Chapter 7: Instrumentation and Control

Table of Contents

Section	Title	Page
7.1	INTRODUCTION	7.1-1
7.1.1	General Design Criteria	7.1-1
7.1.2	Regulatory Guide 1.97 Program	7.1-2
7.1	References	7.1-3
7.2	REACTOR PROTECTION SYSTEM	7.2-1
7.2.1	Design Bases	7.2-2
7.2.1.1	Control Room	7.2-2
7.2.1.2	Core Protection Sequence	7.2-3
7.2.1.3	Reliability, Redundancy, and Independence	7.2-3
7.2.1.4	Reactivity Control	7.2-5
7.2.1.5	Manual Actuation	7.2-5
7.2.1.6	Channel Bypass	7.2-5
7.2.1.7	Calibration and Testing	7.2-5
7.2.1.8	Functional Requirements	7.2-6
7.2.2	System Description	7.2-8
7.2.2.1	System Safety Features	7.2-8
7.2.2.2	Protective Actions	7.2-15
7.2.2.3	Rod Stops	7.2-20
7.2.2.4	Rod Drop Detection	7.2-20
7.2.2.5	Automatic Turbine Load Runback	7.2-21
7.2.2.6	Control Group Rod Insertion Monitor	7.2-21
7.2.2.7	Reactor Coolant Flow Measurement	7.2-21
7.2.2.8	Reactor Coolant Pump Trip	7.2-22
7.2.3	System Evaluation	7.2-22
7.2.3.1	Departure From Nucleate Boiling	7.2-22
7.2.3.2	Control/Protection Interaction	7.2-23
7.2.3.3	Normal Operating Environment	7.2-29
7.2	References	7.2-30
7.2	Reference Drawings	7.2-30
7.3	REACTOR CONTROL SYSTEM	7.3-1
7.3.1	Design Bases	7.3-1
7.3.2	System Description	7.3-2
7.3.2.1	Control Rod Assembly Arrangements	7.3-3

Chapter 7: Instrumentation and Control

Table of Contents (continued)

Section	Title	Page
7.3.2.2	Rod Control	7.3-3
7.3.2.3	Rod Drive Performance	7.3-5
7.3.2.4	Primary System Pressure Control	7.3-7
7.3.2.5	Pressurizer Level Control	7.3-7
7.3.2.6	Secondary System Control	7.3-8
7.3.3	Design Evaluation	7.3-9
7.3.3.1	Unit Stability	7.3-9
7.3.3.2	Step Load Changes Without Steam Dump	7.3-10
7.3.3.3	Loading and Unloading	7.3-10
7.3.3.4	Loss of Load With Steam Dump	7.3-10
7.3.3.5	Turbine-Generator Trip With Reactor Trip	7.3-11
7.3	Reference Drawings	7.3-12
7.4	NUCLEAR INSTRUMENTATION SYSTEM	7.4-1
7.4.1	Design Bases	7.4-1
7.4.1.1	Fission Process Monitors and Controls	7.4-1
7.4.2	System Description	7.4-2
7.4.2.1	Protection Philosophy	7.4-2
7.4.2.2	Source Range Instrumentation	7.4-3
7.4.2.3	Intermediate Range Instrumentation	7.4-3
7.4.2.4	Power Range Instrumentation	7.4-4
7.4.2.5	Equipment Design	7.4-4
7.4.3	Components	7.4-5
7.4.3.1	Detectors	7.4-5
7.4.3.2	Source Range Components	7.4-5
7.4.3.3	Source Range Auxiliary Equipment	7.4-8
7.4.3.4	Intermediate Range Components	7.4-9
7.4.3.5	Intermediate Range Auxiliary Equipment	7.4-10
7.4.3.6	Power Range Components	7.4-10
7.4.3.7	Power Range Auxiliary Equipment	7.4-13
7.4.3.8	Miscellaneous Control and Indication Panel	7.4-14
7.4.3.9	Output Information	7.4-14
7.4.4	System Evaluation	7.4-15
7.4.4.1	Philosophy and Setpoints	7.4-15
7.4.4.2	Reactor Trip Protection	7.4-15

Chapter 7: Instrumentation and Control

Table of Contents (continued)

Section	Title	Page
7.4.4.3	Rod-Drop	7.4-16
7.4.4.4	Control and Alarm Functions	7.4-16
7.4.4.5	Power Supply	7.4-17
7.4.4.6	Safety Factors	7.4-18
7.5	ENGINEERED SAFEGUARDS	7.5-1
7.5.1	Design Bases	7.5-1
7.5.1.1	Safety Injection	7.5-2
7.5.1.2	Consequence Limiting Safeguards	7.5-2
7.5.1.3	Spray Subsystems	7.5-3
7.5.1.4	Containment Vacuum System	7.5-4
7.5.1.5	Containment Isolation	7.5-7
7.5.2	System Description	7.5-8
7.5.2.1	Engineered Safeguards Actuation Instrumentation	7.5-8
7.5.2.2	Instrumentation Used During a Loss-of-Coolant Accident	7.5-9
7.5.2.3	Calibration and Testing	7.5-10
7.5.3	System Evaluation	7.5-12
7.5.3.1	Safety Injection	7.5-12
7.5.3.2	Consequence Limiting Safeguards	7.5-12
7.5.3.3	Containment Isolation System	7.5-13
7.5.3.4	Motor and Valve Control	7.5-13
7.5.3.5	Environmental Capability	7.5-14
7.5	References	7.5-16
7.6	INCORE INSTRUMENTATION	7.6-1
7.6.1	Design Basis	7.6-1
7.6.2	System Description	7.6-1
7.6.2.1	General	7.6-1
7.6.2.2	Thermocouples	7.6-1
7.6.2.3	Movable Neutron Detectors	7.6-2
7.6.3	System Evaluation	7.6-3
7.7	OPERATING CONTROL STATIONS	7.7-1
7.7.1	Design Bases	7.7-1
7.7.2	System Description	7.7-2
7.7.3	System Evaluation	7.7-8

Chapter 7: Instrumentation and Control

Table of Contents (continued)

Section	Title	Page
7.7	Reference Drawings	7.7-8
7.8	[DELETED]	7.8-1
7.9	COMPUTER SYSTEM	7.9-1
7.9.1	Design Bases	7.9-1
7.9.2	System Description	7.9-1
7.9.2.1	Analog Scanning	7.9-1
7.9.2.2	Alarming	7.9-1
7.9.2.3	Alarm Review	7.9-2
7.9.2.4	Analog Trend	7.9-2
7.9.2.5	Digital Trend	7.9-2
7.9.2.6	Digital Display	7.9-2
7.9.2.7	Sequence of Events	7.9-2
7.9.2.8	Normal and Summary Logging	7.9-2
7.9.3	System Evaluation	7.9-3
7.10	INADEQUATE CORE COOLING (ICC) SYSTEM	7.10-1
7.10.1	Design Bases	7.10-1
7.10.2	System Description	7.10-1
7.10.2.1	Core Exit Thermocouple (CET) System - Subsystem of ICC System	7.10-1
7.10.2.2	Reactor Vessel Level Instrumentation Systems (RVLIS) - Subsystem of ICC System.	7.10-1
7.10.2.3	Core Cooling Monitor System - Subsystem of ICC System	7.10-3
7.10	References	7.10-3
7.11	EX-CORE NEUTRON FLUX MONITOR SYSTEM	7.11-1
7.11.1	Design Bases	7.11-1
7.11.2	System Description and Evaluation	7.11-1
7.12	LEVEL INSTRUMENTATION TO PREVENT LOSS OF SHUTDOWN COOLING	7.12-1
7.12.1	System Description	7.12-1
7.12.1.1	Level Standpipe	7.12-1
7.12.1.2	Ultrasonic Level Indication System.	7.12-1

Chapter 7: Instrumentation and Control

List of Tables

Table	Title	Page
Table 7.2-1	Reactor Trips	7.2-31
Table 7.2-2	Logic Symbols	7.2-33
Table 7.2-3	Protection Interlocks	7.2-36
Table 7.2-4	Rod Stops	7.2-38
Table 7.4-1	Source Range Signals	7.4-19
Table 7.4-2	Intermediate Range Signals	7.4-20
Table 7.4-3	Power Range Signals	7.4-21
Table 7.5-1	Engineered Safeguards Actuation Functions	7.5-17
Table 7.5-2	Valves/Dampers Actuated by Engineered Safeguards Signals	7.5-19
Table 7.5-3	Safety-Related Systems	7.5-28

Chapter 7: Instrumentation and Control

List of Figures

Figure	Title	Page
Figure 7.2-1	Typical Illustration of DT -T_{avg} Protection.	7.2-39
Figure 7.2-2	Reactor Trip Signals	7.2-40
Figure 7.2-3	Logic Diagram for Low Reactor Coolant Flow Trips	7.2-41
Figure 7.2-4	Design to Achieve Isolation Between Channels	7.2-42
Figure 7.2-5	Basic Elements of an Analog Protection Channel	7.2-43
Figure 7.2-6	Trip Logic Channels	7.2-44
Figure 7.2-7	Analog Channels	7.2-45
Figure 7.2-8	Logic Channel Test Panels	7.2-46
Figure 7.2-9	Control Group Rod Insertion Monitor	7.2-47
Figure 7.2-10	T_{avg} - DT Protection	7.2-48
Figure 7.2-11	Pressurizer Pressure Control and Protection.	7.2-49
Figure 7.2-12	Pressurizer Level Control and Protection System	7.2-50
Figure 7.2-13	Steam Generator Level Control and Protection System	7.2-51
Figure 7.3-1	Simplified Block Diagram of Reactor Control System	7.3-13
Figure 7.3-2	T_{avg} Control System	7.3-14
Figure 7.3-3	Power Supply to Control Rod Equipment and Control Rod Drive Mechanisms	7.3-15
Figure 7.4-1	Ranges of NIS Instrumentation.	7.4-23
Figure 7.4-2	Nuclear Instrumentation System.	7.4-24
Figure 7.4-3	Neutron Detector Locations	7.4-25
Figure 7.5-1	Safety Injection System Actuation	7.5-29
Figure 7.5-2	Consequence-Limiting Safeguards Initiation System (Unit 1).	7.5-30
Figure 7.5-3	Consequence-Limiting Safeguards Initiation System (Unit 2).	7.5-31
Figure 7.5-4	Engineered Safeguards Actuation Circuits	7.5-32
Figure 7.5-5	Simplified Diagram for Overall Logic Relay Test Scheme	7.5-33
Figure 7.5-6	Simplified Diagram Relay Logic Channel Testing.	7.5-34
Figure 7.6-1	Incore Instrumentation - Details Westinghouse Design	7.6-4
Figure 7.6-2	Incore Instrumentation - Details Replacement Design	7.6-5
Figure 7.6-3	Incore Mechanisms	7.6-6
Figure 7.7-1	Main Control Room Arrangement	7.7-9
Figure 7.10-1	Reactor Vessel Level Instrumentation System (RVLIS) Schematic	7.10-4

Chapter 7
INSTRUMENTATION AND CONTROL

7.1 INTRODUCTION

Note: As required by the Renewed Operating Licenses for Surry Units 1 and 2, issued March 20, 2003, various systems, structures, and components discussed within this chapter are subject to aging management. The programs and activities necessary to manage the aging of these systems, structures, and components are discussed in Chapter 18.

7.1.1 General Design Criteria

Instrumentation and controls are provided to monitor and maintain all operationally important reactor operating parameters such as neutron flux, system pressures, flow rates, temperatures, levels, and control rod positions within prescribed operating ranges.

Process variables which are required on a continuous basis for the start-up, power operation, and shutdown of the unit are indicated in, recorded in, and changed as necessary from the control room, which is a controlled access area. With controlled access, the operating staff is cognizant and in control of all test, maintenance, and calibration work and, knowing the extent to which specific and related operating tasks are in process, the staff can fully assess all abnormal plant conditions.

Criteria for instrumentation wires, cables, trays, and conduits are given in Chapter 8.

Several criteria related to all instrumentation and control systems but more specific to other plant features or systems are discussed in other chapters as listed below:

Criterion	Discussion
Suppression of power oscillations	Chapter 3
Reactor core design	Chapter 3
Quality standards	Chapter 1
Performance standards	Chapter 1
Fire protection	Chapter 9
Missile protection	Chapter 5
Emergency power	Chapter 8

7.1.2 Regulatory Guide 1.97 Program

Regulatory Guide 1.97, *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident,* contains tables of instrumentation required by the operators to monitor the plant and environs during and following an accident. This instrumentation consists of indicators that are associated with a variety of plant safe-shutdown and balance of plant systems. The intent of Regulatory Guide 1.97 is to provide the operators with the minimum essential information during and following an accident so that they will be able to mitigate and minimize the consequences of the accident. The regulatory guide has specifically determined four of the five types of instrumentation required to ensure proper indication is available to the operators. These four types (Type B, C, D, and E) are outlined in Table 3 of the regulatory guide along with their specifically assigned category, design, and qualification requirements. The fifth type of instrumentation, Type A variables, are plant specific. A Type A variable provides the operator with essential information necessary to take manual actions to mitigate an accident for which no automatic actions are provided. These instruments are characterized by their definition as stated in the regulatory guide. These definitions are:

1. Type A Variables: those variables to be monitored that provide the primary information required to permit the control room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accident events. Primary information is essential for the direct accomplishment of the specified safety functions; it does not include those variables that are associated with contingency actions that may also be identified in written procedures.

2. Type B Variables: those variables that provide information to indicate whether plant safety functions are being accomplished. Plant safety functions are (1) reactivity control, (2) core cooling, (3) maintaining reactor coolant system integrity, and (4) maintaining containment integrity (including radioactive effluent control). Variables are listed with designated ranges and category for design and qualification requirements. Key variables are indicated by design and qualification Category 1.

3. Type C Variables: those variables that provide information to indicate the potential for being breached or the actual breach of the barriers to fission product releases. The barriers are (1) fuel cladding, (2) primary coolant pressure boundary, and (3) containment.

4. Type D Variables: those variables that provide information to indicate the operation of individual safety systems and other systems important to safety. These variables are to help the operator make appropriate decisions in using the individual systems important to safety in mitigating the consequences of an accident.

5. Type E Variables: those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

To further define the variables, Regulatory Guide 1.97 has assigned each variable a design and qualification category. This categorization consists of either a category 1, 2, or 3 designation,

with a category 1 having the most stringent requirements, and category 3 having the least stringent. The variables are examined against twelve design and qualification criteria. However, category 2 or 3 variables may be exempt from some or all of the individual criterion's requirements. The criteria and how they are to be applied against each of the three categories are listed in Table 1, *Design and Qualification Criteria for Instrumentation,* of Regulatory Guide 1.97. The twelve category requirements consist of the following:

1. Equipment Qualification
2. Redundancy
3. Power Source
4. Channel Availability
5. Quality Assurance
6. Display and Recording
7. Range
8. Equipment Identification
9. Interfaces
10. Servicing, Testing, and Calibration
11. Human Factors
12. Direct Measurement

In response to NUREG 0737, and Regulatory Guide 1.97, Revision 3, Virginia Power has developed a programmatic approach in defining the Regulatory Guide 1.97 required equipment. The Virginia Power Regulatory Guide 1.97 program reviews examined each of the required instrumentation loops against the category design and qualification requirements. The reviews determined whether equipment upgrades to meet the regulatory guide requirements were required. The required equipment upgrades have been performed to meet the *Design and Qualification Criteria for Instrumentation* of the regulatory guide. Virginia Power has also taken exceptions to the category requirements for certain plant instruments. These exceptions to the regulatory guide have been outlined in correspondence between the NRC and Virginia Power. Virginia Power has developed a plant specific Technical Report, PE-0014, that provides a tabular identification of Regulatory Guide 1.97 instrumentation loops and circuits.

7.1 References

1. Technical Report PE-0014, *Surry Power Station Response to Regulatory Guide 1.97.*

Intentionally Blank

7.2 REACTOR PROTECTION SYSTEM

The reactor protection system and the engineered safeguards comprise the protective systems at the Surry Power Station. The equipment, from sensors to actuating devices, is considered a part of a given protective system.

The design objectives and functional implementation of the reactor protection system (tripping) and the engineered safeguards for the Surry units are the same as for H. B. Robinson Unit 2. The Surry reactor coolant systems have loop stop valves, where the H. B. Robinson unit does not. The presence of loop stop valves necessitates additional protection grade interlocks for the stop valve opening circuits.

As the functional requirements were translated into control equipment during the detailed design of the plant, some minor changes in equipment were made, to:

1. Reduce the amount of equipment required to accomplish a specific control function and, therefore, reduce equipment complexity and maintenance time during plant operation.
2. Modify instrument and control ranges to be consistent with the plant parameters corresponding to the increased power rating for Surry compared to that of the H. B. Robinson design.

Specific functions, however, will be accomplished with the same degree of reliability and redundance as they were in H. B. Robinson design. It should also be noted that the steam dump capacity of the Surry plant is approximately half of that provided for the H. B. Robinson plant, since the Surry plant is designed for a 50% load rejection without trip whereas the H. B. Robinson plant is designed for a 95% load rejection without trip.

All protection grade instrumentation and control systems were designed and procured by Westinghouse Electric Corporation, with the exception of containment pressure instrumentation and logic, containment spray systems, and diesel generators, which were in the Stone and Webster scope of supply.

There are no basic differences between Surry and H. B. Robinson with respect to protection grade instrumentation and control systems because both plants are designed in accordance with the criteria established in IEEE-279 and objectives of the General Design Criteria.

Design criteria for the Surry protective systems were chosen to permit maximum effective use of process measurements both for control and protection functions, thus enhancing the capability to provide an adequate system to deal with the majority of common-mode failures as well as to provide redundancy for critical control functions. This design approach provides protective systems that monitor numerous system variables by different means, i.e., protective system diversity. Such diversity has been evaluated for a wide variety of postulated accidents (Reference 1).

Reactor protection system and engineered safety features equipment are identified as safety-related equipment by several means. The electrical cables to vital instruments and control and electrical components are color coded to identify them as vital circuits. Vital circuits are divided into three main categories:

1. The 4160V and 480V ac and 125V dc circuits fed to or from the emergency buses 1H and 2H are color-coded “orange.”
2. The 4160V and 480V ac and 125V dc circuits fed to or from the emergency buses 1J and 2J are color-coded “purple.”
3. The circuits for the four protection instrument channels are identified by red, white, blue, and yellow color coding.

In addition, colored nameplates are affixed to vital instruments and equipment used in operation. These components include air circuit breakers, panels, switchgear, voltmeters, ammeters, control switches, and other associated equipment.

The remainder of Section 7.2 is primarily concerned with the reactor protection system, although some information may also apply to the engineered safeguards. Detailed discussion of the engineered safeguards can be found in Section 7.5.

7.2.1 Design Bases

The reactor protection system and the engineered safeguards are designed in accordance with IEEE-279 *Standard, Nuclear Power Plant Protection Systems,* August 1968. Detailed descriptions of the implementation of these principles are presented in the remainder of Section 7.2 and in Sections 7.4 and 7.5.

7.2.1.1 Control Room

Each unit is equipped with a control room which contains those controls and instruments necessary for operation of the reactor and turbine generator under normal and accident conditions.

The control room is continuously occupied by qualified operating personnel under all operating and design-basis accident (DBA) conditions.

Sufficient shielding, distance, and containment integrity are provided to ensure that under postulated accident conditions during occupancy of the control room, control room personnel shall not be subjected to doses that, in the aggregate, would exceed the limits in 10 CFR 50, Appendix A, GDC 19. The control room ventilation consists of a system having a large percentage of recirculated air. The fresh air intake can be closed to stop the intake of airborne activity if monitors indicate that such action is appropriate, and breathing quality compressed air can be supplied from high-pressure storage bottles to maintain a small positive outflow from the control room for a period exceeding the containment leakage period.

7.2.1.2 **Core Protection Sequence**

If the reactor protection system receives signals which indicate an approach to unsafe operating conditions, the system actuates alarms, prevents control rod withdrawal, initiates load runback, and/or opens the reactor trip breakers.

The basic reactor operating philosophy is to define an allowable region of power, pressure, and coolant temperature conditions. This allowable range is defined by primary tripping functions, which include the overpower delta T trip, the overtemperature delta T trip, and the nuclear overpower trip. The operating region below these trip settings is designed so that no combination of power, temperature, and pressure could result in a departure from nucleate boiling ratio (DNBR) less than the design DNBR limit (Section 3.2.3) for any credible operational transient with all reactor coolant pumps in operation. Tripping functions in addition to the primary tripping functions stated above are provided to back up the primary tripping functions for specific abnormal conditions. A complete list of tripping functions is given in Table 7.2-1.

The dropped control rod is indicated by the rod position flat panel displays and by a rapid flux decrease on any of the power range nuclear channels.

Rod stops from nuclear overpower, overpower delta T, and overtemperature delta T deviation are provided to prevent abnormal power conditions, which could result from excessive control rod withdrawal initiated by a malfunction of the reactor control system or by operator violation of administrative procedures.

7.2.1.3 **Reliability, Redundancy, and Independence**

Protection and operation reliability is achieved in part by providing redundant instrumentation channels for each protective function. These redundant channels are electrically isolated and physically separated. The channel design incorporates separate sensors, separate power supplies, separate rack-mounted and panel-mounted equipment, and separate relays for the actuation of the protective function. For protective functions where two-out-of-three or two-out-of-four redundant-coincident actuation is provided, a single channel failure will not impair the protective function nor will it cause an unnecessary unit shutdown.

Reactor protection system channels are designed with sufficient redundancy for individual channel calibration and testing to be performed during power operation without degrading reactor protection. Bypass removal of one trip channel is accomplished by placing that channel in a partial-trip mode. For example, a two-out-of-three channel becomes a one-out-of-two channel. Testing will not cause a trip unless a trip condition exists concurrently in another channel.

The reactor protection system is designed so that the most probable modes of failure in each channel result in a reactor trip signal. The protection system design combines redundant sensors and channel independence with coincident trip philosophy so that a safe and reliable system is

provided in which a single failure will not defeat the channel function, cause a spurious trip, or violate reactor protection criteria.

In the Westinghouse control and protection system, the control system is separate and distinct from the protection system. Although the protection system is independent of the control system, the control system is dependent upon signals derived from the protection system through isolation amplifiers. The design approach is to use fully and thereby most efficiently, for both control and protection purposes, measurements of unit variables. Little additional safety is achieved by using independent but identical measurements for control and protection.

This approach permits all equipment to be identified for protection or control and to be grouped accordingly, electrically isolated, and physically separated. In this way there is control redundancy, providing a significant increase in overall unit safety and also a protection system continuously monitoring a large number of system variables by different means. That is, there is protection system diversity.

In the reactor protection system, two reactor trip breakers are provided to interrupt power to the control rod assembly drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all control rod assembly drive mechanisms and permits the control rod assemblies to free fall into the core.

A bypass breaker is also provided for each reactor trip breaker. It should be noted that administrative controls alone are not relied upon to prevent simultaneous closure of both reactor trip bypass breakers. When either reactor trip bypass breaker is placed in the operate position, an alarm and annunciator is actuated in the control room. Also, closing one reactor trip bypass breaker when both breakers are in the operate position will generate a trip signal for the other reactor trip bypass breaker.

The components of the protection system are designed and arranged so that, even with an adverse environment accompanying an emergency situation, the components will function as required without interference.

Separation of redundant analog protection channels originates at the process sensors and continues through the wiring route and containment penetrations to the analog protection racks. Physical separation is used to the maximum practical extent 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 components in different protection racks. Each redundant channel is energized from a separate instrument bus.

Further detail on redundancy is provided by the descriptions of the respective systems covered by Section 7.2.2. Required continuous power supply for the protection systems is discussed in Chapter 8.

7.2.1.4 **Reactivity Control**

One of the two reactivity control systems employs control rod assemblies to regulate the position of the neutron absorbers within the reactor core (Chapter 3). The other reactivity control system employs the chemical and volume control system (Chapter 9) to regulate the concentration of boric acid solution neutron absorber in the reactor coolant system.

Reactor shutdown by control rod assemblies is completely independent of the normal control functions, since the trip breakers interrupt the power to the control rod mechanisms regardless of existing control signals. Effects of continuous withdrawal of a control rod assembly and of de-boration are described in Chapter 14.

7.2.1.5 **Manual Actuation**

Means are provided for manual initiation of protective system action. Failure in the automatic system does not prevent the manual actuation of protective functions. Manual actuation is designed to require the operation of a minimum amount of equipment.

7.2.1.6 **Channel Bypass**

The system is designed to permit any one channel to be maintained, tested, or calibrated during power operation without system trip. During such operation the active parts of the system continue to meet the single-failure criterion, since the channel under test is either tripped or makes use of superimposed test signals that do not negate the process signal.

"One-out-of-two" systems are permitted to violate the single-failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated and the bypass time interval is short.

7.2.1.7 **Calibration and Testing**

The bi-stable portions of the protective system (e.g., relays, bi-stables, etc.) provide trip signals only after signals from analog portions of the system reach preset values. Capability is provided for calibrating and testing the performance of the bi-stable portion of protective channels and various combinations of the logic networks during reactor operation.

The analog portion of a protective channel (e.g., sensor and amplifier) provides an analog signal of the reactor or unit parameter. The following methods for checking the analog portion of a protective channel during reactor operation are provided:

1. Varying the monitored parameter.
2. Introducing and varying a substitute transmitter signal.
3. Cross-checking between identical channels or between channels that bear a known relationship to each other and that have readouts available.

The design provides for administrative control in order to manually bypass channels for test and calibration purposes.

The design provides for administrative control of access to all trip settings, module calibration adjustments, test points, and signal injection points.

The signal-conditioning equipment of each protection channel in service at power is capable of being calibrated and tested independently by simulated analog input signals to verify its operation without tripping the reactor. The testing scheme includes checking through the trip logic to the trip breakers. Thus, the operability of each trip channel can be determined conveniently and without ambiguity. Functional operation of the power sources for the protection system is discussed in Chapter 8.

7.2.1.8 **Functional Requirements**

The reactor protection system in conjunction with inherent plant characteristics is designed to prevent anticipated abnormal conditions from exceeding limits established in Chapters 3 and 4.

7.2.1.8.1 Completion of Protective Action (Interlock)

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 part of the protective system and are designed in accordance with the criteria of this section.

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

7.2.1.8.2 Multiple Trip Settings

For monitoring neutron flux, multiple trip settings 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 protective system as designed provides positive assurance that the more restrictive trip setting is used. The devices used to prevent improper use of less restrictive trip settings are considered a part of the protective system and are designed in accordance with the criteria presented in this section.

7.2.1.8.3 Protective Actions

The reactor protection system automatically trips the reactor when the conditions listed in Table 7.2-1 exist.

Interlocking functions of the reactor protection system prevent control rod withdrawal when a specified parameter reaches a specified value that is less than the value at which a reactor trip is initiated.

For anticipated abnormal conditions, protective systems in conjunction with inherent characteristics and engineered safeguards are designed to ensure that limits for energy release to the containment and offsite radiation exposure (as in 10 CFR 50.67 or Regulatory Guide 1.183) are not exceeded.

Each reactor trip channel is designed on the “de-energize to operate” principle; an open channel or a loss of power causes that channel to go into its trip mode.

Reactor trip is implemented by simultaneously interrupting power to the magnetic latch mechanisms on each control rod drive, so that the control rod assemblies insert by free-fall. The entire protection system is thus inherently safe in the event of a loss of power.

7.2.1.8.4 Indication, Alarms, and Annunciators

All transmitted signals (flow, pressure, temperature, etc.) that can lead to a reactor trip are either indicated or recorded for every channel.

All neutron flux power range currents (top detector, bottom detector, and algebraic difference and average of bottom and top detector currents) are indicated and/or recorded.

The protective system provides the operator with complete information pertinent to system status and safety.

Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

Trips 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 corrective action to avoid a reactor trip. Further, actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

7.2.1.8.5 Operating Environment

The protective channels are designed to perform their function when subjected to adverse environmental conditions. See Section 7.5 for the criteria for those portions of the protective systems that must operate in a post-accident environment.

7.2.1.8.6 Seismic Design

Reactor protection system equipment is designed to ensure that it does not lose its capability to perform its function during an operating-basis earthquake or a design-basis earthquake, i.e., the equipment will shut the plant down and maintain it in a safe shutdown condition.

For the design-basis earthquake, there may be permanent deformation of the equipment provided that the capability to perform its function is maintained.

Typical protection system equipment is subjected to type tests under simulated seismic accelerations to demonstrate its ability to perform its functions. Type testing is done by using conservatively large accelerations and applicable frequencies. Analyses done for structures are not done for the reactor protection system equipment; however, the peak accelerations and frequencies are checked against those derived by structural analyses of operating-basis earthquake and design-basis earthquake loadings.

A Westinghouse topical report, WCAP-7397-L, provides the original seismic evaluation of safety-related equipment. The type tests covered by this report are applicable to the Surry Station with the exception of the process control equipment, which is covered in a supplement to WCAP-7397-L.

The control board is designed to withstand earthquake conditions, and an analysis was performed to verify the adequacy of the seismic design. Tests were not performed.

7.2.2 System Description

The reactor protection system provides the means for controlling the reactor in response to various measured primary and secondary variables associated with power, temperature, pressure, level, flow, and the availability of electric power. If the combination of monitored variables indicates an approach to unsafe conditions, the reactor protection system will initiate the appropriate protective action, e.g., load runback, prevention of rod withdrawal, or reactor trip (opening the reactor trip breakers).

Figure 7.2-1 illustrates typical core limits and shows the maximum trip points which are used for the protection system. The solid lines indicate a typical locus of DNBR equal to the design DNBR limit (Section 3.2.3) at four pressures, and the dashed lines indicate maximum permissible trip points for the overtemperature delta T reactor trip. Actual setpoints (the safety limits are given in the Technical Specifications) are lower to allow for measurement and instrumentation errors. The overpower delta T reactor trip limits the maximum core power independent of the DNBR.

Adequate margins exist between the nominal steady-state operating point and required trip points to preclude a spurious trip during design transients.

A block diagram of the reactor protection system showing various reactor trip functions and interlocks is shown in Figure 7.2-2. A logic diagram for the low-reactor-coolant-flow trips is shown in Figure 7.2-3.

7.2.2.1 **System Safety Features**

7.2.2.1.1 Separation of Redundant Protection Channels

The reactor protection system is designed to achieve separation between redundant protection channels. The channel design is applied to the analog and the logic portions of the

protection system and is illustrated by Figure 7.2-4. Although the illustration is for four-channel redundancy, the design is applicable to two-channel and three-channel redundancy.

Separation of redundant analog channels originates at the process sensors and continues along the wiring route and through containment penetrations to the analog protection racks. Isolation of wiring is achieved by using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Analog equipment is separated by locating redundant components in different protection racks. Each redundant channel is energized from a separate ac power feed. Logic equipment separation is achieved by providing separate racks, each associated with individual trip breakers.

Cables have been installed in accordance with VEPCO specification, *Criteria for Installation and Identification of Electrical Cables.*

Cables pertaining to reactor protection and engineered safety features are installed so that redundant circuits are separated and this separation is readily identified. Separation of redundant circuits is obtained by one of the following:

1. Rigid metal conduit (following separate routes).
2. Horizontal separation of horizontal cable trays without barriers.
3. Vertical separation of horizontal cable trays by means of barriers or tray covers (redundant channels are not combined in one tray or conduit).

A color-coded system is provided to identify individual safety channels, and additional colors are used to identify redundant safety trains. The color-coding scheme is an aid to both the installer of cable and the inspector.

1. Power cables and control cables are separated. Where possible, power cables are not installed in the same tray with control cables. Where it is necessary to install power cables in the same tray with control cables, a distance of at least 1/4 diameter of the power cable is maintained between the power and control cables. For safety circuits, where power and control cables are in the same tray, the power cable is contained in interlocked armor. Power cable is defined as any cable carrying 60A or supplying a 30-hp or larger motor. All power cables in trays are installed only one layer deep.
2. Control and instrument cables are usually run in separate trays; however, there are some areas where control and non-sensitive instrumentation cables are run in the same tray.
3. Cables from redundant protection channels or trains are never intermixed within a tray.
4. Non-vital cables such as annunciator, computer, or instrument cables may be routed with the protection system cables; however, they are separated wherever practical.

The cables to the penetrations in the cable tunnel and vaults are routed in two separate cable runs. There is a total of 90 penetrations, 5 rows high by 18 rows long.

The penetrations are arranged so that power, control, and instrumentation cables are separated from each other within a train and the two trains are never intermixed. The minimum distance between redundant services is never less than 2 feet at the penetrations.

Cable de-rating factors are in accordance with standards of the Insulated Power Cable Engineers' Association. Power cables 60A and over are rated and sized for 90°C operation, with the exception of the Station Service Transformer secondary leads that are sized for 85°C operation to provide a 5°C temperature margin for the leads. The sizing of power cables includes service factor where applicable, de-rating factors for maintained cable spacing of 1/4 diameter, and fire stops, if used. Where power cable spacing is less than 1/4 diameter (maintained), the power cables are treated as random filled and de-rated with base ampacities using applicable industry standards.

Control cables may be installed in cable trays in a random manner up to 80% of tray capacity, computed using the cross-sectional area of the cable. Control cables must meet one of the following conditions:

1. No appreciable conductor I^2R heating loss (interlocks, indicating lamps, controls, etc.).
2. Intermittent duty (valve operators).
3. Cable for continuous operation must use a derating factor of 50%-maximum continuous operation 60A or 30 hp - maximum wire size No. 4 AWG copper.

Instrument cables are installed in trays in a random manner up to 80% of tray capacity, computed by using the cross-sectional area of the cable, without derating. The protection of cables is either by protective relays or circuit breakers that are individually selected for each circuit.

Smoke detectors and carbon dioxide protection are provided in non-occupied areas of cable runs, such as cable tray rooms and cable tunnels. The cable purchased will not propagate fire, and sleeves are sealed after installation of cables. Additional horizontal and vertical fire stops are provided where required. No temperature monitoring of cables is provided. Each cable and wireway is permanently identified with markers.

The criteria for location and routing of instrument lines and transmitters were similar to the criteria established for electrical cables run between the transmitters and penetrations. For example, redundant transmitters and sensing lines are separated, and redundant devices are separated by a minimum of 2 feet, or additional protection is provided.

In reference to Reference Drawings 1 and 2, all cables from the Unit 1 reactor containment pass through a common vault area. Two protection channels and one train are routed on one side of the vault separated by metal tray covers, and the redundant channels and train are routed in a similar manner on the other side. This area is free from combustible materials, potential missile-generating devices, and is protected by fire detection equipment and a carbon dioxide deluge system. Unit 2 is completely isolated from Unit 1.

The reactor trip bi-stables are mounted in the analog protection racks and are the final operational component in an analog protection channel.

Each bi-stable drives logic relays “C” and “D” as shown on Figure 7.2-4. The contacts from the “C” relays are interconnected to form the required actuation logic for trip breaker 1. The transition from channel identity to logic identity is made at the logic relay coil/relay contact interface. As such, there is both electrical and physical separation between the analog and the logic portions of the protection system. The above logic network is duplicated from trip breaker 2 by using the contacts from the “D” relays. Therefore, the two redundant reactor trip logic channels will be physically separated and electrically isolated from one another. The reactor protection system consists of identifiable channels that are physically, electrically, and functionally separated and isolated from one another.

7.2.2.1.2 Loss of Power

A loss of power in the reactor protection system causes the affected channel to trip. All bi-stables operate in a normally energized state and go to a de-energized state to initiate action.

7.2.2.1.3 Reactor Trip Signal Testing

Provisions are made, for process variables, to manually place the output of the bi-stable in a tripped condition for “at power” testing of all portions of each trip circuit including the reactor trip breakers. Administrative procedures require that the final element in a trip channel (required during power operation) be placed in the trip mode before that channel is taken out of service for repair or testing so that the single-failure criterion is met by the remaining channels. In the source and intermediate ranges where the trip logic is one out of two for each range, bypasses are provided for this testing procedure.

Nuclear instrument power range channels are tested by superimposing a test signal on the sensor signal so that the reactor trip protection is not bypassed. Based upon coincident logic (two-out-of-four) this will not trip the reactor.

Provision is made for the insertion of test signals in each analog loop. Verification of the test signal is made by portable instruments at test points specifically provided for this purpose. This enables testing and calibration of meters and bi-stables. Transmitters and sensors are checked against each other and against precision readout equipment when required during normal power operation.

7.2.2.1.4 Process Analog Protection Channel Testing

The basic arrangement of elements comprising a representative analog protection channel is shown in Figure 7.2-5. These elements include a sensor or transmitter, power supply, bi-stable, bi-stable trip switch and proving lamp, test-operate switch, test annunciator, test signal injection jack, and test points. A portion of the logic system is also included to illustrate the overlap

between the typical analog channel and the corresponding logic circuits. The analog system symbols are given in Table 7.2-2.

Each protection rack includes a test panel containing those switches, test jacks, and related equipment needed to test the channels contained in the rack. An interlocked, hinged cover encloses the test panel. Opening the cover or placing the test-operate switch in the TEST position automatically initiates an alarm. The test panel cover is designed in such a way that it cannot be closed (and the alarm cleared) unless the test signal plugs (described below) are removed. Closing the test panel cover mechanically returns the test switches to the OPERATE position.

Test procedures require the bi-stable output relays of the channel under test to be placed in the tripped mode before proceeding with the analog channel tests. Thus, for the channel under test, the relay elements in the two-out-of-three or the two-out-of-four coincident matrices are in the tripped mode during the entire test of that channel. This ensures that the remaining channels of the two-out-of-three or the two-out-of-four protective functions meet the single-failure criterion during the entire channel test. Placing the bi-stable trip switch in the tripped mode de-energizes (trips) the bi-stable output relays and connects a proving lamp to the bi-stable output circuit. This permits the electrical operation of the solid-state bi-stable to be observed and the bi-stable setpoint relative to the channel analog signal to be verified. Upon completion of the test of the analog channel, the bi-stable trip switches must be manually reset to their operate mode. Closing the cover of the test panel does not transfer the bi-stable trip switches from their tripped to their operate position.

Analog channel tests are accomplished by simulating a process measurement signal, varying the simulated signal over its signal span, and checking the correlation of bi-stable setpoints, channel readouts, and other loop elements with precision portable readout equipment. Test jacks are provided in the test panel for injection of the simulated process signal into each process analog protection channel. Test points are provided in the channel to facilitate an independent means for precision measurement and correlation of the test signal. With the exception of temperature loops that are monitored by special provisions, this procedure does not require any tools nor does it involve in any way the removal or disconnection of wires in the channel under test. In general, the analog channel circuits are arranged so the channel power supply is loaded and provides sensing circuit power during channel test. Load capability of the channel power supply is thereby verified by the channel test.

7.2.2.1.5 Nuclear Instrumentation Channel Testing

Nuclear instrumentation system channels are tested by superimposing the test signal on the actual detector signal being received by the channel. The output of the bi-stable is not placed in a tripped condition before testing. A valid trip signal would then be added to the existing test signal and thereby cause channel trip at a somewhat lower percent of actual reactor power. Protection bi-stable operation is tested by increasing the test signal (level signal) to the bi-stable trip level and verifying operation at control board alarms and/or at the nuclear instrumentation racks.

A nuclear instrumentation channel that 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 test. The power range channels do not require bypass of the reactor trip function for test, since the protection logic is two out of four. The power range dropped-rod alarm is activated from a one-out-of-four logic. The channel test condition is alarmed on the nuclear instrumentation drawer and at the main control board. Administrative control is required to ensure that only one protection channel is placed in the bypass condition at any one time. The power range reactor trips are not affected by the test function described above. Therefore these power range trips are active if required. No provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the nuclear instrumentation detector.

7.2.2.1.6 Logic Channel Testing

The general design features of the logic system are described below. The trip logic channels for typical two-out-of-three and two-out-of-four trip functions are shown in Figure 7.2-6. The analog portions of these channels are shown in Figure 7.2-7. Each bi-stable drives two relays, one for each train. Contacts from the “A” and “C” relays are arranged in a two-out-of-three and two-out-of-four trip matrix for trip breaker 1.

The above configuration is duplicated for trip breaker 2 by using contacts from the “B” and “D” relays. A series configuration is used for the trip breakers, since they are actuated (opened) by undervoltage coils. This approach is consistent with a de-energize-to-trip preferred failure mode. The planned logic system testing includes exercising the reactor trip breakers to demonstrate system integrity. Bypass breakers are provided for this purpose. During normal operation, these bypass breakers are open. Administrative control will be used to minimize the amount of time these breakers are closed and to prevent simultaneous closure of both bypass breakers. Indication of a closed condition of either bypass breaker is provided locally and on the test panel, and on the control room bench board.

As is shown in Figure 7.2-6, the trip signal from the logic network is simultaneously applied to the main trip breaker associated with the specific logic chain as well as the bypass breaker associated with the alternate trip breaker. Should a valid trip signal occur while bypass breaker AB-1 is bypassing trip breaker TB-1, trip breaker TB-2 will be opened through its associated logic train. The trip signal applied to TB-2 is simultaneously applied to AB-1, thereby opening the bypass around TB-l. Trip breaker TB-l would have either been opened manually as part of the test, or it would be opened through its associated logic train, which would be operational (or tripped) during a test.

An auxiliary relay is located in parallel with the undervoltage coils of the trip breakers. This relay is connected to a test panel mounted white test lamp. The test lamp is used to indicate transmission of a trip signal through the logic network during testing. Lights are also provided to indicate the status of the logic relays.

The following procedure illustrates the method used for testing TB-l and its associated logic network:

1. From the Train B test panel, close bypass breaker AB-1 with the breaker pushbutton, then trip AB-1 from the test panel and visually verify operation. Should AB-1 fail to open, then immediately trip AB-1 with the local trip pushbutton.
2. Close AB-1 from the Train B test panel and make test connections for timing of TB-1.
3. At the trip breaker cubicle, push and hold the “Auto Shunt Trip Block” pushbutton for the TB-1 Breaker.
4. Push the “Auto Shunt Trip Test” pushbutton for TB-1 and verify TB-1 does not trip.
5. Release the “Auto Shunt Trip Test” pushbutton only and sequentially de-energize the trip relays (A1, A2, A3) for the logic combination (1-2, 1-3, 2-3). Verify that the logic network de-energizes the undervoltage coil on TB-l for each logic combination. Verify TB-1 opens by observing breaker position lamps at the test panel and record TB-1 elapsed time.
6. Release the “Auto Shunt Trip Block” pushbutton.
7. For the remaining logic combinations, sequentially de-energize the trip relays (A1, A2, A3) and verify that the logic network de-energizes the undervoltage coil on TB-l (by observing the UV status lamp) for each logic combination.
8. Close TB-1 from the control room benchboard.
9. Depress the “Auto Shunt Trip Test” pushbutton for the “A” reactor trip breaker momentarily and verify TB-1 trips.
10. Remove all test connections and close TB-1 from the benchboard.
11. Open bypass AB-1 from the Train B test panel.

In order to minimize the possibility of operational errors (such as tripping the reactor inadvertently or only partially checking all logic combinations), each logic network includes a logic channel test panel. This panel includes those switches, lights, and pushbuttons needed to perform the logic system tests. This arrangement is illustrated in Figure 7.2-8. The test switches used to de-energize the trip bi-stable relays operate through interposing relays as shown in Figures 7.2-5 and 7.2-7. This approach avoids violating the separation philosophy used in the analog channel design. Thus, although test switches for redundant channels are conveniently grouped on a single panel to facilitate testing, physical and electrical separation of redundant protection channels are maintained by the inclusion of the interposing relay, which is actuated by the logic test switches.

Modifications to the reactor trip switchgear were implemented to satisfy action items in NRC Generic Letter 83-28 (Reference 4), to improve reactor trip system reliability.

The reactor trip switchgear was modified to provide a redundant/backup means to automatically trip the breakers. An automatic shunt trip relay was installed which de-energizes on a reactor trip signal and energizes the shunt trip attachment to trip the breaker. The automatic shunt trip relay, test pushbuttons, and test jack connectors are located on a panel installed into the reactor trip breakers instrument compartment.

Test jack connectors and pushbuttons are provided to test the automatic shunt trip devices and to verify breaker operations and response time.

7.2.2.1.7 Primary Power Source

The source of electrical power for the measuring elements and the actuation of circuits in the engineered safeguards instrumentation and the reactor protection system are described in Chapter 8.

7.2.2.2 **Protective Actions**

Rapid reactivity shutdown is provided by the insertion of control rod assemblies by free-fall. Duplicate series-connected circuit breakers supply all power to the control rod assembly drive mechanisms. The control rod assembly must be energized to remain withdrawn from the core. Automatic reactor trip occurs upon the loss of power to the control rod assemblies. The trip breakers are opened by the undervoltage coils on both breakers. The undervoltage coils, which are normally energized, become de-energized by any one of the several trip signals.

