve depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

TABLE 7.3-6 (SHEET 10 OF 15)

Component Identification 3149Logic Diagram Number NAElementary Number C-177617/D-207617Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-604 fails to operate on safety injection signal	Valve 3149 fails as is; operator can close valves if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed
Contacts of ESF relay K-604 fail to close on safety injection signal	Valve 3149 fails as is; operator can close valves if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center U	Valves fail as are	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

TABLE 7.3-6 (SHEET 11 OF 15)

Component Identification 3149 (cont.)Logic Diagram Number NAElementary Number C-177617/D-207617Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter relay to operate	Valve fails as is; operator can close/open valve depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

TABLE 7.3-6 (SHEET 12 OF 15)

Component Identification 3150Logic Diagram Number NAElementary Number C-177617/D-207617Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-604 fails to operate on safety injection signal	Valve 3150 fails as is; operator can close valves if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed
Contacts of ESF relay K-604 fail to close on safety injection signal	Valve 3150 fails as is; operator can close valves if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center U	Valves fail as are	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

TABLE 7.3-6 (SHEET 13 OF 15)Component Identification 3150 (cont.)Logic Diagram Number NAElementary Number C-177617/D-207617Engineering Flow Diagram Number:
D-175003 Sh. 2, D-205003 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter relay to operate	Valve fails as is; operator can close/open valve depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

TABLE 7.3-6 (SHEET 14 OF 15)

Component Identification 3441A,B,C,DLogic Diagram Number NAElementary Number D-177633/D-207633Engineering Flow Diagram Number:
D-175003 Sh. 1, D-205003 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-610 fails to operate on receipt of safety injection signal	Two valves in the following groupings would not operate: MOV 3441 A/B or MOV 3441 C/D a. If valves initially open, no effect on system b. If valves initially closed, system reduced to 2/4 (minimum requirements)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication light at main control board d. Periodic testing	Valves fail as is; normal valve position is open; post-LOCA position is open; operator can open valves
Loss of power to motor control center U or V	Two valves in the following groupings would not operate: MOV 3441 A/B or MOV 3441 C/D a. If valves initially open, no effect on system b. If valves initially closed, system reduced to 2/4 (minimum requirements) c. Loss of ability to close valve	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Loss of valve position indication at main control board d. Periodic testing	
Contacts of relay K-610 fail to close on receipt of safety injection signal or failure of starter relay to operate	Valve fails as is; if valve is initially closed, system is reduced to 3/4	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication at main control board d. Periodic testing	Operator can open valves

TABLE 7.3-6 (SHEET 15 OF 15)Component Identification 3441A,B,C,D (cont.)Logic Diagram Number NAElementary Number D-177633/D-207633Engineering Flow Diagram Number:
D-175003 Sh. 1, D-205003 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Thermal overload relay contacts open	Loss of ability to close valve; valve fails as is; if valve is initially closed, system is reduced to 3/4	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication at main control board d. Periodic testing	
Loss of 120 V-ac control power	Loss of ability to close valve; valve fails as is; if valve is initially closed, system is reduced to 3/4	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Loss of valve position indication at main control board d. Periodic testing	

TABLE 7.3-7 (SHEET 1 OF 17)

FAILURE MODE AND EFFECTS ANALYSIS, COMPONENT COOLING WATER SYSTEM

Component Identification Component Cooling Water PumpsLogic Diagram Number NAElementary Number D-177183, D-177184, D-177185, D-177187,
D-207183, D-207184, D-207185, D-207187Engineering Flow Diagram Number:
D-175002, Sh. 1, Sh. 2, and Sh. 3,
D-205002, Sh. 1, Sh. 2, and Sh. 3

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 4.16-kV power to one pump	Failure of pump to start when required or automatic stoppage when pump is running	4.16-kV bus U/V or bus breaker auto trip alarm on emergency power board	Redundant train pump can be started.
Loss of 125 V-dc breaker control power	Inability of pump to start on manual or automatic signal, or trip the breaker when required	During monthly testing or observation of control switch red, green, and amber lights	Three pumps are provided; one pump is required for normal, hot shutdown, or post-LOCA heat removal. A failure to trip a breaker may cause loss of bus on one train, redundant train pump can be started manually.
Failure of loss of power sequencer start or ESS sequencer start signals	Inability of pump to start upon receipt of automatic start signal	ESS malfunction alarm on main control board or periodic testing	Pump can be manually started from the main control board
Automatic breaker trip due to overcurrent	Standby (swing) pump automatically starts if aligned with pump that tripped	Breaker auto trip alarm on main control board	Swing pump can be put into service manually; one pump is required for normal, hot shutdown, or post-LOCA heat removal

FNP-FSAR-7

TABLE 7.3-7 (SHEET 2 OF 17)

Component Identification 3067

Logic Diagram Number NA

Elementary Number F-177851/D-207851

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3067 and 3443); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3067 and 3443); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at main control board out b. Computer c. Light monitor panel d. High temperature at discharge of excess letdown heat exchanger (TE-139)	
Solenoid valve 3067 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3067 and 3443); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 3 OF 17)

Component Identification 3067 (Cont.)

Logic Diagram Number NA

Elementary Number F-177851/D-207851

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of instrument air	Valve fails closed	<ul style="list-style-type: none"> a. Valve position light at main control board b. Computer c. Light monitor panel d. High temperature at discharge of excess letdown heat exchanger (TE-139) 	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 4 OF 17)

Component Identification 3095

Logic Diagram Number NA

Elementary Number F-177851/D-207851

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3095 and a check valve); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3095 and a check valve); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at main control board out b. Computer c. Light monitor panel d. High temperature at discharge of excess letdown heat exchanger (TE-139)	
Solenoid valve 3095 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3095 and a check valve); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 5 OF 17)

Component Identification 3095 (cont.)

Logic Diagram Number NA

Elementary Number F-177851/D-207851

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of instrument air	Valve fails closed	<ul style="list-style-type: none"> a. Valve position light at main control board b. Computer c. Light monitor panel d. High temperature at discharge of excess letdown heat exchanger (TE-139) 	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 6 OF 17)

Component Identification 3096A,B

Logic Diagram Number NA

Elementary Number D-177853/D-207853

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-609 fails to operate on receipt of safety injection signal	Valves remains open; operator can close valves from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valves are normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-609 fail to open on receipt of safety injection signal	Valves remain open; operator can close valves from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at main control board out b. Computer c. Light monitor panel	
Solenoid valve 3096A or 3096B fails to vent (sticky operator)	Associated valve remains open; other valve will be operational	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at main control board b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 7 OF 17)

Component Identification 3045

Logic Diagram Number NA

Elementary Number D-177854/D-207854

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-625 fails to operate on receipt of CIAS phase B	Valve remains open; however, there are two valves in series (3045 and 3184); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air; valve operation is not testable with reactor coolant pumps operating
Contacts of ESF relay K-625 fails to open on receipt of CIAS phase B	Valve remains open; however, there are two valves in series (3045 and 3184); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails open control board	Valve position lights at main	
Solenoid valve 3045 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3045 and 3184); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve closes	a. Valve position lights at main control board b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 8 OF 17)

Component Identification 3046

Logic Diagram Number NA

Elementary Number C- 177618/D-207618

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-619 fails to operate on CIAS phase B	Valve fails as is; alternate valve 3182 operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication lights at main control board d. Periodic testing	Normal valve position open; post-LOCA position closed; two containment isolation valves in series; one required for isolation; <u>valve not testable at power</u>
Contacts of ESF relay K-619 fail to close on CIAS phase B	Valve fails as is; alternate valve 3182 operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication at main control board d. Periodic testing	
Loss of power to motor control center U	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Loss of valve position indication light at main control board d. Periodic testing	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 9 OF 17)

Component Identification 3046 (cont.)

Logic Diagram Number NA

Elementary Number C-177618/D-207618

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Loss of valve position light at main control board d. Periodic testing	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication lights at main control board d. Periodic testing	
Failure of starter relay to operate	Valve fails as is; operator can close or open valve depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Position indication lights at main control board d. Periodic testing	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 10 OF 17)

Component Identification 3052

Logic Diagram Number NA

Elementary Number C-177625/D-207625

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-619 fails to operate on CIAS phase B	Valve fails as is; alternate valve is check valve which operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed; two containment isolation valves in series; one required to operate; <u>valve not testable at power</u>
Contacts of ESF relay K-619 fail to close on CIAS phase B	Valve fails as is; alternate valve is check valve which operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center V	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 11 OF 17)

Component Identification 3052 (cont.)

Logic Diagram Number NA

Elementary Number C-177625/D-207625

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter relay to operate	Valve fails as is; operator can close/open valves depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 12 OF 17)

Component Identification 3182

Logic Diagram Number NA

Elementary Number D-177610/D-207610

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-619 fails to operate on CIAS phase B	Valve fails as is; alternate valve 3046 operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	Normal valve position open; post-LOCA position closed; two containment isolation valves in series; one required to operate; <u>valve not testable at power</u>
Contacts of ESF relay K-619 fail to close on CIAS phase B	Valve fails as is; alternate valve 3046 operates to effect isolation; operator can close valve if initially open (normal)	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Loss of power to motor control center V	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 13 OF 17)

Component Identification 3182 (cont.)

Logic Diagram Number NA

Elementary Number D-177610/D-207610

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Loss of valve position indication light at main control board	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	
Failure of starter relay to operate	Valve fails as is; operator can close/open valves depending on which starter coil fails	Depending on initial valve position and plant operating status: a. Computer b. Light monitor panel c. Periodic testing d. Position indication at main control board	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 14 OF 17)

Component Identification 3184

Logic Diagram Number NA

Elementary Number D-177855/D-207855

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-625 fails to operate on receipt of CIAS phase B	Valve remains open; however, there are two valves in series (3184 and 3045); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air; valve operation is not testable with reactor coolant pumps operating
Contacts of ESF relay K-625 fail to open on receipt of CIAS phase B	Valves remains open; however, there are two valves in series (3184 and 3045); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve open	Valve position lights at main control board	
Solenoid valve 3184 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3184 and 3045); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve closes	a. Valve position lights at main control board b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 15 OF 17)

Component Identification 3443

Logic Diagram Number NA

Elementary Number D-177374/D-207374

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3443 and 3067); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valves are normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3443 and 3067); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at main control board out b. Computer c. Light monitor panel d. High temperature at discharge of excess letdown heat exchanger (TE-139)	
Solenoid valve 3443 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3443 and 3067); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 16 OF 17)

Component Identification 3443 (cont.)

Logic Diagram Number NA

Elementary Number D-177374/D-207374

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of instrument air	Valve fails closed	<ul style="list-style-type: none"> a. Valve position light at main control board b. Computer c. Light monitor panel d. High temperature at discharge of excess letdown heat exchanger (TE-139) 	

FNP-FSAR-7

TABLE 7.3-7 (SHEET 17 OF 17)

Component Identification 2229

Logic Diagram Number NA

Elementary Number D-177853/D-207853

Engineering Flow Diagram Number D-175002 Sh. 2, D-205002 Sh. 2

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-609 fails to operate on receipt of safety injection signal	Valve remains open; operator can close valve from local control station	Depending on initial valve position and plant operating status: a. Valve position indication at local control station b. Light monitor panel c. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-609 fail to open on receipt of safety injection signal	Valve remains open; operator can close valve from local control station	Depending on initial valve position and plant operating status: a. Valve position indication at local control station b. Light monitor panel c. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at local control station out b. Light monitor panel	
Solenoid valve 2229A fails to vent (sticky operator)	Associated valve remains open; other valve will be operational	Depending on initial valve position and plant operating status: a. Valve position indication at local control station b. Light monitor panel c. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at local control station b. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 1 OF 18)

FAILURE MODE AND EFFECTS ANALYSIS, CONTROL ROOM AND AIR CONDITIONING AND FILTRATION SYSTEM

Component Identification Filtration Fan

Logic Diagram Number NA

Elementary Number D-177270 Sh. 1

Engineering Flow Diagram Numbers:
D-175012 Sh. 1 & D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-614 fails to operate on CIAS phase A, Unit 1 or 2	Motor fails to start; of two filtration fans, only one is required for operation; operator can start motor if necessary	a. Control room indication lights b. Periodic testing c. Monitor light box abnormal	
Contacts of ESF relay K-614 fail to close on CIAS phase A	Motor fails to start; of two filtration fans, only one is required for operation; operator can start motor if necessary	a. Control room indication lights b. Periodic testing c. Monitor light box abnormal	
Loss of power to 208-V motor control center 1F and 1G	Motor fails to start	a. Control room indication lights b. Periodic testing	
Loss of 120 V-ac control power	Motor fails to start	a. Control room indication lights b. Periodic testing	
Thermal overload relay contacts open	Motor fails to start	a. Control room indication lights b. Periodic testing c. Motor overload trip alarm in the control room	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 2 OF 18)

Component Identification Air Conditioning Unit

Logic Diagram Number NA

Elementary Number D-177270 Sh. 3

Engineering Flow Diagram Numbers:
D-175012 Sh. 1 & D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-614 fails to operate on CIAS phase A, Unit 1 or 2	Motor fails to start; of two air conditioning units, only one is required for operation; operator can start motor if necessary	a. Periodic testing	Redundant train will start
Contacts of ESF relay K-614 fail to close on CIAS phase A	Motor fails to start; of two air conditioning units, only one is required for operation; operator can start motor if necessary	a. Periodic testing	
Loss of power to 600-V motor control center 1F & 1G	Motor fails to start	a. Periodic testing	
Loss of 120 V-ac control power	Motor fails to start	a. Periodic testing	
Thermal overload relay contacts open	Motor fails to start	a. Periodic testing b. Motor overload trip alarm in the control room	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 3 OF 18)

Component Identification 3478A

Elementary Number D-177280 Sh. 1

Logic Diagram Number NA

Engineering Flow Diagram Numbers:
D-175012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-614 or its contact fails to operate on CIAS phase A	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Position indication lights at BOP panel c. Periodic testing	Normal valve position closed; post-LOCA position open on control room pressurization fan start signal Redundant valve will open
Contacts of 42X relay (Control Room Pressurization Fan) fails to operate on CIAS phase A	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Position indication lights at BOP Panel c. Periodic testing	Redundant valve will open
Loss of power to 600-V motor control center 1F	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Loss of valve position indication light at BOP Panel c. Periodic testing	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 4 OF 18)

Component Identification 3478A (cont.)

Logic Diagram Number NA

Elementary Number D-177280 Sh. 1

Engineering Flow Diagram Numbers:
D-175012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Loss of valve position indication lights at BOP panel	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Loss of position indication lights at BOP panel c. Periodic testing	
Failure of (42) starter relay to operate	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Position indication lights at main control board c. Periodic testing	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 5 OF 18)

Component Identification 3478B

Elementary Number D-177280 Sh. 1

Logic Diagram Number NA

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-614 or its contact fails to operate on CIAS phase A	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Position indication at BOP panel	Normal valve position closed; post-LOCA position open on control room pressurization fan start signal; Redundant valve will open
Contact of 42X relay (Control Room Pressurization Fan) fails to operate on CIAS phase A	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Position indication at BOP panel	Redundant valve will open
Loss of power to 600-V motor control center 1G	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Loss of valve position indication light at BOP panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 6 OF 18)

Component Identification 3478B (cont.)

Logic Diagram Number NA

Elementary Number D-177280 Sh. 1

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 120 V-ac control power	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Loss of valve position indication lights at BOP panel	
Thermal overload relay contacts open	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Loss of position indication at BOP panel	
Failure of (42) starter relay to operate	Valve fails as is	Depending on initial valve position and plant operating status: a. Computer b. Periodic testing c. Position indication at main control board	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 7 OF 18)

Component Identification 3622

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3622 and 3623); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3622 and 3623); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at main control board b. Computer c. Light monitor panel	
Solenoid valve 3622 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3622 and 3623); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 8 OF 18)

Component Identification 3623

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3623 and 3622); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3623 and 3622); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3623 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3623 and 3622); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 9 OF 18)

Component Identification 3624

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-606 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3624 and 3625); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-606 fail to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3624 and 3625); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3624 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3624 and 3625); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 10 OF 18)

Component Identification 3625

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3625 and 3624); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fail to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3625 and 3624); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3625 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3625 and 3624); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 11 OF 18)

Component Identification 3626

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3626 and 3627); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3626 and 3627); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3626 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3626 and 3627); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 12 OF 18)

Component Identification 3627

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3627 and 3626); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3627 and 3626); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3627 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3627 and 3626); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 13 OF 18)

Component Identification 3628

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-605 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3628 and 3629); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-605 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3628 and 3629); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3628 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3628 and 3629); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 14 OF 18)

Component Identification 3629

Logic Diagram Number NA

Elementary Number D-177373

Engineering Flow Diagram Numbers:
D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-605 fails to operate on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3629 and 3628); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is normally open and will fail closed on loss of instrument air
Contacts of ESF relay K-605 fails to open on receipt of CIAS phase A	Valve remains open; however, there are two valves in series (3629 and 3628); only one required to operate to cause isolation; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3628 fails to vent (sticky operator)	Valve remains open; however, there are two valves in series (3629 and 3628); only one required to operate to cause isolation	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 15 OF 18)

Component Identification 3649A

Logic Diagram Number NA

Elementary Number D-177883

Engineering Flow Diagram Numbers:
D-175012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is open only for smoke purge; will fail closed on loss of instrument air
Contacts of ESF relay K-613 fail to open on receipt of CIAS phase A	Valve remains open; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3649A fails to vent (sticky operator)	Valve remains open; however, valve is normally closed except for smoke purge	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 16 OF 18)

Component Identification 3649B

Logic Diagram Number NA

Elementary Number D-177883

Engineering Flow Diagram Numbers:
D-175012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	Valve is open only for smoke purge and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fail to open on receipt of CIAS phase A	Valve remains open; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	
Solenoid valve 3649B fails to vent (sticky operator)	Valve remains open; however, valve is normally closed except for smoke purging	Depending on initial valve position and plant operating status: a. Valve position indication at BOP panel b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at BOP panel b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 17 OF 18)

Component Identification 3649C

Logic Diagram Number NA

Elementary Number D-177883

Engineering Flow Diagram Numbers:
D-175012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-613 fails to operate on receipt of CIAS phase A	Valve remains open; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valve is open only for smoke purge and will fail closed on loss of instrument air
Contacts of ESF relay K-613 fail to open on receipt of CIAS phase A	Valve remains open; operator can close valve from main control board	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of 125 V-dc control power	Valve fails closed	a. Valve position light at main control board b. Computer c. Light monitor panel	
Solenoid valve 3696 fails to vent (sticky operator)	Valve remains open; however, the valve is normally closed except for smoke purging	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of instrument air	Valve fails closed	a. Valve position light at main control board b. Computer c. Light monitor panel	

FNP-FSAR-7

TABLE 7.3-8 (SHEET 18 OF 18)

Component Identification Control Room Pressurization Fan

Logic Diagram Number NA

Elementary Number D-177280 Sh. 3

Engineering Flow Diagram Numbers:
D-175012 Sh. 1 and D-205012 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-614 fails to operate on CIAS phase A, Units 1 or 2	Motor fails to start; of two pressurization fans, only one is required for operation; operator can start motor if necessary	a. Control room indication lights b. Periodic testing c. Light monitor panel	
Contacts of ESF relay K-614 fail to close on CIAS phase A	Motor fails to start; of two pressurization fans, only one is required for operation; operator can start motor if necessary	a. Control room indication lights b. Periodic testing c. Light monitor panel	
Loss of power to 600-V motor control center	Motor fails to start	a. Loss of both control room indication lights b. Periodic testing	
Loss of 120 V-ac control power	Motor fails to start	a. Loss of both control room indication lights b. Periodic testing	
Thermal overload relay contacts open	Motor fails to start	a. Control room indication lights b. Periodic testing c. Motor overload trip alarm in the control room	

FNP-FSAR-7

TABLE 7.3-9 (SHEET 1 OF 4)

FAILURE MODE AND EFFECTS ANALYSIS, PENETRATION ROOM FILTRATION SYSTEM

Component Identification Exhaust Fan
 Elementary Number D-177238/D-207238

Logic Diagram Number NA
 Engineering Flow Diagram Numbers:
D-175022 Sh. 1 and D-205022 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-626 fails to operate on CIAS phase B	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Contacts of ESF relay K-626 fail to close on CIAS phase B	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Loss of power to 600-V motor control center A	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Loss of 120 V-ac control power	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Thermal overload relay contacts open	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing d. Motor overload trip alarm at main control board	

FNP-FSAR-7

TABLE 7.3-9 (SHEET 2 OF 4)

Component Identification Recirculation Fan

Logic Diagram Number NA

Elementary Number D-177239/D-207239

Engineering Flow Diagram Numbers:
D-175022 Sh. 1 and D-205022 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-626 fails to operate on CIAS phase B	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Contacts of ESF relay K-626 fail to close on CIAS phase B	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Loss of power to 600-V motor control center A	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Loss of 120 V-ac control power	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing	
Thermal overload relay contacts open	Motor fails to start	a. Light monitor panel b. Indication lights at main control board c. Periodic testing d. Motor overload trip alarm at main control board	

FNP-FSAR-7

TABLE 7.3-9 (SHEET 3 OF 4)

Component Identification 3362A,B

Logic Diagram Number NA

Elementary Number D-177281/D-207281

Engineering Flow Diagram Numbers:
D-175022 Sh. 1 and D-205022 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
ESF relay K-626 train A or B fails to operate on receipt of CIAS phase B	Associated valve remains closed	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	Valve is normally closed
Contacts of ESF relay K-626 train A or B fail to close on receipt of CIAS phase B	Associated valve remains closed	Depending on initial valve position and plant operating status : a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	
Loss of power to 600-V motor control centers U-3362A and V-3362B	Associated valve fails as is; the other valve will open	a. Loss of valve position light at main control board b. Computer c. Light monitor panel	
Loss of 120 V-ac control power	Associated valve fails as is	Loss of valve position light at main control board	
Thermal overload relay contacts open	Associated valve fails as is	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	

FNP-FSAR-7

TABLE 7.3-9 (SHEET 4 OF 4)

Component Identification 3362A,B (cont.)

Logic Diagram Number NA

Elementary Number D-177281/D-207281

Engineering Flow Diagram Numbers:
D-175022 Sh. 1 and D-205022 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Failure of starter relay to operate	Valve fails as is	Depending on initial valve position and plant operating status: a. Valve position indication at main control board b. Light monitor panel c. Computer d. Periodic testing	

TABLE 7.3-10 (SHEET 1 OF 2)

FAILURE MODE AND EFFECTS ANALYSIS, AUXILIARY FEEDWATER SYSTEM

Component Identification Motor-Driven Auxiliary Feedwater PumpsLogic Diagram Number NAElementary Number D-177186 Sheets 1 & 2, D-207186 Sheets 1 & 2Engineering Flow Diagram Number:
D-175007 Sh. 1, D-205007 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 4.16-kV bus power to one pump	Failure of pump to start when required or automatic stoppage when pump is running	4.16-kV bus UV or bus breaker auto trip alarm on emergency power board	Redundant train pump can be started
Loss of 125 V-dc breaker control power	Inability of pump to start on manual or automatic signal, or trip the breaker when required	During periodic testing or observation of control switch red, green, and amber lights	Two motor-driven pumps are provided; one pump is sufficient to meet cooldown requirements
Failure of loss of power sequencer start or ESS sequencer start signals	Inability of pump to start upon receipt of automatic start signal	ESS malfunction alarm on main control board and periodic testing	Pump can be manually started from the main control board
Automatic breaker trip due to overcurrent	Redundant motor-driven pump is available	Breaker auto trip alarm on main control board	One out of two motor-driven pumps is required for cooldown

FNP-FSAR-7

TABLE 7.3-10 (SHEET 2 OF 2)

Component Identification Auxiliary Feedwater Flow Control Valves Logic Diagram Number NA
(HV-3227A, 3227B, and 3227C; HV-3228A, 3228B, and 3228C)

Elementary Number D-177591

Engineering Flow Diagram Number:
D-175007 Sh. 1, D-205007 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 125 V-dc power	Solenoid valve will deenergize and vent the main valve to open	Observation of valve position indicating lights or during monthly testing	Valve fails to the safe position required for cooldown of the RCS early in an accident: manual valve throttling is required for meeting system requirements later in the event.
Loss of primary air supply	Air bleeds from control valve and valve fails to the open	Observation of valve position indicating lights or during monthly testing	Valve fails to the safe position required for cooldown of the RCS early in an accident: manual valve throttling is required for meeting system requirements later in the event. (For HV-3227A/B/C only operator action is required to open emergency air supply isolation valves to restore modulation capability to these FCVs.)
Failure of open signal from ESS sequencer in one train	Valve is opened by redundant solenoid pilot operated by other train	Observation of valve position indicating lights or during monthly testing	

TABLE 7.3-11 (SHEET 1 OF 5)

FAILURE MODE AND EFFECTS ANALYSIS, EMERGENCY SAFEGUARDS PUMP ROOM COOLING SYSTEMComponent Identification Containment Spray Pump Room CoolersLogic Diagram Number NAElementary Number D-177227 Sh. 2, D-207227 Sh. 1Engineering Flow Diagram Numbers:
D-175011 Sh. 3, D-205011 Sh. 3

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 600-V motor control center A or B	Motor stops	a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal	Two spray pumps provided; each unit is provided with its own cooler and fan; emergency core cooling system analysis is based upon operation of one pump
Loss of 120 V-ac control power	Motor stops	a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal	
Thermal overload contacts open	Motor stops	a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal	

FNP-FSAR-7

TABLE 7.3-11 (SHEET 2 OF 5)

Component Identification Residual Heat Removal Pump Room Coolers

Logic Diagram Number NA

Elementary Number D-177227 Sh. 1, D-207227 Sh. 1

Engineering Flow Diagram Numbers:
D-175011 Sh. 3, D-205011 Sh. 3

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 600-V motor control center A or B	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	Two RHR pumps provided; each unit is provided with its own cooler and fan; emergency core cooling system analysis is based upon operation of one pump
Loss of 120 V-ac control power	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	
Thermal overload contacts open	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	

FNP-FSAR-7

TABLE 7.3-11 (SHEET 3 OF 5)

Component Identification Charging/HHSI Pump Room Cooler Fan Motors

Logic Diagram Number NA

Elementary Numbers D-177226, D-177229 Sh. 2, D-177284,
D-207226, D-207229, D-207284

Engineering Flow Diagram Numbers:
D-175011 Sh. 3, D-205011 Sh. 3

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 600-V motor control center A or B train dedicated pump rooms have corresponding train dedicated room coolers; swing pump room cooler can be aligned to either train A or Train B, depending on pumps alignment	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	Three charging/HHSI pumps provided; each unit is provided with its own cooler and fan; emergency core cooling system analysis is based upon operation of one pump
Loss of 120 V-ac control power	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	
Thermal overload contacts open	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Monitor light box abnormal 	

FNP-FSAR-7

TABLE 7.3-11 (SHEET 4 OF 5)

Component Identification Component Cooling Water Pump Room Coolers

Logic Diagram Number NA

Elementary Number D-177243 Sh. 1, D-207243 Sh. 1

Engineering Flow Diagram Numbers:
D-175011 Sh. 3, D-205011 Sh. 3

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 600-V motor control center	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	Three component cooling water pumps provided; there are two coolers for the three pumps; emergency core cooling system analysis is based upon operation of one pump
Loss of 120 V-ac control power	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	
Thermal overload contacts open	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Monitor light box abnormal 	

FNP-FSAR-7

TABLE 7.3-11 (SHEET 5 OF 5)

Component Identification Motor-Driven Auxiliary Feedwater Pump Room Coolers

Logic Diagram Number NA

Elementary Number D-177229 Sh. 1, D-207229 Sh. 1

Engineering Flow Diagram Numbers:
D-175011 Sh. 3, D-205011 Sh. 3

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 600-V motor control center A or B	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	Two MD auxiliary feedwater pumps provided; each unit is provided with its own cooler and fan; emergency core cooling system analysis is based upon operation of one pump
Loss of 120 V-ac control power	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	
Thermal overload contacts open	Motor stops	<ul style="list-style-type: none"> a. Fan fault alarm at main control board b. Loss of red/green indication lights at BOP panel c. Monitor light box abnormal 	

TABLE 7.3-12

**FAILURE MODE AND EFFECTS ANALYSIS,
BATTERY ROOM VENTILATION SYSTEM**

Component Identification Battery Room Exhaust FanLogic Diagram Number NAElementary Number D-177265 Sh. 1, D-207265 Sh. 1Engineering Flow Diagram Numbers:
D-175014 Sh. 1, D-205014 Sh. 1

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 208-V motor control center A or B	Fan stops	a. Loss of red/green indication lights at BOP Panel	One exhaust fan is provided for each battery room; one battery is required during post-LOCA operation; effect of loss of exhaust fan on hydrogen accumulation is discussed in paragraph 9.4.2.3.4
Loss of 120 V-ac control power	Fan stops	a. Loss of red/green indication lights at BOP Panel	
Thermal overload contacts open	Fan stops	a. Fan operating light out	

FNP-FSAR-7

TABLE 7.3-13

**FAILURE MODE AND EFFECTS ANALYSIS,
BATTERY ROOM AIR CONDITIONING SYSTEM**

Component Identification Battery Room Cooler

Logic Diagram Number NA

Elementary Number NA

Engineering Flow Diagram Number NA

See Table 9.4-6.

