

Chapter 7: Instrumentation and Control

Table of Contents

Section	Title	Page
7.1	INTRODUCTION	7.1-1
7.1.1	Definitions	7.1-2
7.1.2	Identification of Safety-Related Systems	7.1-4
7.1.3	Identification of Safety Criteria	7.1-5
7.1.3.1	Design Criteria Compliance	7.1-5
7.1.3.2	Reactor Trip System	7.1-5
7.1.3.3	Engineered Safety Features Actuation System	7.1-7
7.1.3.4	Instrumentation and Control Power Supply	7.1-10
7.1.3.5	Quality Assurance	7.1-10
7.1.3.6	Safety-Related Equipment Identification	7.1-10
7.1.4	Regulatory Guide 1.97	7.1-11
7.1	References	7.1-13
7.1	Reference Drawings	7.1-14
7.2	REACTOR TRIP SYSTEM	7.2-1
7.2.1	Description	7.2-1
7.2.1.1	Reactor Trips	7.2-3
7.2.1.2	Reactor Trip System Accuracies and Response Times	7.2-11
7.2.1.3	Reactor Trip System Interlocks	7.2-11
7.2.1.4	Coolant Temperature Sensor Arrangement	7.2-12
7.2.1.5	Pressurizer Water Level Reference Leg Arrangement	7.2-12
7.2.1.6	Analog System	7.2-12
7.2.1.7	Digital Logic System	7.2-13
7.2.1.8	Isolation Amplifiers	7.2-13
7.2.1.9	Energy Supply and Environmental Variations	7.2-13
7.2.1.10	Trip Setpoints	7.2-13
7.2.1.11	Seismic Design	7.2-13
7.2.2	Analysis	7.2-14
7.2.2.1	Evaluation of Design	7.2-14
7.2.2.2	Evaluation of Compliance to Applicable Codes and Standards	7.2-17
7.2.2.3	Specific Control and Protection Interactions	7.2-25
7.2.3	Tests and Inspections	7.2-31
7.2.3.1	Inservice Tests and Inspections	7.2-31
7.2.3.2	Periodic Testing of the Nuclear Instrumentation System	7.2-31
7.2.3.3	Periodic Testing of the Process Analog Channels of the Protection Circuits	7.2-32

Chapter 7: Instrumentation and Control

Table of Contents (continued)

Section	Title	Page
7.2.3.4	Safety Guide 22	7.2-32
7.2	References	7.2-32
7.3	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM	7.3-1
7.3.1	Description.....	7.3-1
7.3.1.1	Functional Design.....	7.3-1
7.3.1.2	Design Bases: IEEE Std 279-1971 (Reference 2)	7.3-3
7.3.1.3	Implementation of Functional Design	7.3-5
7.3.2	Analysis	7.3-20
7.3.2.1	Evaluation of Compliance With IEEE Std 279-1971 (Reference 2)	7.3-20
7.3.2.2	Evaluation of Compliance With IEEE Std 308-1969 (Reference 5)	7.3-25
7.3.2.3	Evaluation of Compliance With IEEE Std 323-1971 (Reference 6)	7.3-25
7.3.2.4	Evaluation of Compliance With IEEE Std 334-1971 (Reference 7)	7.3-25
7.3.2.5	Evaluation of Compliance With IEEE Std 338-1971 (Reference 8)	7.3-25
7.3.2.6	Evaluation of Compliance With IEEE Std 344-1971 (Reference 9)	7.3-25
7.3.2.7	Evaluation of Compliance With IEEE Std 317-1971 (Reference 10)	7.3-25
7.3.2.8	Evaluation of Compliance With IEEE Std 336-1971 (Reference 11)	7.3-25
7.3.2.9	Summary.....	7.3-26
7.3.2.10	Automatic Changeover From Injection Mode to Recirculation Mode After Loss of Primary Coolant	7.3-27
7.3.2.11	Inside and Outside Recirculation Spray Pump Start Function (Unit 2 only)	7.3-29
7.3	References	7.3-30
7.3	Reference Drawings	7.3-31
7.4	SYSTEMS REQUIRED FOR SAFE SHUTDOWN	7.4-1
7.4.1	Description.....	7.4-1
7.4.1.1	Design Considerations for the Auxiliary Shutdown Panel.....	7.4-1
7.4.1.2	Auxiliary Shutdown Instrumentation	7.4-3
7.4.1.3	Equipment and Services and Approximate Time Required After Incident that Requires Hot Shutdown.....	7.4-4
7.4.1.4	Equipment and Systems Available for Cold Shutdown	7.4-4
7.4.2	Analysis	7.4-5

Chapter 7: Instrumentation and Control

Table of Contents (continued)

Section	Title	Page
7.5	SAFETY-RELATED DISPLAY INSTRUMENTATION	7.5-1
7.5.1	Description.....	7.5-1
7.5.2	Analysis	7.5-1
7.6	ALL OTHER SYSTEMS REQUIRED FOR SAFETY.....	7.6-1
7.6.1	Instrumentation and Control Power Supplies	7.6-1
7.6.2	Residual Heat Removal System Inlet MOV Interlocks.....	7.6-1
7.6.2.1	Description	7.6-1
7.6.2.2	Analysis	7.6-1
7.6.3	Reactor Coolant System Loop Isolation Valve Interlocks	7.6-2
7.6.3.1	Description	7.6-2
7.6.3.2	Analysis	7.6-2
7.6.4	Main Control Room, Relay Room, and Emergency Switchgear Room Air Conditioning, Heating, and Ventilation System Instrumentation and Controls	7.6-3
7.6.4.1	Description	7.6-3
7.6.4.2	Analysis	7.6-3
7.6.5	Refueling Interlocks.....	7.6-3
7.6.6	Accumulator Isolation Valve Control	7.6-3
7.6.7	Pressurizer Relief Valve Flow Indication	7.6-4
7.6	References	7.6-5
7.7	PLANT CONTROL SYSTEMS	7.7-1
7.7.1	Description.....	7.7-1
7.7.1.1	Reactor Control System	7.7-3
7.7.1.2	Rod Control System	7.7-3
7.7.1.3	Plant Control Signals for Monitoring and Indicating	7.7-5
7.7.1.4	Plant Control System Interlocks	7.7-8
7.7.1.5	Pressurizer Pressure Control.....	7.7-9
7.7.1.6	Pressurizer Water-Level Control	7.7-10
7.7.1.7	Steam Generator Water-Level Control.....	7.7-10
7.7.1.8	Steam Dump Control	7.7-10
7.7.1.9	Incore Instrumentation	7.7-12
7.7.1.10	Computer System	7.7-14
7.7.1.11	Process Instrumentation	7.7-15
7.7.1.12	Control Stations	7.7-15

Chapter 7: Instrumentation and Control

Table of Contents (continued)

Section	Title	Page
7.7.1.13	Control Room Availability	7.7-18
7.7.1.14	ATWS Mitigation System Description	7.7-22
7.7.2	Analysis	7.7-23
7.7.2.1	Separation of Protection and Control Systems	7.7-24
7.7.2.2	Reactivity Control Considerations	7.7-25
7.7.2.3	Step-Load Changes Without Steam Dump	7.7-27
7.7.2.4	Loading and Unloading	7.7-28
7.7.2.5	Load Rejection Furnished by Steam Dump System	7.7-28
7.7.2.6	Turbine Trip with Reactor Trip	7.7-28
7.7	References	7.7-30
7.7	Reference Drawings	7.7-30
7.8	EMERGENCY RESPONSE TO ACCIDENTS	7.8-1
7.9	INADEQUATE CORE COOLING MONITOR (ICCM) SYSTEM	7.9-1
7.9.1	Design Bases	7.9-1
7.9.2	Design Description	7.9-1
7.9.2.1	Core Exit Thermocouple (CET) System—Subsystem of ICCM System	7.9-1
7.9.2.2	Reactor Vessel Level Instrumentation Systems (RVLIS)—Subsystem of ICCM System	7.9-2
7.9.2.3	Core Cooling Monitor System—Subsystem of ICCM System	7.9-3
7.9	References	7.9-4

Chapter 7: Instrumentation and Control

List of Tables

Table	Title	Page
Table 7.2-1	List of Reactor Trips	7.2-35
Table 7.2-2	Reactor Trip System Accuracies and Ranges	7.2-37
Table 7.2-3	Reactor Trip System Interlocks	7.2-39
Table 7.2-4	Trip Correlation	7.2-40
Table 7.2-5	Reactor Trip System Instrumentation	7.2-43
Table 7.3-1	Interlocks for Engineered Safety Features Actuation System	7.3-33
Table 7.3-2	Engineered Safety Feature Actuation System Instrumentation	7.3-34
Table 7.5-1	Main Control Board Indicators and/or Recorders Available to the Operator Condition II and III Events	7.5-5
Table 7.5-2	Main Control Board Indicators and/or Recorders Available to the Operator Condition IV Events	7.5-7
Table 7.5-3	Control Room Indicators and/or Recorders Available to the Operator to Monitor Significant Plant Parameters During Normal Operation	7.5-10
Table 7.7-1	Plant Control System Interlocks	7.7-31
Table 7.7-2	Auxiliary Shutdown Panel Monitoring Instrumentation	7.7-32
Table 7.9-1	Inadequate Core Cooling Monitor (ICCM) System Data	7.9-5

Chapter 7: Instrumentation and Control

List of Figures

Figure	Title	Page
Figure 7.2-1	Index and Symbols	7.2-45
Figure 7.2-2	Reactor Trip Signals	7.2-46
Figure 7.2-3	Nuclear Instrumentation and Trip Signals	7.2-47
Figure 7.2-4	Setpoint Reduction Function for Overtemperature ΔT Trips (Typical)	7.2-48
Figure 7.2-5	Primary Coolant System Trip Signals	7.2-49
Figure 7.2-6	Pressurizer Trip Signals	7.2-50
Figure 7.2-7	Steam Generator Trip Signals	7.2-51
Figure 7.2-8	Turbine Trips, Runbacks, and Other Signals	7.2-52
Figure 7.2-9	Safeguards Actuation Signals	7.2-53
Figure 7.2-10	Nuclear Instrumentation and Blocks	7.2-54
Figure 7.2-11	Pressurizer Reference Leg Level System	7.2-55
Figure 7.2-12	Design to Achieve Isolation Between Channels	7.2-56
Figure 7.2-13	Anticipated Transient without Scram Mitigation System Actuation Circuitry (AMSAC)	7.2-57
Figure 7.3-1	Logic Diagram Motor Driven Steam Generator Auxiliary Feed Pumps . . .	7.3-37
Figure 7.3-2	Unit Trip Signal Interfaces	7.3-38
Figure 7.3-3	Engineered Safety Features Signal Interfaces	7.3-39
Figure 7.3-4	Signal Paths to ESF Actuated Devices	7.3-40
Figure 7.3-5	Loss and Restoration of Emergency Bus	7.3-41
Figure 7.3-6	Diesel Load and Sequencing Conditioning Concept	7.3-42
Figure 7.3-7	Reserve Station Service-Undervoltage	7.3-43
Figure 7.3-8	Removal of Unnecessary Load from Emergency Bus During Containment Depressurization	7.3-44
Figure 7.3-9	Station Service-Undervoltage	7.3-45
Figure 7.3-10	Engineered Safety Features Blocking Logic	7.3-46
Figure 7.3-11	Normally Closed Containment Isolation Trip Valves	7.3-47
Figure 7.3-12	Logic Diagram Turbine Driven-Steam Generator Auxiliary Feed Pump	7.3-48
Figure 7.3-13	Logic Diagram Normally Open Containment Isolation Valves	7.3-49
Figure 7.3-14	ECCS Logic/Automatic Switchover from Injection Phase to Recirculation Phase	7.3-50
Figure 7.4-1	Switching Logic, Sheet 1, for Transfer Between Main Control Board and Auxiliary Shutdown Panel (for Switchgear (Typical))	7.4-6
Figure 7.4-2	Switching Logic, Sheet 2, for Transfer Between Main Control Board and Auxiliary Shutdown Panel [for Switchgear (Typical)]	7.4-7
Figure 7.6-1	Loop Stop Valve Interlocks	7.6-6
Figure 7.6-2	Typical Reactor Coolant System Loop With Loop Stop Valves	7.6-7
Figure 7.6-3	Functional Block Diagram for Opening Accumulator Isolation Valve	7.6-8
Figure 7.7-1	Simplified Block Diagram of Reactor Control System	7.7-33
Figure 7.7-2	Rod Controls and Rod Blocks	7.7-34

Chapter 7: Instrumentation and Control**List of Figures (continued)**

Figure	Title	Page
Figure 7.7-3	Control Bank Rod Insertion Monitor	7.7-35
Figure 7.7-4	Rod Deviation Comparator	7.7-36
Figure 7.7-5	Steam Dump Control	7.7-37
Figure 7.7-6	Pressurizer Pressure and Level Control	7.7-38
Figure 7.7-7	Pressurizer Heater Control	7.7-39
Figure 7.7-8	Feedwater Control and Isolation.	7.7-40
Figure 7.7-9	Block Diagram of Pressurizer Pressure Control System	7.7-41
Figure 7.7-10	Block Diagram of Pressurizer Level Control System.	7.7-42
Figure 7.7-11	Block Diagram of Steam Generator Water Level Control System.	7.7-43
Figure 7.7-12	Block Diagram of Steam Dump Control System	7.7-44
Figure 7.7-13	Basic Flux-Mapping System.	7.7-45

Intentionally Blank

Chapter 7

INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

Note: As required by the Renewed Operating Licenses for North Anna 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.

This chapter describes the various plant instrumentation and control systems by presenting the functional performance requirements, design bases, system descriptions, design evaluations, and tests and inspections for each. The information provided in this chapter applies particularly to those instruments and associated equipment that constitute the protection system as defined in Institute of Electrical and Electronics Engineers (IEEE) IEEE Std 279-1971, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*.

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

It is shown that the applicable criteria and codes concerned with the safe generation of nuclear power, such as the Atomic Energy Commission's (AEC) General Design Criteria and IEEE Standards, were met by these systems.

Instrument loops which support safety-related functions include both those which initiate a protective action, such as a reactor trip or a safety injection, and also those which are used to monitor Technical Specifications or other safety-related parameters. Instrumentation loops include both analog and digital instrumentation signals that initiate protective actions that represent acceptable conditions of the physical processes. The Technical Specification describes and limits appropriate parameters. Appropriately selected reactor protection setpoints and associated analog instrument signal uncertainties define the bases upon which safety is established and proved by the UFSAR Chapter 15 analysis. The verification of actual allowable analog instrumentation signal uncertainties must consider various instrumentation hardware constraints when proving appropriate analog channel statistical allowances. Examples of the kinds of hardware considerations that determine the proper accuracy are as follows:

- Transmitter model

- Calibration tolerances, methods, and frequencies
- Measurement and test equipment ranges and accuracies
- Loop scaling

These hardware considerations have all been accounted for in verifying the allowable instrument uncertainty associated with each safety-related instrument loop.

7.1.1 Definitions

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

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

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

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

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

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

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

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

Degree of Redundancy - The difference between the number of channels monitoring a variable and the number of channels that, when tripped, will cause an automatic system trip.

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

Hot-Shutdown Condition - When the reactor is subcritical by an amount greater than or equal to the margin specified in the Technical Specifications, and T_{avg} is greater than or equal to the temperature specified in the Technical Specifications.

Containment Isolation Phase A - Closure of all nonessential process lines that penetrate containment. Initiated by the safety injection activation signal.

Containment Isolation Phase B - Closure of remaining process lines. Initiated by containment high-high-pressure signal (process lines do not include engineered safety features lines).

Trip Accuracy - The tolerance band of the difference between (1) the desired trip point value of a process variable, and (2) the actual value at which a comparator trips (and thus actuates some desired result).

Technically, trip accuracy describes the maximum inaccuracy or maximum uncertainty associated with the desired trip setpoint. Trip accuracy is usually expressed in percent of instrument span. Trip accuracy identifies, in both the positive and negative directions, the furthest point from the desired trip setpoint at which trip actuation could occur. This is also referred to as the channel statistical allowance, CSA. Thus, the trip setpoint accuracy envelopes a range around the desired trip setpoint within which an actual trip must occur.

The following instrument loop error terms are included, as required, when determining trip accuracy: systematic error, process measurement accuracy, primary element accuracy, sensor calibration accuracy, sensor measuring and test equipment, sensor drift, sensor pressure effect, sensor temperature effect, sensor power supply effect, rack calibration accuracy, rack measuring and test equipment, rack temperature effect, rack drift, and environmental allowances. The use of these error terms are addressed in Reference 6 and associated engineering standards or calculations.

Actuation Accuracy - Synonymous with trip accuracy, but used where the word “trip” may cause ambiguity.

Indicated Accuracy - The tolerance band containing the highest expected value of the difference between (1) the value of a process variable read on an indicator or recorder and (2) the actual value of that process variable. The tolerance band includes the inaccuracies associated with the instrument channel and the readout devices. It also includes process rack environmental effects, but does not include process effects such as fluid stratification.

Reproducibility - This term may be substituted for “accuracy” in the above definitions for those cases where a trip value or indicated value need not be referenced to an actual process variable

value, but rather to a previously established trip or indication value; this value is determined by test.

7.1.2 Identification of Safety-Related Systems

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

1. Reactor trip system, discussed in Section 7.2.
2. Engineered safety features actuation system, discussed in Section 7.3.
3. Vital ac power systems, discussed in Section 8.3.1.2.
4. Service water system, discussed in Section 9.2.1.
5. Air conditioning and ventilation systems for safety-related equipment, discussed in Section 9.4.
6. Charging pump auxiliary lube-oil pump.
7. Component cooling pumps, discussed in Section 9.2.2.
8. Onsite power system, discussed in Section 8.3.

The reactor trip system and the engineered safety features actuation system are functionally defined systems. The functional descriptions of these systems are in Sections 7.2 and 7.3 respectively. The equipment that provides the trip functions identified in Section 7.2, Reactor Trip System, is contained in the following:

1. Process instrumentation and control system (Reference 1).
2. Nuclear instrumentation system (Reference 2).
3. Solid-state logic protection system (Reference 3).
4. Reactor trip switchgear (Reference 3).
5. Manual actuation circuit.

The equipment that provides the actuation functions identified in Section 7.3, Engineered Safety Features Actuation System, is contained in the following:

1. Process instrumentation and control system. (Reference 1).
2. Solid-state logic protection system (Reference 3).
3. Engineered safety features test cabinet (Reference 4).
4. Manual actuation circuits.
5. Actuation devices.

7.1.3 Identification of Safety Criteria

7.1.3.1 Design Criteria Compliance

The compliance of safety-related systems with the following documents is discussed in the appropriate sections of Chapter 7:

1. *General Design Criteria for Nuclear Power Plants*, Appendix A to 10 CFR 50, July 7, 1971.
2. *Safety Guides for Water Cooled Nuclear Power Plants*, Division of Reactor Standards, Atomic Energy Commission, October 27, 1971.
3. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*, IEEE Std 279-1971.
4. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard Criteria for Class IE Electric Systems for Nuclear Power Generating Stations*, IEEE Std 308-1971.
5. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations*, IEEE Std 317-1971.
6. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations*, IEEE Std 323-1971.
7. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations*, IEEE Std 334-1971.
8. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard: Installation, Inspection, and Testing Requirements for Instrumentation and Electrical Equipment During the Construction of Nuclear Power Generating Stations*, IEEE Std 336-1971.
9. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems*, IEEE Std 338-1971.
10. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations*, IEEE Std 344-1971.

7.1.3.2 Reactor Trip System

The reactor trip system acts to limit the consequences of Condition II events (faults of moderate frequency such as loss of feedwater flow) by, at most, a shutdown of the reactor and turbine, with the plant capable of returning to operation after corrective action. The reactor trip system features impose a limiting boundary region to plant operation that ensures that the reactor

safety limits are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions.

7.1.3.2.1 Functional Performance Requirements

7.1.3.2.1.1 *Reactor Trips.* The reactor trip system automatically initiates reactor trip as follows:

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

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

7.1.3.2.1.3 *Manual Trip.* The reactor trip system provides for manual initiation of reactor trip by operator action.

7.1.3.2.1.4 *Feedwater Isolation.* The reactor trip system provides a signal whenever reactor trip is initiated (in conjunction with interlock P-4), which closes main feedwater valves on T_{avg} below setpoint. The signal also prevents opening main feedwater valves that were closed by safety injection or high steam generator water level.

7.1.3.2.1.5 *Safety Injection.* The reactor trip system provides a signal whenever reactor trip is initiated (in conjunction with interlock P-4), which automatically blocks the automatic re-actuation of safety injection (after safety injection has been reset).

7.1.3.2.2 Design Bases

The design requirements for the reactor trip system are derived by analyses of plant operating and fault conditions where automatic rapid control rod insertion is necessary to prevent or limit core or reactor coolant boundary damage. The design limits for this system are as follows:

1. Minimum departure from nucleate boiling ratio (DNBR) shall not be less than the design DNBR limit as a result of any anticipated transient or malfunction (Condition II faults).
2. Power density shall not exceed the rated linear power density for Condition II faults. See Chapter 4 for fuel design limits.
3. The stress limit of the reactor coolant system for the various conditions shall be as specified in Chapter 5.
4. The release of radioactive material shall not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius as a result of any Condition III fault.

5. For any Condition IV fault, the release of radioactive material shall not result in an undue risk to public health and safety.

7.1.3.2.3 Codes and Standards

The reactor protection instrumentation meets IEEE criteria as set forth in IEEE Std 279-1971, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*. An exception to the criteria is justified in Section 7.2.2.3.5.

7.1.3.2.4 Environmental Requirements

The environmental design bases are given in Sections 3.10 and 3.11 and in IEEE Std 279-1971. A list of the nuclear steam supply system (NSSS) protection channels required to operate in the postaccident environment, and the required duration of operation, is included in Section 3.11.

In the North Anna Units 1 and 2 spaces containing Class 1E equipment where Class 1E redundant ventilation or air conditioning systems are not provided and the temperature could exceed that for which the Class 1E equipment is qualified, a temperature monitoring system is provided that will meet the following requirements:

1. An alarm will occur in the control room when the qualified temperature range is exceeded. The necessary instrumentation:
 - a. Is of high quality.
 - b. Has testing facilities to verify its functional capability.
 - c. Is powered from a reliable power source (semi-vital bus originating from an emergency bus).
2. Operating procedures require the control room operator to log the receipt of all alarms, the action taken, and the alarm clearing. The temperature in the alarmed area will be recorded periodically, either manually or automatically, during the time that the temperature is above the alarm setpoint.

For alarms of temperature exceeding the equipment qualification, an analysis will be provided to demonstrate that the excess temperature has not degraded the equipment below a level acceptable for continued operations.

7.1.3.3 Engineered Safety Features Actuation System

The engineered safety features (ESF) system acts to limit the consequences of Condition III events (infrequent faults such as primary coolant spillage from a small rupture that exceed normal charging system makeup and require the actuation of the safety injection system). The ESF system also acts to mitigate Condition IV events (limiting faults, which include the potential for significant release of radioactive material). The ESF system consists of the ESF actuation system as discussed in Section 7.3 and the ESF-actuated devices discussed in Chapter 6.

7.1.3.3.1 Functional Performance Requirements

7.1.3.3.1.1 *General Performance Requirements.* Signals additional to those developed by the reactor trip system are generated by the ESF actuation system to protect against the effects (and reduce the consequences) of more serious types of accidents designated as Condition III and IV events. These are serious abnormal conditions in the reactor coolant system, main steam system, or containment vessel, and include a loss-of-coolant accident (LOCA) or a steam-line break.

The functional performance requirements for the ESF system are discussed in detail in Chapter 6.

7.1.3.3.1.2 *Automatic Actuation Requirements.* The primary functional requirement of the ESF actuation system is to receive input signals (information) from the various operating processes within the reactor plant and containment and automatically provide, as output, timely and effective signals to actuate the various components and subsystems comprising the ESF actuated devices. These output signals, in conjunction with the actuated devices, ensure that the ESF system will meet its performance objectives as outlined in Chapter 6.

The logic diagrams and functional diagrams represented in Reference Drawings 1 through 15 and Figures 7.2-5, 7.2-6, 7.2-7, 7.2-9, 7.3-1, 7.3-5, 7.3-7, 7.3-8, 7.3-10, 7.3-12, and 7.3-14 provide a graphic outline of the functional requirements of the actuation system and its devices.

7.1.3.3.1.3 *Manual Actuation Requirements.* The ESF actuation system has provisions for manually initiating from the control room all of the functions of the ESF system. Manual actuation serves as backup to the automatic initiation and provides selective control of ESF service features.

7.1.3.3.2 Design Bases

The design bases for the engineered safety features are in Chapter 6.

The following is a discussion of the design requirements imposed on the ESF actuation system by the design-base objectives.

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

To accomplish these design objectives, the ESF system shall have proper and timely initiating signals supplied by the sensors, transmitters, and logic components making up the

various instrumentation channels of the ESF actuation system. The specific functions that rely on the ESF actuation system for initiation are the following:

1. A reactor trip, provided one has not already been generated by the reactor trip system.
2. Proper load application sequencing of ESF power demands on the ESF buses (supplied by either preferred or standby power supply).
3. Cold-leg injection isolation valves, which are opened for the injection of borated water by charging/safety injection pumps into the cold legs of the reactor coolant system.
4. Charging/safety injection pumps, and associated valving, which provide the injection of water to the cold leg of the reactor coolant system following a LOCA.
5. Low-head safety injection pumps, which start to provide borated makeup water to the cold legs of the reactor coolant loops.
6. Service water system pumps and valves, which provide cooling water to the recirculation spray heat exchangers and are thus the heat sink for containment cooling.
7. Auxiliary feedwater pumps.
8. Containment isolation phase A, whose function is to prevent fission product release.
9. Steam-line isolation, to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled reactor coolant system cooldown.
10. Main feedwater-line isolation, to limit the energy release in the case of a steam-line break and to limit the magnitude of the reactor coolant system cooldown.
11. Emergency diesel starting, to ensure backup supply of power to emergency and supporting systems components.
12. Containment depressurization system actuation, which performs the following functions:
 - a. Initiates containment quench and recirculation spray subsystems, which serve to reduce containment pressure and temperature following a loss-of-coolant or steam-line-break accident.
 - b. Initiates containment isolation phase B, which isolates the containment following a LOCA or a feedwater-line or steam-line break within containment.

7.1.3.3.3 Codes and Standards

The ESF actuation system meets the criteria as set forth in IEEE Std 279-1971, *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*. An exception is justified in Section 7.2.2.3.5.

In addition, the minimum performance for each of the ESF actuation systems specified in terms of time response, accuracy, and range is in accordance with the requirements set forth in this document.

7.1.3.3.4 Environmental Requirements

The environmental design bases are given in Sections 3.10 and 3.11 and in IEEE Std 279-1971.

7.1.3.4 Instrumentation and Control Power Supply

The functional performance requirements for the instrumentation and control power supplies are described in detail in Chapter 8.

7.1.3.5 Quality Assurance

The quality assurance program applied to safety-related instrumentation and control system components is described in Chapter 17.

7.1.3.6 Safety-Related Equipment Identification

There are two sets of separate process analog racks. One set contains instrumentation furnished by the architect-engineer, the other contains instrumentation furnished by the NSSS supplier. The separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and analog protection racks to the redundant trains in the logic racks. Redundant analog channels are separated by locating modules in different rack sets. Since all equipment within any analog rack is associated with a single protection set, there is no requirement for the separation of wiring and components within the rack. Barriers are provided in the logic rack to separate channel inputs. A color-coded nameplate on each analog rack is used to differentiate between protective and nonprotective sets. The color coding of the nameplates is as follows:

Protection Set	Color Coding
I	Red with white lettering
II	White with black lettering
III	Blue with white lettering
IV	Yellow with black lettering

All non-rack-mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on their enclosures. All cable identification is discussed in Chapter 8.

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

There are identification nameplates on the input panels of the digital logic system. For details of the digital logic system, see Sections 7.2 and 7.3.

The installation of all cable, including separation requirements for control board wiring, complies with the criteria presented in Chapter 8.

Redundant sensors, sensing lines, and actuating devices are separated by either space, physical barriers, or both. The sensing lines are normally routed to missile-protected areas where the transmitters are located. In areas where the potential for missiles is high and where no physical barriers are provided, sensors, sensing lines, and actuating devices are physically separated by a minimum distance of 4 feet in any direction. Sensing lines passing through walls are also physically separated, or each sensing line is protected by rigid steel conduit when passage is made through a common opening in a wall.

In areas where the potential for missiles is very low, sensors, sensing lines, and actuating devices are separated by at least 12 inches where barriers are not used.

7.1.4 Regulatory Guide 1.97

Reg. 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 Reg. 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 Reg. 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 Reg. 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 Reg. 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, Reg. 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 to 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. Any required equipment upgrades will be 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. Any further exceptions to the Regulatory Guide will also be relayed to the NRC by correspondence for their review and approval. Virginia Power maintains a plant specific technical report, PE-0013, that provides a tabular identification of Regulatory Guide 1.97 associated equipment (Reference 5).

7.1 REFERENCES

1. J. A. Nay, *Process Instrumentation for Westinghouse Nuclear Steam Supply Systems*, WCAP-7547-L, March 1971 (Westinghouse NES Proprietary); WCAP-7671, May 1971 (non proprietary); and J. B. Reid, *Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, (W CID 7300 Series)*, WCAP-7913.
2. J. B. Lipchak and R. A. Stokes, *Nuclear Instrumentation System*, WCAP-7380-L, January 1971 (Westinghouse NES Proprietary); and WCAP-7669, May 1971 (non proprietary).
3. D. N. Katz, *Solid State Logic Protection System Description*, WCAP-7488-L, March 1971 (Westinghouse NES Proprietary); and WCAP-7672, May 1971 (non proprietary).
4. J. T. Haller, *Engineered Safeguards Final Device or Activator Testing*, WCAP-7705.
5. Technical Report PE-0013, *North Anna Power Station Response to Regulatory Guide 1.97*.
6. Technical Report EE-0101, *Setpoint Bases Document*.

7.1 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.	11715-LSK-27-12A	Typical Loop Diagram for Each Channel Hi-Hi Containment Pressure Protection
2.	11715-LSK-27-12B	Hi-Hi Containment Pressure Protection and Indication, Unit 1
3.	11715-LSK-27-12C	Containment Depressurization Actuation and Reset, Train A
4.	11715-LSK-27-12D	Hi Containment Pressure Protection
5.	11715-LSK-27-12E	Intermediate Hi-Hi Containment Pressure Protection Protection
6.	11715-LSK-27-12F	Containment Depressurization Actuation and Reset, Train B
7.	11715-LSK-28-5C	Safety Injection System, Actuated Devices
8.	11715-LSK-27-12G	Containment Depressurization Actuated Devices
9.	11715-LSK-5-13A	Logic Diagram: Motor Driven Steam Generator, Auxiliary Feedwater Pumps
10.	11715-LSK-5-8H	Feedwater Isolation Trip Valves
11.	11715-LSK-32-1C	Logic Diagram: Normally Closed Containment Isolation Trip Valves
12.	11715-LSK-5-13B	Turbine Driven, Steam Generator, Auxiliary Feedwater Pumps
13.	11715-LSK-5-13C	Auxiliary Feedwater Control Valves
14.	11715-LSK-8-18A	Main Steam Isolation Trip Valve
15.	11715-LSK-8-18D	Main Steam Isolation Bypass Valve

7.2 REACTOR TRIP SYSTEM

Electrical schematic diagrams for the reactor trip system and its supporting systems were included in reports NA-TR-1001 and NA-TR-1002, *Safety Related Electrical Schematics*, dated May 10, 1973, which were submitted to the Atomic Energy Commission (AEC) on May 18, 1973, as separate documents. Figure 7.2-1 shows the symbols used in the logic diagrams that are included as appropriate throughout the chapter.

7.2.1 Description

The reactor trip system uses sensors that feed analog circuitry consisting of two to four redundant channels that monitor various plant parameters. The reactor trip system also contains the digital logic circuitry necessary to automatically open the reactor trip breakers. The digital circuitry consists of two redundant logic trains that receive inputs from the analog protection channels.

Each of the two trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively. The two trip breakers in series connect three-phase ac power from the rod drive motor-generator sets to the rod drive power cabinets, as shown in Figure 7.2-2. During plant power operation, a dc undervoltage coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For reactor trip, a loss of dc voltage to the undervoltage coil releases the trip plunger and trips open the breaker. A shunt trip relay is installed in parallel with the undervoltage attachment. Upon de-energization, contacts from the relay energize the reactor trip breaker shunt trip attachment and trips open the breaker. This provides a redundant/backup means to automatically trip the breakers upon the receipt of a trip signal from the reactor trip system. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall by gravity into the core. The rods cannot be withdrawn until an operator resets the trip breakers. The trip breakers cannot be reset until the bi-stable that initiated the trip is re-energized. Bypass breakers BYA and BYB are provided to permit the testing of the trip breakers, as discussed below.

The following are the generating station conditions requiring reactor trip (see Section 7.1.3.2.2):

1. Core approaching thermal hydraulic limits.
2. Power density (kW/ft) approaching rated value for Condition II faults (see Chapter 4 for fuel design limits).
3. Reactor coolant system overpressure creating stresses approaching the limits specified in Chapter 5.

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

1. Neutron flux.
2. Reactor coolant temperature.
3. Reactor coolant system pressure (pressurizer pressure).
4. Pressurizer water level.
5. Reactor coolant flow.
6. Reactor coolant pump operational status (bus voltage and frequency, and breaker position).
7. Steam generator feedwater flow.
8. Steam generator water level.
9. Turbine-generator operational status (autostop oil pressure and stop valve position).