The design of the devices providing signals to the circuit breaker undervoltage trip coils is such as to cause these coils to trip the breaker on reactor trip signal or power loss.

Certain reactor trip channels are automatically bypassed at low power where they are not required for safety. Nuclear source range and intermediate range trips are specifically provided for protection at low power or subcritical operation. At higher power operations they are bypassed by manual action.

During power operation, a sufficient amount of rapid shutdown capability in the form of control rod assemblies is administratively maintained by means of the control rod insertion limit monitors. Administrative control requires that all shutdown group rods be in the fully withdrawn position during power operation except during low power physics testing.

Reactor trips, means of actuation, and the coincident circuit requirements are listed in Table 7.2-1. The interlocks, referred to in Table 7.2-1, are listed in Table 7.2-3.

7.2.2.2.1 Manual Reactor Trip

The manual actuating devices are independent of the automatic trip circuitry and are not subject to failures which make the automatic circuitry inoperable. Actuating either of two manual trip devices located in the control room initiates a reactor trip and a turbine trip.

7.2.2.2.2 Power Range High-Neutron-Flux Reactor Trip

This circuit trips the reactor when two of the four power range channels read above the trip setpoint. There are two independent trip settings, a high and a low setting. The high trip setting provides protection during normal power operation. The low setting, which provides protection during start-up, can be manually bypassed when two out of the four power range channels read above approximately 10% power (P-10). A reading of three out of the four channels below 10% automatically reinstates the trip function. The high setting is always active.

7.2.2.2.3 Intermediate Range High-Neutron-Flux Reactor Trip

This circuit trips the reactor when one out of the two intermediate range channels reads above the trip setpoint. This trip, which provides protection during reactor start-up, can be manually bypassed if two out of four power range channels are above approximately 10%. Three out of four channels reading below this value automatically reinstate the trip function. The intermediate channels (including detectors) are separate from the power range channels.

7.2.2.2.4 Source Range High-Neutron-Flux Reactor Trip

This circuit trips the reactor when one of the two source range channels reads above the trip setpoint. This trip, which provides protection during reactor start-up, can be manually bypassed when one of two intermediate range channels reads above the P-6 setpoint value, and it is automatically reinstated when both intermediate range channels decrease below this value (P-6). This trip is also bypassed by two out of four high-power-range signals (P-10). The trip function can also be reinstated below the P-10 setpoint value by an administrative action requiring coincident manual actuation. The trip point is set between the source range power level corresponding to the P-6 setpoint value and the maximum source range power level.

7.2.2.2.5 Overtemperature Delta T Reactor Trip

The purpose of this trip is to protect the core against departure from nucleate boiling. The allowable delta T for this tripping function is continuously calculated for each loop from the following equation:

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

where:
ΔT_0 = indicated ΔT at rated thermal power, °F
T = average reactor coolant temperature, °F
T' = reference average reactor coolant temperature, °F
P = pressurizer pressure, psig
P' = reference pressurizer pressure, psig
K_1 = OTΔT equation coefficient, unitless
K_2, K_3 = OTΔT equation coefficients accounting for DNB effect of variations in system temperature and pressure, $°F^{-1}$, $psig^{-1}$

ΔI = P_{top}-P_{bot}, where P_{top} and P_{bot} are the percentage of power in the top and bottom halves of the core, respectively
$f(\Delta I)$ = function to account for DNB effect of axial power skewing
τ_1, τ_2 = lead-lag time constants, sec
s = Laplace transform variable, sec^{-1}

The allowable delta T is calculated for each reactor coolant loop. A trip occurs when the delta T in two out of the three (2/3) loops exceed the allowable delta T as calculated by the above equation. Initiation of automatic turbine load runback by means of an overtemperature delta T signal is discussed in Section 7.2.2.5.

7.2.2.2.6 Overpower Delta T Reactor Trip

The purpose of this trip is to protect against excessive power level (fuel rod rating protection). The allowable delta T for this tripping function is continuously calculated for each loop from the following equation:

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

where:
ΔT_0 = indicated ΔT at rated thermal power, °F
T = average reactor coolant temperature, °F
T' = reference average reactor coolant temperature, °F
K_4 = OPΔT equation coefficient, unitless
K_5, K_6 = OPΔT equation coefficients accounting for effect of variations in system temperature $°F^{-1}$
ΔI = P_{top}-P_{bot}, where P_{top} and P_{bot} are the percentage of power in the top and bottom halves of the core, respectively
$f(\Delta I)$ = function to account for effect of axial power skewing
τ_3 = lead-lag time constant, sec
s = Laplace transform variable, sec^{-1}

The allowable delta T is calculated for each reactor coolant loop. A trip occurs when the delta T in two of the three (2/3) loops exceeds the allowable delta T as calculated by the above equation. Initiation of automatic turbine load runback by means of an overpower delta T signal is discussed in Section 7.2.2.5.

7.2.2.2.7 Pressurizer Low-Pressure Reactor Trip

The purpose of this trip is to protect against excessive core steam voids and to limit the necessary range of protection afforded by the overtemperature delta T trip. This trips the reactor on coincidence of two out of the three low pressurizer pressure signals. This trip is blocked when

three of the four power range channels and two of the two turbine first-stage pressure channels read below approximately 10% power (P-7). Each channel is lead-lag compensated.

7.2.2.2.8 Pressurizer High-Pressure Reactor Trip

The purpose of this trip is to limit the range of required protection from the overtemperature delta T trip and to protect against reactor coolant system overpressure. The reactor is tripped on coincidence of two out of the three high pressurizer pressure signals.

7.2.2.2.9 Pressurizer High Water Level Reactor Trip

This trip is provided as a backup to the pressurizer high-pressure reactor trip. The coincidence of two out of the three pressurizer high water level signals trips the reactor. This trip is blocked when three of the four power range channels or two of two turbine first-stage pressure channels read below approximately 10% power.

7.2.2.2.10 Low Reactor Coolant Flow Reactor Trips

These trips protect the core from departure from nucleate boiling following a loss-of-coolant flow. The means of sensing loss-of-coolant flow are described below:

1. A low-flow signal generated by two out of three low-flow signals per primary coolant loop will cause a reactor trip. Above the P-7 setpoint (approximately 10% power), low flow in any two loops results in a reactor trip. Above the P-8 setpoint (approximately 35% power), low flow in any loop results in a reactor trip.
2. Opening of the reactor coolant pump breakers results in a reactor trip by acting directly on the reactor trip circuits. Above the P-7 setpoint the reactor trips on two open-breaker signals. Above the P-8 setpoint the reactor trips on one open-breaker signal. One open-breaker signal is generated for each reactor coolant pump.
3. Above the P-7 setpoint an undervoltage or underfrequency signal from any two reactor coolant pump buses results in a reactor trip. There is one underfrequency and two undervoltage sensors per bus. An underfrequency signal (2/3) directly trips all of the reactor coolant pumps, and if the power level is above the P-7 setpoint, a reactor trip will also result. These trips do not meet IEEE-279 from sensor to actuation device and are therefore backup trips.

The logic for these tripping functions is shown schematically in Figure 7.2-3.

7.2.2.2.11 Safety Injection System Actuation Reactor Trip

A reactor trip occurs when the safety injection system is actuated. The means of actuating the safety injection system trips are:

1. Low-low pressurizer pressure.
2. High steam-line differential pressure.

3. High steam flow in coincidence with low steam-line pressure or low T_{avg}.
4. High containment pressure.
5. Manual.

These trips are listed in Table 7.2-1. Since the safety injection system actuations not only trip the reactor but initiate various components of the engineered safeguards, the logic diagrams and chain of events may be found in Figure 7.5-1.

7.2.2.2.12 Turbine Trip Reactor Trip

A turbine trip is sensed by two out of three signals from autostop oil pressure or four out of four stop valve closure signals. A turbine trip causes a direct reactor trip above approximately 10% power and results in a controlled short-term release of steam to the condenser, which removes sensible heat from the reactor coolant system and thereby avoids steam generator safety valve actuation.

In addition, this trip is independently actuated by the Anticipated Transient Without Scram (ATWS) Mitigation System Actuation Circuitry (AMSAC) should the RPS fail to actuate a trip. Above a preset turbine power (C-20 permissive), two out of three low steam generator water level signals in two out of three steam generators will initiate a trip provided a time delay incorporated into the AMSAC is satisfied.

The following conditions automatically trip the turbine generator:

1. Turbine overspeed.
2. Generator transformer and line faults or both output breakers open above 15% turbine power.
3. Low condenser vacuum.
4. Thrust-bearing oil high pressure.
5. Low lube oil pressure.
6. Low auto-stop oil pressure.
7. Low intake canal level.
8. Both feedwater pumps tripped.
9. Electro-hydraulic control power failure.
10. Anti-motoring.
11. Safety Injection.
12. High-high steam generator level.
13. High-high sixth point feedwater heater level (time delay).

14. Stop valves shut.
15. Reactor trip.
16. Manual trip.
17. AMSAC actuation.

7.2.2.2.13 Low Feedwater Flow Reactor Trip

This trip protects the reactor from a sudden loss of its heat sink. The trip is actuated by a steam/feedwater flow (low feedwater flow) mismatch (one out of two) in coincidence with low water level (one out of two) in any steam generator.

7.2.2.2.14 Low-Low Steam Generator Water Level Reactor Trip

The purpose of this trip is to protect the steam generator in the case of a sustained steam/feedwater flow mismatch of insufficient magnitude to cause a flow mismatch reactor trip. The trip is actuated on two out of the three low-low water level signals in any steam generator. This trip is blocked for a steam generator in a loop with the loop stop valves closed.

In addition, a further drop in steam generator water level will cause an independently actuated trip by AMSAC under the same conditions specified in Section 7.2.2.2.12 above.

7.2.2.3 **Rod Stops**

Rod stops are added to prevent a reactor trip or prevent an abnormal condition from increasing in magnitude, which would cause a reactor trip.

Rod stops are given in Table 7.2-4. Some of these have been previously noted under permissive circuits but are listed again, for completeness.

Rod stops actuated by overpower delta T or overtemperature delta T initiate turbine runback via load reference.

7.2.2.4 **Rod Drop Detection**

Two independent systems are provided to sense a rod drop: a rod bottom position detection system, and a system that senses sudden reduction in ex-core neutron flux. Both detection systems initiate alarms in the main control room.

The rod drop detection circuit from neutron flux consists basically of a derivative network. Since a dropped control rod assembly rapidly depresses the local neutron flux, the decrease in flux is detected by one or more of the power range detectors. The sudden decrease in detector current appears as a signal out of the derivative network. A signal output greater than a preset value (approximately 5%) trips an associated bi-stable. Any one of the four power range channels will actuate the rod drop alarm. The dropped-rod circuit is described in Section 7.4.3.

The backup indication for the dropped control rod assembly is the rod bottom signal derived for each rod from its individual position indication system. With the position indication system, initiation of protection is not dependent on location, reactivity worth, or power distribution changes.

Figure 7.4-2 indicates schematically the nuclear instrumentation system, including the dropped control rod assembly alarm.

7.2.2.5 **Automatic Turbine Load Runback**

Load runback is also initiated by an approach to an overpower or overtemperature condition. This will prevent high power operation, which might lead to a minimum DNBR less than 1.3.

A turbine load reference reduction is initiated by an overtemperature or overpower delta T signal in two out of three loops.

The turbine runback signal is accompanied by rod withdrawal stops.

7.2.2.6 **Control Group Rod Insertion Monitor**

The control group rod insertion limit, Z_{LL}, is calculated as a linear function of power. The equation is:

$$Z_{LL} = A(\Delta T)_{auct} + C$$

where A is a preset, manually adjustable gain and C is a preset, manually adjustable bias. The $(\Delta T)_{auct}$ is the auctioneered value of the temperature differences. Each loop has its measured value for delta T; the auctioneered value is the median value.

An insertion limit monitor with two alarm setpoints is provided for the control banks. See Figure 7.2-9 for illustration of the monitor circuit. A description of control and shutdown rod groups is provided in Section 7.3. The “low” alarm alerts the operator of an approach to a reduced shutdown reactivity situation requiring boron addition by following procedures with the chemical and volume control system. If the actuation of the “low-low” alarm occurs, the operator should take immediate action to add boron to the system.

7.2.2.7 **Reactor Coolant Flow Measurement**

Elbow taps are used on each of the three loops in the reactor coolant system as an instrument device that indicates 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 rate has occurred. The correlation between flow reduction and elbow tap readout has been well established by the following equation: $\Delta P/\Delta P_o = (\omega/\omega_o)1.8$, where ΔP_o is the referenced pressure differential with the corresponding referenced flow rate ω_o and ΔP is the pressure differential with the

corresponding referenced flow rate ω. The full-flow reference point was established during initial unit start-up. The low-flow trip point was then established by extrapolating along the correlation curve. The technique has been well established in providing core protection against low coolant flow in Westinghouse pressurized water reactor plants. The expected absolute accuracy of the channel is within ±10%, and field results have shown the repeatability of the trip point to be within ±1%. The analysis of the loss-of-flow transient presented in Section 14.2.9 assumes instrumentation error of ±3%.

7.2.2.8 **Reactor Coolant Pump Trip**

Generic Letter 85-12 (Reference 2) required the implementation of an approved manual reactor coolant pump (RCP) trip criterion. The need for RCP trip is a result of excessive peak clad temperatures during small-break LOCA events with forced reactor coolant flow. The trip criteria must distinguish between LOCA and non-LOCA events where forced reactor coolant flow is beneficial to transient mitigation. RCP trip criterion is based on subcooling margin concurrent with at least one HPSI pump in operation and capable of delivering flow to the RCS.

7.2.3 System Evaluation

7.2.3.1 **Departure From Nucleate Boiling**

The following is a description of how the reactor protection system prevents departure from nucleate boiling.

The variables affecting the DNBR are:

1. Thermal power.
2. Coolant flow.
3. Coolant temperature.
4. Coolant pressure.
5. Core power distribution.

Figure 7.2-1 illustrates the typical core limits for which the DNBR for the hottest fuel rod is equal to the design DNBR limit (Section 3.2.3) and shows the locus of the overpower and overtemperature delta T reactor trips as a function of T_{avg} and pressure. This illustration is derived from the inlet-temperature versus power relationships.

Figure 7.2-10 illustrates "T_{avg} - delta T" protection. Periodic measurements using the incore instrumentation system are used to verify that the actual core power distribution is within design limits.

Reactor trips for a fixed high pressurizer pressure and for a fixed low pressurizer pressure are provided to limit the pressure range over which core protection depends on the overpower and overtemperature delta T trips.

Reactor trips on nuclear overpower and low reactor coolant flow are provided for direct, immediate protection against rapid changes in these parameters. However, for all cases in which the calculated DNBR approaches the design DNBR limit (Section 3.2.3), a reactor trip on overpower and/or overtemperature delta T would also be actuated.

The delta T trip functions are based on the differences between measured hot-leg and cold-leg temperatures. These differences are proportional to core power.

The delta T trip functions are provided with a nuclear differential flux feedback to reflect a measure of axial power distribution. This will assist in preventing an adverse axial distribution that could lead to exceeding the allowable core conditions.

In the event of a difference between the upper and lower ion chamber signals that exceeds the desired range, automatic feedback signals are provided to reduce the overpower/overtemperature trip setpoints, to block rod withdrawal, and to reduce the load to maintain appropriate operating margins to these trip setpoints.

7.2.3.2 **Control/Protection Interaction**

7.2.3.2.1 Nuclear Flux

Four power range nuclear flux channels are provided for overpower protection. On three-loop plants only one signal is used for automatic control. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection. In principle, the same failure may cause rod withdrawal and hence overpower. The two-out-of-four overpower trip logic will ensure an overpower trip if needed even with an independent failure in another channel.

In addition, the control system will respond only to rapid changes in indicated nuclear flux; slow changes or drifts are compensated by the temperature control signals. Finally, an overpower signal from any nuclear channel will block automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.3.2.2 Coolant Temperature

The delta-T and T_{avg} signals developed in the reactor protection system for overtemperature delta-T and overpower delta-T reactor trips are also used in the reactor control system for rod position, steam dump, feedwater and pressurizer level control. Circuit isolators are installed to prevent a failure in the reactor control system from propagating back into the protection channels. In the control system, the delta-T and T_{avg} signals from each of the three protection channels are sent to Median Signal Selector (MSS) auctioneering circuits. The MSS is designed to prevent a failed protection system delta-T or T_{avg} signal from precipitating an inaccurate control system response. Under normal operating conditions with no failures in any RCS narrow range temperature instrument channel, the MSS will reject both the highest and lowest of the three signals received and pass to the control system only the signal whose value falls between the

high/low extremes (i.e., median signal). If two of the three input signals have identical values, the MSS will select one of the two identical signals for control until a deviation between the two is detected, at which point the median signal will be passed to the control system as discussed above. If one of the three inputs should fail completely, the MSS will reject the failed signal and select the highest of the remaining two valid inputs for reactor control. The use of the Median Signal Selector circuits in the reactor control system satisfies the Control and Protection System interaction requirements of IEEE 279-1971, and prevents a spurious low temperature signal from causing rod withdrawal.

7.2.3.2.3 Pressurizer Pressure

Three pressurizer pressure protection channel signals are used for high-pressure and low-pressure protection and as inputs to the overtemperature delta T trip protection function (Figure 7.2-11). Two separate channels are used to control pressurizer spray and heaters and power-operated relief valves.

A spurious high-pressure signal from one channel can cause low pressure by actuation of pressurizer spray and/or a relief valve. Additional redundancy is provided in the protection system to ensure underpressure protection, i.e., two-out-of-three low-low-pressure reactor trip logic and two-out-of-three logic for safety injection.

The pressurizer heaters are incapable of overpressurizing the reactor coolant system. The maximum steam production rate of the pressurizer heaters is a fraction of the steam relief capacity of the pressurizer. Therefore, overpressure protection is not required for a pressure control failure; however, two-out-of-three high-pressure trip logic is used.

In addition, either of the two power-operated relief valves can easily maintain pressure below the high-pressure trip point. Each relief valve is controlled by an independent pressure channel, one of which is independent of the pressure channel used for heater control. Separation between heater control and one relief valve further precludes the likelihood of overpressurization of the system by a spurious low-pressure signal. Finally, the rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available for operator action.

7.2.3.2.4 Pressurizer Level

High pressurizer level in two of the three pressurizer level channels will initiate a reactor trip. Isolated output signals from these channels are used for pressurizer level control. A level control failure could fill or empty the pressurizer at a slow rate (on the order of half an hour or more) (Figure 7.2-12).

A reactor trip on pressurizer high level is provided to prevent filling the pressurizer in the event of a rapid thermal expansion of the reactor coolant. A rapid change from high rates of steam relief to water relief could be damaging to the safety valves, relief piping, and pressure relief tank. However, a level control failure cannot actuate the safety valves because the high-pressure reactor

trip is set below the safety valve set pressure. With the slow rate of charging available, overshoot in pressure before the trip is effective is much less than the difference between reactor trip and safety valve set pressures. Therefore, a control failure does not require protection system action. In addition, ample time and alarms are available for operator action.

7.2.3.2.5 Steam Generator Water Level/Feedwater Flow

Before describing control and protection interaction for these channels, it is beneficial to review the protection system basis for this instrumentation (Figure 7.2-13).

The basic function of the reactor protection circuits associated with low steam generator water level and low feedwater flow is to preserve the steam generator heat sink for removal of long-term residual heat. Should a complete loss of feedwater occur with no protective action, the steam generators would boil dry and cause an overtemperature/overpressure excursion in the reactor coolant. Reactor trips on temperature, pressure, and pressurizer water level will trip the unit before there is any damage to the core or reactor coolant system. Redundant auxiliary feedwater pumps are provided to prevent residual heat after trip from causing thermal expansion and discharge of the reactor coolant through the pressurizer relief valves. Reactor trips act before the steam generators are dry to reduce the required capacity and starting time requirements of these pumps and to minimize the thermal transient on the reactor coolant system and steam generators. Independent trip circuits are provided for each steam generator for the following reasons:

1. Should severe mechanical damage occur to the feedwater line to one steam generator, it is difficult to ensure the functional integrity of level and flow instrumentation for that unit. For instance, a major pipe break between the feedwater flow element and the steam generator would cause high flow through the flow element. The rapid depressurization of the steam generator would drastically affect the relation between downcomer water level and steam generator water inventory.
2. It is desirable to minimize thermal transients on a steam generator for credible loss of feedwater accidents. It should be noted that controller malfunctions caused by a protection system failure affect only one steam generator. Also, they do not impair the capability of the main feedwater system under either manual control or automatic control. Hence, these failures are far from being the worst case with respect to decay heat removal with the steam generators.

A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow and prevent that channel from tripping. A reactor trip on low-low water level, independent of indicated feedwater flow, will ensure a reactor trip if needed.

In the event of an Anticipated Transient Without Scram (ATWS) event, the ATWS Mitigation System Circuitry (AMSAC) will trip the turbine, trip the reactor, isolate blowdown lines, and start the auxiliary feedwater pumps.

In addition, the three-element feedwater controller incorporates reset on level, such that with expected controller settings a rapid increase in the flow signal would cause only a small decrease in level before the controller reopened the feedwater valve. A slow increase in the feedwater signal would have no effect at all.

A spurious low steam flow signal would have the same effects as a high feedwater signal, discussed above.

A spurious high water level signal from the protection channel used for control will tend to close the feedwater valve. This level channel is independent of the level and flow channels used for reactor trip on low-flow coincident with low level.

The actual plant response to the controlling steam generator level channel depends on the initial power level, as discussed in the subparagraphs below. In the evaluation which follows, it is postulated that in addition to the spurious high signal from the steam generator level channel controlling feedwater flow, there is a failure in an additional level channel, consistent with the design requirements of IEEE-279 for evaluation of control and protection channel interactions. Since the steam generator low-low level protection function requires two out of three channels, this function would be rendered inoperable on the steam generator experiencing the loss of feedwater.

1. 0% to approximately 20% power

   Below approximately 20% power, feedwater is normally manually controlled via the main feedwater regulating valve bypass valves. Therefore it is highly unlikely that the failure of the single level channel will result in reduced feedwater flow to a steam generator. In addition, the low power level condition results in a significant allowed operator action time to respond to reduced feedwater flow conditions before the ANS Condition II criteria applicable to the loss of normal feedwater accident are violated. Manual control of the feedwater flow also serves to increase the level of operator awareness to the status of the feedwater system and steam generator inventory. If the operator does not take action, either a high pressurizer water level trip or a low-low steam generator level signal in one of the other steam generators will trip the reactor prior to exceeding any of the applicable acceptance criteria.

2. Approximately 20% power to approximately 54% power

   The low feedwater flow trip may not be available at power levels below approximately 54% power for a 1/N loss of feedwater event because measure steam flow may not be high enough to trip the high steam flow bistables. If the heatup is severe enough, the pressurizer water level could exceed the pressurizer high water level trip setpoint.

   If a reactor trip were generated, it would: (1) alert the operator of an abnormal condition and (2) cause the voids in the shell-side inventories of the unaffected steam generators to collapse and drop the water levels below the low-low level trip setpoint, thereby actuating the auxiliary feedwater system.

In addition, secondary heat sink requirements at power levels below 54% power can be satisfied by the unaffected steam generators due to the reduced decay heat loads. These unaffected steam generators will continue to remove heat from the RCS until a low-low level signal is generated. If the RCS heats up rapidly, or if the letdown capacity is sufficient to prevent the high pressurizer water level trip, the overtemperature delta-T trip will preclude any potential violations of the core thermal limits. Thus, due to diversity in the design of the reactor protection system, an automatic reactor trip signal will be generated by one of the signals identified above if required.

3. Approximately 54% to 100% power

   If power level is greater than approximately 54%, the IEEE-279 scenario is protected by the steam/feed flow mismatch coincident with 1/3 low steam generator level reactor trip function. The low feedwater flow function is not a direct substitute for steam generator low-low level in that it does not provide for automatic initiation of auxiliary feedwater. However, the inventory in the unaffected steam generators will provide the necessary secondary heat sink for decay removal until the water level drops sufficiently to generate a low-low signal in the unfaulted generators and initiate AFW. Again, the high pressurizer water level signal will trip the reactor before the pressurizer can go water solid and overtemperature delta-T will provide backup protection in the event that the core thermal limits are approached.

7.2.3.2.6 Steam-Line Pressure

Three pressure channels per steam line are used for steam-line break protection. These are combined with other signals as shown in Table 7.2-1. Two-out-of-three high steam flow in coincidence with two-out-of-three low T_{avg} or in coincidence with two-out-of-three low steam-line pressure and two-out-of-three differential pressure between any steam line and steam-line header will actuate safety injection.

7.2.3.2.7 Anticipated Transient Without Scram (ATWS) Mitigation System Actuation Circuitry (AMSAC)

Pursuant to the requirements of 10 CFR 50.62, an AMSAC system has been installed to respond to an accident sequence should the reactor protection system (RPS) fail to shut down the reactor. The design basis for the system is summarized in Reference 4. The AMSAC provides a turbine trip, reactor trip, and auxiliary feedwater initiation, sends a signal to automatically close the steam generator blowdown valves, and trips the power supply breakers to the control rod motor generators.

The AMSAC design utilizes two turbine impulse chamber pressure sensors (one from two separate channels), as well as nine steam generator narrow range level sensors (three per steam generator) set at a range below the existing low-low level trip settings. The coincidence of two out of three steam generator level sensors taken twice and two out of two turbine impulse chamber pressure sensors detecting a pressure (load) greater than 37% automatically initiates the AMSAC.

Time delays, which are set inverse to power, have been incorporated into the AMSAC circuitry to allow the RPS to function initially, if functioning properly. However, if the RPS does not initiate a reactor trip, the AMSAC will trip the reactor. These time delays are set based on consideration of the time that the steam generators take to boil down to the low-low level setpoint upon loss of main feedwater.

The AMSAC has been designed and installed to meet the following criteria:

1. Diversity - The AMSAC logic circuits have been designed and installed to be diverse from the RPS to the extent practicable.
2. Logic Power Supplies - The AMSAC logic circuit power supplies are normally powered from non-safety-related power sources independent of the RPS and capable of operating on a loss of offsite power. They can be powered from EDG #1 (Unit 1) and EDG #2 (Unit 2) by manual action.
3. Maintenance Bypasses - Bypass switches have been installed in the control room to block operation of the AMSAC's output relays when performing maintenance on the AMSAC.
4. Operating Bypasses - The C-20 permissive is utilized as the AMSAC operating bypass to enable the control room operator to bring the plant up in power during start-up to avoid spurious AMSAC actuations at power levels below 37% nominal turbine load.

   The AMSAC generic design specified in Reference 6 called for AMSAC to be enabled when first stage turbine impulse pressure exceeded 40% (nominal) turbine load. This generic setpoint applies to all Westinghouse PWRs and is based on representative ATWS analyses which show that below 40% power an ATWS event without AMSAC produced only limited reactor coolant system (RCS) voiding. The Virginia Power AMSAC design specifies a nominal permissive (C-20) setpoint based on the generic setpoint of 40% turbine load minus an allowance for channel inaccuracies in the turbine impulse pressure channels themselves.

   In some of the Reference 6 discussions, turbine load and reactor power are used interchangeably. In reality, turbine load, as represented by impulse pressure, and reactor power are not linearly related and the two values tend to deviate as power and load are reduced. The setpoint development did not specifically address this nonlinearity between turbine impulse pressure and reactor power.

   As discussed in Reference 6 and supporting documents, the power level at which AMSAC is required to maintain the peak RCS pressure below the 3200 psig faulted stress limit for an ATWS has been shown generically to be 70% Rated Thermal Power (RTP). At power levels below 40% reactor power, an ATWS with no AMSAC would limit RCS voiding in the first 10 minutes to values less than obtained for the full power case with AMSAC.

   For power levels between 40% and 70%, voiding is not predicted to occur until well after the peak RCS pressure is reached. Additional studies of the loss of feedwater ATWS have shown

that for a C-20 setpoint corresponding to 50% RTP, the voiding that would occur without AMSAC was still less than that expected for the full power case with AMSAC (Reference 7).

Therefore the current Surry AMSAC design meets its design basis, provided AMSAC is armed at ≤40% turbine load (nominal) or ≤50% Rated Thermal Power.

Above 37% turbine load, the C-20 permissive will automatically arm the AMSAC logic. Upon the loss of a turbine impulse pressure signal or when turbine load decreases below 37%, the C-20 permissive will be blocked as noted in Table 7.2-1. The time delay is sufficient to avoid spurious trips while ensuring that the AMSAC will perform its function in the event of a turbine trip (loss of load trip).

5. Manual Initiation - Installation of the AMSAC does not preclude manual initiation of the AMSAC functions by utilizing existing manual controls for turbine trip, reactor trip, and auxiliary feedwater actuation, if necessary.
6. Electrical Independence from the RPS - Isolators have been installed at the interfaces in the AMSAC between safety-related and non-safety-related circuitry.
7. Physical Separation from Existing RPS - The AMSAC receives signals from the existing steam generator level and turbine impulse pressure instrumentation systems. However, the AMSAC cable routing is independent of RPS cable and the AMSAC equipment cabinets are located such that interaction with the RPS cabinets is precluded. Train separation requirements have also been maintained.
8. Environmental Qualification - AMSAC mitigation equipment is not required to be environmentally qualified, however, the equipment is located in mild environments in the station and will not be impacted by anticipated operational occurrences.
9. Testability at Power - End-to-end testing of the AMSAC system is performed every refueling outage. When the plant is at power, the system can be tested with the AMSAC outputs bypassed. The bypass is accomplished through permanently installed bypass switches. Status outputs to the main control board provide indication to the control room operator that the AMSAC system's outputs have been bypassed.
10. Seismic Qualification - The AMSAC panel and its components are Seismic Class I and have been seismically qualified to the requirements of IEEE-344-1975.

7.2.3.3 **Normal Operating Environment**

The normal operating environment for the main control room, and the qualification of protective equipment therein, is discussed in Section 7.7.

The average operating environment for equipment within the containment is normally maintained below 125°F. The reactor protection system instrumentation within the containment is designed for continuous operation. The temperature of the ex-core neutron detectors is maintained

at or below 135°F. The detectors are designed for continuous operation at 135°F and will withstand operation at 175°F for short durations.

7.2 REFERENCES

1. T. W. Burnet, D. H. Risher, and A. C. Hall, *Reactor Protection System Diversity in Westinghouse PWR*, WCAP 7306.
2. Generic Letter 85-12, *Implementation of TMI Action Item II.K.3.5 Automatic Trip of Reactor Coolant Pumps,* June 28, 1985.
3. Letter from W. L. Stewart (Virginia Electric and Power Company) to H. R. Denton (NRC), *Response to Generic Letter 85-12: Automatic Trip of Reactor Coolant Pumps,* Serial No. 85-510B, December 6, 1985.
4. Letter from L.B. Engle (NRC) to D.S. Cruden (Virginia Electric and Power Company) *Compliance with ATWS Rule, 10 CFR 50.62,* Surry Power Station Units 1 and 2, and North Anna Power Station Units 1 and 2 (TAC Nos. 59147, 59148, 59117 and 59118), dated May 26, 1988.
5. Generic Letter 83-28, *Required Actions Based on Generic Implications of Salem ATWS Event,* July 8, 1983.
6. WCAP-10858, Rev. 1-P-A, *AMSAC Generic Design Package,* July 1987.
7. Westinghouse Technical Bulletin ESBU-TB-08, *AMSAC C-20 Interlock Permissive,* November 26, 1997.

7.2 REFERENCE DRAWINGS

The list of Station Drawings below is provided for information only. The referenced drawings are not part of the UFSAR. This is not intended to be a complete listing of all Station Drawings referenced from this section of the UFSAR. The contents of Station Drawings are controlled by station procedure.

	Drawing Number	Description
1.	11448-FM-1B	Machine Location: Reactor Containment, Elevation 18'- 4"
	11548-FM-1B	Machine Location: Reactor Containment, Elevation 18'- 4"
2.	11448-FE-45A	Conduit and Cable Tray Plan, Cable Tunnel and Vaults
	11548-FE-45A	Conduit and Cable Tray Plan, Cable Tunnel and Vaults

Table 7.2-1
REACTOR TRIPS

Reactor Trip	Coincidence Circuitry and Interlocks	Comments
1. Manual	1/2, no interlocks	Either one trips reactor
2. Power range high neutron flux		
Low setpoint	2/4, low setpoint interlocked with P-10	Manual block and automatic reset of low setting by P-10, Table 7.2-2
High setpoint	2/4, no interlocks	
3. Overtemperature delta T	2/3, no interlocks	
4. Overpower delta T	2/3, no interlocks	
5. Low pressurizer pressure (fixed setpoint)	2/3, interlocked with P-7	
6. High pressurizer pressure (fixed setpoint)	2/3, no interlocks	
7. High pressurizer water level	2/3, interlocked with P-7	
8. Low reactor coolant flow	2/3 signals per loop, interlocked with P-7 and P-8	Blocked below P-7. Low flow in 1 loop permitted below P-8
9. Monitored electrical supply to reactor coolant pumps (non-safety-related backup trip)		
Undervoltage	Low voltage on 2 out of 3 buses, interlocked with P-7	
Underfrequency	Underfrequency on 2 out of 3 buses, interlocked with P-7	Underfrequency on 2 out of 3 buses will trip all reactor coolant pumps and cause reactor trip via trip of pump breakers; indicated in next entry
Reactor coolant pump breakers	Interlocked with P-7 and P-8	Blocked below P-7. Open breaker in 1 loop permitted below P-8.

Table 7.2-1 (continued)
REACTOR TRIPS

Reactor Trip	Coincidence Circuitry and Interlocks	Comments
10. Safety injection signal (actuation)	Low-low pressurizer (2/3); or 3/4 high containment pressure; or 2/3 high differential pressure between any steam line and steam-line header; or high main steam flow in 2/3 steam lines (1/2 per line) in coincidence with either 2/3 low T_{avg} or 2/3 low stem-line pressure; or manual 1/2 (see 7.2, System Description - Protective Action for Interlocks)	Trips main feedwater pumps, which closes the associated discharge valves. Closes all feedwater control valves. Low pressurizer pressure coincident with low pressurizer level. SIS may be blocked below 2000 psig. High steam flow in coincidence with low T_{avg} or low steam-line pressure may be manually blocked below approximately 543°F.
11. Turbine-generator trip	2/3 low auto stop oil pressure interlocked with P-7 or closure of all turbine stop valves as sensed by 2 switches per stop valve (interlocked with P-7)	
12. Steam/feedwater flow mismatch, coincident with low steam generator level	1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level, any loop.	
13. Low-low steam generator water level	2/3, any loop.	
14. Intermediate range neutron flux	1/2, manual block permitted by P-10.	Below P-10 automatic reset.
15. Source range neutron flux	1/2, manual block permitted by P-6, interlocked with P-10.	Automatic block above P-10 and automatic reset below P-6.
16. Steam generator water level (AMSAC)	2/3 per steam generator in 2/3 loops after a time delay, interlocked with C-20.	Blocked below C-20 after a time delay.

Table 7.2-2
LOGIC SYMBOLS

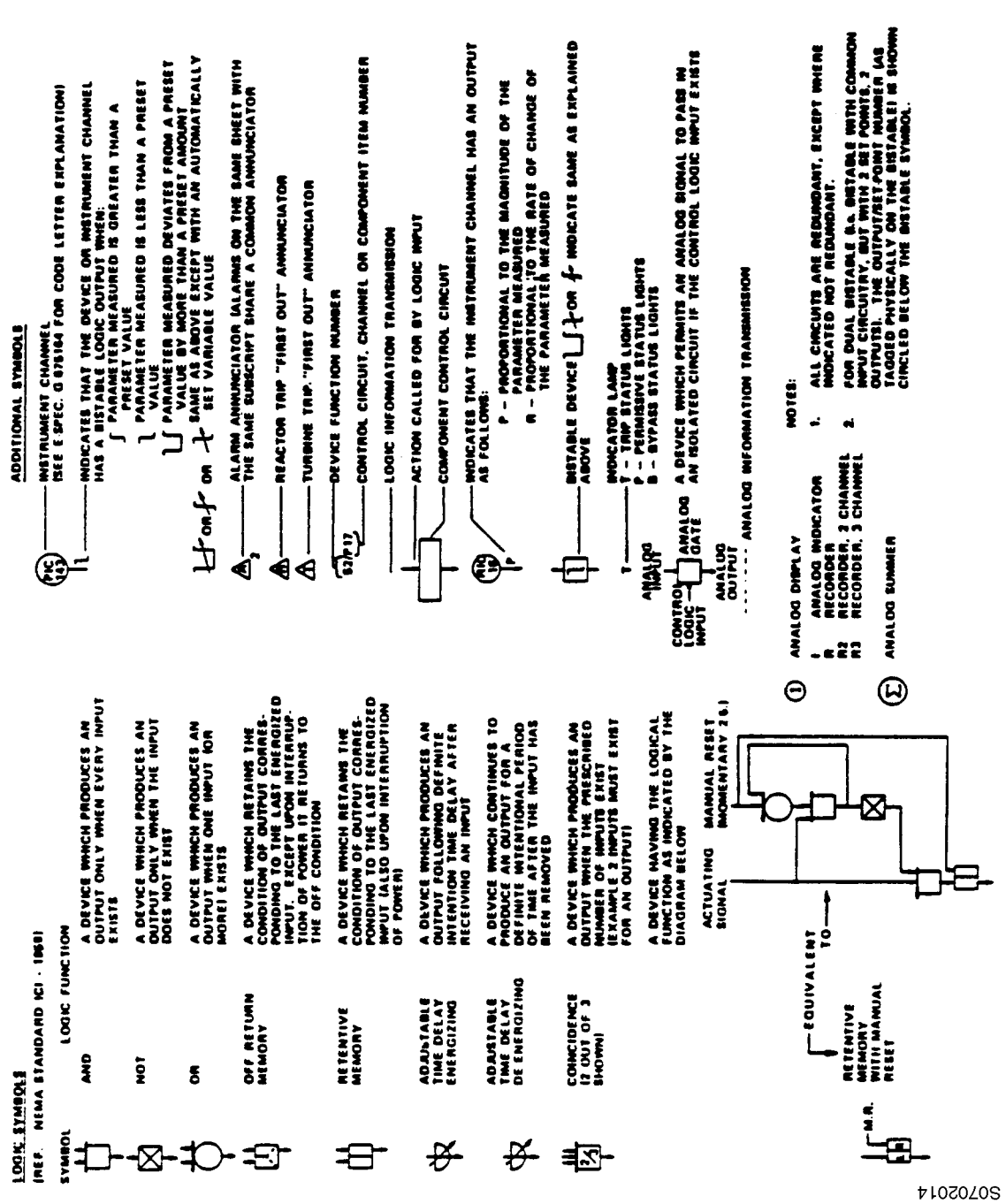


Table 7.2-2 (continued)
LOGIC SYMBOLS

Legend	
Al	alarm
Buf	buffer
f	special function (such as pressure compensation unit or lead/lag compensation)
F	amplifier
FC	flow controller (off-on unless output signal is shown)
FI	flow indicator
FLTR	filter
FS	flow steam
FT	flow transmitter
FW	flow water
Hi LRT	high-level reactor trip
Hi PRT	high-pressure reactor trip
I/I	isolation current repeater
ISOL	isolation (other than I/I)
LC	level controller (off-on unless output signal is shown)
LI	level indicator
L-Low	low level
Lo L	low level
Lo LRT	low-level reactor trip
Lo PRT	low-pressure reactor trip
L_{ref}	programmed reference level
L/L	lead/lag
LT	level transmitter
NC	nuclear flux controller
NE	nuclear detector
NI	nuclear flux indicator
NM	nuclear modifier
NQ	nuclear power
P	pressure
PC	pressure controller (off-on unless output signal is shown)
PI	pressure indicator
PM	pressure modifier
P_{ref}	programmed reference pressure

Table 7.2-2 (continued)
LOGIC SYMBOLS

Legend	
PS	power supply
PT	pressure transmitter
QM	flux modifier
R/I	resistance to current connector
RT	reactor trip
RTD	resistance temperature detector
S	control channel transfer switch (used to maintain auto channel during test of the protection channel)
SI	safety injection
sp	setpoint
T	transmitter
TC	temperature controller
TE	temperature element
TI	temperature indicator
TJ	test signal insertion jack
TM	temperature modifier
TP	test point
ϕU, L	out of core upper or lower ion chamber flux signals
$\frac{d}{dt}$	time rate of exchange
Σ	sum
f(Δq)	function of flux difference between upper and lower long ion chamber sections, f

Table 7.2-3
PROTECTION INTERLOCKS

Number	Derivation	Function
P-1	1/2 neutron flux (intermediate range) above setpoint; 1/4 neutron flux (power range) above setpoint	Blocks automatic and manual rod withdrawal
	2/3 overtemperature delta T above setpoint, 2/3 overpower delta T above setpoint	1. Blocks automatic and manual rod withdrawal 2. Initiates turbine runback via load reference
P-2	1/1 first-stage turbine pressure below setpoint	Blocks automatic rod withdrawal at low power
P-4	Reactor trip	1. Actuates turbine trip 2. Allows auto closing of main feedwater regulating valves on T_{avg} below setpoint 3. Prevents opening of main feedwater regulating and bypass valves which were closed by safety injection or high steam generator level
P-6	1/2 neutron flux (intermediate range) above setpoint; 2/2 neutron flux (intermediate range) below setpoint	1. Allows manual block of source range reactor trip 2. Automatically defeats block of source range reactor trip
P-7	3/4 neutron flux (power range) below setpoint (from P-10); 2/2 first-stage turbine pressure below setpoint	Blocks reactor trip on low flow, reactor coolant pump breakers open in more than one loop, undervoltage, underfrequency, turbine trip, pressurizer low pressure, pressurizer high level
	2/4 power range above setpoint or 1/2 turbine impulse chamber set above setpoint (power level increasing)	Allows reactor trip on: low flow or reactor coolant pump breakers open in more than one loop, undervoltage (RCP busses), underfrequency (RCP busses), turbine trip, pressurizer low pressure and pressurizer high level
P-8	3/4 neutron flux (power range) below setpoint	Blocks reactor trip on low flow or reactor coolant pump breaker open in a single loop

Table 7.2-3 (continued)
PROTECTION INTERLOCKS

Number	Derivation	Function
	2/4 power range above setpoint (power level increasing)	Permit reactor trip on low flow or reactor coolant pump breaker open in a single loop
P-9	1/2 condenser pressure above setpoint or all circulating water outlet valves closed	Blocks air supply to condenser steam dump valves
P-10	2/4 neutron flux (power range) above setpoint	1. Allows manual block of intermediate range reactor trip 2. Allows manual block of power range (low setpoint) reactor trip 3. Allows manual block of intermediate range rod stop (P-1) 4. Automatically blocks source range reactor trip (back-up for P-6) 5. Input to P-7
	3/4 neutron flux (power range) below setpoint	1. Defeats automatically the manual block of intermediate range reactor trip 2. Defeats automatically the manual block of power range (low setpoint) reactor trip 3. Defeats automatically the manual block of intermediate range rod stop

Table 7.2-4
ROD STOPS

Rod Stop	Actuation Signal	Rod Motion To Be Blocked
Nuclear overpower	1/4 high power range nuclear flux or 1/2 high intermediate range nuclear flux	Automatic and manual withdrawal
High delta T	2/3 overpower delta T or 2/3 overtemperature delta T	Automatic and manual withdrawal
Low power	1/1 low turbine impulse pressure	Automatic withdrawal