TABLE 7.3-14 (SHEET 1 OF 3)

**FAILURE MODE AND EFFECTS ANALYSIS,
EMERGENCY DIESEL GENERATOR**

Component Identification Diesel Generator Supply Breaker

Elementary Number D-172761, D-177142, and D-177143

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 125 V-dc control power	Loss of ability to tie diesel generator to bus when necessary	Loss of dc annunciator in control room	Redundant diesel generator will be started
Failure of 2AJX contacts to close in emergency	Loss of ability to tie diesel generator to bus when necessary	Incomplete sequence annunciator	Redundant diesel generator will be started
Failure of 59/81X contacts	Loss of ability to tie diesel generator to bus when necessary	Indicating light on control board	Redundant diesel generator will be started
Mechanical or electrical failure of breaker	Loss of ability to tie diesel generator to bus when necessary	Breaker position indicating lights in control room	Redundant diesel generator will be started

TABLE 7.3-14 (SHEET 2 OF 3)Component Identification Diesel Generator Start, Stop, and Shutdown ControlsElementary Numbers D-172774, D-172778, D-172782

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Loss of 125 V-dc control power	Loss of ability to start diesel generator in emergency	Annunciator and loss of indicating lights on board	Redundant diesel generator will be started
Failure of start contact in diesel starting circuit A or B to close in emergency	None; redundant starting circuit will start diesel	Testing	
Failure of a relay in starting circuit A or B	None; redundant starting circuit will start diesel	Testing	
Failure of signal contact or relay in diesel stop circuit	Loss of ability to stop diesel from control room	Diesel running light in control room	Diesel can be stopped manually
Failure of contact or relay in diesel shutdown circuit	Diesel would not shut down when trouble occurred	Observation of diesel failure	All safety features are cut out except overspeed and low oil pressure during emergency operation

TABLE 7.3-14 (SHEET 3 OF 3)Component Identification Diesel Generator Excitation and Miscellaneous ControlsElementary Numbers D-172775, D-172779, D-172783

<u>Failure Mode</u>	<u>Effect on System</u>	<u>Detection of Failure</u>	<u>Remarks</u>
Failure of governor control	Diesel generator may not pick up load or may drop load during load fluctuations	Observation of voltage and frequency on board	Redundant generator can be used
Failure of excitation circuit	Improper voltage output from generator	Observation of meter on board	Redundant generator can be used
Failure of auto voltage	Improper voltage output from generator	Observation of meter on board	Redundant generator manual voltage control can be used

TABLE 7.3-15 (SHEET 1 OF 6)

**FAILURE MODE AND EFFECTS ANALYSIS,
ENGINEERED SAFETY FEATURES ACTUATION SYSTEM**

Train A

<u>Component</u>	<u>Malfunction</u>	<u>Comment</u>
A1	Fail logic zero	Prevents manual reset and block of safety injection train A
	Fail logic one	Safety injection from train A not affected if failure occurs before safety injection is called for at M1; safety injection signal will be removed upon reactor trip indicated by P-4, safeguards sequencer must latch in and continue sequence If failure occurs after safety injection is called for at M1, safety injection signal will be reset; no effect provided safeguards sequencer latches in
A2	Fail logic zero	Prevents reset of safety injection if one of the four inputs to O4 is still calling for safety injection
	Fail logic one	Automatic safety injection actuation will be prevented; manual safety injection is still possible
A3	Fail logic zero	Automatic safety injection actuation train A will be prevented; manual safety injection train A is still possible
	Fail logic one	Spurious safety injection train A; no direct reactor trip
A4	Fail logic zero	Prevents high containment pressure safety injection actuation train A if called for
A5	Fail logic zero	Prevents low steam line pressure; safety injection actuation in train A if called for
	Fail logic one	Spurious safety injection; reactor trip and steam line isolation in train A
A6	Fail logic zero	Prevents steam line isolation on high steam line flow coincident with low-low T_{avg} (train A only)
	Fail logic one	Spurious steam line isolation in train A
A7	Fail logic zero	Prevents steam line isolation on high steam line flow coincident with low-low T_{avg} (train A only)
	Fail logic one	Spurious steam line isolation (train A) if false logic one output of A7 occurs coincident with low-low T_{avg}

FNP-FSAR-7

TABLE 7.3-15 (SHEET 2 OF 6)

<u>Component</u>	<u>Malfunction</u>	<u>Comment</u>
A8	Fail logic zero	Prevents train A safety injection actuation by low steam line pressure
	Fail logic one	Spurious safety injection and steam line isolation (train A) if false logic one output of A8 occurs coincident with low-low T_{avg}
A9	Fail logic zero	Prevents low-low T_{avg} and low steam line pressure safety injection block
	Fail logic one	Prevents low steam line pressure safety injection and steam line isolation actuation in train A if called for
A10	Fail logic zero	Partial protection for high steam line differential pressure lost, i.e., low pressure loop 1
	Fail logic one	Spurious train A safety injection and reactor trips
A11	Fail logic zero	Partial protection for high steam line differential pressure lost, i.e., low pressure loop 1
	Fail logic one	Spurious safety injection and reactor trip if false output occurs coincident with low (P-1, P-3) indicated by 2/3 logic at A12
A12	Fail logic zero	Partial protection for high steam line differential pressure lost, i.e., low pressure loop 1
	Fail logic one	Spurious safety injection and reactor trip if false output occurs coincident with low (P-1, P-2) indicated by 2/3 logic at A11
A13	Fail logic zero	Partial protection for high steam line differential pressure lost, i.e., low pressure loop 2
	Fail logic one	Spurious safety injection train A and reactor trip
A14	Fail logic zero	Loss of protection against high steam line differential pressure, i.e., low pressure loop 2
	Fail logic one	Spurious safety injection and reactor trip if false output occurs coincident with low (P-2, P-3) indicated by 2/3 logic at A15
A15	Fail logic zero	Loss of protection against high steam line differential pressure, i.e., low pressure loop 2
	Fail logic one	Spurious safety injection and reactor trip if false output occurs coincident with high (P-1, P-2) indicated by 2/3 logic at A14
A16	Fail logic zero	Partial protection for high steam line differential pressure lost, i.e., low pressure loop 3
	Fail logic one	Spurious safety injection train A and reactor trip

FNP-FSAR-7

TABLE 7.3-15 (SHEET 3 OF 6)

<u>Component</u>	<u>Malfunction</u>	<u>Comment</u>
A17	Fail logic zero	Loss of protection against high steam line differential pressure lost, i.e., low pressure loop 3
	Fail logic one	Spurious safety injection and reactor trip if false output occurs coincident with high (P-1, P-3) indicated by 2/3 logic at A18
A18	Fail logic zero	Loss of protection against high steam line differential pressure lost, i.e., low pressure loop 3
	Fail logic one	Spurious safety injection and reactor trip if false output occurs coincident with high (P-2, P-3) indicated by 2/3 logic at A17
A19	Fail logic zero	Prevents train A low pressurizer pressure safety injection and reactor trip actuation if called for
	Fail logic one	Spurious safety injection and reactor trip
A20	Fail logic zero	Prevents train A low pressurizer pressure safety injection and reactor trip
	Fail logic one	Spurious safety injection and reactor trip train A if not blocked
A21	Deleted	
A22	Deleted	
A23	Fail logic zero	Prevents pressurizer safety injection block
	Fail logic one	Prevents train A low pressurizer pressure safety injection and reactor trip actuation if called for
A24	Fail logic zero	Allows train A safety injection blocks when no block is called for
	Fail logic one	Prevents pressurizer safety injection block

FNP-FSAR-7

TABLE 7.3-15 (SHEET 4 OF 6)

<u>Component</u>	<u>Malfunction</u>	<u>Comment</u>
A25	Fail logic zero	Prevents steam line safety injection block of low steam line pressure; also prevents train A steam line isolation due to high steam line flow coincident with low-low T_{avg}
	Fail logic one	Allows operator to block safety injection whether or not block should be allowed; if safety injection is not blocked and false output occurs coincident with low steam line pressure, spurious safety injection would result
		Spurious steam line isolation would occur if high steam line flow (2/3) occurs
O1	Fail logic zero	Prevents safety injection actuation train A
	Fail logic one	Spurious safety injection; no direct reactor trip
O2	Fail logic zero	Prevents reset of safety injection if one of the four inputs to O4 is still calling for safety injection
	Fail logic one	Safety injection actuation from train A not affected if failure occurs after safety injection is called for at M1; if failure occurs before safety injection actuation, train A safety injection can be spuriously blocked (if P-4 is also logic one)
O3	Fail logic zero	Prevents manual safety injection actuation train A
	Fail logic one	Spurious reactor trip and safety injection train A
O4	Fail logic zero	Automatic safety injection actuation train A will be prevented; manual safety injection train A is still possible
	Fail logic one	Spurious reactor trip; spurious safety injection train A if safety injection has not been manually blocked
O5	Fail logic zero	Loss of protection in train A against high steam line flow in loop 1; logic at A7 changed to 2/2
	Fail logic one	Logic at A7 changed to 1/2
O6	Fail logic zero	Loss of protection in train A against high steam line flow in loop 2; logic at A7 changed to 2/2
	Fail logic one	Logic at A7 changed to 1/2
O7	Fail logic zero	Loss of protection in train A against high steam line flow in loop 3; logic at A7 changed to 2/2
	Fail logic one	Logic at A7 changed to 1/2

FNP-FSAR-7

TABLE 7.3-15 (SHEET 5 OF 6)

<u>Component</u>	<u>Malfunction</u>	<u>Comment</u>
O8	Deleted not necessary	
O9	Fail logic zero	Prevents safety injection block and allows spurious safety injection and steam line isolation if in coincidence with low steam line pressure
	Fail logic one	Blocks safety injection (train A) if low steam line pressure occurs coincident with low-low T_{avg} ; safety injection is not prevented if low steam line pressure occurs alone (not in coincidence with low-low T_{avg})
O10	Fail logic zero	Prevents train A high steam line differential pressure safety injection and reactor trip actuation
	Fail logic one	Spurious safety injection and reactor trip
O11	Deleted	
O12	Fail logic zero	Prevents pressurizer safety injection block
	Fail logic one	Blocks pressurizer safety injection if failure occurs coincident with P-11 (-1)
O13	Fail logic zero	Prevents safety injection from actuating reactor trip
	Fail logic one	Spurious reactor trip
O14	Fail logic zero	Prevents steam line isolation actuation of high steam line flow coincident with low-low T_{avg} and prevents steam line isolation of low steam line pressure when safety injection is called for
	Fail logic one	Spurious steam line isolation actuation
N1	Fail logic zero	Safety injection will be blocked at A3 although no attempt to reset has taken place
	Fail logic one	Prevents safety injection block at A3 when resetting
N2	Fail logic zero	Blocks safety injection actuation (train A) of low steam line pressure when no block is called for
	Fail logic one	Fails to block safety injection when block is called for
N3	Fail logic zero	Prevents steam line safety injection block
	Fail logic one	Prevents manual reset of steam line safety injection block control; allows continuous block

FNP-FSAR-7

TABLE 7.3-15 (SHEET 6 OF 6)

<u>Component</u>	<u>Malfunction</u>	<u>Comment</u>
N4	Fail logic zero	Blocks train A safety injection actuation due to low pressurizer pressure coincident with low pressurizer level when no block is called for
	Fail logic one	Prevents manual block
N5	Fail logic zero	Prevents operator block of safety injection and reactor trip train A when block should occur
	Fail logic one	Allows operator block of safety injection and reactor trip train A when block should not be allowed
N6	Fail logic zero	Prevents pressurizer safety injection block
	Fail logic one	Prevents manual reset of pressurizer safety injection block control; allows continuous block
TD1	Fail logic zero	Prevents manual reset and block
	Fail logic one	
	Short time delay	Allows resetting of safety injection train A before safety injection sequence time delay has been completed
	Constant output	Allows a manual block and reset at any time
M1	Fail logic zero	Prevents safety injection train A
	Fail logic one	Spurious safety injection train A; prevents reset of safety injection signal
Bistable inputs to solid state protection	Any one bistable input fails logic one	Protection ensured by operation of other bistable inputs in the same system (coincidence changed from 2/3 to 1/2, etc.)
	Any one bistable input to solid state protection fails logic zero	Protection ensured by operation of other bistable inputs in the same system (coincidence changed from 2/3 to 2/2, etc.)

TABLE 7.3-16 (SHEET 1 OF 3)

ENGINEERED SAFETY FEATURES RESPONSE TIMES

<u>Initiating Signal and Function</u>	<u>Response Time (s)</u>
1. <u>Manual</u>	
a. Safety injection (ECCS)	NA
Feedwater isolation	NA
Reactor trip (SI)	NA
Containment isolation-Phase "A"	NA
Containment purge isolation	NA
Auxiliary feedwater pumps	NA
Service water system	NA
Containment air coolers	NA
b. Containment spray	NA
Containment isolation-Phase "B"	NA
Containment purge isolation	NA
c. Containment isolation-Phase "A"	NA
Containment purge isolation	NA
d. Steam line isolation	NA
2. <u>Containment Pressure-High</u>	
a. Safety injection (ECCS)	$\leq 27.0^{(a)}$
b. Reactor trip (from SI)	≤ 2.0
c. Feedwater isolation	$\leq 32.0^{(f)}$
d. Containment isolation-Phase "A"	$\leq 17.0^{(d)}/27.0^{(e)}$
e. Containment purge isolation	≤ 5.0
f. Auxiliary feedwater pumps	NA
g. Service water system	$\leq 100.0^{(d)}/110.0^{(e)}$
h. Containment air cooler fan	≤ 27.4
3. <u>Pressurizer Pressure-Low</u>	
a. Safety injection (ECCS)	$\leq 27.0^{(a)}/12.0^{(d)}$
b. Reactor trip (from SI)	≤ 2.0
c. Feedwater isolation	$\leq 32.0^{(f)}$
d. Containment isolation-Phase "A"	$\leq 17.0^{(d)}/27.0^{(e)}$
e. Containment purge isolation	≤ 5.0
f. Auxiliary feedwater pumps	NA
g. Service water system	$\leq 100.0^{(d)}/110.0^{(a)}$
4. <u>Differential Pressure Between Steam Lines-High</u>	
a. Safety injection (ECCS)	$\leq 12.0^{(d)}/22.0^{(e)}$
b. Reactor trip (from SI)	≤ 2.0
c. Feedwater isolation	$\leq 32.0^{(f)}$
d. Containment isolation-Phase "A"	$\leq 17.0^{(d)}/27.0^{(e)}$
e. Containment purge isolation	NA
f. Auxiliary feedwater pumps	NA
g. Service water system	$\leq 100.0^{(d)}/110.0^{(e)}$

TABLE 7.3-16 (SHEET 2 OF 3)

<u>Initiating Signal and Function</u>	<u>Response Time (s)</u>
5. <u>Steam Flow in Two Steam Lines-High Coincident with Tavg--Low-Low</u>	NA
a. Steam line isolation	NA
6. <u>Steam Line Pressure-Low</u>	$\leq 12.0^{(d)}/22.0^{(e)}$
a. Safety injection (ECCS)	≤ 2.0
b. Reactor trip (from SI)	$\leq 32.0^{(f)}$
c. Feedwater isolation	$\leq 17.0^{(d)}/27.0^{(e)}$
d. Containment isolation-Phase "A"	NA
e. Containment purge isolation	NA
f. Auxiliary feedwater pumps	$\leq 100.0^{(d)}/110.0^{(e)}$
g. Service water system	≤ 9.0
h. Steam line isolation	≤ 9.0
7. <u>Containment Pressure--High-High</u>	≤ 9.0
a. Steam line isolation	≤ 9.0
8. <u>Containment Pressure--High-High-High</u>	$\leq 14^{(h)}/\leq 27^{(i)}/\leq 33^{(j)}$
a. Containment spray	NA
b. Containment isolation-Phase "B"	NA
9. <u>Steam Generator Water Level--High-High</u>	≤ 2.5
a. Turbine trip	$\leq 32.0^{(f)}$
b. Feedwater isolation	$\leq 32.0^{(f)}$
10. <u>Steam Generator Water Level--Low-Low</u>	≤ 60.0
a. Motor-driven auxiliary feedwater pumps(b)	≤ 60.0
b. Turbine-driven auxiliary feedwater pump (c)	≤ 60.0
11. <u>Undervoltage RCP</u>	≤ 60.0
a. Turbine-driven auxiliary feedwater pump	≤ 60.0
12. <u>S.I. Signal</u>	≤ 60.0
a. Motor-driven auxiliary feedwater pumps	≤ 60.0
13. <u>Trip of Main Feedwater Pumps</u>	NA
a. Motor-driven auxiliary feedwater pumps	NA
14. <u>Loss of Power</u>	(g)
a. 4.16-kV emergency bus undervoltage (Loss of Voltage)	(g)
b. 4.16-kV emergency bus undervoltage (Degraded Voltage)	(g)

a. Diesel generator starting and sequence loading delays included. Response time limit includes opening of valves to establish SI path and attainment of discharge pressure for centrifugal charging pumps and RHR pumps.

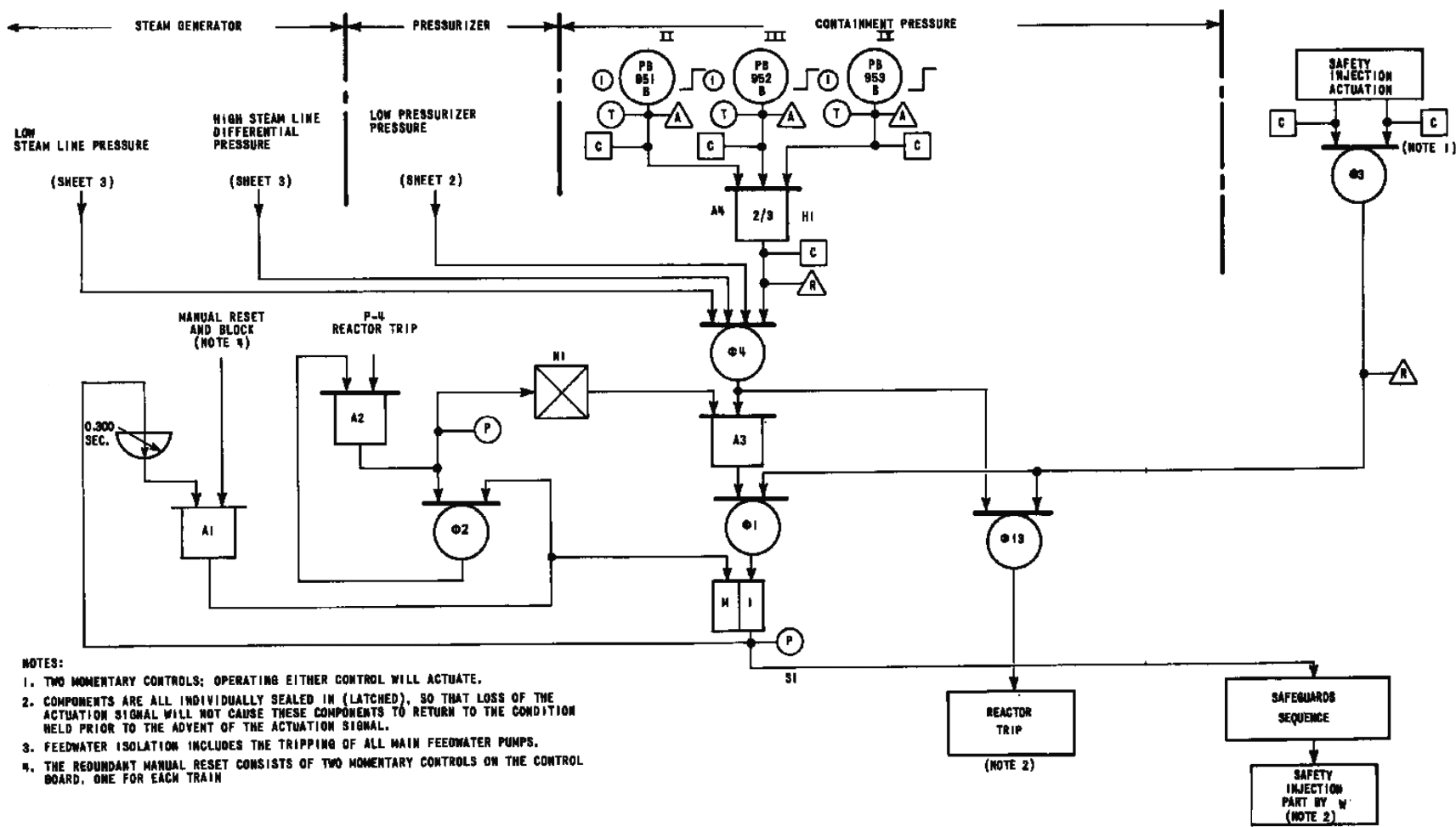
b. One 2/3 any steam generator.

c. On 2/3 in 2/3 steam generators.

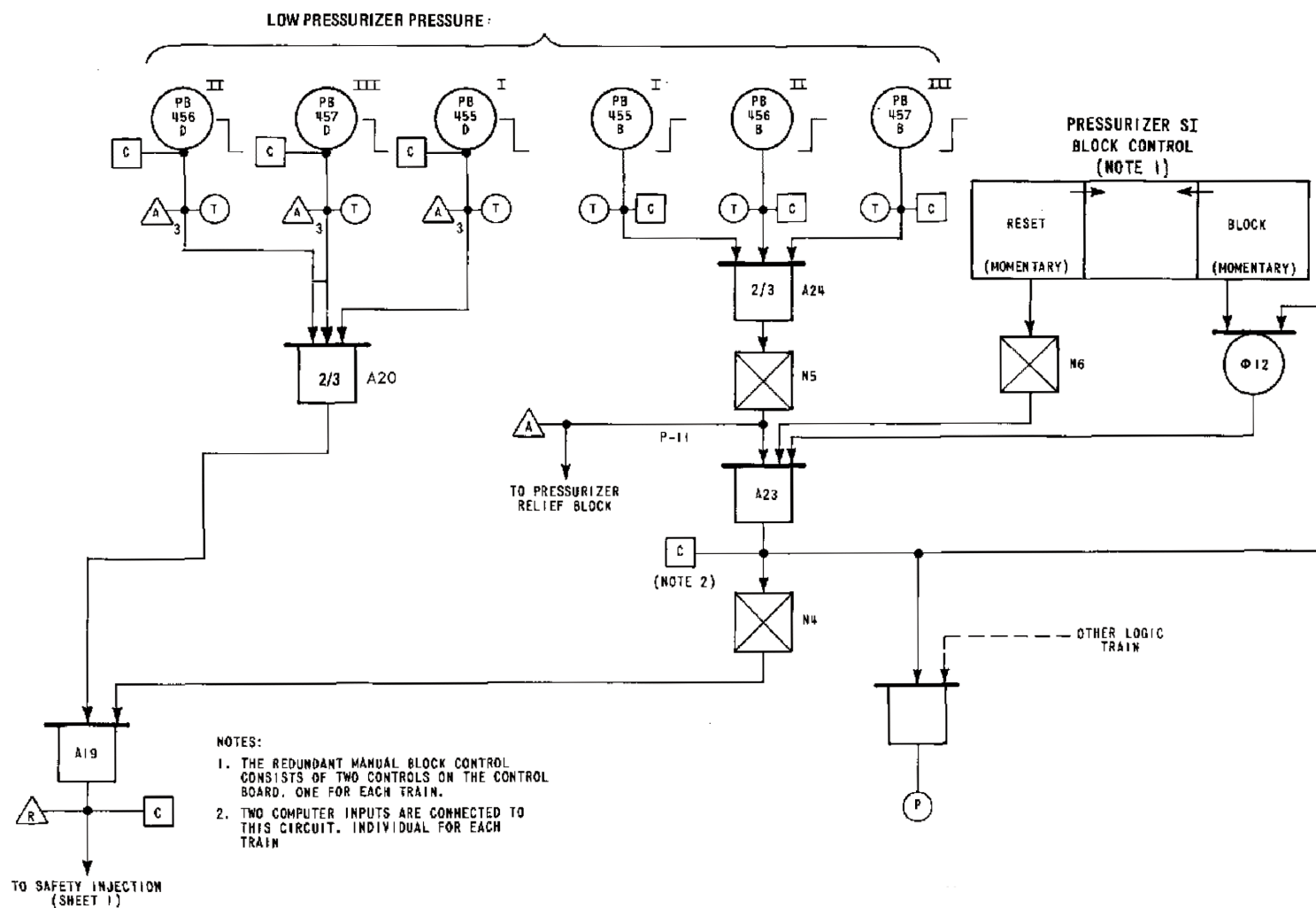
d. Diesel generator starting and sequence loading delay not included. Offsite power available. Response time limit includes opening of valves to establish SI path and attainment of discharge pressure for centrifugal charging pumps.

TABLE 7.3-16 (SHEET 3 OF 3)

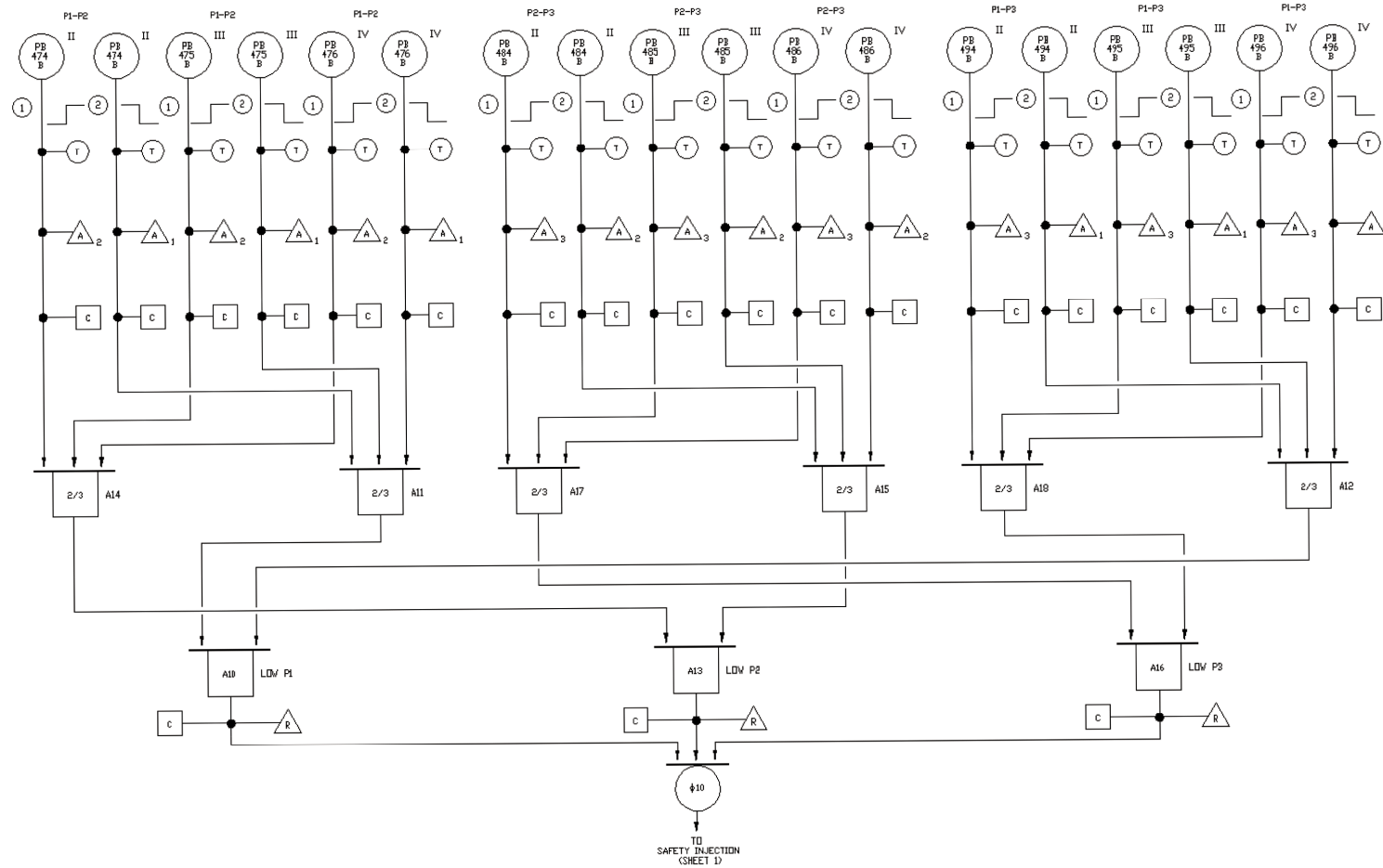
- e. Diesel generator starting and sequence loading delays included. Response time limit includes opening of valves to establish SI path and attainment of discharge pressure for centrifugal charging pumps.
- f. Verification shall include testing of all instrumentation, the isolation valves (MOV-3232A, 3232B, 3232C), and the control valves (FCV-478, 479, 488, 489, 498, 499). The isolation valves must function within 30 s and the control valves within 5 s.
- g. The response time shall include the time delay associated with the undervoltage relays as determined by the appropriate relay setting sheet calibration requirements plus an additional second associated with interposing relay and circuit operation.
- h. Diesel generator starting and sequence loading delays not included. Response time includes containment HI-3 signal generation and signal processing delays, opening of valves to establish a flow path, and attainment of discharge pressure for the pumps.
- i. Diesel generator starting and step 2 sequence loading delays included. (Containment HI-3 signal generation and signal processing occur prior to ESS loading timer step 2; therefore, these HI-3 signal delays are not included.) Response time includes LOSP signal generation and signal processing delay, opening of valves to establish a flow path, and attainment of discharge pressure for the pumps.
- j. Step 6 sequence loading delays included. (Containment HI-3 signal generation and signal processing occur just after ESS loading timer step 2; therefore, the diesel generator start and step 2 sequence loading delays are not included.) Response time includes timer step 6 and the associated time delay pickup (less the time delay for timer step 2), containment HI-3 signal generation and signal processing, opening of valves to establish a flow path, and attainment of discharge pressure for the pumps.



REV 21 5/08

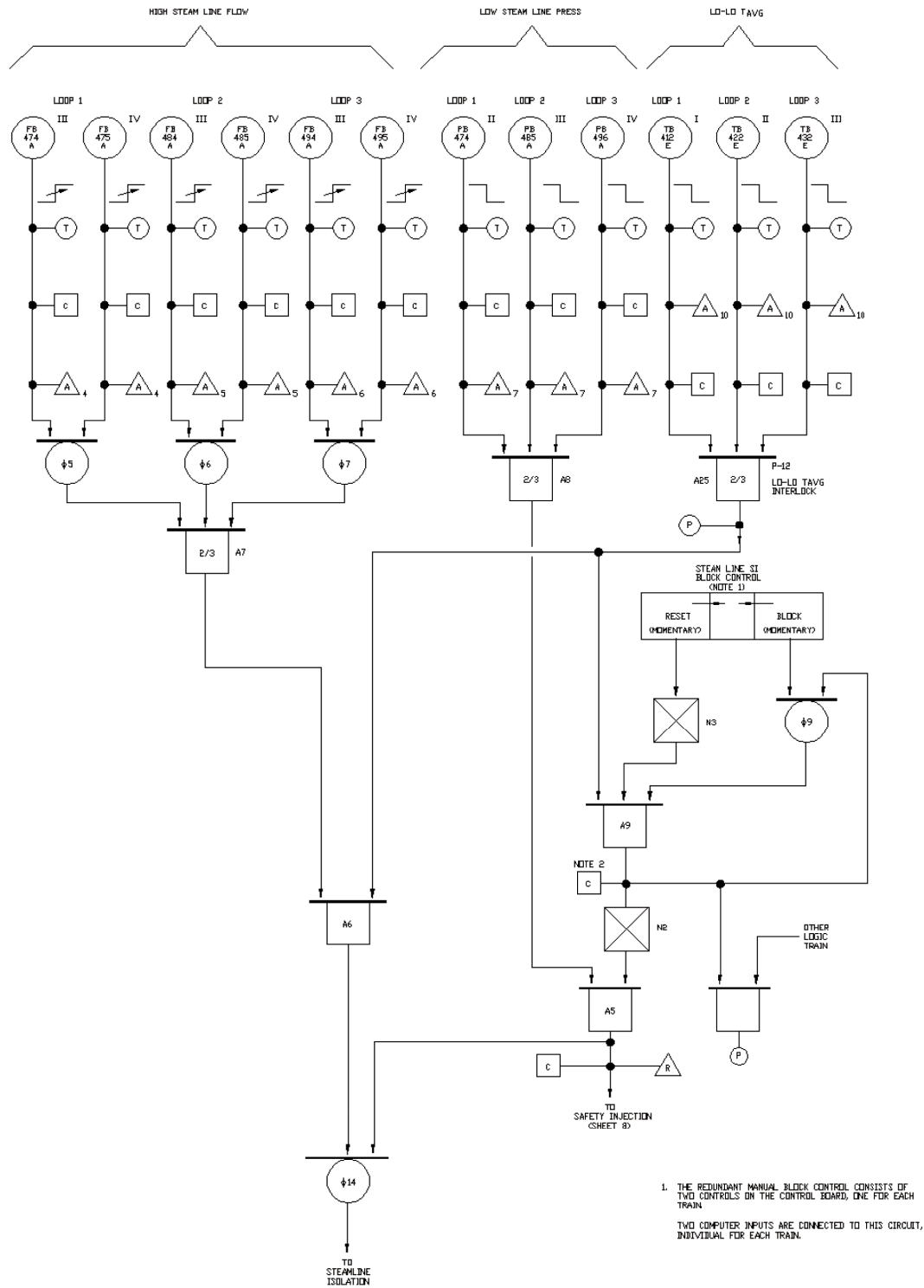


REV 21 5/08



REV 21 5/08

7000-3



REV 21 5/08

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

The functions necessary for safe shutdown are available from instrumentation channels that are associated with the major systems in both the primary and secondary sides of the nuclear steam supply system. These channels are normally aligned to serve a variety of operational functions, including startup and shutdown as well as protective functions. In achieving a safe shutdown, benefit is taken from many of these systems and equipment having multiple functions, and as such there are no specifically identifiable safe shutdown systems per se. However, prescribed procedures for securing and maintaining the plant in a safe condition can be instituted by appropriate alignment of selected nuclear steam supply systems. The discussion of these systems and the applicable codes, criteria, and guidelines are to be found in other sections of the report. In addition, the alignment of shutdown functions associated with the engineered safety features, which are invoked under postulated limiting fault situations, is discussed in chapter 6 and section 7.3.