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

The allowable values associated with the parameters that will require reactor trip are given in the Technical Specifications and in Chapter 15, Accident Analyses. Chapter 15 proves that the setpoints used in the Technical Requirements Manual are conservative.

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

1. Minimum DNBR greater than the limit value.
2. Maximum system pressure = 2750 psia.
3. Fuel rod maximum linear power less than the value corresponding to fuel centerline melting.

The accident analyses described in Section 15.2 demonstrate that the functional requirements as specified for the reactor trip system are adequate to meet the above considerations, even assuming, for conservatism, adverse combinations of instrument errors (refer to Tables 15.1-3 and 15.1-4). A discussion of the safety limits associated with the reactor core and reactor coolant system, plus the limiting safety system setpoints (allowable values), is presented in the Technical Specifications.

For a discussion of energy supply and environmental variations, see Sections 8.3.1.2 and 3.11, respectively.

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

1. Earthquakes, discussed in Chapters 2 and 3.
2. Fire, discussed in Section 9.5.
3. Explosion (hydrogen buildup inside containment), discussed in Section 6.2.
4. Missiles, discussed in Section 3.5.
5. Flood, discussed Chapters 2 and 3.
6. Wind and tornadoes, discussed in Section 3.3.

The performance requirements are as follows:

1. System response times:

The reactor trip system response time, or total delay to trip, is defined in the Technical Specifications. During periodic testing as required by Technical Specifications, it is demonstrated that instrument errors and time delays are equal to or less than the values assumed in the safety analyses.

Maximum allowable time delays in generating the reactor trip signal are given in the Technical Requirements Manual.

2. Reactor trip accuracies and ranges are given in Table 7.2-2 and Reference 19.

7.2.1.1 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the reactor trip system reaches a preset level. In addition to redundant channels and trains, the design approach provides a reactor trip system that monitors numerous system variables, that is, provides reactor trip system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in Reference 1.

Table 7.2-1 provides a list of reactor trips, coincidence requirements, and interlocks, which are described below.

Table 7.2-5 provides a list of reactor trip system instrumentation with the number of channels to trip and the minimum channels that are required operable.

7.2.1.1.1 Nuclear Overpower Trips

The specific trip functions generated are as follows:

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

There are two independent bi-stables, each with its own trip setting used for a high and a low setting. The high trip setting provides protection during normal power operation and is always active. The low trip setting, which provides protection during startup, can be manually bypassed when two out of the four power range channels read above approximately 10% power (P-10). Three out of the four channels below 10% automatically reinstate the trip function. Refer to Table 7.2-3 for a listing of all reactor trip system interlocks.

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

4. Power range neutron flux rate trips (PRRT)—Refer to Figure 7.2-3. The functional diagram shown includes reactor trip logic provided to trip the reactor when an abnormal rate of increase or decrease in nuclear power occurs in two out of four power range channels.
 - a. Power range high positive neutron flux rate trip—The bi-stables associated with high positive flux rate trip for an abnormal rate of increase in nuclear power. The reactor is tripped when a high positive rate occurs in two out of the four power range channels. This trip provides protection against rod ejection accidents of low worth from midpower and is always active.
 - b. Power range high negative neutron flux rate trip—The bi-stables associated with high negative flux rate trip for an abnormal rate of decrease in nuclear power. The reactor is tripped when a high negative rate occurs in two out of the four power range channels. This trip provides protection against two or more dropped rods and is always active. Protection against one dropped rod is not required to prevent the occurrence of DNBR at full power per the analysis in Section 15.2.3.

These channels of the reactor trip system derive signals from the power range uncompensated ion chambers. In the nuclear instrumentation system, the rate sensor assembly is an operational amplifier unit that incorporates an adjustable lag network at one input and a nondelayed 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 two bi-stable units that trip when the level of the signal exceeds a preset value. The bi-stable units are the latching type to ensure that the necessary action, once initiated, will be carried to completion. The bi-stable outputs are provided to the solid-state protection system where the logic shown in Figure 7.2-3 is performed to provide a reactor trip when abnormal nuclear power rates occur.

The operability of the rate trip functions associated with dropped rod and ejected rod protection is verified by the introduction of a signal step change using the channel drawer test circuits. The time delay setting of the rate module is predetermined by analysis to correspond to high positive or negative power rate associated with the above events and is tested during initial startup testing.

Figure 7.2-3 shows the logic for all of the nuclear overpower and rate trips. A detailed functional description of the equipment associated with the negative flux rate (dropped rod) function is given in Reference 2. The positive rate trip function is generated by the same device but uses an additional bi-stable amplified in each protection channel.

7.2.1.1.2 Core Thermal Overpower Trips

The specific trip functions generated are as follows:

1. Overtemperature delta T trip—This trip protects the core against low DNBR and trips the reactor on coincidence as listed in Table 7.2-1 using one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by analog circuitry for each channel by solving the following equation:

$$\Delta T_{\text{setpoint}} = \Delta T_o \left\{ K_1 - K_2 \frac{1 + \tau_1 s}{1 + \tau_2 s} (T_{\text{avg}} - T') + K_3 (P - 2235) - f_1(\Delta q) \right\} \quad (7.2-1)$$

where:

$\Delta T_{\text{setpoint}}$ = ΔT reactor trip setpoint, °F

ΔT_o = indicated ΔT at full power (RTP), °F

T_{avg} = measured average reactor coolant temperature, °F

T' = nominal average reactor coolant temperature at full power, °F

P = measured pressurizer pressure, psig

K_1 = setpoint bias, dimensionless

K_2 = constant based on the effect of temperature on the DNB limits, °F⁻¹

K_3 = constant based on the effect of pressure on the DNB limits, psig⁻¹

τ_1, τ_2 = time constants, sec

s = Laplace transform variable, sec⁻¹

$f_1(\Delta q)$ = a function of the neutron flux difference between upper and lower long ion chambers, dimensionless. One power range channel separately feeds each overtemperature ΔT trip channel. A non-zero $f_1(\Delta q)$ can only lead to a decrease in trip setpoint. Refer to Figure 7.2-4.

The single pressurizer pressure parameter required per channel is obtained from separate sensors that are connected to three pressure taps at the top of the pressurizer. This results in one pressure tap per channel. Refer to Section 7.2.2.3.3 for an analysis of this.

Figure 7.2-5 shows the logic for the overtemperature delta T trip function. A detailed functional description of the process equipment associated with this function is contained in Reference 3.

2. Overpower delta T trip—This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence, as listed in Table 7.2-1, with one set of

temperature measurements per loop. The setpoint for each channel is continuously calculated using the following equation:

$$\Delta T_{\text{setpoint}} = \Delta T_o \left\{ K_4 - K_5 \frac{\tau_3 s}{1 + \tau_3 s} T_{\text{avg}} - K_6 (T_{\text{avg}} - T') - f_2(\Delta q) \right\} \quad (7.2-2)$$

where:

$\Delta T_{\text{setpoint}} = \Delta T$ reactor trip setpoint, °F

$\Delta T_o =$ indicated ΔT at full power (RTP), °F

$f_2(\Delta q) =$ a function of the neutron flux difference between upper and lower long ion chamber section, dimensionless

$K_4 =$ a preset, manually adjustable bias, dimensionless

$K_5 =$ a constant based on the effect of rate of change of T_{avg} on overpower ΔT limit, °F⁻¹

$K_6 =$ a constant based on the effect of T_{avg} on overpower ΔT limit, °F⁻¹

$T' =$ nominal average reactor coolant temperature at full power, °F

$T_{\text{avg}} =$ measured average reactor coolant temperature, °F

$\tau_3 =$ time constant, sec

$s =$ Laplace transform variable, sec⁻¹

The source of temperature and flux information is identical to that of the overtemperature delta T trip, and the resultant delta T setpoint is compared to the same measured delta T. Figure 7.2-5 shows the logic for this trip function. The detailed functional description of the process equipment associated with this function is contained in Reference 3.

7.2.1.1.3 Reactor Coolant System Pressurizer Pressure and Water Level Trips

The specific trip functions generated are as follows:

1. Pressurizer low-pressure trip—The purpose of this trip is to protect against low pressure, which could lead to a DNBR less than the design limit and to limit the necessary range of protection afforded by the overtemperature delta T trip. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 the reactor is tripped when the compensated pressurizer pressure measurements fall below preset limits. This trip is blocked below P-7 to permit startup.

The trip logic is shown in Figure 7.2-6. A detailed functional description of the process equipment associated with the function is contained in Reference 3.

2. Pressurizer high-pressure trip—The purpose of this trip is to protect the reactor coolant system against system overpressure.

The same sensors and transmitters used for the pressurizer low-pressure trip are used for the high-pressure trip except that separate bi-stables are used for the high-pressure trip. These bi-stables trip when uncompensated pressurizer pressure signals exceed preset limits. There are no interlocks or permissives associated with this trip function.

The logic for this trip is shown in Figure 7.2-6. The detailed functional description of the process equipment associated with this trip is provided in Reference 3. See also Section 3.11 for details concerning the environmental qualification of the pressurizer pressure transmitters.

3. Pressurizer high water level trip—This trip is provided as a backup to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves. This trip is blocked below P-7 to permit startup.

The trip logic for this function is shown in Figure 7.2-6. A detailed description of the process equipment associated with this function is contained in Reference 3.

7.2.1.1.4 Reactor Coolant System Low-Flow Trips

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

1. The parameter sensed is reactor coolant flow. Three elbow taps in each coolant loop are used as a flow device that indicates the status of reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow rate has occurred. An output signal from two out of the three bi-stables in a loop would indicate a low flow in that loop.

The detailed functional description of the process equipment associated with the trip function is contained in Reference 3.

2. Reactor coolant pump bus undervoltage trip—This trip is required to protect against low flow, which can result from a loss of voltage to more than one reactor coolant pump (e.g., from station blackout).

There are two undervoltage sensing relays connected to each reactor coolant pump bus. These relays provide an output signal when the bus voltage goes below approximately 70% of rated voltage. Signals from these relays are time delayed to prevent spurious trips caused by short-term voltage perturbations.

3. Reactor coolant pump bus underfrequency trip—This trip is required to protect against low flow resulting from bus underfrequency, for example, a major power grid frequency disturbance. The function of this trip is to trip the reactor for an underfrequency condition.

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

4. An additional input into this sensing system is provided by the reactor coolant pump breaker trip—The opening of one or two reactor coolant pump breakers (depending on power level), which is indicative of an imminent loss of coolant flow in that loop, or loops, will also cause a reactor trip.

Two sets of auxiliary contacts on each pump breaker serve as the input signal to the trip logic. The logic is designed on an energize-to-trip basis. However, this is an anticipatory trip and no credit has been taken for this function since other de-energize to trip logics provide reactor trip on loss of coolant flow.

Figure 7.2-5 shows the logic for the reactor coolant system low-flow trips.

7.2.1.1.5 Steam Generator Trips

The specific trip functions generated are as follows:

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

Figure 7.2-7 shows the logic for this trip function.

A detailed functional description of the process equipment associated with this function is provided in Reference 3.

2. Low-low steam generator water level trip—This trip protects the reactor from a loss of heat sink in the event of a sustained steam/feedwater flow mismatch of insufficient magnitude to cause a steam/feedwater flow mismatch and low SG water level trip. This trip is actuated on two out of three low-low water level signals occurring in any steam generator, provided that the stop valves for that loop are open.

The logic is shown in Figure 7.2-7. A detailed functional description of the process equipment associated with this trip is provided in Reference 3.

In addition, an independent trip may be actuated by the anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC). This system is operational when the C-20 permissive is satisfied by the unit being above a specific power level based on turbine first stage pressure. When the narrow range steam generator level detected by two out of three channels on each of two out of three steam generators is below the AMSAC setpoint and the C-20 permissive is satisfied, an AMSAC trip can be generated. The AMSAC steam generator level can be the same as the RPS low-low level setpoint or may be set as much as 5% lower than the RPS setpoint, providing certain criteria are met. The AMSAC trip is time delayed to allow the RPS to

function prior to AMSAC action. AMSAC trips the turbine directly and trips the reactor by tripping the power feeder breakers for the rod control motor generator sets. This logic is shown in Figure 7.2-13. Further description of the C-20 permissive setpoint and its basis is provided in Section 7.7.1.14.

7.2.1.1.6 Turbine Trip-Reactor Trip

The turbine trip-reactor trip is actuated by either two-out-of-three logic from the low auto-stop oil pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above P-8. This is shown in Figure 7.2-8.

In addition, an independent turbine trip may be actuated by the anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC). This system is operational when the C-20 permissive is satisfied by the unit being above a specific power level based on turbine first stage pressure. When the narrow range steam generator level detected by two out of three channels on each of two out of three steam generators is below the AMSAC setpoint and the C-20 permissive is satisfied, an AMSAC trip can be generated. The AMSAC steam generator level can be the same as the RPS low-low level setpoint or may be set as much as 5% lower than the RPS setpoint, providing certain criteria are met. The AMSAC trip is time delayed to allow the RPS to function prior to AMSAC action. AMSAC trips the turbine directly. The logic is shown in Figure 7.2-13. Further description of the C-20 permissive setpoint and its basis is provided in Section 7.7.1.14.

High-high steam generator level signals in two out of three channels for any steam generator will actuate a turbine trip, trip the main feedwater pumps, close the main and bypass feedwater control valves, and close the main feed line isolation valves. The purpose is to protect the turbine and steam piping from excessive moisture carryover caused by high-high steam generator water level. Other turbine trips are discussed in Chapter 10.

The logic for this trip is shown in Figure 7.2-7.

The analog portion of the trip shown in Figure 7.2-8 is represented by dashed (---) lines. When the turbine is tripped, turbine auto-stop oil pressure drops, which will be sensed by three pressure sensors. A digital output is provided from each sensor when the auto-stop oil pressure drops below a preset value. These three outputs are transmitted to two redundant two-out-of-three logic matrices, either of which trips the reactor if above P-8.

The auto-stop oil pressure signal also dumps the electro-hydraulic control oil closing all of the turbine steam throttle valves. When all throttle valves are closed, a reactor trip signal will be initiated if the reactor is above P-8. This trip signal is generated by redundant (two each) limit switches on the stop valves.

7.2.1.1.7 Safety Injection Signal Actuation Trip

A reactor trip occurs when the safety injection system is actuated. The means of actuating the safety injection system are described in Section 7.3. This trip protects the core during a loss of reactor coolant or steam-line break.

Figure 7.2-9 shows the logic for this trip. A detailed functional description of the process equipment associated with this trip function is provided in Reference 3.

7.2.1.1.8 Manual Trip

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

There are no interlocks that can block this trip. Figure 7.2-3 shows the manual trip logic.

7.2.1.2 Reactor Trip System Accuracies and Response Times

The system accuracies and the system response times of the instrument trip signals required for plant safety are given in Tables 7.2-2 and 15.1-3, respectively.

Periodic response time testing of the reactor trip and ESF systems has been established in the Technical Specifications to meet the intent of IEEE Std 338-1971.

7.2.1.3 Reactor Trip System Interlocks

7.2.1.3.1 Power Escalation Permissives

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

A one-of-two intermediate range permissive signal (P-6) is required before 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 is a manual reset switch for administratively reactivating the source range level trip and detector high voltage when between the permissive P-6 and P-10 level if required. Source range level trip block and high-voltage cutoff are always maintained when above the permissive P-10 level.

The intermediate range level trip and power range (low setpoint) trip can 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 low-range power range trip and intermediate range trip can be independently blocked. These trips are automatically

reactivated when any three of the four power range channels are below the permissive (P-10) level, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown in Figure 7.2-10. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

See Table 7.2-3 for the list of reactor trip system interlocks.

7.2.1.3.2 Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip at low power (below approximately 10% of full power) on a low reactor coolant flow or reactor coolant pump open breaker signal in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, or pressurizer high water level. See Figures 7.2-5, 7.2-6 and 7.2-8 for permissive applications. The low-power signal is derived from three out of four power range neutron flux signals below the setpoint in coincidence with two out of two turbine impulse chamber pressure signals below the setpoint (low plant load).

The P-8 interlock blocks a reactor trip when the plant is below approximately 30% of full power, on a low reactor coolant flow in any one loop, a reactor coolant pump breaker open signal in any one loop, or turbine trip signal. Below the P-8 setpoint, the reactor will not trip with a turbine trip, or with one inactive loop. The reactor could be allowed to operate with one inactive loop, provided Technical Specifications are amended to authorize this mode of operation. See Figure 7.2-10 for the derivation of P-8 and Figures 7.2-5 and 7.2-8 for applicable logics.

See Table 7.2-3 for the list of protection system blocks.

7.2.1.4 Coolant Temperature Sensor Arrangement

Three thermowell mounted resistance temperature detectors are installed in the hot leg of each loop near the inlet to the steam generator for reactor protection and control. One thermowell mounted resistance temperature detector is installed in the cold leg of each loop at the discharge of the reactor coolant pump for reactor protection and control.

7.2.1.5 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water-level instrumentation includes the usual tank level arrangement using differential pressure between an upper and a lower tap. Refer to Section 7.2.2.3.4 for an analysis of this arrangement.

7.2.1.6 Analog System

The process analog system is described in Section 7.7.1.11 and Reference 3.

7.2.1.7 Digital Logic System

The solid-state protection logic system takes binary inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light, and computer input signals, which indicate the condition of bi-stable input signals, partial-trip and full-trip functions, and the status of the various blocking, permissive, and actuation functions. In addition, the system includes means for semi-automatic testing of the logic circuits. A detailed description of this system is given in Reference 4.

7.2.1.8 Isolation Amplifiers

In certain applications, Westinghouse considers it advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel, as permitted by IEEE Std 279-1971. IEEE Std 279-1971 specifies design criteria for protection channels which also provide a control function. An exception to these criteria is justified in Section 7.2.2.3.5.

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

Isolation amplifier qualification tests are described in References 5 and 6.

7.2.1.9 Energy Supply and Environmental Variations

The energy supply for the reactor trip system, including the voltage and frequency variations, is described in Section 8.3. The environmental variations throughout which the system will perform are given in Section 3.11.

7.2.1.10 Trip Setpoints

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

7.2.1.11 Seismic Design

The seismic design considerations for the reactor trip system are given in Section 3.10. This design meets the requirements of General Design Criterion 2.

7.2.2 Analysis

7.2.2.1 Evaluation of Design

7.2.2.1.1 General Discussion

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

While most setpoints used in the reactor protection system are fixed, there are variable setpoints, most notably the overtemperature delta T and overpower delta T setpoints. All setpoints in the reactor trip system have been selected either on the basis of applicable engineering code requirements or engineering design studies. The capability of the reactor trip system to prevent a loss of integrity of the fuel clad and/or reactor coolant system pressure boundary during Condition II and III transients is demonstrated in Chapter 15. These safety analyses are carried out using setpoints determined from results of the engineering design studies. The associated allowable values are presented in the Technical Specifications. A discussion of the intent for each of the various reactor trips and the accident analysis (where appropriate) that uses this trip is presented in Section 7.2.2.1.2. It should be noted that the selected trip setpoints all provide for margin before protection action is actually required, to allow for uncertainties and instrument errors. The design meets the requirements of General Design Criteria 10 and 20.

7.2.2.1.2 Trip Setpoint Discussion

It has been pointed out that below a DNBR equal to the limit value there is likely to be significant local fuel clad failure. The DNBR existing at any point in the core for a given core design can be determined as a function of the core inlet temperature, power output, operating pressure, and flow. Consequently, core safety limits in terms of a DNBR equal to the limit value for the hot channel can be developed as a function of core delta T, T_{avg} , and pressure for a specified flow as illustrated by the solid lines in Figure 15.1-1. Also shown as solid lines in Figure 15.1-1 are the loci of conditions equivalent to 118% of power as a function of delta T and T_{avg} representing the overpower (kW/ft) limit on the fuel. The dashed lines indicate the maximum permissible setpoint (delta T) as a function of T_{avg} and pressure for the overtemperature and overpower reactor trip. Actual setpoint constants in the equation representing the dashed lines are given in the Core Operating Limits Report (COLR). These values are conservative to allow for

instrument errors. The design meets the requirements of General Design Criteria 10, 15, 20, and 29.

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

Therefore, the reactor trip system has been designed to provide protection for fuel clad and reactor coolant system pressure boundary integrity where: (1) a rapid change in a single variable will quickly result in exceeding a core or a system safety limit and (2) a slow change in one or more variables will have an integrated effect that will cause safety limits to be exceeded. Overall, the reactor trip system offers diverse and comprehensive protection against fuel/clad failure and/or loss of reactor coolant system integrity for Condition II and III accidents. This is demonstrated by Table 7.2-4, which lists the various trips of the reactor trip system, and correlates them to the Technical Specifications and the appropriate accident discussed in the safety analyses in which the trip could be used.

The nuclear power plant reactor trip system design employed by Westinghouse was evaluated in detail with respect to common-mode failure and is presented in References 1 and 7. The design meets the requirements of General Design Criterion 21.

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

Analyses of the results of Condition I, II, III, and IV events, including considerations of instrumentation installed to mitigate their consequences, are presented in Chapter 15. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in Section 7.7.

7.2.2.1.2.1 *Nonstandard Operating Configuration.*

The reactor trip system automatically provides core protection during nonstandard operating configuration, that is, operation with a loop out of service. Although operating with a

loop out of service over an extended time is unlikely and is currently prohibited by the Technical Specifications, no protection system setpoints need to be reset. This is because the nominal value for the power (P-8) interlock setpoint restricts the power levels such that DNBRs smaller than the design limit will not be realized during any Condition II transients occurring during this mode of operation. This restricted power level is considerably below the boundary of permissible values, as defined by the core safety limits for operation with a loop out of service. Thus, the P-8 interlock acts essentially as a high nuclear power reactor trip when operating with one loop not in service. By first resetting the coefficient setpoints in the overtemperature delta T function to more restrictive values as would be listed in the Technical Specifications, the P-8 setpoint could then be increased to the maximum value consistent with maintaining DNBR above the design limit for Condition II transients in the one-loop shutdown mode. The resetting of the delta T overtemperature trip and P-8 would be carried out under prescribed administrative procedures and only under the direction of authorized supervision.

The steam-line differential pressure signal is designed to provide a safety injection signal when the steam-line nonreturn valve closes following a Condition IV steam-line break upstream of the nonreturn valve. If the nonreturn valve fails to close following a break upstream of it, then a high steam flow signal coincident with either low steam-line pressure or low-low T_{avg} would actuate safety injection, and the steam-line differential pressure signal is not required.

The steam-line differential pressure logic will actuate safety injection if any one steam line has a pressure that is 100 psi lower than the pressure in the remaining steam lines.

When a primary reactor coolant loop is isolated, the logic is in a condition to provide safety injection if any one of the nonisolated loops has a steam pressure that is 100 psi lower than the steam pressure in the remaining nonisolated loop. Therefore, the steam-line differential pressure signal possesses redundancy both with and without an isolated loop and can accept a single failure in any channel without a loss of function.

The steam-line differential pressure bi-stable status is constantly displayed on the main control board by the following:

1. Annunciator panels with an associated alarm when the panels are first lit.
2. Trip status lights for each bi-stable.

The operator can see from the control room if the proper bi-stables have been placed in the trip mode.

Even if the operator fails to place the proper bi-stables in the trip mode, the steam-line differential pressure system possesses redundancy unless the isolated steam generator is depressurized.

The maximum rate of depressurization from natural heat losses would be less than approximately 12 psi/hr; thus, it would be more than an hour before the depressurization could

significantly affect the operability of the differential pressure actuation signal. Faster depressurizations would result only following accident conditions in the isolated loop. The design basis does not require the consideration of an additional, nonconsequential accident in an operable loop following the first accident in the isolated loop.

The isolation of a primary reactor coolant loop and the closure of the main steam stop valve in the isolated loop never cause a loss of function in the steam line differential pressure safety injection actuation system. Redundancy in this system is also maintained unless the operator permits the isolated loop steam generator to depressurize and fails to trip the proper bi-stables in spite of the fact that he:

1. Has specific operating instructions to trip the bi-stables.
2. Has a period of more than an hour to trip the bi-stables before redundancy is lost.
3. Has two control board indications telling him whether or not the bi-stables have been tripped.

In order to defeat the protective action of the differential pressure bi-stables, the operator must make an error, the isolated loop must be allowed to cool down significantly, and a failure must occur in the protection system circuitry.

7.2.2.1.3 Reactor Coolant Flow Measurement

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

$$\frac{\Delta P}{\Delta P_o} = \left[\frac{w}{w_o} \right]^2 \quad (7.2-3)$$

where ΔP_o is the pressure differential at the referenced flow rate, w_o , and ΔP is the pressure differential at the corresponding flow rate, w . The full-flow reference point was established during initial plant startup. The low-flow trip point was then established by extrapolating along the correlation curve.

The expected absolute accuracy of the channel is within $\pm 10\%$, and field results have shown the repeatability of the trip point to be within $\pm 1\%$.

7.2.2.2 Evaluation of Compliance to Applicable Codes and Standards

7.2.2.2.1 Evaluation of Compliance with IEEE Std 279-1971

The reactor trip system meets the criteria of IEEE Std 279-1971 (Reference 8), as indicated below, with exceptions noted.

7.2.2.2.1.1 Single-Failure Criterion. The protection system is designed to provide redundant (one out of two, two out of three, or two out of four) instrumentation channels for each protective

function and one-out-of-two logic train circuits. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required. This design meets the requirements of General Design Criterion 21. A loss of input power, the most likely mode of failure, to a channel or logic train will result in a signal calling for a trip. This design also meets the requirements of General Design Criterion 23.

To prevent the occurrence of common-mode failures, such additional measures as functional diversity, physical separation, and testing, as well as administrative control during design, production, installation, and operation are employed, as discussed in Reference 7. This design also meets the requirements of General Design Criteria 21 and 22.

7.2.2.2.1.2 *Quality of Components and Modules.* For a discussion of the quality of the components and modules used in the reactor trip system, refer to Chapter 17. The quality used also meets the requirements of General Design Criterion 1.

7.2.2.2.1.3 *Equipment Qualification.* For a discussion of the type tests made to verify the performance requirements, refer to Section 3.11. The test results also demonstrate that the design meets the requirements of Criterion 4 of the GDC.

7.2.2.2.1.4 *Independence.* Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. See Figure 7.2-12. Physical separation is used to achieve the separation of redundant transmitters. The separation of wiring is achieved by using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in different protection rack sets. Each redundant channel is energized from a separate ac power feed. This design also meets the requirements of General Design Criterion 21.

The independence of the logic trains is discussed in Reference 4. Two reactor trip breakers are actuated by two separate logic matrices that interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full-length control rod drive mechanisms, permitting the rods to free fall into the core.

The design philosophy is to make maximum use of a wide variety of measurements. The protection system continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in Reference 1. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. This design also meets the requirements of General Design Criterion 22.

7.2.2.2.1.5 *Control and Protection System Interaction.* The protection system is designed to be independent of the control system. In certain applications, the control signals and other nonprotective functions are derived from individual protective channels through isolation

amplifiers. The isolation amplifiers are classified as part of the protection system and are located in the analog protective racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring. The isolation amplifiers are designed such that a short circuit, open circuit, or the application of 120V ac or 140V dc on the isolated output portion of the circuit (i.e., the nonprotective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation amplifiers are never returned to the protective racks. This design also meets the requirements of General Design Criterion 24.

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

In addition to the fault tests on the isolation amplifiers, system tests on the nuclear instrumentation system (NIS), the solid-state protection system (SSPS), and the 7300 Series process control system (7300 PCS) have been conducted by Westinghouse. These tests have demonstrated that credible externally applied electrical faults or interference, which could be postulated to be propagated back into redundant instrument and control protection cabinets, would not prevent these systems from performing their safety functions (or cause their spurious actuation).

The NIS and SSPS system tests are covered in the report *Westinghouse Protection System Noise Tests*, which was submitted and accepted by the NRC in support of the Diablo Canyon application (Docket Numbers 50-275 and 50-323). The 7300 PCS tests are reported in Reference 9, the conclusions having been accepted by the NRC for the North Anna Power Station.

Where failure of a protection system component can cause a process excursion that requires protective action, the protection system can withstand another, independent failure without loss of protective action. This design also meets the requirements of General Design Criterion 24. An exception to this feature is justified in Section 7.2.2.3.5.

7.2.2.2.1.6 Capability for Testing. The reactor trip system is capable of being tested during power operation. When only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to ensure complete system operation.

The protection system is designed to permit periodic testing of the analog channel portion of the reactor trip system during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. Note, however, that the source and intermediate range high-neutron-flux trips must be bypassed during testing.

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

Analog channel testing is performed at the analog instrumentation rack set by individually introducing simulated input signals into the instrumentation channels and observing the tripping of the appropriate output bi-stables. Process analog output to the logic circuitry is interrupted during individual channel test by a test switch that, when thrown, de-energizes the associated logic input and inserts a proving lamp in the bi-stable output. The interruption of the bi-stable output to the logic circuitry for any cause (test, maintenance purposes, or removed from service) will cause that portion of the logic to be actuated (partial trip), accompanied by a partial trip alarm and channel status light actuation in the control room. Each channel contains those switches, test points, etc., necessary to test the channel. See Reference 3 for additional information.

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

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

It should be noted that a valid trip signal would cause the channel under test to trip at a lower actual reactor power level. A reactor trip would occur when a second bi-stable trips. No specific provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the nuclear instrumentation system detector.

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

For a detailed description of the nuclear instrumentation system, see Reference 2.

The reactor logic trains of the reactor trip system are designed to be capable of complete testing at power. Annunciation is provided in the control room to indicate when a train is in test, when a reactor trip is bypassed, and when a reactor trip breaker is bypassed. Details of the logic system testing are given in Reference 4. See Section 7.2.3.4 for a discussion of compliance to Safety Guide 22.

The reactor coolant pump breakers cannot be tripped at power without causing a plant upset by loss of power to a coolant pump. However, the reactor coolant pump breaker open trip logic can be tested at power. Manual trip cannot be tested at power without causing a reactor trip since operation of either manual trip switch actuates both train A and train B. Initiating safety injection or opening the turbine trip breakers cannot be done at power without upsetting normal plant operation. However, the logic for the associated trips is testable at power.

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

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

Each train contains a multiplexing test switch. At the start of a process or nuclear instrumentation system test, this switch (in either train) is placed in the A + B position. The A + B position alternately allows information to be transmitted from the two trains to the control board. Status lamps and annunciators indicate that input relays in both trains have been de-energized. Contact inputs to the logic protection system, such as reactor coolant pump bus underfrequency relays, operate input relays, which are tested by operating the remote contacts as described above and using the same type of indications as those provided for bi-stable input relays.

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

2. *Check of logic matrices*—Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semiautomatic test panel in the train. Details of semiautomatic tester operation are given in Reference 4. At the completion of the logic matrix tests, one bi-stable in each channel of process instrumentation or nuclear instrumentation may be tripped to check closure of the input error inhibit switch contacts.

The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

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

The general design features and details of the testability of the logic system are described in Reference 4. The testing capability meets the requirements of General Design Criterion 21.

7.2.2.2.1.7 Testing of Reactor Trip Breakers. Normally the reactor trip breakers 52/RTA and 52/RTB are racked in and closed; and the bypass breakers are racked in and open. Testing of the trip breakers is included in the procedure for the testing of their associated protection logic and is performed on a per train basis at staggered intervals. Although pulse techniques are used in protection logic testing, which avoids the tripping of the reactor trip breakers, the associated bypass breaker is closed providing redundancy. The following procedure illustrates the testing of the reactor trip breaker (RTA), the bypass breaker (BYA) and its associated protection logic:

1. Close BYA. Trip BYA to verify its operation.
2. Close BYA. Test Auto shunt trip block of RTA.
3. Trip RTA manually via UV coil to verify its operation. Close RTA.
4. Trip RTA via Shunt Trip to verify its operation. Close RTA.
5. Perform Reactor Protection and ESF logic tests.
6. Verify RTA is closed. If not, close and verify.
7. Trip BYA and leave racked in.
8. Repeat the analogous steps for testing the “B” train.

Modifications to the reactor trip switchgear were implemented to satisfy action items in NRC Generic Letter 83-28 dated July 8, 1983, 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 deenergizes 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.

Approved station procedures describe the method used to test reactor trip breaker operation through the shunt trip relay.

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

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

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

The complete reactor trip system is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, the Technical Specifications define the operability requirements for the reactor trip system. The Technical Specifications also define the required restriction to operation in the event that the channel operability cannot be met.

The reactor trip system is designed in such a way that response time tests can be performed only during shutdown. However, the safety analyses use conservative numbers for trip channel response time. The measured channel response times are compared with those used in the safety evaluations. In accordance with Technical Specifications, the actual response times measured are required to be less than or equal to the times used in the safety analyses.

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

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

7.2.2.2.1.10 *Completion of Protective Action.* The reactor trip system is so designed that, once initiated, a protective action goes to completion. Return to normal operation requires action by the operator.

7.2.2.2.1.11 *Manual Initiation.* Switches are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment.

7.2.2.2.1.12 *Access.* The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, testpoints, and the means for manually bypassing channels or protective functions. For details refer to Reference 3.

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

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

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

7.2.2.2.1.14 *Identification.* The identification described in Section 7.1 provides immediate and unambiguous identification of the protection equipment.

7.2.2.2.2 Evaluation of Compliance with IEEE Std 308-1971 (Reference 10)

See Section 7.6 and Chapter 8 for a discussion of the power supply for the protection system and compliance with IEEE Std 308-1971.

7.2.2.2.3 Evaluation of Compliance with IEEE Std 323-1971 (Reference 11)

Reactor trip system equipment is type tested to substantiate the adequacy of design. This is the preferred method, as indicated in Reference 11.