Figure 7.2-1
TYPICAL ILLUSTRATION OF $\Delta T - T_{avg}$ PROTECTION

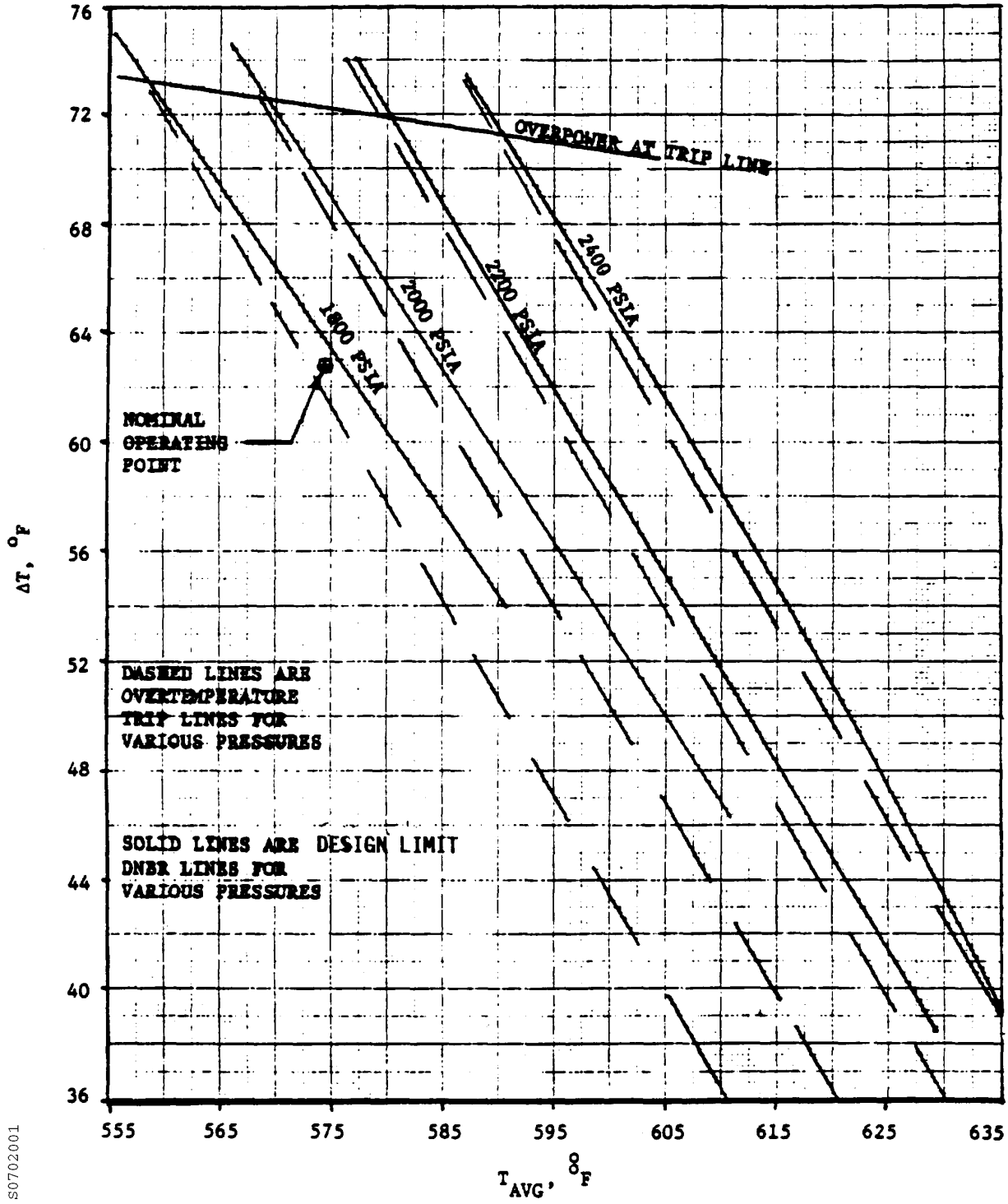


Figure 7.2-2
REACTOR TRIP SIGNALS

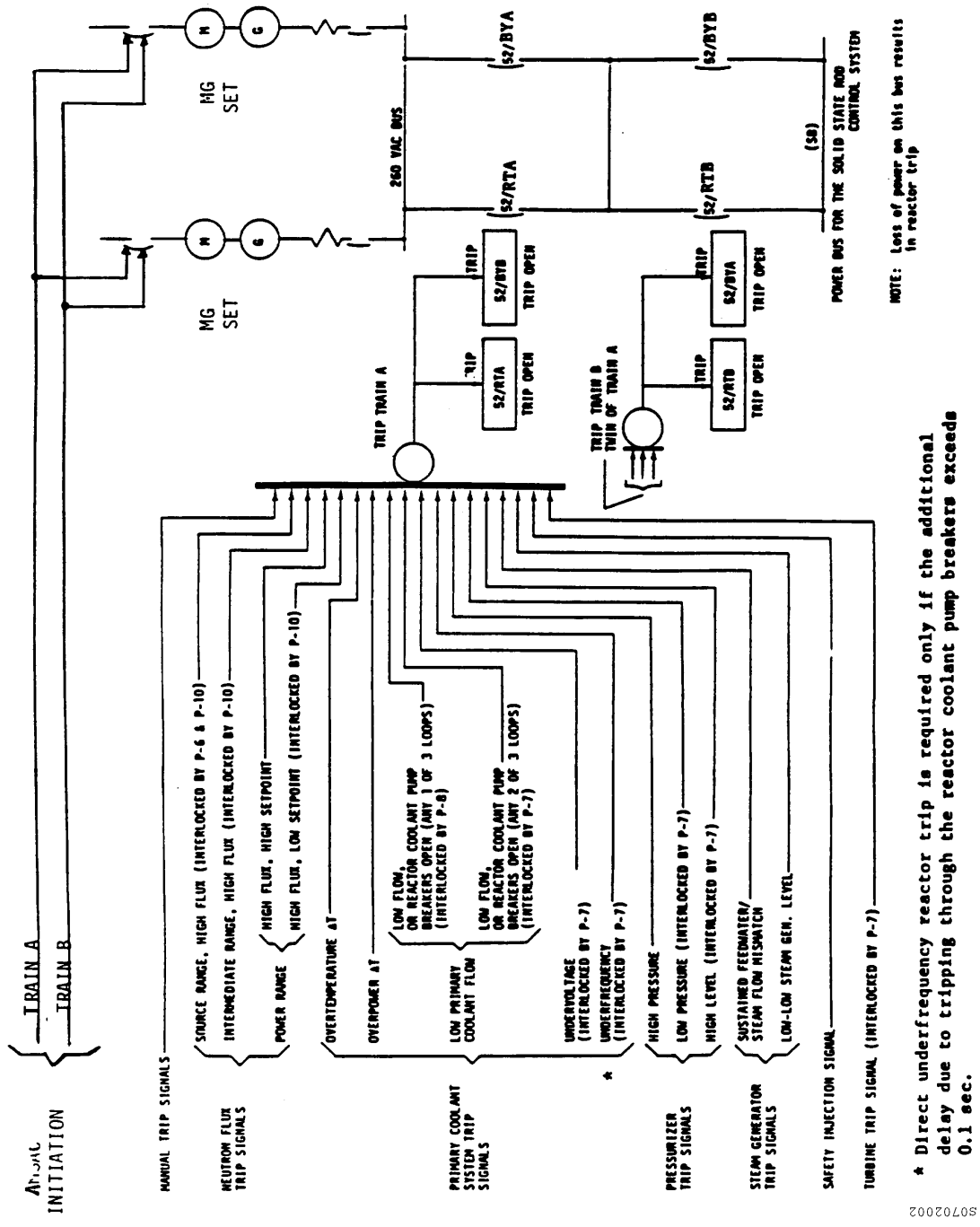


Figure 7.2-3
LOGIC DIAGRAM FOR LOW REACTOR COOLANT FLOW TRIPS

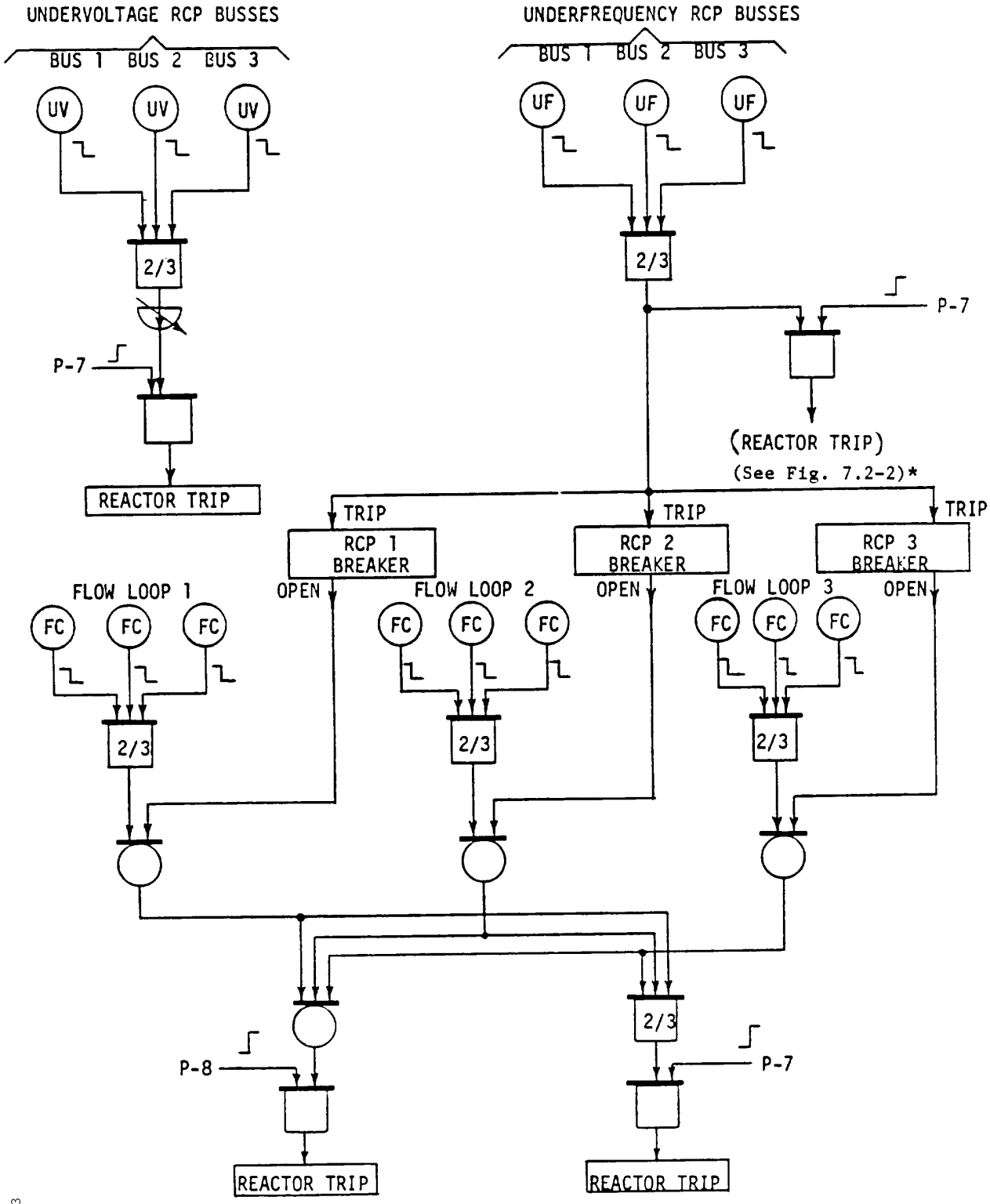


Figure 7.2-4
DESIGN TO ACHIEVE ISOLATION BETWEEN CHANNELS

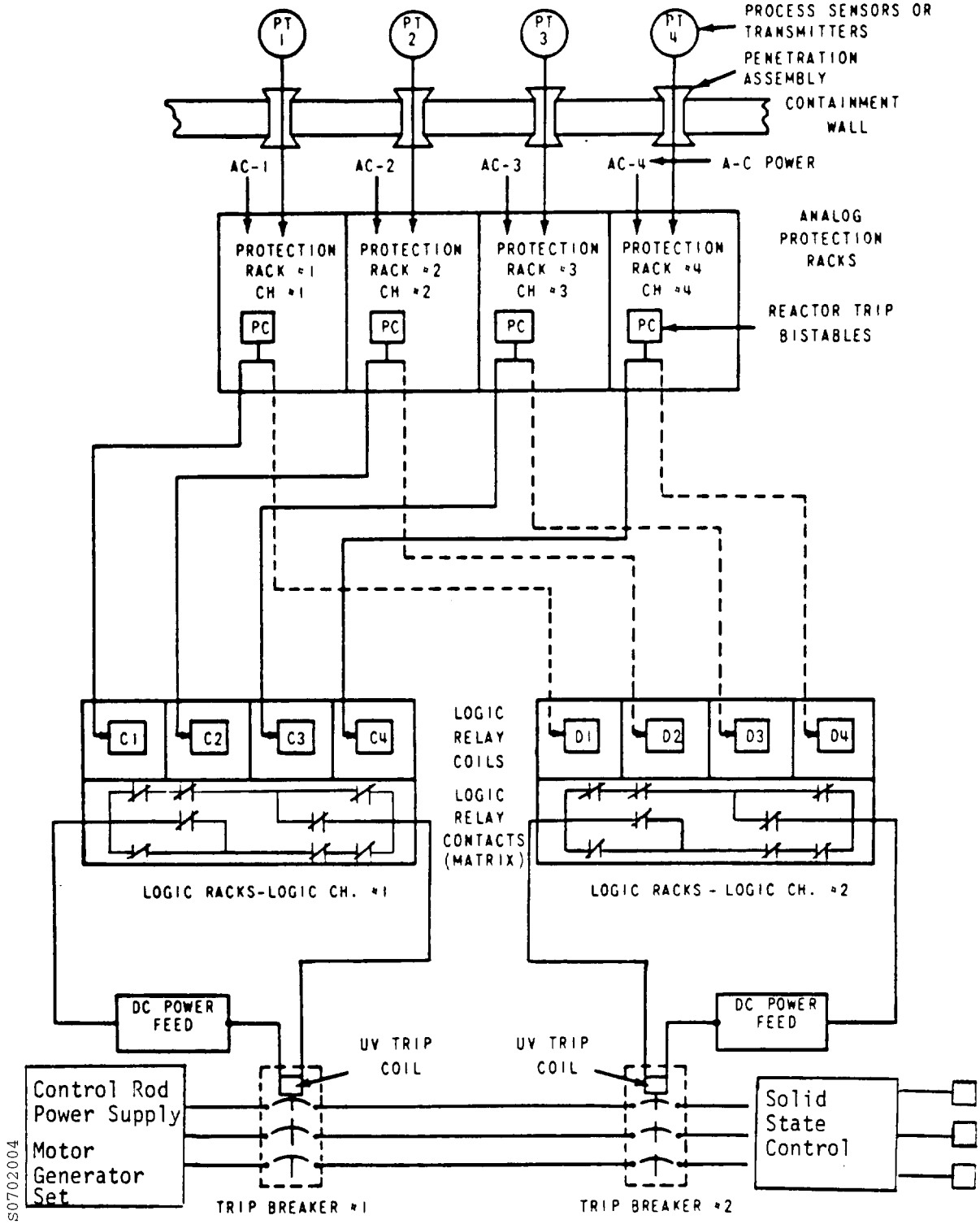
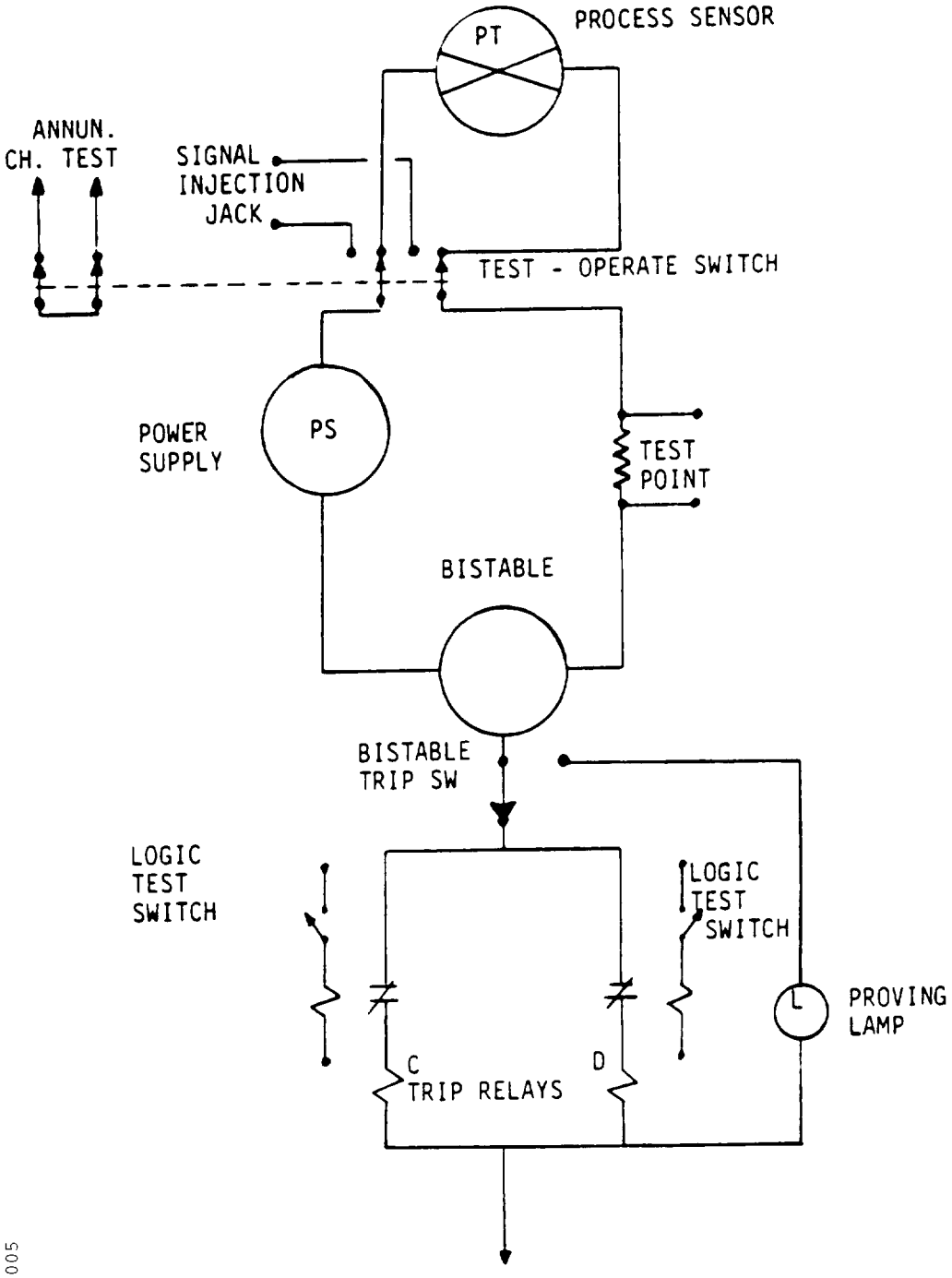


Figure 7.2-5
BASIC ELEMENTS OF AN ANALOG PROTECTION CHANNEL



SEE LEGEND OF ANALOG SYMBOLS TABLE 7.2-2

Figure 7.2-6
TRIP LOGIC CHANNELS

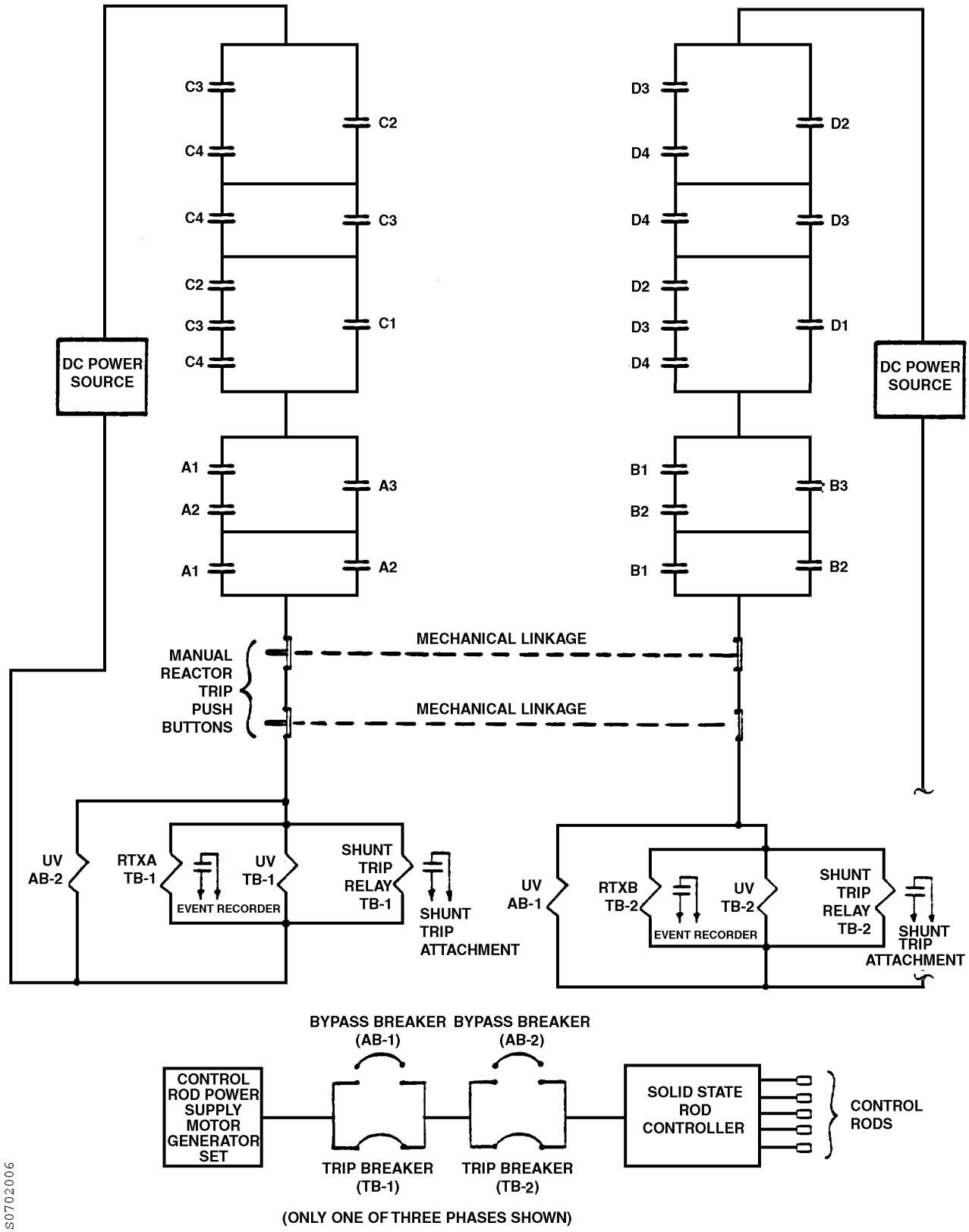
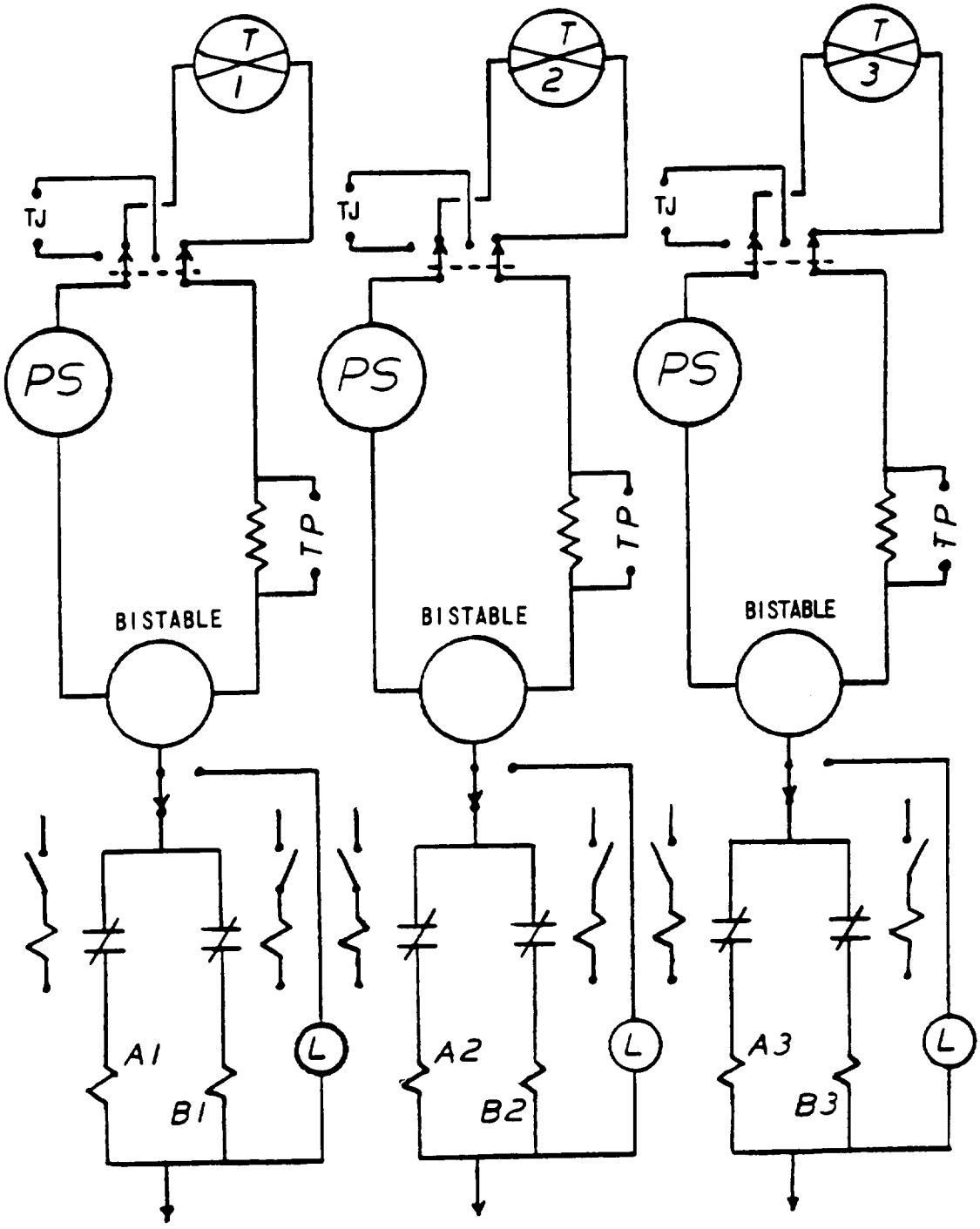


Figure 7.2-7
ANALOG CHANNELS



NOTE - REDUNDANT CHANNELS ARE ISOLATED

SEE LEGEND OF ANALOG SYMBOLS TABLE 7.2-2

S0702007

Figure 7.2-8
LOGIC CHANNEL TEST PANELS

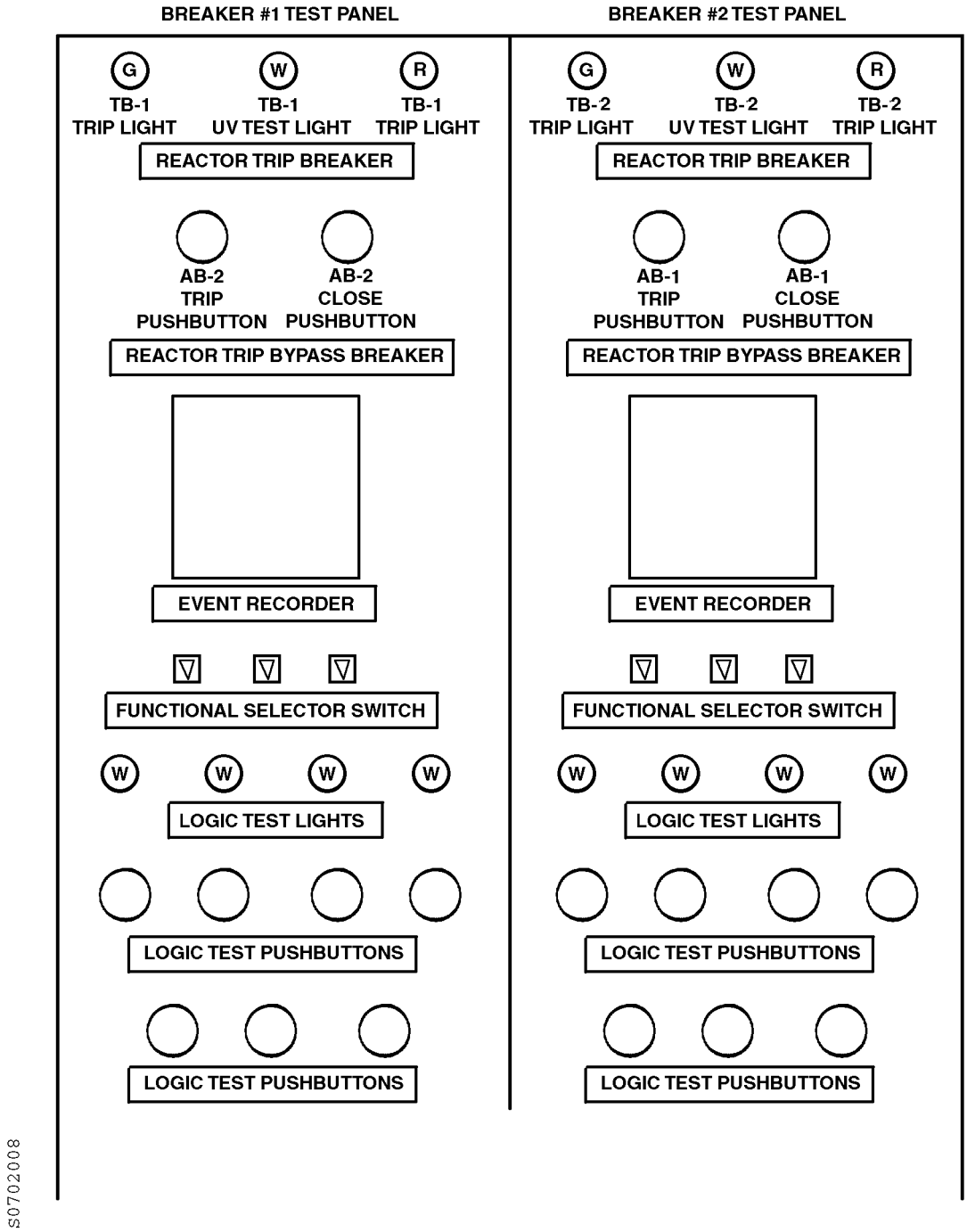
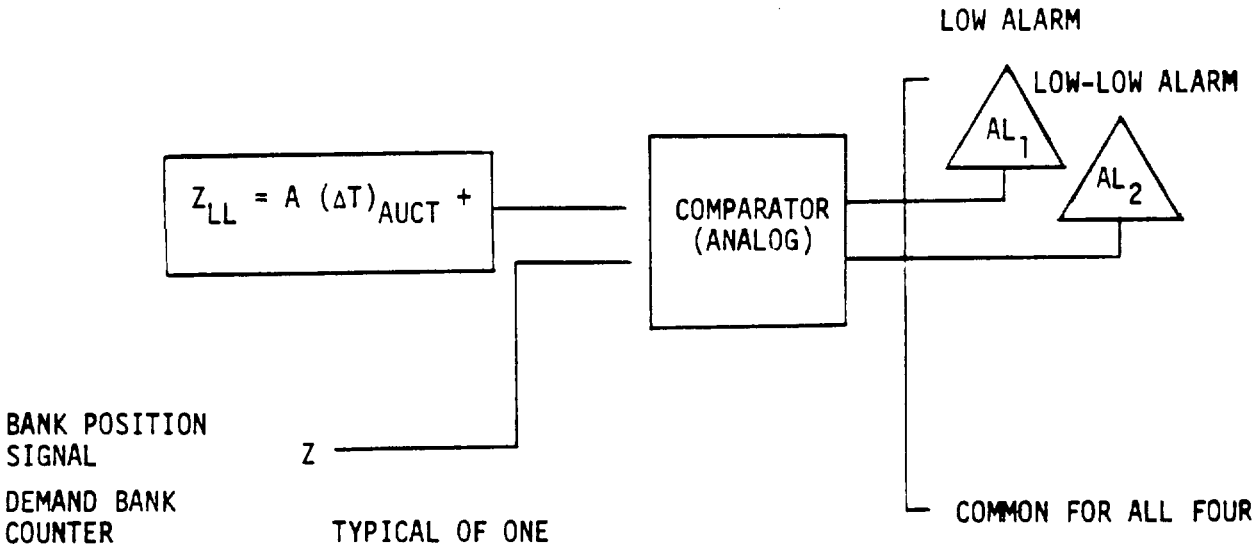


Figure 7.2-9
CONTROL GROUP ROD INSERTION MONITOR



NOTE:

1. ANALOG CIRCUITRY IS USED FOR THE COMPARATOR NETWORK.
2. COMPARATOR WILL ENERGIZE LOW ALARM (AL_1) IF THE DIFFERENCE BETWEEN Z AND Z_{LL} IS LESS THAN D.
3. COMPARATOR WILL ENERGIZE LOW-LOW ALARM (AL_2) IF THE DIFFERENCE BETWEEN Z AND Z_{LL} IS LESS THAN E.
4. D > E.
5. COMPARISON IS DONE FOR ALL CONTROL BANKS.

S0702009

Figure 7.2-10
T_{avg} - ΔT PROTECTION

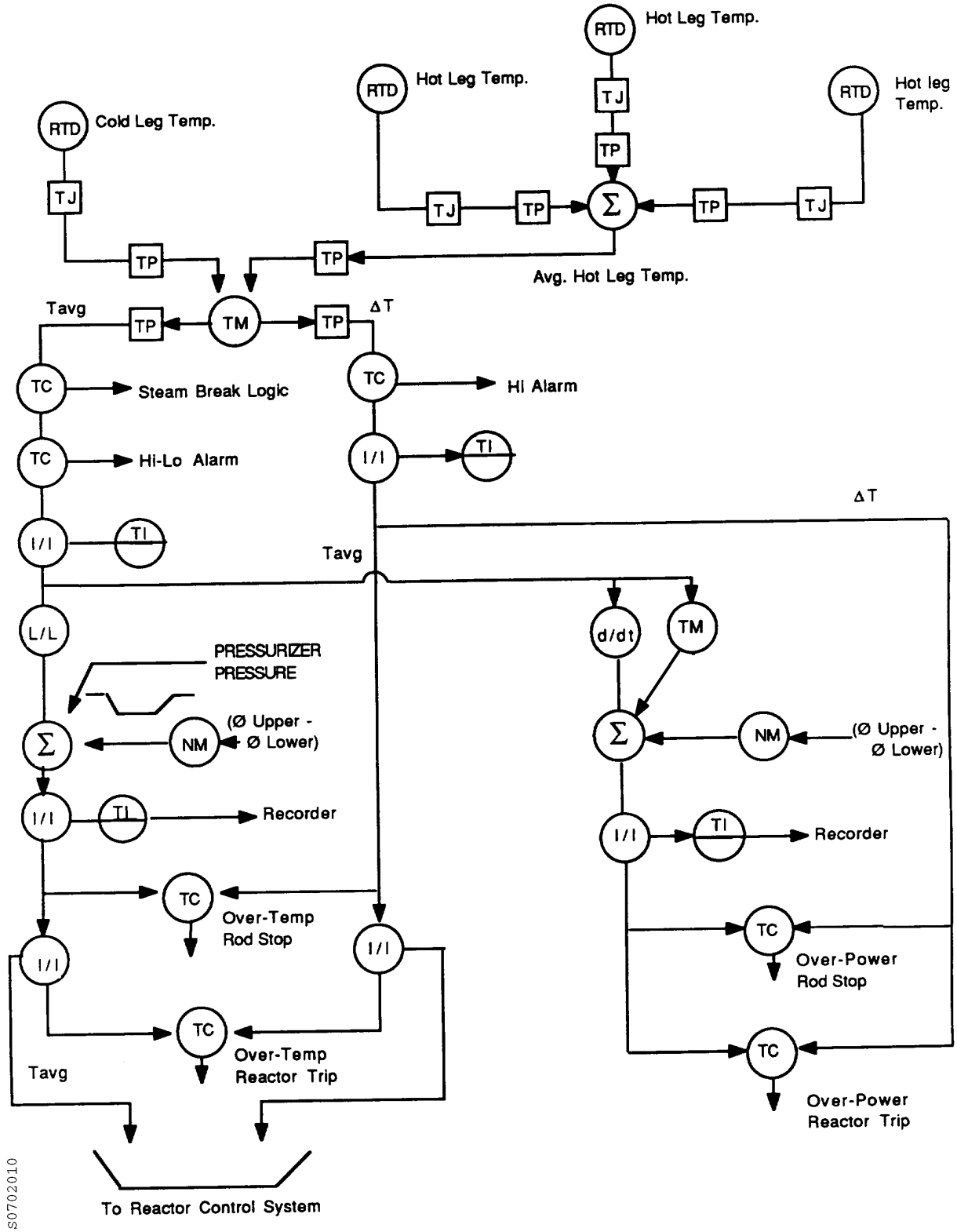


Figure 7.2-11
PRESSURIZER PRESSURE CONTROL AND PROTECTION

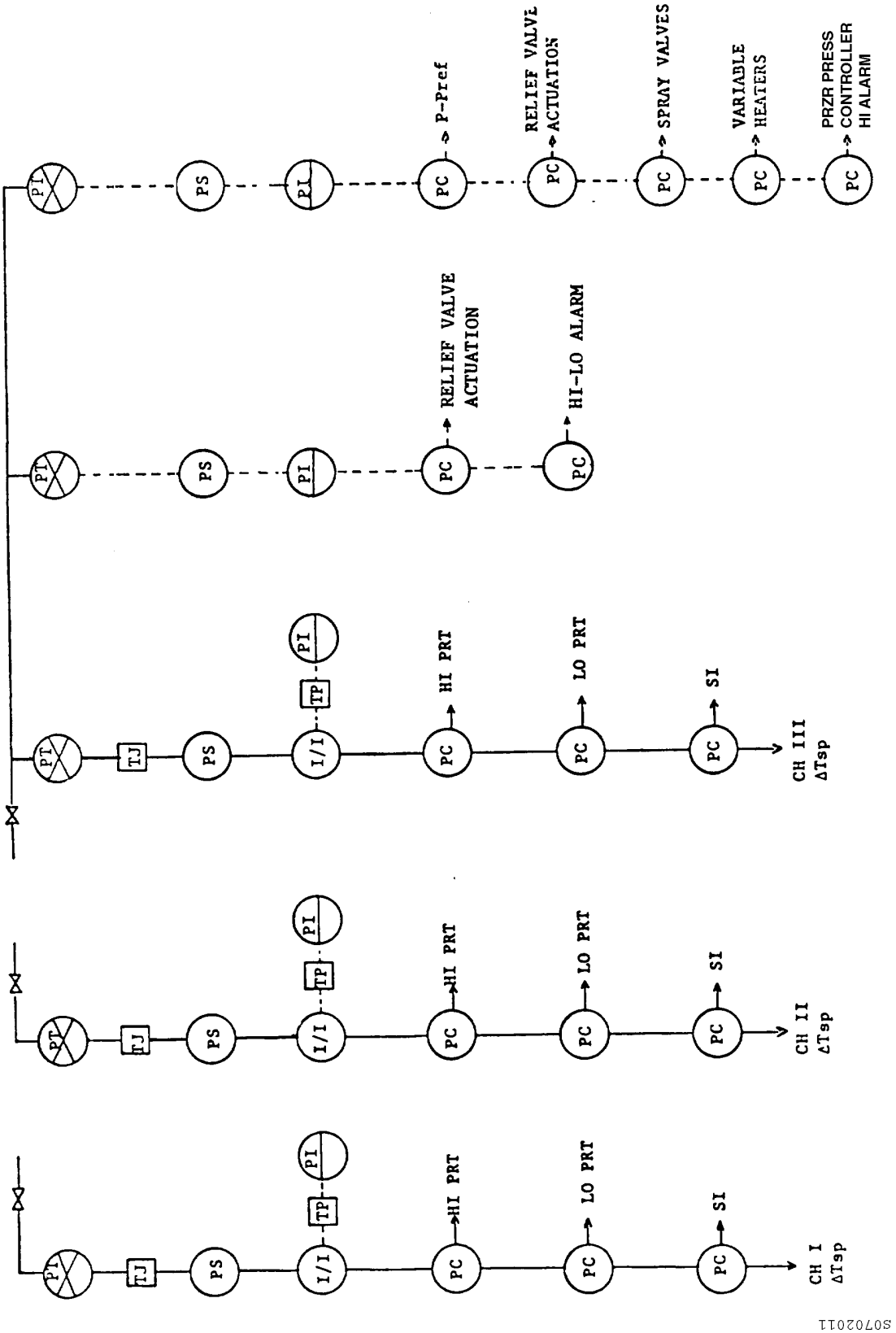
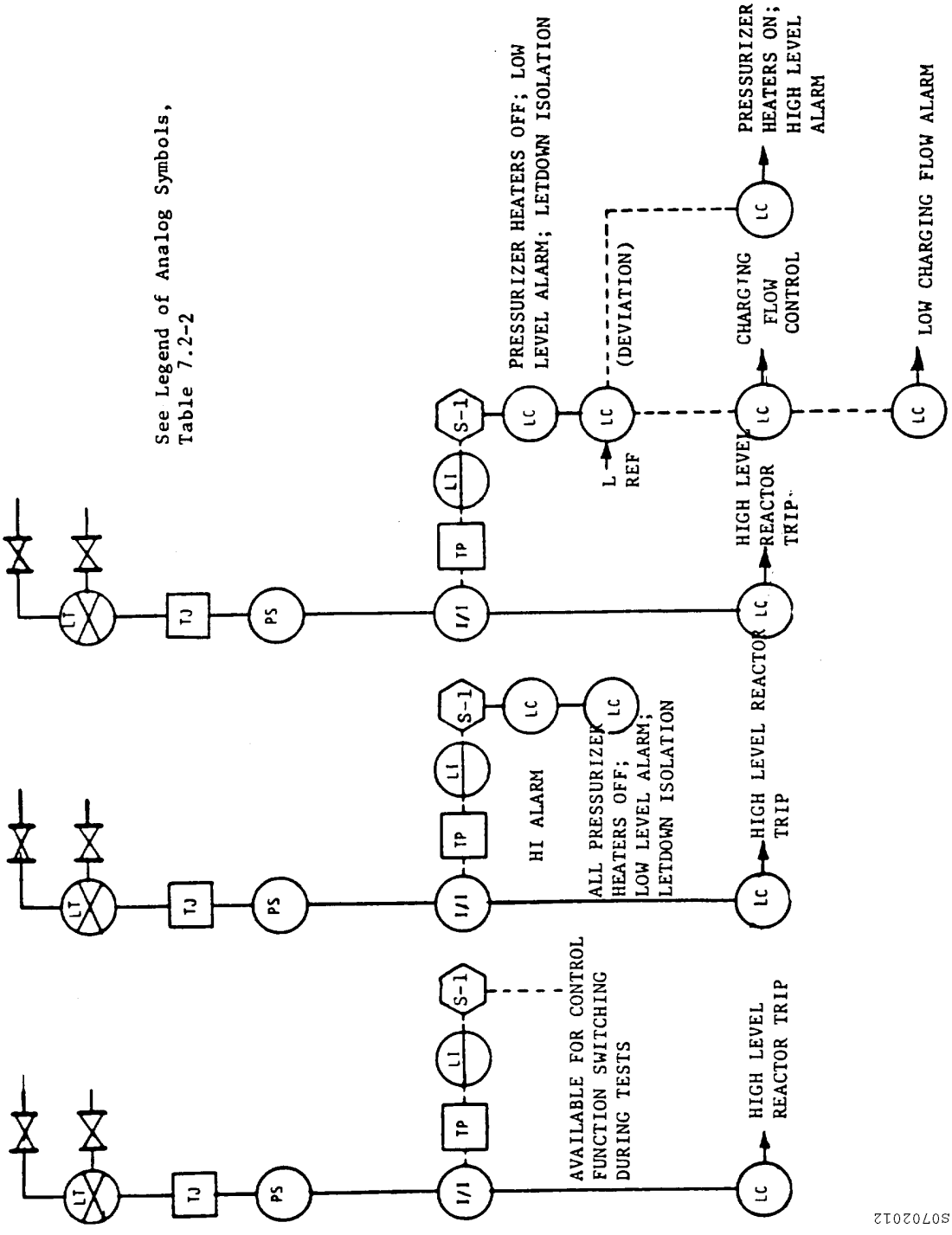


Figure 7.2-12
PRESSURIZER LEVEL CONTROL AND PROTECTION SYSTEM



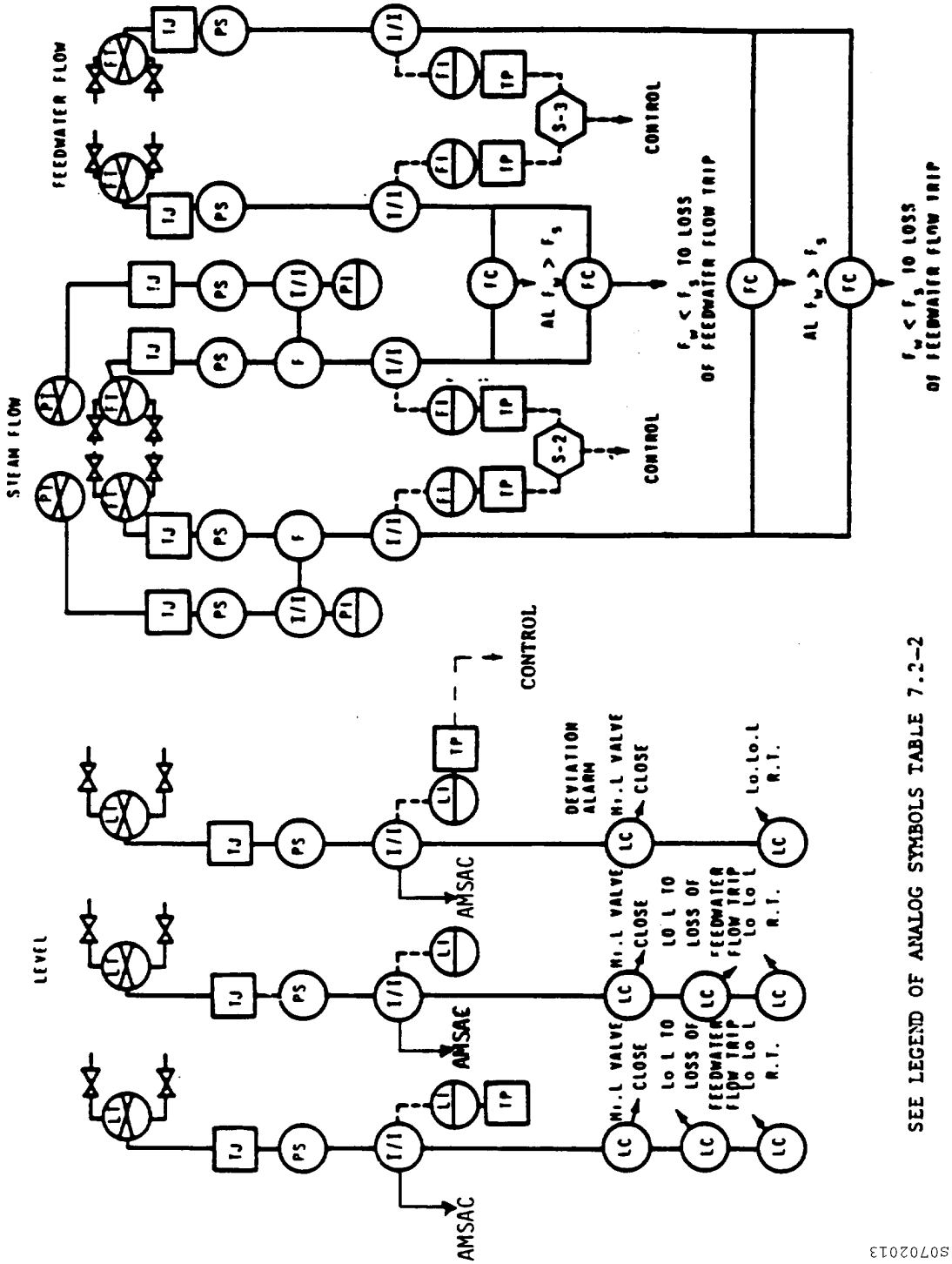


Figure 7.2-13
STEAM GENERATOR LEVEL CONTROL AND PROTECTION SYSTEM

Intentionally Blank

7.3 REACTOR CONTROL SYSTEM

7.3.1 Design Bases

The reactor automatic control system is designed to reduce transients for the designed load perturbations, so that reactor trips will not occur for these load changes.