The instrumentation and control functions which are identified as being required for maintaining safe shutdown of the reactor are by definition the minimum required under nonaccident conditions. (Control room inaccessibility as well as offsite power interruptions during a hot shutdown are considered as incidents.)

These functions will permit the necessary operations that will:

- A. Prevent the reactor from achieving criticality in violation of the plant technical specifications.
- B. Provide an adequate heat sink such that design and safety limits are not exceeded.

7.4.1 DESCRIPTION

The designation of systems that can be used for safe shutdown depends on identifying those systems which provide the following capabilities for maintaining a safe shutdown:

- A. Boration with related charging and letdown.
- B. Adequate supply for auxiliary feedwater.
- C. Residual heat removal.

These systems and the associated instrumentation and controls provisions are identified in the following lists. The identification of the monitoring indicators (paragraph 7.4.1.1) and controls (paragraph 7.4.1.2) are those necessary for maintaining a hot shutdown. The essential services for the capabilities necessary for maintaining a hot shutdown are listed in paragraph 7.4.1.3, with the equipment and services available for a cold shutdown identified in paragraphs 7.4.1.4 and 7.4.1.5.

See subsection 7.1.4 and Table 7.1-1 for a list of supplemental drawings.

Periodic testing of remote shutdown system instrumentation and controls is conducted in accordance with the Technical Specifications.

7.4.1.1 Monitoring Indicators

The characteristics of these indicators, which are provided outside as well as inside the control room, are described in Section 7.5. The necessary indicators are as follows:

- A. Water level indicator for each steam generator.
- B. Pressure indicator for each steam generator.
- C. Pressurizer water level indicator.
- D. Pressurizer pressure indicator.
- E. Reactor coolant loop 1 hot leg temperature.
- F. Reactor coolant loop 1 cold leg temperature.
- G. Neutron flux.
- H. Condensate storage tank level.

7.4.1.2 Controls

7.4.1.2.1 General Considerations

- A. The turbine is tripped. (Note that this can be accomplished at the turbine as well as in the control room.)
- B. The reactor is tripped. (Note that this can be accomplished at the reactor trip switchgear as well as in the control room.)
- C. All automatic systems continue functioning. (These are discussed in Sections 7.2 and 7.7.)
- D. For equipment having motor controls outside the control room (which duplicate the functions inside the control room), the controls will be provided with a selector switch which transfers control of the switchgear from the control room to a selected local station. Placing the local selector switch in the local operating position will give an annunciating alarm in the control room and will turn off the motor control position lights on the control room panel.

7.4.1.2.2 Pumps

A. Auxiliary Feedwater Pumps

Auxiliary feedwater pumps (electric) will start automatically on the loss of both main feedwater pumps. Start/stop motor controls positioned locally (and inside the control room) as well as handwheel control for the valves are provided. It is noted below that emergency power is available from the diesels which can be started locally and that the loads such as valves and pumps will be sequenced as necessary.

B. Charging and Boric Acid Transfer Pumps

Start/stop motor controls are provided for these pumps. The controls for the charging and boric acid pumps are positioned locally (and in the control room).

C. Service Water Pumps

These pumps, by means of the onsite power system, will start automatically following a loss of normal electrical power. Start/stop motor controls located outside and inside the control room will be provided.

D. Component Cooling Water Pumps

These pumps, energized from the diesel generator, start automatically following a loss of normal electrical power. Start/stop controls located outside and inside the control room are provided.

E. Instrument Air Compressors

These compressors start automatically on low air pressure.

F. Reactor Containment Fan Cooler Units

Start/stop motor controls with a selector switch are provided for the fan motors. The controls are located outside and inside the control room.

G. Control Room Ventilation Unit Including the Control Room Air Inlet Dampers

A start/stop switch located outside the control room is provided for this unit(s). Also a control to close the inlet air damper(s) is provided. These controls duplicate functions inside the control room.

7.4.1.2.3 Diesels

These units start automatically following a loss of normal ac power. However, manual controls for diesel startup are also provided locally at the diesel generators (as well as in the control room), and loading is sequenced automatically.

7.4.1.2.4 Valves

A. Charging Flow Control Valves

Manual control with a selector switch outside the control room is provided for the charging line flow control valves. This control duplicates functions available in the control room.

B. Letdown Orifice Isolation Valves

Open/close controls with a selector switch for the letdown orifice isolation valves are grouped with the controls for the charging flow control valve. These controls duplicate functions that are inside the control room.

C. Auxiliary Feedwater Control Valves

Manual control is provided in the auxiliary feedwater pump area that duplicates functions that are inside the control room. A handwheel is also provided for each valve.

D. Atmospheric Steam Relief Valves

Atmospheric relief valves are automatically controlled. Manual control is provided locally and inside the control room for the atmospheric relief valves. A handwheel is also provided for each valve.

E. Auxiliary Feedwater Pump Speed Control

Manual speed control (mechanical device) is provided locally and in the control room for the steam-driven auxiliary feedwater pump.

F. Pressurizer Heater Control

On/off control with selector switches are provided for two backup heater groups. The heater group will be connected to separate buses, such that each can be connected to separate diesels in the event of loss of outside power.

The control is grouped with the charging flow controls and duplicates functions available in the control room.

It is noted that the instrumentation and controls listed in subsections 7.4.1.1 and 7.4.1.2 for achieving and maintaining a safe shutdown are available in the event an evacuation of the control room is required. Cable routing of key instrumentation loops will allow the plant to be brought to hot standby from the hot shutdown panel with the loss of either the cable spreading room, control room, or a cable chase. These controls and instrumentation channels, with the equipment and services identified in subsections 7.4.1.3 and 7.4.1.4 which are available for both hot and cold shutdown, identify the potential capability for cold shutdown of the reactor subsequent to a control room evacuation through the use of suitable procedures. Therefore, the applicable requirements of 1971 General Design Criterion 19 are met.

7.4.1.3 Essential Services after Incident That Requires Hot Shutdown

- A. Auxiliary feedwater pumps which start automatically within 1 min for blackout condition. (See chapter 10.)
- B. Reactor containment air recirculation fans and coolers. (See chapter 6.)
- C. Diesel generators, loaded within 1 min. (See chapter 8.)
- D. Lighting in the areas of plant required during this condition. (See subsection 9.5.3.)
- E. Pressurizer heaters. (See chapter 5.)
- F. Communication network (see subsection 9.5.2) to be available for prompt use between feedwater pumps area and the following areas:
 - 1. Feedwater source from outside.
 - 2. Charging pump.
 - 3. Boric acid transfer pump.
 - 4. Diesel generator.
 - 5. Switchgear room.
 - 6. Steam relief valves.
- G. Boric acid transfer pumps. (See chapter 9.)
- H. Charging pumps. (See chapter 9.)
- I. Service water pumps. (See chapter 9.)
- J. Component cooling pumps. (See chapter 9.)
- K. Instrument air compressors. (See chapter 9.)
- L. Control room ventilation unit and air inlet damper. (See chapter 9.)

7.4.1.4 Equipment and Systems Available for Cold Shutdown

- A. Reactor coolant pump. (See chapter 5.)^(a)
- B. Auxiliary feedwater pumps. (See chapter 10.)
- C. Boric acid transfer pump. (See chapter 9.)
- D. Charging pumps. (See chapter 9.)
- E. Service water pumps. (See chapter 9.)
- F. Containment fans. (See chapter 6.)
- G. Control room ventilation. (See chapter 9.)
- H. Component cooling pumps. (See chapter 9.)
- I. Residual heat removal pumps. (See chapter 5.)^(a)
- J. Motor control center and switchgear sections associated with above loads.
- K. Controlled steam release and feedwater supply. (See section 7.7 and chapter 10.)
- L. Boration capability. (See chapter 9.)
- M. Nuclear instrumentation system (source range and intermediate range). (See sections 7.2 and 7.7.)^(a)
- N. Reactor coolant inventory control (charging and letdown). (See chapter 9.)
- O. Pressurizer pressure control including opening control for pressurizer relief valves (heaters and spray). (See chapter 5.)^(a)

In addition, the safety injection signal trip circuit must be defeated and the accumulator isolation valves closed.^(a) The performance of the emergency core cooling system under these conditions was evaluated. Conditions during plant cooldown were divided into the following four

a. Instrumentation and controls for these systems may require some modification in order that their functions may be performed from outside the control room. Note that the reactor plant design does not preclude attaining the cold shutdown condition from outside the control room. An assessment of plant conditions can be made on a long term basis (a week or more) to establish procedures for making the necessary physical modifications to instrumentation and control equipment in order to attain cold shutdown. During such time the plant could be safely maintained at hot shutdown condition.

Detailed procedures to be followed in effecting cold shutdown from outside the control room are best determined by plant personnel at the time of the postulated incident.

phases: (1) from operating reactor coolant pressure to 1900 psig, (2) from 1990 to 1000 psig, (3) from 1000 to 400 psig, and (4) from 400 psig to cold shutdown. The break size used in the analysis was determined using the moderate energy line break criteria identified in Branch Technical Positions APCSB 3-1 and MEB 3-1. Based on the analysis, the available emergency core cooling system can cool the core under plant cooldown conditions and, therefore, meets the NRC acceptance criteria, as applicable, contained in 10 CFR 50.46 and 10 CFR 50, Appendix K.

7.4.2 ANALYSIS

Hot shutdown is a stable plant condition, automatically reached following a plant shutdown. The hot shutdown condition can be maintained safely for an extended period of time either automatically or manually. In the unlikely event that access to the control room is restricted, the plant can be safely kept at a hot shutdown until the control room can be reentered by the use of the monitoring indicators and the controls listed in paragraphs 7.4.1.1 and 7.4.1.2. These indicators and controls are provided outside and inside the control room. The safety evaluation of the maintenance of a shutdown with these systems and associated instrumentation and controls has included consideration of the accident consequences that might jeopardize safe shutdown conditions. The accident consequences that are germane are those that would tend to degrade the capabilities for boration, adequate supply for auxiliary feedwater, and residual heat removal.

The results of the accident analyses are presented in chapter 15. Of these the following produce the most severe consequences that are pertinent:

- A. Uncontrolled boron dilution.
- B. Loss of normal feedwater.
- C. Loss of external electrical load and/or turbine trip.
- D. Loss of all ac power to the station auxiliaries (station blackout).

It is shown by these analyses that safety is not compromised by these incidents, with the associated assumptions being that the instrumentation and controls indicated in paragraphs 7.4.1.1 and 7.4.1.2 are available to control and/or monitor shutdown. These available systems will allow a maintenance of hot shutdown even under the accident conditions listed above which would tend toward a return to criticality or a loss of heat sink.

7.5 POSTACCIDENT MONITORING DISPLAY INSTRUMENTATION

7.5.1 DESCRIPTION

Table 7.5-1 lists the instrumentation provided to the operator to perform necessary functions, assess plant conditions, and verify system performance during accident situations. Listed below are the five classifications of variables that have been identified to provide this instrumentation.

- Type A: Those variables to be monitored that provide the primary information required to permit the control room operators to take the specified manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety function for design basis accident events.
- Type B: Those variables to be monitored that provide to the control room operator information to assess the process of accomplishing or maintaining critical safety functions.
- Type C: Those variables to be monitored that provide to the control room operator information to monitor (1) the extent to which parameters, which have the potential for causing a breach of the primary reactor containment or fuel cladding, have exceeded the design basis values, or (2) that the in-core fuel clad, the reactor coolant system pressure boundary or the primary reactor containment may have been breached.
- Type D: Those variables that provide information to indicate the operation of individual safety systems and other systems important to safety.
- Type E: Those variables that are to be monitored as required for use in determining the magnitude of the release of radioactive materials and in continuously assessing such releases.

These variables are subdivided into three categories which define the qualification requirements of the instrumentation. Table 7.5-1 identifies the variable category identified in the R. G. 1.97 Compliance Report. The qualification and configuration requirements and the Farley Evaluation Criteria for specific R. G. 1.97 requirements are described in the Design and Qualification Review Criteria section of the R. G. 1.97 Compliance Report.

The instrumentation channels that provide the information for the variables listed in Table 7.5-1, are powered as described in the R. G. 1.97 Compliance Report, and are energized from the onsite electrical power supplies as described in chapter 8.

Table 7.5-3 lists the information available to the operator for monitoring conditions in the reactor, in the reactor coolant system, and in the containment and process systems throughout all normal operating conditions of the plant, including anticipated operational occurrences.

Post-accident monitoring instrumentation is discussed in the Technical Specifications.

Containment hydrogen monitoring instrumentation surveillance is discussed in FSAR section 16.1.

7.5.2 ANALYSIS

With the issuance of Regulatory Guide 1.97, Alabama Power Company performed a comprehensive review and issued a R. G. 1.97 Compliance Report documenting Farley's commitment to R. G. 1.97.

The display instrumentation for postaccident monitoring enables the required manual functions to be performed following a Condition II, III, or IV event to provide the necessary information to maintain the plant at a safe hot shutdown or to proceed to a cold shutdown condition consistent with the technical specification limits. Other design criteria used in the display system are given at the end of this section.

All commitments concerning recording, separation, qualification, and redundancy are provided in the R. G. 1.97 Compliance Report.

For postaccident scenarios (see table 7.5-1), sufficient duplication of information is provided to ensure that the minimum information required will be available. The information is part of the operational monitoring of the plant which is under surveillance by the operator during normal plant operation. This is functionally arranged on the control board to provide the operator with ready understanding and interpretation of plant conditions. Comparisons between duplicate information channels or between functionally related channels will enable the operator to readily identify a malfunction in a particular channel.

It is noted that there is a degree of functional redundancy between those display channels that are required for postaccident monitoring and many other diverse instrumentation channels which are also located on the main control board. For example, after the actuation of safety injection, the residual heat removal pump flow, high head (charging) pump flow, and spray pump flow can be verified by their respective flow channels. The transmitters for these flow channels are outside the containment. In addition, the containment sump level is continuously read out on the main control board. This information provides a diverse means for checking refueling water storage tank level data obtained from the safety-related display information.

Channel separation is provided between sensors and the process cabinets. From the process cabinets to the main control board, the interconnecting circuits meet the separation requirements between safety trains, with two channels being associated with one train.

The design criteria used in the display system are listed below:

- A. Range and accuracy requirements are determined through the analyses of postaccident conditions as described in chapter 15. The display system meets the following requirement: the range of the readouts extends over the maximum expected range of the variable being measured.
- B. Power for the display instruments is obtained from the instrumentation and control power supply system. This system is described in section 7.6 and complies with

paragraph 5.4 of the Institute of Electrical and Electronics Engineers standard 308.

- C. Those channels determined to provide useful information in charting the course of events are recorded.

7.5.3 DELETED

7.5.4 INADEQUATE CORE COOLING MONITORING SYSTEM

The inadequate core cooling monitoring system (ICCMS) is a safety grade processing and display system which meets the NRC requirements to provide the capability to monitor the approach to, existence of, and recovery from potential reactor core inadequate core cooling situations. The requirements addressed by the ICCMS are defined in paragraph II.f.2 of NUREG 0737, "Clarification of TMI Action Plan" and Generic Letter 82-28. Inadequate core cooling monitoring requirements are met by measuring and displaying margin to saturation, reactor vessel water level above the core, and core exit temperatures.

7.5.4.1 Reactor Vessel Level

The redundant heated junction thermocouple (HJTC) probes are described in paragraph 4.4.5.5. Redundant processors are located in the control room. Redundant level indication is provided on a reactor vessel mimic display on the main control board. The mimic indicates covered or uncovered for each of the eight heated junctions for each probe. The mimic background shows the elevation of each sensor and its location in the reactor vessel in relation to major components and penetrations.

The redundant signal processors, one per HJTC probe, monitor the HJTC probe thermocouples, control power to the HJTC probe heaters, and drive the level displays. The processor HJTC calculations are as follows:

The differential temperature (ΔT) is calculated from the temperature values for the unheated junction (T_u) and the heated junction (T_H) thermocouple inputs. ΔT is equal to T_H minus T_u , and that ΔT is compared against a low ΔT setpoint (25°F). If ΔT is less than the low ΔT setpoint the corresponding error number is set. A low ΔT error indicates that there is a loss of heater power or a heater controller malfunction. There are two heater controllers per channel. Each heater controller is connected to four heaters in series. If one heater fails open then all the rest of the heaters will be turned off. This will cause either all the odd numbered T_s or even numbered T_s to have a low ΔT error.

ΔT or T_u is used to determine percent level for both the head area and the plenum area. A sensor is considered uncovered whenever ΔT or T_u is greater than 200°F or 700°F, respectively. Five-degree dead bands exist in both the ΔT and T_u setpoints for uncovered sensors to prevent cycling.

A maximum T_H and a maximum ΔT are selected and are used to calculate separate setpoint signals for the heater controllers. The minimum of the two heater controller setpoint signals is selected and sent to each of the heater controllers. The T_H and ΔT heater controller setpoint signals are reduced at a constant rate, when their respective T_H and ΔT values increase above a predetermined value. The T_H and ΔT heater controller setpoints will decrease until they equal zero at a second predetermined setpoint.

7.5.4.2 Subcooling Margin Monitor

The subcooling margin monitor (SMM) provides continuous, redundant indication of the margin to saturated conditions in the reactor coolant system (RCS). The SMM inputs are RCS hot leg and cold leg temperatures from loop RTDs, core exit thermocouple temperature, RCS wide range pressure, and pressurizer pressure. The margin to saturation, displayed in degrees F, is the difference between the measured RCS temperature and the saturation temperature. The highest RCS loop temperature and the highest core exit thermocouple temperature, excluding upper head thermocouples, are used to calculate margins to saturation. The lowest pressure value is used to calculate the saturation temperature. The control board SMM display has a switch to select margin to saturation indication based on RCS loop RTD temperature or core exit thermocouple temperature.

7.5.4.3 Core Exit Temperature

Core exit temperature is continuously indicated on redundant control board displays. The chromel-alumel thermocouples in the vessel measure temperature at the flow exit of selected fuel assemblies and locations within the reactor vessel head plenum.

The redundant displays each normally indicate the temperature of the hottest thermocouple for that channel. The operator can interrogate the display to indicate the temperature of any individual thermocouple or the highest temperature in each core quadrant.

7.5.5 NUCLEAR INSTRUMENTATION

In addition to the Westinghouse nuclear instrumentation system that is described in section 7.2 and whose indications are listed in table 7.5-3, an independent channel of Gamma-Metrics nuclear instrumentation is provided to satisfy alternate shutdown requirements.

The Gamma-Metrics channel provides neutron flux indication at the hot shutdown panel and the control room via isolated outputs. A fission chamber detector measures neutron flux from shutdown to full power. Detector sensitivity is 10^{-2} to 10^{10} nv. The following displays are provided on the main control board and the hot shutdown panel:

FNP-FSAR-7

	Source Range	0.1 to 10 ⁵ counts/s
	Source Range Startup Rate	-1 to 7 decades/min.
	Log Power Level	10 ⁻⁸ to 100-percent power

TABLE 7.5-1 (SHEET 1 OF 16)
POST ACCIDENT INSTRUMENTATION
TYPE A VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Plant Specific	1	Information required for operator action	1	RCS Pressure (wide range)	1
			2	RCS Hot Leg Temperature (wide range)	1
			3	RCS Cold Leg Temperature (wide range)	1
			4	Steam Generator Level (wide range)	1
			5	Steam Generator Level (narrow range)	1
			6	Pressurizer Level	1
			7	Containment Pressure (normal range)	1
			8	Main Steam Line Pressure	1
			9	Refueling Water Storage Tank Level	1
			10	Containment Water Level	1
			11	Condensate Storage Tank Level	1
			12	Auxiliary Feedwater Flow	1
			15	Core Exit Temperature	1
			132	Core Subcooling Monitor	2

FNP-FSAR-7

TABLE 7.5-1 (SHEET 2 OF 16)

TYPE B VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Reactivity Control Neutron Flux	1	Function detection; accomplishment of mitigation	17	Neutron Flux (intermediate range)	1
Control Rod Position	3	Verification	1009	Control Rod Position	3
RCS Soluble Boron Concentration	3	Verification	1017	Post Accident Sample	3
RCS Cold Leg Water Temperature	3	Verification	3	RCS Cold Leg Temperature (wide range)	1
Core Cooling RCS Hot Leg Water Temperature	1	Function detection; accomplishment of mitigation; verification; long-term surveillance	2	RCS Hot Leg Temperature (wide range)	1
RCS Cold Leg Water Temperature	1	Function detection; accomplishment of mitigation; verification; long-term surveillance	3	RCS Cold Leg Temperature (wide range)	1

TABLE 7.5-1 (SHEET 3 OF 16)**TYPE B VARIABLES**

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
RCS Pressure	1	Function detection; accomplishment of mitigation; verification; long-term surveillance	1	RCS Pressure (wide range)	1
Core Exit Temperature	3	Verification	15	Core Exit Temperature	1
Coolant Inventory	1	Verification; accomplishment of mitigation;	18	Reactor Water Level	1
Degrees of Subcooling	2	Verification and analysis of plant conditions	132	Core Subcooling Monitor	2
Maintaining Reactor Coolant System Integrity					
RCS Pressure	1	Function detection; accomplishment of mitigation	1	RCS Pressure (wide range)	1
Containment Sump Water Level (narrow range)	2	Function detection; accomplishment of mitigation; verification	111	Reactor Cavity Sump Level	2

TABLE 7.5-1 (SHEET 4 OF 16)

TYPE B VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Containment Sump Water Level (wide range)	1	Function detection; accomplishment of mitigation; verification	10	Containment Water Level	1
Containment Pressure	1	Function detection; accomplishment of mitigation; verification	7	Containment Pressure (normal range)	1
Maintaining Containment Integrity Containment Isolation Valve Position (excluding check valves)	1	Accomplishment of isolation	19	Containment Isolation Valve Position	1
Containment Pressure	1	Function detection; accomplishment of mitigation; verification	7	Containment Pressure (normal range)	1

TABLE 7.5-1 (SHEET 5 OF 16)

TYPE C VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Fuel Cladding Core Exit Temperature	1	Detection of potential for breach; accomplishment of mitigation; long-term surveillance	15	Core Exit Temperature	1
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	1	Detection of breach	14	Primary Coolant Radioactivity Concentration	1
Analysis of Primary Coolant (gamma spectrum)	3	Detail analysis; accomplishment of mitigation; verification; long-term surveillance	1017	Post Accident Sample	3
Reactor Coolant Pressure Boundary RCS Pressure	1	Detection of potential for or actual breach; accomplishment of mitigation; long-term surveillance	1	RCS Pressure (wide range)	1

TABLE 7.5-1 (SHEET 6 OF 16)**TYPE C VARIABLES**

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Containment Pressure	1	Detection of breach; accomplishment of mitigation; verification; long-term surveillance	7	Containment Pressure (normal range)	1
Containment Sump Water Level (narrow range)	2	Detection of breach; accomplishment of mitigation; verification; long-term surveillance	111	Reactor Cavity Sump Level	2
Containment Sump Water Level (wide range)	1	Detection of breach; accomplishment of mitigation; verification; long-term surveillance	10	Containment Water Level	1
Containment Area Radiation	3	Detection of breach; verification	13	Containment Radiation (high range)	1
Effluent Radioactivity – Noble Gas Effluent from Condenser Air Removal System Exhaust	3	Detection of breach; verification	120	Condenser SJAE Radiation	2

TABLE 7.5-1 (SHEET 7 OF 16)**TYPE C VARIABLES**

<u>R.G. 1.97 VARIABLES</u>		<u>FNP POSITION</u>			
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Containment RCS Pressure	1	Detection of potential for breach; accomplishment of mitigation	1	RCS Pressure (wide range)	1
Containment Hydrogen Concentration	1	Detection of potential for breach; accomplishment of mitigation; long-term surveillance	1006	Containment Hydrogen Concentration	3
Containment Pressure	1	Detection of potential for or an actual breach; accomplishment of mitigation	16	Containment Pressure (extended range)	1
Containment Effluent Radioactivity – Noble Gases from Identified Release Points	2	Detection of breach; accomplishment of mitigation; verification	121	Plant Vent Effluent Radiation	2
Effluent Radioactivity – Noble Gases (from buildings or areas where penetrations and hatches are located, e. g., secondary containment and auxiliary buildings and fuel handling buildings that are in direct contact with primary containment)	2	Indication of breach	121	Plant Vent Effluent Radiation	2

TABLE 7.5-1 (SHEET 8 OF 16)
TYPE D VARIABLES

<u>R.G. 1.97 VARIABLES</u>		<u>FNP POSITION</u>			
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Residual Heat Removal (RHR) or Decay Heat Removal System					
RHR System Flow	2	To monitor operation	101	RHR/LHSI Flow	2
RHR Heat Exchanger Outlet Temperature	2	To monitor operation and for analysis	114	RHR HX Discharge Temperature	2
Safety Injection Systems					
Accumulator Tank Level and Pressure	2	To monitor operation	125	Accumulator Tank Pressure	2
			1018	Accumulator Tank Level	3
Accumulator Isolation Valve Position	2	Operation status	126	Accumulator Tank Isolation Valve Position	2
Boric Acid Charging Flow	2	To monitor operation	102	Boric Acid Flow	2
Flow in HPI System	2	To monitor operation	103	HHSI Flow	2
Flow in LPI System	2	To monitor operation	101	RHR/LHSI Flow	2
Refueling Water Storage Tank Level	2	To monitor operation	9	Refueling Water Storage Tank Level	1
Primary Coolant System					
Reactor Coolant Pump Status	3	To monitor operation	1011	RCP Motor Current	3

TABLE 7.5-1 (SHEET 9 OF 16)

TYPE D VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Primary System Safety Relief Valve Positions (including PORV and code valves) or Flow Through or Pressure in Relief Valve Lines	2	Operation status; to monitor for loss of coolant	127 128	Pressurizer PORV Position Pressurizer Safety Valve Position	2 2
Pressurizer Level	1	To ensure proper operation of pressurizer	6	Pressurizer Level	1
Pressurizer Heater Status	2	To determine operating status	130 112	Pressurizer Heater Breaker Position Pressurizer Pressure	2 2
Quench Tank Level	3	To monitor operation	1002	Pressurizer Relief Tank level	3
Quench Tank Temperature	3	To monitor operation	1004	Pressurizer Relief Tank Temperature	3
Quench Tank Pressure	3	To monitor operation	1007	Pressurizer Relief Tank Pressure	3
Secondary System (Steam Generator)					
Steam Generator Level	1	To monitor operation	4	Steam Generator Level (wide range)	1
Steam Generator Pressure	2	To monitor operation	8	Main Steam Line Pressure	1
Safety/Relief Valve Positions or Main Steam Flow	2	To monitor operation	104	Main Steam Flow	2
Main Feedwater Flow	3	To monitor operation	1001	Main Feedwater Flow	3

FNP-FSAR-7

TABLE 7.5-1 (SHEET 10 OF 16)

TYPE D VARIABLES

<u>R.G. 1.97 VARIABLES</u>				<u>FNP POSITION</u>	
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Auxiliary Feedwater or Emergency Feedwater System					
Auxiliary or Emergency Feedwater Flow	2	To monitor operation	12	Auxiliary Feedwater Flow	1
Condensate Storage Tank Water Level	1	To ensure water supply for auxiliary feedwater (can be Category 3 if not primary source of AFW. Then whatever is primary source of AFW should be listed and should be Category 1)	11	Condensate Storage Tank Level	1
Containment Cooling Systems					
Containment Spray Flow	2	To monitor operation	105	Containment Spray Flow	2
Heat Removal by the Containment Fan	2	To monitor operation	115	Temperature of Service Water to Aux. Bldg	2
Heat Removal System			116	CTMT Cooler Service Water Outlet Temperature	2
			133	Service Water Flow to CTMT Coolers	2
Containment Atmosphere Temperature	2	To indicate accomplishment of cooling	117	Containment Atmosphere Temperature	2

TABLE 7.5-1 (SHEET 11 OF 16)

TYPE D VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Containment Sump Water Temperature	2	To monitor operation	118	RHR HX Inlet Temperature	2
Chemical and Volume Control System					
Makeup Flow - In	2	To monitor operation	106	Charging Line Flow	2
			110	RCP Seal Injection Flow	2
Letdown Flow- Out	2	To monitor operation	107	Letdown Flow	2
Volume Control Tank Level	2	To monitor operation	113	Volume Control Tank Level	2
Cooling Water System					
Component Cooling Water Temperature to ESF System	2	To monitor operation	119	Component Cooling Water Heat Exchanger Discharge Temperature	2
Component Cooling Water Flow to ESF Sys	2	To monitor operation	108	CCW HX Inlet Flow	2
Radwaste Systems					
High-level Radioactive Liquid Tank Level	3	To indicate storage volume	1003	Radioactive Liquid Tank Levels	3
Radioactive Gas Holdup Tank Pressure	3	To indicate storage capacity	1008	Waste gas Decay Tank Pressure	3
Ventilation Systems					
Emergency Ventilation Damper Position	2	To indicate damper status	129	HVAC Emergency Damper Position	2