Most Westinghouse-supplied electrical equipment essential to safe shutdown was qualified before the issuance of IEEE Std 323-1971. For this reason, the format of test documentation is not as listed in Section 5.2 of Reference 11. The testing and documentation that was accomplished is comparable to that required by IEEE Std 323-1971. Test data, considered proprietary by Westinghouse or its suppliers, can be made available for audit purposes at Westinghouse or its suppliers.

7.2.2.2.4 Evaluation of Compliance with IEEE Std 334-1971 (Reference 12)

There are no continuous duty, Class I motors in the reactor trip system. Therefore, IEEE Std 334-1971 does not apply to the reactor trip system.

7.2.2.2.5 Evaluation of Compliance with IEEE Std 338-1971 (Reference 13)

Periodic response time testing of reactor trip system response times has been established in the Technical Specifications to meet the intent of IEEE Std 338-1971.

7.2.2.2.6 Evaluation of Compliance with IEEE Std 344-1971 (Reference 14)

The seismic testing, as discussed in Section 3.10 and the references, conforms to the guidelines set forth in IEEE Std 344-1971, with the exceptions noted in Section 3.10.

7.2.2.2.7 Evaluation of Compliance with AEC General Design Criteria (Reference 15)

The reactor trip system meets the requirements of the General Design Criteria wherever appropriate. Specific cases are noted as they are discussed in Chapter 7.

7.2.2.2.8 Evaluation of Compliance with IEEE Std 317-1971 (Reference 16)

See Section 3.8.2.1.4 for a discussion of electrical penetrations and compliance with IEEE Std 317-1971.

7.2.2.2.9 Evaluation of Compliance with IEEE Std 336-1971 (Reference 17)

Instrumentation and electrical equipment was installed, inspected, and tested in accordance with IEEE Std 336-1971. See Section 8.3.1.1.2.2 for a discussion of compliance with IEEE Std 336-1971.

7.2.2.3 **Specific Control and Protection Interactions**

7.2.2.3.1 Neutron Flux

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

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

7.2.2.3.2 Coolant Temperature

The delta-T and T_{avg} signals developed in the reactor protection system for the overtemperature delta-T and overpower delta-T reactor trips also provide input to the rod control, steam dump control, and pressurizer level control systems. 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 the Median Signal Selector (MSS) auctioneering circuits. The MSS is designed to prevent the 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 the lowest of the three channels 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 deviate significantly from normal (i.e., -3°F for T_{avg} ; -3.2% delta-T power for a delta-T input at 100% power based on a 63.4°F delta-T condition), the MSS will transfer to a high select mode and select the higher of the remaining two valid inputs for reactor control. The use of the MSS circuits in the reactor control system satisfies the Control and Protection System interaction requirements of IEEE Std 279-1971, and prevents a spurious low temperature signal from causing rod withdrawals.

In addition, channel deviation signals in the control system will give an alarm if any temperature channel deviates significantly from the auctioneered (median) value. Automatic rod withdrawal blocks will also occur if any two of the temperature channels indicate an overtemperature or overpower condition.

Two hot leg temperature indications are available at the Auxiliary Monitoring Panel. One of them is installed with a specific separation from the additional temperature indication available in the control room. This separation meets 10 CFR 50 Appendix R Section III.G.2.

7.2.2.3.3 Pressurizer Pressure

North Anna uses separate transmitters for pressurizer pressure protection and control functions. There are three transmitters used to provide inputs to three protection channels. There are two additional transmitters used for reactor coolant pressure control functions. The protection channels provide high- and low-pressure protection, input to the overtemperature delta T protection function, and indication. The indication is isolated from the protection functions.

A spurious high-pressure signal from a pressurizer pressure control channel can cause decreasing pressure by the actuation of either spray or relief valves. Additional redundancy is provided in the low pressurizer pressure reactor trip logic and in the logic for safety injection to ensure low-pressure protection.

An additional pressurizer pressure indication is available at the Auxiliary Monitoring Panel and is installed with a specific separation from the additional pressurizer pressure indication available in the control room. This separation meets Appendix R Section III.G.2.

7.2.2.3.4 Pressurizer Water Level

Three pressurizer water level channels are used for reactor trip. Isolated signals from these channels are used for pressurizer water level control. A failure in the water level control system could fill or empty the pressurizer at a slow rate (on the order of half an hour or more).

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

Experience has shown that during normal operating conditions hydrogen gas can accumulate in the upper part of the reference leg of the pressurizer water level instruments. At reactor coolant system pressures, high concentrations of dissolved hydrogen in the water of the reference leg are possible. It has been hypothesized that a sudden primary system depressurization would cause rapid effervescence of the dissolved hydrogen in the water of the reference leg. This phenomenon could blow out the reference leg, creating a large error in measured pressurizer level. Accurate calculations of this effect have been difficult to obtain. Thus, the effect of a sudden primary system depressurization on the pressurizer high level reactor trip is to generate a reactor trip somewhat below the actual pressurizer high-level trip setpoint. To generate a high pressurizer level reactor trip at a lower level than the true setpoints is conservative and will not require changes in the plant safety analysis report. Pressurizer low level is not used for either reactor trip or safety injection. It should be noted that the relatively large error caused by the rapid depressurization is of a transient nature due to the ongoing condensation process within the reference leg. This will correct the level error in a short period of time as the condensate fills the reference leg to its normal level.

Significant leaks of the reference leg to atmosphere will be immediately detectable by off-scale indication and alarms on the control board. Small leaks are detectable by deviations from other channels. A closed pressurizer level instrument shutoff valve would be detectable by comparing the level indications from the redundant channels (three channels). A control room alarm is installed to indicate an error between measured pressurizer water level and the programmed pressurizer water level. There is no single instrument valve which could affect more than one of the three channels.

A pressurizer water level indication is available at the Auxiliary Monitoring Panel and is installed with a specific separation from the addition pressurizer water level indication available in the control room. This separation meets 10 CFR 50 Appendix R Section III.G.2.

7.2.2.3.5 Steam Generator Water Level and Feedwater Flow

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 the removal of long-term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on coincidence of steam/feedwater flow mismatch and low water level or on low-low steam-generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater to maintain residual heat removal after trip, preventing eventual thermal expansion and discharge of the reactor coolant through the pressurizer relief valves into the relief tank even when main feedwater pumps are incapacitated.

These reactor trips act before the steam generators are dry to reduce the required capacity and starting time requirements of these auxiliary feedwater pumps and to minimize the thermal transient on the reactor coolant system and steam generators. Therefore, the following reactor trip circuits are provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient:

1. A mismatch in steam and feedwater flow coincident with low steam generator water level.
2. A low-low steam generator water level regardless of steam/feedwater flow mismatch.

A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow, preventing that channel from ultimately tripping. However, the mismatch between steam demand and feedwater flow produced by this spurious signal will actuate alarms to alert the operator of this situation in time for manual correction or, if the condition is allowed to continue, the reactor will eventually trip either on coincidence with low level or on a low-low water level signal independent of indicated feedwater flow.

A spurious low signal from the feedwater flow channel being used for control would cause an increase in feedwater flow. The mismatch between steam flow and feedwater flow produced by the spurious signal would actuate alarms to alert the operator of the situation in time for manual correction.

If the condition is allowed to continue, a two-out-of-three high-high steam generator water level signal from any steam generator, independent of the indicated feedwater flow, will cause feedwater isolation and trip the turbine. The turbine trip will result in a subsequent reactor trip if reactor power is above the setpoint of P-8.

In addition, the three-element feedwater controller incorporates reset action on the level error signal, such that with expected controller settings a rapid increase or decrease in the flow signal would cause only a small change in level before the controller would compensate for the

level error. A slow change in the feedwater signal would have no effect at all. A spurious low or high steam flow signal would have the same effect as high or low feedwater signal, discussed above.

The actual plant response to the failure of 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 or low 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 Std 279-1971 for evaluation of control and protection channel interactions. Since the steam generator low-low and high-high level protection functions require two of three channels, this function would be rendered inoperable on the steam generator experiencing the flow and level excursion.

1. Steam Generator Controlling Level Channel Fails High (Feedwater Flow Reduction)

- a. 0% power to approximately 20% power

Below approximately 20% power, feedwater is either being manually controlled via the operator or automatically controlled by the level control system via the main feedwater regulating valve bypass valves. 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 a loss of normal feedwater accident are violated. The non-standard mode of controlling the feedwater flow also serves to increase the level of operator awareness of the status of the feedwater system and steam generator inventory.

If plant control systems are operating normally, the expected response to a loss of feedwater to one steam generator is a gradual shift in steam load to the two unaffected generators as the affected generator dries out, followed by continued power operation. If all control systems were not operating normally, a decrease in steam generator level in the two active generators would eventually result in a reactor trip and auxiliary feedwater actuation.

In addition to the low-low steam generator level trip and auxiliary feedwater actuation, backup core protection is also provided by the high pressurizer level and overtemperature Delta-T reactor trips.

- b. Approximately 20% power to approximately 50% power

The low feedwater flow trip may not be available at power levels below approximately 50% power for a 1 to 3 steam generator loss of feedwater event because measured steam flow may not be high enough to trip the high steam flow/feed flow mismatch bi-stables. Therefore the requirements of IEEE Std 279-1971, Section 4.7.3, are not met for the SG level channels over this operating range, since failure of the controlling level channel plus an additional level channel failure would eliminate the low-low SG level trip. However, based on the considerations below, this exception to the IEEE Std 279-1971 requirements is acceptable.

If plant control systems are operating normally, the expected response to a loss of feedwater to one steam generator is a gradual shift in steam load to the two unaffected generators as the affected generator dries out, followed by a continued power operation. If all control systems were not operating normally, a decrease in steam generator level in the two active generators would eventually result in a reactor trip and auxiliary feedwater actuation.

In addition to the low-low steam generator level trip and auxiliary feedwater actuation, backup core protection is also provided by the high pressurizer level and overtemperature Delta-T reactor trips.

As discussed above, the secondary heat sink requirements at power levels below 50% power can be satisfied by the unaffected steam generators due to the reduced power condition. For the case where main feedwater is being controlled manually, even if flow were inadvertently isolated to a generator, the unaffected steam generator would continue to remove heat from the RCS until a low-low steam generator level signal, or one of the other trips discussed above, is generated. If the RCS heats up rapidly, the overtemperature delta-T 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.

c. Approximately 50% power to 100% power

If power level is greater than approximately 50%, the IEEE Std 279-1971 scenario is protected by the steam/feed flow mismatch coincident with 1/2 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 heat removal until the water level drops sufficiently to generate a low-low signal in the unaffected generators and initiate auxiliary feedwater. 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.

2. SG Controlling Level Channel Fails Low (Feedwater Flow Increase)

If reactor power is above approximately 20%, the feedwater flow is being controlled from the automatic SG level control circuit. If the SG level channel which feeds the level control circuit fails low, feedwater flow to the affected SG will increase, with a subsequent increase in SG level. Protection against SG overfill is provided by turbine trip and feedwater flow isolation on 2/3 high-high steam generator level in any SG (an Engineered Safety Feature, Section 7.3). The potential for SG overfill due to failure of a controlling SG level channel coincident with an additional level channel failure was examined generically in

Reference 18. It was concluded that the potential risk of SG overfill was not high enough to justify backfits to ensure compliance with the IEEE Std 279-1971, Section 4.7.3, criterion. Therefore, an exception to this criterion is taken for these channels.

In the event of an Anticipated Transient Without Scram (ATWS), the ATWS Mitigation System Actuation Circuitry (AMSAC) would operate provided that the C-20 permissive is satisfied by the unit being above a specific power level based on turbine first stage pressure. When the narrow range steam generator level detected by two out of three channels on each of two out of three steam generators is below the AMSAC setpoint and the C-20 permissive is satisfied, an AMSAC trip can be generated. Further description of the C-20 setpoint and its basis is provided in Section 7.7.1.14. The AMSAC steam generator level can be the same as the RPS low-low level setpoint or may be set as much as 5% lower than the RPS setpoint, providing certain criteria are met. The AMSAC trip is time delayed to allow the RPS to function prior to AMSAC action. AMSAC trips the turbine, trips the reactor by tripping the power feeder breakers for the rod control motor generator sets, isolates the sample and blowdown lines, and start all auxiliary feedwater pumps. This logic is shown in Figure 7.2-13.

7.2.3 Tests and Inspections

The reactor trip system meets the testing requirements of Reference 13 with the exceptions given in Section 7.2.2.2.5. The testability of the system is discussed in Section 7.2.2.2.1. Test intervals are specified in the Technical Specifications.

7.2.3.1 Inservice Tests and Inspections

Periodic surveillance of the reactor trip system is performed to ensure proper protective action. This surveillance consists of checks, calibrations, and channel operational testing, which are defined in the Technical Specifications.

The minimum frequency for checks, calibration, and testing are defined in the Technical Specifications.

7.2.3.2 Periodic Testing of the Nuclear Instrumentation System

Periodic tests of the nuclear instrumentation system are performed as specified in the Technical Specifications.

Any deviations noted during the performance of these tests are investigated and corrected in accordance with the established calibration and troubleshooting procedures provided in the Plant Technical Manual for the nuclear instrumentation system. Protection trip and permissive interlock settings are indicated in the Technical Requirements Manual. Control settings are indicated in the North Anna Setpoint Document.

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

Periodic tests of the analog channels of the protection circuits are performed as specified in the Technical Specifications.

7.2.3.4 Safety Guide 22

Periodic testing of the reactor trip system actuation functions, as described, complies with AEC Safety Guide 22, *Periodic Testing of Protection System Actuation Functions*, February 1971. Under the present design, there are protection functions that are not tested at power. These are as follows:

1. Generation of a reactor trip by tripping the main coolant pump breakers.
2. Generation of a reactor trip by tripping the turbine.
3. Generation of a reactor trip by use of the manual trip switch.
4. Generation of a reactor trip by actuating the safety injection system.

The actuation logic for the functions listed is tested off-line. As required by Safety Guide 22, where equipment is not tested during reactor operation it has been determined that:

1. There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant.
2. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation.
3. The equipment can routinely be tested when the reactor is shut down.

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the main control room by a separate annunciator for the train in test. Test circuitry does not allow two trains to be tested at the same time, so that extension of the bypass condition to redundant systems is prevented. See Section 7.2.2.2.1 for details of testing the channels and trains of the reactor trip system.

7.2 REFERENCES

1. T. W. Burnett, *Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors*, WCAP-7306, April 1969.
2. J. B. Lipchak and R. A. Stokes, *Nuclear Instrumentation System*, WCAP-7380-L, January 1971 (Westinghouse NES Proprietary); and WCAP-7669, May 1971 (nonproprietary).

3. J. A. Nay, *Process Instrumentation for Westinghouse Nuclear Steam Supply Systems*, WCAP-7547-L, March 1971 (Westinghouse NES Proprietary); WCAP-7671, May 1971 (nonproprietary); J. B. Reid, *Process Instrumentation for Westinghouse Nuclear Steam Supply Systems (W CID 7300 Series)*, WCAP-7913.
4. D. N. Katz, *Solid State Logic Protection System Description*, WCAP-7488-L, March 1971 (Westinghouse NES Proprietary); and WCAP-7672, May 1971 (nonproprietary).
5. I. Garber, *Isolation Tests Process Instrumentation Isolation Amplifier Westinghouse Computer and Instrumentation Division Nucana 7300 Series*, WCAP-7862, September 1972.
6. J. B. Lipchak and R. R. Bartholomew, *Test Report Nuclear Instrumentation System Isolation Amplifier*, WCAP-7506-L, October 1970 (Westinghouse NES Proprietary); and WCAP-7819, Rev. 1, January 1972 (nonproprietary).
7. W. C. Gangloff, *An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactors*, WCAP-7486, May 1971.
8. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*, IEEE Std 279-1971.
9. *Westinghouse 7300 Series Process Control System Noise Tests*, WCAP-8892-A, June 1977.
10. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard Criteria for Class IE Electric Systems for Nuclear Power Generating Stations*, IEEE Std 308-1971.
11. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Standard; General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations*, IEEE Std 323-1971.
12. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations*, IEEE Std 334-1971.
13. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems*, IEEE Std 338-1971.
14. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations*, IEEE Std 344-1971.
15. *General Design Criteria for Nuclear Power Plants*, Appendix A to Title 10 CFR 50, July 7, 1971.
16. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations*, IEEE Std 317-1971.

17. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations*, IEEE Std 336-1971.
18. NUREG-1218, *Regulatory Analysis for Resolution of USI A-47, Safety Implications of Control Systems in LWR Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, July 1989.
19. Technical Report EE-0101, *Setpoint Bases Document Analytical Limits, Setpoints and Calculations for Technical Specifications Instrumentation at North Anna and Surry Power Stations*.

Table 7.2-1
LIST OF REACTOR TRIPS

Reactor Trip	Coincidence Logic	Interlocks	Comments
1. High neutron flux (power range)	2/4	Manual block of low setting permitted by P-10	High and low settings; manual block and automatic reset of low setting by P-10.
2. Intermediate range	1/2	Manual block permitted by P-10	Manual block and automatic reset.
3. Source range neutron flux	1/2	Manual block permitted by P-6, interlocked with P-10	Manual block and automatic reset. Automatic block above P-10. Manual reset available below P-10.
4. Power range high positive neutron flux rate	2/4	No interlocks	
5. Power range high negative neutron flux rate	2/4	No interlocks	
6. Overtemperature delta T	2/3	No interlocks	
7. Overpower delta T	2/3	No interlocks	
8. Pressurizer low pressure	2/3	Interlocked with P-7	Blocked below P-7.
9. Pressurizer high pressure	2/3	No interlocks	
10. Pressurizer high water level	2/3	Interlocked with P-7	Blocked below P-7.
11. Low reactor coolant flow	2/3 per loop	Interlocked with P-7 and P-8	Low flow in one loop will cause a reactor trip when above P-8 and a low flow in two loops will cause a reactor trip when above P-7 Blocked below P-7.
12. Reactor coolant pump breakers open	2/3	Interlocked with P-7	Blocked below P-7. Open breaker in 1 loop permitted below P-8.
	1/3	Interlocked with P-8	Blocked below P-8
13. Reactor coolant pump bus under-voltage	2/3	Interlocked with P-7	Low voltage on all buses permitted below P-7.

Table 7.2-1 (continued)
LIST OF REACTOR TRIPS

Reactor Trip	Coincidence Logic	Interlocks	Comments
14. Reactor coolant pump bus under-frequency	2/3	Interlocked with P-7	Underfrequency on two buses will cause reactor trip; reactor trip blocked below P-7.
15. Low feedwater flow	1/2 per loop ^a	No Interlocks	
16. Low-low steam generator water level	2/3 per loop	No Interlocks	Blocked for a loop in which the primary coolant stop valves are closed.
17. Safety injection signal	Coincident with actuation of safety injection	No Interlocks	(See Section 7.3 for engineered safety features actuation conditions.)
18. Turbine-generator trip	2/3	Interlocked with P-8	Blocked below P-8.
a. Low auto-stop oil pressure			
b. Turbine stop valve close	4/4	Interlocked with P-8	Blocked below P-8.
19. Manual		No interlocks	
20. General warning	2/2 trains (1 per train)	No interlocks	
21. Steam generator water level (AMSAC)*	2/3 per loop per 2/3 steam generators after time delay	Interlocked with C-20	Blocked below C-20 after time delay.

^a 1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level.

*AMSAC trips the reactor by tripping the power supply breakers to the rod control motor generator sets which in turn trips the unit.

Table 7.2-2
REACTOR TRIP SYSTEM ACCURACIES AND RANGES
REACTOR TRIP SYSTEM TRIP SETPOINT ACCURACIES

Reactor Trip Signal	Trip Accuracy	See Note
1. Power range high neutron flux	$\pm 5.61\%$ of span	
2. Intermediate range high neutron flux	not calculated	(a)
3. Source range high neutron flux	$\pm 4.412\%$ of linear span	
4. Power range high positive neutron flux rate	not required	(a, b)
5. Power range high negative neutron flux rate	not required	(a, b)
6. Overtemperature ΔT	$\pm 5.59\%$ of span with $f(\Delta I) < 0$ $\pm 4.48\%$ of span with $f(\Delta I) = 0$ $\pm 6.00\%$ of span with $f(\Delta I) > 0$	
7. Overpower ΔT	$\pm 3.68\%$ of span	
8. Pressurizer low pressure	$\pm 1.941\%$ of span	
9. Pressurizer high pressure	$\pm 1.875\%$ of span	
10. Pressurizer high water level	$\pm 6.887\%$ of span	
11. Low reactor coolant flow	$\pm 2.34\%$ of span (Foxboro transmitters) $\pm 2.25\%$ of span (Rosemount transmitters)	
12. Reactor coolant pump breakers open	not required	(a, b)
13. Reactor coolant pump bus undervoltage	± 143.5 volts	(a, b)
14. Reactor coolant pump bus underfrequency	± 0.30 hertz	(a, b)
15. Steam/Feedwater flow mismatch with low SG water level	$\pm 6.21\%$ of SF/FF span $+6.42\%$ to $+10.38\%$ of narrow range span	(b) (b)
16. Low-low steam generator water level	$+6.42\%$ to $+10.38\%$ of narrow range span	
17. Safety injection actuation	not applicable - digital input from ESF	
18. Turbine-generator trip:		
a. Low auto-stop oil pressure	not required	(a, b)
b. Turbine stop valves closed	not required	(a, b)
19. Manual reactor trip	not required	(a, b)
20. General warning	not required	(a, b)
21. AMSAC (SG water level)	$\pm 0.23\%$ of narrow range span	(a, b)

a. Reactor trip signal protection is not credited in plant safety analyses.

b. A safety analysis setpoint limit has not been established; calculation of setpoint accuracy is not required.

Table 7.2-2 (continued)
 REACTOR TRIP SYSTEM TRIP ACCURACIES AND RANGES
 REACTOR TRIP SYSTEM PROCESS RANGES

Reactor Trip Signal	Range	See Note
1. Power range high neutron flux	0 to 120% power	
2. Intermediate range high neutron flux	10^{-11} to 10^{-3} amperes	(a)
3. Source range high neutron flux	10^0 to 10^6 counts/second	
4. Power range high positive neutron flux rate	0 to 120% power	(a)
5. Power range high negative neutron flux rate	0 to 120% power	(a)
6. Overtemperature ΔT :		
Trip setpoint	0 to 150% power	
T_{hot}	530 to 650°F	
T_{cold}	510 to 630°F	
T_{avg}	530 to 630°F	
Pressurizer pressure	1700 to 2500 psig	
$F(\Delta I)$	-30 to +30%	
7. Overpower ΔT	(See Overtemperature ΔT)	
8. Pressurizer low pressure	1700 to 2500 psig	
9. Pressurizer high pressure	1700 to 2500 psig	
10. Pressurizer high water level	0 to 100% level	
11. Low reactor coolant flow	0 to 120% rated flow	
12. Reactor coolant pump breakers open	not applicable	(a, c)
13. Reactor coolant pump bus undervoltage	0 to 4200 volts	(a)
14. Reactor coolant pump bus underfrequency	55 to 59.5 hertz	(a)
15. Steam/Feedwater flow mismatch	0 to 5×10^6 lb/hr	
With low SG water level	0 to 100% narrow range level	
16. Low-low steam generator water level	0 to 100% narrow range level	
17. Safety injection actuation	not applicable	(c)
18. Turbine-generator trip:		
a. Low auto-stop oil pressure	15 to 150 psig	(a)
b. Turbine stop valves closed	not applicable	(a, c)
19. Manual reactor trip	not applicable	(a, c)
20. General warning	not applicable	(a, c)
21. AMSAC	0 to 100% narrow range level	(a)

a. Reactor trip signal protection is not credited in plant safety analyses.

c. Process input to reactor trip system is digital only; no process range exists.

Table 7.2-3
REACTOR TRIP SYSTEM INTERLOCKS

Designation	Derivation	Function
<u>Power Escalation Permissives</u>		
P-6	1/2 neutron flux (intermediate range) above setpoint	Allows manual block of source range reactor trip
	2/2 neutron flux (intermediate range) below setpoint	Defeats the block of source range reactor trip
P-10	2/4 neutron flux (power range) above setpoint	Allows manual block of power range (low setpoint) reactor trip
		Allows manual block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Blocks source range reactor trip (back-up for P-6)
	3/4 neutron flux (power range) below setpoint	Defeats the block of power range (low setpoint) reactor trip
		Defeats the block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Input to P-7
<u>Blocks of Reactor Trips</u>		
P-7	3/4 neutron flux (power range) below setpoint (from P-10) and 2/2 turbine impulse chamber pressure below setpoint (from P-13)	Blocks reactor trip on low flow or reactor coolant pump breakers open in more than one loop, undervoltage, underfrequency, 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 and on turbine trip
P-13	2/2 turbine impulse chamber pressure below setpoint	Input to P-7

Table 7.2-4
TRIP CORRELATION

Trip	Accident	Technical Specification
1. Source range, high neutron flux	15.2.1 1) Uncontrolled RCCA bank withdrawal from a subcritical condition	Yes
2. Intermediate range, high neutron flux	15.2.1 1) Uncontrolled RCCA bank withdrawal from a subcritical condition	Yes ^a
3. Power range, high neutron flux (low setpoint)	15.2.1 1) Uncontrolled RCCA bank withdrawal from a subcritical condition	Yes
4. Power range, high neutron flux (high setpoint)	15.2.1 1) Uncontrolled RCCA bank withdrawal from a subcritical condition 15.2.2 2) Uncontrolled RCCA bank withdrawal at power 15.2.6 3) Startup of an inactive reactor coolant loop 15.2.7 4) Loss of external electrical load and/or turbine trip 15.2.10 5) Excessive heat removal due to feedwater system malfunction 15.2.11 6) Excessive load increase 15.2.13 7) Accidental depressurization of the main steam system	Yes
5. Power range high positive neutron flux rate	15.4.6 Rod ejection	Yes ^a
6. Power range high negative neutron flux rate	15.2.3 1) RCCA misalignment	Yes
7. Overpower delta T	15.2.2 1) Uncontrolled RCCA bank withdrawal at power 15.2.10 2) Excessive heat removal due to feedwater system malfunction	Yes

^a Credit not taken for trip for reasons of conservatism in the safety analyses.

Table 7.2-4 (continued)
TRIP CORRELATION

Trip	Accident	Technical Specification
7. Overpower delta T (continued)	15.2.11 3) Excessive load increase 15.2.13 4) Accidental depressurization of the main steam system	
8. Overtemperature delta T	15.2.2 1) Uncontrolled RCCA bank withdrawal at power 15.2.4 2) Uncontrolled boron dilution 15.2.7 3) Loss of external electrical load and/or turbine trip 15.2.10 4) Excessive heat removal due to feedwater system malfunction 15.2.11 5) Excessive load increase 15.2.12 6) Accidental depressurization of the RC system 15.2.13 7) Accidental depressurization of the main steam system	Yes
9. Low primary coolant flow	15.2.5 1) Partial loss of forced reactor coolant flow a. Undervoltage b. Underfrequency c. Low flow or pump breaker open 1 of 3 loops 15.2.9 2) Loss of offsite power to the station auxiliaries (station blackout) d. Low flow or pump breaker open 2 of 3 loops 15.3.4 3) Complete loss of forced reactor coolant flow	Yes
10. Pressurizer high pressure	15.2.2 1) Uncontrolled RCCA bank withdrawal at power	Yes

^a Credit not taken for trip for reasons of conservatism in the safety analyses.

Table 7.2-4 (continued)
TRIP CORRELATION

Trip	Accident	Technical Specification
10. Pressurizer high pressure (continued)	15.2.7 2) Loss of external electrical load and/or turbine trip 15.4.2.2 3) Main feedline break	
11. Pressurizer high water level	15.2.2 1) Uncontrolled RCCA bank withdrawal at power 15.2.7 2) Loss of external electrical load and/or turbine trip	Yes
12. Pressurizer low pressure	15.2.12 1) Accidental depressurization of the RC system	Yes
13. Low steam generator water level with steam flow greater than feedwater flow	15.2.8 1) Loss of normal feedwater	Yes ^a
14. Low-low steam generator level	15.2.8 1) Loss of normal feedwater 15.4.2.2 2) Main feedline break	Yes

^a Credit not taken for reasons of conservatism in the safety analyses.

Table 7.2-5
REACTOR TRIP SYSTEM INSTRUMENTATION

Functional Unit	Channels to Trip	Minimum Channels Operable
1. Manual Reactor Trip	1	2
	1	2
2. Power Range, Neutron Flux	2	3
3. Power Range, Neutron Flux, High Positive Rate	2	3
4. Power Range, Neutron Flux, High Negative Rate	2	3
5. Intermediate Range, Neutron Flux	1	2
6. Source Range, Neutron Flux		
a. Startup	1	2
b. Shutdown	1	2
c. Shutdown (Indication only)	0	1
7. Overtemperature ΔT	2	2
8. Overpower ΔT	2	2
9. Pressurizer Pressure—Low	2	2
10. Pressurizer Pressure—High	2	2
11. Pressurizer Water Level—High	2	2
12. Loss of Flow—(Above P-7)	2/loop in any loop > P-8	2/loop in each loop
	2/loop in any 2 loops > P-7	
13. Steam Generator Water Level—Low-Low	2/loop	2/loop
14. Steam/Feedwater Flow Mismatch and Low Steam Generator Water Level	1/loop-level coincident with 1/loop-flow mismatch in same loop	1/loop level and 2/loop-flow mismatch or 2/loop-level and 1/loop-flow mismatch
15. Undervoltage—Reactor Coolant Pump Busses	2	2

Table 7.2-5 (continued)
 REACTOR TRIP SYSTEM INSTRUMENTATION

Functional Unit	Channels to Trip	Minimum Channels Operable
16. Underfrequency—Reactor Coolant Pump Busses	2	2
17. Turbine Trip		
a. Low Auto Stop Oil Pressure	2	2
b. Turbine Stop Valve Closure	4	3
18. Safety Injection Input from ESF	1	2
19. Reactor Coolant Pump Breaker Position Trip Above P-7	1 > P-8 2 > P-7	1/breaker
20. a. Reactor Trip Breakers	1	2
b. Reactor Trip Bypass Breakers	1	1
21. Automatic Trip Logic	1	2
22. Reactor Trip System Interlocks		
a. Intermediate Range Neutron Flux, P-6	1	2
b. Low Power Reactor Trips Block, P-7		
P-10 Input	2	3
or		
P-13 Input	1	2
c. Power Range Neutron Flux, P-8	2	3
d. Power Range Neutron Flux, P-10	2	3
e. Turbine Impulse Chamber Pressure, P-13	1	2

Figure 7.2-1
INDEX AND SYMBOLS

LOGIC SYMBOLS

SYMBOL

LOGIC FUNCTION

AND

NOT

OR

OFF RETURN MEMORY

INTERLIVE MEMORY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADDITIONAL SYMBOLS

INSTRUMENT CHANNEL BISTABLE

INDICATES THAT THE DEVICE OR INSTRUMENT CHANNEL HAS A BISTABLE LOGIC "1"

PARAMETER MEASURED IS GREATER THAN A PRESET VALUE

PARAMETER MEASURED IS LESS THAN A PRESET VALUE

PARAMETER MEASURED DEVIATES FROM A PRESET VALUE BY MORE THAN A PRESET AMOUNT

SAME AS ABOVE EXCEPT WITH AN AUTOMATICALLY SET VARIABLE VALUE

SAME AS ABOVE EXCEPT WITH REQUIRED HYSTERESIS BETWEEN TURN ON AND TURN OFF

NON-INSTRUMENT BISTABLE

OUTPUT INDICATOR SAME AS EXPLAINED ABOVE

ALARM INDICATOR ALARMS ON THE START SHEET WITH THE SAME SUBSCRIPT

SHARE A COMMON ANALOG INPUT

REACTOR TRIP "1" FIRST OUT - ANALOG INPUT

TUBERIAL TRIP "1" FIRST OUT - ANALOG INPUT

INDICATOR LAMP

ACTUATOR SIGNAL LIGHTS

TRIP STATUS LIGHTS

PERMISSIVE STATUS LIGHTS

BYPASS STATUS LIGHTS

COMMON "1" INPUT

LOGIC INFORMATION TRANSMISSION

ANALOG DISPLAY

ANALOG INDICATOR

REORDER 2 CHANNEL

REORDER 3 CHANNEL

ANALOG SUMMER

A DEVICE WHICH PERMITS AN ANALOG SIGNAL TO PASS TO AN ISOLATED CIRCUIT IF THE CONTROL LOGIC INPUT EXISTS.