The functional design of the reactor control and protection systems for the Surry Station is the same as that for H. B. Robinson Unit 2. In translating the functional requirements into control and protection equipment during the detailed design of the plant, there were some minor changes in equipment in order to:

1. Reduce the amount of equipment required to accomplish a specific control or protection function, and therefore reduce equipment maintenance time during plant operation.
2. Modify instrument and control ranges to be consistent with the plant parameters corresponding to the increased power rating of the Surry Station over that of the reference design (H. B. Robinson Unit 2).

Specific functions, however, are accomplished with the same degree of reliability and redundancy as the reference design.

Overall reactivity control is achieved by the combination of chemical shim and control rod 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 moving control rod assemblies.

The function of the reactor control system is to provide automatic control of the control rod assemblies during power operation of the reactor. The system uses input signals including neutron flux, isolated delta T and T_{avg} signals from the reactor protection system, and turbine load. The chemical and volume control system (Section 9.1) supplements the reactor control system by boration and dilution.

There is no provision for a direct continuous visual display of primary coolant boron concentration. When the reactor is critical, the best indication of reactivity status in the core is the position of the control group in relation to power and average coolant temperature.

There is a direct relationship between control rod position and power, and it is this relationship that establishes the calculated lower insertion limit displayed on the rod insertion limit recorder. There are two alarm setpoints to alert the operator to take corrective action in the event a control group approaches or reaches its lower limit.

Any unexpected change in the position of the control group 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, periodic samples are taken for

determination of the coolant boron concentration. The variation in concentration during core life provides a further check on the reactivity status of the reactor, including core depletion.

The reactor control system is designed to enable the reactor to follow load changes automatically when the output is above approximately 15% of nominal power. Control rod positioning may be performed automatically when plant output is above this value, and manually at any time.

The operator is able to select any single bank of rods for manual operation. This is accomplished with a multi-position switch so that he may not select more than one bank. He may also select automatic or manual reactor control; in either case, however, the control banks can be moved only in their normal sequence, with some overlap as one bank reaches its full withdrawal position and the next bank begins to withdraw. Relay interlocks, designed to meet the single-failure criterion, are provided to preclude simultaneous withdrawal of more than one bank of rods except in overlap regions.

The system enables the nuclear unit to accept a step load increase of 10% and a ramp increase of 5% per minute within the load range of 15% to 100% without reactor trip, subject to possible xenon limitations. Similar step and ramp load reductions are possible within the range of 100% to 15% of nominal power.

The control system is capable of restoring coolant average temperature to within the programmed temperature deadband following a scheduled or transient change in load.

The pressurizer water level is programmed to be a function of the average coolant temperature. This is to minimize the requirements on the chemical and volume control and waste disposal systems resulting from coolant density changes during loading and unloading from full power to zero power.

Following a reactor and turbine trip, sensible heat stored in the reactor coolant is removed, without actuating the steam generator safety valves, by means of controlled steam dump to the condenser and by injection of feedwater into the steam generators. Reactor coolant system temperature is reduced to the no-load condition. This no-load coolant temperature is maintained by steam dump to the condensers, which removes residual heat.

7.3.2 System Description

The reactor control system is designed to provide stable system control over the full range of automatic operation throughout core life without requiring operator adjustment of setpoints other than normal calibration.

A simplified block diagram of the reactor control system is shown in Figure 7.3-1. The reactor control system controls the reactor coolant average temperature by regulation of control bank rod position. The system is capable of restoring reactor coolant average temperature to the

programmed value following a change in load. The programmed coolant average temperature increases linearly from zero power to the full-power condition.

The reactor control system will also compensate, to a certain extent, for reactivity changes caused by fuel depletion and/or xenon transients. Long-term compensation for these two effects is periodically made by adjustments of the boron concentration to return the control rod bank to its normal operating range.

The reactor coolant loop average temperatures are determined from hot-leg and cold-leg measurements in each reactor coolant loop. These signals are derived in the reactor protection system and sent to the reactor control system via circuit isolators. The error between the programmed average temperature and the median value of the average measured temperatures from each of the reactor coolant loops constitutes the primary control signal, as shown on Figure 7.3-2. 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 and reducing transient peaks. From these input signals, the rod direction command signals are derived. The rod speed command signal varies over the corresponding range of 3.75 to 45 inches per minute, depending on the magnitude and the rate of change of the input signals. The rod direction command signal is determined by the positive or negative value of the temperature difference signal. The rod speed and rod direction command signals are fed to the rod control system.

7.3.2.1 **Control Rod Assembly Arrangements**

There are 48 control rod assemblies (Section 3.3). The rods are divided among control and shutdown banks. There is a total of 16 control rod assemblies in the two shutdown banks. There are four control banks containing eight control rod assemblies each. The only control rod assemblies that can be manipulated under automatic control are the control rod assemblies in the control banks. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All control rod assemblies in a group are electrically paralleled to move simultaneously. There is individual position indication for each assembly.

7.3.2.2 **Rod Control**

7.3.2.2.1 Control Group Rod Control

The automatic rod control system maintains the average reactor coolant temperature by adjusting the positions of the control rod assemblies.

The rod control system is capable of restoring programmed average temperature following a change in load. The reactor coolant average temperature increases linearly from zero power to full power.

The control system will also initially compensate for reactivity changes caused by fuel depletion and/or xenon transients. Final compensation for these two effects is made by adjusting

the boron concentration. The control system then readjusts the control group in response to changes in coolant average temperature resulting from changes in boron concentration.

The control rod assemblies are divided into two shutdown and four control banks, and each bank is divided into two groups, to follow load changes over the full range of power operation. Each group in a bank is driven by the same variable-speed rod drive control unit, which moves the groups sequentially one step at a time. The sequence of motion is reversible; that is, a withdrawal sequence is the reverse of the insertion sequence. The variable-speed sequential rod control affords the ability to insert a small amount of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband.

Manual control is provided to move a control bank in or out at a preselected fixed speed.

When the reactor power reaches approximately 15%, the operator may select the AUTOMATIC position, where the IN-HOLD-OUT lever is out of service and rod motion is controlled by the reactor control and protection systems. An interlock (P-2, Table 7.2-3) limits automatic control to reactor power levels above 15%. In the AUTOMATIC position, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

Programming is set so that, as the first control bank out reaches a preset position near the top of the core, the second bank begins to move out simultaneously with the first bank. This staggered withdrawal sequence continues until the unit reaches the desired power level. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank out is the first control bank in.

With the simplicity of the rod program, the minimal amount of operator selection, and two separate direct position indications available to the operator, there is very little possibility that rearrangement of the control rod sequencing could occur.

7.3.2.2.2 Shutdown Banks Control

The shutdown banks of control rods, together with the control banks, are capable of shutting the reactor down. The shutdown banks are used in conjunction with the control banks to provide shutdown margin of at least 1.77% following reactor trip, with the most reactive control rod in the fully withdrawn position for all normal operating conditions. The shutdown groups are manually controlled during normal operation and are moved at a constant speed. Any reactor trip signal causes them to fall into the core. They are fully withdrawn during power operation and are withdrawn first during start-up. Criticality is always approached by withdrawing the control groups after withdrawal of the shutdown groups.

7.3.2.2.3 Interlocks

The rod control banks used for automatic control are interlocked with measurements of turbine first-stage pressure to prevent automatic control rod withdrawal below 15% of nominal

power (P-2, Table 7.2-3). The manual and automatic controls are further interlocked with measurements of nuclear flux and delta T to prevent approach to an overpower condition (P-1).

7.3.2.3 **Rod Drive Performance**

7.3.2.3.1 Control Rod Assemblies

The control banks are driven by a sequencing, variable-speed rod drive programmer. In a control bank of assemblies, control groups (each containing a small number of assemblies) are moved sequentially in a cycle so that all groups are maintained within one step of each other. The sequence of motion is reversible; that is, the withdrawal sequence is the reverse of the insertion sequence. The sequencing speed is proportional to the control signal from the reactor control system. This provides control group speed control proportional to the demand signal from the control system. A rod drive mechanism control center is provided to receive sequenced signals from the programmer and to actuate switches in series with the coils of the rod drive mechanisms. Two reactor trip breakers are placed in series with the supply for the coils. To permit on-line testing, a bypass breaker is provided across each of the two trip breakers.

The power for the entire complement of control and shutdown rod drive mechanisms is provided by a system composed of two ac motor-generator sets. The sets consist of squirrel cage induction motors driving synchronous alternators.

The total capacity of the system, including the overload capability of each motor-generator set, is such that a single set out of service does not cause limitations in rod motion during normal plant operation. In order to minimize reactor trip as a result of a unit malfunction, the power system is normally operated with both units in service.

Figure 7.3-3 shows the power supply to the rod control equipment and control rod drive mechanisms. The power supply connections from the reactor trip breakers to the rod control equipment are in protective enclosures and are sized to handle 1000A. The minimum current required to hold the control rods is approximately 150A. A failure in this power supply bus downstream of the trip breakers that results in an open circuit or short circuit would be detected by the dropping of the rods. There are no other power sources in the reactor trip breaker switchgear or the rod control equipment with sufficient capacity to hold a control rod assembly in position in the event that it became crossed with the trip breaker output bus and the trip breakers were tripped.

Flywheels on the motor-generator sets and high-speed regulators on each unit enable the rods to ride through a complete loss of ac power for one second during electrical transients.

7.3.2.3.2 Rod Position Indication

Two separate systems are provided to sense and display control rod position, as described below:

1. Analog system - An analog signal is generated by measuring the position of each control rod assembly. This is accomplished by means of a linear position transmitter.

   An electrical coil stack is placed above the stepping mechanisms of the control rod magnetic jacks external to the pressure housing.

   When the associated control rod is at the bottom of the core, the magnetic coupling between a primary and secondary is small, and there is a small voltage induced in the secondary. As the control rod is raised by the magnetic jacks, the relatively high permeability of the lift rod causes an increase in magnetic coupling. Thus, an analog signal proportional to rod position is obtained.

   Direct, continuous readout of every control rod assembly position is presented to the operator by redundant rod position flat panel displays.

   The individual analog rod position signals are fed to the plant computer system for monitoring and readout. A deviation monitor alarm is actuated if any rod differs in its measured position from its group step demand position by a preset value. The alarm will reflash in the event of subsequent rod deviations which exceed the preset value. When reactor power is below 50%, the preset deviation values are increased. However, the increased limits may not be utilized for more than one hour in the previous 24 hours prior to increasing power above 50%. When reactor power is less than 50%, the amount of time in the past 24 hours that the increased deviation limits have been utilized will be tracked by the computer. The deviation monitor alarm also indicates bank sequence errors and when any shutdown bank has inappropriately left its fully withdrawn position.

   A rod bottom condition for each rod is indicated on the redundant rod position flat panel displays.

2. Digital system - The digital system counts pulses generated in the rod drive control system programmer. One counter is associated with each group of control rod assemblies. Readout of the digital system is in the form of electromechanical add-subtract counters reading the number of steps of demanded rod position with one display for each group. These readouts are mounted on the control panel.

The digital and analog systems are separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the digital and analog 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.

7.3.2.4 **Primary System Pressure Control**

Reactor coolant system pressure is controlled by the use of the pressurizer. Inside the pressurizer water and steam are maintained at saturation temperature and pressure by electrical heaters and water spray. The electrical immersion heaters are located near the bottom of the pressurizer. The pressurizer has five heater groups comprised of one proportional heater group and four (backup) heater groups.

The pressurizer pressure control is normally operated with the proportional heater group in automatic. Each group of the backup heaters can be operated in standby or manually energized. When all backup heater groups are in standby, the proportional heater group is used to control small pressure variations due to heat losses, including losses due to a small continuous spray. The spray nozzle is located in the top of the pressurizer. A small continuous spray flow is maintained to reduce thermal stresses and maintain uniform water chemistry. Any backup heater groups that are in standby will automatically energize when the pressurizer pressure controller signal drops below a given value, or when pressurizer level rises above a given value.

Operation with one or more backup heater groups manually energized will result in an increase in pressure controller signal. Additional spray is automatically initiated when the pressure controller signal is above a given setpoint. The spray rate increases proportionally with increasing pressure, until it reaches a maximum value. Steam condensed by the spray reduces the pressurizer pressure. Adequate spray flow exists to maintain pressure when all of the backup heaters are energized. A continuous spray is maintained automatically, in equilibrium with the heat output of the energized backup heaters. Operation in this configuration allows stable pressure control. It reduces thermal stresses and thermal shock, by avoiding thermal stratification in the surge line. It also allows a rapid equalization of boron concentration between the pressurizer and the RCS.

Two power-operated relief valves limit system pressure for large load reduction transients. Spring-loaded safety valves limit system pressure following a complete loss of load without direct reactor trip or turbine bypass.

7.3.2.5 **Pressurizer Level Control**

The water inventory in the reactor coolant system is maintained by the chemical and volume control system. During normal unit operation, the pressurizer level is controlled by the charging-flow controller, which controls the charging-flow control valve to produce the flow demanded by the pressurizer-level controller. The pressurizer water level is programmed as a function of coolant average temperature. The pressurizer water level decreases as the load is reduced from full load. This is the 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 permit manual control of pressurizer level during start-up and shutdown operations, the charging-flow control valve can be manually regulated from the control room.

7.3.2.6 **Secondary System Control**

A review of the effects of the power uprate to a core power of 2546 MWt was conducted and the control systems and instrumentation were found to be adequate. The secondary system includes the steam generators and the condensate and feedwater systems.

The main steam, condensate, and feedwater systems are shown on Reference Drawings 1, 2, and 3.

All equipment is designed with highly reliable components. Maximum use is made of solid-state components in the electronic instruments; spring-loaded diaphragm control valves are employed to fail safe on loss of air or power.

All instrumentation and controls, where possible, are installed outside of the containment structure and in locations accessible for inspection and maintenance. Automatic control instruments in selected systems are provided with backup manual control through transfer switches. Alarms are provided to warn of abnormal conditions.

7.3.2.6.1 Turbine Steam Dump

The purpose of the steam dump valve system is to reduce reactor coolant system transients following a substantial turbine load reduction by dumping main steam directly to the condenser, thereby maintaining an artificial load on the steam generators. The control rod system can then reduce the reactor power to a new equilibrium value without causing overtemperature and/or overpressure conditions.

Following a reactor and turbine trip, sensible heat stored in the reactor coolant is removed without actuating the steam generator safety valves by means of a controlled steam dump to the condenser and by injection of feedwater to the steam generators. Reactor coolant system temperature is reduced to the no-load condition. This no-load coolant temperature is maintained by steam dump to the condensers, which removes residual heat.

The steam dump control system is designed to relieve steam from the steam generators to the condenser, to reduce the sensible heat in the primary system in the event of complete load rejection down to auxiliary load, and to maintain the steam generator pressure during hot standby conditions.

The turbine steam dump capacity is 40% of full-load steam flow at full-load steam pressure, all of which flows to the main condenser via the steam dump lines.

When a load rejection occurs, if the change in the required program temperature of the reactor coolant system differs from the actual average temperature by more than a predetermined

amount, a signal will actuate that portion of the steam dump system needed to reach the new program temperature.

The required number of steam dump valves choke or modulate full open, depending upon the magnitude of the temperature error signal upon receiving a loss-of-load signal. The dump valves can be modulated after they are full open by the reactor coolant average temperature signal.

The turbine steam dump flow reduces proportionally as the control rods act to reduce the average reactor coolant temperature. The artificial load is therefore removed as the reactor coolant average temperature is restored to its programmed equilibrium value.

7.3.2.6.2 Steam Generator Water Level Control

Each steam generator is equipped with a three-element feedwater controller (Figure 7.2-13) that maintains a programmed water level as a function of load on the secondary side of the steam generator. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, and the steam flow signal, which is compensated by steam pressure signal. The steam generators are operated in parallel, both on the feedwater and on the steam side.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor coolant following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature or when the respective steam generator level rises to a given value.

Following a turbine trip, the main feedwater valves are closed on low T_{avg}. This provides an optimum heat sink. Subsequently, the operator remotely controls the feedwater regulating bypass valves to maintain the steam generator water level. Manual override of the feedwater control system is available at all times.

7.3.2.6.3 Turbine Control

The turbine control system is designed to regulate the steam flow to the turbine as a function of load or speed.

7.3.3 Design Evaluation

7.3.3.1 Unit Stability

The rod control system is designed to limit the amplitude and the frequency of continuous oscillation of reactor coolant average temperature about the control system setpoint within acceptable values. Continuous oscillation can be induced by the introduction of a feedback control loop with an effective loop gain that is either too large or too small with respect to the process transient response, i.e., instability induced by the control system itself. Because stability is more difficult to maintain at low power under automatic control, no provision is made to provide automatic control below 15% of full power.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life.

7.3.3.2 Step Load Changes Without Steam Dump

A typical power control requirement is to restore equilibrium conditions, without a trip, following a ±10% step change in load demand, over the 15% to 100% power range for automatic control. The design must necessarily be based on conservative conditions, and a greater transient capability is expected for actual operating conditions. A load demand greater than full power plus a small tolerance band is prohibited by the turbine control load limit devices.

The function of the control system is to minimize the reactor average coolant temperature deviation during the transient within a given value, and to restore average temperature to the programmed setpoint within a given time. Excessive pressurizer pressure variations are prevented by using spray and heaters in the pressurizer.

The margin between the overtemperature delta T setpoint and the measured delta T is of primary concern for step load changes. This margin is influenced by nuclear flux, pressurizer pressure, average reactor coolant temperature, and temperature rise across the core.

7.3.3.3 Loading and Unloading

Ramp loading and unloading of 5% per minute can be accepted over the 15% to 100% power range under automatic control without tripping the unit. The function of the control system is to maintain the reactor coolant average temperature and pressure as functions of turbine-generator load. The minimum control rod speed provides a sufficient reactivity insertion rate to compensate for the reactivity changes resulting from the moderator and fuel temperature changes.

The coolant average temperature increases during loading and causes a continuous insurge 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 heaters limit the resulting system pressure decrease. The pressurizer level is programmed so that the water level is above the setpoint at which the heaters cut out during the loading and unloading transients. The primary concern during loading is to limit the overshoot in average coolant temperature and to provide sufficient margin in the overtemperature delta T setpoint.

The automatic load controls are designed to safely adjust the unit generation to match load requirements within the limits of the unit capability and warranted power.

7.3.3.4 Loss of Load With Steam Dump

The reactor control system is designed to accept 50% load rejection without trip. No reactor trip or turbine trip should be actuated for load losses in this range. The automatic turbine steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of this

transient imposed upon the reactor coolant system. The reactor power is reduced at a rate consistent with the capability of the rod control system. Reduction of the reactor power is automatic down to 15% of full power. The steam dump flow reduction occurs as fast as the control rod assemblies are capable of inserting negative reactivity.

The pressurizer 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 conditions.

7.3.3.5 **Turbine-Generator Trip With Reactor Trip**

Whenever the turbine-generator unit trips at an operating level above 10% power, 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 saturation temperature corresponding to the steam generator pressure at 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 steam 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 average coolant temperature signal, whose setpoint values are reset upon trip to the no-load value. Actuation of the steam dump must be rapid, to prevent actuation of the steam generator safety valves. With the steam dump valves 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 that is dumped.

Following the turbine trip, the steam voids in the steam generator will collapse, and the fully opened feedwater valves will provide sufficient feedwater flow to restore water level in the downcomer. The feedwater flow is cut off when the average coolant temperature decreases below a given temperature value 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 level while ensuring that the reactor coolant temperature is at the desired value. 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 the same steam dump valves to the condensers that are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and level fall rapidly during the transient because of coolant contraction. The pressurizer water level is programmed to match as near as possible the level changes as a result of coolant temperature changes and so that the water level is above the setpoint

at which the heaters are turned off on low pressurizer level. If heaters become uncovered following the trip, 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.

7.3 REFERENCE DRAWINGS

The list of Station Drawings below is provided for information only. The referenced drawings are not part of the UFSAR. This is not intended to be a complete listing of all Station Drawings referenced from this section of the UFSAR. The contents of Station Drawings are controlled by station procedure.

	Drawing Number	Description
1.	11448-FM-064A	Flow/Valve Operating Numbers Diagram: Main Steam System, Unit 1
	11548-FM-064A	Flow/Valve Operating Numbers Diagram: Main Steam System, Unit 2
2.	11448-FM-067A	Flow/Valve Operating Numbers Diagram: Condensate System, Unit 1
	11548-FM-067A	Flow/Valve Operating Numbers Diagram: Condensate System, Unit 2
3.	11448-FM-068A	Flow/Valve Operating Numbers Diagram: Feedwater System, Unit 1
	11548-FM-068A	Flow/Valve Operating Numbers Diagram: Feedwater System, Unit 2

Figure 7.3-1
SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL SYSTEM

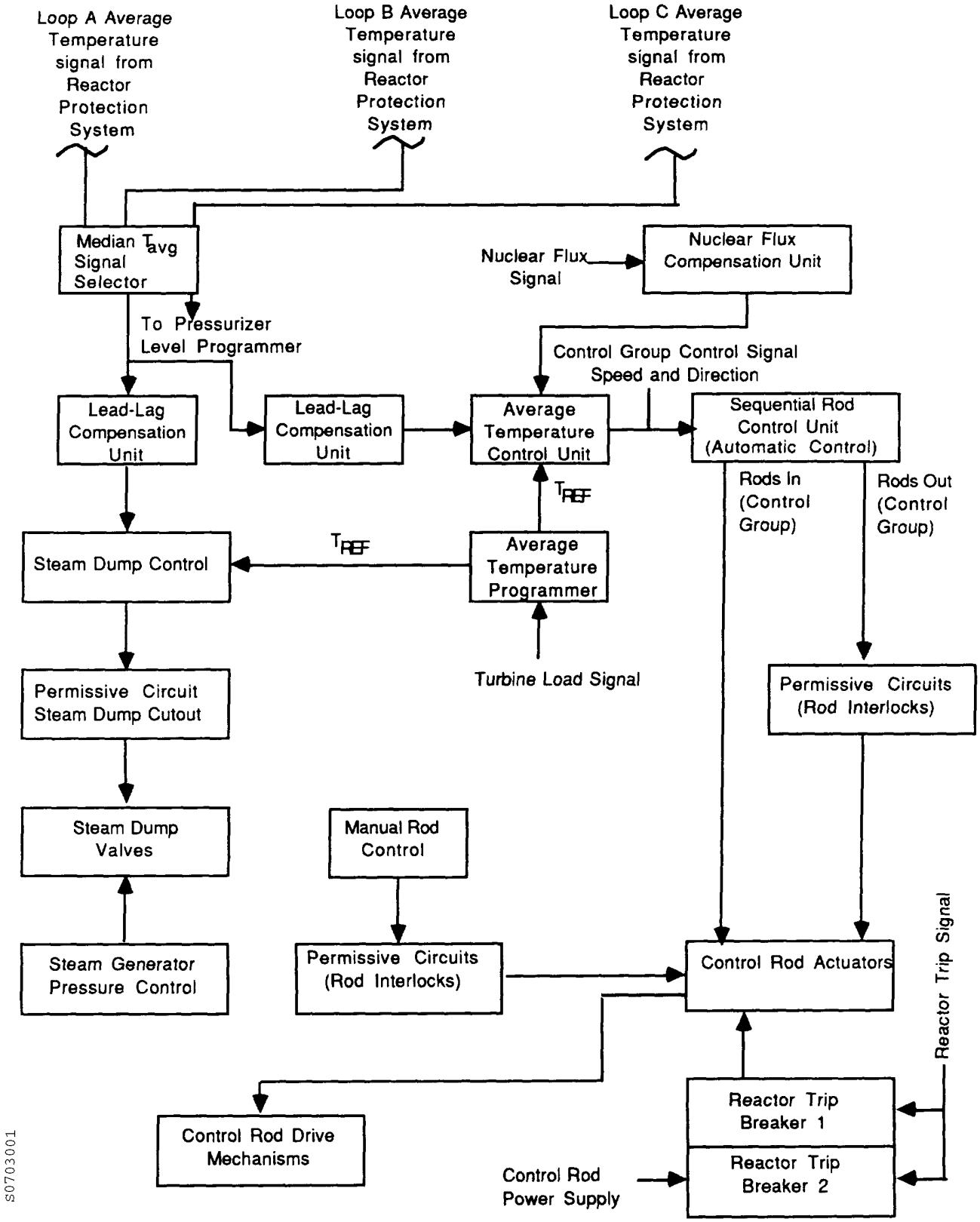
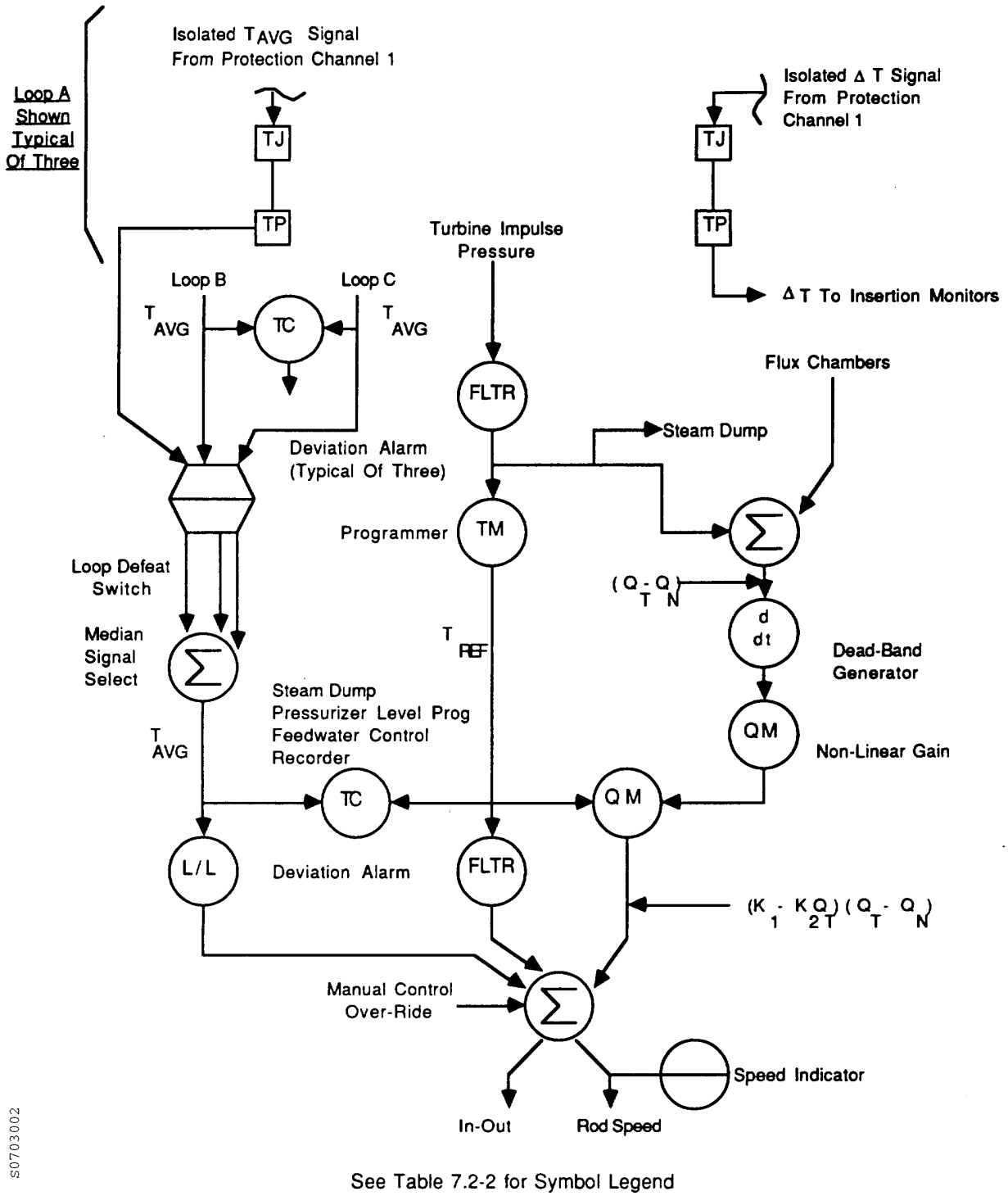
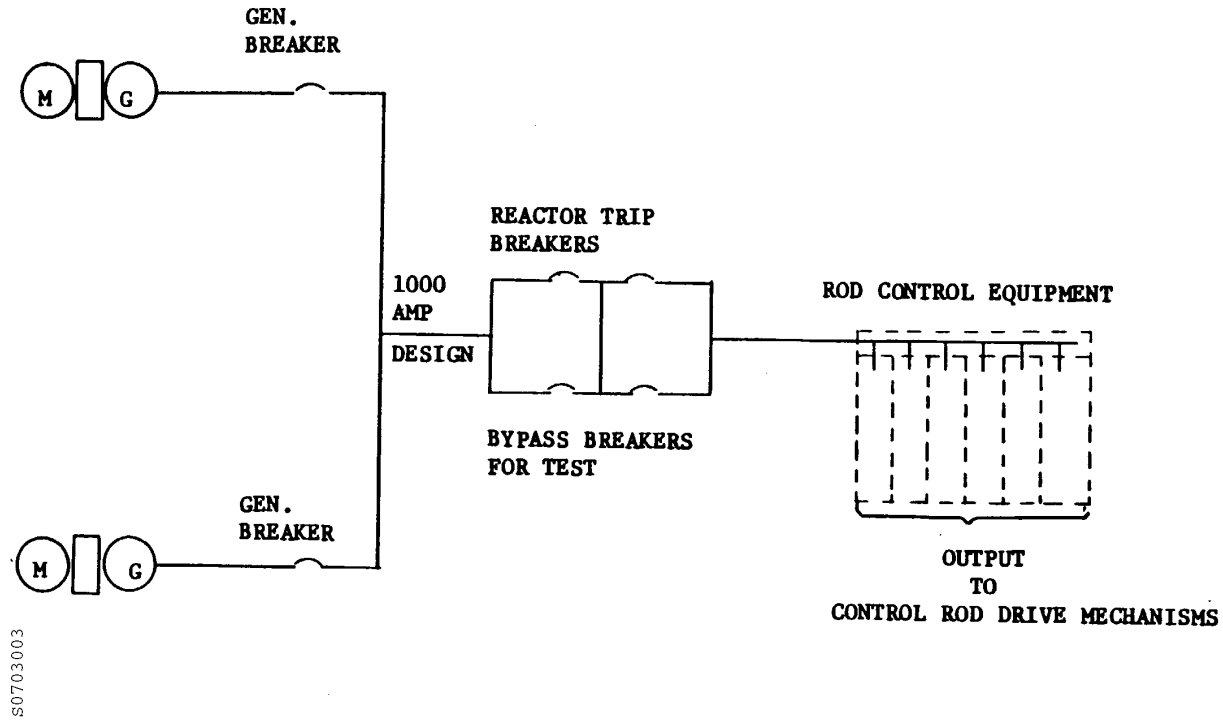


Figure 7.3-2
T_{avg} CONTROL SYSTEM



See Table 7.2-2 for Symbol Legend

Figure 7.3-3
POWER SUPPLY TO CONTROL ROD EQUIPMENT AND CONTROL ROD DRIVE MECHANISMS



Intentionally Blank

7.4 NUCLEAR INSTRUMENTATION SYSTEM

7.4.1 Design Bases

7.4.1.1 Fission Process Monitors and Controls

The Nuclear Instrumentation System is used primarily for reactor protection. It permits monitoring of neutron flux and generates appropriate trip and alarm functions for various phases of reactor operating and shutdown conditions. It also provides a secondary control function, and indicates reactor status during start-up and power operation. Ex-core neutron flux detectors were added to meet R.G. 1.97 and Appendix R requirements. These are discussed in Section 7.11. The nuclear instrumentation system uses information from the three separate types of instrumentation channels to provide three discrete protection levels. Each range of instrumentation (source, intermediate, and power) provides the necessary overpower reactor trip protection required during operation in that range. The overlap of instrument ranges provides reliable continuous protection from source to the intermediate and low power ranges. As the reactor power increases, the overpower protection level is increased (administratively) after satisfactory higher-range instrumentation operation is obtained. Automatic reset to more restrictive trip protection is provided when reducing power.

Several types of neutron detectors, with appropriate solid-state electronic circuitry, are used to monitor the leakage neutron flux from a completely shut down condition to 120% of full power. The power range channels are capable of recording overpower excursions up to 200% of full power.

The neutron flux covers a wide range between these extremes. Therefore, monitoring with several ranges of instrumentation is necessary. The lowest range (source range) covers six decades of leakage neutron flux.

The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This is generally greater than one count per second. The next range (intermediate range) covers approximately eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers slightly more than two decades of the total instrumentation range. This is a linear range that overlaps with the higher portion of the intermediate range (the intermediate range monitors go off-scale at any point greater than 70% of rated power based on the core loading pattern). The overlap for all detector ranges is shown in Figure 7.4-1 in terms of leakage neutron flux. Start-up-rate indication for the source and intermediate range channels is provided at the control console and on the nuclear instrumentation panel.

The system described above provides control room indication and recording of reactor neutron flux during core loading, shutdown, start-up, and power operation, as well as during subsequent refueling. Reactor trip and rod-stop control and alarm signals are provided by this

system for safe plant operation. Control and permissive signals are transmitted to the reactor control and protection system for automatic plant control. Equipment failures and test status information are annunciated in the control room.

7.4.2 System Description

The nuclear instrumentation system (Figure 7.4-2) consists of eight independent channels: two of these are the source range, two are the intermediate range, and four are the power range channels. In addition, there are three auxiliary channels: the visual-audio count rate channel, the comparator channel, and the start-up-rate channel. The various detectors associated with the eight primary channels are shown in relative position with respect to the core configuration on Figure 7.4-3.

7.4.2.1 Protection Philosophy

Nuclear unit protection assurance, is obtained from the three ranges of ex-core nuclear instrumentation. Separation of redundant protective channels is maintained from the neutron sensor with its associated cables to the signal conditioning equipment in the control room with its associated output wiring, indicating or recording devices, and protective devices. Where redundant protective channels are combined to provide non-protective functions, the required signals are derived through isolation amplifiers. These devices are designed so that open or short-circuit conditions, as well as the application of 120V ac or 140V dc to the isolated side of the circuit will have no effect on the input or protective side of the circuit. As such, failures on the non-protective side of the system will not affect the individual protection channels. Redundant channels are powered from independent power sources, each channel being provided with the necessary power supplies for its detectors, signal conditioning equipment, trip bi-stables, and associated trip relays. The nuclear instrumentation channels are mounted in four separate racks to provide the necessary physical separation between redundant channels.

The overpower protection provided by the ex-core nuclear instrumentation consists of three discrete levels. Continuation of start-up 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.

A one-out-of-two intermediate-range permissive signal (P-6, Table 7.2-3) is required prior to source range level trip blocking 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 are provisions for administratively reactivating the source range level trip and detector high voltage if required. Source range level trip block and high-voltage cutoff are automatically maintained by the same power range permissive (P-10), which permits blocking of the intermediate range and power range (low range) flux level trips.

The intermediate range level trip and power range (low range) level trip can only be blocked after satisfactory operation and permissive information are obtained from two out of four power

range channels. Individual blocking switches are provided so that the power range (low 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 of more restrictive trip protection.

Blocking of any reactor trip function is indicated by the control board permissive status lights. Channels that provide reactor unit protection through one-out-of-two or one-out-of-four logic matrices are equipped with positive detent-type trip-bypass switches to enable channel testing. The trip-bypass condition for individual channels is indicated at the control board and at the nuclear instrumentation racks. The reactor unit protection afforded by the highest-setpoint, power range trip is never blocked or bypassed.

7.4.2.2 **Source Range Instrumentation**

Two independent source range channels are provided. Each receives pulse-type signals from a proportional counter. The preamplified detector signal is received by the source range instrumentation conditioning equipment located in the control room racks. The detector signal, which is a random count rate proportional to leakage neutron flux, is conditioned for conversion to an analog signal proportional to the logarithm of the neutron flux count rate.

The isolated analog signals from each channel are sent to various recording and indicating devices to provide the operator with necessary start-up information. Bi-stable units also located in the racks are used to generate alarms and reactor trip signals. Trip signals from the bi-stables are transmitted to relays in the protection relay racks, where the necessary logic involved in generating reactor trip signals is performed.

An isolated count-rate signal derived from either channel is connected to a scaler-timer. This same signal also feeds the audio count-rate channel, which provides an audible count-rate signal, proportional to the neutron flux. Speakers are provided both in the containment and in the control room. Start-up-rate indication is also provided for each source range channel. These signals are generated from the isolation amplifier output, since there is no protection function involved.

7.4.2.3 **Intermediate Range Instrumentation**

Two independent, compensated ionization chambers provide extended flux coverage from the upper end of the source range to any point greater than 70% of rated power based on core loading patterns. The equipment for each channel, including the high-voltage and compensating voltage power supplies, are located in separate drawers. To maintain separation between these redundant channels, the drawers are mounted in separate racks. The signal conditioning equipment furnishes an analog output voltage proportional to the logarithm of the neutron flux spectrum. Each channel covers approximately eight decades of leakage flux. Isolation amplifiers (for start-up-rate circuits, remote recording, remote indication, etc.) and bi-stable amplifiers (for permissives, rod-stop, and reactor trip) use this analog voltage to indicate plant status and provide

the necessary plant protection functions. All relays associated with plant control or protection are located in the logic or auxiliary relay racks.

7.4.2.4 **Power Range Instrumentation**

Four dual-section, uncompensated ionization chambers are used for power range flux detection. Each chamber provides two current signal outputs (one from each section) to signal conditioning equipment in the control room racks. Each chamber has an independent high-voltage power supply. The individual current signals obtained from each section of the detector are proportional to upper-core and lower-core neutron flux, respectively. These provide core flux status information at the instrument racks and, through isolation amplifiers, provide the same information at the control console. A separate output furnishes bias signals used in the overpower and overtemperature delta T reactor trip functions. The individual current signals are combined to provide an average signal proportional to average core flux in the associated core quadrant. This average signal is conditioned to provide an analog voltage signal for use in permissive, control, and protection bi-stable amplifiers.

Isolation amplifiers, which provide remote control signals and core power status information to the operator and plant computer system (PCS), also utilize the average power analog signal. The four power range channels are operated from separate ac sources and are housed in separate racks so that a single failure will not cause loss of protection functions. Redundant relays for the protection functions are located in the logic portion of the protection system.

Isolated analog outputs from each power range channel are compared in a separate auxiliary channel drawer. This comparator provides the operator with annunciation of deviations in average power between the four power range channels. Switches are provided to defeat this comparison for a failed channel so that subsequent deviations or failures among the three remaining channels are annunciated.

7.4.2.5 **Equipment Design**

The ex-core nuclear instrumentation system consists of various plug-in-type modules that perform the functions indicated on Figure 7.4-2 for the source, intermediate, and power ranges. Components designed to military specifications are used, where possible, in conjunction with a conservative design stressing reliability, derating of components and circuits, and the use of field-proven circuits. On-line testing and calibration features are provided for each channel. The test signals are superimposed on the normal sensor signal during plant operation. This permits valid trip conditions to override the test signal, since the sensing elements are never removed from the circuit.

7.4.3 Components

7.4.3.1 Detectors

The nuclear instrumentation system employs six detector radial locations containing a total of eight detectors (two proportional counters, two compensated ionization chambers, and four dual-section, uncompensated ionization chamber assemblies) installed around the reactor in the primary shield. Windows in the primary shield minimize leakage flux attenuation and distortion.

Boron fluoride proportional counters having a nominal thermal neutron sensitivity of 10 counts/neutron/cm^2/sec (cps/nv) provide pulse signals to the source range channels. These detectors are installed on opposite "flat" portions of the core at an elevation approximating the quarter-core height.

Compensated ionization chambers serve as neutron sensors for the intermediate range channels, and are located in the same instrument wells and detector assemblies as the source range detectors. These detectors have a nominal thermal neutron sensitivity of 4×10^{-14}A/n/cm^2/sec. Gamma sensitivity is less than 3×10^{-11}/Roentgen/hr when operated uncompensated, and is reduced to approximately 3×10^{-13}A/R/hr in compensated operation. The detectors are positioned at an elevation corresponding to the center of the quarter-core height.

The detector assemblies containing one each of the above-mentioned detectors use watertight, corrosion-resistant, steel enclosures. High-density polyethylene, used as a moderator-insulator within the detector assemblies, will be confined at temperatures associated with a LOCA. The detectors are connected to the junction box at the bottom of the detector well by special high-temperature, radiation-resistant cables.

The remaining four detector assemblies contain the power range ionization chambers. Each provides two current signals corresponding to the neutron flux in the upper and lower sections of a core quadrant. These detectors have a total neutron sensitive length of 10 feet and a nominal thermal neutron sensitivity for each section of 1.7×10^{-13}A/n/cm^2/sec. Gamma sensitivity of each section is approximately 10^{-10}A/R/hr.

The detector assemblies for power range operation are installed vertically and located equidistant from the reactor vessel at all points, and, to minimize neutron flux pattern distortions, within one foot of the reactor vessel. Cabling from individual detector wells to the containment penetrations and to the instrument racks in the control room is routed in individual conduits, with physical separation between the penetrations and conduits associated with redundant protective channels.

7.4.3.2 Source Range Components

The source range output information is tabulated in Table 7.4-1. The detector for each source range channel is a Boron-10 lined proportional counter. The signal received from the counter has a range of 1 to 10^6 pulses per second randomly generated, and is received through a

fixed gain pulse preamplifier located outside the containment. The preamplifier optimizes the signal-to-noise ratio and also furnishes high-voltage coupling to the detector.