FNP-FSAR-7

TABLE 7.5-1 (SHEET 12 OF 16)
TYPE D VARIABLES

<u>R.G. 1.97 VARIABLES</u>		<u>FNP POSITION</u>			
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Power Supplies Status of Standby Power and Other Energy Sources Important to Safety (electric, hydraulic, pneumatic) (voltages, currents, pressures)	2	To indicate system status	131	Emergency Power Status	2

FNP-FSAR-7

TABLE 7.5-1 (SHEET 13 OF 16)

TYPE E VARIABLES

<u>R.G. 1.97 VARIABLES</u>		<u>FNP POSITION</u>			
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Containment Radiation Containment Area Radiation – High Range	1	Detection of significant releases; release assessment; long-term surveillance; emergency plan actuation	13	Containment Radiation (high range)	1
Area Radiation Radiation Exposure rate (inside buildings or areas where access is required to service equipment important to safety)	3	Detection of significant releases; release assessment; long-term surveillance	122 1005	Accessible Area Radiation Portable Plant/Environs Radiation	2 3
Airborne Radioactive Materials Released from Plant Noble Gases and Vent Flow Rate					
Containment or Purge Effluent	2	Detection of significant releases; release assessment		Not Applicable, see Common Plant vent	
Reactor Shield Building Annulus (if in design)	2	Detection of significant releases; release assessment		Not Applicable, not in design	

TABLE 7.5-1 (SHEET 14 OF 16)
TYPE E VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Auxiliary Building (including any building containing primary system gases, e. g., waste gas decay tank)	2	Detection of significant releases; release assessment; long-term surveillance		Not Applicable, see Common Plant Vent	
Condenser Air Removal System Exhaust	2	Detection of significant releases; release assessment	120	Condenser SJAE Radiation	2
Common Plant Vent or Multi-purpose Vent Discharging Any of Above Releases (if containment purge is included)	2	Detection of significant release; release assessment; long-term surveillance	121	Plant Vent Effluent Radiation	2
			109	Plant Vent Stack Flow	2
Vent From Steam Generator Safety Relief Valves or Atmospheric Dump Valves	2	Detection of significant releases; release assessment	104	Main Steam Flow	2
			123	Main Steam Effluent Radiation	2
			124	TDAFW Effluent Radiation	2
All Other Identified Release Points	2	Detection of significant releases; release assessment; long-term surveillance		Not Applicable	

TABLE 7.5-1 (SHEET 15 OF 16)

TYPE E VARIABLES

<u>R.G. 1.97 VARIABLES</u>			<u>FNP POSITION</u>		
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Particulates and Halogens					
All Identified Plant Release Points (except steam generator safety relief valves or atmospheric steam dump valves and condenser air removal system exhaust). Sampling with Onsite Analysis Capability	3	Detection of significant releases; release assessment; long-term surveillance	1012	Particulates and Halogens Sampling (Vent Stack)	3
Environs Radiation and Radioactivity					
Airborne Radiohalogens and Particulates (portable sampling with onsite analysis capability)	3	Release assessment; analysis	1013	Airborne Radiohalogens and Particulates (Environs)	3
Plant and Environs Radiation (portable instrumentation)	3	Release assessment; analysis	1005	Portable Plant/Environs Radiation	3
Plant and Environs Radioactivity (portable instrumentation)	3	Release assessment; analysis	1019	Portable Plant/Environs Radioactivity (Gamma-ray Spectrometer)	3
Meteorology					
Wind Direction	3	Release assessment	1014	Wind Direction	3
Wind Speed	3	Release assessment	1015	Wind Speed	3
Estimation of Atmospheric Stability	3	Release assessment	1016	Estimation of Atmospheric Stability	3

TABLE 7.5-1 (SHEET 16 OF 16)

TYPE E VARIABLES

<u>R.G. 1.97 VARIABLES</u>				<u>FNP POSITION</u>	
<u>VARIABLE</u>	<u>CATEGORY</u>	<u>PURPOSE</u>	<u>VARIABLE NO.</u>	<u>DESCRIPTION</u>	<u>CATEGORY</u>
Accident Sampling Capability (Analysis Capability On Site)					
Primary Coolant and Sump	3	Release assessment; verification; analysis	1017	Post Accident Sample	3
-Gross Activity					
-Gamma Spectrum					
-Boron Content					
-Chloride Content					
-Dissolved Hydrogen or Total Gas					
-Dissolved Oxygen					
-pH					
Containment Air	3	Release assessment; verification; analysis	1010	Post Accident Sample – CTMT Air	3
-Hydrogen Content					
-Oxygen Content					
-Gamma Spectrum					

FNP-FSAR-7

TABLE 7.5-2

(This table has been deleted.)

FNP-FSAR-7

TABLE 7.5-3 (SHEET 1 OF 6)

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO
MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

<u>Parameter</u> <u>Notes</u>	<u>No. of</u> <u>Channels</u> <u>Available</u>	<u>Range</u>	<u>Indicated</u> <u>Accuracy</u>	<u>Indicator/</u> <u>Recorder</u>	<u>Location</u>	<u>Notes</u>
<u>Nuclear Instrumentation</u>						
Source range						
Count rate	2	1 to 10 ⁶ counts/s	±7% of the linear full scale analog voltage	Both channels indicated; either may be selected for recording	Control board	One 2-pen record- er is used to re- cord any of the 8 nuclear chan- nels (2 source range, 2 intermediate range, and 4 power range).
Startup rate	2	-0.5 to 5.0 decades/min	±7% of the linear full scale analog voltage	Both channels indicated	Control board	
Intermediate range						
Flux level	2	8 decades of neutron flux (corresponds to 0 to full scale analog voltage) overlapping the source range by 2 decades	±7% of the linear full scale analog voltage and ±3% of the linear full scale voltage in the range of 10 ⁻⁴ to 10 ⁻³ A	Both channels indicated; either may be selected for recording		
Startup rate	2	-0.5 to 5.0 decades/min	±7% of the linear full scale analog voltage	Both channels indicated	Control board	

FNP-FSAR-7

TABLE 7.5-3 (SHEET 2 OF 6)

<u>Parameter</u>	<u>No. of Channels Available</u>	<u>Range</u>	<u>Indicated Accuracy</u>	<u>Indicator/ Recorder</u>	<u>Location</u>	<u>Notes</u>
Power range Uncalibrated ion chamber current (top and bottom uncompensated ion chambers)	4	0 to 120% of full power current	±1% of full span	All 8 current signals indicated	NIS racks in control room	
Calibrated ion chamber current (top and bottom uncompensated ion chambers)	4	0 to 120% of full power	±2% of full power	These 8 current signals are available for selectable trending by the operator		
Upper and lower ion chamber current difference	4	-50 to +50%	±3% of full power	Diagonally opposed; any 2 of the 4 channels may be se- lected for recording at the same time using intermediate range recorder	Control board	
Average flux of the top and bottom ion chamber	4	0 to 120% of full power	±3% of full power for indication; ±2% for recording	All 4 channels indicated; any 2 of the 4 channels may be recorded using source range recorder	Control board	
Average flux of the top and bottom ion chambers	4	0 to 200% of full power	±2 to 120% of full power; ±6 to 200% of full power	All 4 channels recorded	Control board	

FNP-FSAR-7

TABLE 7.5-3 (SHEET 3 OF 6)

<u>Parameter</u>	<u>No. of Channels Available</u>	<u>Range</u>	<u>Indicated Accuracy</u>	<u>Indicator/ Recorder</u>	<u>Location</u>	<u>Notes</u>
Flux difference of the top and bottom ion chambers	4	-30 to +30%	±4%	All 4 channels indicated	Control board	
<u>Reactor Coolant System</u>						
T _{avg} (measured)	1 per loop	530° to 630°F	±4°F	All channels indicated	Control board	
ΔT (measured)	1 per loop	0 to 150% of full power ΔT	±4% of full power ΔT	All channels indicated	Control board	
T _{cold} or T _{hot} (measured, wide range)	1 T _{hot} , 1 T _{cold} per loop	0°F to 700°F	±4%	Both channels recorded	Control board	
Overpower ΔT setpoint	1 per loop	0 to 150% of full power ΔT	±4% of full power ΔT	All channels indicated	Control board	
Overtemperature ΔT setpoint	1 per loop	0 to 150% of full power ΔT	±4% of full power ΔT	All channels indicated	Control board	
Pressurizer pressure	5	1700 to 2500 psig	±20 psi	All channels indicated	Control board	
Pressurizer level	3	Entire distance between taps	±3.5% of ΔP at 2250 psia	All channels indicated; 1 channel is selected for recording	Control board	2-pen recorder used; second pen records reference level signal
Primary coolant flow	3 per loop	0 to 120% of rated flow	Repeatability of ±4% of full flow	All channels indicated	Control board	
Reactor coolant pump bus amperes	1 per loop	0 to 1200 amps	-	All channels indicated	Control board	One channel for each bus
System pressure wide range	2	0 to 3000 psig	±4%	All channels indicated and recorded	Control board	

FNP-FSAR-7

TABLE 7.5-3 (SHEET 4 OF 6)

<u>Parameter</u>	<u>No. of Channels Available</u>	<u>Indicated Range</u>	<u>Indicated Accuracy</u>	<u>Recorder</u>	<u>Location</u>	<u>Notes</u>
<u>Reactor Control System</u>						
Demanded rod speed	1	0 to 75 steps/min	±2%	1 channel is indicated	Control board	
Median T _{avg}	1	530°F to 630°F	±4°F	1 channel is recorded	Control board	
T _{ref}	1	530°F to 630°F	±4°F	1 channel is recorded	Control board	
Control rod position						If system not available, borate and sample accordingly
Number of steps of demanded rod withdrawal	1 per group	0 to 231 steps ^(a)	±1 step	Each group is indicated	Control board	These signals are used in conjunction with the full-length rod measured position signals to detect deviation of any individual rod from the demanded position; a deviation will actuate an alarm
Full-length rod measured position	1 per rod	0 to 228 steps ^(b)	±4 steps at full accuracy; ±8 steps at 1/2 accuracy	Each rod position is indicated	Control board	

a. Fully withdrawn position can be varied from 225 to 231 steps to reduce RCCA wear. The NRC acceptance criteria regarding the range associated with the fully withdrawn RCCA position are that the fully withdrawn position selected for use throughout each cycle will be evaluated as part of the reload safety evaluation process to verify that sufficient margin exists in the safety analyses to bound the related effects.

b. Digital Rod Position Indication (DRPI) system maximum indication is 228 steps.

FNP-FSAR-7

TABLE 7.5-3 (SHEET 5 OF 6)

<u>Parameter</u>	<u>No. of Channels Available</u>	<u>Range</u>	<u>Indicated Accuracy</u>	<u>Indicated Recorder</u>	<u>Location</u>	<u>Notes</u>
Control rod bank position	4	0 to 100% ^(a)	±3% of total bank travel	All 4 control rod bank positions are recorded along with the low-low limit alarm for each bank	Control board	1 channel for each control rod; an alarm and annunciator are actuated when the rod control bank to be withdrawn reaches withdrawal limit, when any rod control bank reaches the low insertion limit, and when any rod control bank reaches the low-low insertion limit
<u>Containment System</u>						
Containment pressure	4	-5 to 65 psig	±3%	All 4 channels indicated	Control board	
<u>Feedwater and Steam Systems</u>						
Auxiliary feedwater flow - Unit 1	1 per steam line	0 to 400 gal/min	±3%	All channels	Control board	1 channel to measure the flow to each steam generator
Auxiliary feedwater flow - Unit 2	1 per steam line	0 to 400 gal/min	±3%	All channels	Control board	1 channel to measure the flow to each steam generator
Steam generator level (narrow range)	3 per steam generator	+6.2 to -11.5 ft from nominal full load level	±3% of level (hot)	All channels indicated; channels used for control are recorded	Control board	
Steam generator level (wide range)	1 per steam generator	+6.2 to -41.7 ft from nominal full load level	±5% of level (cold)	All channels recorded	Control board	

a. One-hundred percent is the fully withdrawn position.

FNP-FSAR-7

TABLE 7.5-3 (SHEET 6 OF 6)

<u>Parameter</u>	<u>No. of Channels Available</u>	<u>Range</u>	<u>Indicated Accuracy</u>	<u>Indicated Recorder</u>	<u>Location</u>	<u>Notes</u>
Main feedwater flow	2 per steam generator	0 to 120% of maximum calculated flow	±5%	All channels indicated; channels used for control are recorded	Control board	
Magnitude of signal controlling main	1 per main, 1 per bypass	0 to 100% of valve opening	±1.5%	All channels indicated	Control board	1 channel for each main feedwater control valve; open/shut indication is provided in control room for each main feedwater control valve
Steam flow	2 per steam generator	0 to 120% of maximum calculated flow	±5.5%	All channels indicated; channels used for control are recorded	Control board	Accuracy is equipment capability; however, absolute accuracy depends on applicant calibration against feedwater flow
Steam line pressure	3 per loop	0 to 1200 psig	±4%	All channels indicated	Control board	
Steam dump modulate signal	1	0 to 85% maximum calculated steam flow	±1.5%	1 channel is indicated	Control board	Open/shut indication is provided in the control room for each steam dump valve
Turbine impulse chamber pressure	2	0 to 120% of maximum calculated turbine load	±3.5%	Both channels indicated	Control board	Open/shut indication is provided in the control room for each turbine stop valve

7.6 ALL OTHER SYSTEMS REQUIRED FOR SAFETY

7.6.1 INSTRUMENTATION AND CONTROL POWER SUPPLY SYSTEM

7.6.1.1 Description

The following is a description of the instrumentation and control power supply system. (Refer to section 8.3 for line diagrams of instrumentation and control power supply system.)

There are four inverters supplying power to four separate distribution panels. Each inverter is connected independently to one distribution panel. The distribution panels are labeled channels 1 through 4. These inverters provide power for the operation of the nuclear steam supply system instrumentation. To ensure redundancy is maintained, two inverters are supplied by train A and two inverters are supplied by train B.

To ensure continuous operation, the four inverters are each supplied by two sources -- a preferred source and an alternate source.

- A. The preferred power source is derived from the 125 V-dc switchgear via the 125 V-dc Class 1E battery chargers. In the event of a loss of a battery charger, the preferred source is automatically supplied by the station batteries.
- B. The alternate power source is derived from the Class 1E 575-208/120-V constant voltage transformer (CVT). Should the inverter voltage deviate from specified limits while connected to the preferred source, the static transfer switch, located in the inverter, automatically transfers to the alternate source. A manual transfer switch is provided to realign to the preferred source.

A manual bypass switch is provided on each inverter to allow the distribution panel to be supplied by the alternate source when the inverter is removed from service for maintenance purposes.

See subsection 7.1.4 and table 7.1-1 for a list of supplementary drawings.

7.6.1.2 Analysis

There are two independent battery chargers and station batteries. Each train of 125 V-dc switchgear is normally supplied by its associated battery charger. Should the charger fail or lose power, the station battery automatically assumes bus loads. Each 125 V-dc bus serves two inverters. Since no more than two inverters are connected to the same bus, a loss of a single bus can only affect two of the four inverters.

Each inverter is independently connected to its respective instrument distribution panel so that the loss of an inverter cannot affect more than one of the four distribution panels.

FNP-FSAR-7

The two A train associated inverters are provided an alternate power source from an A train 600-V MCC via a CVT and distribution panel. Likewise, the two B trains are provided an alternate power source via the B train CVT and distribution panel. The static transfer switches built into the inverters automatically transfer from the preferred source (dc) to the alternate source (ac) when the inverter output is outside specified limits, providing an uninterrupted 120 V-ac supply to the distribution panels.

Therefore, no single failure in the instrumentation and control power supply system or its associated power supplies can cause a loss of power to more than one of the redundant loads.

The inverters are designed to maintain their outputs within the limits of 60 Hz \pm 0.5 % and at a nominal 120 V-ac with \pm 2 % voltage regulation. The loss of the ac or dc inputs are alarmed in the control room, as is the loss of an inverter's output. There are no inverter breaker controls on the control board, since no manual transfers are necessary in the event of loss of the preferred dc power source.

Physical separation and provisions to protect against fire are discussed in chapter 8 and appendix 9B.

Based on the scope definitions presented in Institute of Electrical and Electronics Engineers (IEEE) 308-1971,⁽¹⁾ 279-1971,⁽²⁾ and 338-1971,⁽³⁾ the criterion which is applicable to the instrumentation and control power supply system is IEEE 308-1971. The design is in compliance with this standard and Regulatory Guide 1.6. Availability of this system is continuously indicated by the operational status of the systems it serves (drawings D-177024, D-207024, D-177025, and D-207025) and is verified by periodic testing performed on the served systems. The inverters have been seismically qualified as class 1E equipment.

Concerning electrical power systems important to safety, it should be noted that the testability requirements of General Design Criterion 18 and Regulatory Guide 1.22 for the reactor trip system and the engineered safety features actuation system are covered in subsections 7.2.3 and 7.3.2, respectively.

Provision has been made on the safety-related 4-kV switchgear buses for testing the undervoltage and underfrequency sensor relay during plant operation and also on the diesel generator sequencer for circuit integrity testing. (Refer to drawings D-177645; D-207645; D-177646; D-207646; D-177647; D-207647; D-177648; D-207648; D-177649; D-207649; D-177650; D-207650; D-177653; D-207653; D-177654; D-207654; D-177659; D-207659; D-177660, sheets 1 and 2; and D-207660, sheets 1 and 2.) Starting and loading the diesel generators is covered in section 8.3.

The 120-V vital ac and the 125 V-dc systems are continuously energized systems with instrumentation provided for indication of the integrity of the systems. The system components will be routinely tested. In view of the above, the reliability of the operation of these systems is reasonably ensured.

7.6.2 RESIDUAL HEAT REMOVAL ISOLATION VALVES

7.6.2.1 Description

There are two motor-operated gate valves in series in each of two RHR loop suction lines from the reactor coolant system (RCS) to the residual heat removal (RHR) system. These RHR isolation valves are normally closed and are only opened for residual heat removal and for protection of the RCS against low temperature overpressurization via the RHR relief valves. The isolation valves are opened whenever the RCS pressure is approximately 383 psig and the RCS temperature is $\leq 325^{\circ}\text{F}$. (See chapter 5 for details of the RHR system.)

- A. One set of isolation valves (8701B-B and 8702B-B), those adjoining the RCS, is interlocked with a pressure signal to prevent their being opened whenever the RCS pressure is greater than approximately 383 psig. This interlock is derived from the RCS wide range pressure transmitter P-403 process control channel (see section 5.6).
- B. The other set of valves (8701A-A and 8702A-A), those adjoining the RHR system, is similarly interlocked to prevent their being opened whenever the RCS pressure is greater than approximately 383 psig. This interlock is derived from the RCS wide range pressure transmitter P-402 process control channel. These valves are also interlocked by use of the pressurizer vapor space temperature detector.

The vapor space temperature detector has been added to the open permissive interlock circuitry for the RHR valves closest to the system. Figures 7.6-1 and 7.6-2 indicate the diverse interlock system of this modified design.

- C. The autoclosure interlock on each set of valves in series was removed per WCAP-11746. Two MCB annunciator alarms are installed to warn operators when the RHR suction/isolation valve(s) is not fully closed and the RCS pressure reaches the alarm setpoint. The arrangement of the RHR relief and isolation valves is shown in drawings D-175041 and D-205041.
- D. The RCS to RHR pump suction isolation valves are also interlocked with the RHR heat exchanger to charging pump suction motor-operated valves (MOVs) (8706A-A and 8706B-B) and the RWST to RHR pump suction isolation MOVs (8809A-A and 8809B-B). MOVs 8706A-A and 8809A-A must be closed before MOVs 8701A-A and 8701B-B can be opened. MOVs 8706B-B and 8809B-B must be closed before MOVs 8702A-A and 8702B-B can be opened. MOVs 8706A-A and 8706B-B are normally closed and are opened by operator action only when the emergency core cooling system (ECCS) is placed in recirculation mode. As part of the ECCS, MOVs 8809A-A and 8809B-B are normally open to provide low-head safety injection (LHSI) but must be closed before the system is placed in recirculation mode to prevent contamination or overflow of the refueling water storage tank (RWST) (see section 6.3).

7.6.2.2 Analysis

Based on the scope definitions presented in IEEE 279-1971⁽²⁾ and 338-1971,⁽³⁾ these criteria do not apply to the RHR isolation valve interlocks; however, because of the possible severity of the consequences of loss of function, the requirements of IEEE 279-1971 will be applied with the following comments:

- A. For the purpose of applying IEEE 279-1971 to this circuit, the following definitions will be used:
 - 1. Protection System
The two valves in series in each line and all components of their interlocking circuits.
 - 2. Protective Action
The maintenance of RHR system isolation from the RCS from RCS pressures above RHR design pressure.
- B. The requirement of paragraph 4.10 of IEEE 279-1971 for online test and calibration capability is applicable only to the actuation signal and not to the isolation valves, which are required to remain closed during power operation.
- C. The requirement of paragraph 4.15 of IEEE 279-1971 does not apply since the setpoints are independent of mode of operation and are not changed.

Environmental qualification of the valves and wiring is discussed in section 3.11.

7.6.3 REFUELING INTERLOCKS

A functional description of the refueling system equipment covered in section 9.1 includes a discussion of the interlocks which are provided on the refueling equipment to prevent damage to the fuel assemblies. Although there are no electrical interlocks associated with the spent-fuel bridge and the fuel handling tools, there are electrical interlocks employed by the manipulator crane and the fuel transfer system. These electrical interlocks are nonsafety related.

The electrical interlocks on the manipulator crane provide the following functions:

- A. The bridge, trolley, and hoist are mutually interlocked to prevent operation of more than one mode at a time.
- B. The bridge and trolley drives are interlocked to prevent movement that could cause collision of the mast with the guide studs, stored internals, or cavity walls. Additionally, the fuel assembly is carried inside the outer mast which is 16-in. outside diameter, 1 3/4-in. wall thickness. This prevents the fuel from being struck by an obstacle in the refueling canal.

FNP-FSAR-7

- C. Movement of the bridge and trolley is permissible only when the fuel is withdrawn completely into the outer mast. Two position indicating switches wired in series for the associated interlock are specified on the equipment purchase specification.
- D. The solenoid valve cuts off air to the operating cylinder gripper except when the weight indicator shows there is no fuel assembly suspended from the gripper. This is to prevent the operator from opening the gripper and dropping the fuel. An independent mechanical locking device as redundant protection for the associated interlock is provided.
- E. The hoist drive is operable only when the gripper position switches show that the gripper is either fully engaged or disengaged. This interlock is to prevent a fuel assembly from being lifted if the gripper has hung up in a partially engaged position. A monitoring circuit to notify the operator of failure of the associated interlock circuit is provided.
- F. Hoist operation is interrupted if either of two methods of assessing load limits indicates a rapid load change due to grid snags or other impediments to movement. Unit 2 uses the PLC-based control system and inputs provided by the load sensor and position transducer to automatically set the load limits based on the type of fuel assembly being handled and whether or not it includes an RCCA, whereas Unit 1 utilizes the originally supplied control system consisting of relays, timers, thyristor motor speed control, and computers to achieve automatic setting of the load limits. Both units retain a second load control method, which is similar to conventional load control systems in that fixed, absolute load limits are set regardless of the weight of the fuel assembly and component being handled, and consistent with F-5 recommendations for fuel handling. The hoist drive is also limited by fixed position gear, limit switches, and an overload limit switch which indicate the physical limits of hoist travel and overload load conditions, respectively.

The following electrical interlocks are provided for the fuel transfer system:

- A. Both lifting frames must be in the horizontal position before the conveyor car can be moved.
- B. The conveyor car must be against its travel limit stops before the lifting frames can be operated. This interlock makes sure the fuel container on the conveyor car is properly positioned before an attempt is made to raise it.
- C. The manipulator crane must be over the core or the gripper must be at the top stop position before the lifting frame can be operated. This interlock is to prevent the operator from lowering the transfer system fuel container while the manipulator crane is in the process of inserting or removing a fuel assembly.

7.6.4 MONITORING COMBUSTIBLE GAS IN CONTAINMENT

7.6.4.1 Description

Two independent and redundant systems for containment hydrogen monitoring will be provided. The design of these systems will follow, as applicable, the requirements for safety-related protection systems and will meet the requirements of IEEE 279-1971.

Isolation valves will be provided on both sides of the containment for the containment gas sample lines. Individual valve control switches are provided in the main control room.

There will be two operator selectable sampling points for each sampling and analysis system. Sample point locations are shown in drawings D-175019 and D-205019. The operator may select any of the sampling points from the main control room.

Sampling lines will be free of water traps (runs where liquid could accumulate) and will have a sample conditioning system. The analyzer effluent will be returned to the containment.

The sample conditioning system will maintain constant sample and reference gas flow, as required. The analyzers will have a range of 0 to 10 volume percent hydrogen and a minimum accuracy of ± 4 % of range.

The output signal of the analyzers will be indicated at the analyzer mounting location and recorded and alarmed in the main control room.

The operation of the hydrogen gas analyzer is based on the measurement of thermal conductivity of the gaseous containment atmosphere sample. The thermal conductivity of the gas mixtures changes proportionally to the changes in the concentration of the individual gas constituents of the mixture.

The thermal conductivity of hydrogen is far greater (approximately seven times the thermal conductivity of air) than any other gases or vapors expected to be present. The performance of the hydrogen gas analyzer will be periodically verified by comparing the response of the thermal conductivity instrument to a known sample of reference gas.

Each system will be supplied electrical power from an independent and redundant Class 1E power supply.

The containment combustible gas control system is also discussed in subsection 6.2.5.

7.6.4.2 Analysis

The system will satisfy the single failure criteria and remain operable under the most severe postulated incidents. Any single failure in one hydrogen monitoring system does not affect its redundant and independent counterpart.

7.6.5 SEMIAUTOMATIC BACKUP TO SWITCHOVER FROM INJECTION TO RECIRCULATION

The containment sump isolation valves (8811A-A and 8812A-A in train A and 8811B-B and 8812B-B in train B) are automatically opened on the train-oriented safety injection signal coincident with RWST low-low level setpoint signals. Four level sensors are installed on the RWST, with the level signals generated by individual pressure switches. A separate level channel for each sump valve ensures that a single failure early in a postulated event would not damage both RHR pumps by spurious alignment of the RHR pumps to the containment sump. The energize-to-actuate design further enhances this protection design by providing additional protection from spurious alignment due to a failed circuit or inadvertent loss of power to these circuits. The valve train assignment of the level instrumentation channels is as follows:

<u>Train Assignment for Safety Injection Signal</u>	<u>Valve No.</u>
A	8811A-A
A	8812A-A
B	8811B-B
B	8812B-B

The logic diagram for this semiautomatic backup to switchover from injection to recirculation is as shown in figure 7.6-3. It should be noted that there is a coincident signal from the train-oriented safety injection signal, which is latched in by means of a separately resettable retentive memory logic. It should also be noted that during the switchover sequence from injection to recirculation these latched in signals will not be reset when safety injection is reset (see drawing U-170148).

Each instrumentation low-low RWST level channel is tested on line in two steps by the safeguards test cabinets for the logic test, by an overlapping test for the discrete signal, and by strict administrative procedures that ensure only one sump valve at a time is tested.

7.6.6 ACCUMULATOR MOTOR-OPERATED ISOLATION VALVES

The functional logic diagram of the modification for the accumulator motor-operated isolation valve interlock circuit for one accumulator is shown in figure 7.6-4. The circuit for each of the other accumulators is similar. The controls of the motor-operated accumulator isolation valves include the following:

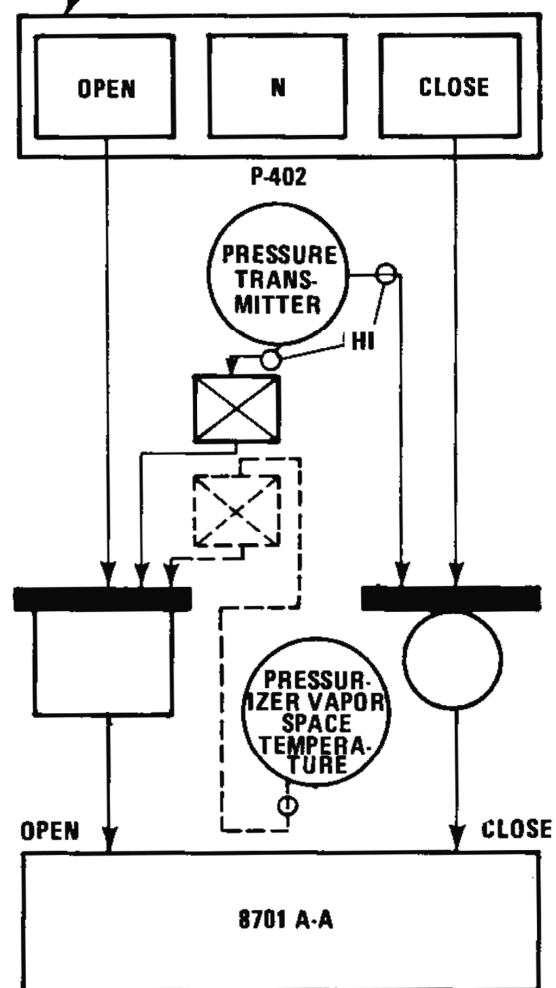
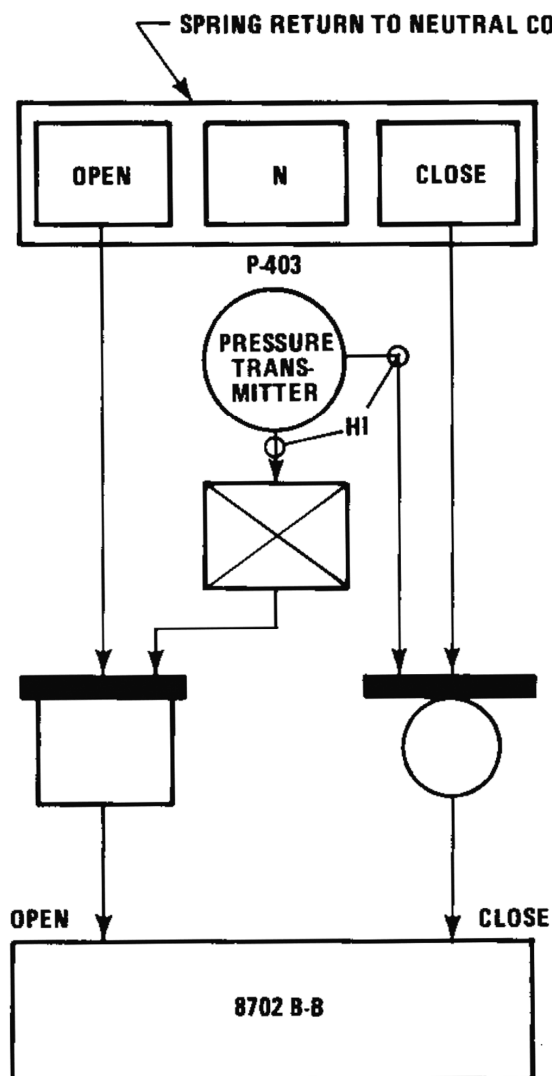
- A. Automatic opening is provided whenever the RCS pressure exceeds the safety injection system unblock pressure signal point (P-11, as shown in table 7.3-4), which is approximately 2000 psig.
- B. Automatic opening is provided upon initiation of a safety injection signal. In the event a valve is closed for accumulator maintenance within the time limits specified by the Technical Specifications or during testing for check valve leakage (or otherwise inadvertently closed) at the time injection is required, a safety injection signal (5 min) from one train is applied to open the valve, overriding the test closure.