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

DEVICE FUNCTION LETTERS AND NUMBERS

POSITION (DISPLACEMENT) CHANNEL

FLOW CHANNEL

LEVEL CHANNEL

PRESSURE CHANNEL

PRESSURE CHANNEL

TEMPERATURE CHANNEL

TEMPERATURE CHANNEL

ELECTRIC OPERATED VALVE

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

POSITION SWITCH

LOGIC SYMBOLS

SYMBOL

LOGIC FUNCTION

AND

NOT

OR

OFF RETURN MEMORY

INTERLIVE MEMORY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADJUSTABLE TIME RELAY

ADDITIONAL SYMBOLS

INSTRUMENT CHANNEL BISTABLE

INDICATES THAT THE DEVICE OR INSTRUMENT CHANNEL HAS A BISTABLE LOGIC "1"

PARAMETER MEASURED IS GREATER THAN A PRESET VALUE

PARAMETER MEASURED IS LESS THAN A PRESET VALUE

PARAMETER MEASURED DEVIATES FROM A PRESET VALUE BY MORE THAN A PRESET AMOUNT

SAME AS ABOVE EXCEPT WITH AN AUTOMATICALLY SET VARIABLE VALUE

SAME AS ABOVE EXCEPT WITH REQUIRED HYSTERESIS BETWEEN TURN ON AND TURN OFF

NON-INSTRUMENT BISTABLE

OUTPUT INDICATOR SAME AS EXPLAINED ABOVE

ALARM INDICATOR ALARMS ON THE START SHEET WITH THE SAME SUBSCRIPT

SHARE A COMMON ANALOG INPUT

REACTOR TRIP "1" FIRST OUT - ANALOG INPUT

TUBERIAL TRIP "1" FIRST OUT - ANALOG INPUT

INDICATOR LAMP

ACTUATOR SIGNAL LIGHTS

TRIP STATUS LIGHTS

PERMISSIVE STATUS LIGHTS

BYPASS STATUS LIGHTS

COMMON "1" INPUT

LOGIC INFORMATION TRANSMISSION

ANALOG DISPLAY

ANALOG INDICATOR

REORDER 2 CHANNEL

REORDER 3 CHANNEL

ANALOG SUMMER

A DEVICE WHICH PERMITS AN ANALOG SIGNAL TO PASS TO AN ISOLATED CIRCUIT IF THE CONTROL LOGIC INPUT EXISTS.

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

ANALOG GATE

ANALOG OUTPUT

CONTROL LOGIC INPUT

ANALOG INPUT

Figure 7.2-2
REACTOR TRIP SIGNALS

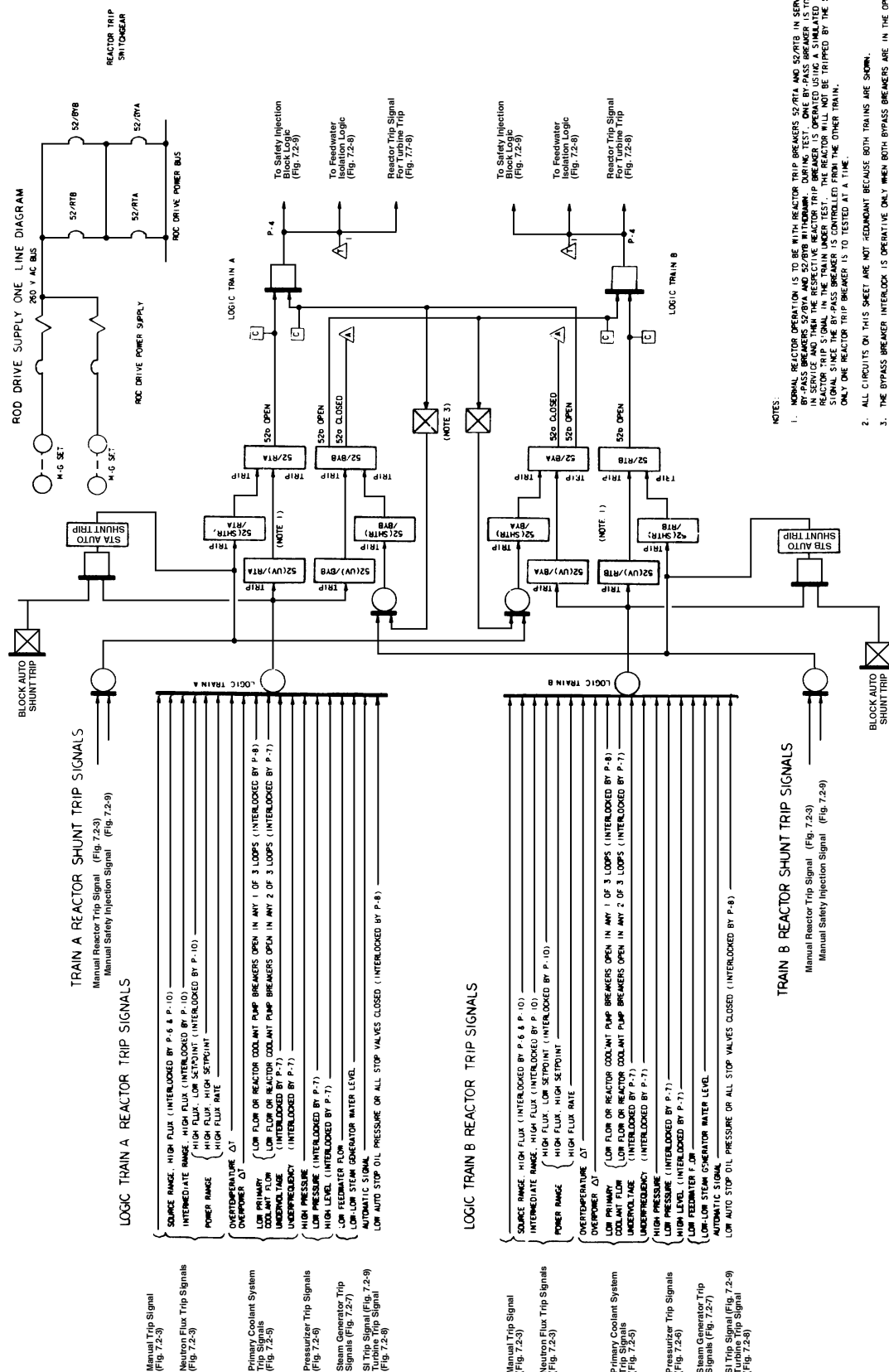
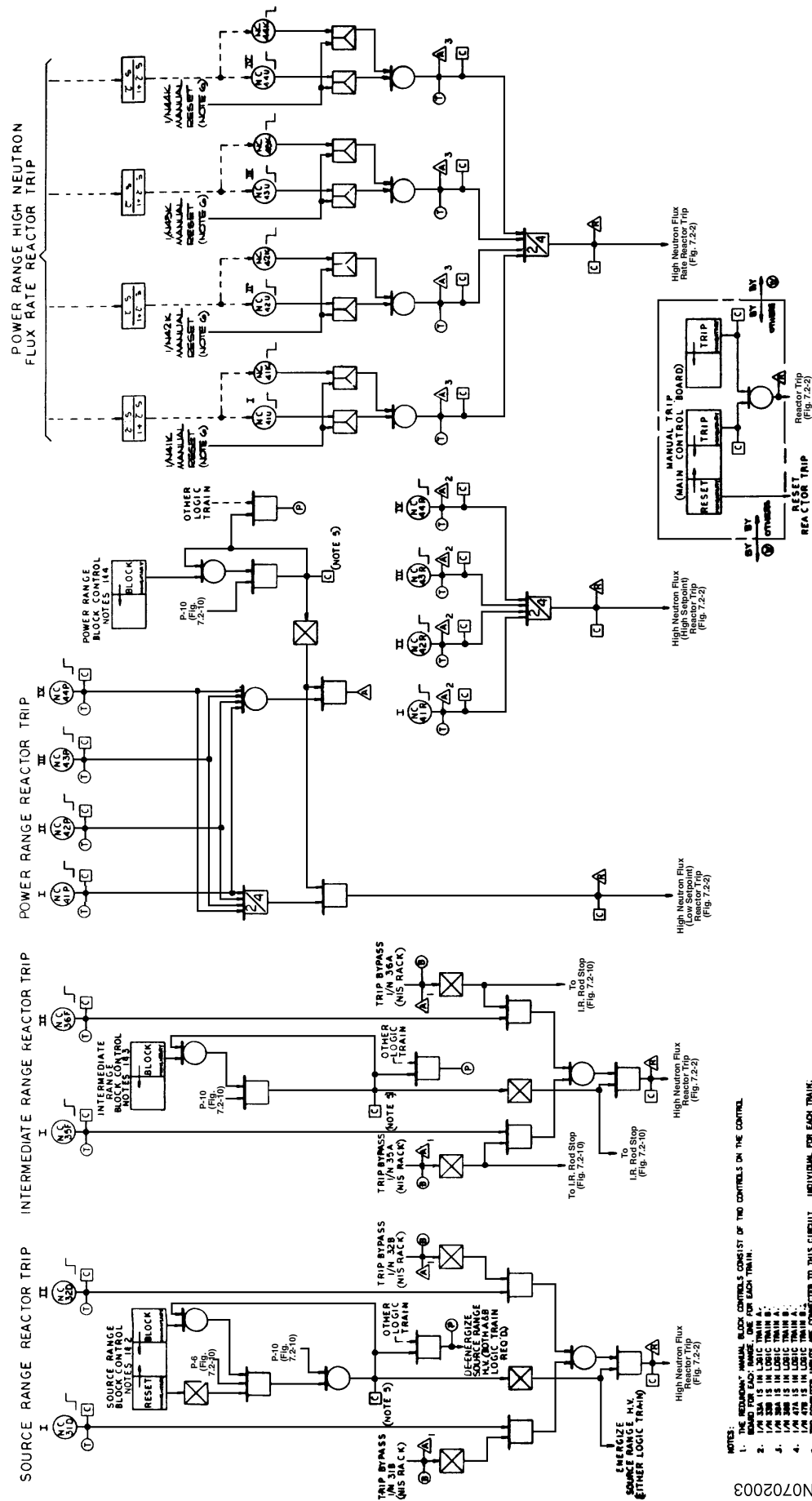
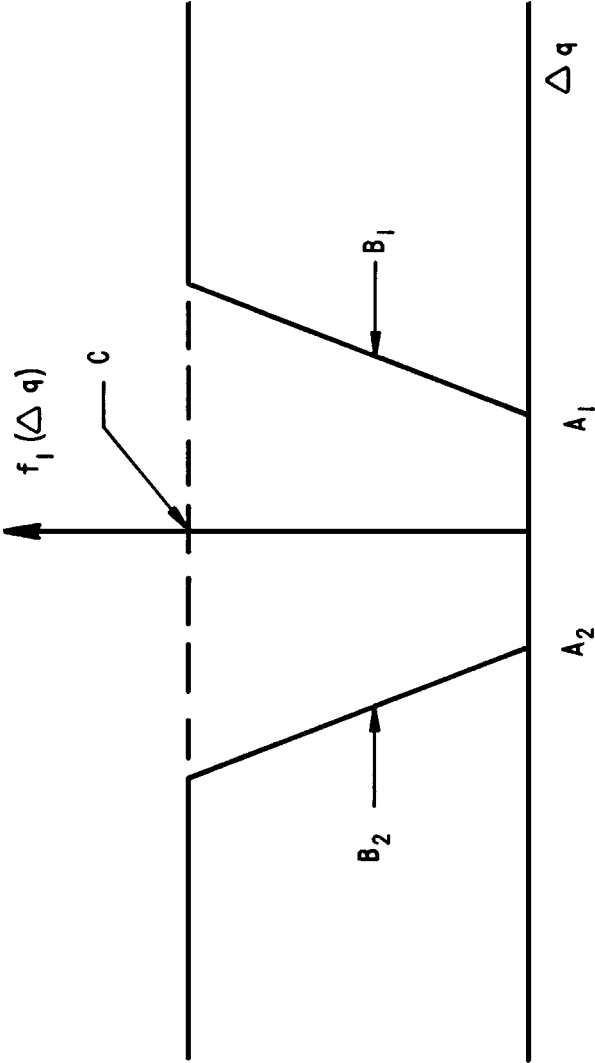


Figure 7.2-3
NUCLEAR INSTRUMENTATION AND TRIP SIGNALS



N072003

Figure 7.2-4
SETPOINT REDUCTION FUNCTION FOR OVERTEMPERATURE ΔT TRIPS (TYPICAL)

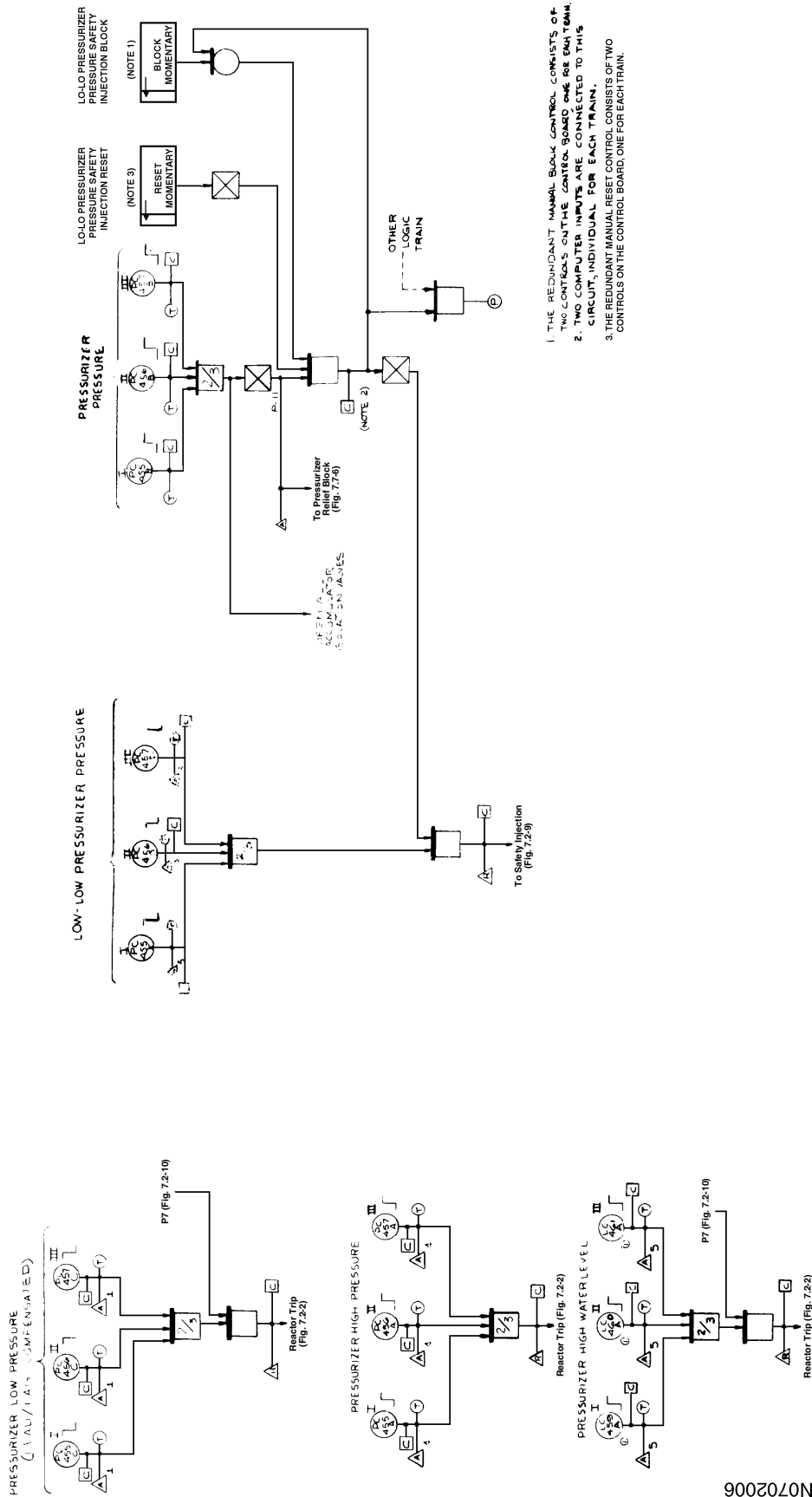


- Δq -NEUTRON FLUX DIFFERENCE BETWEEN UPPER AND LOWER LONG ION CHAMBERS
- A_1, A_2 -LIMIT OF $f_1(\Delta q)$ DEADBAND
- B_1, B_2 -SLOPE OF RAMP; DETERMINES RATE AT WHICH FUNCTION REACHES IT'S MAXIMUM VALUE ONCE DEADBAND IS EXCEEDED
- C -MAGNITUDE OF MAXIMUM VALUE THE FUNCTION MAY ATTAIN

NOTE: THE SPECIFIC SETPOINT REDUCTION FUNCTION FOR NORTH ANNA UNITS 1 AND 2 IS GIVEN IN THE TECHNICAL SPECIFICATIONS.

N0702004

Figure 7.2-6
PRESSURIZER TRIP SIGNALS



N0702006

Figure 7.2-7
STEAM GENERATOR TRIP SIGNALS

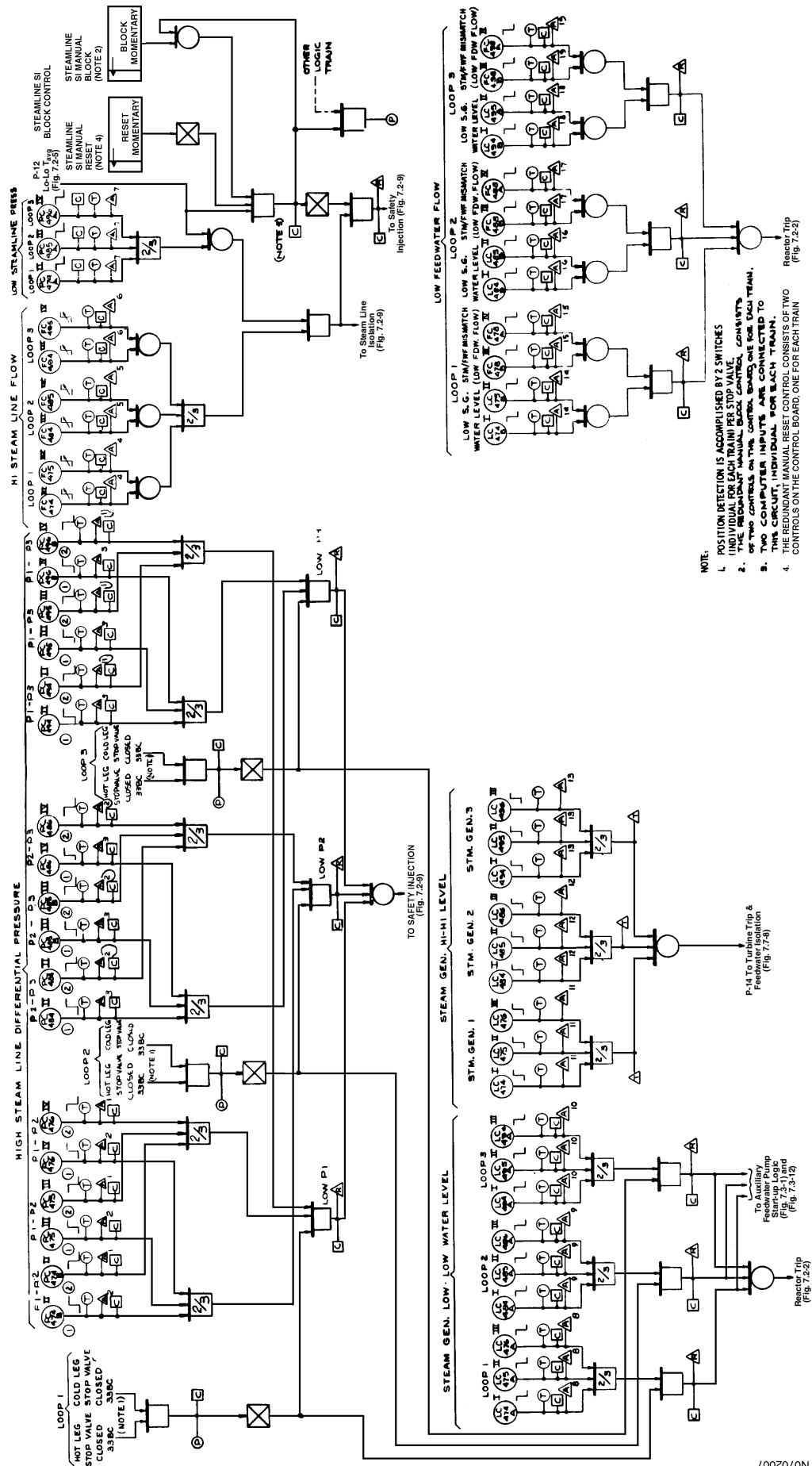
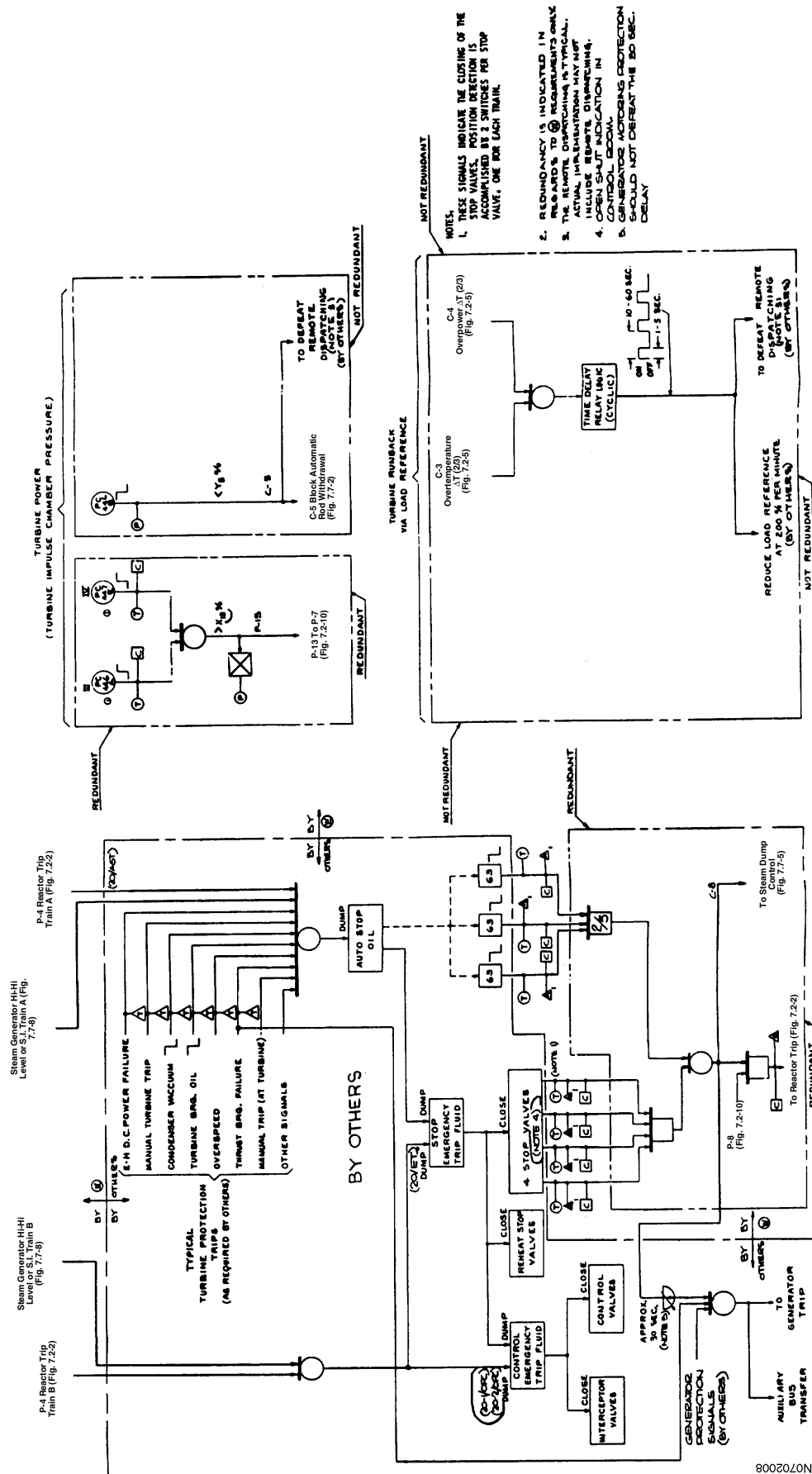
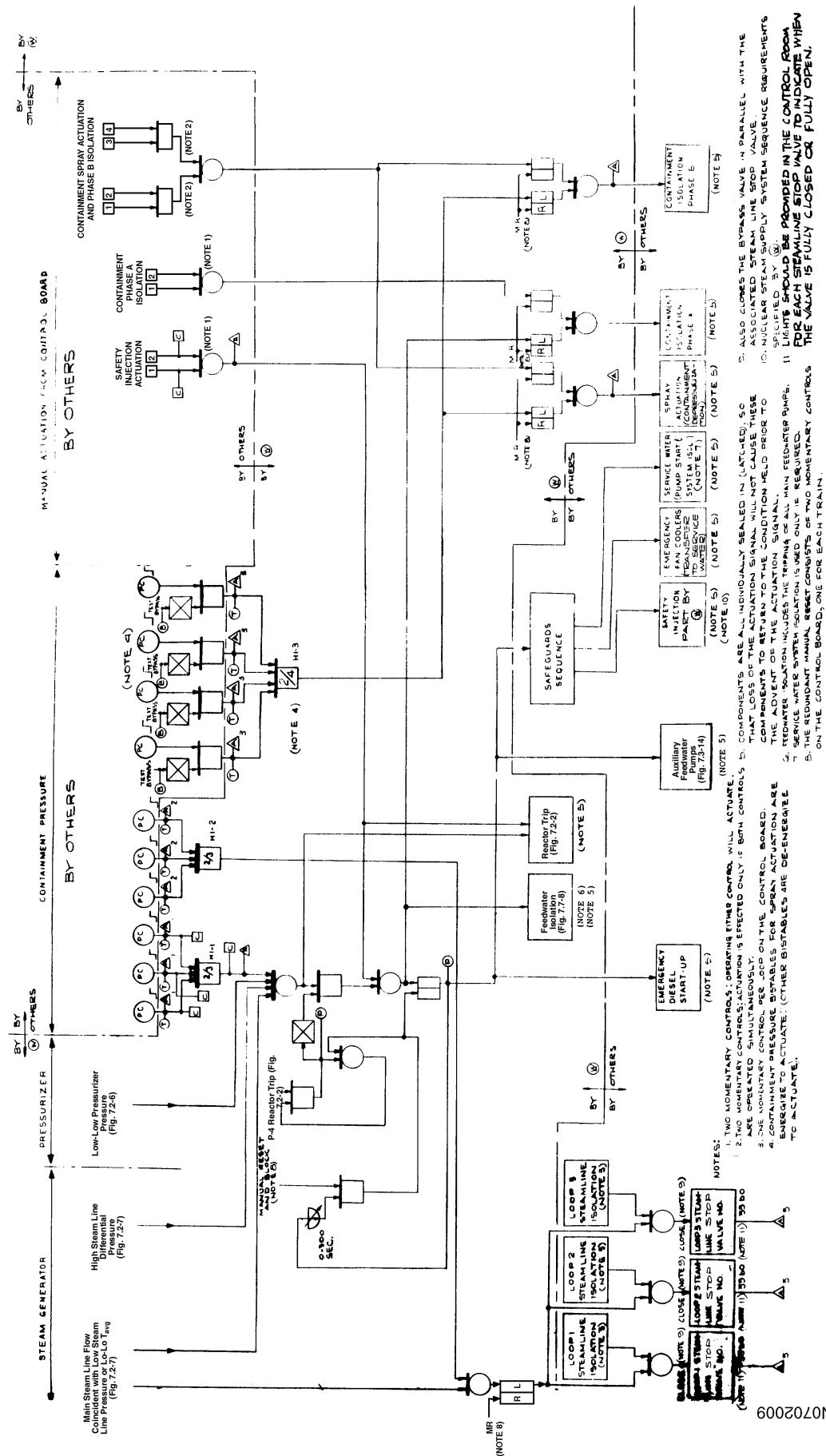


Figure 7.2-8
TURBINE TRIPS, RUNBACKS, AND OTHER SIGNALS



N0702008

Figure 7.2-9
SAFEGUARDS ACTUATION SIGNALS



N0702009

Figure 7.2-10
NUCLEAR INSTRUMENTATION AND BLOCKS

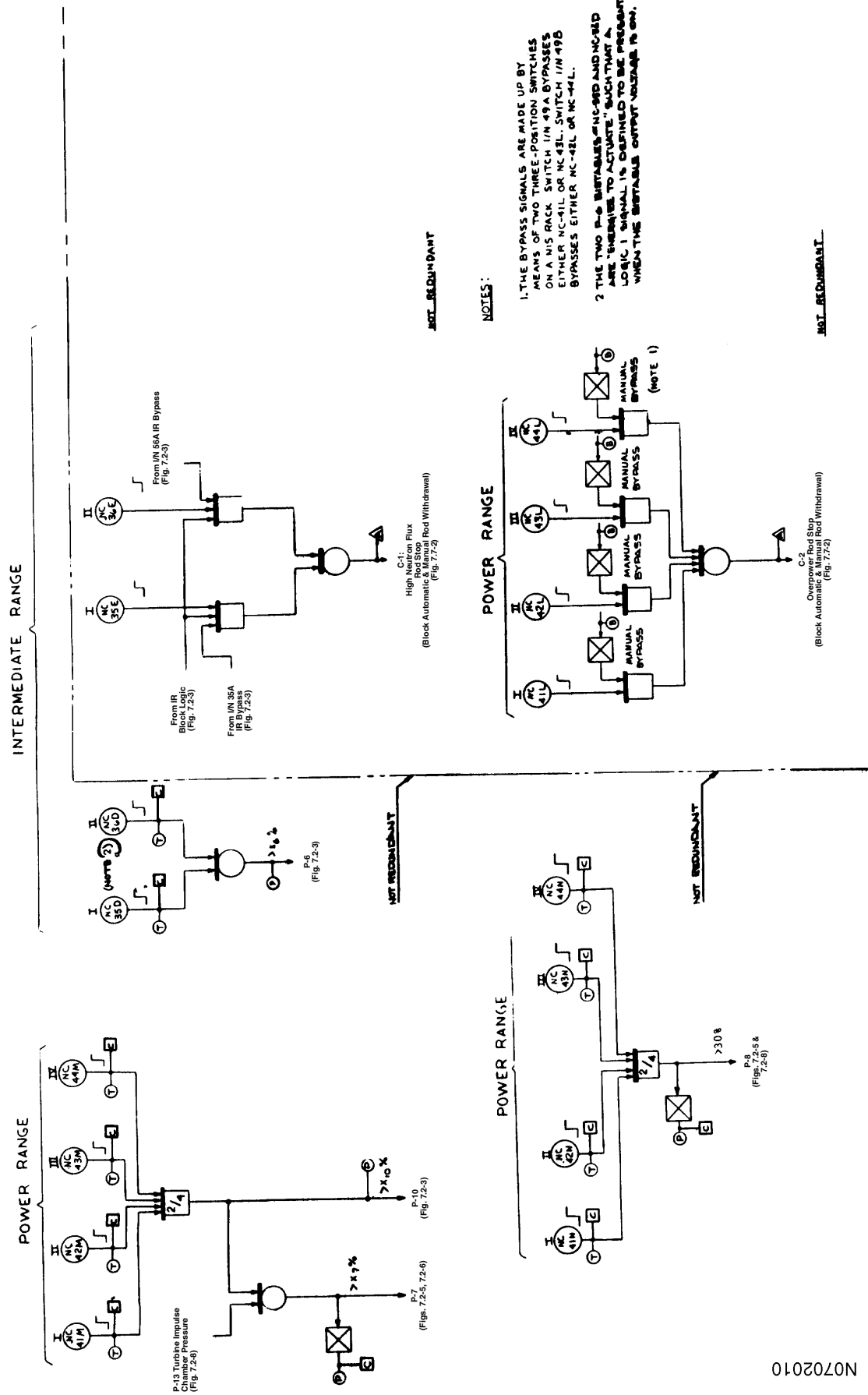
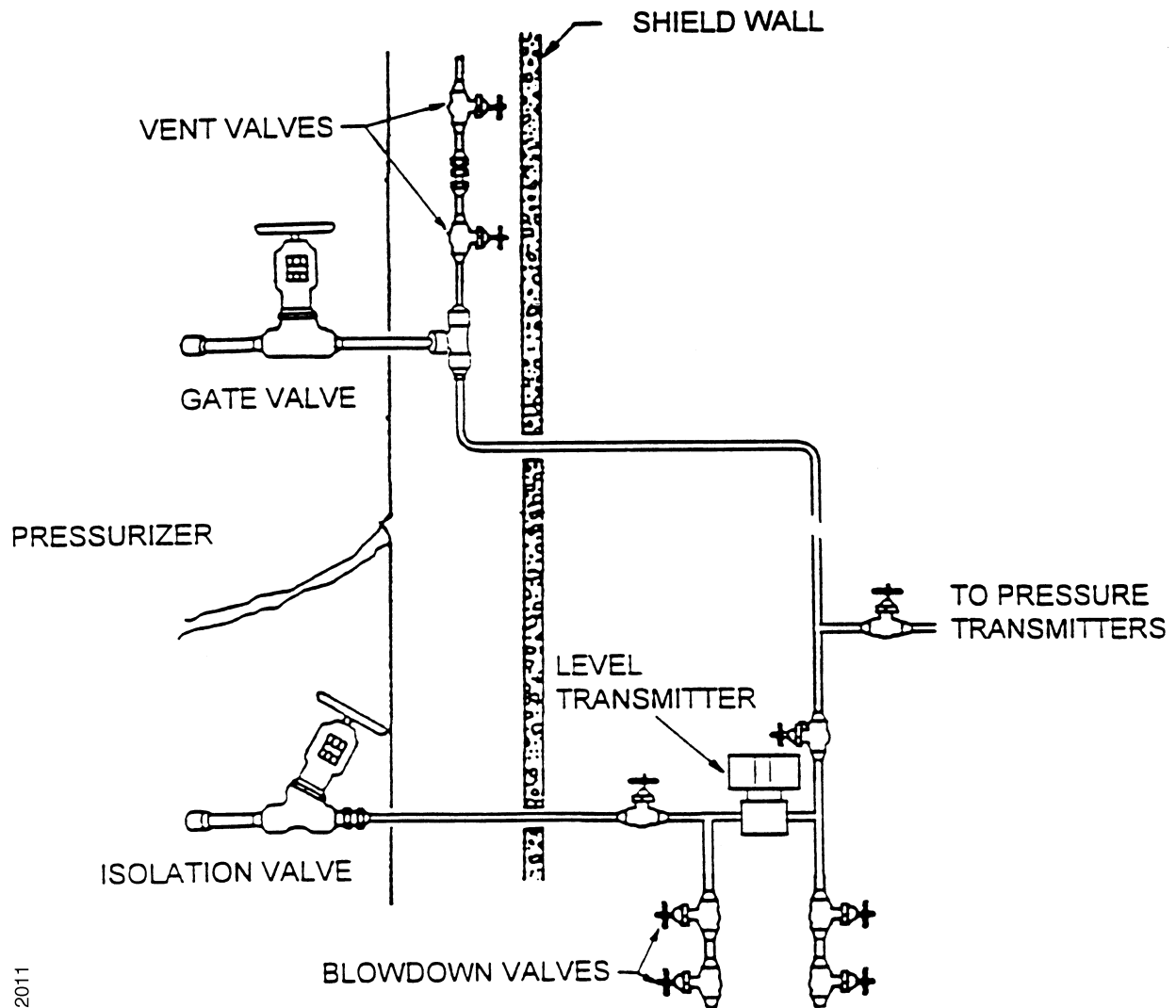
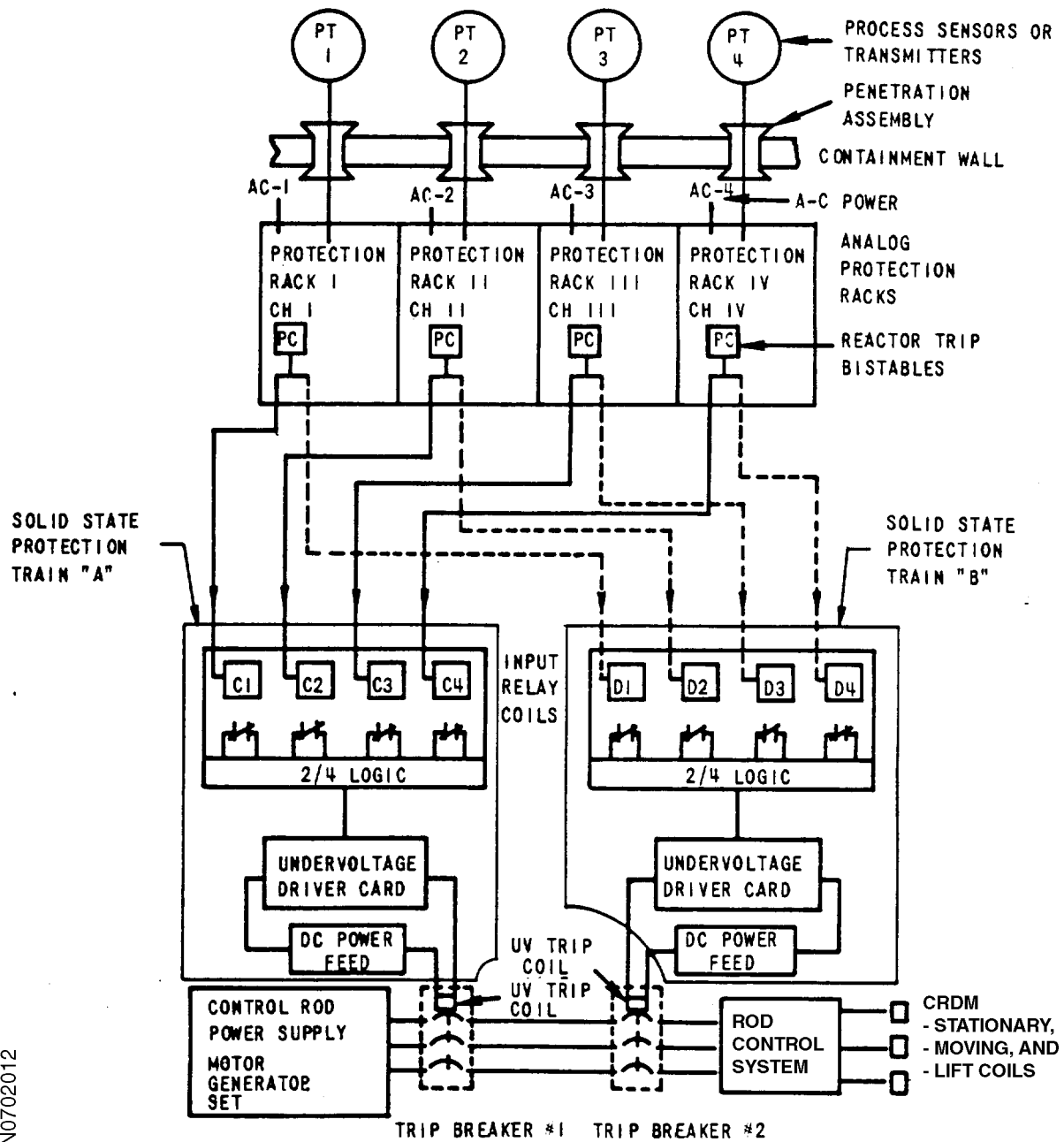