The preamp has internal provisions for generating self-test frequencies of 60 counts per second (cps) and 10^6 cps. These test oscillator circuits are energized by a switch located on the associated source range drawer. The source range channel power supplies furnish low voltage for preamp operation as well as low voltage for the drawer-mounted modules. The preamp is solid-state in design, with discrete components, and includes an impedance matching network between the preamp output and the 75-ohm triaxial or superscreen cable.

The preamp output is received at the postamplifier located on the source range drawer. This module provides amplification and discrimination, both of which are adjustable. Discrimination is provided between neutron flux pulses and combined noise and gamma-generated pulses. The discriminator supplies two outputs: one output (isolated) to a scaler-timer unit on the visual-audio channel drawer (see source range auxiliary equipment), and the other to a pulse shaper (transistorized flip-flop circuit) that supplies a constant amplitude pulse to the log integrator module within the source range drawer.

Logarithmic integration of the pulse signal is performed in another modular unit to obtain an analog dc signal. The log signal is then amplified for local indication on the front panel of the source range drawer, and is also delivered through a parallel run to the source range level bi-stables and isolation amplifier. The analog output signal is proportional to the count rate being received from the sensor, and is displayed by the front panel meter on a scale calibrated logarithmically from 10^0 to 10^6 cps. The solid-state isolation amplifier provides five analog outputs, all of which are adjustable through attenuator controls. Three outputs are used as follows: as remote indication (0–1 ma); as remote recording (0–37.5 mV dc); and as an input to the PCS (0–5V dc). A 0–10V dc output is used by the start-up-rate amplifier to produce a start-up-rate indication at the main control board. The remaining output (0–5V dc) is a spare.

All bi-stables employ a basic plug-in module with the external wiring determining the mode of operation (latching or non-latching) and direction of output change with rising power. Bi-stables have two adjustments: “Trip Level” and “Differential.” The first adjustment determines the trip point of the bi-stable, while the second determines the “dead zone” difference between the trip and release points of the bi-stable. The bi-stable module card includes a relay driver circuit made up of a silicon-controlled rectifier and full-wave bridge configuration. The bi-stable output controls are the silicon-controlled rectifier gate, which, in turn, controls conduction of the full-wave bridge supplying the power to drive up to four 115V ac Westinghouse BF relays. Relays are located remote from the nuclear instrumentation system racks.

Of the three bi-stables monitoring the source range level amplifier signal, one is a spare, one is used to monitor shutdown flux level only, and the third monitors source range operation during shutdown and start-up operation and provides a reactor trip on high flux level. The reactivity of the core during shutdown is monitored by a bi-stable to ensure protection of plant personnel

working in the containment. Bi-stable tripping will initiate local visual and audible annunciation and remote audible annunciation of any abnormal increase in core activity. Visual annunciation occurs at the nuclear instrumentation system rack and on the main control board. Audible annunciation is handled by the annunciator located in the control room, and the evacuation horn located in the containment.

These annunciators ensure that plant personnel are alerted to any potentially hazardous condition. This bi-stable action is manually blocked by deliberate operator action during plant start-up. Blocking is continuously annunciated at the control board during source range operation and is automatically blocked by permissive P-6. The bi-stable trip point is approximately one-half decade above the flux level recorded during full shutdown.

The source range level bi-stable monitors the core reactivity during the full span of source range operation, until such time as the intermediate range channels assume control of that portion of the reactor protection that is being supplied by nuclear instrumentation. At that time, when the intermediate range permissive P-6 is available, the source range reactor trip bi-stable may be manually blocked, and high voltage removed from the B10 detector by the operator's actuation of two momentary-contact switches located on the main control board.

A fourth bi-stable-relay driver unit is used as a high-voltage failure monitor. Loss of this voltage actuates the bi-stable, the relay driver, and then the associated relay. The relay provides control board annunciation through a one-out-of-two matrix formed with a similar relay controlled by the other source range channel. Failure of either source range high voltage actuates this common annunciator on the main control board. During normal operation, the source range high voltage will be cut off (as described above) when manual block of the source range trips is initiated. In this instance, loss of high-voltage annunciation will be intentionally defeated to prevent the alarming of a condition that is not abnormal.

A test-calibrate module is also included in each source range drawer for self-check of that particular channel. A multiposition switch on the source range front panel controls this module and also the operation of the built-in oscillator circuits in the preamp. The module is capable of injecting test signals of either 60, 10^3, 10^5 or 10^6 cps at the input to the post amplifier, or a variable dc voltage corresponding to 1 to 10^6 cps at the input to the log amplifier. An interlock between the trip bypass switch and the test-calibrate switch will prevent inadvertent actuation of the reactor trip circuits, (i.e., the channel cannot be put in the test mode unless the trip is defeated). Trip bypass will be annunciated on the source range drawer and on the main control board, per IEEE 279 Standard, Section 4.13. Operation of the test-calibrate module will be annunciated on the control board as "Nuclear Instrumentation System Channel Test." This common annunciator for all nuclear instrumentation system channels is alarmed when any channel is placed in the test position, and alerts the operator that a test is being performed at the nuclear instrumentation system racks.

7.4.3.3 **Source Range Auxiliary Equipment**

7.4.3.3.1 Visual-Audio Count Rate

The visual-audio count rate receives a signal from each of the source range channels. This isolated signal originates at the discriminator output in each source range channel. A switch on the audio count-rate drawer selects either source range channel for monitoring. The selected signal is fed to a scaler-timer unit that permits count accumulation in the preset time or preset count mode. A visual display to five decimal places is presented through counting strips located on the front of the audio count-rate drawer.

A "Scale Factor" switch permits division of the scaler output signal by 10, 100, or 1000. This signal, derived from the printer output of the scaler, is conditioned and sent to two of the audio amplifiers, which power two speakers: one speaker located in the control room, and the other in the containment. These speakers give personnel an audible indication of the count rate. Since the audio amplifier signal is taken from the coded scaler output, adjustment of the scale factor switch will alter only the audible count rate. This enables the operator to maintain the audible count rate at a distinguishable level.

7.4.3.3.2 Remote Count-Rate Meter

The remote meter indication is an analog signal proportional to the count rate being received, and is obtained from the 0 to 1 mA isolation amplifier output.

The meter is mounted on the main control board and calibrated logarithmically from 10^0 to 10^6 cps. This meter gives the same indication at the control board as is displayed by the local meter on the corresponding source range drawer.

7.4.3.3.3 Remote Recorder

This recorder is capable of continuously recording the nuclear instrumentation system channels. Each channel is directly connected to the multipen recorder. In the case of the source ranges, a 0 to 37.5 mV dc signal, proportional to the count rate range of 10^0 to 10^6 cps, is supplied for recording during source range operation.

7.4.3.3.4 Start-up-Rate Circuitry

The start-up-rate drawer receives four input signals (0–10V dc), one from each of the source and intermediate range channels. Four rate amplifier modules condition these signals and output four rate signals to the respective control room start-up-rate meters. A test module is provided that can inject a test signal into any one of the rate circuits, and can be monitored on a test meter mounted on the front panel of this drawer. Two power supplies are provided to ensure rate indication from at least one source and intermediate range channel pair.

7.4.3.4 **Intermediate Range Components**

Intermediate range output information is tabulated in Table 7.4-2. Each intermediate range channel receives a direct current signal from a compensated ion chamber, and supplies positive high voltage and compensating (negative) high voltage to its respective detector. The compensating high voltage is used to cancel the effects of gamma radiation on the signal current being delivered to the intermediate range channel. Both high-voltage supplies will be adjustable through controls located inside the channel drawer. The detector signal is received by the intermediate range logarithmic amplifier. The modular unit, comprising several operational amplifiers and associated discrete solid-state components, produces an analog voltage output signal that is proportional to the logarithm of the input current. This signal is used for local indication and is monitored by the isolation amplifier and the various bi-stable relay-driver modules within the intermediate range drawer. A 10^{-11}A signal is continuously inserted, and serves as a reference during gamma compensation. Local indication is provided by a meter mounted on the front panel of the drawer, which has a logarithmic scale calibration of 10^{-11} to 10^{-3}A.

The isolation amplifier is the same solid-state module that is used in the source range; it supplies the same five outputs for the same usage. Six bi-stable relay-driver units are used in the intermediate range drawer to provide the following functions:

1. One monitors the positive high voltage.
2. One monitors the compensating high-voltage.
3. One provides the permissive P-6.
4. One provides rod-stop (blocks automatic and manual rod withdrawal).
5. One provides reactor trip.
6. One serves as a spare.

The intermediate range permissive P-6 bi-stable drives two Westinghouse BF relays (for redundancy), and the relays from each channel are combined in one-out-of-two matrices to provide the permissive function and control board annunciation of permissive availability. Permissive P-6 permits simultaneous manual blocking of the source range trips, and removal of the source range detector high voltage. Once source range blocking has been performed, the operator may, through administrative action, defeat permissive P-6 and reactivate the source range high-voltage and trip functions if required. This defeat is accomplished by the coincident operation of two control-board-mounted, momentary-contact switches. This provision, however, is only operational below permissive P-10, which is supplied by the power range channels. Above P-10, the defeat circuit is automatically bypassed and permissive P-6 is maintained which, in effect, maintains source range cutoff. The level bi-stable relay-driver unit that provides the intermediate range rod-stop function also drives two Westinghouse BF relays. Again, one-out-of-two matrices formed by the relays from the two intermediate range channels supply

the rod-stop function and control board annunciation. Blocking of the outputs of these matrices is administratively performed when nuclear power is above permissive P-10, and can only be accomplished by deliberate operator action on two control-board-mounted switches.

The intermediate range reactor trip function is provided by a similar circuit arrangement, the only difference being the trip point of the bi-stable units. The same control board switches that control blocking of the rod-stop matrices also provide blocking action for the reactor trip matrices. These blocks are manually inserted when the power range instrumentation indicates proper operation through activation of the P-10 permissive function. On decreasing power, however, the more restrictive intermediate range trip functions are automatically reinserted in the protective system. While these trips are blocked, there will be continuous illumination on the main control board of "Intermediate Range Trip and Rod Stop Blocked." The high-voltage failure monitors provide both local and remote annunciation upon failure of the respective high-voltage supplies. A common "Intermediate Range Loss of Detector Voltage" and separate "Intermediate Range Loss of Compensate Voltage" are provided as control board annunciators for the intermediate ranges.

Administrative testing of each intermediate range channel is provided by a built-in test-calibrate module that injects a test signal at the input to the log amplifier. The signal is controlled by a multiposition switch on the front of each intermediate range drawer. A fixed 10^{-11}A signal is available, along with a variable 10^{-10} through 10^{-3}A signal, selectable in decade increments.

As in source range testing, the test switch on the intermediate range must be operated in coincidence with a trip bypass on the drawer. An interlock between these switches prevents injection of a test signal, until the trip bypass is in operation. Removal of the trip bypass also removes the test signal.

7.4.3.5 **Intermediate Range Auxiliary Equipment**

7.4.3.5.1 Remote Meter

The remote meter indication is in the form of an analog signal (0–1 mA) proportional to the ion chamber current. The isolation amplifier in each channel supplies this output to a separate meter. Meter calibration is 10^{-11} to 10^{-3}A.

7.4.3.5.2 Remote Recorder

This is the same recorder described above for the source range. A 0 to 50 mV dc signal from the isolation amplifier is supplied to the recorder and is proportional to the ion chamber current range of 10^{-11} to 10^{-3}A. All the intermediate range signals are connected to the recorder.

7.4.3.6 **Power Range Components**

The power range output information is tabulated in Table 7.4-3. The power range detector is a long, uncompensated ion chamber assembly consisting of two separate neutron-sensitive

sections. Each section supplies a current signal to the associated power range. There is one high-voltage power supply per channel that supplies voltage to both sections of the associated detector. The two signals are received at the channel input and handled through separate shunt, filter board assemblies. There is a meter range/rate switch for each digital ammeter located on the front panel of the power range drawer. Each meter range/rate switch has four positions, namely 400μA/slow, 4000μA/slow, 400μA/fast, and 4000μA/fast. The switch selects shunt resistors for the meter but never interrupts the ion chamber signal to the power range channel. The circuit is so designed that a failure of the meter or switch will not interrupt the signal to the average power circuitry.

The individual currents are displayed on the two front ion chamber current meters and are then sent to separate isolation amplifiers. There are two isolation amplifiers monitoring each of the two individual current signals. The unit feeding the delta T protection function is being used for its impedance-matching characteristics rather than isolation. All of the isolation amplifiers are capable of providing the same five output ranges as the isolation amplifiers previously described in relation to the source and intermediate ranges. Two of the isolation amplifiers (used as impedance matching networks), one monitoring each of the currents, supply signals to the delta T reset. The other two isolation amplifiers provide output for the remote recorder, remote meter, and PCS. The individual current signals are then sent to a summing amplifier module that outputs a linear 0 to 10V dc signal proportional to their average. The output of this unit will feed a linear amplifier with two controls: one a “Zero” adjust located on the module itself, the other a “Gain” adjust with a calibrated dial located on the drawer’s front panel. The output signal from this unit corresponds to 0% to 120% of full power and is displayed on a percent full-power meter on the front panel of the power range drawer. This same signal is delivered directly to three isolation amplifiers, a dropped-rod sensing assembly, and six bi-stable relay-driver modules. These isolation amplifiers are identical to those previously described, and the outputs are the same in number and range but are used in different functions. (Specific outputs from the amplifiers are discussed in the auxiliary equipment section that follows.)

The dropped-rod sensor assembly is an operational amplifier unit that incorporates an adjustable lag network at one input and a non-delayed signal on the other. The unit compares the actual power signal with the delayed power signal received through the lag network, and amplifies the difference. This amplified differential signal is delivered to a bi-stable relay-driver unit that trips when the level of this signal exceeds a preset amount. Tripping of this unit indicates a power level change over the lag period, which would be indicative of a dropped rod. This bi-stable unit is a latching type, ensuring that the necessary action will be initiated and carried to completion. Specifically, the unit controls dual Westinghouse BF relays which, in one-out-of-four logic matrices, provide a control board annunciation signal, and a PCS input signal. A reset switch on the associated power range drawer must be operated manually to reset the bi-stable.

The bi-stable units that sense the power level signal, as derived by the linear amplifier, are non-latching and perform the following functions: (1) overpower rod-stop (blocks automatic and

manual rod withdrawal); (2) permissive functions; (3) low-range reactor trip; and (4) high-range reactor trip.

The overpower rod-stop and permissive bi-stables are units that trip on high power level and control Westinghouse BF relays in the remote relay racks. The rod-stop relay matrices (one-out-of-four) provide a rod-stop function to the rod control system and a main control board annunciation. Two-out-of-four logic, developed by relays controlled through the respective power range bi-stables, provide the signals required for the permissive functions. One set of relays provides permissive P-10, as previously discussed regarding its use in the source range and intermediate range. One set of relays provides permissive P-8, as previously discussed in Section 7.2.2 regarding low reactor coolant flow trips. One other group of relays is provided as a spare.

Permissives P-8 and P-10 are supplied solely by nuclear instrumentation. For this reason, the nuclear instrumentation design provides for main control board annunciation of P-8 and P-10 availability. Permissive P-10 is used in all three ranges of nuclear instrumentation, while P-8 is provided by nuclear instrumentation for use in the reactor protection system.

The low-range trip bi-stable actuates two Westinghouse BF relays in the logic system. The two relays provide redundance within the logic portion of the protection system. Each relay is used in a separate matrix with the relays from the other power range channels to continue the redundancy. The logic circuitry formed by the contacts on these relays provide for one-out-of-four and two-out-of-four logic outputs. The low-range trip relays provide the following functions: (1) PCS input (single channel); (2) low-range trip annunciation (two-out-of-four coincidence); (3) reactor trip signal to reactor protection system (two-out-of-four coincidence); and (4) annunciation of “Single Channel Low-Range Trip” (one-out-of-four).

Provisions for manually blocking the low-range trip become available when two-out-of-four power ranges exceed the permissive P-10 level. Operator action on two control-board-mounted momentary-contact switches then initiates the blocking action. A control board permissive status light, “Power Range Low-Range Trip Blocked,” will be illuminated continuously when the trip function is blocked. On decreasing power, three of four power ranges below the P-10 power level will automatically reactivate the low-range trip.

The high-range reactor trip logic circuitry is developed identical to the low-range reactor trip circuitry, but no provision for blocking is included. The high-range trip remains active at all times to prevent any continuation of an overpower condition.

An additional bi-stable unit monitors the high-voltage power supply in the power range. Operation of this unit is identical to that for the source and intermediate ranges. The bistable provides relay actuation in the remote relay racks on failure of power range high voltage. While there is a separate relay for each power range, they control a common “Power Range Loss of Detector Voltage” annunciator on the main control board. Separate local indication of high-voltage failure is provided on the power range drawers.

The test-calibrate module provided on each power range is capable of injecting test signals at several points in the channel. In all cases, the test signals are superimposed on the normal signal. A bypass of the dropped-rod circuit is not required during channel test since this circuit produces only an alarm through one-out-of-four logic matrix for a sudden power change. Test signals can be injected independently or simultaneously at the input of either ammeter-shunt assembly to appear as the individual ion chamber currents. Operation of the test-calibrate switch on any power range will cause the "Channel Test" annunciator to be alarmed on the main control board.

7.4.3.7 **Power Range Auxiliary Equipment**

7.4.3.7.1 Comparator

The comparator receives an isolated signal from each of the four power range detectors. These signals are conditioned in separate operational amplifier circuits and then compared with one another to determine if a preset amount of deviation of power levels has occurred between any two power ranges. Should such a deviation occur, the comparator output will operate a remote relay to actuate the control board annunciator, "Power Range Channel Deviation." This alarm will alert the operator to either a power unbalance being monitored by the power ranges, or to a channel failure. Through other indicators, the operator can then determine the deviating channel(s) and take corrective action. Should correction of the situation not be immediately possible (e.g., a channel failure, rather than reactor condition), provisions are available to eliminate the failed channel from the comparison function. The comparator can then continue to monitor the active channels.

7.4.3.7.2 Remote Recorder

Each power range channel supplies a 0 to 50 mV dc signal proportional to 0-120% full power to the nuclear power recorder. The signals from Power Ranges Number 1, Number 2, Number 3, and Number 4 are connected directly to the recorder. All four signals are continually indicated on control board meters.

7.4.3.7.3 Remote Meter

The remote meters receive the 0 to 1 mA isolated output that is available from each power range. This indication corresponds to that shown on the power range drawer. The signal is displayed on a meter scale calibrated from 0 to 120% of full power.

7.4.3.7.4 Overpower Recorders

A pair of recorders is used to monitor the individual average power indications from the four power ranges. Each recorder provides continuous monitoring of two power range channels, and has a full-scale deflection time of 0.25 second. The recorders are capable of displaying overpower excursions up to 200% of full power. A power range isolated output of 0-50 mV dc will correspond to the range of 0 to 200% full power for these recorders.

7.4.3.7.5 Ion Chamber Current Recorders

A recorder is provided to record the upper and lower ion chamber currents for each power range detector. Two isolated outputs (0–5V dc), one from each of the ion chamber isolation amplifiers, are provided for each recorder. Comparison of the two traces is an indication of the flux difference between the upper and lower sections of a given detector.

7.4.3.7.6 Delta Flux Remote Meter

Four control-board-mounted meters display the flux difference between the upper and lower ion chambers directly for each of the power range detectors.

7.4.3.8 **Miscellaneous Control and Indication Panel**

Switches are provided on this panel to permit a failed power range channel's overpower-rod-stop function to be bypassed, and its overpower-rod-stop signal to the rod control system to be supplied by signals derived from active channels. This allows normal power operation to continue while the failed channel is repaired.

Two panel mounted indicating lights, one for the upper section of the core and one for the lower section of the core are provided and are illuminated for a deviating condition or for a failed power range detector. Each power range detector provides an upper and a lower flux signal corresponding to the neutron flux in the upper section and in the lower section of a core quadrant. These upper and lower flux signals are compared and alarm the following conditions:

1. A high deviation of any upper section from the average of all the upper sections.
2. A high deviation of any lower section from the average of all the lower sections.

High deviation alarms will occur, one for the upper section and one for the lower section, when any individual section is greater than a preset amount above the average. These alarms warn the operator that a quadrant power tilt exists when the power level is above 50% power. The alarm circuits are automatically defeated when all sections are below 50% of rated power.

Additionally, two panel mounted indicating lights, one for each deviation comparison, are illuminated when all sections are below 50% of rated power.

In the event of a failed power range channel, bypass switches located on the panel are provided to defeat a failed power range channel input to an upper or lower section deviation comparison. This feature permits the continued monitoring of the core with a power range channel out of service.

7.4.3.9 **Output Information**

Tables 7.4-1, 7.4-2, and 7.4-3 provide the nuclear instrumentation system control and indication output information for the source, intermediate, and power ranges, respectively.

7.4.4 System Evaluation

7.4.4.1 Philosophy and Setpoints

During plant shutdown and operation, three discrete, independent levels of nuclear protection are provided from the three ranges of ex-core nuclear instrumentation. The basic protection philosophy is that the level protection is present in all three ranges to provide a reliable, rapid, and restrictive protection system that is not dependent upon operation of higher-range instrumentation.

Reliability is obtained by providing redundant channels that are physically and electrically separated. Fast trip response is an inherent advantage of using level trip protection in lieu of start-up-rate protection (with a long time constant) during plant start-up. More restrictive operation is an inherent feature, since an increase in power cannot be performed until satisfactory operation is obtained from higher-range instrumentation, which permits administrative bypass of the lower-range instrumentation. On decreasing power level, protection is automatically made more restrictive. Start-up accidents while in the source range are rapidly terminated without significant increases in nuclear flux, and with essentially no power generation or reactor coolant temperature increase.

The indications and administrative actions required by this protection system are readily available to the operator and should result in a safe, uncomplicated increase of power.

7.4.4.2 Reactor Trip Protection

During reactor start-up, the operator is made aware of satisfactory operation of one or more intermediate range channels by annunciation (audible and visual) at the control board. The source and intermediate range flux level information is also readily available on recorders and indicators at the control console. At this time, if both intermediate range channels are functioning properly, the operator would depress the two manual block switches associated with the source range logic circuitry, thus causing cutoff of source range detector voltages and blocking the trip logic outputs. The manual block should not be initiated, however, until at least one decade of satisfactory intermediate range operation is obtained. The permissive P-6 annunciation is continuously displayed by the control board status lights.

Continuation of the start-up procedure in the intermediate range would result in a normal power increase and the receipt of a permissive signal from the power range channels when two out of four channels exceed 10% of full power. The operator is alerted to this condition by a control board permissive status light. Indicators (one per channel) and a recorder also indicate unit status in terms of percent full power. If the operator does not block the intermediate range trip and continues the power increase, a rod stop will automatically occur from either of the intermediate range channels. The operator should depress the momentary “Manual Block” push-buttons associated with the intermediate range rod stop and reactor trip logic. This would transfer protection to the low-range trips for the four power range channels. The permissive P-10 status light would be continuously displayed, as was P-6. The two low-range manual block switches

must be depressed to initiate blocking prior to continuation of the power increase. The permissive functions associated with administrative trip blocking and automatic reactivation are provided with the same separation and redundancy as the trip functions.

When power operation is decreasing to lower levels, more restrictive trip protection is automatically afforded when three out of four power range channels are below permissive P-10, and when two out of two intermediate range channels are below the permissive P-6.

7.4.4.3 **Rod-Drop**

An additional alarm function provided by the power range instrumentation is backup to the rod-drop detection of the rod bottom bi-stables on the rod position system. The nuclear instrumentation rod-drop detection is provided by comparison of the average nuclear power signal with the same signal, as conditioned by an adjustable lag network. This method provides a response to dynamic signal changes associated with a dropped-rod condition, but does not respond to the slower signal changes associated with normal plant operation. Main control room alarm actuation from at least one of the four power range channels will occur for any dropped-rod condition.

Each rod-drop sensing circuit has associated with it a bi-stable amplifier driving two relays in separate logic relay racks. The logic relay matrices are connected in a one-out-of-four “OR” configuration to initiate a control room alarm. The dropped rod detection circuit also illuminates the dropped rod window on the individual NIS rack that detected the dropped rod.

7.4.4.4 **Control and Alarm Functions**

Various control and alarm functions are obtained from the three ranges of ex-core nuclear instrumentation during shutdown, start-up, and power operation. These functions are used to alert the operator to conditions that require administrative action, and alert personnel to unsafe reactor conditions. They also provide signals to the rod control system for automatic blocking of rod withdrawal during plant operation to avoid unnecessary reactor trips.

7.4.4.4.1 Source Range

No control functions are obtained from the source range channels. Alarm functions are provided, however, to alert the operator of any inadvertent changes in shutdown reactivity. Visual annunciation of this condition is at the control board, with audible annunciation in the containment and control room. This alarm can either be blocked before start-up or can serve as the start-up alarm in conjunction with administrative procedures.

7.4.4.4.2 Intermediate Range

Both alarm and control functions are supplied by the intermediate range channels. Blocking of rod withdrawal is initiated by either intermediate range channel on high flux level. This condition is alarmed at the control board to alert the operator that rod stop has been initiated. In addition, the intermediate range actuates the P-6 permissive status light when either channel

exceeds the P-6 permissive level. This alerts the operator to the fact that he must take administrative action to manually block the source range trips to prevent an inadvertent trip during normal power increase.

7.4.4.4.3 Power Range

The power range channels provide alarm and control functions similar to those in the intermediate range. An overpower rod-stop function from any of the four power range channels inhibits rod withdrawal and is alarmed at the control board. The power range channels also actuate the P-10 permissive status light when two of the four channels exceed the permissive P-10 level. As in the case of P-6 in the intermediate range, this alerts the operating personnel that administrative action (namely, blocking of intermediate and low-range trips) is required before any further power increase may take place.

A permissive status light is provided for P-8, "Nuclear Power Below P-8." The extinguishing of the P-8 permissive status light alerts the operator that the one-out-of-three low-flow trips and one-out-of-three pump-breaker-open trips are now active. These trips are blocked while the status light is illuminated. Additional functions are provided in the power range of operation. A dropped control rod will be sensed by one or more of the power range channels, and this condition will initiate an alarm on the main control room annunciator and illuminate a dropped rod window on the individual NIS rack that detected the dropped rod.

Another function is a power range channel deviation alarm. This alarm is furnished by the comparator channel through a comparison of the average power level signals being supplied by the power range channels. Actuation of this alarm alerts the operator to a power imbalance between the channels so that corrective action can be taken. Additionally, two signals, supplied through isolation amplifiers, are provided by each power range channel: one signal is used for the upper section deviation alarm and one signal is used for the lower section deviation alarm. Actuation of these alarms alerts the operator to a power imbalance between the detector upper or between the detector lower sections so that corrective action can be taken. These ion chamber signals are discussed in Section 7.4.3.8.

In the case of a failed channel, defeat switches are provided to defeat a channel's input to the channel deviation comparison as well as the detector section deviation comparisons.

7.4.4.5 **Power Supply**

The nuclear instrumentation system draws its primary power from the vital instrument buses, whose reliability is discussed in Chapter 8. Redundant nuclear instrumentation system channels are powered from separate buses. The loss of a single vital instrument bus would result in the initiation of all reactor trips associated with the channels deriving power from that source. During power operation, the loss of a single bus would not result in a reactor trip, since the power range reactor trip function operates from two-out-of-four logic. If the bus failure occurred during

source or intermediate range operation (one-out-of-two logic), a reactor trip condition would result.

7.4.4.6 **Safety Factors**

The relation of the power range channels to the reactor protection system has been described in Section 7.2. To maintain the desired accuracy in trip action, the total error from drift in the power range channels will be held to ±1.0% at full power. Routine tests and calibration will ensure that this degree of deviation is not exceeded. Bi-stable trip setpoints of the power range channels will also be held to an accuracy of ±1.0% of full power.

Table 7.4-1
SOURCE RANGE SIGNALS

Signal and Source	Destination and/or Function
Isolation amplifier	
0–10V dc	Auxiliary channel start-up rate (SUR)
0–5V dc	PCS
0–5V dc	Spare
0–1 mA dc	Remote meter counts per second (cps)
0–37.5 mV dc	Remote recorder
Bistable amplifiers	
115V ac	Miscellaneous process relay rack (spare)
115V ac	Miscellaneous process relay rack (high flux level at shutdown)
115V ac	Reactor protection relay rack (source range reactor trip)
115V ac	Miscellaneous process relay rack (annunciate “source range loss of detector voltage”)
Manual block	
115V ac	Miscellaneous process relay rack (block high flux level at shutdown)
Trip bypass	
115V ac	Reactor protection relay rack (block of source range reactor trip)
Test-calibrate	
115V ac	Relay rack (nuclear instrumentation system channel test - control room)
Discriminator	
$1–10^6$ Cps	Source range auxiliary channel (visual-audio)

Table 7.4-2
INTERMEDIATE RANGE SIGNALS

Signal and Source	Destination and/or Function
Isolation amplifier	
0–10V dc	Auxiliary channel start-up rate
0–1 mA dc	Remote meter (A)
0–50 mV dc	Remote recorder
0–5V dc	Spare
0–5V dc	PCS
Bistable amplifiers	
115V ac	Relay rack (spare)
115V ac	Reactor protection relay rack (intermediate range permissive P-6)
115V ac	Miscellaneous process relay rack (intermediate range rod stop)
115V ac	Reactor protection relay rack (intermediate range reactor trip)
115V ac	Miscellaneous process relay rack (annunciate “intermediate range loss of detector voltage”)
115V ac	Miscellaneous process relay rack (annunciate “intermediate range loss of compensating voltage”)
Trip bypass	
115V ac	Reactor protection relay rack (block of rod-stop and reactor trip)
Test-calibrate	
115V ac	Miscellaneous process relay rack (NIS channel test - control room)

Table 7.4-3
POWER RANGE SIGNALS

Signal and Source	Destination and/or Function
Isolation amplifier (ion chamber A)	
0–10V dc	Upper flux comparator
0–5V dc	PCS
0–1 mA dc	Remote meter (delta flux)
0–5V dc	Remote recorder
0–50 mV dc	Spare
Isolation amplifier (ion chamber A)	
0–10V dc	Delta T overpower-overtemperature compensation
Isolation amplifier (ion chamber B)	
0–10V dc	Lower flux comparator
0–5V dc	PCS
0–1 mA dc	Remote meter (delta flux)
0–5V dc	Remote recorder
0–50 mV dc	Spare
Isolation amplifier (ion chamber B)	
0–10V dc	Delta T overpower-overtemperature compensation
Isolation amplifier (average power)	
0–10V dc	Spare
0–5V dc	PCS
0–1 mA dc	Remote meter (% of full power)
0–50 mV dc	Remote recorder
0–5V dc	Spare
Isolation amplifier (average power)	
0–10V dc	Power mismatch
0–5V dc	Spare
0–1 mA dc	Spare
0–50 mV dc	Spare
0–5V dc	Spare
Isolation amplifier (average power)	
0–10V dc	Comparator
0–5V dc	Spare
0–1 mV dc	Spare
0–50V dc	Overpower recorder
0–5V dc	Spare

Table 7.4-3 (continued)
POWER RANGE SIGNALS

Signal and Source	Destination and/or Function
Bi-stable amplifiers	
115V ac	Reactor protection relay rack (annunciator “NIS dropped rod flux decrease > 5% per 2 sec”)
115V ac	Miscellaneous process relay rack (overpower rod stop)
115V ac	Reactor protection relay rack (permissive P-8)
115V ac	Reactor protection relay rack (permissive P-10)
115V ac	Reactor protection relay rack (spare permissive)
115V ac	Reactor protection relay rack (low range reactor trip)
115V ac	Reactor protection relay rack (high range reactor trip)
115V ac	Miscellaneous process relay rack (annunciate “power range loss of detector voltage”)
Test-calibrate	
115V ac	Miscellaneous process relay rack (nuclear instrumentation system channel test - control room)
Test bypass	
115V ac	Miscellaneous process relay rack (NIS overpower rod stop bypass)

Figure 7.4-1
RANGES OF NIS INSTRUMENTATION

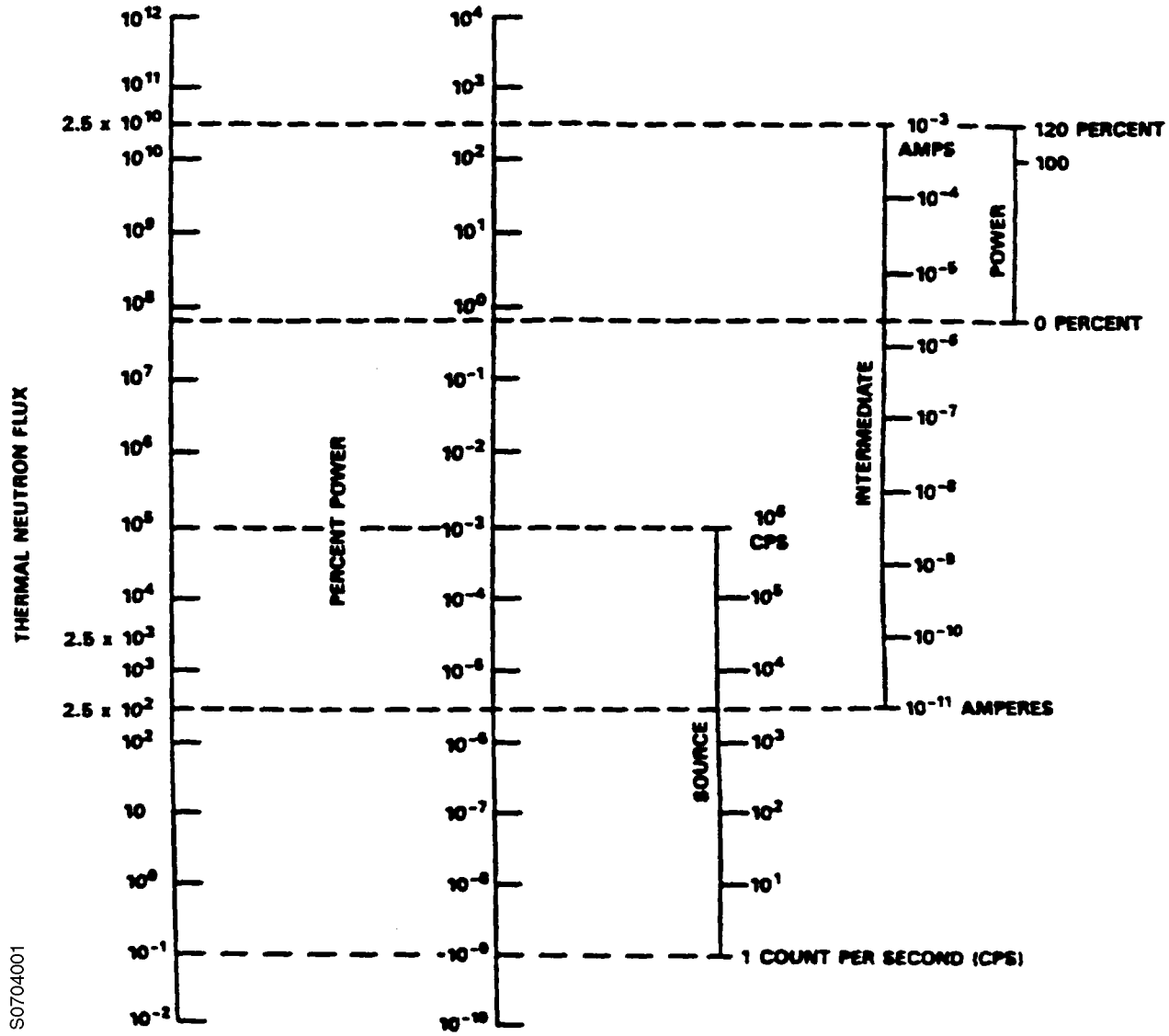


Figure 7.4-2
NUCLEAR INSTRUMENTATION SYSTEM

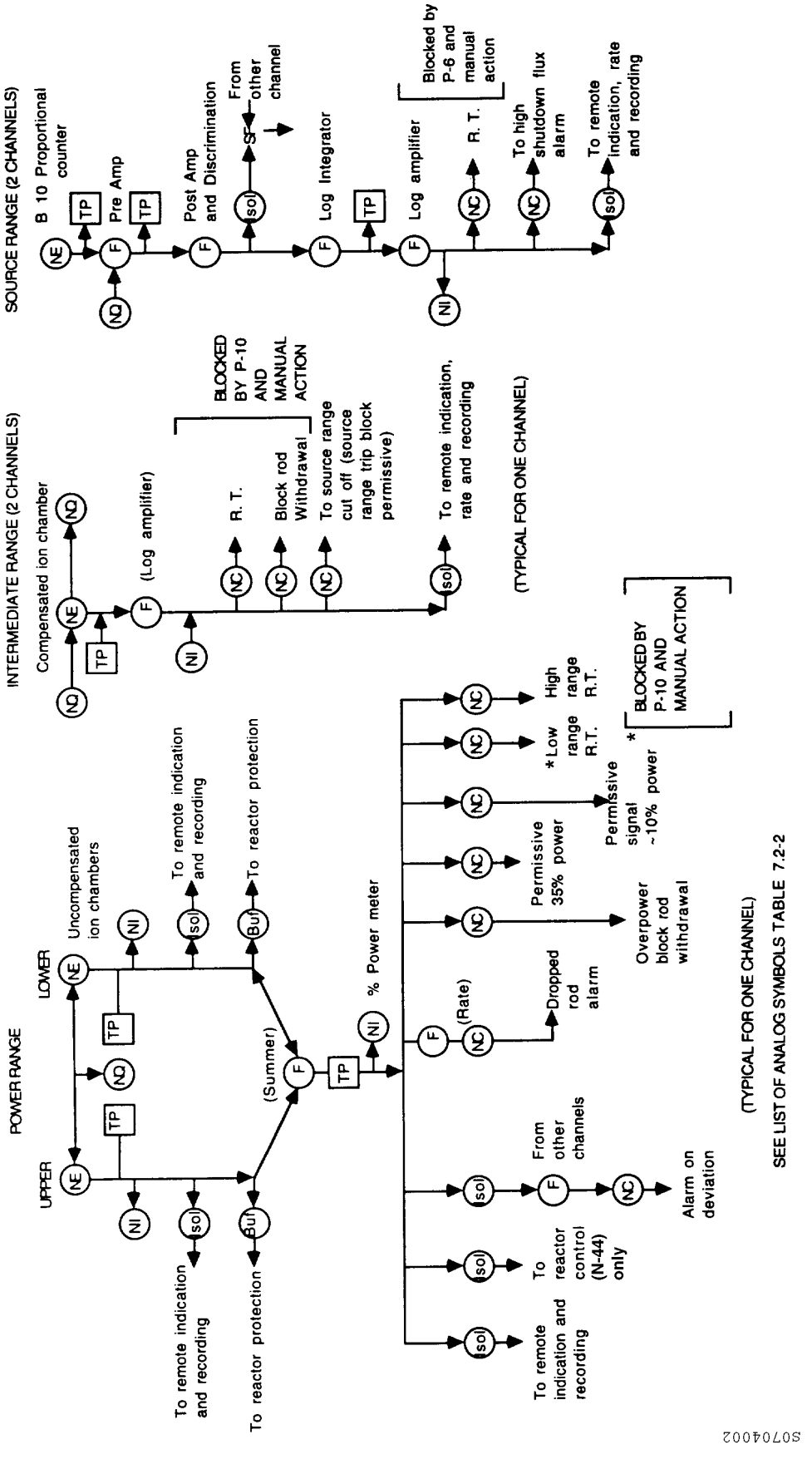
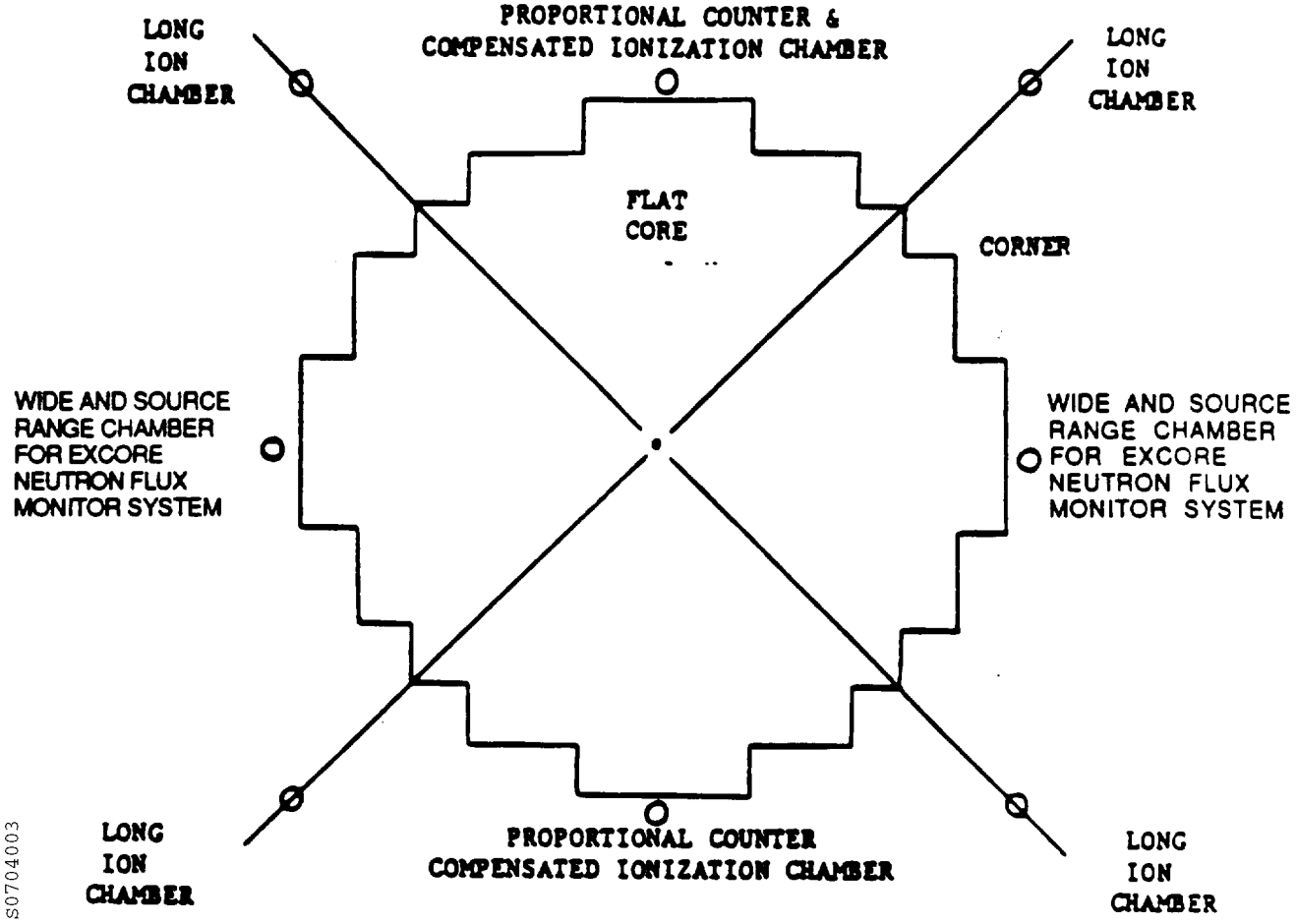


Figure 7.4-3
NEUTRON DETECTOR LOCATIONS



Intentionally Blank

7.5 ENGINEERED SAFEGUARDS

7.5.1 Design Bases

The engineered safeguards instrumentation measures temperatures, pressures, flows, and levels in the reactor coolant system, main steam system, reactor containment, and auxiliary systems. They actuate the engineered safeguards systems, and monitor their operation. Transmitted signals (flow, pressure, temperature, etc.) that can cause actuation of the engineered safeguards are either indicated or recorded in the control room.

The instrumentation and control systems provided to initiate the engineered safeguards systems are defined as safety-grade equipment and meet the safety standards applicable at the time of purchase and installation. Accident mitigation equipment subjected to a changing environment was evaluated in response to the NRC I&E Bulletin 79-01B (Reference 1) as described in Section 7.5.3.5.1.

Design criteria for redundancy and separation are similar to those used for the reactor protection system (Section 7.2). A list of emergency safeguards actuation functions is given in Table 7.5-1.