FNP-FSAR-7

- C. The accumulator isolation valve position indication functions as described in subsection 6.3.5.
- D. A visual/audible alarm is actuated by redundant valve position limit switches whenever the valve is not in the fully open position, i.e., when the safety injection system unblock pressure is above its setpoint. A timer circuit recycles the annunciator alarm periodically until the valve is opened.

REFERENCES

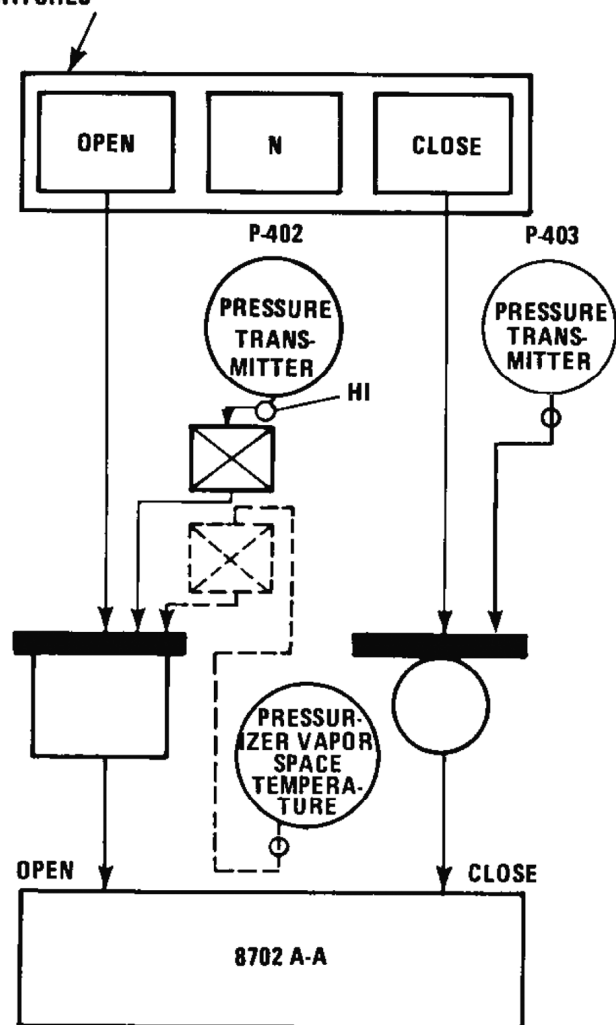
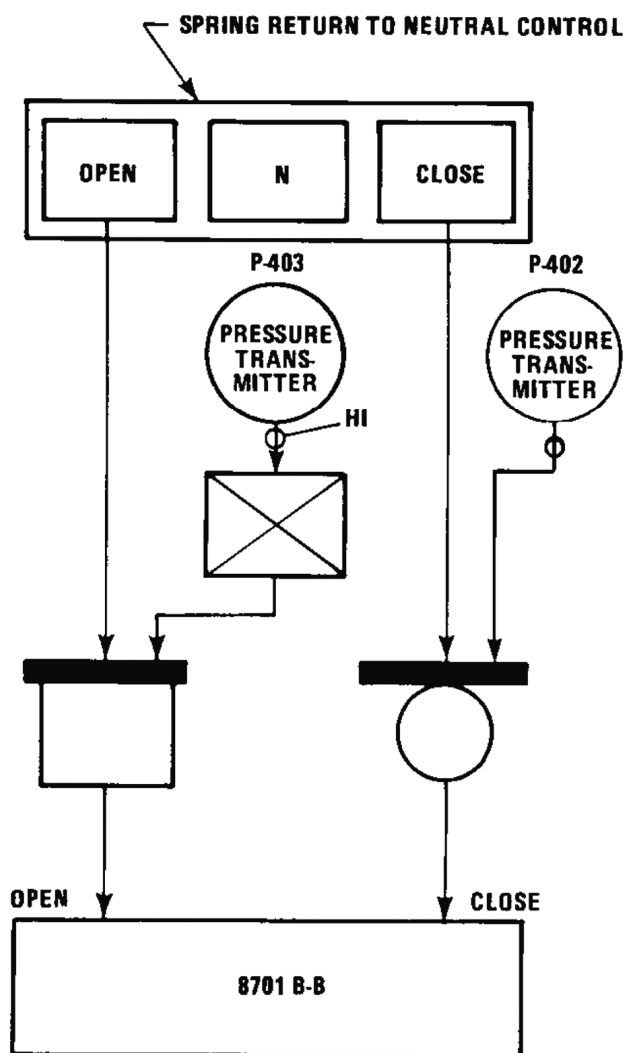
1. Institute of Electrical and Electronics Engineers, "Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations," IEEE 308-1971.
2. Institute of Electrical and Electronics Engineers, "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE 279-1971.
3. Institute of Electrical and Electronics Engineers, "Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE 338-1971.
4. Vogeding, E. L., "Seismic Testing of Electrical and Control Equipment," WCAP-7817, December 1971.



NOTES:

1. THE INTERLOCK SHOWN IN DOTTED LINES INDICATES THE METHOD OF APPLYING DIVERSE PRINCIPLES.

REV 21 5/08



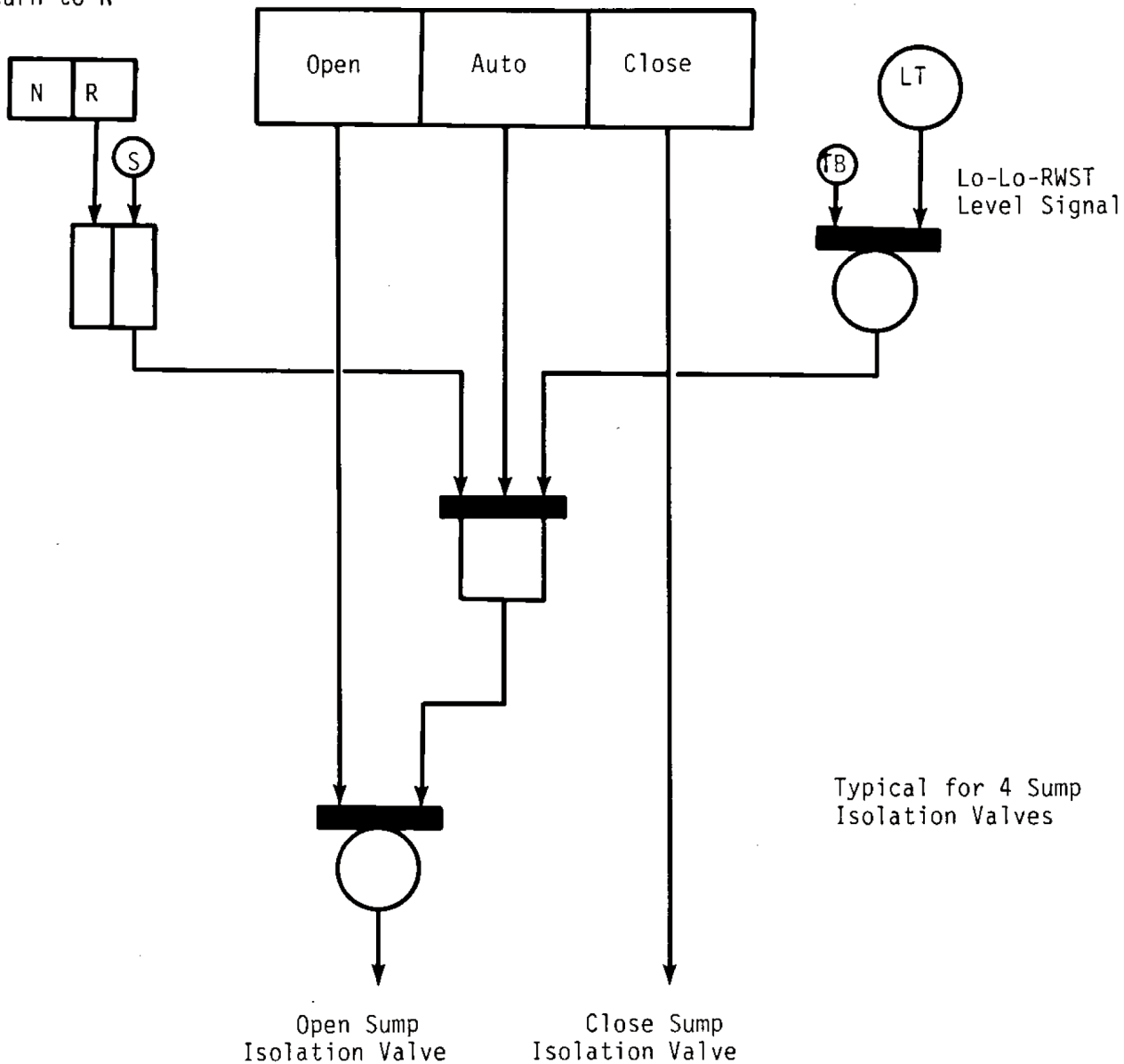
NOTES:

1. THE INTERLOCK SHOWN IN DOTTED LINES INDICATES THE METHOD OF APPLYING DIVERSE PRINCIPLES.

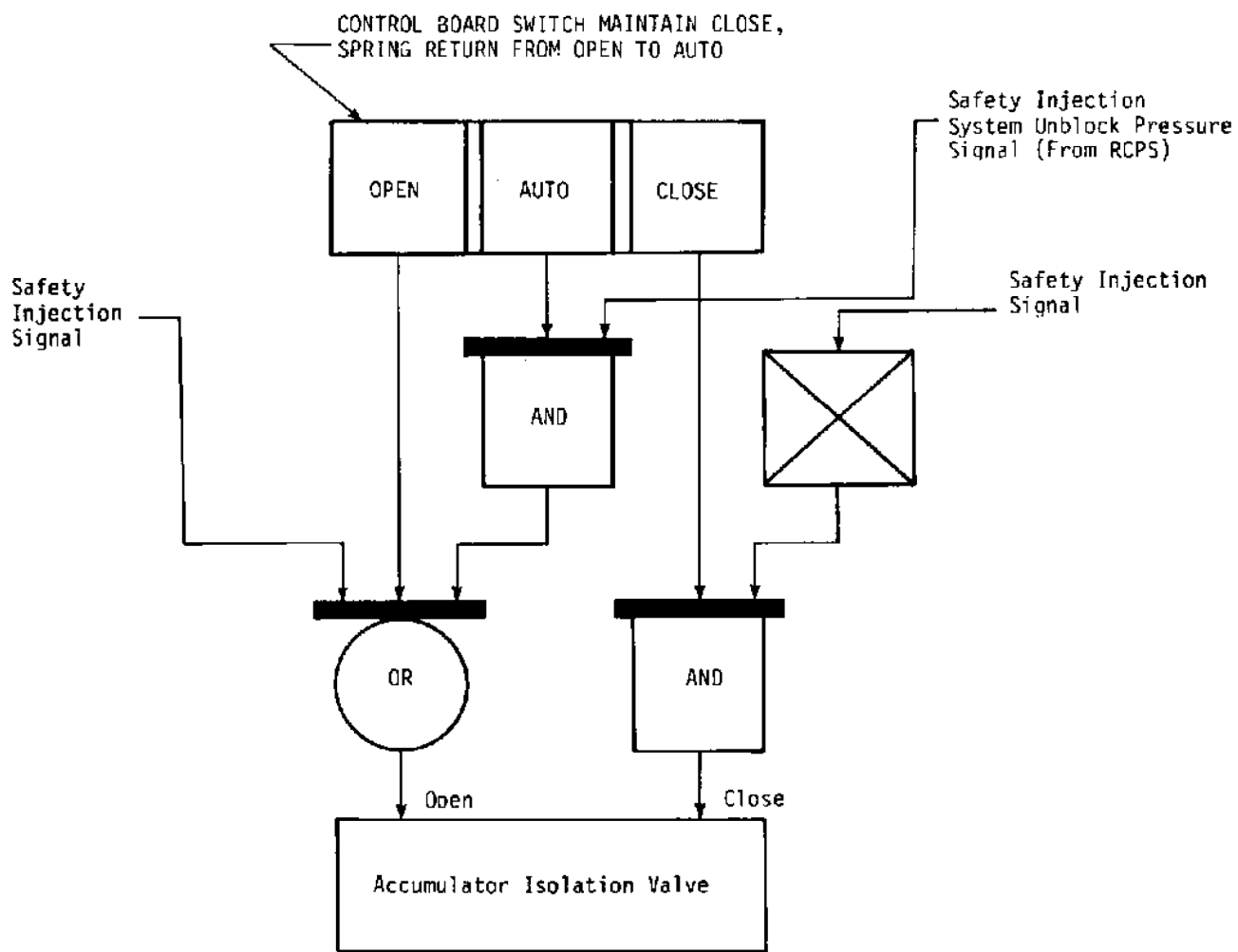
REV 21 5/08

Manual Reset Spring
Return to N

Spring Return to Auto From Both Sides



REV 21 5/08



REV 21 5/08

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

The general design objectives of the plant control systems are:

- A. To establish and maintain power equilibrium between primary and secondary systems during steady state unit operation.
- B. To constrain operational transients (Condition I) to preclude unit trip and reestablish steady state unit operation.
- C. To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the operator the capability of assuming manual control of the system.

7.7.1 DESCRIPTION

The plant control systems described in this section perform the following functions:

- A. Reactor Control System
 - 1. Enables the nuclear plant to accept a step load increase or decrease of 10 percent/min and a ramp increase or decrease of 5 percent/min within the load range of 15 to 100 percent without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.
 - 2. Maintains reactor coolant average temperature T_{avg} within prescribed limits by creating the bank demand signal of full length rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies signals to pressurizer level control and steam dump control.
- B. Rod Control System
 - 1. Provides for reactor power modulation by manual or automatic control of full length control rod banks in a preselected sequence and for manual operation of individual banks.
 - 2. Systems for Monitoring and Indicating
 - a. Provide alarms to alert the operator if the required core reactivity shutdown margin is not available as a result of excessive control rod insertion.
 - b. Display control rod position.
 - c. Provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit.

C. Plant Control System Interlocks (table 7.7-1)

1. Prevent further withdrawal of the control banks when signal limits are approached that predict the approach of a departure from nucleate boiling ratio (DNBR) limit or kW/ft limit.
2. Inhibit automatic turbine load change as required by the nuclear steam supply system.

D. Pressurizer Pressure Control

Maintains or restores the pressurizer pressure to the design pressure +35 psi (which is well within reactor trip and relief and safety valve actuation setpoint limits) following normal operational transients that induce pressure changes by control (manual or automatic) of heaters and spray in the pressurizer. Also provides steam relief by controlling the power-operated relief valves.

E. Pressurizer Water Level Control

Establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature. Changes in level are caused by coolant density changes induced by loading, operational, and unloading transients. Level changes are produced by changing flow control (manual or automatic) as well as by manual selection of letdown orifices. Maintaining coolant level in the pressurizer within prescribed limits by actuating the charging and letdown system thus provides control of the reactor coolant water inventory.

F. Steam Generator Water Level Control

1. Establishes and maintains the steam generator water level to within predetermined physical limits during normal operating transients.
2. Restores the steam generator water level to within predetermined limits at unit trip conditions. Regulates the feedwater flow such that under operational transients the heat sink for the reactor coolant system does not decrease below a minimum. Steam generator water inventory control is manual or automatic through use of feedwater control valves.

G. Steam Dump Control

1. Permits the nuclear plant to accept a sudden 50 percent loss of net load without incurring reactor trip. Steam is dumped to the condenser as necessary to accommodate excess power generation in the reactor during turbine load reduction transients.
2. Ensures that stored energy and residual heat are removed following a reactor trip to bring the plant to equilibrium no-load conditions without actuation of the steam generator safety valves.

3. Maintains the plant at no-load conditions and permits a manually controlled cooldown of the plant.

H. Incore Instrumentation

Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

7.7.1.1 Reactor Control System

The reactor control system enables the nuclear plant to follow load changes automatically, including the acceptance of step load increase or decrease of 10 percent/min and ramp increases or decreases of 5 percent/min within the load range of 15 to 100 percent without reactor trip, steam dump, or pressure relief, subject to possible xenon limitations. The system is also capable of restoring coolant average temperature to within the programmed temperature deadband following a change in load. Manual control rod operation may be performed at any time.

The reactor control system controls the reactor coolant average temperature by regulation of control rod bank position.

The reactor coolant loop average temperatures are determined from hot leg and cold leg measurements in each reactor coolant loop. There is an average coolant temperature (T_{avg}) computed for each loop, where:

$$T_{avg} = \frac{T_{hot} + T_{cold}}{2}$$

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the median of the average measured temperatures (which is then processed through a lead lag compensation unit) from each of the reactor coolant loops constitutes the primary control signal, as shown in general in figure 7.7-1 and in more detail on the functional diagrams shown in drawing U-166239. The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full power condition. The median T_{avg} signal is also supplied to the pressurizer level control, steam dump control, and rod insertion limit monitoring systems.

The temperature inputs to the above control systems are derived using the median signal selector (MSS). The input signals to the MSS are provided by electronically isolated output signals from the protection channels.

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response.

7.7.1.2 Rod Control System

7.7.1.2.1 Full-Length Rod Control System

The full-length rod control system receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 5 to 45 in./min (8 to 72 steps/min) depending on the magnitude of the error signal. The rod direction demand signal is determined by the positive or negative value of the error signal. Manual control is provided to move a control bank in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15 percent of rated load, the operator may select the automatic mode, and rod motion is then controlled by the reactor control systems. A permissive interlock C-5 (see table 7.7-1) derived from measurements of turbine impulse chamber pressure prevents automatic control when the turbine load is below 15 percent. In the automatic mode, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment. The manual and automatic controls are further interlocked with the control interlocks. (See table 7.7-1.)

The shutdown banks are always in the fully withdrawn position during normal operation and are moved to this position at a constant speed by manual control prior to criticality. A reactor trip signal causes them to fall by gravity into the core. There are two shutdown banks.

The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All rod cluster control assemblies in a group are electrically paralleled to move simultaneously. There is individual position indication for each rod cluster control assembly.

Power to rod drive mechanisms is supplied by two motor generator sets operating from two separate three-phase buses. Each generator is the synchronous type and is driven by a 150-hp induction motor. The ac power is distributed to the rod control power cabinets through the two series-connected reactor trip breakers.

The variable speed full length rod control system rod drive programmer affords the ability to insert small amounts of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband and to furnish control at high speed. A summary of the rod cluster control assembly sequencing characteristics is given below.

- A. Two groups within the same bank are stepped such that the relative position of the groups will not differ by more than one step.
- B. The control banks are programmed such that withdrawal of the banks is sequenced in the following order: control bank A, control bank B, control bank C, and control bank D. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank withdrawn (bank D) is the first control bank inserted.

- C. The control bank withdrawals are programmed such that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank. When the first bank reaches the top of the core, it stops, while the second bank continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the unit reaches the desired power. The control bank insertion sequence is the opposite.
- D. Overlap between successive control banks is adjustable between 0 to 50 percent (0 and 115 steps), with an accuracy of 1 step.
- E. Rod speeds for either shutdown banks or control banks are capable of being controlled between a minimum of 8 steps/min and a maximum of 72 steps/min.

Surveillance testing of the Reactor Control System and the Rod Control System is performed at periodic intervals to detect failures that could lead to an increase in the rod speed.

7.7.1.3 Plant Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

The power range channels are important because of their use in monitoring power distribution in the core within specified safe limits. They are used to measure reactor power levels, axial power imbalance, and radial power imbalance. These channels are capable of recording overpower excursions up to 200 percent of full power. Suitable alarms are derived from these signals and are described below.

Basic power range signals are:

- A. Total current from a power range detector (four signals from separate detectors); these detectors are vertical and have an active length of 10 ft.
- B. Current from the upper half of each power range detector (four signals).
- C. Current from the lower half of each power range detector (four signals).

Derived from these basic signals are the following (including standard signal processing for calibration):

- A. Indicated nuclear flux (four).
- B. Indicated axial flux imbalance, derived from upper half flux minus lower half flux (four).

Alarm functions derived are as follows:

- A. Deviation (maximum minus minimum of four) in indicated nuclear power.

- B. Upper radial tilt (maximum to average of four) on upper half currents.
- C. Lower radial tilt (maximum to average of four) on lower half currents.

Additionally, provisions for monitoring axial flux difference are derived from the plant process computer using excore detector outputs.

Provision is made to trend the eight ion chamber signals, i.e., upper and lower currents for each detector. Nuclear power and axial imbalance is selectable for recording as well. Indicators are provided on the control board for nuclear power and for axial power imbalance.

A comprehensive discussion of the nuclear instrumentation system can be found in reference 1.

7.7.1.3.2 Rod Position Monitoring of Full-Length Rods

Two separate systems are provided to sense and display control rod position as described below:

A. Digital Rod Position Indication System

The digital rod position indication system measures the actual position of each full-length rod using a detector which consists of 42 discrete coils mounted concentrically with the rod drive pressure housing.

The coils are located axially along the pressure housing on 3.75-in. spacing. They magnetically sense the entry and presence of the rod drive shaft through the center line. The coils are interlaced into two data channels and are connected to the containment electronics (data A and B) by separate multiconductor cables. Multiplexing is used to transmit the digital position signals from the containment electronics to the control board display unit.

Unit 1

The digital position signal is displayed on the main control board by LCD monitors. Both colored bars and numeric values are shown to indicate the position for each rod. By employing two separate channels of information, the digital rod position indication system can continue to function (at reduced accuracy) when one channel fails.

Unit 2

The digital position signal is displayed on the main control board by light emitting diodes (LED) for each full length control rod. The one LED illuminated in the column shows the position for that particular rod. By employing two separate channels of information, the digital rod position indication system can continue to function (at reduced accuracy) when one channel fails.

Included in the system is a rod at bottom signal that operates a local alarm and a control room annunciator.

B. Demand Position System

The demand position system counts pulses generated in the rod drive control system to provide a digital readout of the demanded bank position.

The digital rod position indication and demand position systems are separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the demand and digital (actual) readings upon recognition of any apparent malfunction. Therefore, a single failure in rod position indication does not in itself lead the operator to take erroneous action in the operation of the reactor.

The demand position indication system is described in detail in reference 2 for the full length rods.

The digital rod position indication system and demand position system are discussed in the Technical Specifications and the Technical Requirements Manual.

7.7.1.3.3 Control Bank Rod Insertion Monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the reactor coolant system loop ΔT) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank:

- A. The low alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the chemical and volume control system.
- B. The low-low alarm alerts the operator to take immediate action to add boron to the reactor coolant system by any one of several alternate methods.

The purpose of the control bank rod insertion monitor is to give warning to the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip, provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection, and limits rod insertion such that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power, the allowable rod insertion limits must be decreased (the rods must be withdrawn further) with increasing power. Two parameters which are proportional to power are used as inputs to the insertion monitor. These are the ΔT between the hot leg and the cold leg, which is a direct function of reactor power, and T_{avg} , which is programmed as a function of power. The rod insertion monitor uses parameters for each control rod bank as follows:

$$Z_{LL} = A(\Delta T)_{median} + B(T_{avg})_{median} + C$$

FNP-FSAR-7

where:

Z_{LL} = Maximum permissible insertion limit for affected control bank.

$(\Delta T)_{\text{median}}$ = Median ΔT of all loops.

$(T_{\text{avg}})_{\text{median}}$ = Median T_{avg} of all loops.

A,B,C = Constants chosen to maintain $Z_{LL} \geq$ actual limit based on physics calculations.

The control rod bank demand position (Z) is compared to Z_{LL} as follows:

If $Z - Z_{LL} \leq D$, a low alarm is actuated.

If $Z - Z_{LL} \leq E$, a low-low alarm is actuated.

Since median values of T_{avg} and ΔT are always utilized, an accurate representation of power is used in the insertion limit calculation.

Actuation of the low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Administrative procedures require the operator to add boron through the chemical and volume control system. Actuation of the low-low alarm requires the operator to initiate emergency boration procedures. The value for E is chosen such that the low-low alarm would normally be actuated before the insertion limit is reached. The value for D is chosen to allow the operator to follow normal boration procedures. Figure 7.7-2 shows a block diagram representation of the control rod bank insertion monitor. The monitor is shown in more detail on the functional diagrams shown in drawing U-166239. In addition to the rod insertion monitor for the control banks, an alarm system is provided to warn the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are established by:

- A. Establishing the allowed rod reactivity insertion at full power consistent with the purposes given above.
- B. Establishing the differential reactivity worth of the control rods when moved in normal sequence.
- C. Establishing the change in reactivity with power level by relating power level to rod position.
- D. Linearizing the resultant limit curve. All key nuclear parameters in this procedure are measured as part of the initial and periodic physics testing program.

Any unexpected change in the position of the control bank under automatic control, or a change in coolant temperature under manual control, provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, samples are taken periodically of

coolant boron concentration. Variations in concentration during core life provide an additional check on the reactivity status of the reactor, including core depletion.

7.7.1.3.4 Rod Deviation Alarm

The demanded and measured rod position signals are displayed on the control board. They are also monitored by the plant computer which provides a visual printout and an audible alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors.

Figure 7.7-3 is a block diagram of the rod deviation comparator and alarm system.

7.7.1.3.5 Rod Bottom Alarm

A rod bottom signal for the full length rods in the digital rod position system, as described in reference 2, is used to operate a control relay, which generates the rod bottom-rod drop alarm.

7.7.1.4 Plant Control System Interlocks

The listing of the plant control system interlocks and a description of their derivations and functions are presented in table 7.7-1. It is noted that the designation numbers for these interlocks are preceded by "C". The development of these logic functions is shown in the functional diagrams (U-166239, U-166240, U-166241, U-166242, U-166243, U-166244, U-166245, and figure 7.2-1).

7.7.1.4.1 Rod Stops

Rod stops are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

Rod stops are the C-1, C-2, C-3, C-4, and C-5 control interlocks identified in table 7.7-1.

7.7.1.5 Pressurizer Pressure Control

The reactor coolant system pressure is controlled by using either the heaters (in the water region) or the spray (in the steam region) of the pressurizer plus steam relief for large transients. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure controlled signal demands approximately 100 percent proportional heater power.

The spray nozzles are located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Two power-operated relief valves limit system pressure for large positive pressure transients. In the event of a large load reduction not exceeding the design plant load rejection capability, the pressurizer power-operated relief valves might be actuated for the most adverse conditions, e.g., the most negative Doppler coefficient and the minimum incremental rod worth. The relief capacity of the power-operated relief valves is sized large enough to limit the system pressure to prevent actuation of high pressure reactor trip for the above condition.

A block diagram of the pressurizer pressure control system is shown in figure 7.7-4.

7.7.1.6 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant adjusts to the various temperatures, the steam water interface moves to absorb the variations with relatively small pressure disturbances.

The water inventory in the reactor coolant system is maintained by the chemical and volume control system. During normal plant operation, the charging flow varies to produce the flow demanded by the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the median average temperature being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the main control room.

A block diagram of the pressurizer water level control system is shown in figure 7.7-5.

7.7.1.7 Steam Generator Water Level Control

Each steam generator is equipped with a three-element feedwater flow control system, which maintains a constant level to ensure the feedring and spray nozzles are covered during normal operation. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, the fixed level setpoint, and the pressure compensated steam flow signal. The water level signal provided to the feedwater flow control system is derived from an MSS which selects the median input of the three narrow range level channels for each steam generator. In addition, for the turbine-driven main feedwater pumps, the feedwater pump speed is varied to maintain a programmed

pressure differential between the steam header and the feed pump discharge header. The speed controller continuously compares the actual ΔP with a programmed ΔP_{ref} which is the linear function of steam flow. (See figure 7.7-6.) Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual control of the feedwater control system is available at all times.

A block diagram of the steam generator water level control system with an MSS is shown in figure 7.7-7. The MSS will automatically select one of the steam generator input signals as the control signal in the event of an MSS failure. A detailed discussion of the MSS and its operation can be found in section 7.2, reference 17.

7.7.1.8 Steam Dump Control

The steam dump system is designed to accept a 50-percent loss of net load without tripping the reactor.

The automatic steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the reactor coolant system. By bypassing main steam directly to the condenser, an artificial load is thereby maintained on the primary system. The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The plant has a 50-percent loss of net load capability. The steam dump steam flow capacity is 40 percent of full load steam flow at full load steam pressure.

If the difference between the reference $T_{avg}(T_{ref})$ based on turbine impulse chamber pressure and the lead/lag compensated median T_{avg} exceeds a predetermined amount and if the interlock mentioned below is satisfied, a demand signal will actuate the steam dump to maintain the reactor coolant system temperature within control range until a new equilibrium condition is reached.

To prevent actuation of steam dump on small load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure. It is provided to unblock the dump valves when the rate of load rejection exceeds a preset value corresponding to a 10-percent step load decrease or a sustained ramp load decrease of 5 percent/min.

A block diagram of the steam dump control system is shown in figure 7.7-8.

7.7.1.8.1 Load Rejection Steam Dump Controller

This circuit prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is a difference between the lead/lag compensated median T_{avg} , and the reference T_{avg} (i.e., T_{ref}) is based on turbine impulse chamber pressure.

The T_{avg} median signal is the same as that used in the reactor control system. The lead/lag compensation for the T_{avg} signal is to compensate for lags in the plant thermal response and in valve positioning. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase, thus generating an immediate demand signal for steam dump. Since control rods are available in this situation, steam dump terminates as the error comes within the maneuvering capability of the control rods.

7.7.1.8.2 Plant Trip Steam Dump Controller

Following a reactor trip, as sensed by the reactor trip signal (P-4), the load rejection steam dump controller is defeated and the plant trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the lead/lag compensated median T_{avg} and the no-load reference T_{avg} . When the error signal exceeds a predetermined setpoint, the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude, indicating that the reactor coolant system T_{avg} is being reduced toward the reference no-load value, the dump valves are modulated by the plant trip controller to regulate the rate of removal decay heat and thus gradually establish the equilibrium hot shutdown condition.

The error signal determines whether a group of valves is to be tripped open or modulated open. In either case, they are modulated when the error is below the trip open setpoints.