Figure 7.2-11
PRESSURIZER REFERENCE LEG LEVEL SYSTEM



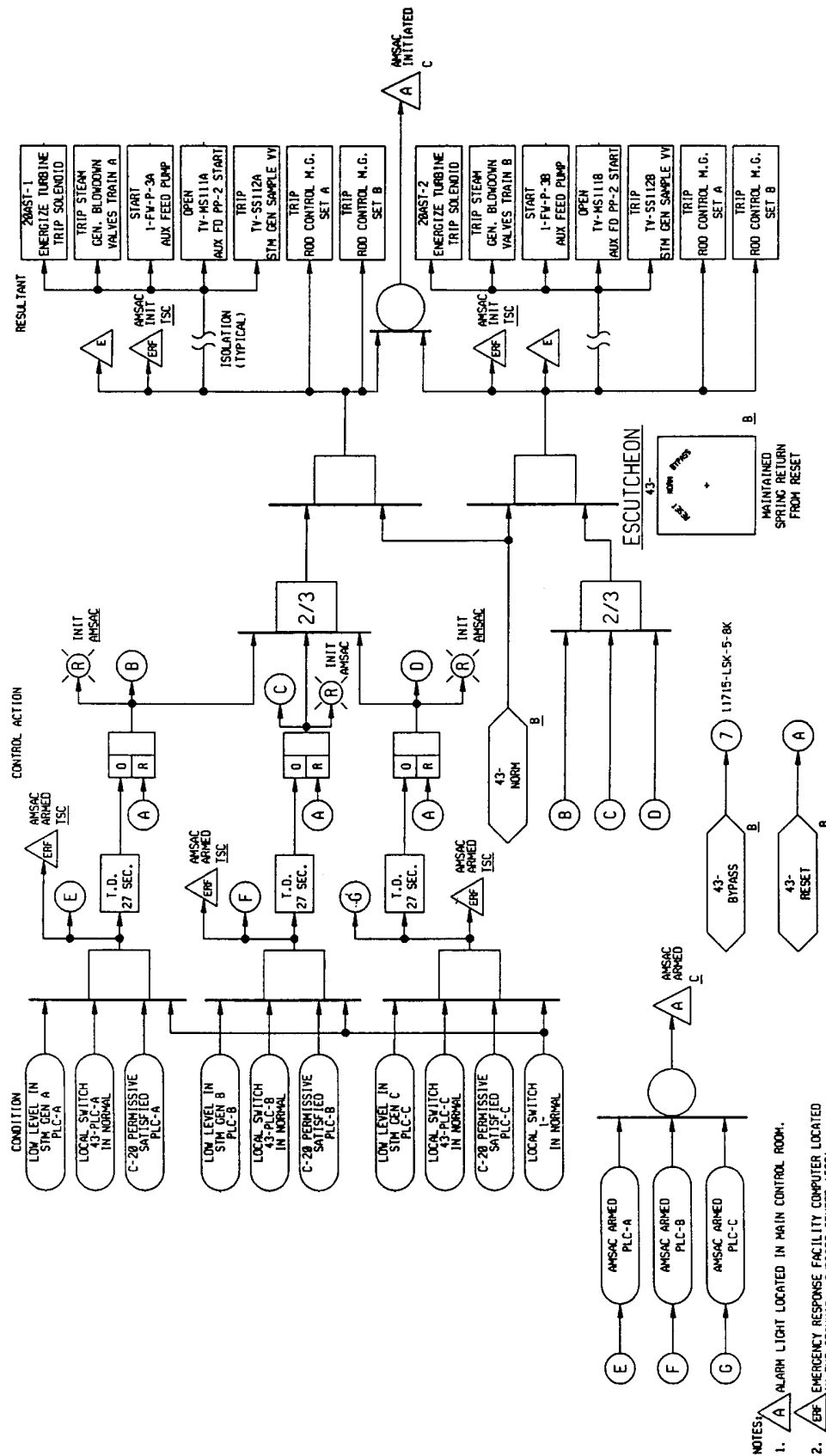
N0702011

Figure 7.2-12
DESIGN TO ACHIEVE ISOLATION BETWEEN CHANNELS



N0702012

Figure 7.2-13
ANTICIPATED TRANSIENT WITHOUT SCRAM MITIGATION SYSTEM ACTUATION CIRCUITRY (AMSAC)



NO702013

Intentionally Blank

7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Electrical schematic diagrams for the engineered safety features (ESF) actuation system, ESF actuator circuits, and their supporting systems are included in reports NA-TR-1001 and NA-TR-1002, *Safety Related Electrical Schematics*, dated May 10, 1973, which were submitted to the Atomic Energy Commission (AEC) on May 18, 1973, as separate documents. For general notes, diagram symbols, and terminology, refer to Reference Drawings 1 through 4.

7.3.1 Description

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

The design meets the requirements of General Design Criteria 13, 20, 21, 22, 23, and 24.

7.3.1.1 Functional Design

The following is a summary of generating station conditions requiring protective action:

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

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

1. Rupture in small pipes or cracks in large primary system pipes:
 - a. Pressurizer pressure.
 - b. Pressurizer water level.
 - c. Containment pressure.

2. Rupture of a reactor coolant pipe (LOCA):
 - a. Pressurizer pressure.
 - b. Pressurizer water level.
 - c. Containment pressure.
3. Steam generator tube rupture:
 - a. Pressurizer pressure.
 - b. Pressurizer water level.
4. Minor secondary system pipe breaks:
 - a. Pressurizer pressure.
 - b. Pressurizer water level.
 - c. Steam-line pressures.
 - d. Steam-line differential pressures.
 - e. Steam flows.
 - f. Reactor coolant average temperatures (T_{avg}).
 - g. Containment pressure.
5. Rupture of a major steam pipe: Same as 4 above.

7.3.1.1.1 Signal Computation

The ESF actuation system consists of two discrete portions of circuitry: an analog portion consisting of redundant channels that monitor various plant parameters such as the reactor coolant system and steam system pressures, temperatures, and flows, and containment pressures; and a digital portion consisting of two redundant logic trains that receive inputs from the analog protection channels and perform the needed logic to actuate the ESF actuation devices. Each digital train can actuate the minimum ESF actuation devices required. The intent is that any single failure within the ESF system shall not prevent system action when required.

The redundant concept is applied to both the analog and logic portions of the system. The separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment vessel penetrations, and analog protection racks, terminating at the redundant groups of ESF logic racks. The design meets the requirements of General Design Criterion 21.

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

The variables are sensed by the analog circuitry as discussed in Reference 1 and in Section 7.2. The outputs from the analog channels are combined into actuation logic as shown in Figures 7.2-5, 7.2-6, 7.2-7, and 7.2-9. The Technical Specifications give additional information pertaining to logic and function. Table 7.3-2 provides the number of channels required to trip and the minimum channels that are required operable.

The interlocks associated with the ESF actuation system are outlined in Table 7.3-1, the Technical Specifications, and the Technical Requirements Manual. These interlocks satisfy the functional requirements discussed in Section 7.1.3.

Manual reset controls on the main control board are provided to switch from the injection to the recirculation phase after a LOCA.

7.3.1.1.2 Devices Requiring Actuation

The following are the actions that the ESF actuation system initiates when it is called on to perform its function:

1. Safety injection.
2. Reactor trip.
3. Feedwater line isolation.
4. Auxiliary feedwater system actuation.
5. Service water (pump start and system valve operation).
6. Containment depressurization system.
7. Containment isolation (phase A and B).
8. Emergency diesel start-up (and loading on loss of power).
9. Main steam line isolation.

7.3.1.2 Design Bases: IEEE Std 279-1971 (Reference 2)

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

The only variable sensed by the ESF actuation system that has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by taking multiple samples from the reactor coolant hot leg. The outputs from three hot leg resistance temperature detectors (RTDs) are summed and averaged to obtain a representative hot leg temperature value for a given loop.

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

The malfunctions, accidents, or other unusual events that could physically damage protection system components or could cause environmental changes and for which provisions have been made to retain the necessary protection system are as follows.

1. LOCA.
2. Steam-line breaks.
3. Earthquakes.
4. Fire.
5. Explosion (hydrogen buildup inside containment).
6. Missiles.
7. Flood.

Minimum performance requirements are as follows:

1. System response times—The ESF actuation response time, or time delay, is defined in the Technical Specifications. The delay time includes sensor, process (analog), and logic (digital) delay plus, for conservatism, the time delay associated with tripping open the reactor trip breakers and control and latching mechanisms, although the reactor trip (or ESF actuation signal) theoretically occurs before or simultaneously with ESF sequence initiation (see Figure 7.2-9).

Maximum allowable time delays in generating the actuation signal for accident protection are listed in the Technical Requirements Manual.

2. System accuracies (Reference 12)—Accuracies required for generating the required actuation signals for loss-of-coolant protection are:

- a. Pressurizer pressure ± 65 psi
- b. Containment pressure $\pm 3.7\%$ of full scale

Accuracies required in generating the required actuation signals for steam-line break protection are:

- a. Steam-line pressure $\pm 11.1\%$ of span
- b. Steam flow signals $\pm 20\%$ ΔP span over the range of 0% to 110% full steam flow
- c. Containment pressure signal $\pm 3.7\%$ of full scale

3. Ranges of sensed variables to be accommodated until the conclusion of protective action is ensured—Ranges required in generating the required actuation signals for loss-of-coolant protection are:

- a. Pressurizer pressure 1700 to 2500 psig
- b. Containment pressure 0 to 65 psia

Ranges required in generating the required actuation signals for steam-line break protection are:

- a. T_{avg} 530°F to 630°F
- b. Steam-line pressure 0 to 1400 psig
- c. Steam-line flow 0 to 120% maximum steam flow
- d. Containment pressure 0 to 65 psia

7.3.1.3 Implementation of Functional Design

7.3.1.3.1 Analog Circuitry

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

See Section 7.7.1.11 for a discussion of electrical separation between safety- and nonsafety-related portions of the process analog system.

The sensors monitoring the primary system are located as shown on the piping flow diagrams and reference drawings in Chapter 5, *Reactor Coolant System*. The secondary system sensor locations are shown on the steam system flow diagrams and reference drawings given in Chapter 10.

7.3.1.3.2 Containment Pressure

Narrow range containment pressure (0-65 psia) is sensed by four physically separated absolute pressure transmitters mounted outside the containment, connected to containment atmosphere by four independent 3/8-inch stainless steel lines. The distance from penetration to transmitter is kept to a minimum, and separation is maintained. Wide range containment pressure (0-180 psia) is sensed by two absolute pressure transmitters mounted outside the containment. Their sensing lines are tapped off the narrow range containment pressure transmitted sensing lines.

The containment pressure instrumentation system is illustrated in Reference Drawings 5 through 10 (for Units 1 and 2) and Reference Drawings 28 and 29 for Unit 2. The design and operation of the system are described in Sections 7.3.1.3.2.1 and 7.3.1.3.2.2. Reference Drawings 1 through 4 contain notes and symbols applicable to the logic diagrams in these sections.

7.3.1.3.2.1 *Design.* The four narrow range pressure transmitters form four redundant pressure measuring channels, which provide inputs to two isolated separated actuating logic trains. The four channels generate initiating signals for the following three conditions:

1. High containment pressure.
2. Intermediate high-high containment pressure.
3. High-high containment pressure.

The high containment pressure signal, on 2/3 channels, is one of four conditions that will initiate a safety injection actuation signal, which, in turn, actuates containment isolation phase A.

Note: The inputs to the logic matrices are implemented via three normally energized logic input relays, which become de-energized on the receipt of a high containment pressure signal.

The intermediate high-high containment pressure signal, on 2/3 channels, is one of two conditions that will initiate a steam-line isolation.

Note: The inputs to the logic matrices are implemented via three normally energized logic input relays, which become de-energized on the receipt of an intermediate high-high containment pressure signal.

High-high containment pressure, on 2/4 channels, is the only condition that will initiate containment depressurization actuation and containment isolation phase B.

Note: The inputs to the logic matrices are implemented via four normally de-energized logic input relays, which become energized on the receipt of a high-high containment pressure signal.

Contacts of input relays enter the signal into the logic portion of the system where the applicable coincidence logic is performed. The solid-state logic operates master relays in the output section, which then operate slave relays, for ESF actuation. The slave relays are used for contact multiplication.

Containment depressurization actuation signals are used in the following ESF systems:

1. Quench spray pumps.
2. Recirculation spray pumps.
3. Refueling water chemical addition system.

4. Service water valves.
5. Diesel loading logic.

Containment isolation phase B occurs simultaneously with containment depressurization actuation, that is, as a direct result of high-high containment pressure. The wide range pressure transmitters provide indication in the control room and are used to monitor containment structural integrity during and following an accident. No protection or control function is associated with these transmitters.

Each instrument channel of the containment pressure instrumentation can be tested and calibrated while the plant is at full power.

Since four batteries are available for emergency instrument power, a loss of station power will not result in the initiation of safety injection, containment isolation, or main steam line isolation.

All equipment actuated by high, intermediate high-high, and high-high containment pressure can be manually actuated from the control room as a final backup.

During normal plant operation, essentially all of the engineered safeguards components, analog, logic, and actuation circuitry can be fully tested. The few remaining components can be partially tested (see Section 7.3.2.1.5).

7.3.1.3.2.2 Operation. The operation of the containment pressure instrumentation system is illustrated in Reference Drawings 5 through 10 (for Units 1 and 2) and Reference Drawings 28 and 29 for Unit 2.

Refer to Reference Drawing 6, which illustrates the operation of high-high containment pressure protection. A high-high containment pressure signal will be initiated if the containment pressure exceeds its setpoint on any 2/4 channels, provided that the associated test switches are closed.

Reference Drawing 7 illustrates containment depressurization actuation, which is initiated by either of the following two conditions:

1. Both of the board-mounted manual spray actuation switches are turned to INITIATE.
2. High-high containment pressure is present on at least two channels.

Reference Drawing 8 illustrates the initiation of high containment pressure. A high containment pressure signal will be initiated if channel pressure exceeds 17 psia in any 2/3 channels or any 2/3 test switches are opened.

Reference Drawing 9 illustrates intermediate high-high containment pressure protection. An intermediate high-high containment pressure signal is initiated when channel pressure exceeds its setpoint on any 2/3 channels, or any 2/3 test switches are opened.

Reference Drawing 10 illustrates the initiation of high-high containment pressure and containment depressurization (train B), which previously have been described for train A.

Two position reset selector switches for containment spray trains A & B exist in the control room.

For Unit 2, Reference Drawings 28 and 29 illustrate the operation of the Recirculation Spray Subsystems, which are a part of the Containment Spray System. Further description of the Recirculation Spray instrumentation is contained in Section 7.3.2.11.

7.3.1.3.3 Safety Injection

Figure 7.2-9 and the design and operation sections below explain the safety injection actuation system. The respective actuation logic is shown in Reference Drawing 11.

7.3.1.3.3.1 *Design.* The four parameters that will initiate a safety injection signal are as follows:

1. Low-low pressurizer pressure.
2. High steam-line pressure differential between the steam generators.
3. High steam-line flow in two out of three steam lines, coincident with either low steam-line pressure or low-low T_{avg} in two out of three loops.
4. High containment pressure.

The purpose of the safety injection system is to maintain clad integrity and thus minimize the release of fission products from the fuel during a LOCA.

The safety injection system provides for the injection of borated water into the reactor coolant system from the accumulators following a LOCA. The three accumulators are self-contained and are designed to supply borated water as soon as the reactor coolant system pressure drops below accumulator pressure. Additional borated water to the reactor coolant system is provided by the charging pumps and the low-head safety injection pumps.

Safety injection actuation signals initiate the following:

1. Reactor trip.
2. Safety injection system operation.
3. Containment isolation phase A.
4. Emergency diesel starting.
5. Main feedwater isolation.
6. Start-up of auxiliary feedwater system.

7. Start signals to service water pumps and repositioning of the valves.
8. Turbine trip.

7.3.1.3.3.2 *Operation.* Refer to Figure 7.2-9, which illustrates the makeup of safety injection actuation. A safety injection actuation signal will be initiated by any of the following conditions:

1. Manual—Turning either of the two board-mounted, manual safety injection switches to INITIATE.
2. Auto—Any of the following:
 - a. High steam flow with low steam-line pressure or low-low T_{avg} .
 - b. High steam-line differential pressure.
 - c. Low-low pressurizer pressure.
 - d. High containment pressure.

A safety injection actuation signal may be manually reset by rotating the two position (NORM/RESET) safety injection reset selector switch to the RESET position, provided that the 1-min time delay has timed out and that the reactor trip breakers are open. One selector switch is provided for each train, train A and train B.

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

1. Refueling water storage tank level—Level instrumentation on the refueling water storage tank consists of four channels. All four channels provide a remote indication at the main control board and two channels provide low-level alarm functions. All four channels provide signals to initiate automatic changeover from injection mode to the recirculation mode of the emergency core cooling system (ECCS), as described in Section 7.3.2.10.
2. High-head safety injection pumps discharge pressure—The discharge header pressure channel clearly shows that the safety injection pumps are operating. This transmitter is outside the containment.
3. Pump energization—Pump motor power feed breakers indicate that they have closed by energizing indicating lights on the control board.
4. Valve position—All ESF remote-operated valves have position indication on the control board to show proper positioning of the valves. Red and green indicator lights are located next to the manual control station showing open and closed positions. These lights thus enable the operator to quickly assess the status of the ESF systems. These indications are derived from contacts integral to the valve operators. In the cases of the accumulator isolation valves, the redundancy of position indication is provided by valve stem-mounted limit

switches, which actuate annunciators on the control board when the valves are not correctly positioned for ESF. The stem-mounted switches are independent of the limit switches in the motor operators. See Section 7.6 for additional information.

5. Containment recirculation air coolers—The air coolers cooling water flow is indicated in the control room. The cooling water exit temperatures are provided to the plant computer. The sensors are outside the reactor containment.
6. Sump instrumentation—The containment sump wide range instrumentation consists of redundant level sensors designed to operate in a post accident environment. LT-RS151A-1, LT-RS151A-2, LT-RS151B-1, and LT-RS151B-2 sump wide range level transmitters are qualified in accordance with IEEE Std 323-1974, to meet post accident conditions, including submergence. The indicators are located in the control room.

7.3.1.3.4 Digital Circuitry

The ESF logic racks are discussed in detail in Reference 3. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 3 also covers certain aspects of on-line test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separation, and provisions for ensuring instrument qualification. The outputs from the analog channels are combined into actuation logic as shown in Figure 7.2-5 (T_{avg}), Figure 7.2-6 (pressurizer pressure and water level), Figure 7.2-7 (steam flow, pressure, and differential pressure), Figure 7.2-9 (ESF actuation), and Figure 7.3-1 (auxiliary feedwater).

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

7.3.1.3.5 Engineered Safety Features Actuation Devices

The outputs of the solid-state logic protection system (the slave relays) are energized to actuate, as are the switchgear and motor control centers for all ESF-actuated devices. The following descriptions and referenced diagrams explain and illustrate the manner in which the engineered safety features are actuated by the ESF actuation signals. Unit protection features and emergency diesel-generator start-up and loading are also described and illustrated. Should an accident occur coincident with a station electrical blackout, the ESF loads are sequenced onto the diesel generators. This loading is discussed in Chapter 8. The design meets the requirements of General Design Criterion 35.

1. Figure 7.3-2 is a general illustration of the relationship of unit trip signals. The interrelation of tripping between the generator, turbine, and reactor is as follows:
 - a. A generator trip will result in a turbine trip.
 - b. A turbine trip after the generator is on line will result in a generator trip.

- c. A turbine trip at a preset minimum power will result in a reactor trip.
 - d. A reactor trip will result in a turbine trip.
2. Figure 7.3-3 illustrates the signal interfaces of ESF actuation and actuated devices. These interfaces are the basis of the ESF system terminology and logic, and the actuation signals are shown in relation to each other as well as the actuated systems.
 3. Figures 7.3-4 and 7.3-5 illustrate that there are two paths provided to actuate the ESF-actuated devices: the first, when emergency bus power is not interrupted; the second, when there is a loss of emergency bus power. Should there be a loss of power, the equipment is started sequentially.
 4. Figure 7.3-6 illustrates the concepts used to adjust and sequence the loads on diesel generators. The inputs will be combined by the logic circuit as required, to initiate the appropriate sequence and loading of the diesel generator for given accident input conditions. The resultant blocks represent typical actions taken on equipment assigned to the emergency bus. Detailed logic for specific loads is shown in Reference Drawings 11 and 12, and Figures 7.3-5, 7.3-7 and 7.3-8.
 5. Reference Drawing 13, Figure 7.3-1, and Figure 7.3-7 illustrate the development of the loss of reserve station service power signal for both Units 1 and 2. Also shown are the resultant actuation of the service water pumps, and the start of auxiliary steam generator feed pumps.
 6. Figures 7.3-5 and 7.2-9 illustrate the auto-start signals for an emergency diesel generator. The emergency diesel generator starts whenever the respective emergency bus voltage is less than 74%, whenever the bus voltage drops below 90% and remains there for 60 seconds or longer, or whenever a safety injection actuation signal is initiated. This is described in Section 8.3.1.1.1.

Also shown in Figure 7.3-5 are the resultants, should the emergency bus voltage continue to decay below 71% nominal. These resultants are the automatic trip of specified loads.

Also illustrated is the subsequent restoration of voltage to the emergency bus, after the emergency diesel-generator supply breaker is closed. Refer to Reference Drawing 12 (containment depressurization) and Reference Drawing 11 (safety injection) for the subsequent restart of the affected ESF actuation devices.

7. Figure 7.3-8 illustrates the equipment that is tripped on a signal from the containment depressurization actuation (CDA) signal. This is done to remove unnecessary loads from the emergency diesel generators.
8. Figure 7.3-9 is a diagram of the undervoltage signal for the normal station service buses. When voltage drops below 70% on 2/3 station service buses (1A, 1B, or 1C), the reactor is tripped, providing the reactor power level is greater than P-7.

Undervoltage on the station service bus results in the following:

- a. Main feedwater pump trips.
 - b. Reactor coolant pump trips.
 - c. Condensate pump trips.
 - d. Low-pressure heater drain pump trips.
 - e. High-pressure heater drain pump trips.
 - f. Normal supply bus breaker trips.
 - g. Bearing cooling water pump trips.
9. If an ESF-actuated device has been actuated by a safety features actuation signal, it cannot be returned to the non-safety-features actuation mode by operator action until the actuation signal has been reset. The protection system is designed such that once initiated, a protection action at the system level (initiation of the final actuation device associated with a given protective function, i.e., quench spray, recirculation spray, chemical addition, safety injection, etc.) goes to completion. Reset capability of ESF signals is required to permit action in the postaccident period. One example is stopping the quench spray pump when the refueling water storage tank level will no longer support continued quench spray pump operation.

The manual reset logic is designed such that any preaccident operation of the reset control switch will not block a subsequent bona fide accident signal. It is important to note that manual control of the spray system cannot be achieved (once protective action at the system level has been initiated) by just resetting the associated actuation signal. The manual reset is the first of a set of deliberate operator actions required to return the system to the non-safety-feature mode.

The circuitry for the feedwater bypass valves is provided with an administratively controlled keylock selector switch. During station operation this switch is placed in the “Normal” position which prevents the blocking of any ESF actuation signals when depressing the feedwater bypass valve reset pushbutton. During cold shutdown or refueling the switch is placed in the “SG Wet Layup” position which allows resetting of the feedwater bypass valves which is necessary to place the steam generators in wet layup. In this case the ESF actuation signal being blocked (steam generator level) is not a valid core protection ESF actuation signal.

Having gone to completion, that is, once breakers are closed or motor-operated valves or other actuators are operated, deliberate operator action is required to return a device to the

non-ESF mode. Specifically, the following two actions per train are required for any device in a given train except for the feedwater bypass valves:

- a. Push reset for the appropriate actuation signal.
- b. Subsequently operate the control switch for the device.

This is illustrated in Figure 7.3-10. Electrical protection trips and emergency diesel-generator sequenced trips are, however, not affected by the blocking logic. In the case of the feedwater bypass valves, during station operation, two operator actions are required to return these valves to the non-ESF actuation mode. The two actions per train which are required are as follows:

- a. Push reset for the appropriate actuation signal.
 - b. Push reset for the feedwater bypass valve.
10. Reference Drawing 14, in conjunction with Figure 7.7-8, illustrates the initiating logic and the actuation devices required for feedwater isolation. The logic shown in Reference Drawing 14 provides a redundant means of isolating feedwater in the event a main feedwater regulating valve should fail to close when required.
 11. Reference Drawing 11, in conjunction with Figure 7.3-4, illustrates automatic actuation logic for all actuation devices initiated by a containment depressurization actuation signal. The effect of the availability of emergency bus voltage on containment depressurization actuated devices is also shown. When emergency bus voltage has been restored for a specified time period, the actuated devices will start, providing the containment depressurization actuation signal is present.
 12. Figure 7.3-8 shows how some devices on the emergency bus are tripped off on the initiation of a containment depressurization signal.
 13. Reference Drawing 11, in conjunction with Figure 7.3-4, illustrates the effect that emergency bus power availability has on devices actuated by the safety injection actuation signal. When emergency bus voltage has been restored for a predetermined time, the ESF-actuated devices will operate, providing the safety injection signal is present.
 14. The diagrams in Reference Drawings 15 and 16 and Figures 7.3-11 and 7.3-13, and the design and operation sections below explain the containment isolation system and its related function.
 15. Service Water spray array MOVs are aligned from either a Train A or Train B SI signal.

7.3.1.3.5.1 *Containment Isolation System Description.* Containment isolation trip valves are provided in the piping of various systems in accordance with the design basis established in Section 6.2.4.

Containment isolation trip valves are air-operated valves operating on an air-to-open signal. Compressed air is supplied to the underside of the valve diaphragm, which compresses the spring and opens the valve. The air above the diaphragm vents to the containment or auxiliary building. A containment isolation signal will de-energize the solenoid valve, blocking the compressed air supply and venting the air from below the diaphragm. The spring will close the valve. The closing action of the valve will be independent of the ambient pressure since both the top and bottom of the diaphragm will be vented to the same atmosphere. The containment isolation valves inside the containment will be ensured of operating regardless of the containment pressure.

Containment isolation valves are tripped closed as a result of containment isolation phase A or phase B, which results from safety injection and high-high containment pressure, respectively. The valves must be manually reset when tripped. The valve controls are designed so that a loss of electric power or air supply will also close the containment isolation valve. The trip signals must be removed and the electric power and air supply restored before the valves can be reset.

The position of each isolation trip valve and the availability of power is monitored on the main control board.

Certain trip valves, in addition to the normal tripping functions, are automatically opened and closed from process control signals as required (refer to Figures 7.3-11 and 7.3-12, and Reference Drawing 16). The trip signals will always override process signals. These combination operational and isolation valves are provided in the following systems:

1. Primary drain transfer pumps.
2. Containment sump pump.
3. Air ejectors.
4. Containment vacuum system.
5. Steam generator blowdown trip valves.

Containment isolation trip valves are powered from 120V ac vital bus panels or from the 120V dc panels.

The containment isolation trip signals are tested in a manner similar to that described in Section 7.2.2.2.1.6.

7.3.1.3.5.2 Containment Isolation System Operation. Containment isolation signals that trip the isolation valves are generated as follows:

1. *Phase A containment isolation*—refer to Figure 7.2-9. Containment isolation phase A actuation will occur as a result of any of the following conditions:
 - a. Either of two containment isolation phase A momentary selector switches being placed in the phase A position. (This actuates trains A and B.)

- b. A safety injection actuation signal.
2. *Phase B containment isolation*—refer to Reference Drawing 10. Containment isolation phase B actuation will occur as a result of any of the following conditions:
- a. Manual containment spray actuation (placement of both bench-mounted switches to INITIATE). This actuates trains A and B.
 - b. High-high containment pressure signal, on 2/4 channels.

The resetting of containment isolation phase A or B is accomplished by the depression of the bench-mounted RESET push buttons. There is one reset push button per train, per isolation phase (four reset push buttons). These push buttons are provided with safety covers to prevent inadvertent operation.

Operating reset push buttons before an isolation signal initiation will not block the isolation signal. However, once the isolation signal is initiated, it can be reset at any time by the operator. Once the signal is reset, it can only be reinitiated (reset-removed) by either of the following:

- 1. Manual switch actuation of containment isolation from the control board.
- 2. Returning respective memory circuits to normal by the disappearance of the (SI or high-high) signal and subsequently having them reoccur.