The engineered safeguards systems are actuated by the redundant logic and coincidence networks similar to those used for reactor protection. Each network actuates a device that operates the associated engineered safeguards equipment, motor starters, and valve operators. The channels are designed to combine redundant sensors, independent channel circuitry, and coincident trip logic. Where possible, different but related parameter measurements are utilized. This ensures a safe and reliable system in which a single failure will not defeat the intended function. The action-initiating sensors, bi-stables, and logic are shown in the figures included in the detailed engineered safeguards actuation instrumentation description given in Section 7.5.2. The engineered safeguards instrumentation system actuates (depending on the severity of the condition) the safety injection system, containment isolation, containment spray system, and the diesel-generators, and trips the containment vacuum system.

Availability of control power to the engineered safeguards trip channels is continuously indicated. The loss of instrument power to the sensors, instruments, or logic devices in the engineered safeguards instrumentation places that channel in the trip mode, except for containment spray initiating channels and the recirculation mode transfer (RMT) circuitry, which have been designed on an energize to operate basis. These systems were designed in this way to preclude their spurious operation on a loss of power.

The redundant batteries supplying power to the vital bus system are classified as passive components and are therefore subject to passive type failures. The definition of a passive failure is a failure which will not occur until after accident mitigation has entered the recirculation phase (post-RMT). Thus, should a LOOP/LOCA occur, the loss of a battery or dc bus will not credibly

occur until after the unit enters the recirculation phase. This ensures the CLS Hi-Hi and RMT energize to actuate circuitry has power available during all credible design basis events.

The engineered safeguards systems are divided into protective safeguards and consequence limiting safeguards. The protective safeguards consist of the safety injection system. The consequence limiting safeguards include the spray system, containment isolation system, and the containment vacuum system. These systems are described in detail in Chapter 6. The control system logic diagrams for these safeguards are shown in Figures 7.5-1, 7.5-2 and 7.5-3.

7.5.1.1 **Safety Injection**

Active safety injection components are actuated upon low-low pressurizer pressure, high containment pressure signals, high differential steam pressure between any steam lines and the main steam header, or high steam-line flow signals coincident with either low temperature average or low steam-line pressure signals. These actuating channel circuits are described in Section 7.2.

The signal that actuates safety injection low-low pressurizer pressure can be manually blocked when the pressurizer pressure reaches 2000 psig. This is only done during a controlled plant cooldown when the reactor is shut down. The signal that actuates safety injection on high containment pressure cannot be blocked and thus is available even when the low pressurizer pressure actuation signal is blocked. The purpose of the manual block of the signal on low pressurizer pressure is to prevent inadvertent safety injection actuation when the plant is being cooled down and depressurized.

A safety injection signal will isolate the feedwater lines by closing all control valves (main and bypass valves), trip the main feedwater pumps which in turn close the pump discharge valves, and thereby actuate the auxiliary feedwater system (Section 10.3.5), and will actuate the necessary valves required to allow the safety injection system to operate properly. Section 6.2 describes the safety injection system.

The passive accumulators of the safety injection system do not require signal or power sources to perform their functions. The actuation of the active portion of the engineered safeguards is from signals described in Table 7.2-1.

7.5.1.2 **Consequence Limiting Safeguards**

The consequence limiting safeguards system is operated by three signals: two initiation signals and one reset signal. The two initiation signals are the high containment pressure signal and the high-high containment pressure signal. The reset signal is the containment low-pressure signal. The high containment pressure signal is actuated when the containment pressure increases to a value in the range of 3.0 psig. The high-high containment pressure signal is actuated when the containment pressure increases to a value in the range of 8.3 psig. The containment low-pressure signal is actuated when the containment pressure is reduced to approximately atmospheric pressure after either a high containment pressure or high-high containment pressure signal.

The high containment pressure signal allows for a reactor shutdown without initiation of the spray system. This signal generates a safety injection signal. The high containment pressure signal also closes trip valves located in normally operating systems penetrating the containment that are not required to control the reactor coolant system pressure and containment pressure rise (Table 7.5-2).

The high-high containment pressure signal, indicating a LOCA, initiates the spray system and completes the containment isolation by actuating the remaining isolation trip valves.

The containment low-pressure signal indicates a return of the containment pressure to approximately atmospheric, and allows manual reset of the control circuits of the consequence limiting safeguards system.

Four pressure channels are connected to operate on a three-out-of-four basis, and are designed to operate on pressure increase. Each pressure channel sends a signal to two sets of redundant matrices, one set for the high containment pressure point and the other set for the high-high containment pressure point. Each of the two matrices in the high containment pressure matrix set sends a backup signal to initiate a safety injection, which in turn de-energizes the containment vacuum pumps and trips containment isolation valves. Each of the two redundant matrices in the high-high containment pressure matrix set operates one containment spray subsystem, one recirculation spray subsystem, trips containment isolation valves, and sends a backup signal to the electrical circuit that is normally actuated by one of the two redundant high containment pressure matrices. When three out of four signals of the correct value are received simultaneously from the pressure channels by a matrix, an initiation signal (either a high containment pressure signal or a high-high containment pressure signal) is emitted accordingly. When two out of four signals are received simultaneously from the pressure channels by a matrix indicating a return to low containment pressure, the initiation signal emitted by that matrix is canceled and the electrical circuit controlling the components operated by the matrix can be manually reset. The pressure channels are connected to the open taps of the leakage monitoring system outside the containment at a point before the pressure monitoring instrument (Section 5.3.2), and the containment isolation trip valves.

The safeguards design provides physically separated redundant components, and a capability to test devices used to derive a final output signal, in accordance with IEEE-279 requirements.

7.5.1.3 **Spray Subsystems**

Each redundant high-high containment pressure matrix emits a signal that actuates an electrical control circuit that operates one of the two redundant containment spray trains, and two of the four redundant recirculation spray trains. Each signal opens the appropriate motor-operated valves and starts a containment spray pump by supplying power to the electric motor for the pump.

In the case of the Unit 1 recirculation spray system, each control circuit starts an inside recirculation spray pump two minutes after the actuating signal, and an outside recirculation spray pump five minutes after the actuating signal. The delays for starting the recirculation spray pumps ensure that, in the event of a small pipe rupture, sufficient water for recirculation is available in the containment sump.

In the case of the Unit 2 recirculation spray system, each CLS Hi Hi actuation circuit in conjunction with a RWST low level signal immediately starts an inside recirculation spray pump and initiates a two minute delayed start of the outside recirculation spray pump. The delay for starting the outside recirculation spray pump is sufficient to avoid overloading the EDG with high starting loads from two RS pumps.

The containment spray pumps may be stopped manually, after the control circuit controlling the pump has been manually reset. The control circuit can only be reset after a containment low-pressure signal is activated. Containment spray flow status is provided to the plant NUREG-0696 MUX system for remote display in the control room and other locations.

The recirculation spray system can also be stopped manually. The inside recirculation spray pumps can be stopped after the respective control circuits have been manually reset following a containment low-pressure signal. The outside recirculation spray pumps can be stopped at any time. This ability is necessary to control possible leakage in the suction and discharge piping (Section 6.3).

7.5.1.4 **Containment Vacuum System**

7.5.1.4.1 Normal Operation

The control system for the vacuum pumps compares an input signal of the containment air partial pressure with the actual containment air partial pressure, and provides for starting of the mechanical vacuum pumps if the actual containment air partial pressure is 0.1 psia greater than the desired input value. The containment air partial pressure may be varied between 9 and 10.3 psia depending upon the capability of the engineered safeguards to depressurize the containment within 60 minutes after a design-basis accident. Two redundant control channels are provided to operate the containment vacuum pumps. Each vacuum pump is operated through a three-position HAND-OFF-AUTO switch to permit either manual or automatic vacuum pump start. Either redundant control channel can actuate either containment vacuum pump. If the switch is in the OFF position, and the containment air partial pressure is greater than 0.1 psia above the setpoint, an alarm will alert the operator in the control room to manually start a vacuum pump, using the HAND position of the switch. If the switch is in the AUTO position, the alarm is received and a vacuum pump starts automatically. The actual partial pressure of air in the containment is not measured, but is obtained by subtracting the partial water vapor pressure signal from the containment total pressure signal.

The total containment pressure signal is measured in each channel by a pressure transmitter that transmits a signal functionally related to the actual containment total pressure. The partial water vapor pressure in the containment is derived by locating resistance temperature detectors, one for each channel, at the cooling coil outlet in each of three transition duct sections in the containment air recirculation system. The temperature measured in each transition duct is virtually saturated, and the sensed temperature is essentially the dewpoint temperature. The three temperature signals in each channel are transmitted to an auctioneer unit associated with the same channel, which selects the lowest temperature (lowest water vapor partial pressure condition). The temperature signal from the auctioneer in each channel is transmitted to an instrument that relates the temperature reading to a corresponding water vapor pressure, and transmits a signal functionally related to the water vapor partial pressure. The water vapor partial pressure signal and the total air pressure signal in each channel are sent to an instrument that subtracts the vapor partial pressure from the total air pressure, and transmits a signal functionally related to the partial air pressure. The value of partial air pressure desired in the containment is set on an instrument common to both channels and containing an adjustable setpoint mechanism, which transmits a signal functionally related to the desired partial pressure of air. The desired partial air pressure signal from the common instrument and the actual partial air pressure of each channel are compared. To eliminate the possibility of two different setpoints, a common instrument is used to set the desired partial air pressure in both channels.

When the actual containment air partial pressure increases 0.1 psia above the desired value, either channel of the control system energizes an electrical circuit that either sounds an alarm to signal the operator in the control room to manually start and operate a mechanical vacuum pump, or sounds the alarm and initiates starting and operating one mechanical vacuum pump directly, depending on the setting of the three-position switch in the control system. If the containment air partial pressure continues to increase, an alarm indicating that containment pressure is still rising is actuated. This alarm sounds when the partial containment air pressure has increased 0.20 psia above the desired containment air partial pressure. When the alarm is sounded in the control room, the operator initiates an orderly reactor shutdown in accordance with Technical Specifications.

When the actual containment air partial pressure falls 0.1 psia below the desired containment air partial pressure, the mechanical vacuum pump stops. If the pump does not stop, an alarm sounds.

The high-capacity steam jet air ejector is used to evacuate the containment before plant start-ups, and at other times is secured by administrative control.

7.5.1.4.2 Off-Normal Operation

The containment vacuum pumps are manually or automatically started in the event of a small rupture in the reactor coolant system piping. When the containment air partial pressure is 0.1 psia greater than the desired value, a containment vacuum pump automatically starts, or an

alarm signals the operator to manually start a containment vacuum pump, depending on the setting of the three-position switch in the control system.

A small rupture in the reactor coolant piping will cause an increase in the vapor partial pressure in the containment, due to the mass of vapor added to the containment atmosphere by the flashed reactor coolant. Total pressure of the containment atmosphere will be further increased due to the heating of air in the containment resulting from energy released from the flashing reactor coolant in addition to the increase caused by the vapor partial pressure. The result is that total pressure will increase more rapidly than vapor pressure, which would be interpreted as an increase in the containment air partial pressure by the instrumentation provided to perform this calculation. Several measurements, as described in Section 7.5.1.4.1 are made to determine the air partial pressure. They are recorded in the control room.

An increase in temperature measured in each transition duct, and the vapor partial pressure derived from these temperature readings when the vacuum pump is started, could indicate a small rupture in the coolant system or main steam system within the containment. The operator would then take steps to determine the location of the leak, isolate it, and shut down the vacuum pump as required.

The option to operate the containment vacuum pumps automatically is provided in keeping with the overall plant concept of automatic control, since automatic operation of these pumps would not result in an excessive or uncontrolled release of radioactivity.

Alarms are provided to signal that pump operation is required and to signal that the containment pressure has continued to rise with a vacuum pump in operation. The only difference between the manual and automatic mode of operation is that, in the automatic mode, the vacuum pump automatically starts at the same time an alarm is sounded to signal that pump operation is required, whereas, in the manual mode, the pump must be started by the operator when the alarm sounds. In addition, in the automatic mode, the vacuum pump is shut down automatically if the containment air partial pressure continues to rise.

The alarm that signals that the containment pressure is still rising while the vacuum pump is operating is provided for both the manual and the automatic modes of operation. In the manual mode, the operator immediately takes over pump operation manually, determines the cause of the continual pressure rise in the containment, shuts off the vacuum pump if necessary, and also, if necessary, begins to initiate an orderly reactor shut down. In the automatic mode, the vacuum pump is automatically shut down when this alarm is initiated. Since this alarm and trip are set at 0.10 psia above the pressure that signals that pump operation is required (0.20 psia above the desired setpoint), the amount of radioactivity that will be released, even with a small rupture in the reactor coolant piping and with automatic pump operation, will be minor, since this incremental pressure increase will occur in a short period of time.

In addition to the alarms and trips described above, the containment vacuum pumps are disconnected from the automatic control circuits on actuation of a safety injection signal, i.e., the

vacuum pumps receive a signal to shut down and the vacuum system isolation valve solenoids are de-energized.

The following information is HISTORICAL and is not intended or expected to be updated for the life of the plant.

The following discussion was the response to a request from the NRC during initial licensing to analyze the expected radioactive release from the containment in the event of a DBA and a small rupture in the reactor coolant system piping. Although the X/Q value used in the discussion is non-conservative compared to current standards, this analysis is considered bounded by the current large break LOCA dose analysis.

A small rupture in the reactor coolant system piping, assumed to be equivalent to a 2.6-inch-inside-diameter pipe, will cause the containment pressure to reach the high-pressure value in approximately four minutes. If the containment vacuum pumps are operating during the four-minute period before the pumps are de-energized and the isolation valves tripped, i.e., if the operator did not consider pump shutdown necessary when the alarm sounded to indicate continual containment pressure rise, then the expected radioactive release from the containment will be 0.288 Ci of Xe-133 equivalent and 0.00058 Ci of I-131 equivalent. This activity release is based on 1% failed fuel and equilibrium corrosion products in the reactor coolant. An unfiltered, uncontrolled release of this activity from the containment, χ/Q of 8×10^{-4} sec/m^3, and the assumption of a "puff" ground release, will result in a whole-body dose at the exclusion boundary of 0.01 mrem and a thyroid dose of about 0.25 mrem, both well below the limits suggested in 10 CFR 100. This incident is therefore not considered to be a hazard to the public.

The vacuum pump discharge passes through charcoal and particulate filters and the radiation monitors of the waste gas system before entering the environment. The particulate and charcoal filters further reduce the activity released. In addition, activity released to the environment in excess of the limits of 10 CFR 20 will be terminated by radiation monitors, which isolate the discharge of the containment vacuum pumps on high activity levels.

In the event of a design-basis accident as the containment pressure rises, the vacuum pumps will be automatically de-energized when the pressure increases to 0.20 psia above the setpoint. The vacuum pumps receive additional trip signals directly from a safety injection signal and indirectly from high containment pressure to ensure that the pumps are shut down. Therefore, the radioactive releases from the containment through the vacuum pump flow path will be negligible.

7.5.1.5 **Containment Isolation**

The containment isolation system is described in Section 5.2. The containment isolation system is designed to actuate and stroke the isolation valves completely closed to seal off the containment from the outside atmosphere when the pressure inside the containment reaches a predetermined setpoint.

The isolation trip valves are actuated by the safety injection system, the high containment pressure signal, or the high-high containment pressure signal, according to the functions of the line in which the trip valve is located (see Table 5.2-1). When the pressure setpoints are reached, each matrix operates electrical circuits to actuate electrically operated isolation valves directly, or to de-energize solenoid valves that release air from the diaphragm of pneumatically operated valves. Where two containment isolation trip valves are located on the same line, each trip valve is operated by a different redundant matrix. In lines containing only one trip valve, the trip valve is operated by both redundant matrices. However, lines containing one automatic trip valve have another isolation barrier, such as a check valve or a membrane barrier. All instruments, controls, and electrical equipment are supplied in accordance with ANSI, IEEE, and NEMA standards.

7.5.2 System Description

7.5.2.1 Engineered Safeguards Actuation Instrumentation

The engineered safeguards system actuation circuitry and hardware layout are designed to maintain channel isolation up to and including the bi-stable-operated logic relay similar to that of the reactor protection circuitry, as discussed in Section 7.2. The general arrangement of this layout is shown in Figure 7.5-4, with supplemental detailing in Figures 7.5-5 and 7.5-6. Although a four-channel system is illustrated in Figure 7.5-4, circuitry and hardware layout discussion is sufficiently general to apply to an n-channel system. Channel separation is maintained by providing separate racks for each analog protection channel, and separate relay rack compartments for each logic train. Channel identity is lost in the relay wiring required for matrix logic makeup. It should be noted that although channel individualization is lost, twin matrix logic trains are developed, thus ensuring a redundant actuation system.

The engineered safeguards system bi-stables drive the logic relay coils “C” and “D” as shown in Figures 7.5-4 and 7.5-6. These logic relay coils are de-energized by their bi-stables when an abnormal condition exists; the only exceptions to this “de-energized to operate” principle are the initiation of containment spray on CLS Hi Hi and the initiation of RWST recirculation mode transfer (RMT). Contacts of the relay are arranged so as to develop the logic matrix or combinations of signals required to initiate action. For example, in Figure 7.5-4 these relay contacts are shown directly below the relay coil. Since these coils would normally be energized, their contacts would remain open, and thus an open circuit between the voltage source and master actuating relay would exist. Dropping any of the two logic relay coils that would cause their corresponding contacts to close would complete the circuit and energize the master actuating relays. Although the illustration here is for a two-out-of-four (2/4) matrix make, the design and sequence of operation for (x_1/x_2) logic matrices makeup is the same. The master actuating relay (M) is a latch-type relay with two coils, an operate (M/0) and reset (M/R) coil, and electric reset. Once the logic matrix is made up, as described above, the circuit that energizes the master actuating relay is complete. Figure 7.5-4 illustrates the master actuating relay, and an enlarged view may be found in Figure 7.5-5. With a potential across the relay, the operate coil is energized, thus closing the M contacts, which energizes the slave relays (SRs and TD) as shown in

Figure 7.5-4; the master relay is latched into this position until the reset coil is energized. Manual reset of the master actuating relay may be accomplished, after a time delay following its operation to ensure completion of the actuation sequence, by operating the reset switch (see Figures 7.5-4 and 7.5-5). With the reset coil energized, all of the M contacts are returned to their de-energized positions, as shown in Figure 7.5-4. It should be noted that once reset action is taken, the master relay operation is blocked by the reset relay R until the safeguards initiating signal clears, at which time it is automatically unblocked and restored to service. Resetting the master relay does not interfere with the operational status of the engineered safeguards equipment.

Annunciation is provided for the consequence-limiting-safeguards-initiated signal, the consequence-limiting-safeguards-reset-permissive signal, the safety-injection-initiated signal, and the safety-injection-blocked signal.

7.5.2.2 **Instrumentation Used During a Loss-of-Coolant Accident**

Instruments provided and designed to function following the major LOCA are those that govern the operation of engineered safeguards. Pressurizer pressure and level, and steam generator flow, and level sensors are located inside the containment because an equivalent signal cannot be obtained from a sensor location more isolated from the reactor. Steam generator pressure sensors are located outside the containment. It should be emphasized, however, that for the large LOCAs the initial suppression of the transient is independent of any detection or actuation signal because the water level will be restored to the core by the passive accumulator system.

Pumps used for safety injection and initial containment spray are located outside the containment. The operation of the equipment can be verified by instrumentation that reads in the control room. This instrumentation will not be affected by the accident. The containment sump level and refueling water storage tank instrumentation will provide information for evaluating the conditions necessary to initiate the recirculation mode of operation.

The containment level instrumentation has been changed to meet the requirements of TMI-2, NUREG-0578, Section 2.1.9. The system now utilizes redundant wide range level transmitters and redundant narrow range transmitters installed inside the reactor containment. The transmitters are qualified to IEEE-323-1974 and IEEE-344-1975 standards.

The wide-range level loops have the capability of measuring a level in the containment equivalent to approximately 580,000 gallon capacity and the narrow-range level loops have the capability of measuring to the top of the containment sump.

One of the redundant loops for wide-range level and one of the loops for narrow-range level is recorded on the postaccident monitoring recorder in the control room. The second redundant loop for both wide and narrow-range level can be real-time plotted through the PCS Emergency Response and Safety Parameter (ERG/SPDS) displays in the MCR, Technical Support Center and other locations.

Instrumentation has been added to monitor containment spray flow and backup pressurizer heater status during and following an accident. Containment spray flow instrumentation will provide a direct means for the Control Room operator to determine if containment spray flow is being provided. Likewise, pressurizer heater status will provide a direct means for the Control Room operator to determine satisfactory operation of the pressurizer heaters. Both containment spray flow and pressurizer heater status provide input to the plant NUREG-0696 MUX system for remote display in the Control Room and other locations.

Wide-range pressure transmitters have been added outside containment to measure containment pressure as described in Section 7.5.3.5.

Depending upon the magnitude of the loss-of-coolant incident, information relative to the pressure of the reactor coolant system will be useful to the operator to determine when it would be permissible to stop one of two LHSI pumps in the event of a small break. Regulatory Guide 1.97 reactor coolant system instrumentation as well as the discharge pressure of the charging pumps, as read on instrumentation outside the containment, will serve this purpose.

Consideration has been given to all the instrumentation and information that is necessary for recovery following a loss-of-coolant incident. Instrumentation external to the reactor containment, such as radioactivity monitoring equipment, will not be affected by this postulated incident, and will be available to the operator.

Safety-related postaccident monitoring panels for Units 1 and 2 have been installed in the control room, in response to NUREG-0578, Sections 2.1.5a, 2.1.6b, and 2.1.9. The panels are designed to IEEE 344-1975 and the original plant separation criteria. The components have been designed to meet, as a minimum, IEEE 323-1971. The panel contains switches and indicators for equipment such as containment isolation valves, RCS vent valves, and postaccident hydrogen indicators.

7.5.2.3 **Calibration and Testing**

The engineered safeguards actuation channels are designed with sufficient redundancy to provide the capability for channel calibration and test during power operation. Bypass removal of one actuation channel is accomplished by placing that channel in a tripped mode; i.e., a two-out-of-three matrix logic becomes a one-out-of-two matrix logic. Testing does not trip the system unless a trip condition occurs in a concurrent channel.

7.5.2.3.1 Analog Channel Testing

Engineered safeguards analog channel testing is identical to process analog protection channel testing as described in Section 7.2.2.1.4.

7.5.2.3.2 Logic Testing

Figures 7.5-4, 7.5-5, and 7.5-6 illustrate the basic logic test scheme. Test switches are located in the associated relay racks rather than in a single test panel. The following procedures indicate the method of testing the logic matrices:

1. Test of either train A or train B is made at one time; this is under administrative control.
2. A selection of the function to be tested is made. Figure 7.5-5, for example, illustrates some of these functional matrices.
3. The relay logic test switch is first turned to the test position, which opens the circuit to the master actuating relay (logic test switches as shown in Figure 7.5-5 or location 1 as shown in Figures 7.5-4 or 7.5-6) and energizes the "on test" labeled lamp (see position 3 of switch C_1 or D_1 in Figure 7.5-6).

   The master actuating relay is removed from this part of the test in order to avoid unintentional starting of the engineered safeguards equipment. Intentional start is available through the other train that has operational status and the other functional matrices not under test.
4. When the logic test switch is depressed in the test position, the circuit that normally energizes the logic relay coil is de-energized, thus closing the logic relay contacts operated by that coil (i.e., opening of C_1 at location 2 shown in Figure 7.5-4 or 7.5-6 will close the two logic relay contacts directly below C_1 in Figure 7.5-4). By repeating the above sequence for C_2, C_3, C_4, one can simulate all actuating logic combinations required to make up the logic required to develop the matrix. Thus, in Figure 7.5-4, a complete test of a two-out-of-four matrix is made with the following combinations: C_1 and C_2, C_1 and C_3, C_1 and C_4, C_2 and C_3, C_2 and C_4, and C_3 and C_4.
5. Proper development of a logic matrix would be indicated by the lighting of the matrix test lamps, as shown in Figure 7.5-5, and identified in Figure 7.5-6 as L_2.
6. With the testing of the logic matrix complete (i.e., steps 1 to 5), the matrix is returned to operational status by returning all test switches for that particular functional matrix to the "operate" position. The control board annunciator warns the operator of any test switch left in the test position, and thus the return to operational status through the action of the individual performing the test is verified by the operator at the control board. Testing procedures for the logic matrix of train B are identical to those described above for train A.
7. Verification of master actuating coil integrity is made by connecting an ohmmeter across the coil terminals.
8. Verification of slave coil integrity can be checked by connecting an ohmmeter across the coil terminals.

7.5.3 System Evaluation

Redundant instrumentation has been provided for all inputs to the protective systems and vital control circuits. Where wide process variable ranges and precise control are required, both wide-range and narrow-range instrumentation is provided. Instrumentation components are selected from standard commercially available products with proven operating reliability. The instrument power to electrical and electronic instrumentation required for safe and reliable operation is supplied from the four instrument buses.

The engineered safeguards systems are arranged so that there are multiple, separate, and independent pumping paths for delivering and circulating borated water to the reactor coolant system and to the spray system. This philosophy of multiplicity, separation, and independence has been extended to include the power sources as well as the signal sources, cabling, relays, etc., required for system actuation.

7.5.3.1 Safety Injection

Credible accident conditions requiring emergency core cooling would involve low pressurizer pressure and level. The present design for emergency core cooling is accomplished by the safety injection system actuation from primary system variables. Actuation is initiated by low-low-pressurizer pressure.

Pressurizer pressure is sensed by fast response pressure transmitters. An overall one-second channel response time is used, which is more than adequate to cover the response characteristics of the tripping channels.

Instrument delays are small in comparison with the computed lag in pressurizer pressure, which lags behind the reactor coolant pressure during blowdown. The successful operation of the engineered safeguards involves only actuation control function, with the single exception of the steam generator water level control function associated with unit cooldown using the auxiliary feedwater pump.

A safety injection block switch is provided to permit the primary system to be depressurized and its water level lowered for maintenance or refueling operations without actuation of the safety injection system. This manual block switch is interlocked with pressurizer pressure in such a way that the blocking action is automatically removed as operating pressure is approached. If two out of three pressure signals are above this preset pressure, blocking action cannot be initiated. The block condition is annunciated in the control room.

7.5.3.2 Consequence Limiting Safeguards

The design of the control system for the consequence limiting safeguards includes manual test switches for individual testing of all equipment in the system and for testing the system itself.

The containment vacuum control system, which starts and operates the mechanical vacuum pumps and the alarms, has adjustable setpoint mechanisms that allow the operator to change the

setpoint value as required due to atmospheric conditions or experience gained in operating the plant.

7.5.3.3 Containment Isolation System

The system design offers a reliable and safe method for achieving the design-basis objectives.

Reliability in this system is ensured by the ability to calibrate and test each pressure-sensing device and monitor each manual reset relay during plant operation without removal from the system.

A fail-safe design is provided. On loss of air or control power, the pneumatically and solenoid-operated isolation valves close.

The three features that ensure the proper operation of this system are the location of pressure-sensing devices outside containment, continuous monitoring of valve positions, and indication of the availability of control power on the main control board.

The electrical circuits have manual reset relays, and each solenoid valve has a manual reset pushbutton designed to prevent accidental reopening of any isolation valve. The reset buttons on the control board must be set before the manual pushbutton on each solenoid valve can open any trip valve. As each pushbutton is reset, air is admitted through the solenoid valve to open the isolation valve. When all solenoid valves have been reset and isolation valves opened, tripping of the circuits can occur only if a trip signal initiates the action or the operator manually trips the relays in the control room.

See Section 5.2.2 for a discussion of the condenser air ejector discharge and vent system.

7.5.3.4 Motor and Valve Control

For starting pump and fan motors, the control relays are energized to energize the closing coil on the circuit-breaker of the motor-starter. When motor-starters are used, the starter operating coil is supplied by power from the same source as the subject motor. When circuit-breakers are used for motor control, the circuit-breakers close, and trip coils are supplied by power from a 125V dc battery bus, as outlined in Chapter 8.

For valve motor control, the control relay causes the coil on the main contactor for the closing circuit to be energized. The closing circuit is de-energized by the torque or limit switch on the valve operator, thereby ensuring that the valves have closed to a leak-tight position.

Air-actuated containment isolation valves are spring-loaded to close upon loss of air pressure.

An as-built tabulation of all valves and dampers actuated by engineered safeguards signals is provided in Table 7.5-2. The table includes component designation, service, safety function, signal source, and a statement of whether the safety function can be overridden or bypassed.

7.5.3.5 **Environmental Capability**

The engineered safeguards instrumentation equipment inside containment is designed to operate under the postaccident environment of a steam-air mixture and radiation.

Electrical equipment for the engineered safeguards is located inside the containment and in the auxiliary building. The equipment located inside the containment that must function in the postaccident environment is listed below. The expected length of time that the equipment will be required to function following an accident is also given.

1. Emergency core cooling system containment isolation actuation sensors (first five minutes after accident).
2. Emergency core cooling system motor-operated valves and flow instrumentation (first five minutes after accident).
3. Accumulator level instrumentation (first five minutes after accident).
4. Containment sump level instrumentation three hours after accident, which is considered to be the maximum period after a LOCA for emptying the refueling water storage tank into the sump, thereby ensuring that the sump is sufficiently filled for the recirculation phase.
5. Air-operated and motor-operated containment isolation valves (operation completed in first five minutes after accident).
6. Containment pressure instrumentation (continuous service).
7. Power and instrumentation cables for the above-listed equipment.

The design considerations and specifications to be used in the selection of motors that must function in the postaccident environment are discussed in Chapter 6. Similar application criteria apply to the specifications of control and instrumentation equipment and other electrical equipment.

Failure of the above equipment after the specific time will not increase the severity or consequences of the accident. The reactor protection control and instrumentation equipment and electrical equipment for engineered safeguards located in the Auxiliary Building will operate in a normal ambient environment following a LOCA. Auxiliary Building equipment in the containment sump-water recirculation loop is listed below:

1. Safety injection/charging lines and charging pumps.
2. Flow, temperature, and pressure instrumentation for the safety injection/charging system.
3. Power and instrument cables for the above.

Areas of high radiation would exist inside the containment and in those portions of the auxiliary building near safety injection/charging system equipment following a major LOCA. The maximum intregrated six-month LOCA dose in the containment would be approximately 3.7×10^7 rads. The maximum intregrated six-month LOCA dose plus sixty year normal operation dose in the charging cubical (lower elevation) of the Auxiliary Building would be approximately 1.2×10^7 rads. The ability of electrical equipment in the emergency core cooling system to withstand radiation exposure would be limited by radiation effects on electrical insulation materials and motor bearing lubrication.

The electrical equipment for the emergency core cooling system located in the containment use only radiation-resistant insulating materials. These insulating materials have a threshold for radiation damage that might affect their function of 10^8 rad or higher. They therefore provide considerable margin above the maximum postaccident radiation dose that would result from the exposure times specified above.

The lower ambient temperatures and radiation levels in the auxiliary building permit the use of normal elastomer or plastic insulation materials. These materials have a threshold for radiation damage of 10^6 rad or higher. Where required, because of location in possible high-radiation areas, motor bearings are lubricated with radiation-rated lubricants.

The pressure sensors that monitor containment conditions subsequent to a LOCA are capable of indicating pressures from 0 psia to 65 psia. The temperature sensors that monitor containment conditions subsequent to a LOCA are capable of indicating temperatures from 40°F to 400°F. The pressure and temperature sensors that monitor containment conditions subsequent to a LOCA are capable of indicating conditions more severe than those associated with the design basis of the containment. The pressure and temperature conditions for the design basis of the containment are 45 psig and 280°F.

The requirements of TMI-2 Short Term Lessons Learned, NUREG-0578 and subsequent clarifications contained in the NRC letter dated October 30, 1979, required that there be a continuous indication of containment pressure provided in the control room with an indication capability to three times the containment design pressure. As a result, redundant Class 1E pressure transmitters were added to the existing containment pressure measuring tubing with the capability of measuring a pressure range of 0 to 180 psia. The pressure transmitters are qualified to IEEE 323-1971 and IEEE 344-1975.

Each transmitter has an indicator associated with it. These indicators are mounted on the main control board and provide continuous indication of the containment pressure over the range of 0 to 180 psia. One of the redundant loops for the containment pressure measurement is recorded in the control room on the postaccident monitoring recorder. The second redundant loop can be real-time plotted through the PCS ERG/SPDS displays in the MCR, Technical Support Center, and other locations.

7.5.3.5.1 Environmental Qualification of Safety-Related Electrical Equipment

In response to IE Bulletin 79-01B, a program was established to review the environmental qualification of safety-related electrical equipment located inside the containment. Later, a supplement to IE Bulletin 79-01B was issued and further defined the scope of the review to include not only equipment inside the containment, but also equipment in areas of the plant where changing environmental conditions (temperature, pressure, humidity, radiation) occur during and as a result of the accident conditions being reviewed.

The IE Bulletin 79-01B review was submitted in two separate parts. The 45-day review (Reference 1), reflected equipment qualifications to FSAR commitments. The review included a list of safety-related systems that are required to achieve or support (1) emergency reactor shutdown, (2) containment isolation, (3) reactor core cooling, (4) containment heat removal, (5) core residual heat removal, and (6) prevention of significant release of radioactive material to the environment. This list is included on Table 7.5-3. Equipment identified as requiring a review were analyzed for conditions of temperature, pressure and humidity inside and outside the containment, and for submergence, aging, chemical spray, and radiation.

Revision 4 to the 90-day review (Reference 2), was also submitted. It included a list of electrical equipment required to mitigate an accident and/or safely shut down the plant and that are subjected to a changing environment due to the accidents. The report reflects the updated Status of Qualification of the electrical equipment. Results of the NRC's safety evaluation for the environmental qualification of safety-related equipment at the Surry Power Station are contained in Reference 3.

7.5 REFERENCES

1. Letter from Vepco to NRC, Subject: *45-Day Response to IE Bulletin 79-01B,* dated June 16, 1980 (Serial No. 527).

2. Letter from Vepco to NRC, Subject: *Response to Safety Evaluation Report for Environmental Qualification of Safety Related Electrical Equipment IE Bulletin 97-01B 90-Day Review (Revision 4 of 90-Day Response to IE Bulletin 79-01B),* dated August 24, 1981 (Serial No. 329).

3. Letter from S. A. Varga, NRC, to W. L. Stewart, Vepco, Subject: *Transmittal of the Safety Evaluation Report for Environmental Qualification of Safety-Related Equipment at Surry Power station, Unit Nos. 1 and 2,* dated January 26, 1983.

Table 7.5-1
ENGINEERED SAFEGUARDS ACTUATION FUNCTIONS

Actuation Signal	Coincidence Circuitry and Interlocks	Comments
I. Containment Isolation Actuation Function		
1. Hi CLS	Coincidence of 3/4 containment high pressure or 1/2 manual	Closes containment isolation valves for the following lines: instrumentation air suction supply line, radiation monitoring gas and particulate sample supply line, air ejector vent to containment line.
2. HiHi CLS	Coincidence of 3/4 containment high-high pressure or 2/2 manual	Closes containment isolation valves for the following systems: CC, IA, MS.
3. Safety injection actuation	Coincidence of 2/3 Low Low pressurizer pressure or 1/2 manual	Closes containment isolation valves for the following systems: CH, RC, BD, CC, CV, DA, DG, LM, SS, VG, SI (N2 supply), MS (drains).
II. Main Steam Lines Isolation Actuation Function		
1. Main steam line isolation	High steam line flow in 2 out of 3 lines (1/2 per line) coincident with either low T_{avg} in 2 out of 3 loops or low steam pressure in 2 out of 3 lines	Closes main steam line isolation valves.
2. Hi Hi CLS	3/4 high-high containment pressure signal or 2/2 manual	Closes main steam line isolation valves.
3. Manual per steam loop	1/1 per steam line	Closes main steam line isolation valves.
III. Auxiliary Feedwater Actuation Function		
1. Turbine driven pump start	Coincidence of 2/3 low-low level in any two steam-generators, or loss of power to station service busses; or manual 1/1, or AMSAC initiated	Starts turbine driven pump.
2. Motor-driven pumps start	2/3 low-low level in any steam-generator, or trip of both main feedwater pumps, or safety injection signal, or manual 1/1, or total loss of reserve station service power, or AMSAC initiated	Start motor driven pump.

Table 7.5-1 (continued)
ENGINEERED SAFEGUARDS ACTUATION FUNCTIONS

Actuation Signal	Coincidence Circuitry and Interlocks	Comments
IV. Main Feedwater Isolation Function		
1. Safety injection actuation	SI actuation	Close main feedwater control valves (fast closure).
2. Hi Hi steam generator level	2/3 high high level in steam generator	Close main feedwater control valves (fast closure).

Table 7.5-2
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-BD-TV-100A	Steam generator 1A blowdown inside cont isolation valve	Closed	SGLLWL	None
1-BD-TV-100B	Steam generator 1A blowdown outside cont isolation valve	Closed	SGLLWL	None
1-BD-TV-100C	Steam generator 1B blowdown inside cont isolation valve	Closed	SGLLWL	None
1-BD-TV-100D	Steam generator 1B blowdown outside cont isolation valve	Closed	SGLLWL	None
1-BD-TV-100E	Steam generator 1C blowdown inside cont isolation valve	Closed	SGLLWL	None
1-BD-TV-100F	Steam generator 1C blowdown outside cont isolation valve	Closed	SGLLWL	None
1-CC-TV-105A	RCP A CC water cooler outside cont isolation valve	Closed	CLS-HiHi	None
1-CC-TV-105B	RCP B CC water cooler outside cont isolation valve	Closed	CLS-HiHi	None
1-CC-TV-105C	RCP C CC water cooler outside cont isolation valve	Closed	CLS-HiHi	None
1-CC-TV-109A	CC water from RHR HX outside cont isolation valve	Closed	SI	None
1-CC-TV-109B	CC water from RHR HX outside cont isolation valve	Closed	SI	None
1-CC-TV-110A	Reactor cont recirc cooler A CC water outside cont isolation valve	Closed	CLS-HiHi	None
1-CC-TV-110B	Reactor cont recirc cooler B CC water outside cont isolation valve	Closed	CLS-HiHi	None
1-CC-TV-110C	Reactor cont recirc cooler C CC water outside cont isolation valve	Closed	CLS-HiHi	None
1-CC-TV-140A	RCP thermal barrier CC water inside isolation valve	Closed	CLS-HiHi	None
1-CC-TV-140B	RCP thermal barrier CC water outside isolation valve	Closed	CLS-HiHi	None
1-CH-HCV-1200A [a]	Letdown orifice isolation valve	Closed	SI	None

a. These circuits have features that could prevent immediate operation of the component when the engineered safeguards signal is actuated. Such features are a necessary part of the circuit (such as a limit switch), or they require conscious effort by an operator to prevent operation (such as manipulation of a pushbutton or a selector switch). A valve limit switch could act to delay safeguards-initiated operation if the valve was in mid-travel and had to complete the travel sequence before operating in response to the safeguards signal. A pushbutton or selector switch held in the actuated position gives the operators an option, in some cases, of delaying component response to an emergency safeguards signals.

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-CH-HCV-1200B [a]	Letdown orifice isolation valve	Closed	SI	None
1-CH-HCV-1200C [a]	Letdown orifice isolation valve	Closed	SI	None
1-CH-MOV-1115B [a]	RWST to charging pump suction isolation valve	Open	SI	None
1-CH-MOV-1115C [a]	VCT to charging pump suction isolation valve	Closed	SI	None
1-CH-MOV-1115D [a]	RWST to charging pump suction isolation valve	Open	SI	None
1-CH-MOV-1115E [a]	VCT to charging pump suction isolation valve	Closed	SI	None
1-CH-MOV-1289A [a]	Charging line to regenerative HX isolation valve	Closed	SI	None
1-CH-MOV-1289B [a]	Charging line to regenerative HX isolation valve	Closed	SI	None
1-CH-MOV-1381 [a]	RCP seal water return isolation valve	Closed	SI	None
1-CH-TV-1204A	Letdown line inside cont isolation valve	Closed	SI	None
1-CH-TV-1204B	Letdown line outside cont isolation valve	Closed	SI	None
1-CS-MOV-100A [a]	Cont spray pump A from RWST isolation valve	Open	CLS-HiHi	None
1-CS-MOV-100B [a]	Cont spray pump B from RWST isolation valve	Open	CLS-HiHi	None
1-CS-MOV-101A [a]	Cont spray pump A discharge isolation valve	Open	CLS-HiHi	None
1-CS-MOV-101B [a]	Cont spray pump A discharge isolation valve	Open	CLS-HiHi	None
1-CS-MOV-101C [a]	Cont spray pump B discharge isolation valve	Open	CLS-HiHi	None
1-CS-MOV-101D [a]	Cont spray pump B discharge isolation valve	Open	CLS-HiHi	None

a. These circuits have features that could prevent immediate operation of the component when the engineered safeguards signal is actuated. Such features are a necessary part of the circuit (such as a limit switch), or they require conscious effort by an operator to prevent operation (such as manipulation of a pushbutton or a selector switch). A valve limit switch could act to delay safeguards-initiated operation if the valve was in mid-travel and had to complete the travel sequence before operating in response to the safeguards signal. A pushbutton or selector switch held in the actuated position gives the operators an option, in some cases, of delaying component response to an emergency safeguards signals.

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-CS-MOV-102A [a]	Cont spray chem add tank isolation valve	Open	CLS-HiHi	None
1-CS-MOV-102B [a]	Cont spray chem add tank isolation valve	Open	CLS-HiHi	None
1-CV-TV-150A	Cont vacuum pump B outside cont isolation valve	Closed	SI	None
1-CV-TV-150B	Cont vacuum pump B outside cont isolation valve	Closed	SI	None
1-CV-TV-150C	Cont vacuum pump A outside cont isolation valve	Closed	SI	None
1-CV-TV-150D	Cont vacuum pump A outside cont isolation valve	Closed	SI	None
1-CW-MOV-100A [a]	Circ water condenser outlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-100B [a]	Circ water condenser outlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-100C [a]	Circ water condenser outlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-100D [a]	Circ water condenser outlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-106A [a]	Circ water condenser inlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-106B [a]	Circ water condenser inlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-106C [a]	Circ water condenser inlet isolation valve	Closed	CLS-HiHi *	None
1-CW-MOV-106D [a]	Circ water condenser inlet isolation valve	Closed	CLS-HiHi *	None
1-DA-TV-100A	Reactor cont sump pump inside containment isolation valve	Closed	SI	None
1-DA-TV-100B	Reactor cont sump pump outside containment isolation valve	Closed	SI	None
1-DA-TV-103A	Post accident SS return to cont sump outside cont isolation valve	Closed	SI	None

a. These circuits have features that could prevent immediate operation of the component when the engineered safeguards signal is actuated. Such features are a necessary part of the circuit (such as a limit switch), or they require conscious effort by an operator to prevent operation (such as manipulation of a pushbutton or a selector switch). A valve limit switch could act to delay safeguards-initiated operation if the valve was in mid-travel and had to complete the travel sequence before operating in response to the safeguards signal. A pushbutton or selector switch held in the actuated position gives the operators an option, in some cases, of delaying component response to an emergency safeguards signals.