7.7.1.8.3 Steam Header Pressure Controller

Residual heat removal is maintained by the steam generator pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers which are used during the initial transient following turbine/reactor trip or load rejection.

7.7.1.9 Incore Instrumentation

The incore instrumentation system consists of chromel alumel thermocouples at fixed core outlet positions and movable miniature neutron detectors which can be positioned at the center of selected fuel assemblies anywhere along the length of the fuel assembly vertical axis. The basic system for insertion of these detectors is shown in figure 7.7-9. Sections 1 and 2 of reference 3 outline the incore instrumentation system in more detail.

7.7.1.9.1 Thermocouples

Chromel alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies and terminate at the exit flow end of the fuel assemblies and the reactor vessel head plenum. The thermocouples are provided with two primary seals, a core exit thermocouple nozzle assembly and swage-type seal from conduit to head. The thermocouples are supported in guide tubes in the upper core support assembly.

7.7.1.9.2 Movable Neutron Flux Detector Drive System

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. See reference 3 for neutron flux detector parameters. The stainless steel detector shell is welded to the leading end of helical wrap drive cable and to stainless steel sheathed coaxial cable. The retractable thimbles into which the miniature detectors are driven are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table.

The thimbles are closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal line. During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal line is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of drive assemblies, five-path rotary transfer operation selector assemblies, and ten-path rotary transfer selector assemblies as shown in figure 7.7-9. These assemblies are described in reference 3. The drive system pushes hollow helical wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter, sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor which pushes a helical wrap drive cable and detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

The leakage detection and gas purge provisions are discussed in reference 3.

Manual isolation valves (one for each thimble) are provided for closing the thimbles. When closed, the valve forms a 2500-psig barrier. The manual isolation valves are not designed to isolate a thimble while a detector/drive cable is inserted into the thimble. The detector/drive cable must be retracted to a position above the isolation valve prior to closing the valve.

A small leak would probably not prevent access to the isolation valves and thus a leaking thimble could be isolated during a hot shutdown. A large leak might require cold shutdown for access to the isolation valve.

7.7.1.9.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position.

The thimbles are distributed nearly uniformly over the core with about the same number of thimbles in each quadrant. The control system consists of two sections, one physically mounted with the drive units and the other contained in the control room. Limit switches in each transfer

device provide feedback of path selection operation. Each gear box drives an encoder for position feedback. One five-path operation selector is provided for each drive unit to insert the detector in one of five functional modes of operation. A ten-path rotary transfer assembly is a transfer device that is used to route a detector into any one of up to ten selectable paths. A common path is provided to permit cross-calibration of the detectors.

The control room contains the necessary equipment for control, position indication, and flux recording for each detector. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting, and gain controls.

Flux mapping consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from top to a point below the bottom. In a similar manner other core locations are selected and plotted. Each detector provides axial flux distribution data along the center of a fuel assembly. Various radial positions of detectors may then be compared to obtain a flux map for a region of the core.

The thimbles are distributed nearly uniformly over the core with approximately the same number of thimbles in each quadrant. The number and location of these thimbles have been chosen to permit measurement of local to average peaking factors to an accuracy of ± 5 percent (95 percent confidence). Measured nuclear peaking factors will be increased by 5 percent to allow for this accuracy when using ≥ 38 detector thimbles. When using ≥ 25 and < 38 detector thimbles, the measurement uncertainty is increased by $[2\{3 - (T/12.5)\}]$, where T equals the number of detector thimbles (reference 4). If the measured power peaking is larger than acceptable, reduced power capability will be indicated.

Operating plant experience has demonstrated the adequacy of the incore instrumentation in meeting the design bases stated.

7.7.1.10 Control Board

Control board switches and associated lights are furnished in modules. Modules provide a degree of physical protection for the switches, associated lights, and wiring.

The control board layout is based on operator ease in relating the control board devices to the physical plant and in determining at a glance the status of related equipment. This is referred to as providing a functional layout. Within the boundaries of a functional layout, modules are arranged in columns of control functions associated with separation trains defined for reactor protection and engineered safeguards systems. Teflon wire is used within the module and between the module and the first termination point.

Termination cabinets located under the control board are used. Train A and B termination cabinets are physically separated. Shielded (braid) cable then go through slots (A in front, B in back) in the floor into their respective tray system which routes the cable to the termination cabinet.

Mutually redundant safety train wiring is routed to maintain a minimum of 6 in. of air separation between wires associated with different trains. Where such air separation is not available, barriers are provided in lieu of air space.

A device such as braided sheath material (known as shielding and bonding cable) is used to provide a barrier in lieu of the 6-in. dimension. An example of this sheath material is Belden braid. When this sheath material is used to provide physical separation, it is sized and secured to the wire bundle to provide a minimum of 90 percent surface coverage.

In order to maintain separation between wiring associated with different trains, mutually redundant safety train wiring is not terminated on a single device. Backup manual actuation switches link the separate trains by mechanical means to provide greater reliability of operator action for the manual reactor trip function and also for the manual engineered safety features actuations. The linked switches are themselves redundant, so that operation of either set of linked switches will actuate safety trains A and B simultaneously. For example, the manual reactor trip circuit will have an A train switch and a B train switch in different board locations not linked in any way. The A train switch may be linked mechanically to a backup B train switch, and similarly the B train switch may be linked with a backup A train switch in a dual module containing outputs to both safety trains.

7.7.1.11 Boron Concentration Measurement System

The boron concentration measurement system employs a sample measurement unit which contains a neutron source and a neutron detector located in a shield tank. (See figure 7.7-10.) Piping within the shield tank is arranged to maintain coolant sample flow between the neutron source and the neutron detector. Neutron absorption by the boron in the coolant sample flow reduces the number of neutrons which contact the detector per unit time. Therefore, the time required to count a fixed number of neutron contacts is variable and dependent upon the concentration of boron solution. Electronic circuitry in the console portion of the boron concentration measurement system accepts an amplified signal from the sample measurement unit and converts the signal to a digital display of ppm boron. The digital display is housed in the console, which may be located up to 5000 ft from the sample measurement unit.

A. Sample Measurement Unit

The sample measurement unit consists of a cylindrical steel tank mounted on steel legs. (See figure 7.7-11). The sample tank is filled with ordinary tap water which is heated to a temperature of approximately 125°F. A coiled heat exchanger is immersed in the sample tank water. The coolant sample temperature is stabilized in the heat exchanger prior to entering the vertical sample chamber. A neutron detector is located in the sample chamber and the coolant sample flows past it.

A neutron source is located outside the sample chamber. (See figure 7.7-11). The reactor coolant sample enters the top of the tank, flows through the heat exchanger and into the bottom of the sample chamber, continues upward past the neutron detector, out of the top of tank through a flow meter, and returns to the chemical and volume control system. Sample flow and pressure are

FNP-FSAR-7

measured and displayed locally. The local flow indicator displays flow within the range of 0 to 1 gal/min. An immersion heater and temperature controller regulate the sample tank water temperature. Local temperature indication is also provided.

In addition to providing for coolant sample temperature control, the tank water also serves as shielding for the neutron source. The volume of water in the tank provides sufficient shielding to limit the radiation levels from a 5-Ci neutron source to less than 2 mr/h at 24 in. from all tank surfaces. In the event of a complete loss of water shielding, the radiation levels would rise to approximately 3.15 mr/h due to gamma and 20 mr/h due to neutrons. These levels should not cause a personnel hazard for short term exposure.

The measurement unit is designed so that all tank connections are at the top to eliminate the possibility of loss of water shielding through accidental leakage. In addition, two water level devices, an alarm and indicator, are provided locally to signal a low water level in the tank. One device actuates a set of contacts on the tank when the water level exceeds a predetermined low level setpoint. The second device provides local level indication.

B. Electronic Console

The electronic console unit is a standard instrument cabinet containing the electronic circuitry and equipment for processing the information received from the measurement unit and for displaying the boron concentration measurement.

A block type schematic diagram of the system is shown in figure 7.7-12. The low level signal from the neutron detector is input to a preamplifier. The output of the preamplifier is coupled to a discriminator which eliminates noise and gamma pulses by pulse height discrimination. The discriminator is followed by a pulse amplifier which drives the logic circuitry of the boron system time unit. This unit measures the count rate for a statistically meaningful period of time and converts the count rate to ppm boron. The output signal from the boron system time unit is transmitted to a digital display where the signal is continuously displayed until a new value is measured and transmitted.

The boron concentration measurement system is designed for use as an advisory system. It is not designed as a safeguards system or component of a safeguards system. The boron concentration measurement system is not part of a control element or control system, nor is it designed for this use. No credit is taken for this system in any accident analysis. Therefore, redundancies of measurement components, self-checking subsystems, malfunction annunciations, and diagnostic circuitry are not included in this system. As a general operating aid it provides information as to when additional check analysis are warranted rather than a basis for fundamental operating decisions.

- A. The boron concentration measurement system measures the neutron absorption characteristics of the reactor coolant, which is directly related to the concentration of natural boron which would produce the same absorption characteristic; the system reports the measurement in terms of ppm total natural

boron. Accurate measurement of the boron worth in terms of natural boron in the reactor coolant is therefore provided irrespective of the boron-10 to total boron ratio which exists. During normal plant operations, the boron concentration varies between 0 and 1800 ppm. The boron concentration measurement system operates within a ± 10 ppm range as shown in figure 7.7-13. This curve presumes sufficient readings to eliminate statistical errors, etc.

- B. The boron concentration measurement system provides continuous monitoring of the reactor coolant boron concentration. Therefore, adjustments of boron concentration in the reactor coolant can be monitored as they are being made. Further, the plant operators can monitor boron concentration directly. There is no time lapse or personnel requirement for collection and laboratory analysis of reactor coolant samples, nor is there any waste material to be processed.
- C. Limited device monitoring is provided to prevent system damage due to heater malfunction. If the heater fails in the off position, the shield tank will come to room temperature. If the malfunction occurs in the on position, the shield water temperature will rise. If no corrective action is taken, the water level will drop as a result of evaporation. A local high temperature alarm and low water level are provided to indicate this condition. Local temperature and level instruments are also provided. If no corrective action is taken, the water will continue to evaporate and the heater element will be exposed to air and will result in damage to the heater. Holes are provided in the top cover to allow for evaporation eliminating the expansion problem and also to allow for additional water if needed. The abnormal reactor coolant sample temperature would cause erroneous boron concentration readings. Erroneous readings would be detected by the operator, since boron concentration changes would affect reactivity control and since changes in reactivity would be indicated on other instruments.
- D. The output of the neutron detector is coupled to a preamplifier which is located on the top of the measurement unit. This is the most desirable location, since it keeps the cable to the detector short, lessens the chance for noise pickup, lessens line reflections which can cause multiple counting, and keeps signal attenuation to a minimum. This also permits location of the electronic console remote from the detector.
- E. System characteristics are listed in table 7.7-2.

7.7.2 ANALYSIS

The plant control systems are designed to ensure high reliability in any anticipated operational occurrences.

Equipment used in these systems is designed and constructed to maintain a high level of reliability.

Proper positioning of the control rods is monitored in the control room by bank arrangements of the individual position columns meters for each rod cluster control assembly. A rod deviation

alarm alerts the operator of a deviation of one rod cluster control assembly from the other rods in that bank position. There are also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the control room for each full length rod cluster control assembly. Four excore long ion chambers also detect asymmetrical flux distribution indicative of rod misalignment.

Overall reactivity control is achieved by the combination of soluble boron and rod cluster control assemblies. Long term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short term reactivity control for power changes is accomplished by the plant control system which automatically moves rod cluster control assemblies. This system uses input signals including neutron flux, coolant temperature, and turbine load.

The plant control systems will prevent an undesirable condition in the operation of the plant that, if reached, will be protected by reactor trip. The description and analysis of this protection is covered in section 7.2. Worst case failure modes of the plant control systems are postulated in the analysis of off-design operational transients and accidents covered in chapter 15, such as the following:

- A. Uncontrolled rod cluster control assembly withdrawal from a subcritical condition.
- B. Uncontrolled rod cluster control assembly withdrawal at power.
- C. Rod cluster control assembly misalignment.
- D. Loss of external electrical load and/or turbine trip.
- E. Loss of all ac power to the station auxiliaries (station blackout).
- F. Excessive heat removal due to feedwater system malfunctions.
- G. Excessive load increase.

These analyses show that a reactor trip setpoint is reached in time to protect the health and safety of the public under these postulated incidents and that the resulting coolant temperatures produce a DNBR well above the safety analysis limit. Thus, there will be no cladding damage and no release of fission products to the reactor coolant system under the assumption of these postulated worst case failure modes of the plant control systems.

7.7.2.1 Separation of Protection and Control Systems

In some cases, it is advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Accordingly, the design meets the requirements of General Design Criterion 24. Test results have shown that a short circuit, or the application of 118 V-ac or 140 V-dc on the isolated output portion of the circuit (the nonprotective side of the circuit), will not affect the input (protective) side of the circuit.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action, even when degraded by a second random failure. This meets the applicable requirements of section 4.7 of Institute of Electrical and Electronics Engineers standard 279.

The loop T_{avg} and ΔT channel required inputs to the steam dump system, reactor control system, the control rod insertion monitor, and the pressurizer level control system are electrically isolated prior to being routed to the control cabinets. A median signal is then selected for T_{avg} and ΔT in the control cabinets utilizing a separate median signal selector (MSS) for the T_{avg} and ΔT input signals to the appropriate control systems.

The pressurizer pressure channels needed to derive the control signals are physically isolated from the pressure channels used to derive protection signals.

7.7.2.2 Response Considerations of Reactivity

Reactor shutdown with control rods is completely independent of the control functions, since the trip breakers interrupt power to the full-length rod drive mechanisms regardless of existing control signals. The design is such that the system can withstand accidental withdrawal of control groups or unplanned dilution of soluble boron without exceeding acceptable fuel design limits. Thus, the design meets the applicable requirements of General Design Criterion 25.

No single electrical or mechanical failure in the rod control system could cause the accidental withdrawal of a single rod cluster control assembly from the partially inserted bank at full power operation. Furthermore, as a result of Generic Letter 93-04, Rod Control System Failure and Withdrawal of Rod Control Cluster Assemblies, 10 CFR 50.54(f), tests are performed following each refueling outage which ensure that the proper timing, communication, and regulation are maintained. Based on WCAP-13864-A Rev. 1, these tests will identify a component failure which may be undetectable during normal testing. The operator could deliberately withdraw a single rod cluster control assembly in the control bank; this feature is necessary to retrieve a rod, should one be accidentally dropped. In the extremely unlikely event of simultaneous electrical failures that could result in single rod cluster control assembly withdrawal, rod deviation would be displayed on the plant annunciator, and the rod position indicators would indicate the relative positions of the rods in the bank. Withdrawal of a single rod cluster control assembly by operator action, whether deliberate or by a combination of errors, would result in activation of the same alarm and the same visual indications.

Each bank of control and shutdown rods in the system is divided into two groups of up to four or five mechanisms each. The rods comprising a group operate in parallel through multiplexing thyristors. The two groups in a bank move sequentially so that the first group is always within one step of the second group in the bank. A definite schedule of actuation or deactuation of the stationary gripper, movable gripper, and lift coils of a mechanism is required to withdraw the rod cluster control assembly attached to the mechanism. Since the four stationary grippers, movable grippers, and lift coils associated with the rod cluster control assemblies of a rod group are driven in parallel, any single failure that could cause rod withdrawal would affect a minimum

FNP-FSAR-7

of one group of rod cluster control assemblies. Mechanical failures are in the direction of insertion or immobility.

The identified multiple failure involving the least number of components consists of open circuit failure of the proper 2 out of 16 wires connected to the gate of the lift coil thyristors. The probability of open wire (or terminal) failure is $0.016 \times 10^{-6}/h$ by MIL-HDB217A. These wire failures would have to be accompanied by failure, or disregard, of the indications mentioned above. The probability of this occurrence is therefore too low to have any significance.

Concerning the human element, to withdraw a single rod cluster control assembly erroneously, the operator would have to improperly set the bank selector switch, the lift coil disconnect switches, and the in-hold-out switch. In addition, the three indicators would have to be disregarded or ineffective. Such series of errors would require a complete lack of understanding and administrative control. A probability number cannot be assigned to a series of errors such as these.

The rod position indication system provides direct visual displays of each control rod assembly position. The plant computer alarms for deviation of rods from their banks. In addition, a rod insertion limit monitor provides an audible and visual alarm to warn the operator of an approach to an abnormal condition due to dilution. The low-low insertion limit alarm alerts the operator to follow emergency boration procedures. The facility reactivity control systems are such that acceptable fuel damage limits will not be exceeded even in the event of a single malfunction of either system.

An important feature of the control rod system is that insertion is provided by gravity fall of the rods.

In all analyses involving reactor trip, the single highest worth rod cluster control assembly is postulated to remain untripped in its full out position.

One means of detecting a stuck control rod assembly is available from the actual rod position information displayed on the control board. The control board position readouts, one for each full length rod, give the plant operator the actual position of the rod in steps. The indications are grouped by banks (e.g., control bank A, control bank B, etc.) to indicate to the operator the deviation of one rod with respect to other rods in a bank. This serves as a means to identify rod deviation.

The plant computer monitors the actual position of all rods. Should a rod be misaligned from the other rods in that bank by more than 7.5 in., the rod deviation alarm is actuated.

Misaligned rod cluster control assemblies are also detected and alarmed in the control room via the flux tilt monitoring system which is independent of the plant computer.

Isolated signals derived from the nuclear instrumentation system are compared with one another to determine whether a preset amount of deviation of average power has occurred. Should such a deviation occur, the comparator output will operate a bistable unit to actuate a control board annunciator. This alarm will alert the operator to a power imbalance caused by a misaligned rod. By use of individual rod position readouts, the operator can determine the

deviating control rod and take corrective action. Thus, the design of the plant control systems meets the requirements of General Design Criterion 23.

The boron system can compensate for all xenon burnout reactivity transients without exception.

The rod system can compensate for xenon burnout reactivity transients over the allowed range of rod travel. Xenon burnout transients of larger magnitude must be accommodated by boration or by reactor trip (which eliminates the burnout).

The boron system is not used to compensate for the reactivity effects of fuel/water temperature changes accompanying power level changes.

The rod system can compensate for the reactivity effects of fuel/water temperature changes accompanying power level changes over the full range from full load to no load at the design maximum load uprate.

Automatic control of the rods is, however, limited to the range of approximately 15 to 100 percent of rating.

The boron system will maintain the reactor in the cold shutdown state irrespective of the disposition of the control rods.

7.7.2.3 Step Load Changes Without Steam Dump

The plant control system restores equilibrium conditions, without a trip, following a ± 10 percent step change in load demand over the 15 to 100 percent power range for automatic control. Steam dump is blocked for load decrease less than or equal to 10 percent. A load demand greater than full power is prohibited by the turbine control load limit function of the DEH control system.

The plant control system minimizes the reactor coolant average temperature deviation during the transient within a given value and restores average temperature to the programmed setpoint. Excessive pressurizer pressure variations are prevented by using spray, heaters, and power relief valves in the pressurizer.

The control system must limit nuclear power overshoot to acceptable values following a 10 percent increase in load to 100 percent.

7.7.2.4 Loading and Unloading

Ramp loading and unloading of 5 percent/min can be accepted over the 15 to 100 percent power range under automatic control without tripping the plant. The function of the control system is to maintain the coolant average temperature as a function of turbine-generator load.

The coolant average temperature increases during loading and causes a continuous surge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading,

there is a continuous outsurge from the pressurizer resulting from coolant contraction. The pressurizer heaters limit the resulting system pressure decrease. The pressurizer water level is programmed so that the water level is above the setpoint for heater cutout during the loading and unloading transients. The primary concern during loading is to limit the overshoot in nuclear power and to provide sufficient margin in the overtemperature ΔT setpoint.

The automatic load controls are designed to adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

7.7.2.5 Load Rejection Furnished by Steam Dump System

When a load rejection occurs, if the difference between the required temperature setpoint of the reactor coolant system and the actual average temperature exceeds a predetermined amount, a signal will actuate the steam dump to maintain the reactor coolant system temperature within control range until a new equilibrium condition is reached.

The reactor power is reduced at a rate consistent with the capability of the rod control system. Reduction of the reactor power is automatic. The steam dump flow reduction is as fast as rod cluster control assemblies are capable of inserting negative reactivity.

The rod control system can then reduce the median reactor coolant temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is 40 percent of full load steam flow at full load steam pressure.

The steam dump flow reduces proportionally as the control rods act to reduce the average coolant temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The dump valves are modulated by the temperature error signal ($T_{avg} - T_{ref}$). The required number of steam dump valves can be tripped quickly to stroke full open or modulate, depending upon the magnitude of the temperature error signal resulting from loss of load.

7.7.2.6 Turbine-Generator Trip with Reactor Trip

Whenever the turbine-generator unit trips at an operating power level above permissive P-9, the reactor also trips. The unit is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the equivalent saturation pressure of the safety valve setpoint. The thermal capacity of the reactor coolant system is greater than that of the secondary system, and because the full load average temperature is greater than the no-load temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for a trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators.

The steam dump system is controlled from the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. With the dump valves

FNP-FSAR-7

open, the average coolant temperature starts to reduce quickly to the no-load setpoint. A direct feedback of temperature acts to proportionally close the valves to minimize the total amount of steam which is bypassed.

The feedwater flow is cut off when the average coolant temperature decreases below a given temperature following the reactor trip (or when the steam generator water level reaches a given high level).

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level while ensuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers, which are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and water level fall rapidly during the transient because of coolant contraction. If heaters become uncovered following the trip, they are deenergized and the chemical and volume control system will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

The steam dump and feedwater control systems are designed to prevent the average coolant temperature from falling below the programmed no-load temperature following the trip to ensure adequate reactivity shutdown margin.

REFERENCES

1. Lipchak, J. B. and Stokes, R. A., "Nuclear Instrumentation System," WCAP-7669, April 1971.
2. Blanchard, A. E., "Rod Position Monitoring," WCAP-7571, March 1971.
3. Loving, J. J., "In-Core Instrumentation (Flux Mapping System and Thermocouples)," WCAP-7607, July 1971.
4. FNP RER SNC799923-01, "Farley Unit 1 & 2 Movable Incore Detector System Thimble Reduction Study."

BIBLIOGRAPHY

Blanchard, A. E. and Calpin, J. E., "Digital Rod Position Indication," WCAP-8014, December 1972.

Blanchard, A. E. and Katz, D. N., "Solid State Rod Control System, Full Length," WCAP-7778, December 1971.

TABLE 7.7-1 (SHEET 1 OF 2)
PLANT CONTROL SYSTEM INTERLOCKS

<u>Designation</u>	<u>Derivation</u>	<u>Function</u>
C-1	1/2 neutron flux (intermediate range) above setpoint	Blocks automatic and manual control rod withdrawal
C-2	1/4 neutron flux (power range) above setpoint	Blocks automatic and manual control rod withdrawal
C-3	2/3 overtemperature ΔT above setpoint	Blocks automatic and manual control rod withdrawal
C-4	2/3 overpower ΔT above setpoint	Blocks automatic and manual control rod withdrawal
C-5	1/1 turbine impulse chamber pressure below setpoint	Blocks automatic control rod withdrawal
C-7	1/1 time derivative (absolute value) of turbine impulse chamber pressure (decrease only) above setpoint	Makes steam dump valves available for either tripping or modulation

TABLE 7.7-1 (SHEET 2 OF 2)

<u>Designation</u>	<u>Derivation</u>	<u>Function</u>
C-9	Any condenser pressure above setpoint	Blocks steam dump to condenser
	or	
	All circulation water pump breakers open	
C-11	1/1 bank D control rod position above setpoint	Blocks automatic rod withdrawal
C-20	Two-of-two turbine impulse chamber pressure above setpoint	Arms AMSAC; below setpoint, blocks AMSAC (Generated in AMSAC; see section 7.8.) Control grade only.
P-4 ^(a)	Reactor Trip	Closes main feedwater valves on low T_{avg} below setpoint
		Blocks steam dump control via load rejection T_{avg} controller
		Makes steam dump valves available for either tripping or modulation
	Reactor not tripped	Block steam dump control via plant trip T_{avg} controller

(a) See table 7.3-4 for safety functions.

TABLE 7.7-2

BORON CONCENTRATION MEASUREMENT SYSTEM SPECIFICATIONS

Operating Conditions

Line voltage: 120 V-AC (± 10 percent); 60 Hz (± 1 percent)

Pressure: 15 to 225 psig (sample)

Temperature: 70°F to 130°F (sample)

Sample flowrate: 0 to 0.4 gal/min

Ambient temperature: 60°F to 105°F

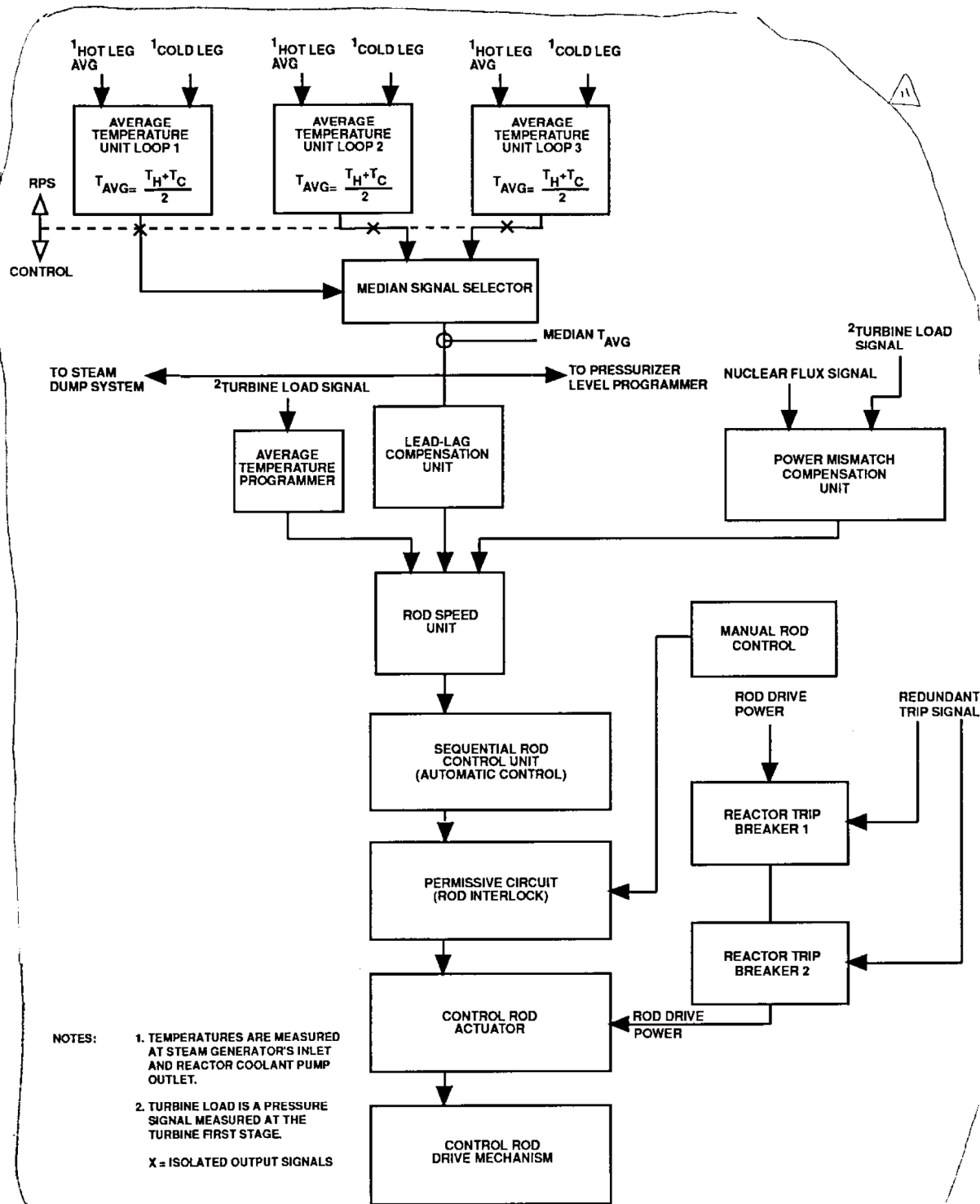
Relative humidity: to 95 percent

Radiation levels: < 2 mr/h at 24 in. from all tank surfaces

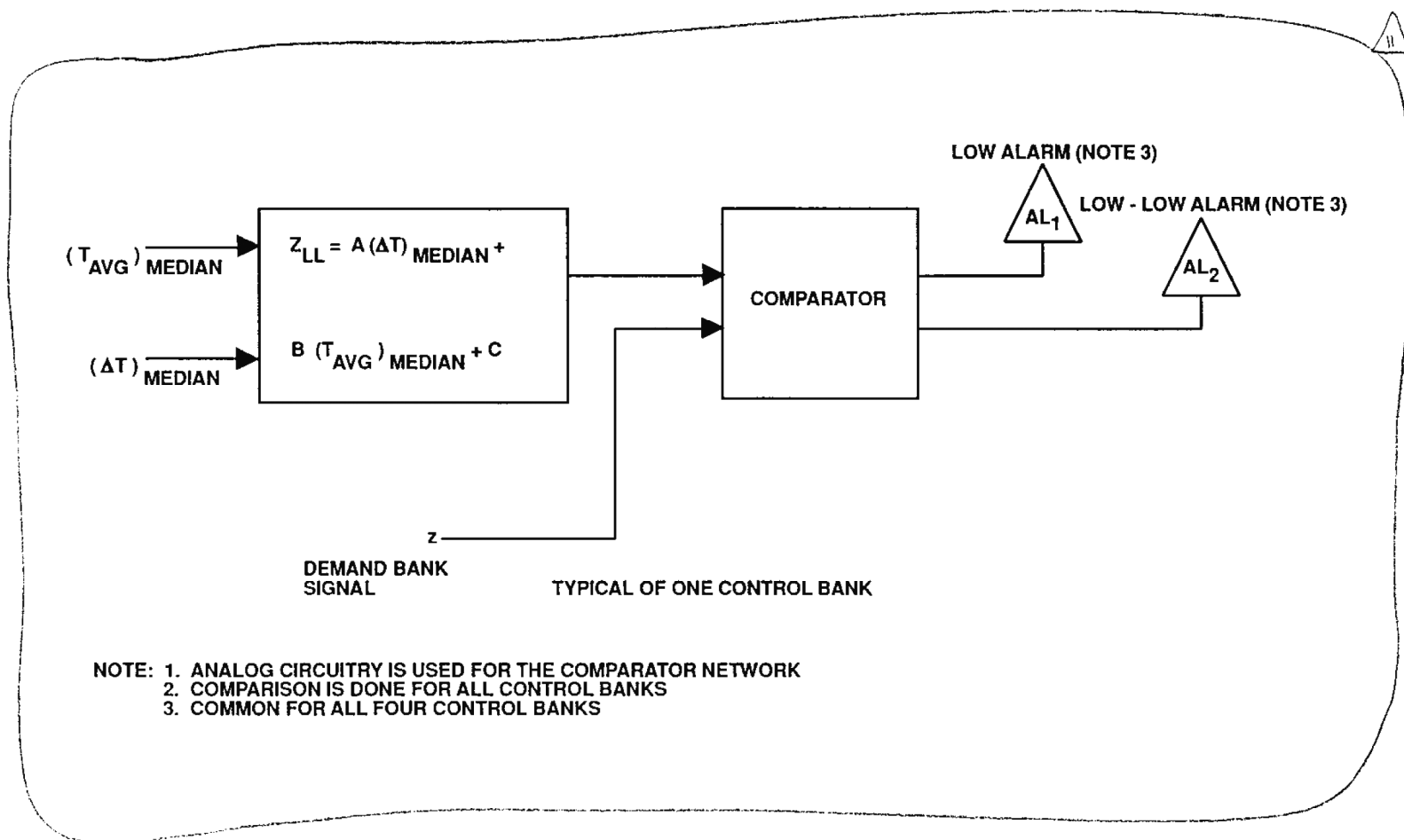
Reading time: Variable depending on boron concentration; maximum time for 5000 ppm is approximately 5 min