Figure 7.3-11 illustrates operation of a typical, normally closed trip valve, which is pneumatically operated with a solenoid-operated air pilot valve. The trip valves to which this diagram applies are listed in Reference Drawings 17 and 18, and operation is as follows:

- 1. The valve will be opened by depressing the OPEN push button, or an auto-open process signal (providing the circuit has been reset) if no containment isolation signal condition exists.
- 2. The valve will be closed if any of the following conditions occur:
 - a. Containment isolation.
 - b. The absence of an auto-open process signal and the OPEN push button is not depressed.
 - c. Depression of the CLOSE push button.

Figure 7.3-13 and Reference Drawing 16 illustrates the operation of a typical, normally open trip valve, which is pneumatically operated with a solenoid-operated air pilot valve. The trip valves for which this diagram applies are listed in Reference Drawings 17 and 18, and operation is as follows:

- 1. The valve will be opened provided there is no containment isolation (phase A or B, as applicable) signal and the OPEN push button is depressed.

2. The valve will be closed if any of the following conditions exist:
 - a. A close process signal.
 - b. Depression of the CLOSE push button.
 - c. Containment isolation signal.

Figure 7.3-2 illustrates and describes the turbine and generator trips.

7.3.1.3.5.3 Auxiliary Feedwater System Description and Operation. Figures 7.3-1, 7.3-12, and Reference Drawings 13, 19 and 20 illustrate the operation of the auxiliary steam generator feedwater pumps system.

A turbine-driven auxiliary feedwater pump, FW-P-2, and two motor-driven auxiliary feedwater pumps, FW-P-3A, 3B, receive suction from the emergency condensate storage tank CN-TK-1, which is encased in concrete for tornado missile protection.

Figure 7.3-1 and Reference Drawing 13 illustrate the start and stop of the motor-driven auxiliary feedwater pumps FW-P-3A & -3B. Reference Drawing 19 and Figure 7.3-12 illustrate the operation of the turbine-driven auxiliary feedwater pump FW-P-2.

Auxiliary feed pump motors can be manually started providing:

1. Control switch is in START either at the control board or at the auxiliary shutdown panel, with the transfer switch in the appropriate position.
2. No motor electrical faults are present, that is, lockout relay is reset.
3. No undervoltage has occurred on the bus in the previous 25 seconds.

Immediate automatic starting will take place if the following conditions exist:

1. Control switch at the control board or the auxiliary shutdown panel is in AUTO with transfer switch in appropriate position.
2. No electrical faults are present.
3. The bus has no undervoltage signal present.
4. No safety injection signal is present.
5. Occurrence of any of the following:
 - a. All main feed pumps tripped.
 - b. Low-low steam generator level on two out of three channels of any steam generator. (This is the same setpoint used for reactor trip.)
 - c. Loss of reserve station power.
 - d. AMSAC initiated.

In addition to the start demand signals a, b, c and d above, there is also a delayed auto start in the event a safety injection signal is initiated. This start is delayed 20 seconds to maintain an acceptable voltage profile from the offsite source. In the event of an undervoltage signal concurrent with safety injection, automatic starting will be delayed until 25 seconds after the voltage is restored, to ensure an acceptable voltage profile while starting multiple loads powered from the emergency diesel generator. Control switch and electrical fault permissives also apply to this start feature.

With the transfer switch properly positioned, the auxiliary feedwater pump motors can be stopped manually with the control switches at either the main control board or the auxiliary shutdown panel. They will stop automatically with a motor protection trip.

Figure 7.3-12 and Reference Drawing 19 illustrates the operation of the full-sized, turbine-driven auxiliary feedwater pump FW-P-2. Steam to the turbine driver can be admitted through either MS-TV-111A & -211A or through MS-TV-111B & -211B.

MS-TV-111A & B and -211A & B can be manually operated using selector switches at the control board or the auxiliary shutdown panel, provided the transfer switch is in the appropriate position.

MS-TV-111A & -211A will open automatically as a result of the following train A signals (similarly train B signals operate MS-TV-111B & -211B), providing the selector switch at the control board or the auxiliary shutdown panel is in the AUTO position and the transfer switch is in the appropriate position:

1. Loss of preferred station power.
2. Safety injection signal.
3. Low-low steam generator level on two out of three channels of any steam generator.
4. All main feed pumps tripped.
5. AMSAC initiated.

With the transfer switches properly positioned, the turbine driven auxiliary feedwater pump can be stopped manually using the control switches either on the main control board or in the auxiliary shutdown panel.

The discharge valve from each auxiliary steam generator feedwater pump to its associated steam generator is normally open. The steam generator blowdown valves trip closed on signals actuating either SOV-MS 111A or SOV-MS 111B.

Refer to Reference Drawing 20. This illustrates the operation of auxiliary feedwater control valve HCV-FW 100A and is typical for HCV-FW 100B and C. The valve can be controlled from a manual loading station at the control board or from a similar station at the auxiliary shutdown panel, providing the transfer switch, located at the shutdown panel, is in the appropriate position.

Auxiliary feedwater flow indication to each steam generator is powered from the 120V ac vital bus, which is battery-backed, and flow is displayed in the control room.

NUREG-0737 requires that the indication to be environmentally qualified, and powered from a highly reliable, battery-backed, non-Class 1E power source. Although the power supply is Class 1E, the power cables to the indicator are not safety-related, and the indicators on the control board do not have barriers for safety-related separation. The indication is environmentally qualified by virtue of being located in a mild environment. The power supply and equipment exceed the requirements of NUREG-0737.

Auxiliary feedwater pump discharge pressure is indicated at the control board and the auxiliary shutdown panel. Auxiliary feedwater pump suction pressure is also indicated at the control board.

Reference Drawing 20 also illustrates the operation of motor-operated valves FW-MOV-100A & -200A. Operation for FW-MOV-100B & -200B, FW-MOV-100C & -200C, and FW-MOV-100D & -200D.

Motor-operated valve FW-MOV-100A may be modulated open, provided both of the following conditions exist:

1. Transfer switch, located at the auxiliary shutdown panel, is in the appropriate position.
2. OPEN/CLOSE switch for FW-MOV-100A is held in the OPEN position.

Motor-operated valve FW-MOV-100A may be modulated closed, provided both of the following conditions exist:

1. Transfer switch, located at the auxiliary shutdown panel, is in the appropriate position.
2. OPEN/CLOSED switch for FW-MOV-100A is held in the CLOSE position.

To improve the reliability of the auxiliary feedwater system, alarms have been added in the control room to indicate abnormal alignment of auxiliary feedwater pump discharge valves FW-MOV-100A, B, C, & D, and -200A, B, C, & D and FW-HCV-100A, B, & C, and -200A, B, & C, and the auxiliary feedwater pump turbine throttle trip valve. Refer to Section 10.4.3.5 for further details.

7.3.1.3.5.4 Main Steam Isolation Trip Valves. Reference Drawing 21, and the description below, show the operation of the main steam isolation trip valves.

The three main steam isolation trip valves, TV-MS 101A, B, and C, are installed in the main steam line outside the reactor containment in a tornado-missile-protected enclosure. They are similar in design to standard swing check valves, except that they are installed counter to the normal steam flow direction with the disk held out of the flow path by an air cylinder operator on each side.

The purpose of these valves is to close immediately in case of a rupture in the main steam line between the valve and the turbine, thus preventing rapid blowdown of the shell side of the steam generator and rapid cooling of the reactor core.

Provisions to test for the operability of SOV-MS-101 Train A, Train B, 101B Train A, Train B, 101C Train A, and Train B are provided by the Westinghouse *Safeguard On-Line Testing System*, which tests for continuity through the safeguard contact and solenoid valve.

Refer to Reference Drawing 21. The following conditions will lead to main steam line isolation trip of all three valves.

1. A high steam flow in two out of three steam lines, coincident with
 - a. Low steam-line pressure in two out of three lines, or
 - b. Low-low average reactor coolant temperature (below approximately 543°F).
2. An intermediate high-high containment pressure signal.
3. The CLOSE push button for either trip solenoid valve (Train A or Train B) is depressed in the main control room for each of the three MSTVs.
4. The control switch in the Main Control Room for trip solenoid valves SOV-MS101A-6, B-6, and C-6, is placed in the EMERG. CLOSE position and depressed.
5. The control switch in the Emergency Switchgear Room for trip solenoid valves SOV-MS101A-7, B-7, and C-7, is in the EMERG. CLOSE position.

Once the main steam-line isolation trip valve receives a close signal (either by manual pushbutton actuation or automatic close signal), a relay contact seals the solenoids in the energized position. This seal-in is broken when the OPEN push button is pressed and the automatic isolation signal is reset.

When the valves are closed by one of the above, the valves can be reopened by depressing the OPEN push button, providing none of the trip conditions exist, both control switches are in the NORMAL position, and the upstream (steam generator) pressure is less than 4 psi greater than the downstream pressure.

Air-operated bypass valves are provided to allow the operator to equalize pressure on either side of the main steam isolation trip valve disk during unit start-up or after spurious trip. These valves are automatically de-energized to vent air to close by the same auto trip logic used to trip the main steam line isolation valves. Refer to Reference Drawing 22.

7.3.2 Analysis

7.3.2.1 Evaluation of Compliance With IEEE Std 279-1971 (Reference 2)

7.3.2.1.1 Single-Failure Criteria

The discussion in Section 7.2.2.2.1 is applicable to the ESF actuation system, with the following exception.

In the engineered safety features, a loss of instrument power will call for the actuation of ESF equipment controlled by the specific bi-stable that lost power (containment spray excepted). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in Chapter 8. For containment spray, the final bi-stables are energized to trip to avoid spurious actuation. In addition, manual containment spray requires simultaneous actuation of both manual controls. This is considered acceptable because spray actuation on high-high containment pressure signal provides automatic initiation of the system via protection channels meeting the criteria in Reference 2. Moreover, all safety-related equipment (valves, pumps, etc.) can be individually manually actuated from the control board. Hence, a secondary mode of containment spray initiation is available.

The design meets the requirements of General Design Criteria 21 and 23.

7.3.2.1.2 Equipment Qualification

Equipment qualification is discussed in Section 3.11 and in Reference 4.

7.3.2.1.3 Channel Independence

The discussion presented in Section 7.2.2.2.1 is applicable. The ESF outputs from the solid-state logic protection cabinets are redundant, and the actuations associated with each train are energized up to and including the final actuators by the separate ac power supplies that power the logic trains.

7.3.2.1.4 Control and Protection System Interaction

The discussions presented in Sections 7.2.2.2.1 and 7.2.2.3.5 are applicable.

7.3.2.1.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in Section 7.2.2.2.1 are applicable to the sensors, analog circuitry, and logic trains of the ESF actuation system.

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

7.3.2.1.5.1 Testing of Engineered Safety Features Actuation Systems. The ESF systems are tested to provide assurance that the systems will operate as designed and will be available to

function properly in the unlikely event of an accident. The testing program, which meets the requirements of General Design Criteria 21, 37, 40 and 43, and Safety Guide 22, is as follows:

1. Prior to initial plant operations, ESF system tests were conducted.
2. Subsequent to initial start-up, ESF system tests are conducted during each regularly scheduled refueling outage.
3. During on-line operation of the reactor, all of the ESF analog and logic circuitry are fully tested. In addition, essentially all of the ESF final actuators are fully tested, except for the contacts of most slave relays. The contacts of these slave relays are tested functionally when the reactor is shut down for refueling.

7.3.2.1.5.2 Performance Test Acceptability Standards for the “S” (Safety Injection Signal) and for the “P” (Automatic Demand Signal for Containment Spray Actuation) Actuation Signals Generation. During reactor operation, the basis for ESF actuation systems acceptability is the successful completion of the overlapping tests performed on the reactor trip and the ESF actuation systems. Analog checks verify the operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits through to and including the logic input relays. Solid-state logic testing checks the digital signal path from and including logic input relay contacts through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays. The only small part of the actuation system logic which is not tested on-line is the contact portion of most slave relays. These slave relays are not actuated on-line because doing so would adversely affect the safety of the plant or disrupt reactor operation. The contacts of these slave relays are proven operable by functionally testing them when the reactor is shut down for refueling. The final actuators are routinely tested on-line by the normal pump and valve surveillances.

Maintenance checks such as resistance to ground testing of signal cables are typically conducted for only the short term purpose of verifying proper installation following a replacement of cabling. In accordance with 10 CFR 50.49, qualification test data for cabling are documented for the long term purpose of establishing what constitutes an acceptable cable qualification life based on typical radiation exposures.

7.3.2.1.5.3 Frequency of Performance of Engineered Safety Features Actuation Tests. During normal reactor operation, complete system testing (excluding sensors or those devices whose operation would cause plant upset) is performed as required by the Technical Specifications. Further testing, including the sensors and actuated devices, as required by the Technical Specifications, is performed during scheduled plant shutdowns for refueling.

7.3.2.1.5.4 Engineered Safety Features Actuation Test Description. The following sections describe the testing circuitry and procedures for the on-line portion of the testing program. The guidelines used in developing the circuitry and procedures were as follows:

1. The test procedures must not involve the potential for damage to any plant equipment.

2. The test procedures must minimize the potential for accidental tripping.
3. The provisions for on-line testing must not adversely affect the safety of the plant or disrupt reactor operations.

7.3.2.1.5.5 *Descriptions of Initiation Circuitry.* Several systems comprise the total ESF system, most of which may be initiated by different process conditions and reset independently of each other.

The remaining functions are initiated by a common signal (safety injection) (see Figure 7.3-3), which in turn may be generated by different process conditions.

In addition, the operation of all other vital auxiliary support systems, such as auxiliary feedwater, component cooling, and service water, is initiated via the ESF starting sequence actuated by the safety injection signal.

Each function is actuated by a logic circuit duplicated for each of the two redundant trains of ESF initiation circuits.

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

7.3.2.1.5.6 *Analog Testing.* Analog testing is identical to that used for reactor trip circuitry and is performed as specified in the Technical Specifications. Briefly, in the analog racks, proving lamps and analog test switches are provided. Administrative control requires, during bi-stable testing, that the bi-stable output be put in a trip condition by placing the test switch in the test position. This action connects the proving lamp to the bi-stable and disconnects and thus de-energizes (operates) the bi-stable output relays in train A and train B cabinets, and allows the injection of a test signal to the channel. Relay logic in the process cabinets automatically blocks the test signal unless all of the channel bi-stables are tripped. This, of necessity, is done one channel at a time. Status lights and single-channel trip alarms in the main control room confirm that the bi-stable relays have been de-energized and the bi-stable outputs are in the trip mode. An exception to this is containment depressurization, which is energized to actuate 2/4 and reverts to 2/3 when one channel is in test.

Refer to Reference Drawing 5. Relay R-4, of channel test switch cards, is operable for test purposes only when all three comparator trip switch cards have been placed in the appropriate positions. Once relay R-4 has been energized, a test signal can be inserted through a test jack via channel test switch card and monitored at the test points shown. Verification of bi-stable trip setting can now be confronted by the proving lamps.

The analog test switch is then operated and a signal is inserted through a test jack. The verification of the bi-stable trip setting is now confirmed by the proving lamps.

7.3.2.1.5.7 Solid-State Logic Testing. After the individual channel analog testing is complete, the logic matrices are tested from the train A or train B logic rack test panels. This step provides overlap between the analog and logic portions of the test program. During this test, each of the logic inputs is actuated automatically in all combinations of trip and nontrip logic. Trip logic is not maintained long enough to permit master relay actuation; master relays are “pulsed” to check continuity. Following the logic testing, the individual master relays are actuated electrically to test their mechanical operation. The actuation of the master relays during this test will apply low voltage to the slave relay coil circuits to allow continuity checking, but not slave relay actuation. During logic testing of one train, the other train can initiate the required ESF function. For additional details, see Reference 3.

7.3.2.1.5.8 Actuator Testing. At this point, the testing of the initiation circuits through the operation of the master relay and its contacts to the coils of the slave relays has been accomplished.

With few exceptions, the units are not designed to actuate the slave relays on-line; therefore, the slave relays are functionally tested during the refueling outages. Various performance tests (PTs) are performed during the refueling cycle to ensure ESF system operability. The slave relay are verified operable during these tests. The PTs verify that each contact on the slave relay performs its safety function.

7.3.2.1.5.9 Time Required for Testing. It is estimated that analog testing for most channels can be performed at a rate of several channels per hour provided that no channels are found out of calibration. Logic testing for one logic train may take as long as 2 hours. The testing of actuated components (including those that can only be partially tested) is a function of control room operator availability. Several shifts are required to accomplish these tests. During this procedure, automatic actuation circuitry will override testing.

7.3.2.1.5.10 Safety Guide 22. Periodic testing of the ESF actuation functions as described complies with AEC Safety Guide 22, *Periodic Testing of Protection System Actuation Functions*, February 1972.

Under the present design of the ESF, testing can be accomplished as described in the preceding sections; all actuated devices and logic can be tested at power except for the contacts of most slave relays and the following protection functions: generation of a safety injection signal by use of the manual safety injection switch; generation of the containment depressurization signal by use of the manual spray actuation switch.

As required by Safety Guide 22, where actuated equipment is not tested during reactor operation it has been determined that:

1. There is no practicable system design that would permit the operation of the actuated equipment without adversely affecting the safety or operability of the plant.
2. The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation.
3. The actuated equipment can routinely be tested when the reactor is shut down.

It should be noted that the above criteria has been applied to the contacts of most slave relays because their actuation has been determined to adversely affect plant safety or disrupt reactor operation.

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

7.3.2.1.5.11 *Summary.* The procedures described provide the capability for checking completely from the process signal to the logic cabinets and from there to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc., including all field cabling actually used in the circuitry called on to operate for an accident condition. For those devices whose operation could adversely affect plant safety or disrupt reactor operation, the procedure provides for checking from the process signal to the logic rack and, testing of most slave relay contacts to the actuated equipment is performed during refueling outages.

The procedures require testing at various locations, as follows:

1. Analog testing and verification of bi-stable setpoint are accomplished at process analog racks. The verification of bi-stable relay operation is done at the main control room status lights.
2. Logic testing through the operation of the master relays and low-voltage application to slave relays is done at the logic rack test panel.
3. The testing of pumps, fans, and valves is accomplished by IWV and IWP Programs. A full functional test is performed during the refueling cycle to ensure all actuated equipment is operable.
4. The contacts of the slave relays are verified operable during the testing mention in 3 above.

7.3.2.1.5.12 *Testing During Shutdown.* Emergency core cooling system tests are performed at each major fuel reloading. With the reactor coolant system pressure less than or equal to 450 psig

and temperature less than or equal to 350°F, a test safety injection signal will be applied to initiate the operation of the system. The low head safety injection and centrifugal charging pumps are made inoperable for this test.

Containment spray system tests are performed at each major fuel reloading. The tests are performed with the isolation valves in the spray supply lines at the containment and spray additive tank blocked closed and are initiated by tripping the normal actuation instrumentation.

The balance of the requirements listed in IEEE Std 279-1971 (Paragraphs 4.11 through 4.22) are discussed in Section 7.2.2.2.1. Paragraph 4.20 receives special attention in Section 7.5.

7.3.2.2 Evaluation of Compliance With IEEE Std 308-1969 (Reference 5)

See Chapter 8, which discusses the power supply for the protection systems, for discussions of compliance with this criterion.

7.3.2.3 Evaluation of Compliance With IEEE Std 323-1971 (Reference 6)

The ESF instrumentation is type tested to substantiate the adequacy of design. This is the preferred method, as indicated in Reference 6. Type tests may not conform to the format guidelines set forth in Reference 6.

7.3.2.4 Evaluation of Compliance With IEEE Std 334-1971 (Reference 7)

See Section 3.11.2.2 for discussion of inside recirculation spray pumps in relation to IEEE Std 334-1971 compliance.

7.3.2.5 Evaluation of Compliance With IEEE Std 338-1971 (Reference 8)

Periodic response time testing of ESF systems has been established in the Technical Specifications to meet the intent of IEEE Std 338-1971. Only those response times used in the accident analysis need to be included in the testing program.

7.3.2.6 Evaluation of Compliance With IEEE Std 344-1971 (Reference 9)

The seismic testing, as set forth in Section 3.10 and References 1, 2, and 4, conforms to the guidelines set forth in Reference 9.

7.3.2.7 Evaluation of Compliance With IEEE Std 317-1971 (Reference 10)

See Section 3.8.2.1.4 for a discussion of electrical penetrations and compliance with IEEE Std 317-1971.

7.3.2.8 Evaluation of Compliance With IEEE Std 336-1971 (Reference 11)

Instrumentation and electrical equipment was installed, inspected, and tested in accordance with IEEE Std 336-1971. See Section 8.3.1.1.2.2 for a discussion of compliance of the vital ac power system with IEEE Std 336-1971.

7.3.2.9 Summary

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

The ESF actuation system must detect Condition III and IV faults and generate signals that actuate the ESF. The system is designed to sense the accident condition and generate the signal actuating the protection function reliably and within a time consistent with the accident analyses in Chapter 15.

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

Operating procedures require that the complete ESF actuation system normally be operable. However, the redundancy of system components is such that the system operability assumed for the safety analyses can still be met with certain instrumentation channels out of service. Channels that are out of service are to be placed in the tripped mode, except the containment high-high bi-stables are blocked (bypassed).

7.3.2.9.1 Loss-of-Coolant Protection

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

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

High containment pressure also actuates the emergency core cooling system, providing additional protection as a backup to actuation on low-low pressurizer pressure. Emergency core cooling actuation can be brought about on sensing this other direct consequence of a primary system break, that is, the protection system detects the leakage of the coolant into the containment. The generation time of the actuation signal, about 1.0 second after detection of the consequences of the accident, is adequate.

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

The delay time between the detection of the accident condition and the generation of the actuation signal for these systems is assumed to be about 1.0 second, well within the capability of the protection system equipment. However, this time is short compared to that required for the start-up of the fluid systems.

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

7.3.2.9.2 Steam-Line Break Protection

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

Additional protection against the effects of steam-line break is provided by feedwater isolation, which occurs on the actuation of the emergency core cooling system. Feedwater line isolation is initiated to prevent excessive cooldown of the reactor.

Additional protection against a steam-line-break accident is provided by the closure of all steam-line trip valves to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (about 2.0 seconds) is again short compared to the time to trip the fast-acting steam-line trip valves, which are designed to close in less than approximately 5 seconds.

In addition to the actuation of the engineered safety features, the effect of a steam-line-break accident generates a signal resulting in a reactor trip on overpower, or following emergency core cooling system actuation. However, the core reactivity is further reduced by the highly borated water injected by the emergency core cooling system.

The analyses in Chapter 15 of the steam-line-break accidents and an evaluation of the protection system instrumentation and channel design shows that the ESF actuation system is effective in mitigating the effects of a steam-line-break accident.

7.3.2.10 **Automatic Changeover From Injection Mode to Recirculation Mode After Loss of Primary Coolant**

The ESF actuation system also provides the logic for the automatic switchover sequence from the injection mode to the recirculation mode following a LOCA.

The automatic switchover sequence is initiated when actuation signals are generated by both the two-of-four refueling water storage tank (RWST) low-low-level protection logic and the safeguards protection logic (SI signal). (See Figure 7.3-14.)

Each of the four RWST level channel bi-stables provides an RWST low-low level signal to both the Train A and Train B solid state protection systems. Thus, when two-of-four RWST level channel bi-stables generate an RWST low-low level actuation signal it is developed in both safeguards protection cabinets. Each of the four RWST level channel bi-stables is aligned to one of four RWST level channels. Each level channel is assigned to a separate vital instrument bus. The RWST level channel bi-stables are the following:

1. Normally de-energized.
2. De-energized on loss of power.
3. Energized on RWST low-low level.

A safeguards protection logic actuation signal (SI signal) is also required to initiate the automatic switchover sequence. This interlock requires the capability for the retention of the safeguards protection logic actuation signal (SI signal) by latching relays located in the safeguards protection cabinets. The retention of this signal is required since plant emergency procedures will instruct the operator to reset the master relays for the safeguards protection logic actuation signal (SI signal) significantly in advance of the generation of the RWST low-low-level actuation signals. The output of these latching relays is retained such that when the two-of-four RWST low-low-level actuation signals are developed, the train A and train B automatic switchover sequence trip signals are generated.

The automatic switchover sequence trip signal is applied to all valves except 1-862A and 1-862B that are automatically repositioned. This ensures that the automatic switchover sequence cannot be unintentionally interrupted by the plant operator by manually repositioning the valve.

Provisions have been included in this interlock to permit on-line testing of the automatic switchover sequence without affecting normal plant operation. The testing provisions have been developed to ensure that an open path from the RWST to the charging/safety injection pump suction does not exist at any time during the testing procedure. Testing addressed in this interlock is restricted to valve sequence testing and does not include the testing of RWST instrumentation and safeguards protection logic. Test buttons are provided to simulate both the safeguards protection logic actuation signal (SI signal) to the latching relay and the two-of-four RWST low-level actuation signal. Each train is tested individually.

The following additional features are included in this interlock to prevent the unintentional remote manual operation of certain valves by the operator:

1. The remote manual opening of a low-head safety injection pump miniflow isolation valve requires that the sump isolation valve in the same train be fully closed. This prevents the inadvertent pumping of sump water to the refueling water storage tank after an accident.

2. The remote manual opening of a sump isolation valve requires that one of the low-head safety injection pump miniflow isolation valves in the same train be fully closed. Again, this is to prevent inadvertent pumping of sump water to the refueling water storage tank after an accident.
3. A RWST-to-LHSI pump isolation valve cannot be manually opened unless the sump isolation valve is fully closed. This avoids the condition where an LHSI pump would continue to take suction from the refueling water storage tank after the switchover to recirculation had been completed. Preferential suction from the refueling water storage tank would drain the tank completely, which is undesirable.

7.3.2.11 Inside and Outside Recirculation Spray Pump Start Function (Unit 2 only)

The ESF actuation system provides the logic for the automatic start of the Inside Recirculation Spray (IRS) and Outside Recirculation Spray (ORS) pumps at appropriate times after the occurrence of a Containment Depressurization Actuation (CDA). The automatic start sequence is initiated when actuation signals are generated by a coincidence of the CDA Containment Pressure High-High, two-of-four safeguards logic and the Refueling Water Storage Tank (RWST) Level-Low, two-of-three safeguards logic. See Reference Drawings 28 and 29.

The Containment Pressure High-High (CDA) portion of the RS pump start logic is described in Section 7.3.1.3.2 and Reference Drawings 5, 6, and 7. Actual pump start is not initiated until both the CDA and RWST Level-Low two-of-three logic is satisfied. This design ensures that the pumps will not start until enough water has been added to containment so that sufficient water level is available to meet sump strainer submergence and pump suction operating requirements.

The RWST Level-Low portion of the RS pump start logic is described in Reference Drawings 28 and 29. The analog inputs to this logic are the same RWST level signals used in the Automatic Recirculation Mode Transfer (RMT) function described in Section 7.3.2.10. The RMT function uses bi-stables that actuate when RWST level reaches a Low-Low setpoint. Separate bi-stables installed in three of the analog loops provide the RWST Level-Low signals for the RS pump start logic. Each of these three RWST Level-Low channels bi-stables provide an RWST Low level signal to both the Train A and Train B Solid State Protection Systems (SSPS). Thus, when two-of-three RWST Level-Low channel bi-stables generate an RWST Low level actuation signal, it is developed in both safeguards protection cabinets. Each of the three RWST Level-Low channel bi-stables is aligned to one of three RWST level channels. Each level channel is assigned to a separate vital instrument bus.

The ORS pump control circuits are configured so that the ORS pumps receive an immediate start signal once the Containment Pressure High-High AND RWST Level-Low coincidence logic is satisfied (Assuming that all electrical permissives are satisfied). The IRS pump control circuits are configured so that the pumps start after a 120-second delay from the coincident actuation signal. This delay minimizes the impact on emergency diesel loading and allows for the ORS

system to fill its piping completely, deliver spray to the containment and reach a stable flow demand on the sump before the IRS pumps start. This method of starting the RS pumps ensures that a reliable mass of liquid is added to the containment to meet the sump strainer submergence requirements for the range of LOCA break sizes requiring the containment sump.

The Inside and Outside Recirculation Spray Pump Start Function is tested using the same methods and design features described in Section 7.3.2.1.5.1.

7.3 REFERENCES

1. J. B. Reid, *Process Instrumentation for Westinghouse Nuclear Steam Supply Systems*, WCAP-7913.
2. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations*, IEEE Std 279-1971.
3. D. N. Katz, *Solid State Logic Protection System Description*, WCAP-7672, June 1971.
4. J. Locante and E. G. Igne, *Environmental Testing of Engineered Safety Features Related Equipment (NSSS - Standard Scope)*, WCAP-7744, Volume I, August 1971.
5. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Standard: Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations*, IEEE Std 308-1969.
6. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Trial Use Standard: General Guide for Qualifying Class 1 Electrical Equipment for Nuclear Power Generating Stations*, IEEE Std 323-1971.
7. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Trial Use Guide for Type Tests of Continuous Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations*, IEEE Std 334-1971.
8. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Trial Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protective Systems*, IEEE Std 338-1971.
9. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Trial Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations*, IEEE Std 344-1971, dated August 11, 1971.
10. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations*, IEEE Std 317-1971.
11. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Standard Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations*, IEEE Std 336-1971.

12. Technical Report EE-0101, *Setpoint Bases Document Analytical Limits, Setpoints and Calculations for Technical Specifications Instrumentation at North Anna and Surry Power Stations*.

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.	11715-LSK-0-1A	Logic Diagram: Digital Symbols
2.	11715-LSK-0-1B	Logic Diagram: Analog Symbols
3.	11715-LSK-0-1C	Logic Diagram: Solenoids
4.	11715-LSK-0-03A	Logic Diagrams: General Notes
5.	11715-LSK-27-12A	Typical Loop Diagram for Each Channel Hi-Hi Containment Pressure Protection
6.	11715-LSK-27-12B	Hi-Hi Containment Pressure Protection and Indication, Unit 1
7.	11715-LSK-27-12C	Containment Depressurization Actuation and Reset, Train A
8.	11715-LSK-27-12D	Hi Containment Pressure Protection
9.	11715-LSK-27-12E	Intermediate Hi-Hi Containment Pressure Protection
10.	11715-LSK-27-12F	Containment Depressurization Actuation and Reset, Train B
11.	11715-LSK-28-5C	Safety Injection System, Actuated Devices
12.	11715-LSK-27-12G	Containment Depressurization Actuated Devices
13.	11715-LSK-5-13A	Logic Diagram: Motor Driven Steam Generator, Auxiliary Feedwater Pumps
14.	11715-LSK-5-8H	Feedwater Isolation Trip Valves
15.	11715-LSK-32-1B	Containment Isolation, Phase B, Actuation and Reset
16.	11715-LSK-32-1D	Normally Open Containment Isolation Trip Valves
17.	11715-LSK-32-1E	Containment Isolation Trip Valves, Train A
18.	11715-LSK-32-1F	Containment Isolation Trip Valves, Train B
19.	11715-LSK-5-13B	Turbine Driven, Steam Generator, Auxiliary Feedwater Pumps

	Drawing Number	Description
20.	11715-LSK-5-13C	Auxiliary Feedwater Control Valves
21.	11715-LSK-8-18A	Main Steam Isolation Trip Valve
22.	11715-LSK-8-18D	Main Steam Isolation Bypass Valve
23.	11715-LSK-1-2E	Logic Diagram: Turbine Trips, Sheet 5
24.	11715-LSK-5-12A	Logic Diagram: Steam Generator Blowdown Trip Valves
25.	11715-LSK-22-12Z	Logic Diagram: Undervoltage Protection, Unit 1
26.	11715-LSK-28-5A	Logic Diagram: Safety Injection System
27.	11715-LSK-32-1A	Logic Diagram: Phase A, Containment Isolation Actuation
28.	11715-LSK-27-1A	Logic Diagram: Recirculation Spray Sub Systems
29.	11715-LSK-27-1B	Logic Diagram: Recirculation Spray Sub Systems

Table 7.3-1

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

In addition to the interlocks in the Technical Specifications,
the following interlocks are installed.