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-DA-TV-103B	Post accident SS return to cont sump outside cont isolation valve	Closed	SI	None
1-DG-TV-108A	Primary drain transfer pump inside containment isolation valve	Closed	SI	None
1-DG-TV-108B	Primary drain transfer pump outside containment isolation valve	Closed	SI	None
1-IA-TV-100	Cont instr air discharge outside cont isolation valve	Closed	CLS-HiHi	None
1-IA-TV-101A	Cont instr air supply inside cont isolation valve	Closed	CLS-Hi	None
1-IA-TV-101B	Cont instr air inside cont isolation valve	Closed	CLS-Hi	None
1-LM-TV-100A	Leakage monitoring tap outside cont isolation valve	Closed	SI	None
1-LM-TV-100B	Leakage monitoring tap outside cont isolation valve	Closed	SI	None
1-LM-TV-100C	Leakage monitoring tap outside cont isolation valve	Closed	SI	None
1-LM-TV-100D	Leakage monitoring tap outside cont isolation valve	Closed	SI	None
1-LM-TV-100E	Leakage monitoring tap 4, 7, 9, 10 outside cont isolation valve	Closed	SI	None
1-LM-TV-100F	Leakage monitoring tap 4, 7, 9, 10 outside cont isolation valve	Closed	SI	None
1-LM-TV-100G	Leakage monitoring tap 2, 5 outside cont isolation valve	Closed	SI	None
1-LM-TV-100H	Leakage monitoring tap 2, 5 outside cont isolation valve	Closed	SI	None
1-MS-TV-101A	Main steam line A isolation valve	Closed	CLS-HiHi	None
1-MS-TV-101B	Main steam line B isolation valve	Closed	CLS-HiHi	None
1-MS-TV-101C	Main steam line C isolation valve	Closed	CLS-HiHi	None
1-MS-TV-109	Main steam drain condensate drain isolation valve	Closed	SI	None
1-MS-TV-110	Main steam drain condensate drain isolation valve	Closed	SI	None
1-RC-TV-1519A	PG water to pzr relief tank - outside cont isolation valve	Closed	SI	None
1-RM-TV-100A	RM gas part supply outside cont isolation valve	Closed	CLS-Hi	None
1-RM-TV-100B	RM gas part supply outside cont isolation valve	Closed	CLS-Hi	None

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-RM-TV-100C	RM gas part supply inside cont isolation valve	Closed	CLS-Hi	None
1-RS-MOV-155A [a]	Outside recirc spray pump A suction isolation valve	Open	CLS-HiHi	None
1-RS-MOV-155B [a]	Outside recirc spray pump B suction isolation valve	Open	CLS-HiHi	None
1-RS-MOV-156A [a]	Outside recirc spray pump A discharge isolation valve	Open	CLS-HiHi	None
1-RS-MOV-156B [a]	Outside recirc spray pump B discharge isolation valve	Open	CLS-HiHi	None
1-SI-MOV-1865A	Accumulator loop A discharge isolation valve	Open	SI	Key Switch [b]
1-SI-MOV-1865B	Accumulator loop B discharge isolation valve	Open	SI	Key Switch [b]
1-SI-MOV-1865C	Accumulator loop C discharge isolation valve	Open	SI	Key Switch [b]
1-SI-MOV-1867C [a]	High head SI to cold leg isolation valve	Open	SI	None
1-SI-MOV-1867D [a]	High head SI to cold leg isolation valve	Open	SI	None
1-SI-TV-100	Central nitrogen supply outside cont isolation valve	Closed	SI	None
1-SI-TV-101A	Accumulator nitrogen relief outside cont isolation valve	Closed	SI	None
1-SI-TV-101B	Accumulator nitrogen relief outside cont isolation valve	Closed	SI	None
1-SI-TV-102A	RWST cross tie to charging pump suction isolation valve	Open	SI	None
1-SI-TV-102B	RWST cross tie to charging pump suction isolation valve	Open	SI	None
1-SS-TV-100A	SS pzr liquid space inside cont isolation valve	Closed	SI	None

a. These circuits have features that could prevent immediate operation of the component when the engineered safeguards signal is actuated. Such features are a necessary part of the circuit (such as a limit switch), or they require conscious effort by an operator to prevent operation (such as manipulation of a pushbutton or a selector switch). A valve limit switch could act to delay safeguards-initiated operation if the valve was in mid-travel and had to complete the travel sequence before operating in response to the safeguards signal. A pushbutton or selector switch held in the actuated position gives the operators an option, in some cases, of delaying component response to an emergency safeguards signals.

b. A key-operated switch is under administrative control to prevent inadvertent component operation and to satisfy the requirements of IEEE Standard 279-1971.

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-SS-TV-100B	SS pzr liquid space outside cont isolation valve	Closed	SI	None
1-SS-TV-101A	SS pzr vapor space inside cont isolation valve	Closed	SI	None
1-SS-TV-101B	SS pzr vapor space outside cont isolation valve	Closed	SI	None
1-SS-TV-102A	SS primary coolant cold leg sample inside cont isolation valve	Closed	SI	None
1-SS-TV-102B	SS primary coolant cold leg sample outside cont isolation valve	Closed	SI	None
1-SS-TV-103A	SS RHR sample inside cont isolation valve	Closed	SI	None
1-SS-TV-103B	SS RHR sample outside cont isolation valve	Closed	SI	None
1-SS-TV-104A	SS pzr relief tank gas space sample inside cont isolation valve	Closed	SI	None
1-SS-TV-104B	SS pzr relief tank gas space sample outside cont isolation valve	Closed	SI	None
1-SS-TV-106A	SS primary coolant hot leg inside cont isolation valve	Closed	SI	None
1-SS-TV-106B	SS primary coolant hot leg outside cont isolation valve	Closed	SI	None
1-SV-TV-102	Air ejector vent to cont isolation valve	Closed	CLS-Hi	None
1-SV-TV-102A	Air ejector vent to cont outside isolation valve	Closed	SI	None
1-SW-MOV-101A [a]	SW to bearing cooling water Hx isolation valve	Closed	CLS-HiHi *	None
1-SW-MOV-101B [a]	SW to bearing cooling water Hx isolation valve	Closed	CLS-HiHi *	None
1-SW-MOV-102A [a]	SW to CC water HX isolation valve	Closed	CLS-HiHi *	None
1-SW-MOV-102B [a]	SW to CC water HX isolation valve	Closed	CLS-HiHi *	None

a. These circuits have features that could prevent immediate operation of the component when the engineered safeguards signal is actuated. Such features are a necessary part of the circuit (such as a limit switch), or they require conscious effort by an operator to prevent operation (such as manipulation of a pushbutton or a selector switch). A valve limit switch could act to delay safeguards-initiated operation if the valve was in mid-travel and had to complete the travel sequence before operating in response to the safeguards signal. A pushbutton or selector switch held in the actuated position gives the operators an option, in some cases, of delaying component response to an emergency safeguards signals.

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-SW-MOV-103A [a]	SW to recirc spray HX (A, D) isolation valve	Open	CLS-HiHi	None
1-SW-MOV-103B [a]	SW to recirc spray HX (A, D) isolation valve	Open	CLS-HiHi	None
1-SW-MOV-103C [a]	SW to recirc spray HX (B, C) isolation valve	Open	CLS-HiHi	None
1-SW-MOV-103D [a]	SW to recirc spray HX (B, C) isolation valve	Open	CLS-HiHi	None
1-SW-MOV-104A [a]	SW to recirc spray HX A inlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-104B [a]	SW to recirc spray HX B inlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-104C [a]	SW to recirc spray HX C inlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-104D [a]	SW to recirc spray HX D inlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-105A [a]	SW to recirc spray HX A outlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-105B [a]	SW to recirc spray HX B outlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-105C [a]	SW to recirc spray HX C outlet isolation valve	Open	CLS-HiHi	None
1-SW-MOV-105D [a]	SW to recirc spray HX D outlet isolation valve	Open	CLS-HiHi	None
1-VG-TV-109A	Primary drains tank vent inside cont isolation valve	Closed	SI	None
1-VG-TV-109B	Primary drains tank vent outside cont isolation valve	Closed	SI	None
1-VS-AOD-101A	Fuel bldg supply fan damper to HEPA emergency filter	Closed	SI	Mode Switch [c]
1-VS-AOD-101B	Fuel bldg supply fan damper to HEPA emergency filter	Closed	SI	Mode Switch [c]
1-VS-AOD-102	Fuel bldg exhaust fans to vent stack	Closed	SI	None

a. These circuits have features that could prevent immediate operation of the component when the engineered safeguards signal is actuated. Such features are a necessary part of the circuit (such as a limit switch), or they require conscious effort by an operator to prevent operation (such as manipulation of a pushbutton or a selector switch). A valve limit switch could act to delay safeguards-initiated operation if the valve was in mid-travel and had to complete the travel sequence before operating in response to the safeguards signal. A pushbutton or selector switch held in the actuated position gives the operators an option, in some cases, of delaying component response to an emergency safeguards signals.

c. A mode switch is under administrative control to prevent inadvertent alignment of this damper during refueling (Section 9.13.4.1).

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-VS-AOD-103A	Decon bldg fan discharge damper to emergency filter	Closed	SI	None
1-VS-AOD-103B	Decon bldg fan discharge damper to emergency filter	Closed	SI	None
1-VS-AOD-104	Decon bldg damper to decon bldg exhaust fans	Closed	SI	None
1-VS-AOD-105A	Unit 1 cont air compressor damper to HEPA emergency filter	Closed	SI	None
1-VS-AOD-105B	Unit 1 cont air compressor damper to HEPA emergency filter	Closed	SI	None
1-VS-AOD-107A	Aux bldg central exhaust fan damper to HEPA emergency filter	Open	SI	Mode Switch [c]
1-VS-AOD-107B	Aux bldg central exhaust fan damper to HEPA emergency filter	Open	SI	Mode Switch [c]
1-VS-AOD-108	Aux bldg central exhaust fan damper to vent stack	Closed	SI	Mode Switch [c]
1-VS-AOD-109A	Aux bldg general area exhaust fans damper	Closed	SI	None
1-VS-AOD-109B	Aux bldg general area exhaust fans damper	Closed	SI	None
1-VS-AOD-110	Aux bldg general area exhaust fans to vent stack	Closed	SI	None
1-VS-AOD-111A	Cont purge exhaust damper to HEPA emergency filter	Closed	SI	None
1-VS-AOD-111B	Cont purge exhaust damper to HEPA emergency filter	Closed	SI	None
1-VS-MOD-100A	Unit 1 safeguards to HEPA emergency filters damper	Open	SI	Mode Switch [c]
1-VS-MOD-100B	Unit 1 safeguards to HEPA emergency filters damper	Open	SI	Mode Switch [c]
1-VS-MOD-103A	Control room supply air isolation damper	Closed	SI	None
1-VS-MOD-103B	Control room exhaust air isolation damper	Closed	SI	None
1-VS-MOD-103C	Control room supply air isolation damper	Closed	SI	None
1-VS-MOD-103D	Control room exhaust air isolation damper	Closed	SI	None
1-VS-PCV-322	Control room bottled air discharge isolation valve	Open	SI	None

c. A mode switch is under administrative control to prevent inadvertent alignment of this damper during refueling (Section 9.13.4.1).

Table 7.5-2 (continued)
VALVES/DAMPERS ACTUATED BY ENGINEERED SAFEGUARDS SIGNALS

Designation (Valve or Damper Tag No.) (Similar for Unit 2)	Service (Actuated Valve or Damper Description)	Function (Actuated Valve or Damper Position)	Signal (Actuation Signal)	Override/Bypass (Override or bypass condition following actuation)
1-VS-PCV-531	Control room bottled air discharge isolation valve	Open	SI	None
1-VS-PCV-532	Control room bottled air discharge isolation valve	Open	SI	None

Legend
SI = Safety Injection
SGLLWL = Steam Generator Low-Low Water Level
CLS-Hi = Consequence Limiting Safeguards - High
CLS-HiHi = Consequence Limiting Safeguards - High High or CLS-HiHi* when coincident with undervoltage

Table 7.5-3
SAFETY-RELATED SYSTEMS

Function	System
Emergency reactor shutdown	Reactor coolant Reactor protection Safeguards actuation Chemical and volume control
Containment isolation	Containment isolation
Reactor core cooling	High pressure injection Low pressure injection Accumulators
Containment heat removal	Containment spray Containment ventilation Containment sump recirculation
Core residual heat	Residual heat removal Pressurizer spray Power-operated relief valves Main feedwater Auxiliary feedwater Main steam Steam dump Component cooling water Service water
Prevention of significant release of radioactive material to environment	Containment spray (iodine removal) Containment air purification Containment gas control Containment radiation monitoring Containment radiation sampling
Supporting systems	Emergency power Control room and safety equipment area ventilation

Figure 7.5-1
SAFETY INJECTION SYSTEM ACTUATION

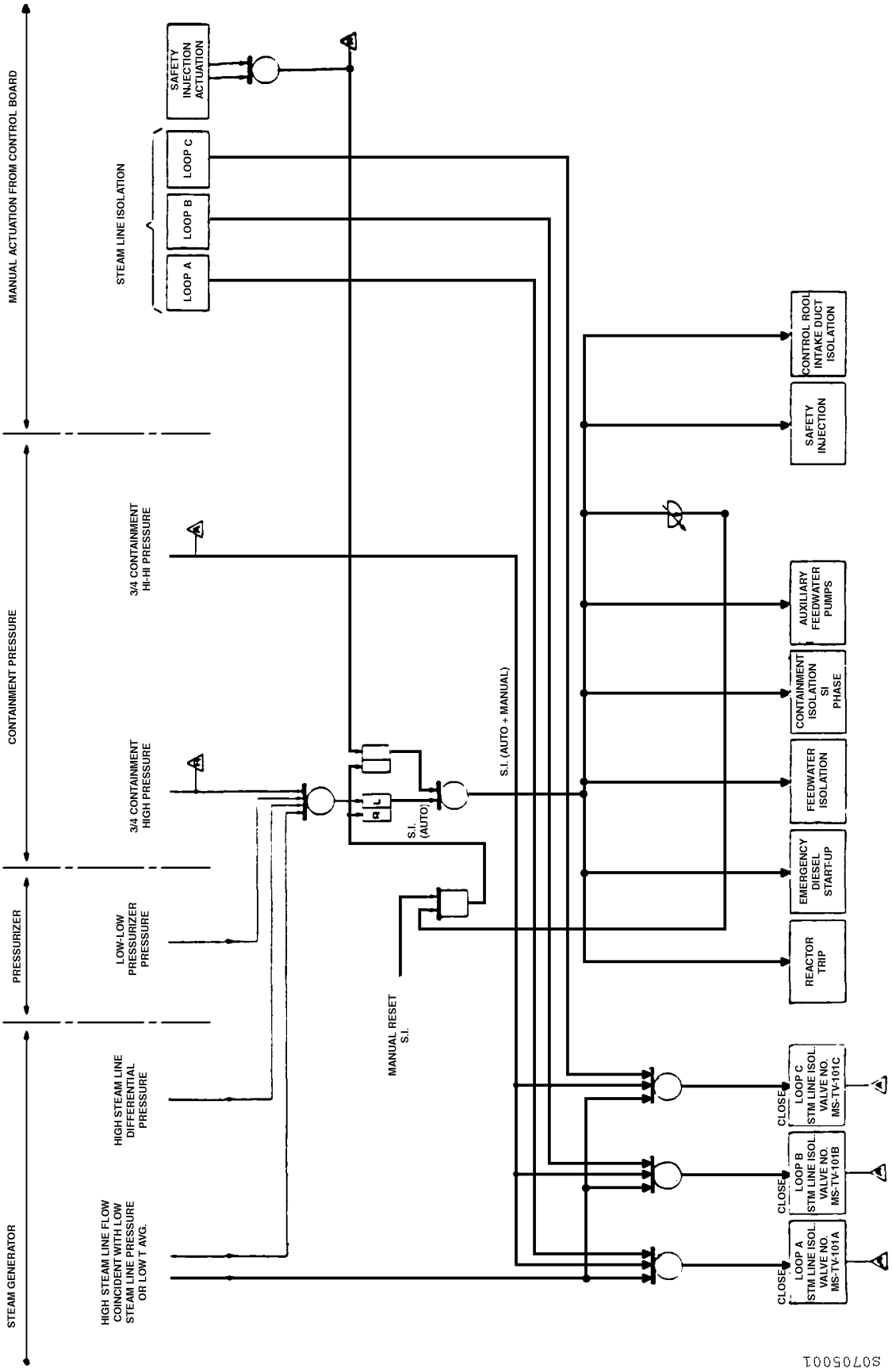


Figure 7.5-2
CONSEQUENCE-LIMITING SAFEGUARDS INITIATION SYSTEM (UNIT 1)

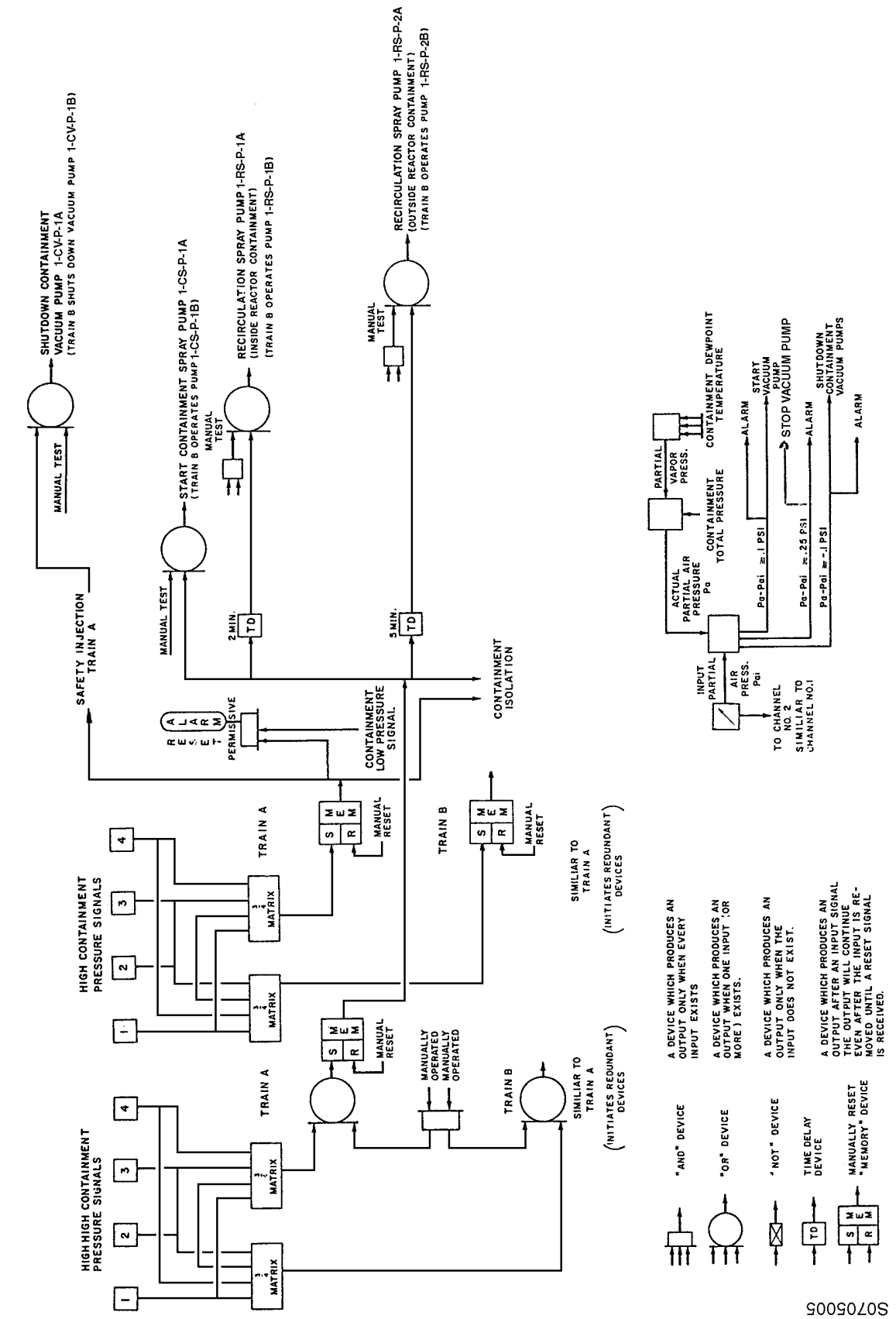


Figure 7.5-3
CONSEQUENCE-LIMITING SAFEGUARDS INITIATION SYSTEM (UNIT 2)

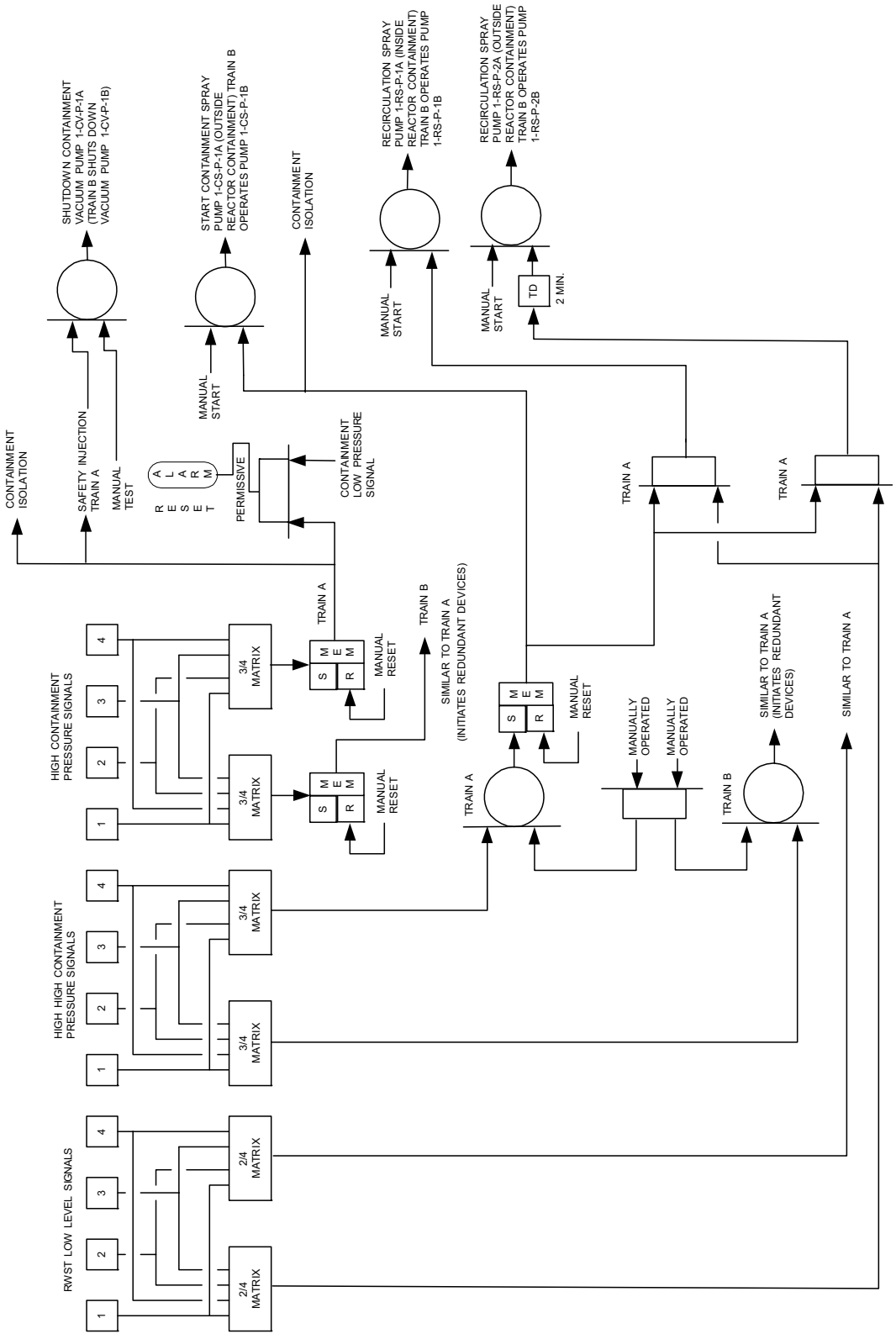


Figure 7.5-4
ENGINEERED SAFEGUARDS ACTUATION CIRCUITS

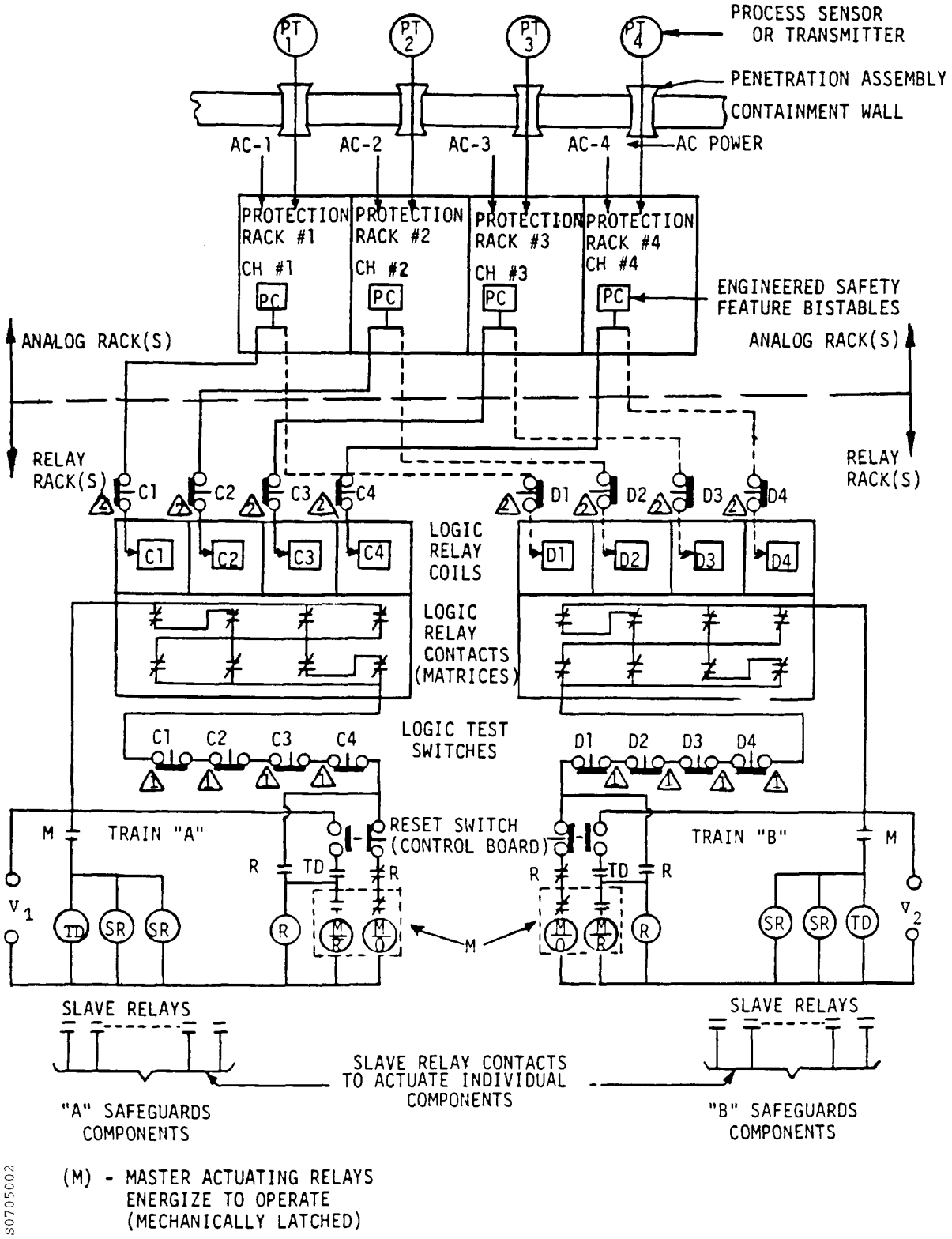


Figure 7.5-5
SIMPLIFIED DIAGRAM FOR OVERALL LOGIC RELAY TEST SCHEME

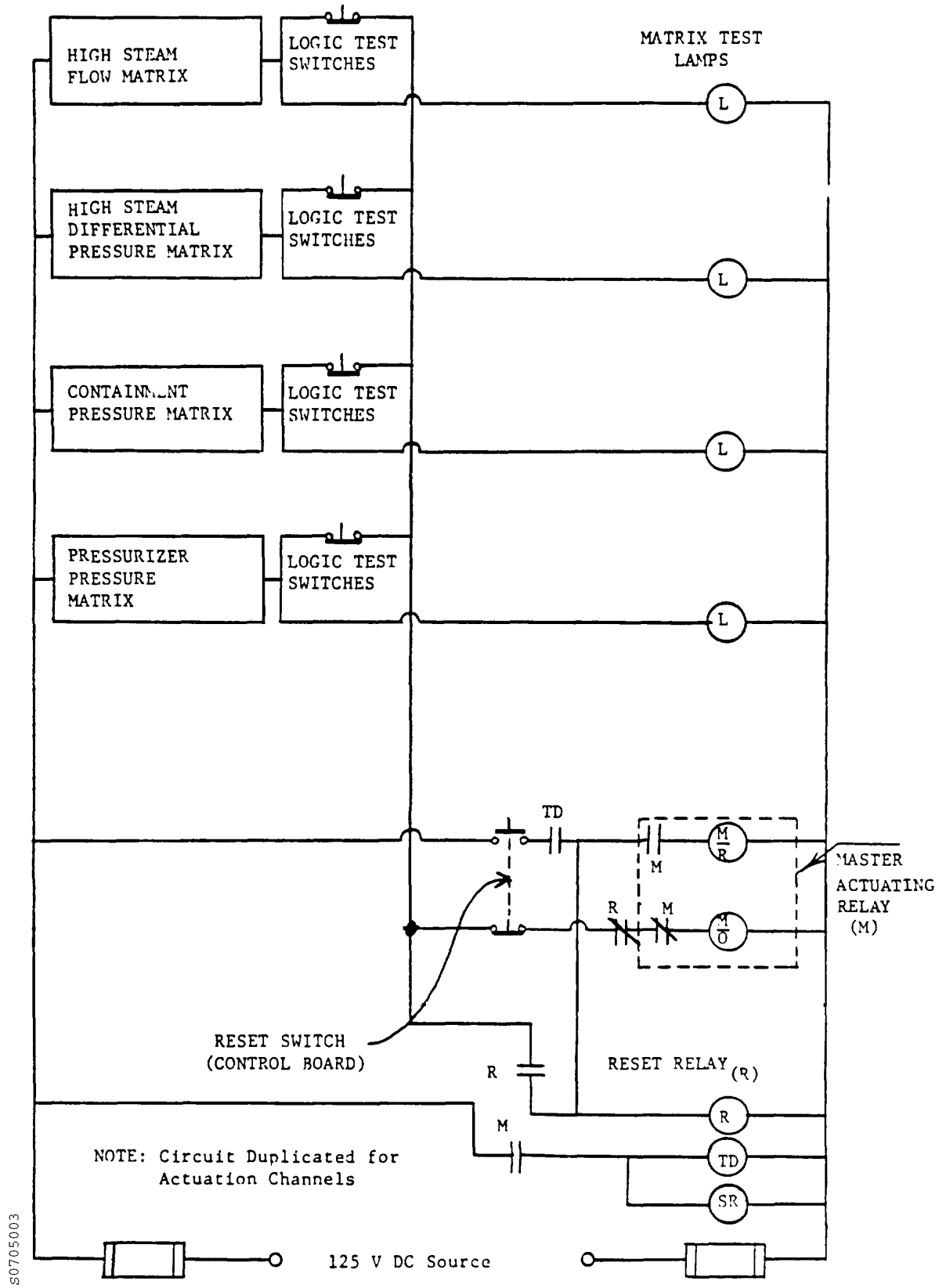
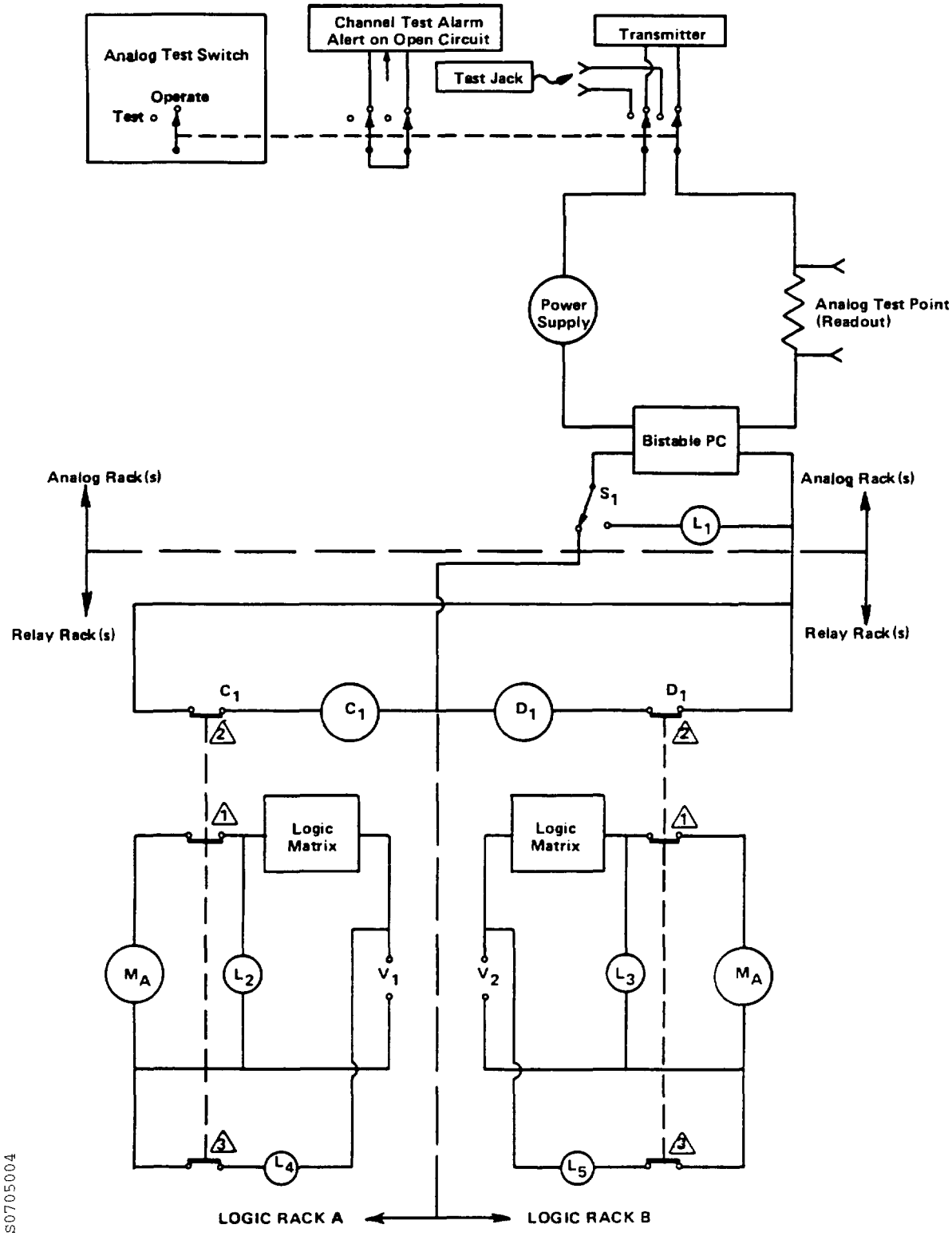


Figure 7.5-6
SIMPLIFIED DIAGRAM RELAY LOGIC CHANNEL TESTING



7.6 INCORE INSTRUMENTATION

7.6.1 Design Basis

The incore instrumentation is designed to yield information on the neutron flux distribution at selected core locations. Using the information thus obtained, it is possible to confirm the reactor core design parameters. The system provides means for acquiring data only, and performs no operational unit control.

7.6.2 System Description

7.6.2.1 General

The incore instrumentation system consists of retractable flux thimbles, which run the length of selected fuel assemblies, and moveable fission detectors which are inserted into the retractable flux thimbles. The detectors are used to collect flux distribution data. The retractable flux thimbles are shown in Figures 7.6-1 and 7.6-2.

Fifty core locations on each unit are capable of housing retractable flux thimbles. Each flux thimble houses 3 core exit thermocouples (1 in service with 2 installed spares) used to measure core exit temperature in post accident conditions as required by Reg Guide 1.97. The core exit thermocouples are not a functional part of the incore system, however, the incore system provides a means of placing the core exit thermocouple in the core. The core exit thermocouples provide input to the Inadequate Core Cooling System and are discussed in more detail in Section 7.10.

The thimbles are retractable and are inserted into the reactor at the seal table. Unit 1 locations F-04, J-03 and J-05 and Unit 2 locations G-07, J-12, N-05, and N-08 are capped. Caps may be installed in the event a thimble location must be removed from service. Technical Specifications provide the requirements for the number and location of operable flux thimble locations.

The data collected by the incore system in conjunction with previously calculated analytical information is used to determine the fission power distribution. This method is more accurate than using calculational methods alone. The data collected by the incore system may also be used to calculate coolant enthalpy distribution ($F_{\Delta h}$), total peaking factor (F_Q), and the fuel burnup distribution. Once analyzed, the measured data is compared to power distribution and thermal/hydraulic limits which is the primary way to determine the maximum allowable power output. The radial and axial power distribution may also be evaluated by comparing the power distribution between quadrants.

7.6.2.2 Thermocouples

Three chromel-alumel, grounded, twinax, thermocouples are permanently installed at the tip of each of the 50 flux thimbles. The thermocouples and extension leads are installed in the annulus of the non-concentric flux thimble inner calibration tube and the outer sheath as shown in Figures 7.6-1 and 7.6-2. The thermocouple extension leads are mineral insulated with stainless

steel sheaths. For each guide tube, one thermocouple circuit is active and monitored by the Emergency Response Facilities Data Acquisition System, which provides parallel data to the Inadequate Core Cooling Monitor System and the PCS. The other two thermocouples associated with each flux thimble are installed spares.

7.6.2.3 **Movable Neutron Detectors**

7.6.2.3.1 Mechanical Configuration

The neutron flux detectors, remotely positioned in the core, provide remote readout for flux mapping. The basic system for the insertion of these detectors is as shown in Figure 7.6-3. Retractable flux thimbles, which contain thermocouples and the calibration tube, are pushed into the reactor core through thimble guide tubes (conduits). These thimble guide tubes extend from the bottom of the reactor vessel down through the concrete shield area, then up to a thimble seal table.

The retractable thimbles are closed at the leading (reactor) ends, are dry inside, and the calibration tube serves as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the thimble guide tubes are provided at the seal table, as shown on Figures 7.6-1 and 7.6-2.

Surry Power Station is in the process of replacing the Westinghouse designed flux thimbles and seal table seals shown on Figure 7.6-1 with the design that is shown on Figure 7.6-2. The replacement project is planned for implementation over several refueling outages. The configuration of the flux thimbles does not change and will consist of an inner calibration tube that is used to insert and withdraw the in-core neutron detectors, three type K, grounded thermocouples and an outer tube. The inner tube is also part of the Reactor Coolant System pressure boundary. The principal difference between the Westinghouse and replacement designs is in the high and low pressure seals and the seal housing at the top of the flux thimble guide tube. Detailed descriptions of each design are included in Surry Power Station vendor technical manuals and applicable vendor drawings.

During reactor operations, 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 table is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists of a combination of drive assemblies, five-path rotary transfer devices, and ten-path rotary transfer devices, as shown in Figure 7.6-3. The drive system pushes hollow helical-wrap drive cables into the core. Miniature detectors are attached to the leading ends of the cables, and small-diameter sheathed coaxial cables are threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor that 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. Further information on mechanical design and support is provided in Chapter 3.

7.6.2.3.2 Control and Readout Description

The control and readout system provides means to rapidly traverse the miniature neutron detectors to and from the reactor core at 72 ft/min, and to traverse the reactor core at 12 ft/min while plotting the thermal neutron flux versus detector position. 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 tubing run provide signals to the path display to indicate the active detector path during the flux mapping operation. Each gear box drives an encoder for position indication. One five-path group path selector is provided for each drive unit to route the detector into one of the flux thimble groups or to storage. A ten-path rotary transfer assembly is used to route a detector into any one of up to ten selectable thimbles. Manually operated isolation valves on each thimble allow free passage of the detector and drive cable when open. When closed, these valves prevent steam leakage from the core in case of a thimble rupture. Provision is made to separately route each detector into a common flux thimble to permit cross calibration of the detectors.

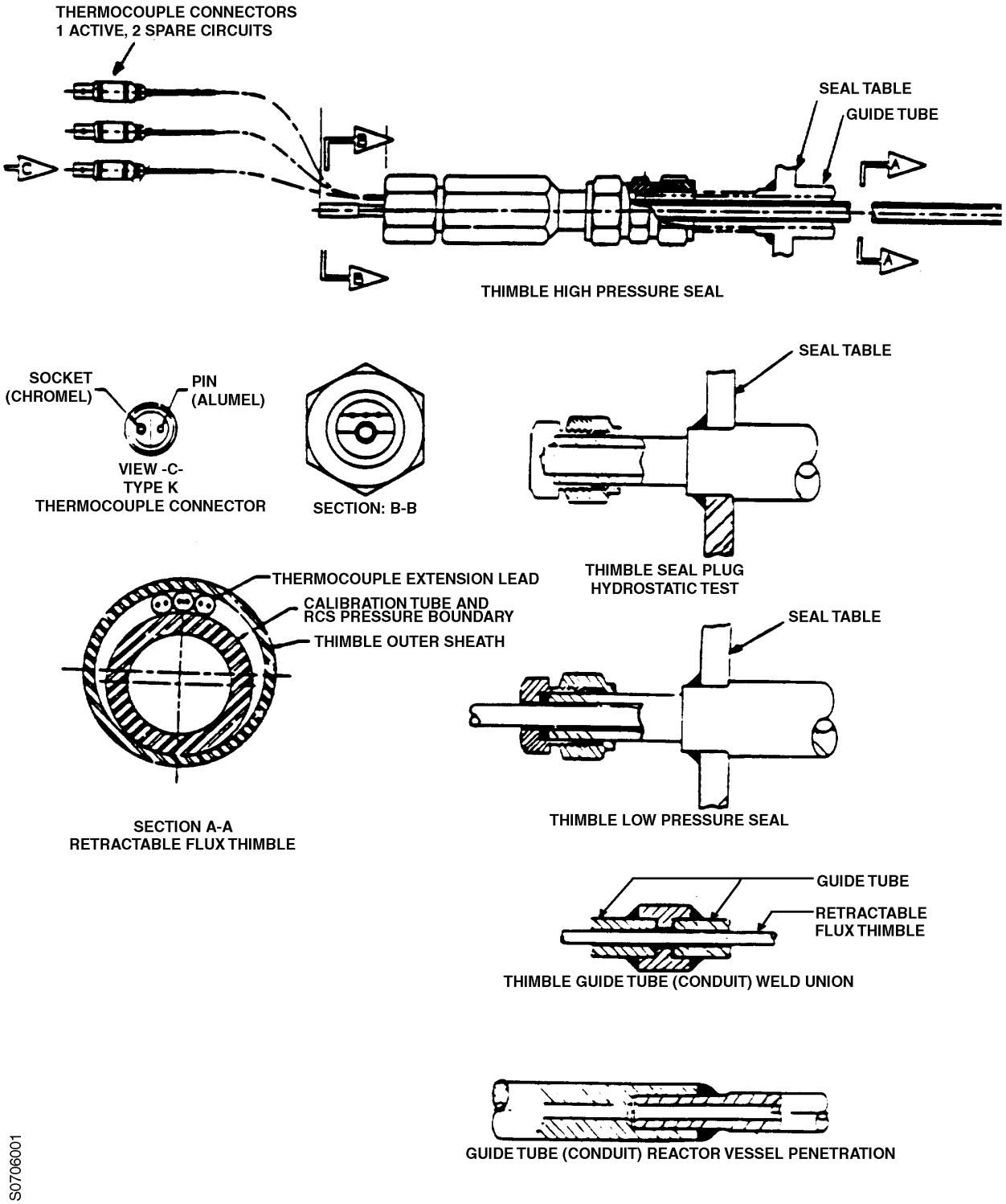
The control room contains the necessary equipment for control, position indication, and flux recording. Panels are provided to indicate the position of the detectors, and for plotting the flux level versus the detector position. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting, and gain controls. A flux-mapping operation consists of selecting (by panel switches) flux thimbles in given fuel assemblies at various core locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot (position vs. flux level) is initiated with the slow withdrawal of the detectors through the core from the 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 are then compared to obtain a flux map for a region of the core.

7.6.3 System Evaluation

The thimbles are distributed nearly uniformly over the core, with about the same number of thimbles in each quadrant. The measured nuclear peaking factor (F_Q) is increased by 8% to account for uncertainties, prior to being compared to its limit. An appropriate allowance for the measurement uncertainty for the nuclear hot-channel factor ($F\Delta h$) has been incorporated into the statistical DNBR limit. If either factor exceeds its limit, core power is reduced until the violation is eliminated.