Accuracy

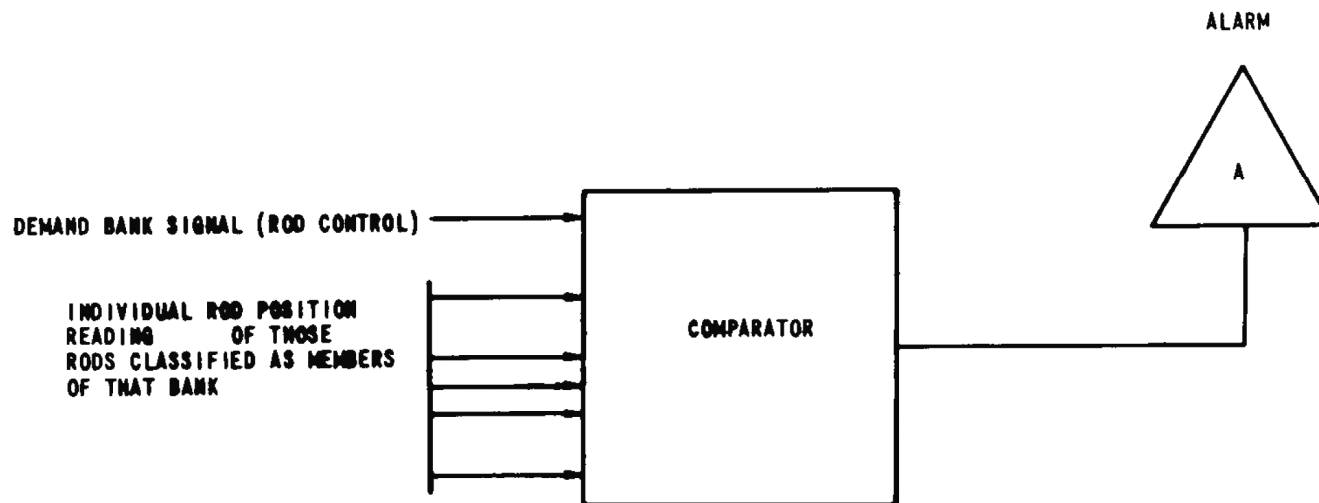
<u>Boron ppm of Water</u>	<u>Accuracy Standard Deviation</u>
0 - 1800 ppm	± 10 ppm
1800 - 5000 ppm	± 1.25 percent
Drift: Less than 10 ppm/week	



REV 21 5/08

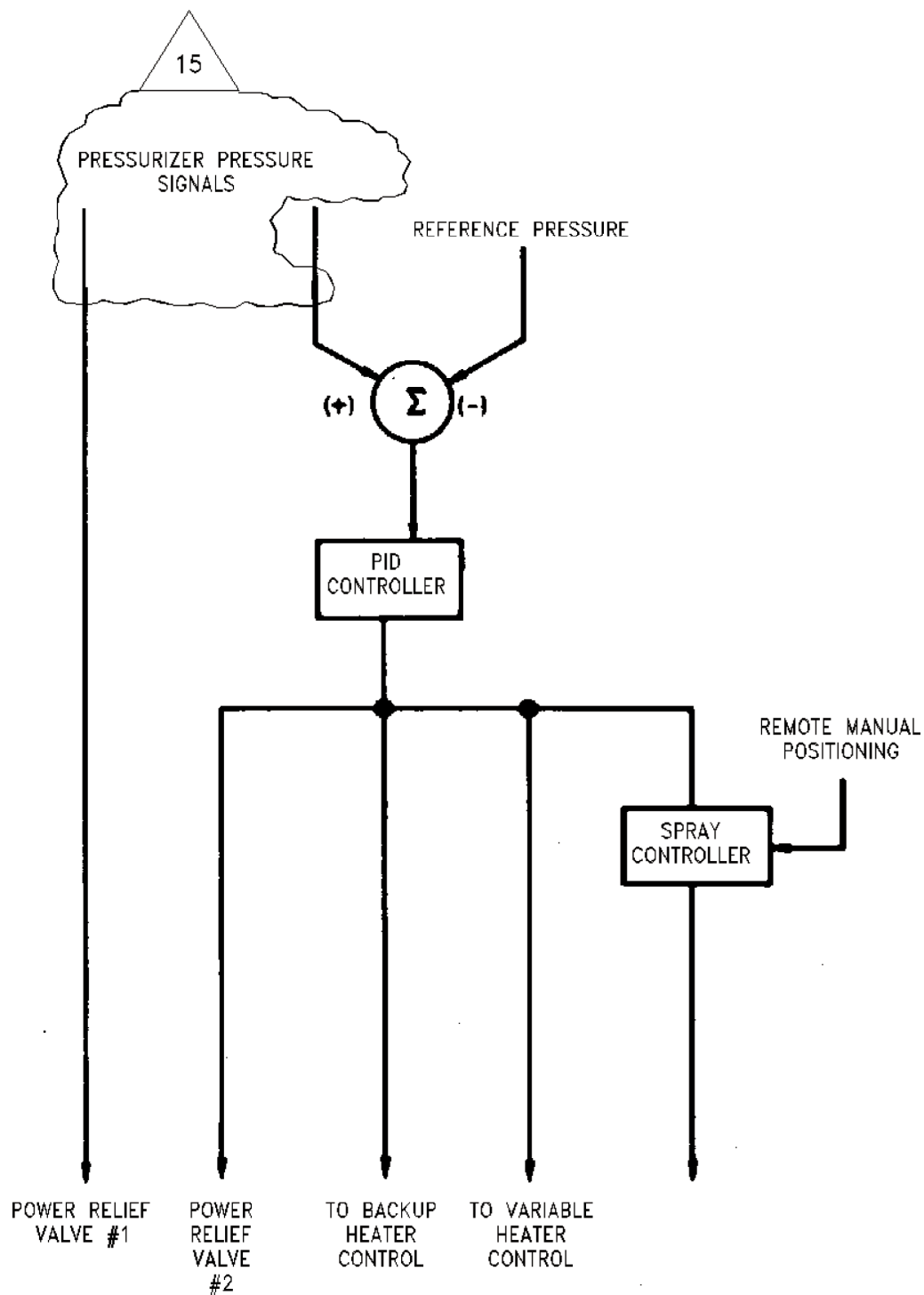


REV 21 5/08

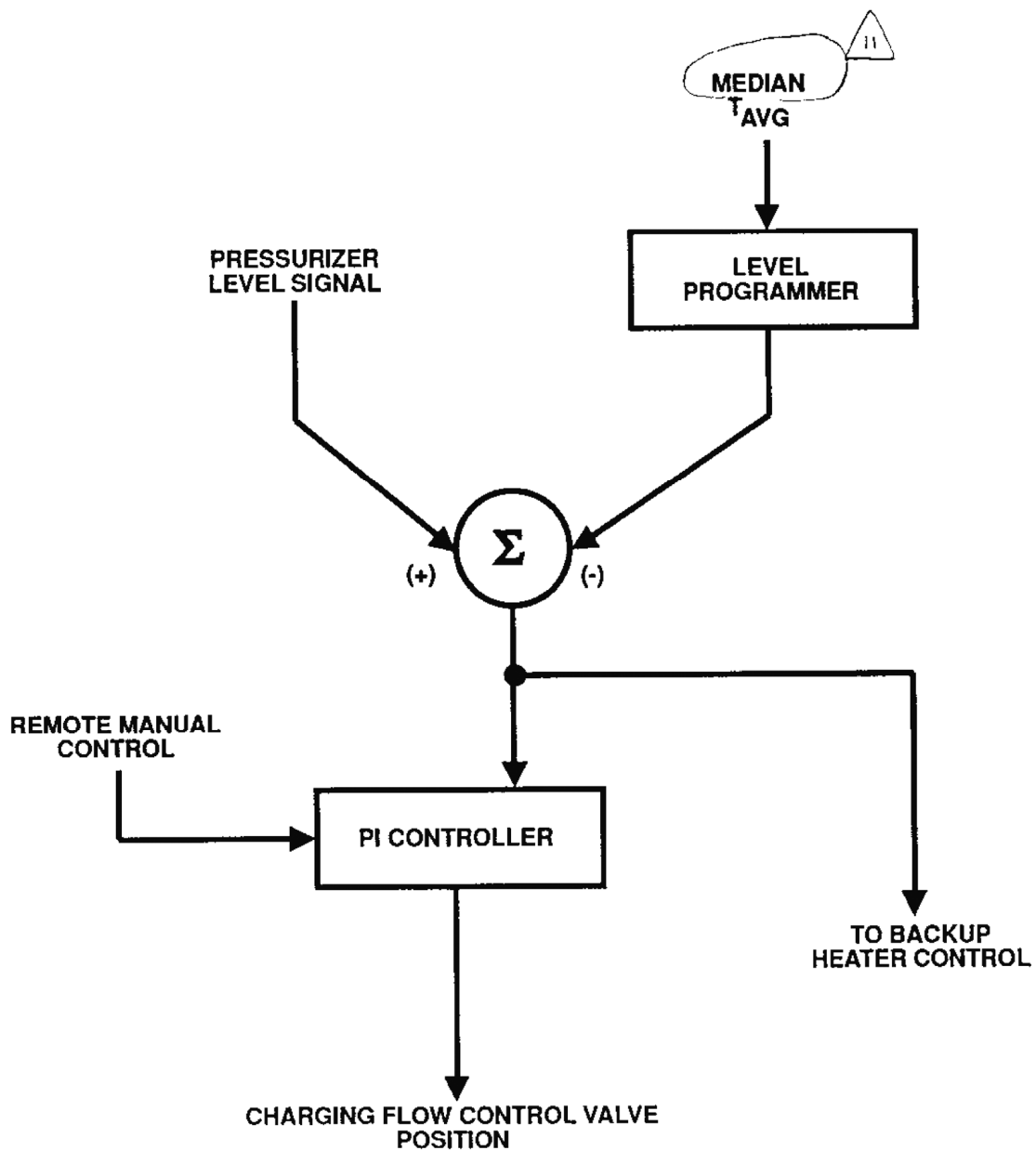


- NOTE:
1. DIGITAL OR ANALOG SIGNALS MAY BE USED FOR THE COMPARATOR COMPUTER INPUTS.
 2. THE COMPARATOR WILL ENERGIZE THE ALARM IF THERE EXISTS A POSITION DIFFERENCE GREATER THAN A PRESENT LIMIT BETWEEN ANY INDIVIDUAL ROD AND THE DEMAND BANK SIGNAL.
 3. COMPARISON IS INDIVIDUALLY DONE FOR ALL CONTROL BANKS.