Designation	Input	Function Performed
P-4	Reactor trip	<p>Actuates turbine trip</p> <p>Closes main feedwater valves on T_{avg} below setpoint</p> <p>Prevents opening of main feedwater valves that were closed by safety injection or high steam generator water level</p> <p>Allows reset of safety injection actuation</p>
	Reactor not tripped	<p>Defeats reset of the safety injection actuation signal</p>
P-14	2/3 steam generator water level above setpoint on any steam generator	<p>Closes all feedwater control valves</p> <p>Trips all main feedwater pumps and closes the feed line isolation valves</p> <p>Actuates turbine trip</p>

Table 7.3-2
ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

Functional Unit	Channels to Trip	Minimum Channels Operable
1. Safety Injection		
a. Manual Initiation	1	2
b. Automatic Actuation	1	2
c. Containment Pressure—High	2	2
d. Pressurizer Pressure—Low-Low	2	2
e. Differential Pressure Between Steam Lines—High	2/steam line twice and 1/3 steam lines	2/steam line
f. Steam Flow in Two Steam Lines—High	1/steam line any 2 steam lines	1/steam line
Coincident with either T_{avg} —Low-Low	1 T_{avg} any 2 loops	1 T_{avg} any 2 loops
or, coincident with Steam Line Pressure—Low	1 pressure any 2 lines	1 pressure any 2 lines
2. Containment Spray		
a. Manual	1 set	2 sets
b. Automatic Actuation Logic	1	2
c. Containment Pressure—High-High	2	3
d. (Unit 2 only) Refueling Water Storage Tank (RWST) Level—Low Coincident with Containment Pressure High-High	2	2
3. Containment Isolation		
a. Phase “A” Isolation		
1) Manual	1	2
2) From Safety Injection Automatic Actuation Logic	1	2
b. Phase “B” Isolation		
1) Manual	1 set	2
2) Automatic Actuation Logic	1	2
3) Containment Pressure—High-High	2	3

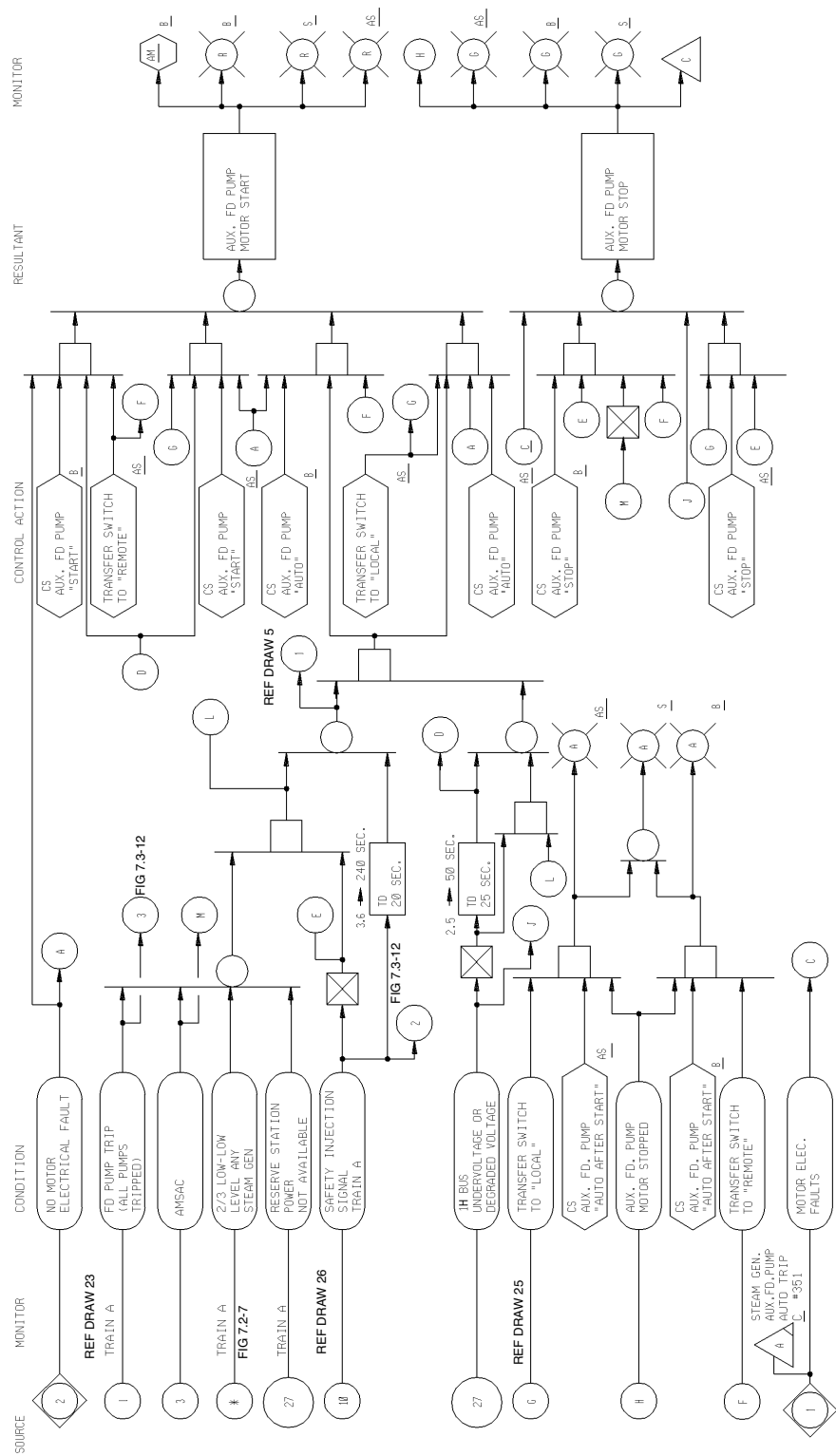
Table 7.3-2 (continued)
ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

Functional Unit	Channels to Trip	Minimum Channels Operable
4. Steam Line Isolation		
a. Manual	1/steam line	2/steam line
b. Automatic Actuation Logic	1	2
c. Containment Pressure—Intermediate High-High	2	2
d. Steam Flow in Two Steam Lines—High	1/steam line any 2 steam lines	1/steam line
Coincident with either T _{avg} —Low-Low	1 T _{avg} any 2 loops	1 T _{avg} any 2 loops
or, coincident with Steam Line Pressure—Low	1 pressure any 2 lines	1 pressure any 2 lines
5. Turbine Trip & Feedwater Isolation		
a. Steam Generator Water Level—High-High	2/loop	2/loop
b. Automatic Actuation Logic and Actuation Relays	1	2
c. Safety Injection (SI)	See #1 above (All SI initiating functions and requirements)	
6. Auxiliary Feedwater Pump Start		
a. Manual Initiation	1	2
b. Automatic Actuation Logic	1	2
c. Steam Generator Water Level—Low-Low	2/steam generator	2/steam generator
d. Safety Injection (SI)	See #1 above (All SI initiating functions and requirements)	
e. Station Blackout	1/bus on 2 busses	1/bus on 2 busses
f. Main Feed Pump Trip	1/pump	1/pump
7. Switchover to Containment Sump		
a. Automatic Actuation Logic and Actuation Relays	1	2
b. Refueling Water Storage Tank (RWST) Level—Low-Low	2	3

Table 7.3-2 (continued)
ENGINEERED SAFETY FEATURE ACTUATION SYSTEM INSTRUMENTATION

Functional Unit	Channels to Trip	Minimum Channels Operable
8. Engineered Safety Feature Actuation System Interlocks		
a. Pressurizer Pressure, P-11	2	2
b. Low-Low T_{avg} , P-12	2	2
c. Reactor Trip, P-4	1	2
9. Loss of Power		
a. 4.16 Kv Emergency Bus Undervoltage (Loss of Voltage)	2/bus	2/bus
b. 4.16 Kv Emergency Bus Undervoltage (Grid Degraded Voltage)	2/bus	2/bus

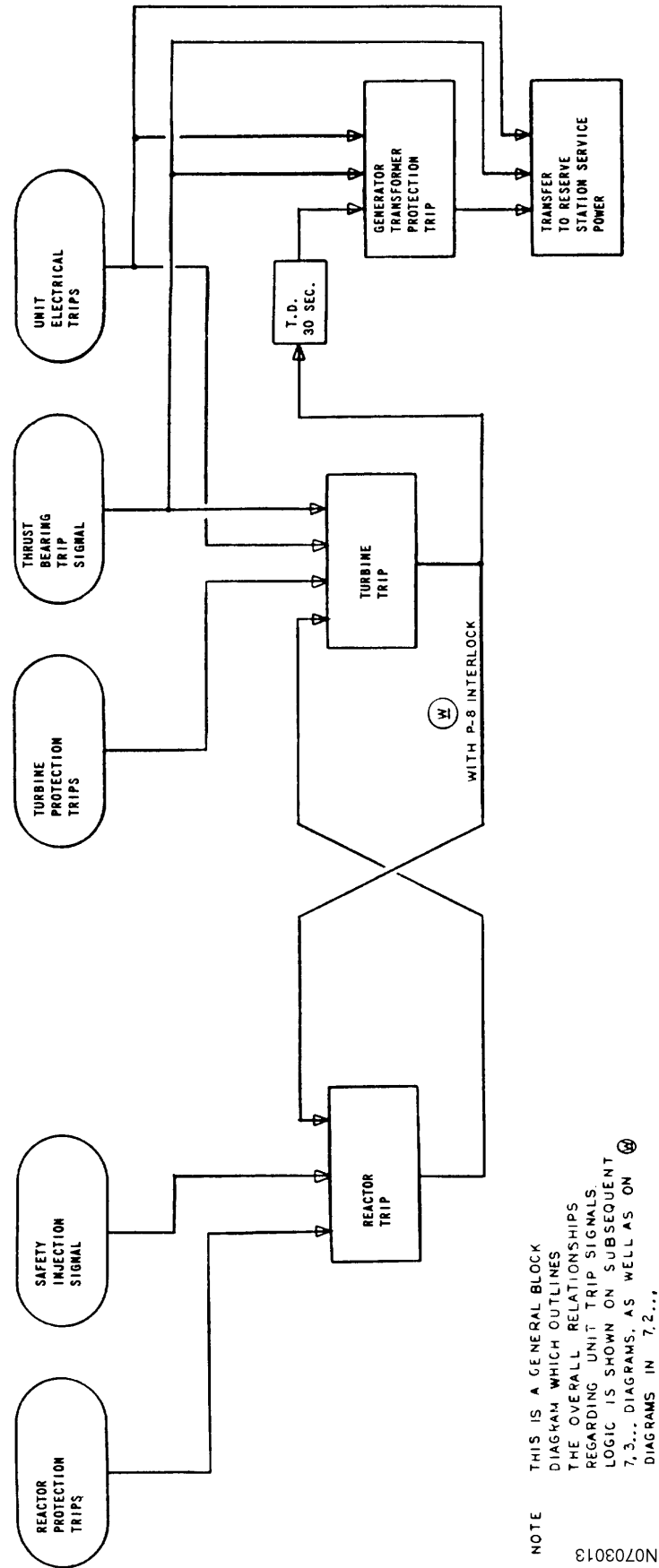
Figure 7.3-1
LOGIC DIAGRAM MOTOR DRIVEN STEAM GENERATOR AUXILIARY FEED PUMPS



- NOTES:
1. LOGIC FOR FW-P-3A SHOWN. LOGIC FOR FW-P-3B SIMILAR.
 2. LOCATION SYMBOL "AS" REFERS TO AUXILIARY SHUTDOWN PANEL.
 3. OTHER POSITION OF TRANSFER SWITCH IS "AS".
 4. TRANSFER SWITCH CHANGED FROM "LOCAL" TO "REMOTE" CONTROL REMAINS LOCAL UNTIL LOCKOUT RELAY AT SWGR. RESET.
 5. LIGHTS AT "AS" ONLY ILLUMINATE WITH TRANSFER SWITCH IN "LOCAL".

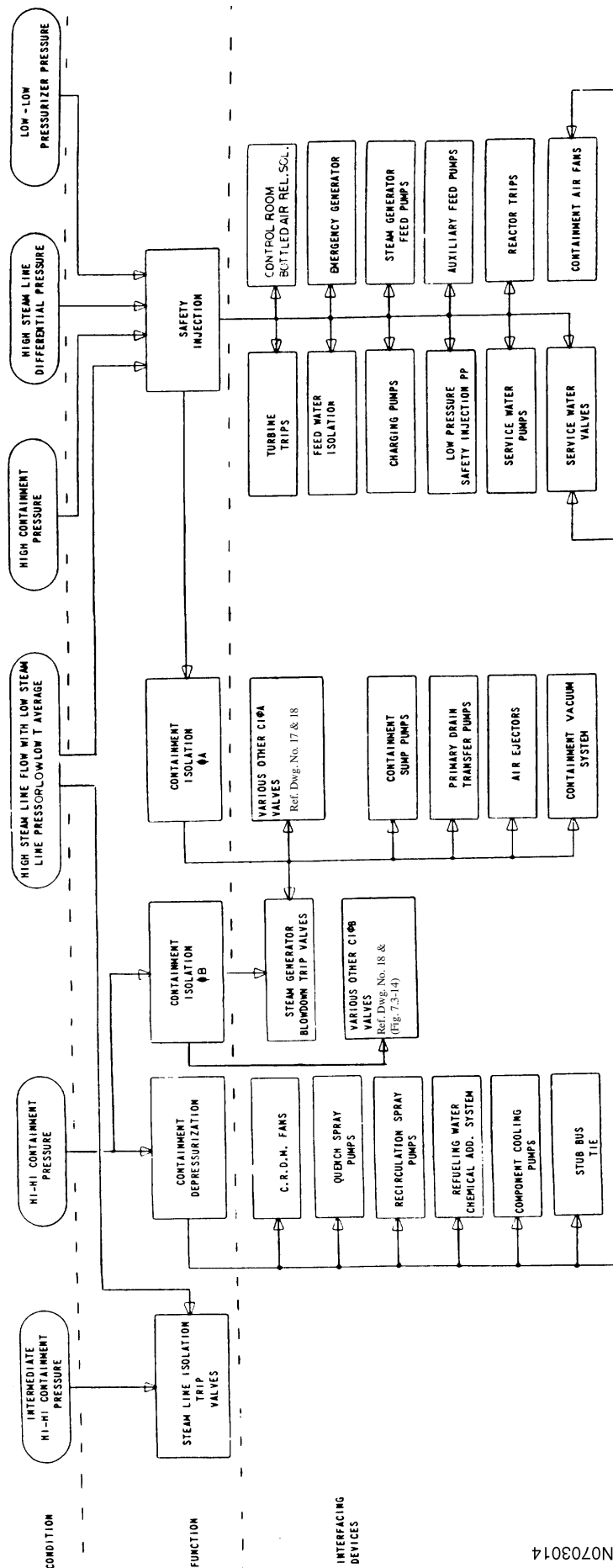
NO703001

Figure 7.3-2
UNIT TRIP SIGNAL INTERFACES



N0703013

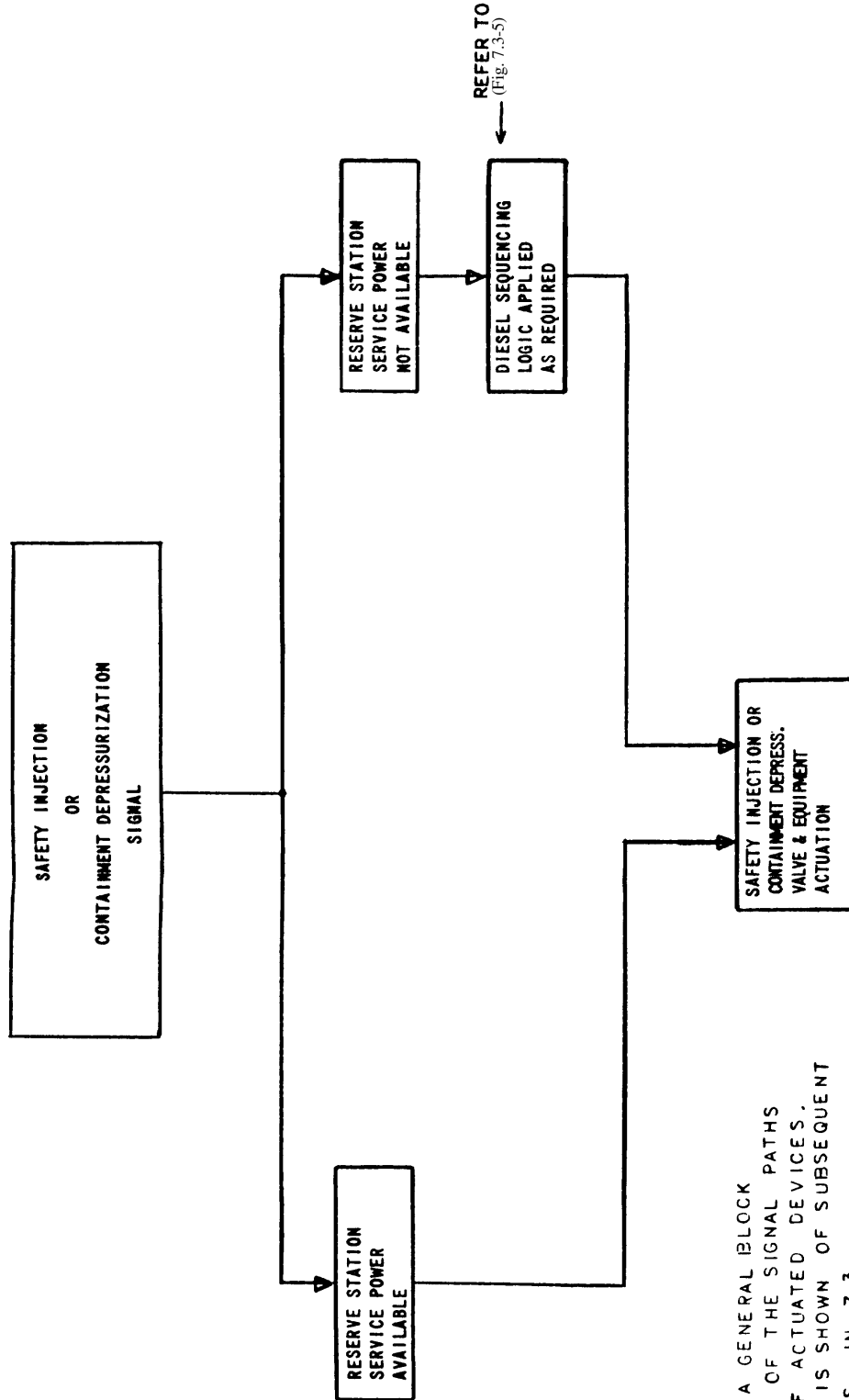
Figure 7.3-3
ENGINEERED SAFETY FEATURES SIGNAL INTERFACES



NOTES: 1. THIS IS A GENERAL BLOCK DIAGRAM WHICH OUTLINES THOSE SYSTEM DEVICES WHICH INTERFACE WITH SAFETY FEATURES SIGNALS.

0703014

Figure 7.3-4
SIGNAL PATHS TO ESF ACTUATED DEVICES

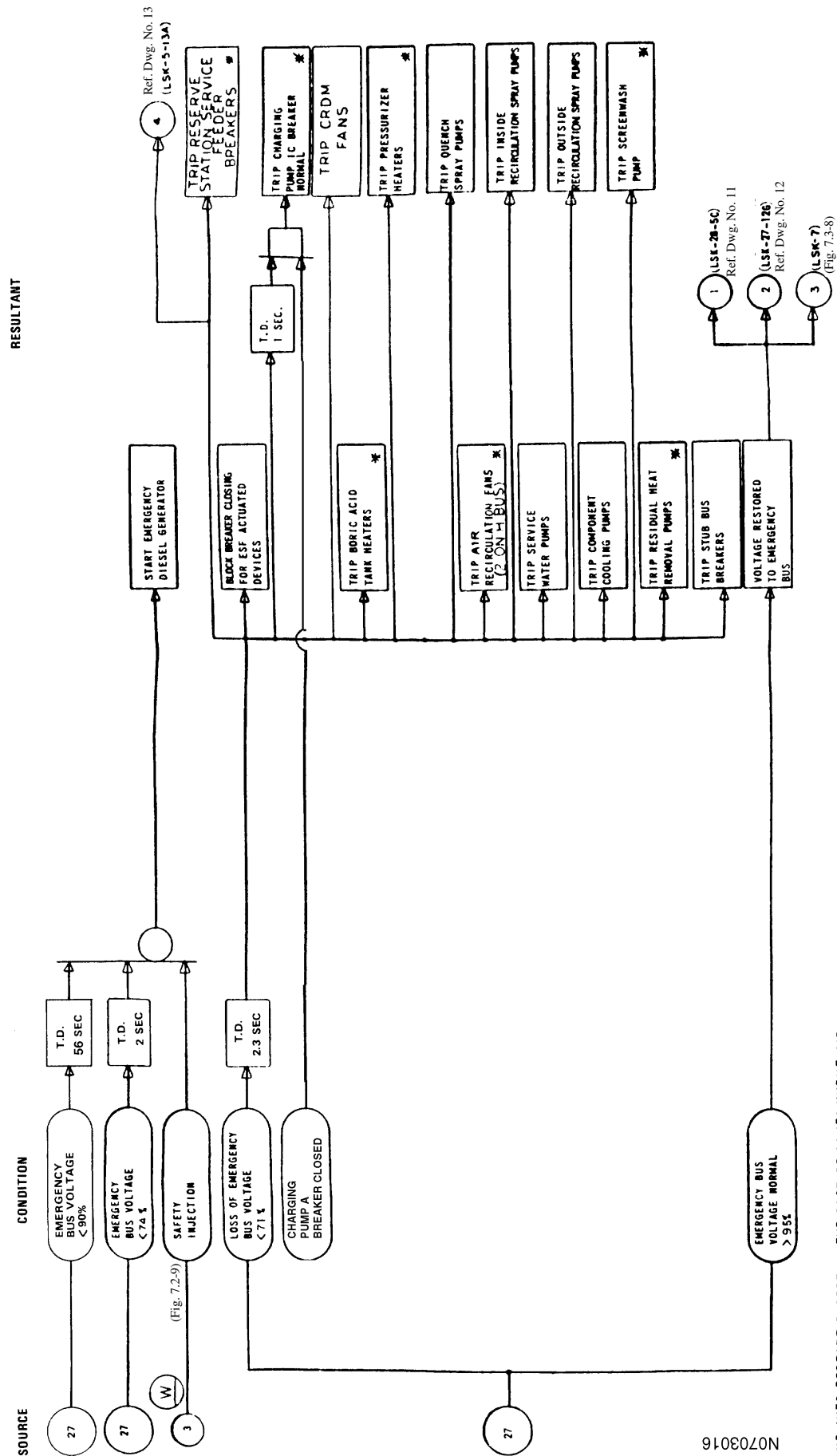


NOTE THIS IS A GENERAL BLOCK
DIAGRAM OF THE SIGNAL PATHS
FOR ESF ACTUATED DEVICES.
LOGIC IS SHOWN OF SUBSEQUENT
DIAGRAMS IN 7.3.

NOTE

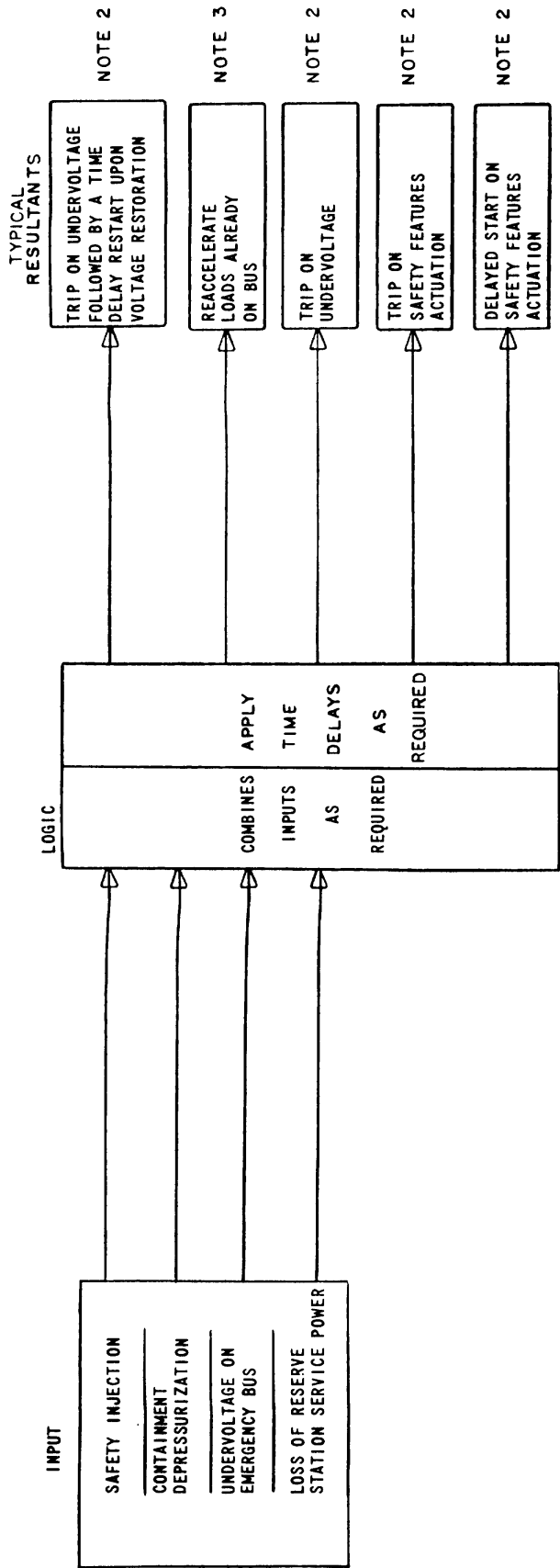
N0703015

Figure 7.3-5
LOSS AND RESTORATION OF EMERGENCY BUS



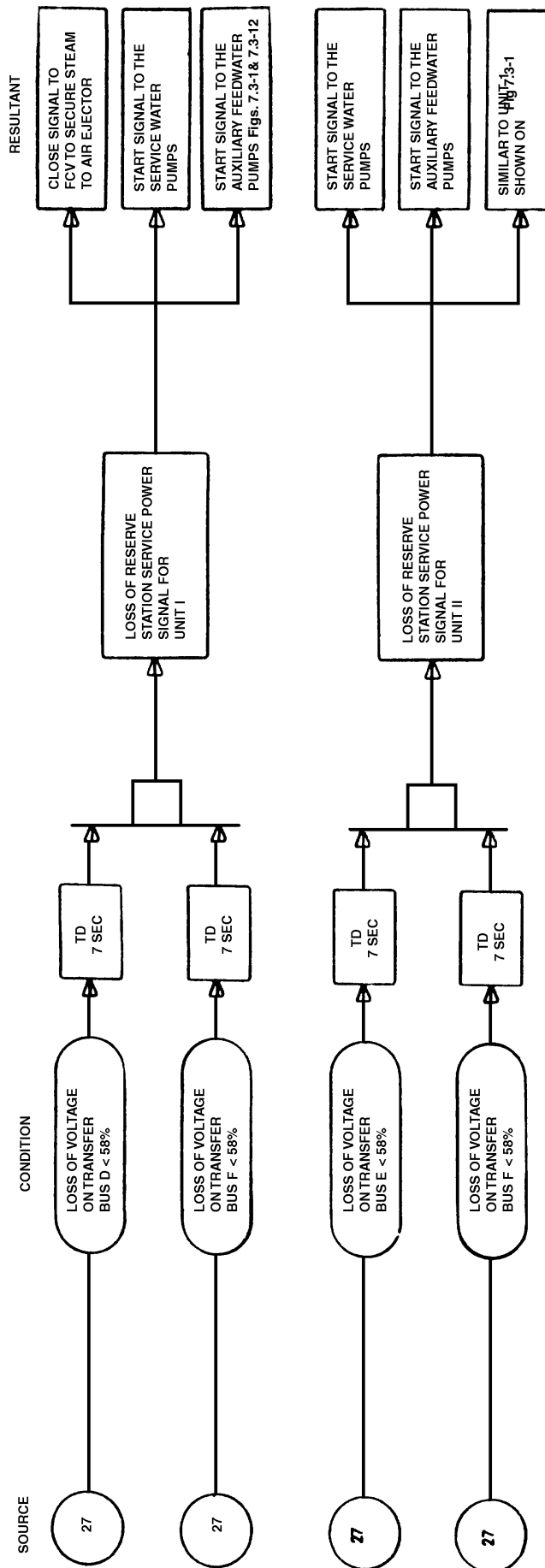
NO AUTO RESTART EXCEPT IN THE CASE OF CONTAINMENT AIR RECIRCULATION FANS—ONLY ONE OF THE TWO FANS ON THE H BUS HAS AUTO RESTART CAPABILITIES

Figure 7.3-6
DIESEL LOAD AND SEQUENCING CONDITIONING CONCEPT



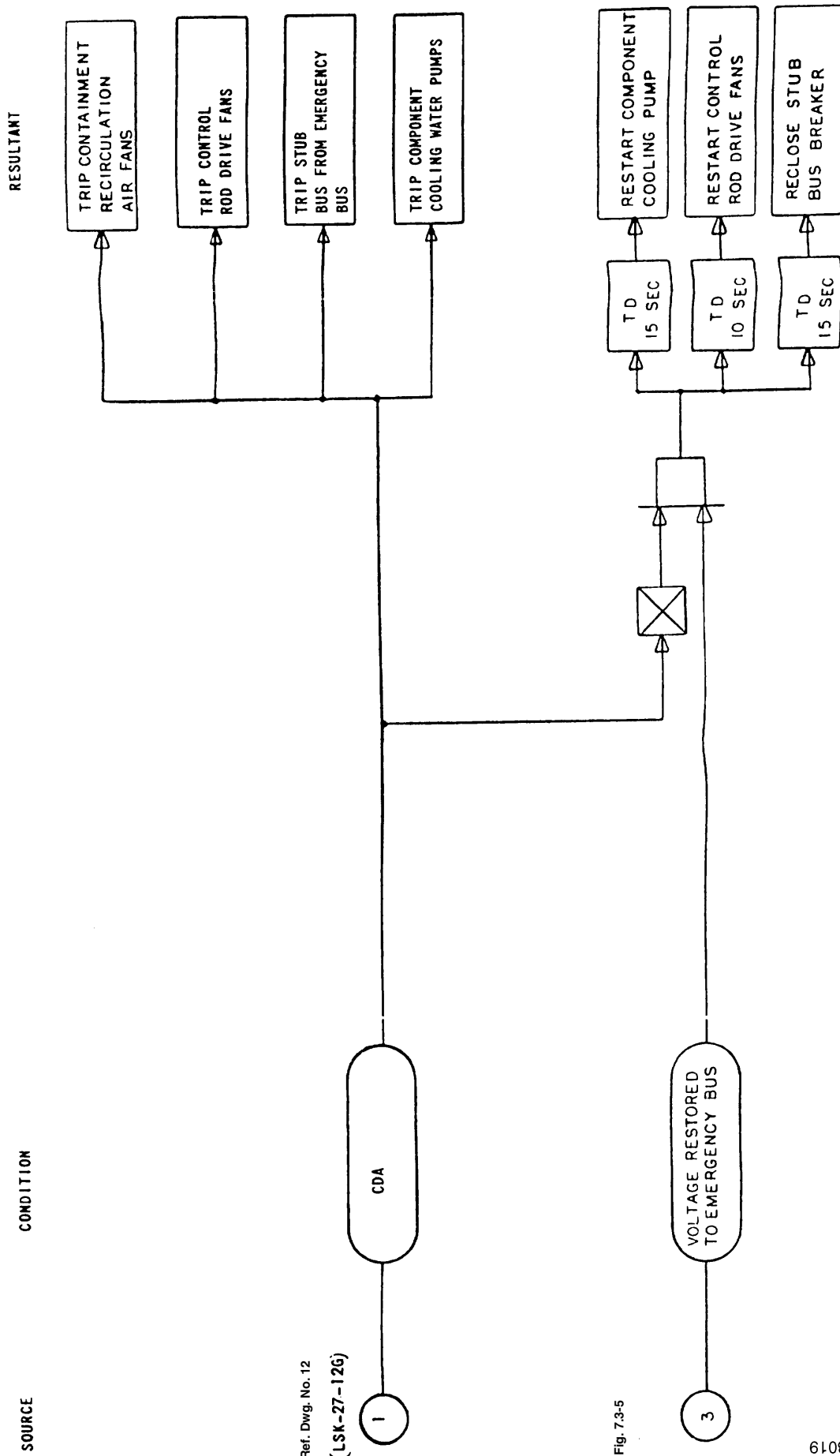
- NOTES: 1, THIS DRAWING IS A GENERAL BLOCK DIAGRAM. LOGIC IS SHOWN ON SUBSEQUENT DIAGRAMS, IN 7.3,
2. THE RESULTANTS SHOWN REFER TO TYPICAL OPERATIONS OF THE BREAKERS WHICH CONNECT SIGNIFICANT LOADS TO THE EMERGENCY BUS.
- 3 THIS RESULTANT REFERS TO EMERGENCY BUS LOADS WHICH WILL NOT REQUIRE ANY DELIBERATE BREAKER OPERATIONS FOR ANY COMBINATION OF THE INPUTS SHOWN.
- DIESEL LOAD AND SEQUENCE CONDITIONING CONCEPT