Figure 7.6-1
INCORE INSTRUMENTATION - DETAILS
WESTINGHOUSE DESIGN



Upon Completion of Design Change 00-003, this figure will no longer be applicable. The configuration of the flux thimble tubes will be as shown on Figure 7.6-2

Figure 7.6-2
INCORE INSTRUMENTATION - DETAILS
REPLACEMENT DESIGN

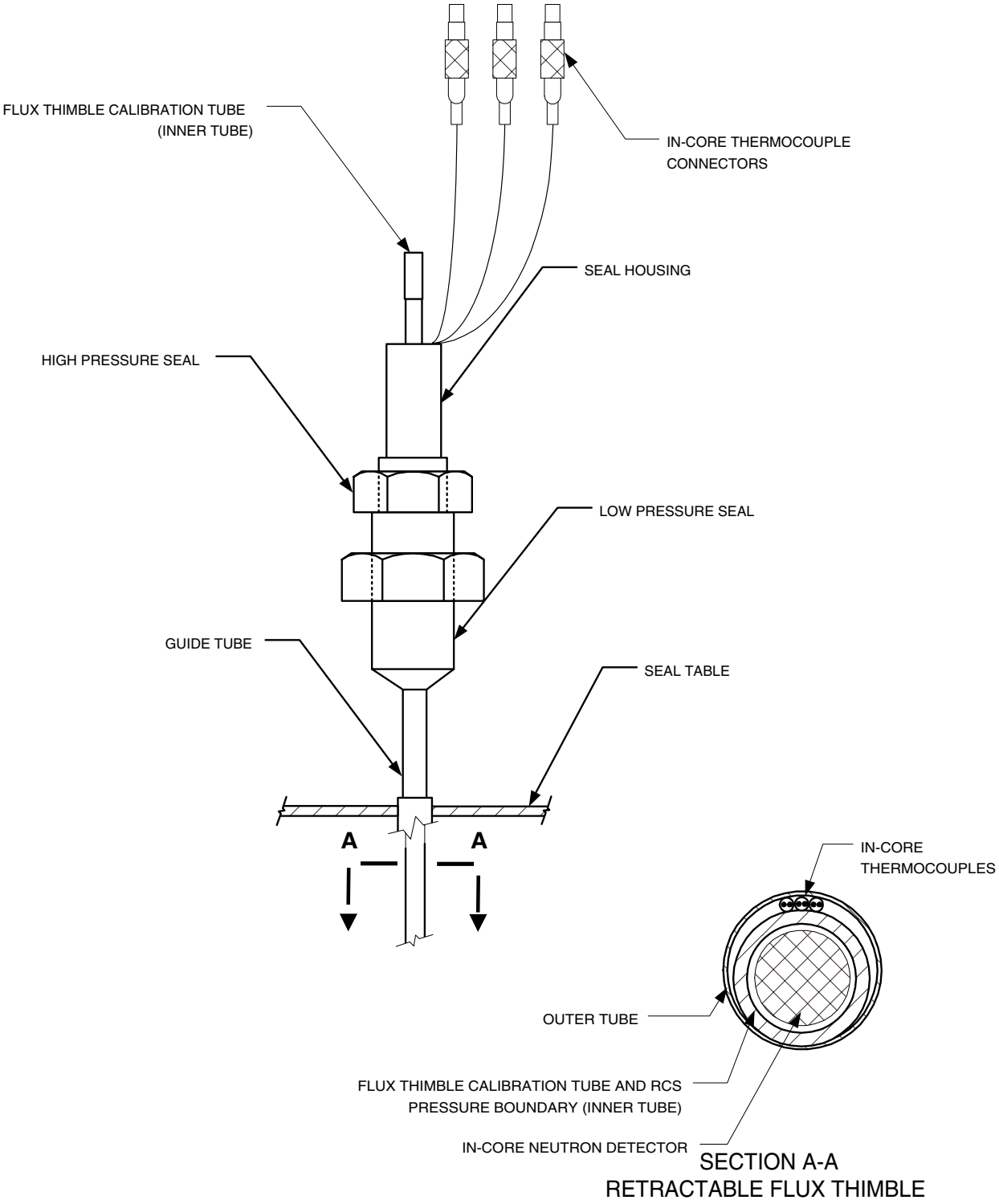
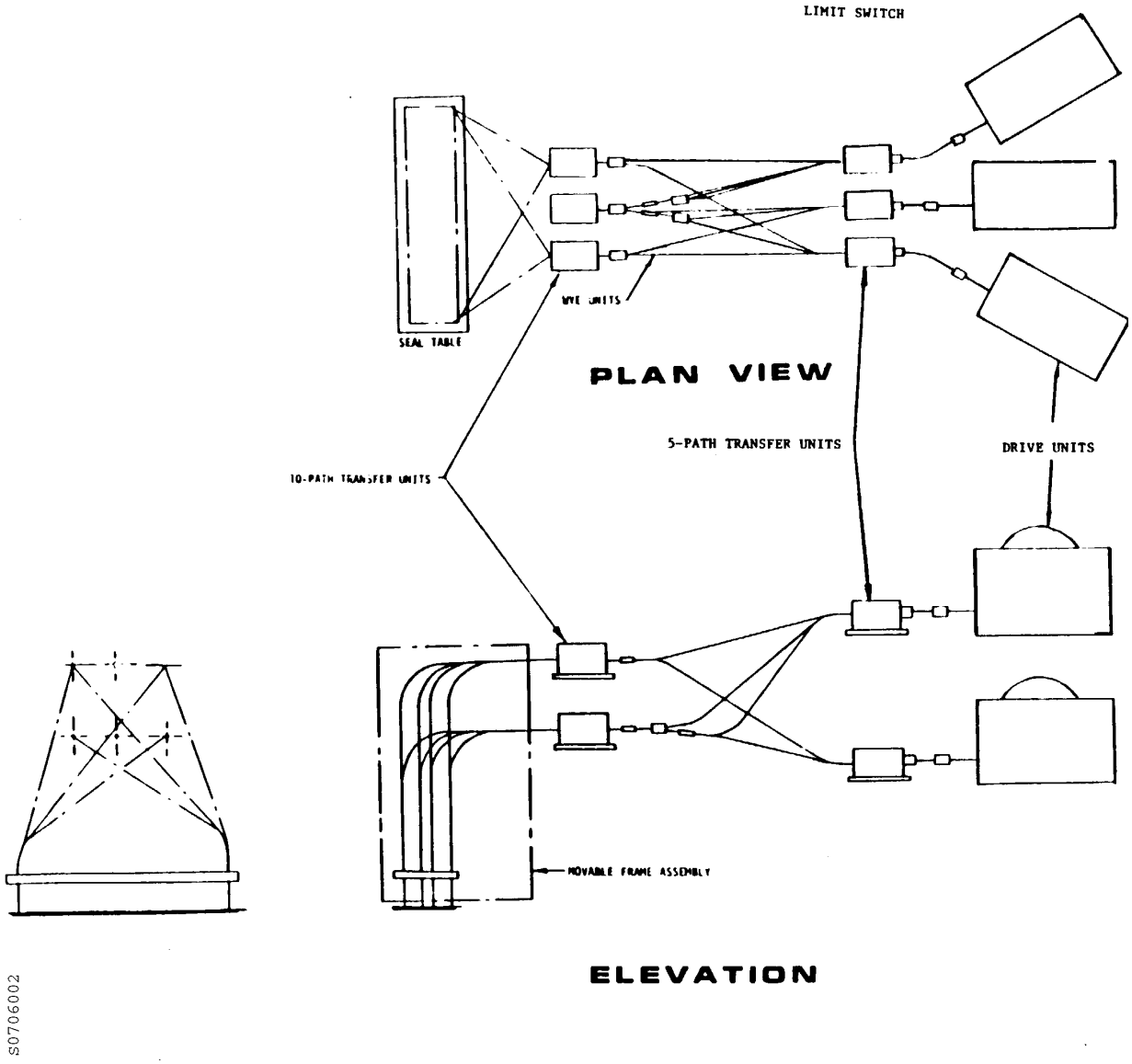


Figure 7.6-3
INCORE MECHANISMS



7.7 OPERATING CONTROL STATIONS

The control room, located in the service building, contains controls and instrumentation necessary to start up, operate, or shut down both units. It is one of the most important parts of the station, with pertinent interrelated information presented for the safe and reliable operation of the plant, including periods of transient and accident conditions. In the event that this area becomes inaccessible, the reactors can be brought to and maintained in a hot-shutdown condition at auxiliary control stations located in the Emergency Switchgear Rooms below the control room. There is a separate auxiliary control station for each unit. In addition, controls for certain auxiliary systems not directly involved with power generation, such as water treating and waste disposal, are located at remote control stations. The control room is shown in Figure 7.7-1 and Reference Drawing 1.

7.7.1 Design Bases

The station is equipped with a control room that contains controls and instrumentation necessary for operation of the reactors and turbine-generators under normal and accident conditions.

The control room, which is continuously occupied by qualified operating personnel under all operating and design-basis accident (DBA) conditions, is designed to permit single operator supervision of the units during normal steady-state conditions and to use additional operators to assist the control room operator during abnormal conditions.

The control room has three independent communication systems. One system consists of telephones leased from the local telephone company. These telephones and several outside trunk lines service the station for outside calls. This system may or may not be available under emergency conditions. A second system, a communication and voice paging system, is provided to interconnect the entire station. This system is energized from the emergency power buses. The third system is sound-powered, with telephone jacks and interconnecting wires at each major control point for test purposes. Sound-powered telephones are installed at various stations in the reactor containment. This system is accessible so that roving operators or service personnel may have easy communication with the control room or one another. This system does not rely on any power source, so it will be available at all times.

In addition to the above communications systems, onsite and offsite communications equipment has been installed to provide for notification of the NRC, as well as corporate, state, and local authorities on a 24-hour basis. An 850 MHz radio trunking system with primary and backup systems exists for radiological monitoring teams and security and recovery operations. Communications with the Corporate Emergency Response Center (CERC) and the Emergency Operations Facility (EOF) are also provided on primary and backup systems.

Sufficient shielding, distance, and containment integrity are provided to ensure that control room personnel shall not be subjected to doses that in the aggregate would exceed the limits in

10 CFR 50, Appendix A, GDC 19 during occupancy of, ingress to, and egress from the control room. All equipment in this area has been designed to minimize the possibility of a condition that could lead to possible inaccessibility or evacuation. For events analyzed to implement the alternate source term, which is described in Regulatory Guide 1.183, the control room dose limits are specified in 10 CFR 50.67.

The auxiliary control stations, also highly protected, are designed with a minimum of simple control actions required to bring and maintain the reactor in a hot-shutdown condition. It is not desirable to include marginal controls that would require more operator coordination, bypassing or deactivating of protective circuits, and unorthodox operating procedures.

Temperature in the control room and adjoining equipment room is maintained for personnel comfort at 75±10°F. The electronic equipment is tested and calibrated at the factory for the design temperature range from 40°F to 110°F. Qualification testing has demonstrated that the instrumentation remains operable up to 120°F, as there is a possible calibration shift above this range. The Plant Computer System equipment in the control room is designed to operate up to 95°F. This 120°F limit establishes the maximum temperature above which plant shutdown is required. Thus, there is a wide margin between design limits and the normal operating environment for control room equipment.

7.7.2 System Description

The primary objectives in the control room layout are to provide the necessary controls to start, operate, and shut down each unit, with sufficient information display and alarm indication to ensure safe and reliable operation under normal and accident conditions. Special emphasis is given to maintaining control integrity during accident conditions.

The equipment in the control room is arranged to reflect the fact that certain systems normally require more operator attention than others. The main control board is the central item in the control room. The control board for Unit 1 is completely independent of the control board for Unit 2. Each control board has a bench section, and a vertical section located behind the bench section. Most of the essential instruments and controls for power operation, and protective equipment that is immediately needed in cases of emergency, are mounted on the bench console sections in functional groupings. Recorders and indicators are mounted on the vertical back panels in agreement, wherever appropriate, with the functional groupings of the bench sections. The engineered safeguards section of the control board is designed to minimize the time required for the operator to evaluate the system performance under accident conditions.

Auxiliary vertical panels are provided in the control room, where their use simplifies control of certain auxiliary systems, or systems that only require occasional operator attention, such as turbine supervision, radiation monitoring, and liquid and gaseous waste disposal.

Illuminated window and audible alarm units are incorporated into the control room to warn the operator if abnormal conditions are approached by any system. Independent annunciator

systems for each unit have their own identifying alarm horn tones. Indications and alarms are also provided so that the control room operator is made aware of any deviation from normal conditions at remote control stations. Many of these conditions are also alarmed by the unit performance-and-alarm monitoring system. Audible containment alarms are initiated automatically by the radiation monitoring system. Audible alarms are sounded in appropriate areas through the station if high-radiation conditions are present.

Instrumentation and control equipment is designed with reliable components. The temperature in the control room and emergency switchgear and relay rooms may vary from 65°F to 85°F. Indicating and control instruments will continue to function within design accuracy in ambient temperatures up to 120°F. In addition, a reliable source of electric power, described in Section 8.4.3, is provided to ensure continual operation of vital unit and station instrumentation. Emergency lighting is also provided. The control room is further discussed in Section 11.3.6.

Two 100% redundant air handling units, fed from different power sources, are provided for the main control room and emergency switchgear and relay room of each unit. Each air handling unit is supplied chilled water by one of two chillers connected to the same power source as the respective air handling unit. Since the main control rooms are common, if only one of the four control room cooling units remains operable, the control room temperature will level off under 90°F. As the latent heat is negligible, humidity is not a factor. A double failure (both operating air-handling units failing concurrently) is required to jeopardize the temperature control. In this very unlikely event, the control room would reach 120°F in about 45 minutes, which would still provide sufficient time to start the redundant air handling units or shut down the reactor. Onsite testing was performed to prove the installed performance of the air-conditioning systems.

Qualification testing has been performed on various safety systems, such as process instrumentation, nuclear instrumentation, and relay racks. This testing involved demonstrating operation of safety functions at elevated ambient temperatures to 120°F for control room equipment and in full postaccident environment for required equipment in containment. Detailed results of some of these tests are proprietary to the suppliers, but are on file at the suppliers and available for audit by qualified parties.

The control room is designed to be available at all times. Accessibility to this area is from three points, thus ensuring entry for emergency personnel. Safe occupancy of the control room during an abnormal condition is provided for in the design of the service building. Adequate shielding and air conditioning are used to maintain tolerable radiation and air temperature levels in the control room. Ventilation consists of totally contained redundant recirculating air-conditioning systems designed to continue operation under all normal and emergency conditions. Fresh air intake and exhaust for normal use are from other independent systems, which can be valved off to stop the intake of airborne activity if monitors indicate that such action is appropriate. Makeup air, under emergency conditions, is available from redundant compressed breathing-air banks, or from emergency ventilating units supplying air through high-efficiency

charcoal filters. With all normal outside air makeup shut off, the quality of the air will be maintained with the compressed air banks or the carbon-filtered emergency ventilation.

To limit the possibility and potential magnitude of a fire in the control room, the following are incorporated into its design:

1. Noncombustible materials are used in construction.
2. Control and instrumentation cable and switchboard wiring are used that meet the flame test described in Insulated Power Cable Engineers Association, Publication S-61-402, and National Electrical Manufacturers Association, Publication WC5-1968.
3. The main control boards are wired with flame-retarding switch-board-type conductors. The two main control boards are physically separated.
4. Control room furnishings are of metal construction with the exception of chairs, Corian desktops for the Senior Reactor Operator console and Plant Computer consoles, anti-fatigue flooring, and carpeting.
5. All control information is transmitted to the control room by electrical signals or low-pressure air signals. Transmitted signals from the containment structure and any other high-radiation areas are electrical.
6. Combustible supplies, such as records, logs, procedures, manuals, etc., are minimized.
7. Fire detection alarms are provided in the control room. These alarms are actuated from remote detectors sensitive to smoke and located in the vicinity of instrumentation cabinets, air-conditioning system ducts, and in other areas susceptible to fire.
8. All areas of the control room are readily accessible for extinguishing.
9. Portable fire extinguishers and breathing apparatuses are provided.
10. The control room is occupied at all times by an operator who has been trained in fire extinguishing techniques.
11. The control room is separated from the emergency switchgear and relay rooms by a 3-hour fire-resistant barrier. The emergency switchgear and relay rooms of each unit are separated from each other by a 3-hour fire wall.

Further description of the fire protection provisions is given in Section 9.10.

Therefore, any fires in the control room are expected to be of such small magnitude that they could be extinguished by a hand fire extinguisher. The resulting smoke and vapors are removed by the ventilation system. In addition, the control room is protected from outside fire, smoke, or airborne radioactivity by pressure-tight penetrations, weather-stripped doors, absence of windows, and by the positive air pressure maintained in the area during normal and emergency operation. Fire-rated doors are installed as access doors leading into the control room complex.

The probability of the control room becoming inaccessible as a result of fire or other causes is considered extremely small. However, if the operator must leave the control room, operating procedures require that he trip the reactors and turbine-generators before leaving so as to bring the station automatically to the no-load condition, thus ensuring control at the auxiliary control stations. Each reactor unit can be brought to and maintained in a hot-shutdown condition from its auxiliary control station, which is provided with the following alternate control provisions:

1. Removal of core residual heat.
2. Boration of the reactor coolant system.
3. Maintenance of pressurizer level and pressure.

These functions require the operation of auxiliary feedwater pumps, charging pumps, and boric acid transfer pumps. Appropriate process instrumentation, such as pressurizer pressure and level, and steam generator pressure and level, are provided in the auxiliary control stations. This equipment is sufficient to safely maintain the unit or units for an extended period of time in a hot-standby condition.

The principal point of control in the auxiliary control station is an instrument panel. The following equipment is controlled at this panel:

1. Turbine driven auxiliary feed pump start-stop control switch.
2. ‘A’ auxiliary feed pump motor start-stop control switch.
3. ‘B’ auxiliary feed pump motor start-stop control switch.
4. Motor-operated valves - auxiliary feed pump discharge open-close control switches (6).
5. Steam generator wide range water level indicators.
6. No. 1A charging pump motor start-stop control switch.
7. No. 1B charging pump motor start-stop control switch.
8. No. 1C charging pump motor start-stop control switch.
9. No. 1A boric acid pump motor start-stop control switch.
10. No. 1B boric acid pump motor start-stop control switch.
11. Charging flow control valve control switch.
12. Boric acid filter discharge to charging pump suction motor-operated valve control switch.
13. Pressurizer pressure indicator.
14. Pressurizer level indicator.
15. Pressurizer heater backup groups control switch.
16. Main steam header pressure indicators.

17. Main steam pressure indicators

18. Charging flow indicator

The capability of operating the residual heat removal pumps and component cooling water pumps from the emergency switchgear room, as discussed in Sections 9.3.2.1, 9.4.3.1, and 9.10.4.1, has been incorporated by the addition of a transfer switch and a control switch on each pump's breaker compartment at the switchgear. This capability, which has been incorporated in both units, has been installed to be used in the event a fire disables or causes evacuation of the control room. These plant features have been added in accordance with the requirements of 10 CFR 50 Appendix R.

Additional remote monitoring panels have been installed in the cable tray area of Unit 1. The panels provide indication of two reactor coolant loops hot- and cold-leg temperatures, RCS and steam generator pressures, pressurizer level, and steam generator wide range water levels, and source and wide-range excore neutron flux. The panels are shared by both units.[1] Signals to the panels are transmitted from instruments dedicated to the panel via cables independently routed from cables transmitting the same data to instrumentation in the control room and on the auxiliary shutdown panel.

Seismically-qualified transmitters are installed in the containments of each unit, parallel to existing RCS and steam generator pressure transmitters, and the pressurizer level, and steam generator wide-range level transmitters. Sensing lines for these transmitters are connected to the existing transmitter sensing lines, outside the crane wall, and are seismically qualified. The spare elements of existing dual head hot-leg RTDs are used and connected to temperature transmitters mounted in the remote monitoring panel. One element of the dual element cold-leg RTD's is used to provide the cold-leg temperature to the remote monitoring panel. Cables inside and outside the containment servicing the transmitters for the remote monitoring panel and spare RTD elements are routed independently from the cables for associated parallel transmitters and RTD element, furnishing identical information to control room and auxiliary shutdown panel instrumentation. In order to meet the requirements of 10 CFR 50 Appendix R additional transmitters and cables providing indication at the remote monitoring panels for RCS pressure, pressurizer level, and steam generator wide-range water levels have also been installed. Instrumentation sensing lines are routed independently with fire barriers as required to maintain specific separation from at least one parallel channel of indication available in the control room or auxiliary shutdown panel. This separation meets the requirements of Appendix R.

1. Panel RMP is powered from either unit's Appendix R Distribution Panel by a selector switch. Panel ASC-RMP, Unit 1 section is powered from Unit 2. Panel ASC-RMP, Unit 2 section is powered from Unit 1.

One remote monitoring panel (ASC RMP-1) contains one indicator for each of the following RCS parameters with a selector switch which aligns the indicator to either the Unit 1 or Unit 2 instrument transmitter outputs.

Steam Generators A, B, and C Wide-Range Levels

Pressurizer Level

RCS Wide-Range Pressure

RCS Loop 1 Hot-Leg Temperature (Units 1 & 2)

RCS Loop 2 Hot-Leg Temperature (Unit 1)

RCS Loop 3 Hot-Leg Temperature (Unit 2)

The 120V ac power from the Appendix R Panels is isolated by a selector switch, which aligns to either Unit's power, and protective relays. Loss of either unit's power at the panel is alarmed by an annunciator on the auxiliary ventilation panel (VNTX) which is shared by both units in the main control room.

The second remote monitoring panel (PNL-REM) contains six indicators for each unit. Indicators are provided for:

Steam Generator A Pressure

Steam Generator B Pressure (Unit 1 only)

Steam Generator C Pressure (Unit 2 only)

RCS Loop 1 Cold Leg Temperature

RCS Loop 2 Cold Leg Temperature (Unit 1 only)

RCS Loop 3 Cold Leg Temperature (Unit 2 only)

Source Range Neutron Flux

Wide Range Neutron Flux

Power for Unit 1 instrumentation on each remote monitoring panel is supplied by the Unit 2 Appendix R power system. Similarly, the Unit 2 instrumentation is supplied by the Unit 1 Appendix R power system. This assures that power will be available to the instrumentation of the affected unit following a fire in that unit's emergency switchgear room, cable tunnel or cable vault. Power to both Remote Monitoring Panels can also be supplied by a portable generator should power be lost to both Unit 1 and 2.

Alternative shutdown instrumentation for either unit's reactor is provided by the remote monitoring panels, which can be used in conjunction with the operation of the unaffected unit's charging pumps and the manual operation of applicable valves in the affected unit. The panels are to be utilized in the event that a fire disables the instrumentation on the affected unit's main board and auxiliary shutdown panel.

7.7.3 System Evaluation

The control room is designed to provide the operator with the controls, indication, and alarms necessary to control the station during normal or abnormal conditions.

Necessary information is available to the operator in the control room following a LOCA. Monitored information is available for postaccident analysis.

7.7 REFERENCE DRAWINGS

The list of Station Drawings below is provided for information only. The referenced drawings are not part of the UFSAR. This is not intended to be a complete listing of all Station Drawings referenced from this section of the UFSAR. The contents of Station Drawings are controlled by station procedure.

	Drawing Number	Description
1.	11448-FE-27A	Arrangement: Main Control Room, Elevation 27'- 0"

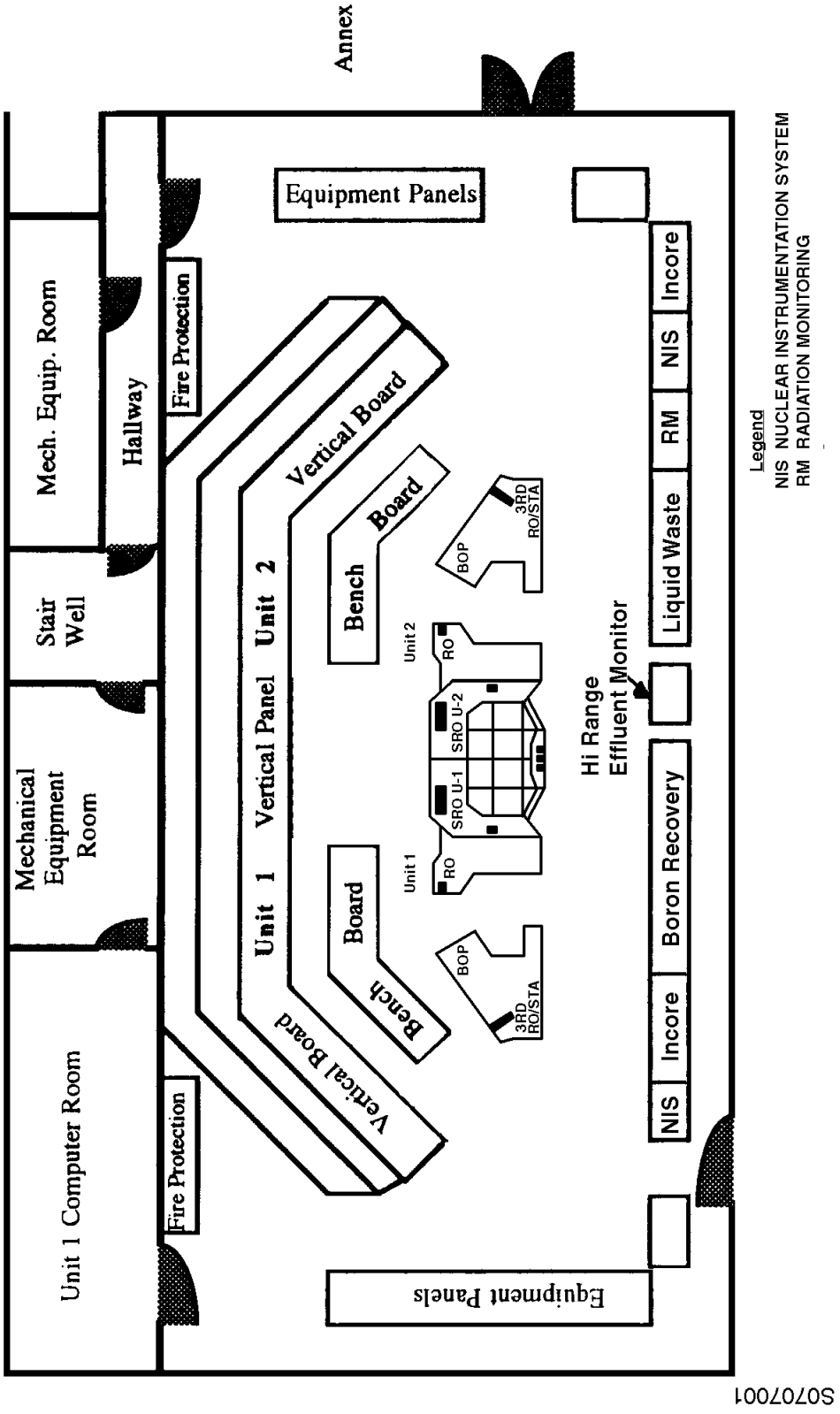


Figure 7.7-1
MAIN CONTROL ROOM ARRANGEMENT

Intentionally Blank

7.8 [DELETED]

Intentionally Blank

7.9 COMPUTER SYSTEM

7.9.1 Design Bases

The main purposes of the computer are to provide supplementary information to the operator, to effectively assist him in the operation of the nuclear steam supply system and turbine-generator cycle of each unit, to inform him of off-normal conditions, and to provide data communication, display and control functions for non-safety related equipment at the Low Level Intake Structure. The design of the control boards provides the operator with sufficient information for proper and safe operation of the unit if the computer system is unavailable.

7.9.2 System Description

The Plant Computer System (PCS) is designed to obtain data by scanning analog and digital field sensors and retrieve data from the Emergency Response Facility (ERF) data acquisition system, feedwater heater level control system and other peripheral plant systems. Operator (OWS) and Engineering (EWS) workstations act as primary data collection devices and then transmit that data to a secondary system historian, which will store easily retrievable data. Engineering workstations also provide the means to program the system. The PCS provides data and trending on visual displays, which can be printed. The system has the capability to log trip and post-trip data, and alarm when various off-normal conditions exist. Monitoring programs are also included for surveillance of reactor control and protection system operations and for nuclear process calculations and performance checks of systems and components. In addition to operator support functions, the PCS also serves as the Emergency Response Facility System, fulfilling the requirements of NUREG-0737 and NUREG-0696.

7.9.2.1 **Analog Scanning**

The computer continuously scans all preselected analog inputs at rates consistent with system requirements. Provisions are included for scanning some points faster than others. Those inputs that can change rapidly, or those associated with safety of the unit and associated with trip functions, are scanned at a rate suitable for detecting abnormal changes.

A limit-checking program is provided for determining that the analog values are within allowable instrument ranges. Out-of-range inputs are recorded and documented.

7.9.2.2 **Alarming**

Multiple high and/or low alarm setpoints can be assigned to each analog input. During each scan cycle, the analog values are compared to the associated setpoints to determine if they are outside the preset limits. A value in alarm is printed out or displayed on the OWS alarm screen and accompanied by an audible signal.

When the off-normal point returns to normal, the system again prints out or indicates a suitable message to this effect.

For example, a Delta-Flux Alarm Program monitors delta-flux in the reactor core and alerts the operator when a delta-flux alarm condition exists. There are two alarm states. They are: (1) above a preset power level when delta-flux has exceeded its allowable limit, and (2) below this power level if the allowable limit has been exceeded for a preset cumulative amount of time in the past 24 hours. Either alarm condition will set a computer contact closure output to actuate an annunciator alarm on the main control board. The annunciator will not clear until both of the computer alarms have returned to normal. Additionally, the alarm screen on the PCS OWS will indicate the associated system alarm point has changed state and requires operator attention. Most PCS alarms do not go to the annunciator system. They are displayed on the PCS alarm screens only.

7.9.2.3 **Alarm Review**

The operator may request a printout of all off-normal alarm inputs. This alarm review program documentation is very useful to a new shift, or for the operator to quickly determine the status of all station measurements.

7.9.2.4 **Analog Trend**

The analog trend function is used for recording suspected fluctuations or ramps in any measurements, or for obtaining data for future analysis of transients during start-up or load changing.

7.9.2.5 **Digital Trend**

The PCS provides visual displays of trends on the OWS. Any point in the system can be monitored on the workstation.

7.9.2.6 **Digital Display**

Visual displays are included on the operator workstations. Any analog input or addressable value can be displayed on this display.

7.9.2.7 **Sequence of Events**

These inputs usually are directly or closely associated with tripping the unit. A review of these events, in proper sequence, helps to analyze the causes and effects of unit trips and assists in trouble-shooting and returning the unit to service.

7.9.2.8 **Normal and Summary Logging**

Normal and summary logging for analog inputs, and calculated unit calorimetric variables, are provided.

7.9.3 System Evaluation

The PCS associated with each unit functions independently from the normal reactor control and protection system and engineered safeguards. The PCS provides control, communication, and display functions for non-safety related systems that do not provide reactor control functions.

Intentionally Blank

7.10 INADEQUATE CORE COOLING (ICC) SYSTEM

In response to NUREG-0578 (Reference 1), instrumentation to detect inadequate core cooling has been installed at Surry Units 1 and 2.

7.10.1 Design Bases

The Inadequate Core Cooling (ICC) system meets all the requirements of Regulatory Guide 1.97 (Reference 2). The ICC system, per unit, consists of the following three redundant subsystems that share common redundant calculator devices and continuous control room displays; Core Exit Thermocouple System, Core Cooling Monitor System, and Reactor Vessel Level Instrumentation System.

The system provides means for acquiring data only, and performs no operational unit control. Redundant displays in the control room graphically depict selected parameters, parameter trends, and system diagnostic information. An alarm is actuated in the control room on ICC system failure.

The safety-grade signal inputs, calculator devices and displays are qualified to IEEE-323 (Reference 3) or IEEE-344 (Reference 4).

7.10.2 System Description

7.10.2.1 Core Exit Thermocouple (CET) System - Subsystem of ICC System

The Core Exit Thermocouple System uses inputs from all the incore thermocouples to calculate and display temperature of the reactor coolant as it exits the core.

The CET system consists of Type K, grounded, stainless steel sheathed thermocouples. Refer to UFSAR Section 7.6.1, 7.6.2.1, and 7.6.2.2 for description of the quantity and design of the thermocouples.

One safety-related thermocouple from each flux thimble (25 for Train A and 25 for Train B) is wired to the redundant ICC calculators in the control room via the electrical penetrations and Station Multiplexer System.

The Cold junction compensation is performed internally at the remote multiplexer (MUX).

The thermocouples measure the core exit temperature in a range of 0 - 2300°F.

7.10.2.2 Reactor Vessel Level Instrumentation Systems (RVLIS) - Subsystem of ICC System.

The Reactor Vessel Level Instrumentation System (RVLIS) uses various parameters to calculate and to display the water level height in the reactor vessel during all plant conditions.

RVLIS uses differential pressure (d/p) measuring devices to measure vessel level or relative void content of the circulating primary coolant system fluid. The system is redundant and includes

automatic compensation for potential temperature variations of the impulse lines. Essential information is displayed in the main control room in a form directly usable by the operator.

The functions performed by the RVLIS are as follows:

- Assist in detecting the presence of a gas bubble or void in the reactor vessel
- Assist in detecting the approach to ICC
- Indicate the formation of a void in the RCS during forced flow conditions

Refer to Figure 7.10-1 for the RVLIS schematic

The RVLIS utilizes two redundant sets of three differential pressure (d/p) cell transmitters. These cells measure the pressure drop from the bottom of the reactor vessel to the top of the vessel, and from the hot legs to the top of the vessel.

This d/p measuring system utilizes cells of differing ranges to cover different flow behaviors with and without reactor coolant pump operation as follows:

- Reactor Vessel - Upper Range. The d/p cell, LT1, shown in Figure 7.10-1 provides a measurement of reactor vessel level above the hot leg pipe when the reactor coolant pump (RCP) in the loop with the hot leg connection is not operating.
- Reactor Vessel - Dynamic Head Range. The d/p cell, LT3, shown in Figure 7.10-1 provides a measurement of the pressure drop across the reactor core and internals assemblies for any combination of RCP operation (1, 2, or 3 pumps running). Comparison of the measured pressure drop with the normal, single-phase pressure drop provides an approximate indication of the relative void content or density of the circulating fluid. This instrument monitors coolant conditions on a continuing basis during forced flow conditions.
- Reactor Vessel - Full Range. The d/p cell, LT2, shown in Figure 7.10-1 provides a measurement of reactor vessel level from the bottom of the vessel to the top of the vessel during natural circulation conditions.

To provide the required accuracy for level measurement, temperature measurements (T1 through T7) of the impulse lines are provided as shown on Figure 7.10-1. These measurements, together with the reactor coolant temperature measurements (hot leg RTDs) and wide range RCS pressure, are employed to compensate the d/p transmitters outputs for differences in system density and reference leg density, particularly during the change in the environment inside the containment structure following an accident.

The d/p cells are located outside of the containment to eliminate the large reduction (approximately 15%) of measurement accuracy associated with the change in the containments environment (temperature, pressure, radiation) during an accident. The cells are also located

outside of containment so that system operation including calibration, cell replacement, reference leg checks, and filling are made easier.

7.10.2.3 **Core Cooling Monitor System - Subsystem of ICC System**

The Core Cooling or Subcooled Margin Monitor System uses various parameters to calculate saturation temperature and subcooled margins for the primary loops during all plant conditions. These input parameters provide the plant operators with complete information on core cooling.

Software algorithms determine the equivalent saturation temperature (T_{sat}) based on RCS wide range pressure. This (T_{sat}) value is used to determine the subcooled margin from the average of the five highest core exit thermocouples. An alarm is actuated in the control room on approach to saturation temperature.

7.10 REFERENCES

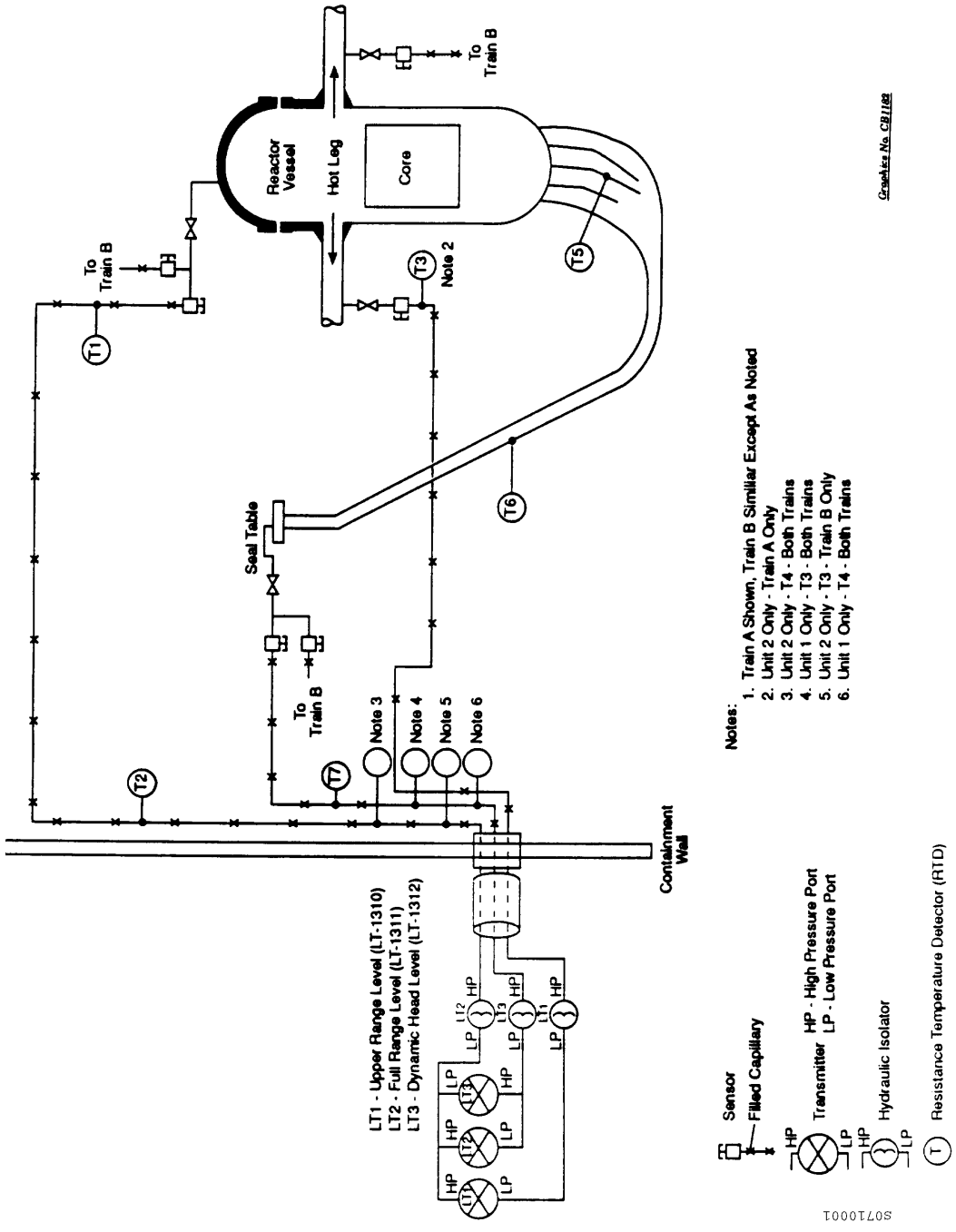
1. U.S. Nuclear Regulatory Commission, *TMI-2 Lessons Learned Task Force Status Report and Short-Term Recommendations,* NUREG-0578, July 1979.

2. U.S. Nuclear Regulatory Commission, *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident,* Regulatory Guide 1.97, December 1980.

3. IEEE Standard 323-1974, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, 1974.

4. IEEE Standard 344-1975, *Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, 1975.

Figure 7.10-1
REACTOR VESSEL LEVEL INSTRUMENTATION SYSTEM (RVLIS) SCHEMATIC



7.11 EX-CORE NEUTRON FLUX MONITOR SYSTEM

7.11.1 Design Bases

The Ex-Core Neutron Flux Monitor System is designed to meet the requirements found in Appendix R of 10 CFR 50 and Regulatory Guide 1.97. These requirements are in addition to those used in the original design basis of the station.

The instrumentation required by R.G. 1.97 is redundant Category I, Seismic Class 1, and Class 1E. R.G. 1.97 requires wide range indication over a range of 10^{-6} to 100% of full reactor power. The system that has been installed provides Source Range Indication over a range of 0.1 to 10^5 cps and Wide Range Indication over a range of 10^{-8} to 200% of full power.

The portions of the system that are required to meet R.G. 1.97 requirements have been designed to meet IEEE-323-1974 and IEEE-344-1975.

7.11.2 System Description and Evaluation

The Ex-Core Neutron Flux Monitor System consists of two redundant Channels. These Channels are made up of detector assemblies, amplifiers and processor units and indicators.

The Ex-Core Neutron Flux Monitor is designed to provide to the operator the reactor neutron flux level from source level (shutdown) to 200% of full reactor power.

Fission chambers were chosen to monitor post-accident neutron flux because of their proven high reliability to a harsh environment and because of their relative insensitivity to a high gamma flux.

The signal from the detector is composed of a series of charge pulses. The pulses result from alpha decay of the uranium coating in the detector, from gamma photon interaction with material in the electrodes of the detector, and from the fissioning of uranium atoms when a neutron is absorbed. The pulse signal from alpha decay and from gamma radiation is an unwanted signal and can be eliminated by amplitude discrimination because the neutron pulse signal is much larger.

The number of pulses per unit time from the detector is proportional to the magnitude of the neutron flux at the detector. The magnitude of the neutron flux in the reactor core is proportional to the fission power being generated in the reactor. Since the magnitude of the neutron flux at the detector is proportional to the magnitude of the neutron flux in the reactor core, the pulse rate from the detector is proportional to reactor power.

The neutron flux monitor measures the number of pulses per unit time from the detector over the range from source level to the level where the error from countrate loss, due to coincident pulses, becomes unacceptable. From about two decades below the upper end of the countrate range to full reactor power, the neutron flux monitor measures the mean square value of the time variant signal from the detector. This mean square value is proportional to the average rate of

neutron pulses and is not dependent on the pulses being individually identifiable, yet provides good discrimination against alpha and gamma signal.

The direct current signal from the detector provides a linear measurement of the reactor power. The direct current signal contains the alpha and gamma signal; however, on a linear scale from 0 to 200% of reactor power, it is less than 0.1% of full scale and, therefore, is not a problem. The direct current measurement inherently contains less statistical variation than the countrate or means square measurements and therefore, the measurement can be provided with a faster response time.

Source and Wide Range outputs from the Processor units are transmitted to the following locations (outputs are also available for the Technical Support Center):

Channel #1 (Red)	NIS Panel 1 Remote Monitoring Panel
Channel #2 (White)	NIS Panel 2

Indication at the NIS Panel and Remote Monitoring Panel consists of a set of two vertical edgewise meters. Displays for each area include both source range (0.1 to 10^5 cps) and wide range (10^{-8} to 200% of Reactor Power) neutron flux levels. They are intended to be available during all plant conditions.

The purpose of reactor power level indication is to confirm that the Reactor Shutdown function has been accomplished following an accident (in the case of the NIS Panel and TSC indicators), or fire (in the case of the Remote Monitoring Panel indicators).

In the event of a fire which requires the evacuation of the Control Room or causes the inoperability of control room reactor parameter indication, the Red Channel will be utilized to monitor reactor neutron flux level at the Remote Monitoring Panel.

The Ex-Core Neutron Flux Monitor System is also equipped with circuitry which provides continuous self-diagnostics of the integrity of the detector, cables, and power supplies. Failure of any of these components will generate a “non-operable” alarm in the Control Room.

The Ex-Core Neutron Flux Monitor System is normally supplied power from the 120V Vital AC Distribution System, Channels 1 and 2. In the event of a fire which causes the loss of control room indication and the normal electric distribution system, Channel 1 can be transferred to a back-up power source that is supplied from the other unit. In the event of a complete loss of ac power, a portable generator can be used to feed the Channel 1 Ex-Core system.

The system is designed so that all components which require calibration are located externally to the containment.

7.12 LEVEL INSTRUMENTATION TO PREVENT LOSS OF SHUTDOWN COOLING

In order to address concerns associated with loss of residual heat removal (RHR) capability while the reactor coolant system (RCS) is partially filled (i.e., mid-loop operation), a level standpipe has been permanently installed in the containment annulus to monitor reactor coolant level during plant shutdown and refueling.

An alternate means of determining the RCS level during mid-loop operation, which is independent of the level standpipe, is the ultrasonic measurement of the water level in the "B" hot leg piping.

7.12.1 System Description

7.12.1.1 Level Standpipe

The level standpipe is connected to the RCS at the top of the pressurizer and at a drain line from the Loop C cold leg. Local visual indication is provided at the standpipe in the containment annulus. Remote indication is also provided on the control room main board. An annunciator, which alarms on low reactor level, is also provided in the control room. The low level setpoint is set at a level prior to reaching RHR pump suction nozzle vortex initiation.

The standpipe and associated instrumentation is used only during shutdown and refueling conditions. During other plant conditions, the standpipe is isolated from the RCS by double isolation valves at each RCS connection.

7.12.1.2 Ultrasonic Level Indication System

An ultrasonic level indication system is installed as a secondary means of monitoring RCS drain down level independent of the level standpipe system. An ultrasonic transducer is mounted on the exterior of the "B" loop hot leg piping to provide RCS level indication. Remote indication is provided via a recorder located on the control room vertical board. A low level alarm is also provided by the ultrasonic level measurement which is connected to the standpipe low level alarm window. Either of the level measurement systems can activate the alarm on low RCS level.

The ultrasonic level indication system is only used in mid-loop operation during shutdown and refueling and is de-energized during normal plant operation.

Intentionally Blank