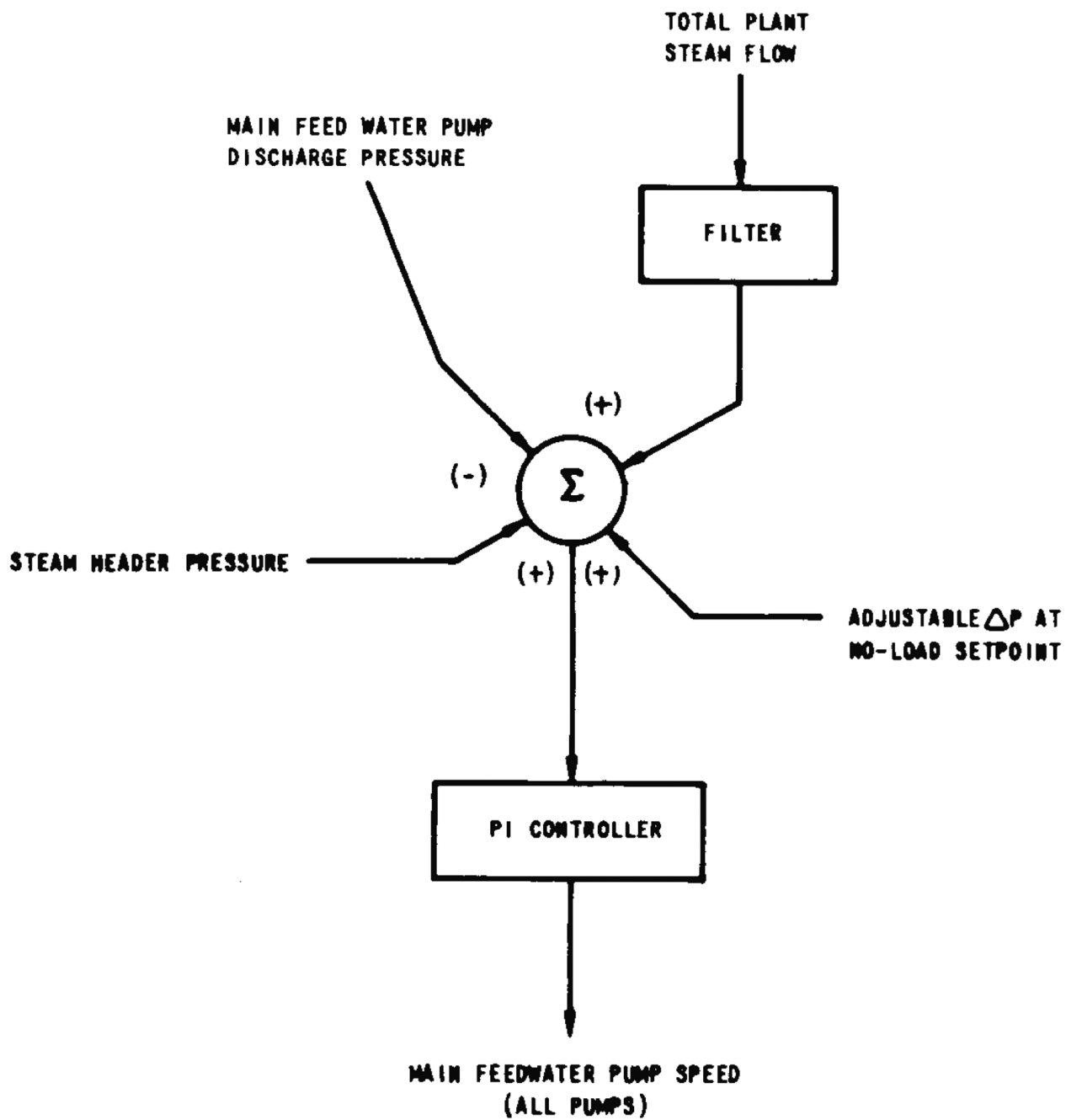
REV 21 5/08



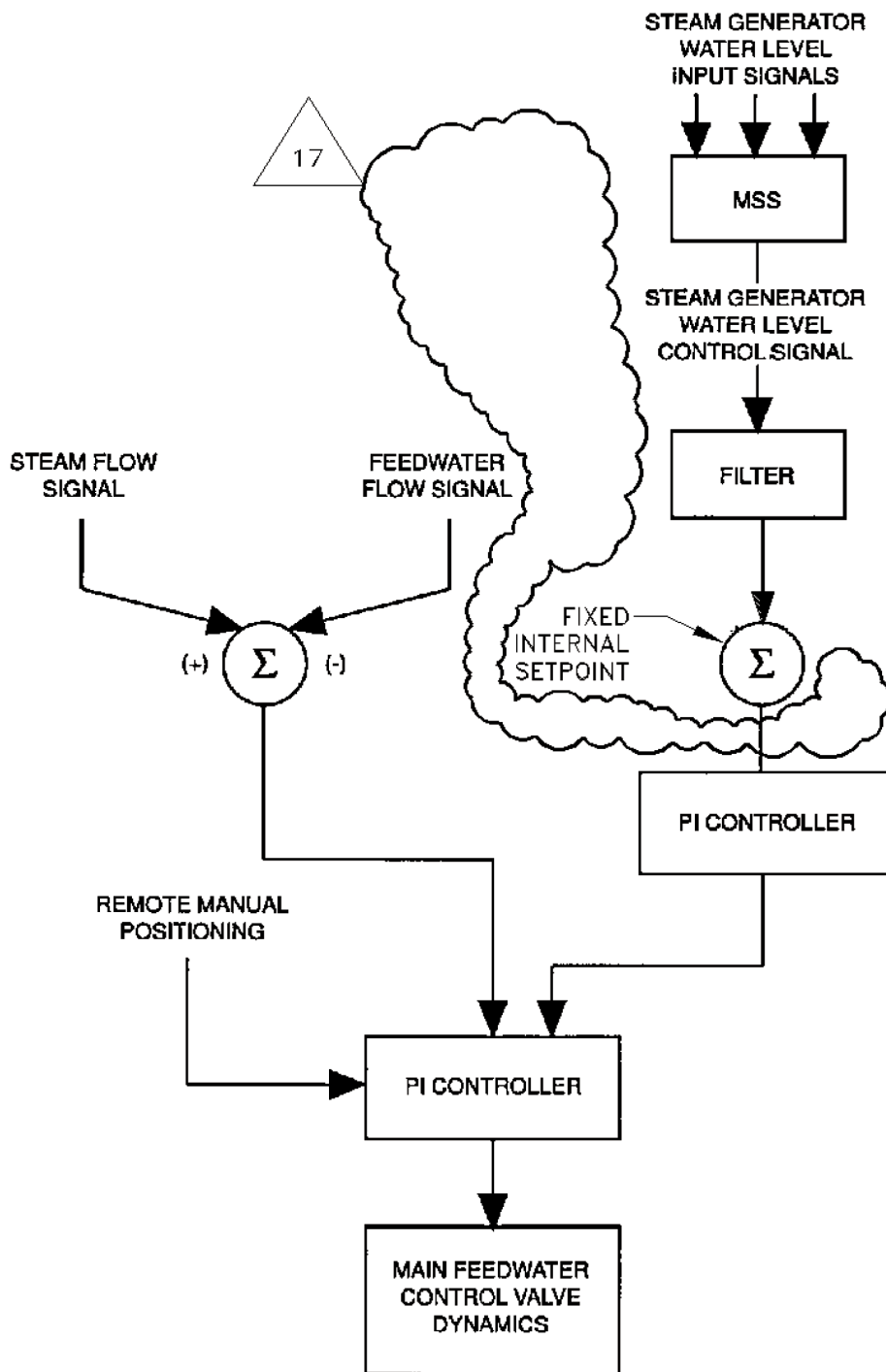
REV 21 5/08



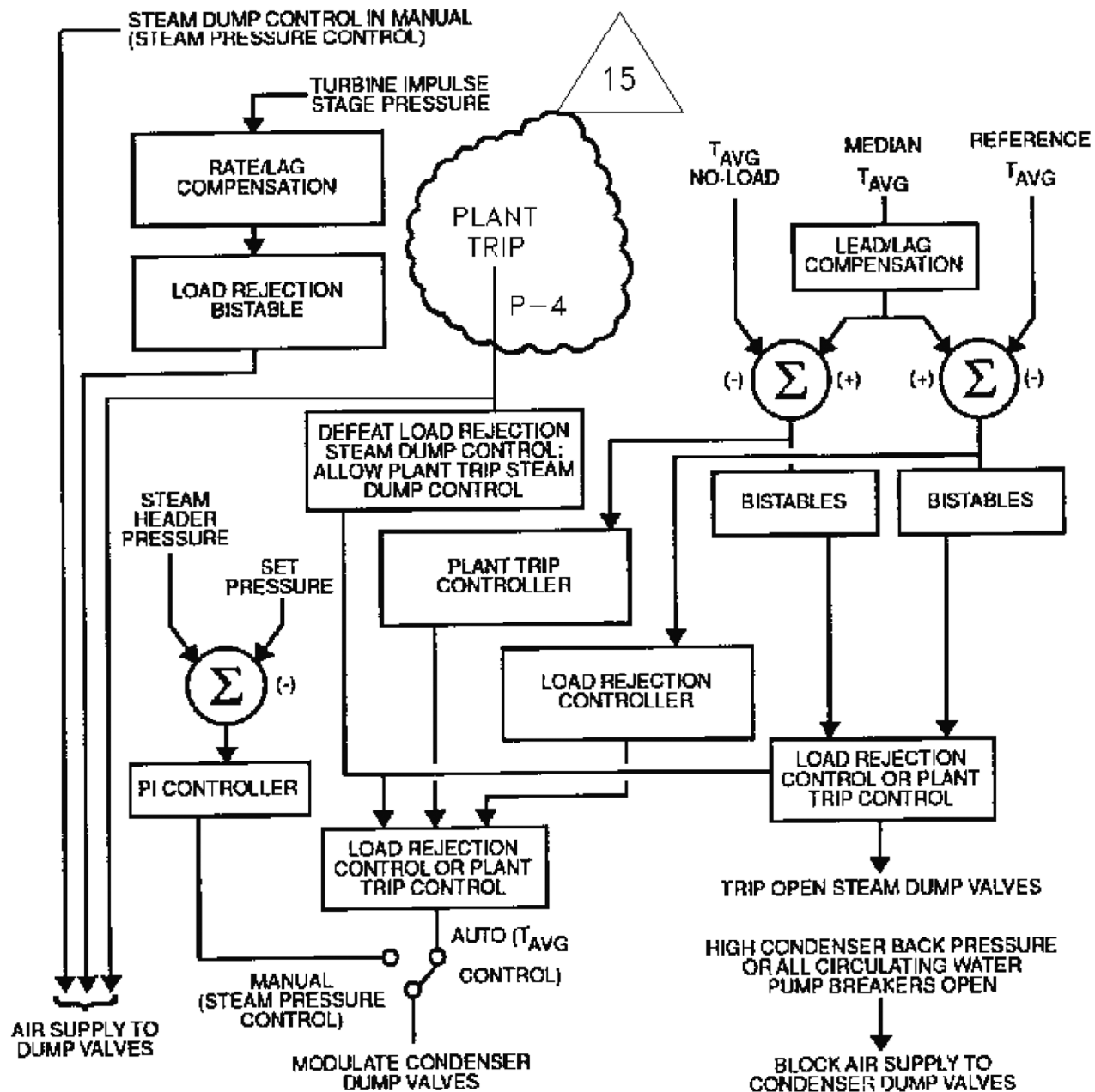
REV 21 5/08



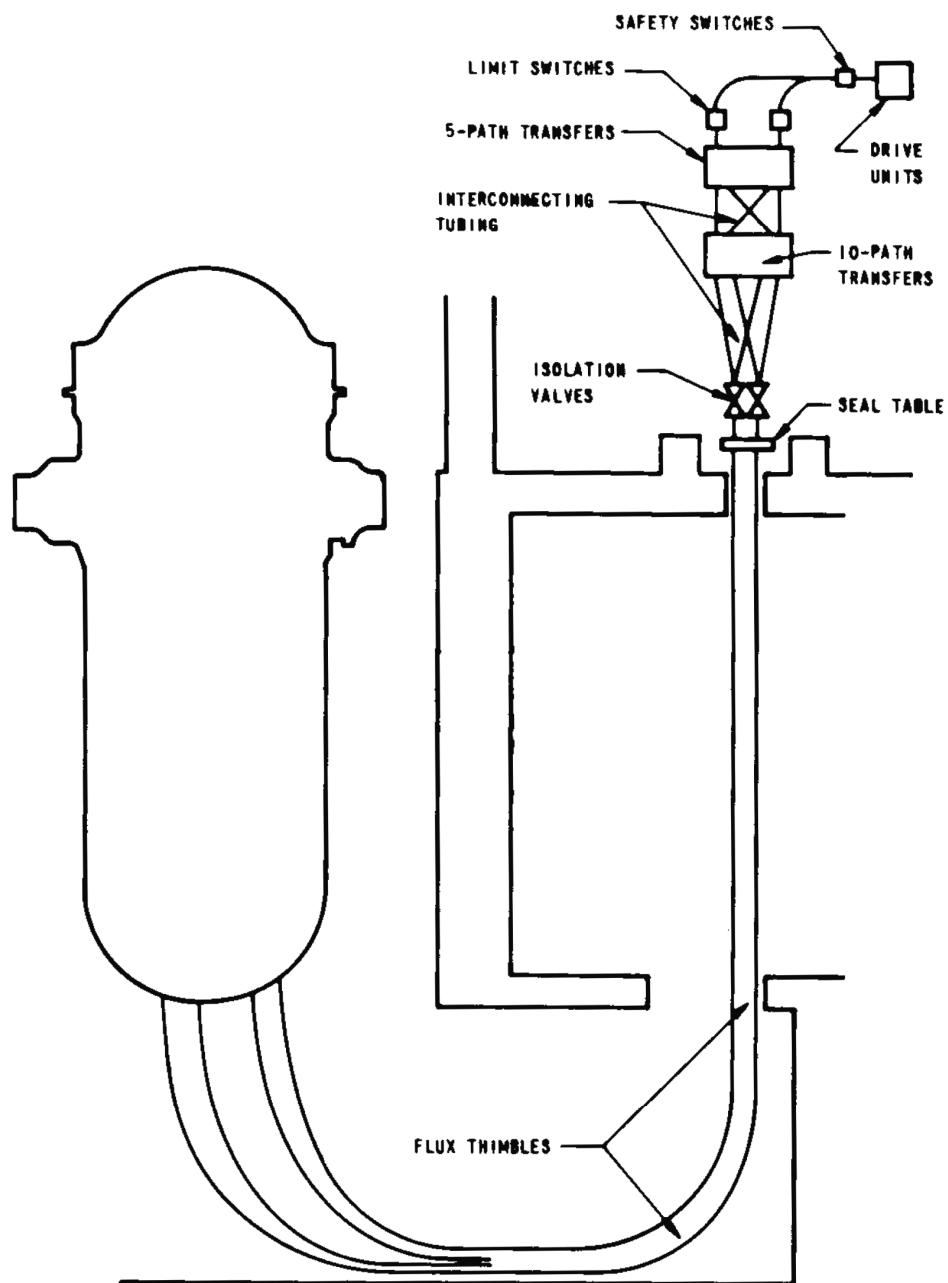
REV 21 5/08



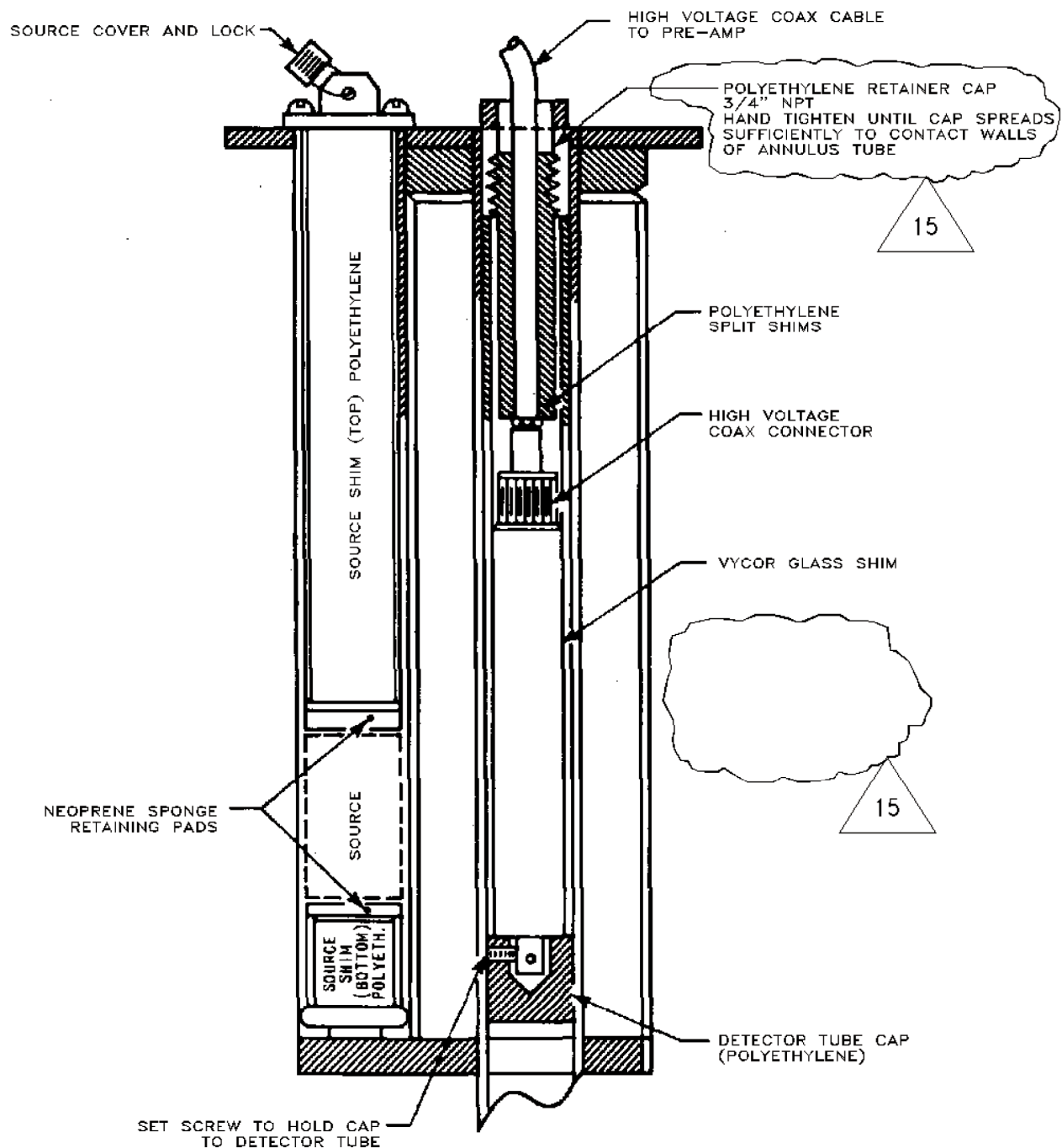
REV 21 5/08



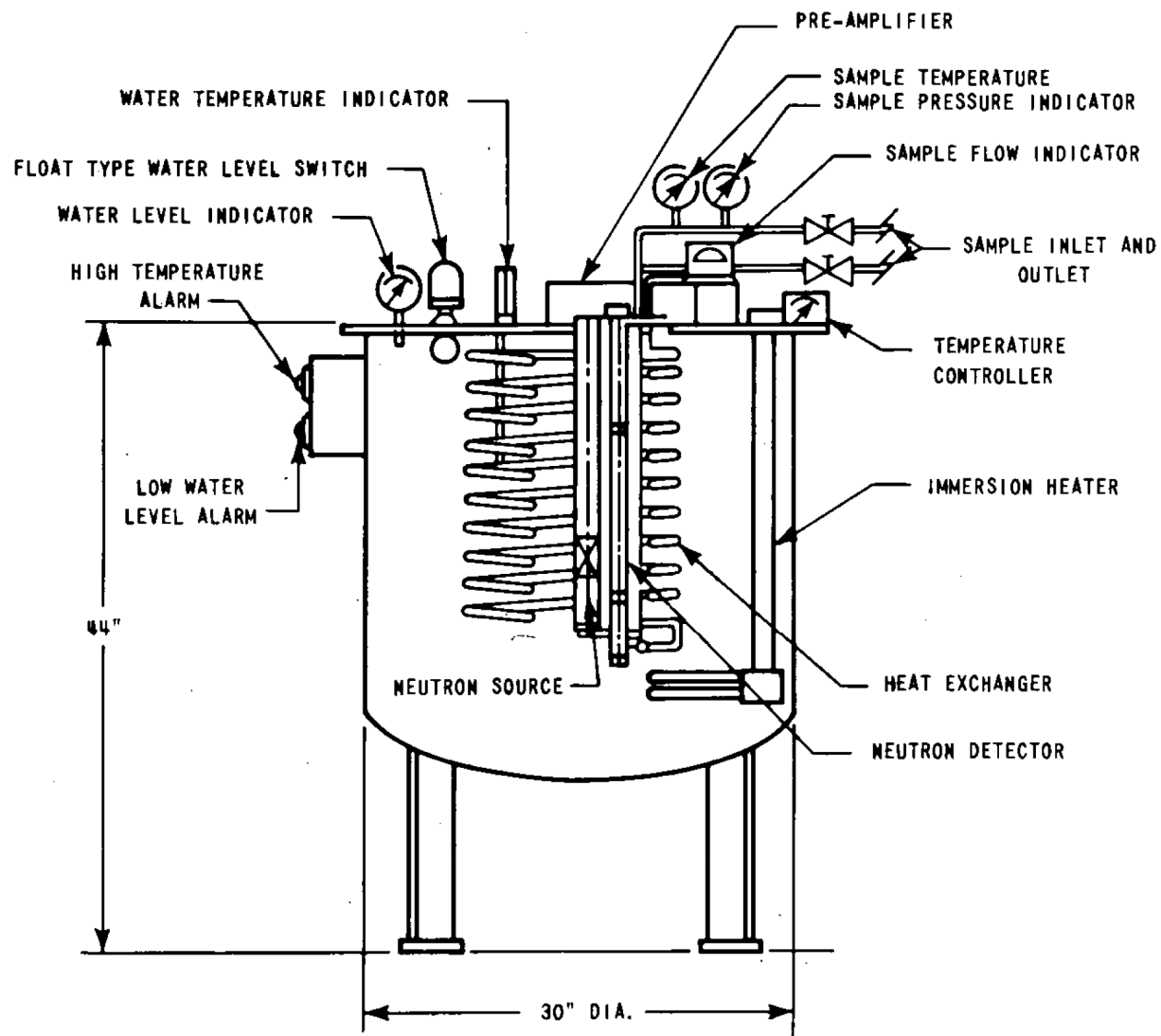
REV 21 5/08



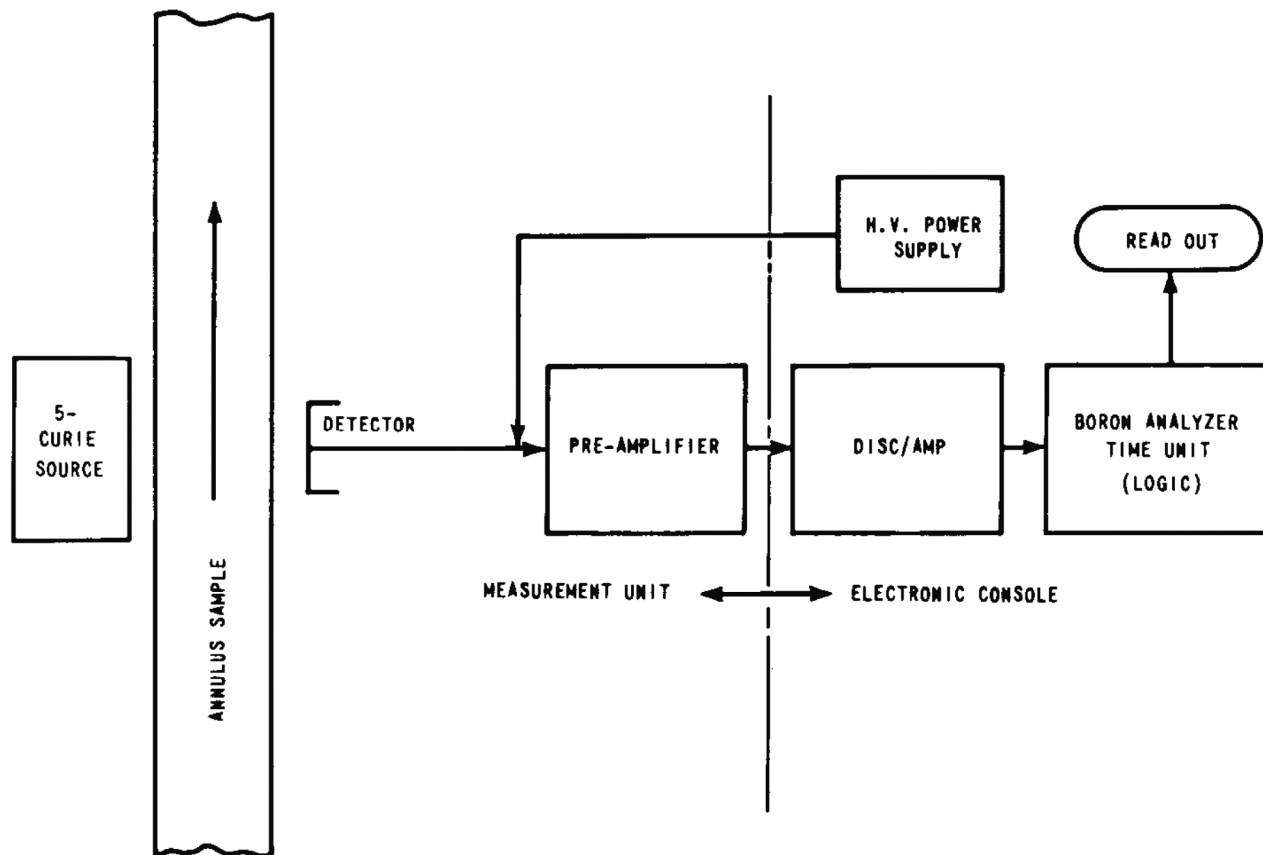
REV 21 5/08



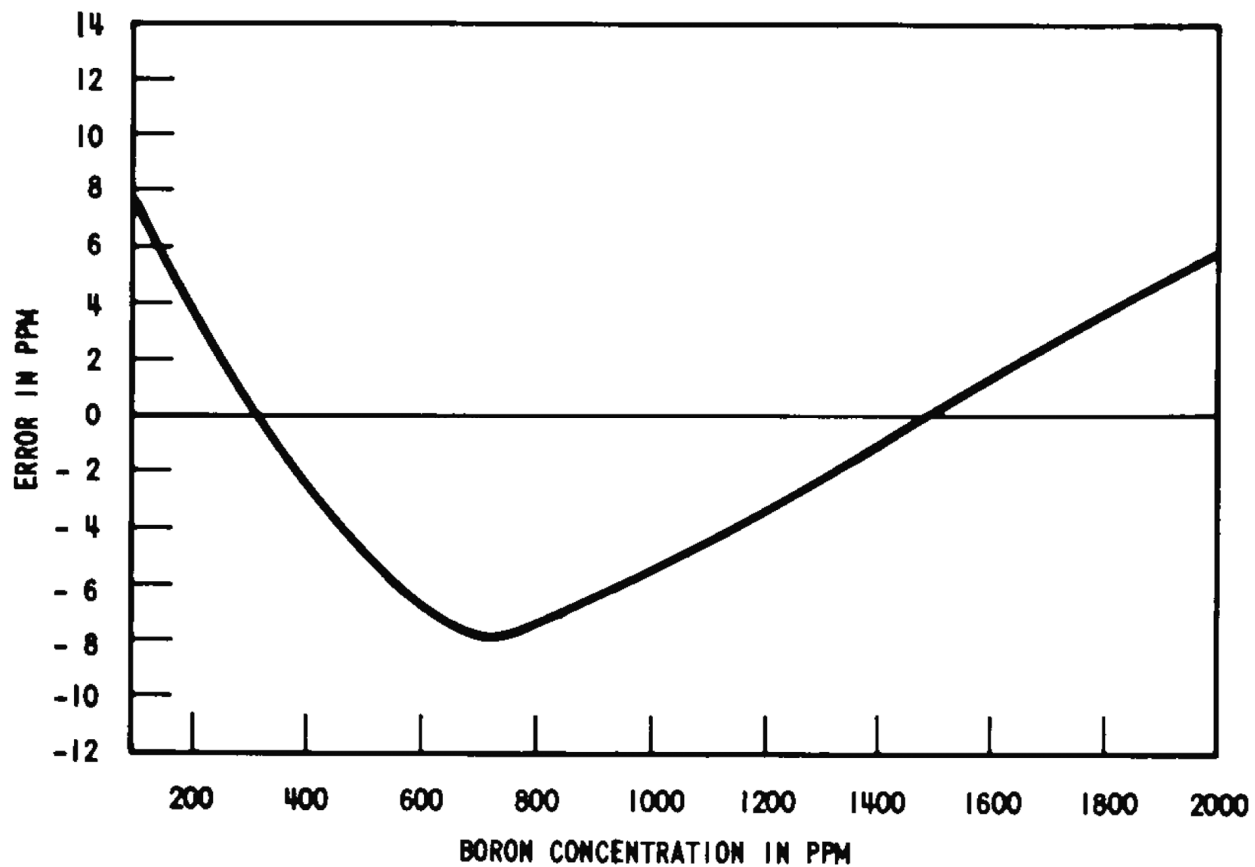
REV 21 5/08



REV 21 5/08



REV 21 5/08



REV 21 5/08

7.8 ATWS MITIGATION SYSTEM ACTUATION CIRCUITRY (AMSAC)

7.8.1 DESCRIPTION

7.8.1.1 System Description

The ATWS (anticipated transient without scram) mitigation system actuation circuitry (AMSAC) provides a backup to the reactor trip system (RTS) and ESF actuation system (ESFAS) for initiating turbine trip and auxiliary feedwater flow in the event of an anticipated transient (e.g., in the complete loss of main feedwater). The AMSAC is independent of and diverse from the RTS and ESFAS, with the exception of the final actuation devices. The AMSAC equipment, with the exception of the output isolation relays, is classified as control-grade equipment. It is a highly-reliable, microprocessor-based, single-train system powered by a non-Class 1E source.

The AMSAC continuously monitors level in the steam generators, which is an anticipatory indication of a loss of heat sink, and initiates certain functions when the level drops below a predetermined setpoint for at least a preselected time and for two of the three steam generator levels. These initiated functions are the tripping of the turbine, the initiation of auxiliary feedwater, and isolation of the steam generator blowdown and sample lines.

The AMSAC is designed to be highly reliable, resistant to inadvertent actuation, and easily maintained. Reliability is assured through the use of internal redundancy and continual self testing by the system. Inadvertent actuations are minimized through the use of internal redundancy and majority voting at the output stage of the system. The time delay on low steam generator level and the coincidence logic used also minimize inadvertent actuations.

The AMSAC automatically performs its actuations when above a preselected power level (determined using turbine impulse chamber pressure) and remains armed sufficiently long after that pressure drops below the setpoint to ensure that its function will be performed in the event of a turbine trip.

7.8.1.2 Equipment Description

The AMSAC consists of a single train of equipment located primarily in a seismically qualified cabinet. The output isolation relays, however, are located in two separate qualified wall-mounted cabinets.

The design of the AMSAC is based on the industry standard Intel multibus format, which permits the use of various readily available, widely used microprocessor cards on a common data bus for various functions.

The AMSAC consists of the following:

FNP-FSAR-7

A. Steam Generator (SG) Level Sensing

AMSAC utilizes the SG level signals as measured with three differential pressure-type level transmitters, measuring the level for each of the main steam generators as shown on drawing U-166237.

B. Turbine Impulse Pressure

AMSAC also utilizes the turbine impulse pressure signal for measuring pressure in the turbine, as shown on drawing U-166245.

C. System Hardware

The system hardware consists of two primary systems: the actuation logic system (ALS) and the test/ maintenance system (T/MS).

1. Actuation Logic System

The ALS monitors the analog and digital inputs, performs the functional logic required, provides actuation outputs to trip the turbine and initiate auxiliary feedwater flow, and provides status information to the T/MS. The ALS consists of three groups of input/output (I/O) modules, three actuation logic processors (ALPs), two majority voting modules, and two output relay panels. The I/O modules provide signal conditioning, isolation, and test features for interfacing the ALS and the T/MS. Conditioned signals are sent to three identical ALPs for analog-to-digital conversion, setpoint comparison, and coincidence logic performance. Each of the ALPs perform identical logic calculations using the same inputs, and derive component actuation demands, which are then sent to the majority voting modules. The majority voting modules perform a two-out-of-three vote on the ALP demand signals. These modules drive the relays providing outputs to the existing turbine trip and auxiliary feedwater initiation circuits.

A simplified block diagram of the AMSAC ALS architecture is presented on figure 7.8-1.

2. Test/Maintenance System

The test/maintenance system provides the AMSAC with automated and manual testing as well as a maintenance mode. Automated testing is the continuously performed self checking done by the system during normal operation. ALS status is monitored by the T/MS and sent to the plant computer and the main control board. Manual testing of the system by the computer services staff can be performed on-line to provide assurance that the ALS system is fully operational. The maintenance mode permits the computer services staff, under administrative control, to modify channel setpoints, channel status, and timer values and to initiate channel calibration.

The T/MS consists of a test/maintenance processor, a digital-to-analog conversion board, a memory board, expansion boards, a self-health board, digital output modules, a test/maintenance panel, and a portable terminal/printer.

D. Equipment Actuation

The output relay panels provide component actuation signals through isolation relays, which then drive the final actuation circuitry as shown on drawings U-166244 and U-166245 for initiation of auxiliary feedwater and for turbine trip.

7.8.1.3 **Functional Performance Requirements**

Analyses have shown that the most limiting ATWS event is a loss of feedwater event without a reactor trip. AMSAC performs the mitigative actuations of automatically initiating auxiliary feedwater, tripping the turbine, and isolating steam generator blowdown and sampling lines. These are initiated in order to ensure a secondary heat sink following an anticipated transient (ANS Condition II) without a reactor trip, in order to limit core damage following an anticipated transient without a reactor trip and to ensure that the energy generated in the core is compatible with the design limits to protect the reactor coolant pressure boundary by maintaining the reactor coolant pressure to within ASME stress level C.

7.8.1.4 **AMSAC Interlocks**

A single interlock, designated as C-20, is provided to allow for the automatic arming and blocking of the AMSAC (drawing U-166245). The system is blocked at sufficiently low reactor power levels when the actions taken by the AMSAC following an ATWS need not be automatically initiated. Turbine impulse chamber pressure in a two-out-of-two logic scheme is used for the blocking function. Turbine impulse chamber pressure above the setpoint will automatically defeat any block, i.e., will arm the AMSAC. Dropping below this setpoint will automatically block the AMSAC. Removal of the C-20 permissive is automatically delayed for a predetermined time. The operating status of the AMSAC is displayed on the main control board.

7.8.1.5 **Trip System**

The SG level and turbine impulse chamber pressure inputs are used by AMSAC to determine trip demand. Signal conditioning is performed on the transmitter output and used by each of the ALPs to derive a component actuation demand. If two of the three steam generators have a low level at a power level greater than the C-20 permissive, a trip demand signal is generated following a time delay. This signal drives output relays for performing the necessary mitigative actions.

7.8.1.6 Isolation Devices

AMSAC is independent of the RTS and ESFAS. The AMSAC inputs for measuring narrow range steam generator water level are derived from existing transmitters and channels within the process protection system. Connections to these channels are made downstream of Class-1E isolation devices located within the process protection cabinets. These isolation devices ensure that the existing protection system continues to meet all applicable safety criteria by providing isolation. Buffering of the AMSAC outputs from the safety-related final actuation device circuits is achieved through qualified relays. A credible fault occurring in the nonsafety-related AMSAC will not propagate through and degrade the RTS and ESFAS.

7.8.1.7 AMSAC Diversity from the Reactor Protection Systems

Equipment diverse from the RTS and ESFAS is used in the AMSAC to prevent common mode failures that might affect the AMSAC and the RTS or ESFAS. The AMSAC is a digital, microprocessor-based system with the exception of the analog SG level and turbine impulse pressure transmitter inputs, whereas the reactor trip system utilizes an analog based protection system. Also, where similar components are utilized for the same function in both AMSAC and the reactor trip system, the components used in AMSAC are provided by a different manufacturer.

Common mode failure of identical components in the analog portion of the RTS that results in the inability to generate a reactor trip signal will not impact the ability of the digital AMSAC to generate the necessary mitigative actuations. Similarly, a postulated common mode failure affecting analog components in ESFAS, affecting its ability to initiate auxiliary feedwater, will not impact the ability of the digital based AMSAC to automatically initiate auxiliary feedwater.

7.8.1.8 Power Supply

The AMSAC power supply is a dedicated uninterruptible power supply (UPS) which is independent from the RTS power supplies and is backed by batteries which are independent from the existing batteries which supply the RTS.

7.8.1.9 Environmental Variations

The AMSAC equipment is located in a controlled environment such that variations in the ambient conditions are minimized.

7.8.1.10 Setpoints

The AMSAC makes use of two setpoints in the coincidence logic in order to determine if mitigative functions are required. Water level in each steam generator is sensed to determine if a loss of secondary heat sink is imminent. The low-level setpoint is selected in such a manner that a true lowering of the level will be detected by the system. The normal small variations in steam generator level will not result in a spurious AMSAC signal.

The C-20 permissive setpoint is selected in order to be consistent with ATWS investigations showing that the mitigative actions performed by the AMSAC need not be automatically actuated below a certain power level. The maximum allowable value of the C-20 permissive setpoint is defined by these investigations.

To avoid inadvertent AMSAC actuation on the loss of one main feedwater pump, AMSAC actuation is delayed by a defined amount of time. This will ensure the reactor protection system will provide the first trip signal.

To ensure that the AMSAC remains armed sufficiently long to permit its function in the event of a turbine trip, the C-20 permissive is maintained for a preset time delay after the turbine impulse chamber pressure drops below the setpoint. The setpoints and the capability for their modification in the AMSAC are under administrative control.

7.8.2 ANALYSIS

7.8.2.1 Safety Classification/Safety-Related Interface

The AMSAC is not safety related, therefore, it need not meet the requirements of IEEE-279-1971. The AMSAC has been implemented such that the RTS and ESFAS continue to meet all applicable safety-related criteria. The AMSAC is independent of the RTS and ESFAS. The isolation provided between the RTS and the AMSAC and between the ESFAS and the AMSAC by the isolator modules and the isolation relays, respectively, ensures that applicable safety- related criteria are met for the RTS and the ESFAS.

7.8.2.2 Redundancy

System redundancy has not been provided. Since AMSAC is a backup nonsafety-related system to the redundant RTS, redundancy is not required. To ensure high system reliability, portions of the AMSAC have been implemented as internally redundant, such that a single failure of an input channel or ALP will neither actuate nor prevent actuation of the AMSAC.

7.8.2.3 Diversity from the Existing Trip System

Diverse equipment has been selected in order that common cause failures affecting both the RTS and the AMSAC or both the ESFAS and the AMSAC will not render these systems inoperable simultaneously. A more detailed discussion of the diversity between the RTS and the AMSAC and between the ESFAS and the AMSAC is presented in paragraph 7.8.1.7.

7.8.2.4 Electrical Independence

The AMSAC is electrically independent of the RTS and ESFAS with the exception of the final actuation devices. Qualified isolation devices are provided to isolate the nonsafety AMSAC

circuitry from the safety-related actuation circuits of the auxiliary feedwater system as discussed in paragraph 7.8.1.6.

7.8.2.5 Physical Separation from the RTS and ESFAS

AMSAC is, by necessity, physically separated from the existing protection system hardware. The two trains of AMSAC outputs are provided from separate wall-mounted enclosures outside of the cabinet.

7.8.2.6 Environmental Qualification

Equipment related to the AMSAC is designed to operate under conditions resulting from anticipated operational occurrences for the respective equipment location. The AMSAC equipment, with the exception of the isolation devices, is not designated as safety-related equipment and, therefore, is not required to be qualified as safety related per the requirements of IEEE Standard 279-1971, "IEEE Standard for Criteria for Protection Systems for Nuclear Power Generating Stations." The safety-related AMSAC output isolation devices are located in a mild environment.

7.8.2.7 Seismic Qualification

It is required that only the isolation devices comply with seismic qualification. The AMSAC output isolation device is qualified in accordance with a program that was developed to implement the requirements of IEEE Standard 344-1975, "IEEE Standard for Seismic Qualification of Class 1E Electrical Equipment for Nuclear Power Generating Stations."

7.8.2.8 Test, Maintenance, and Surveillance Quality Assurance

NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety Related," requires quality assurance procedures commensurate with the nonsafety-related classification of the AMSAC. The quality controls for the AMSAC are, at a minimum, consistent with existing plant procedures or practices for nonsafety-related equipment.

Design of the AMSAC followed procedures relating to equipment procurement, document control, and specification of system components, materials and services. In addition, specifications also define quality assurance practices for inspections, examinations, storage, shipping, and tests as appropriate to a specific item or service.

A computer software verification program and a firmware validation program have been implemented commensurate with the nonsafety-related classification of the AMSAC to ensure that the system design requirements implemented with the use of software have been properly implemented and to ensure compliance with the system functional, performance, and interface requirements.

System testing is completed prior to the installation and operation of the AMSAC as part of normal factory acceptance testing and the validation program. Periodic testing is performed automatically through use of the system automatic self-checking capability and manually under administrative control via the AMSAC test/maintenance panel.

7.8.2.9 Power Supply

Power to the AMSAC is from a battery-backed, dedicated uninterruptible power supply independent of the power supplies for the RTS and ESFAS. The station battery supplying power to the AMSAC is independent of those used for the RTS and ESFAS. The AMSAC is an energize-to-actuate system capable of performing its mitigative functions with a loss-of-offsite power.

7.8.2.10 Testability at Power

The AMSAC is testable at power. This testing is done via the system test/maintenance panel. The capability of the AMSAC to perform its mitigative actuations is bypassed at a system level while in the test mode. Total system testing is performed as a set of three sequential, partial, overlapping tests. The first of the tests checks the analog input portions of the AMSAC in order to verify accuracy. Each of the analog input modules is checked separately. The second test checks each of the ALPs separately to verify that the appropriate coincidence logic is sent to the majority voter. The last test exercises the majority voter and the integrity of the associated output relays. The majority voter and associated output relays are tested by exercising all possible input combinations to the majority voter. The integrity of each of the output relays is checked by confirming continuity of the relay coils without operating the relays. The capability to individually operate the output relays, confirm integrity of the associated field wiring, and operate the corresponding isolation relays and final actuation devices at plant shutdown is provided.

7.8.2.11 Inadvertent Actuation

The AMSAC has been designed such that the frequency of inadvertent actuations is minimized. This high reliability is ensured through use of three redundant ALPs and a majority voting module. A single failure in any of these modules will not result in a spurious AMSAC actuation. In addition, a two-out-of-three low-steam generator level coincidence logic and a time delay have been selected to further minimize the potential for inadvertent actuations.

7.8.2.12 Bypass

7.8.2.12.1 Maintenance Bypasses

The AMSAC is blocked at the system level during maintenance, repair, calibration, or test. While the system is blocked, the bypass condition is indicated in the main control room.

7.8.2.12.2 Operating Bypasses

The AMSAC has been designed to allow for operational bypasses with the inclusion of the C-20 permissive. Above the C-20 setpoint, the AMSAC is automatically unblocked (i.e., armed); below the setpoint, the system is automatically blocked. The operating status of the AMSAC is indicated in the main control room via a bypass and permissive panel window.

7.8.2.12.3 Indication of Bypasses

Whenever the mitigative capabilities of the AMSAC are bypassed or deliberately rendered inoperable, this condition is indicated in the main control room. In addition to the operating bypass, any manual maintenance bypass is indicated via the AMSAC general warning sent to the main control room.

7.8.2.12.4 Means for Bypassing

A permanently installed system bypass selector switch is provided to bypass the system. This is a two-position selector switch with "NORMAL" and "BYPASS" positions. At no time is it necessary to use any temporary means, such as installing jumpers or pulling fuses, to bypass the system.

7.8.2.13 Completion of Mitigative Actions Once Initiated

The AMSAC mitigative actions go to completion as long as the coincidence logic is satisfied and the time delay requirements are met. If the flow in the feedwater lines is reinitiated before the timer expires and the SG water level increases to above the AMSAC low setpoint, the coincidence logic will no longer be satisfied and the actuation signal disappears. If the coincidence logic conditions are maintained for the duration of the time delay, the mitigative actions go to completion. The auxiliary feedwater initiation and the turbine trip signals are latched in at the activated component level through the existing circuits. Deliberate operator action is then necessary to terminate auxiliary feedwater flow, clear the turbine trip signal using the main control board turbine trip reset switch, and proceed with the reopening of the turbine stop valves.

7.8.2.14 Manual Initiation

Manual initiation of the AMSAC is not provided. The capability to initiate the AMSAC mitigative functions manually, i.e., initiate auxiliary feedwater, trip the turbine, and isolate steam generator blowdown and sampling lines, exists at the main control board independent of AMSAC.

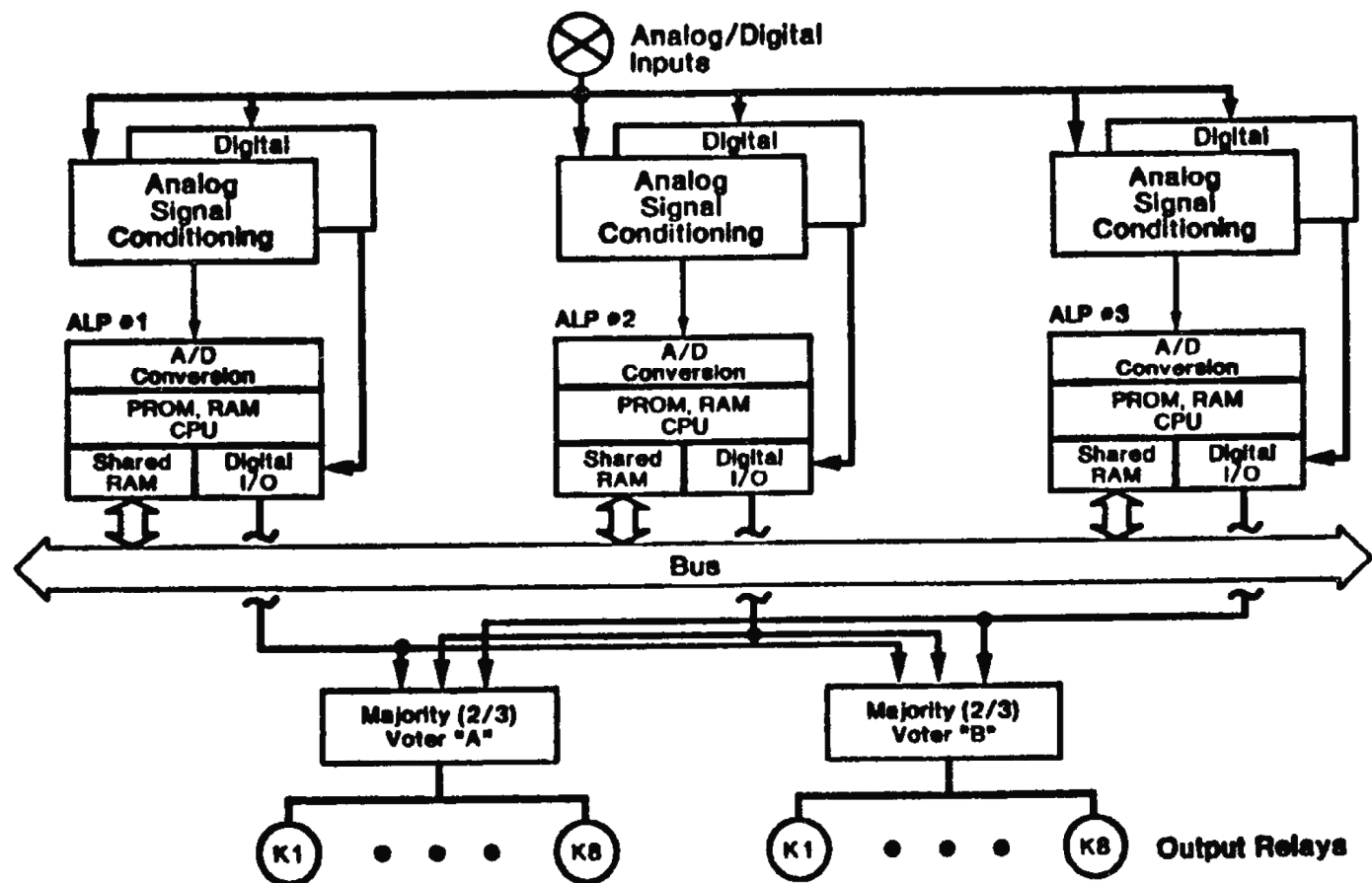
7.8.2.15 Information Readout

The AMSAC has been designed such that the operating and maintenance staffs have accurate, complete, and timely information pertinent to the status of the AMSAC. A system level general

warning alarm is indicated in the control room. Diagnostic capability exists from the test/maintenance panel to determine the cause of any unanticipated inoperability or deviation.

7.8.2.16 Compliance with Standards and Design Criteria

The AMSAC meets the NRC acceptance criteria contained in 10 CFR 50.62 and the quality assurance requirements contained in NRC Generic Letter 85-06. The AMSAC also complies with the generic designs presented in WCAP-10858-P-A, which have been determined to be acceptable by the NRC for meeting the requirements of 10 CFR 50.62. In addition, the time delay design for the AMSAC associated with the C-20 permissive signal is consistent with Revision 1 to WCAP-10858-P-A, which has been accepted by the NRC.



REV 21 5/08