Figure 7.3-7
RESERVE STATION SERVICE-UNDERVOLTAGE



N0703018

Figure 7.3-8
REMOVAL OF UNNECESSARY LOAD FROM EMERGENCY BUS DURING CONTAINMENT DEPRESSURIZATION

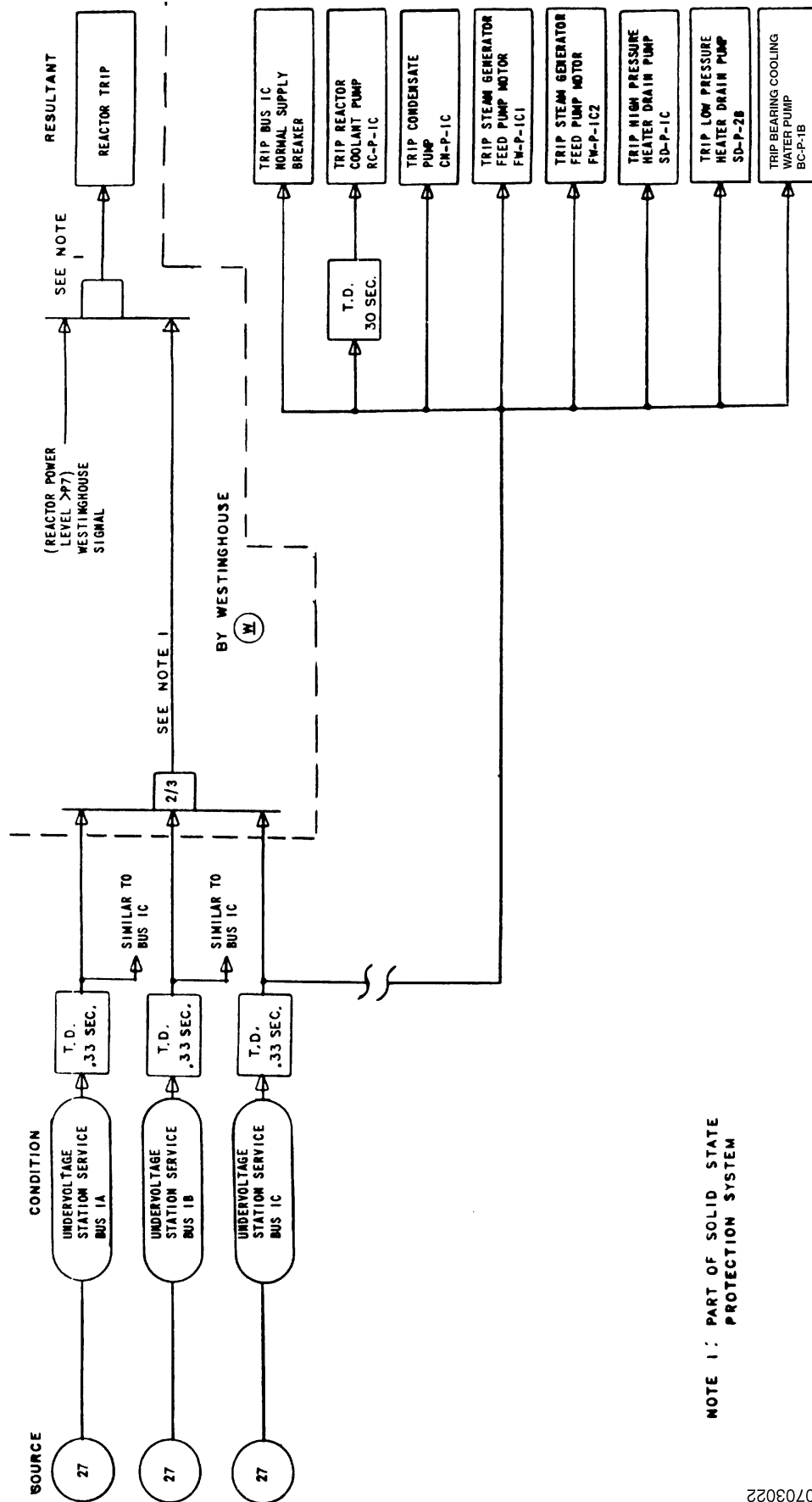


Ref. Dwg. No. 12
(LSK-27-126)

Fig. 7.3-5

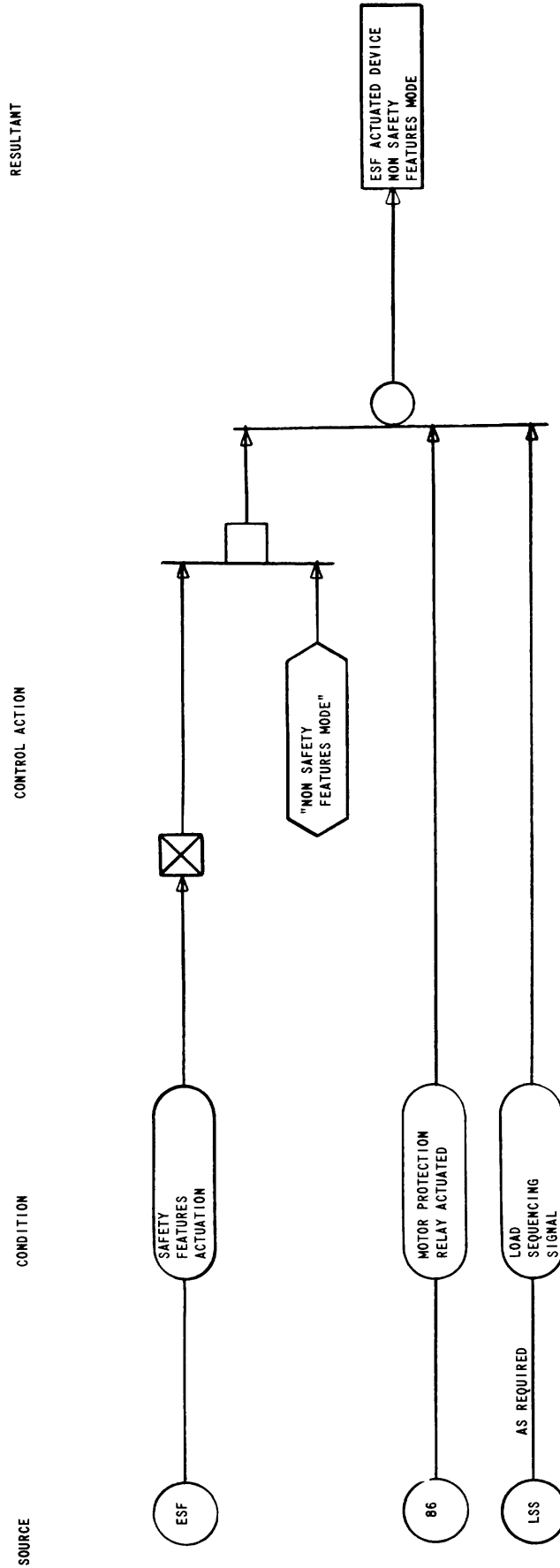
N0703010

Figure 7.3-9
STATION SERVICE-UNDERVOLTAGE



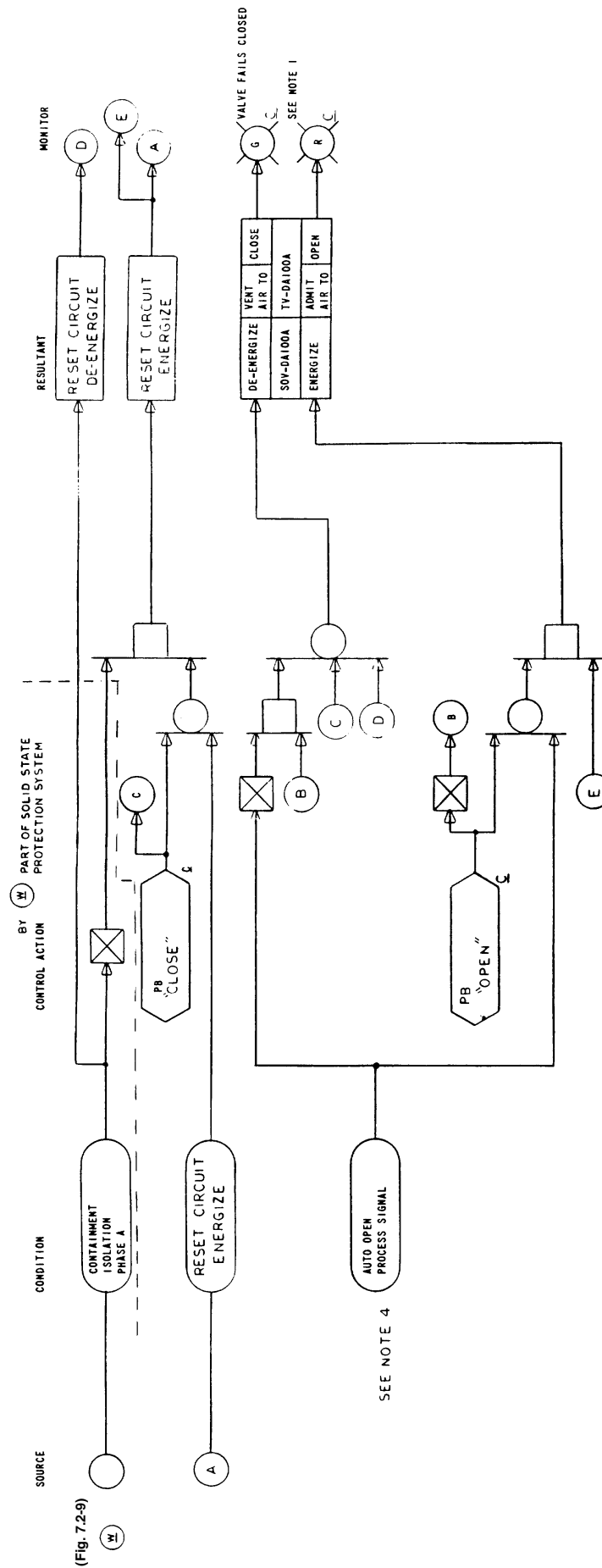
N0703022

Figure 7.3-10
ENGINEERED SAFETY FEATURES BLOCKING LOGIC



NOTE THIS IS A TYPICAL LOGIC
AS IMPLEMENTED ON ALL
ENGINEERED SAFETY
FEATURES DEVICES.

Figure 7.3-11
NORMALLY CLOSED CONTAINMENT ISOLATION TRIP VALVES



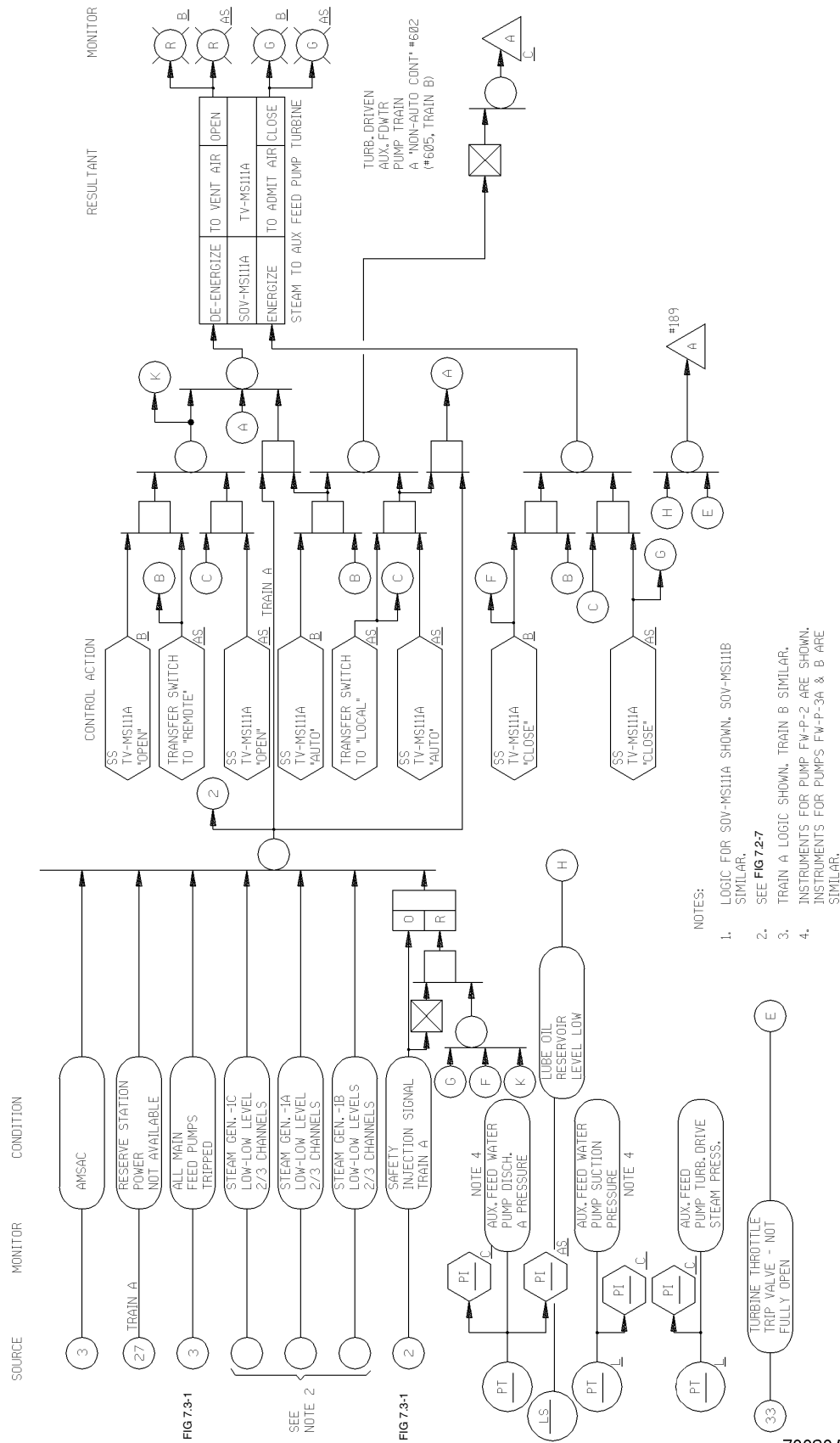
NOTES:

1. Refer To LSK-32-IE and LSK-32-IF (Ref. No. 17 and 18) for normally closed valves.
2. THERE ARE NO CONTAINMENT ISOLATION PHASE B NORMALLY CLOSED VALVES.
3. PB₃ ARE MOMENTARY INPUTS
4. THIS SIGNAL IS THE RESULT OF A PUMP START IN THE REACTOR CONTAINMENT SUMP SYSTEM.
5. TRAIN A SHOWN, TRAIN B SIMILAR

(LSK-32-IC)

N0703026

Figure 7.3-12
LOGIC DIAGRAM TURBINE DRIVEN-STEAM GENERATOR AUXILIARY FEED PUMP



N0703002

Figure 7.3-13
LOGIC DIAGRAM NORMALLY OPEN CONTAINMENT ISOLATION VALVES

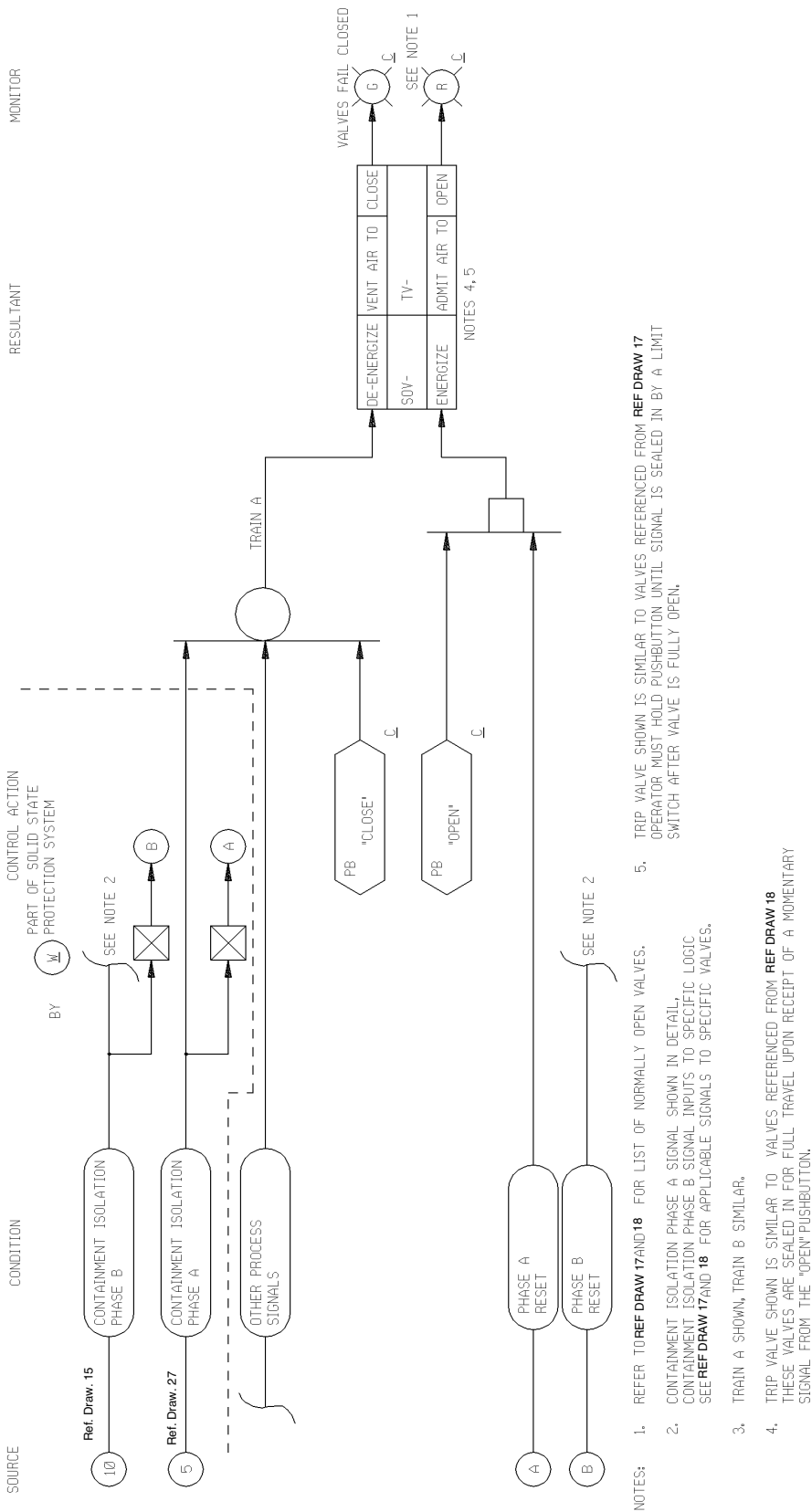
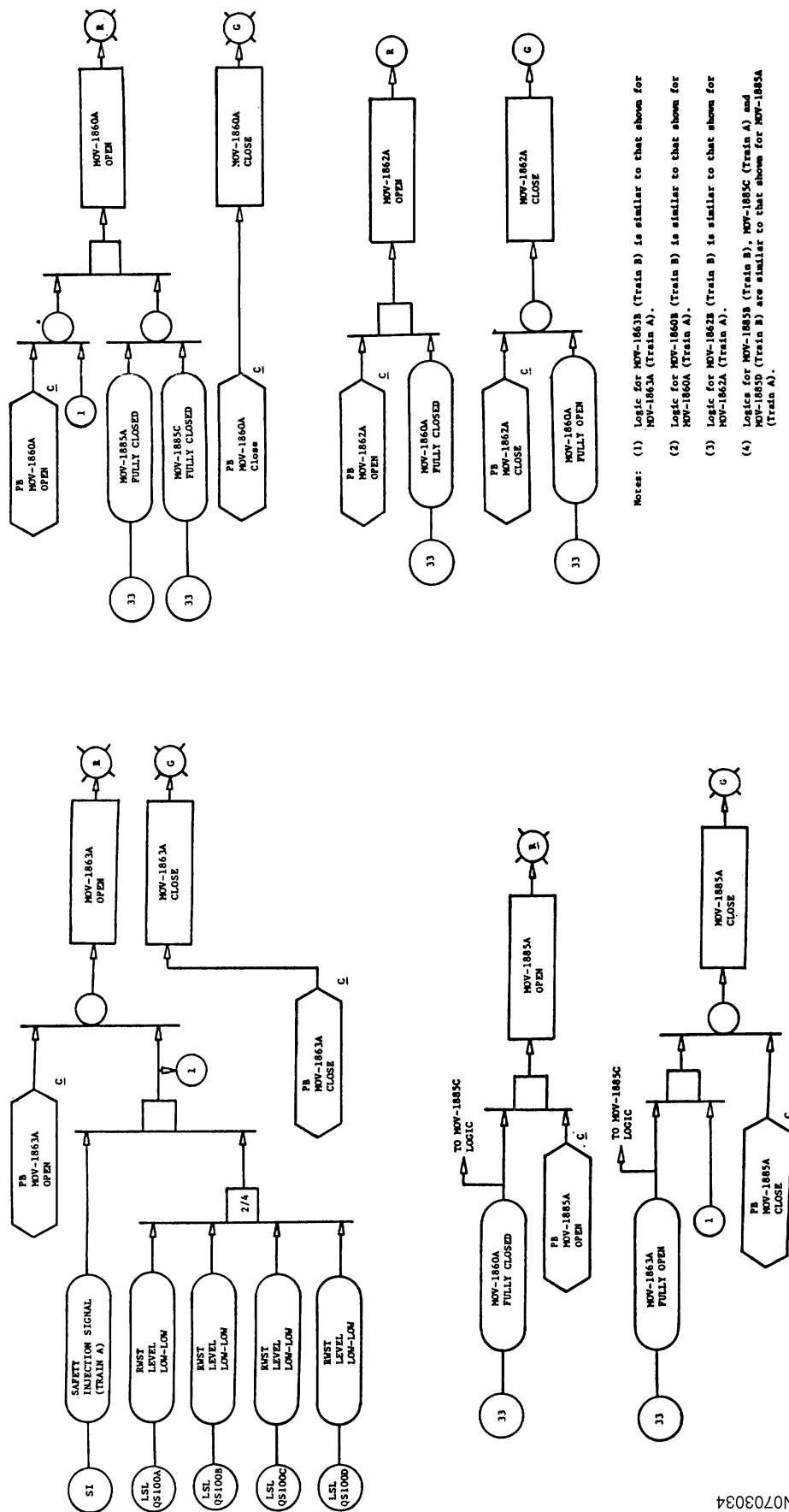


Figure 7.3-14
ECCS LOGIC/AUTOMATIC SWITCHOVER FROM
INJECTION PHASE TO RECIRCULATION PHASE



Notes: (1) Logic for MW-1863B (Train B) is similar to that shown for MW-1862A (Train A).

(2) Logic for MW-1860B (Train B) is similar to that shown for MW-1860A (Train A).

(3) Logic for MW-1862B (Train B) is similar to that shown for MW-1862A (Train A).

(4) Logics for MW-1859B (Train B), MW-1859C (Train A) and MW-1859D (Train B) are similar to that shown for MW-1859A (Train A).

N0703034

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

Electrical schematic diagrams for systems required for shutdown and their supporting systems were included in reports NA-TR-1001 and NA-TR-1002, *Safety Related Electrical Schematics*, dated May 10, 1973, which were submitted to the Atomic Energy Commission (AEC) on May 18, 1973, as separate documents.

The information necessary for safe shutdown is available from instrumentation channels that are associated with the major systems in both the primary and secondary loops of the nuclear steam supply system. These channels normally service a variety of operational functions, including start-up and shutdown as well as protective functions. There are no systems whose only function is safe shutdown. Prescribed procedures for placing and maintaining the plant in a safe condition can be instituted by appropriate alignment of selected nuclear steam supply systems. The discussion of these systems, together with the applicable codes, criteria, and guidelines, is found in other sections of this FSAR. In addition, the implementation of shutdown functions associated with the engineered safety features that are used under postulated limiting fault situations is discussed in Chapter 6 and Section 7.3.

7.4.1 Description

The operator actions, instrumentation, and control features that maintain safe shutdown of the reactor as discussed in this section are the minimum number under nonaccident conditions. These features will permit the necessary operations that will:

1. Prevent the reactor from achieving criticality in violation of the Technical Specifications.
2. Provide an adequate heat sink such that design and safety limits are not exceeded.

The plant is normally controlled from the main control room, which contains all necessary instrumentation and controls to achieve and maintain a safe-shutdown condition. In the unlikely event that the main control room needs to be evacuated, an auxiliary shutdown panel is provided.

The conditions listed below include the design basis for the auxiliary shutdown panel. The identification is given for the control and monitoring features (Section 7.4.1.2) necessary for maintaining a hot shutdown. The equipment and services and approximate time required after an incident that requires a hot shutdown are listed in Section 7.4.1.3; the equipment and service available for a cold shutdown are identified in Section 7.4.1.4.

7.4.1.1 Design Considerations for the Auxiliary Shutdown Panel

1. In the event the control room must be evacuated, it is assumed the control room is inaccessible for at least a period of 10 hours to 1 week.
2. Although it is assumed that the operator trips the reactor before leaving the control room, a turbine trip can be accomplished at the turbine as well as in the control room, and a reactor trip can be accomplished at the reactor trip switchgear as well as in the control room.

3. In the event the control room is inaccessible, the operator must bring the plant to the hot standby condition.
4. It is assumed that loss of external power may occur during evacuation.
5. A sound-powered telephone network exists between the auxiliary shutdown panel and the following areas in the plant:
 - a. Auxiliary feed pump area.
 - b. Normal and emergency switchgear rooms.
 - c. Diesel generators.
 - d. Emergency boration line.
 - e. Steam dump valves.
6. For safety-related circuits, electrical as well as physical isolation exists between the main control board and auxiliary shutdown panel.
7. The diesel generator will have both local-start and auto-start capability.
8. No additional accident conditions are assumed to occur simultaneously with control room inaccessibility.
9. No hardware failures are assumed to occur simultaneously with control room inaccessibility; therefore, all automatic systems continue functioning.
10. Fire in a section of the control board is considered credible. However, with the design of the control board (separation, limited combustibles), control room evacuation should not be required following a fire in the main control board.
11. A source of feedwater will be available for in excess of 1 week. For the first 8 hours, auxiliary feedwater pumps take suction from the 110,000-gallons condensate storage tank. After 8 hours, the auxiliary feedwater pumps can take suction from either the service water system or fire main.
12. Pressurizer heater on-off control with selector switch is provided for two backup heater groups. The heater groups are connected to separate buses, such that each is connected to separate diesels in the event of loss of outside power. The control is grouped with the charging flow controls and duplicates functions available in the control room.
13. The condenser steam dump and atmospheric relief valves are automatically controlled. Manual control is provided locally as well as in the control room for the atmospheric relief valves. Steam dump to the condenser is blocked on high condenser pressure.
14. It is assumed that one operator will be at the auxiliary shutdown panel, using detailed operating instructions in conjunction with instrumentation and controls on the panel. He will

be communicating by sound-powered telephone with other personnel to direct necessary local-manual action.

15. Electric motors can be started or stopped at the switchgear.
16. Motor-operated valves can be operated manually and drivers can be disengaged or locked out if required.
17. The following processes will be available:
 - a. Residual heat removal (reactor coolant system natural circulation).
 - b. Boration capability.
 - c. Reactor coolant sampling.
 - d. Reactor coolant inventory control.
 - e. Instrument air.
18. The following items operate during normal plant operation and will continue to operate from the emergency diesel-generator bus should there be a loss of reserve station service power:
 - a. Service water pumps.
 - b. Component cooling water pumps.
 - c. Reactor containment fan cooler units.
19. For equipment having motor controls outside the control room on the auxiliary shutdown panel (which duplicate the functions inside the control room), the controls will be provided with a selector switch that transfers the control of the switchgear from the control room to a selected local station. Placing the local selector switch in the local operating position will give an annunciating alarm in the control room and will turn off the motor control position lights on the control room panel. (Refer to Figures 7.4-1 and 7.4-2.)
20. It is noted that the instrumentation and controls listed in Section 7.4.1.2, which are critical to achieving and maintaining a safe shutdown, are available in the event an evacuation of the control room is required. These controls and instrumentation channels, together with the equipment and services identified in the following sections (7.4.1.3 and 7.4.1.4), which are available for both hot and cold shutdown, identify the potential capability for cold shutdown of the reactor subsequent to a control room evacuation through the use of suitable procedures. Therefore, the applicable requirements of General Design Criterion 19 (1971 criteria) are met.

7.4.1.2 Auxiliary Shutdown Instrumentation

Should it become necessary to abandon the control room, the plant can be safely brought to and maintained in the hot-shutdown condition from the auxiliary shutdown control panels. This capability, including a list of instruments and controls, is fully described in Section 7.7.1.13.1.

7.4.1.3 Equipment and Services and Approximate Time Required After Incident that Requires Hot Shutdown

1. Auxiliary feedwater pumps—required if main feedwater pumps are not operating. For blackout condition the auxiliary feedwater pumps start automatically within 1 minute. (See Chapter 10 for a discussion of pumps.)
2. Reactor containment fan cooler units—within 15 minutes. (See Chapter 9 for a discussion of fan coolers.)
3. Diesel generators—Initial loads begin in 10 seconds. (See Chapter 8 for a discussion of diesels.)
4. Lighting in the areas of plant required during this condition—immediately. (See Chapter 9 for a discussion of lighting.)
5. Pressurizer heaters—within 8 hours. (See Chapter 5 for a discussion of heaters.)
6. Communication network to be available immediately.

7.4.1.4 Equipment and Systems Available for Cold Shutdown

1. Reactor coolant pump. (See Chapter 5.)
2. Auxiliary feedwater pumps. (See Chapter 10.)
3. Boric acid transfer pump. (See Chapter 9.)
4. Charging pumps. (See Chapter 9.)
5. Service water pumps. (See Chapter 9.)
6. Containment fans. (See Chapter 9.)
7. Control room ventilation. (See Chapter 9.)
8. Component cooling pumps. (See Chapter 9.)
9. Residual heat removal pumps. (See Chapter 5.)
10. Certain motor control center and switchgear sections.
11. Controlled steam release and feedwater supply. (See Section 7.7 and Chapter 10.)
12. Boration capability. (See Chapter 9.)
13. Nuclear instrumentation system (source range and intermediate range). (See Sections 7.2 and 7.7.)
14. Reactor coolant inventory control (charging and letdown). (See Chapter 9.)
15. Pressurizer pressure control including opening control for pressurizer relief valves (heaters and spray). (See Chapter 5.)

The reactor plant design does not preclude attaining the cold-shutdown condition from outside the control room. An assessment of plant conditions can be made on a long-term basis (a week or more) to establish procedures for bringing the plant to cold shutdown. During such time the plant could be safely maintained at hot-shutdown condition. Detailed procedures to be followed in effecting cold shutdown from outside the control room are best determined by plant personnel at the time it is decided to go to cold shutdown.

7.4.2 Analysis

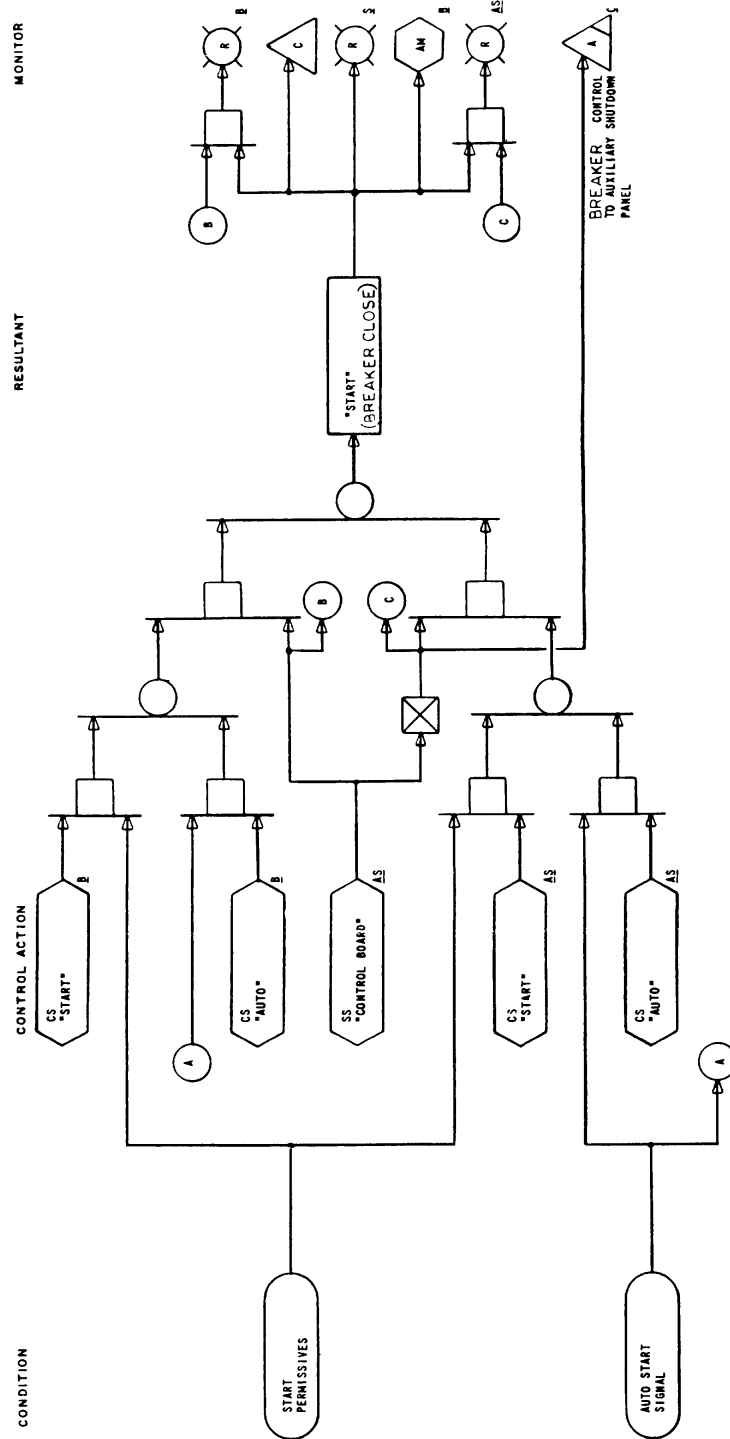
Hot shutdown is a stable plant condition, reached following a plant shutdown. The hot-shutdown condition can be maintained safely for an extended period of time. In the unlikely event that access to the control room is restricted, the plant can be safely kept at hot shutdown until the control room can be re-entered.

The evaluation of the ability to maintain a safe shutdown has included a consideration of the accident consequences that might jeopardize safe-shutdown conditions. The accident consequences that are germane are those that would tend to degrade the capabilities for boration, adequate supply for auxiliary feedwater, and residual heat removal. The results of the accident analyses are presented in Chapter 15. Of these the following produce the most severe consequences that are pertinent:

1. Uncontrolled boron dilution.
2. Loss of normal feedwater.
3. Loss of offsite ac power to the station auxiliaries (station blackout).

It is shown by these analyses that safety is not adversely affected by these accidents, with the associated assumptions being that the instrumentation and controls indicated in Section 7.4.1 are available to control and/or monitor shutdown. These available systems will allow the maintenance of hot shutdown, even under the accident conditions listed above, which would tend toward a return to criticality or a loss of heat sink.

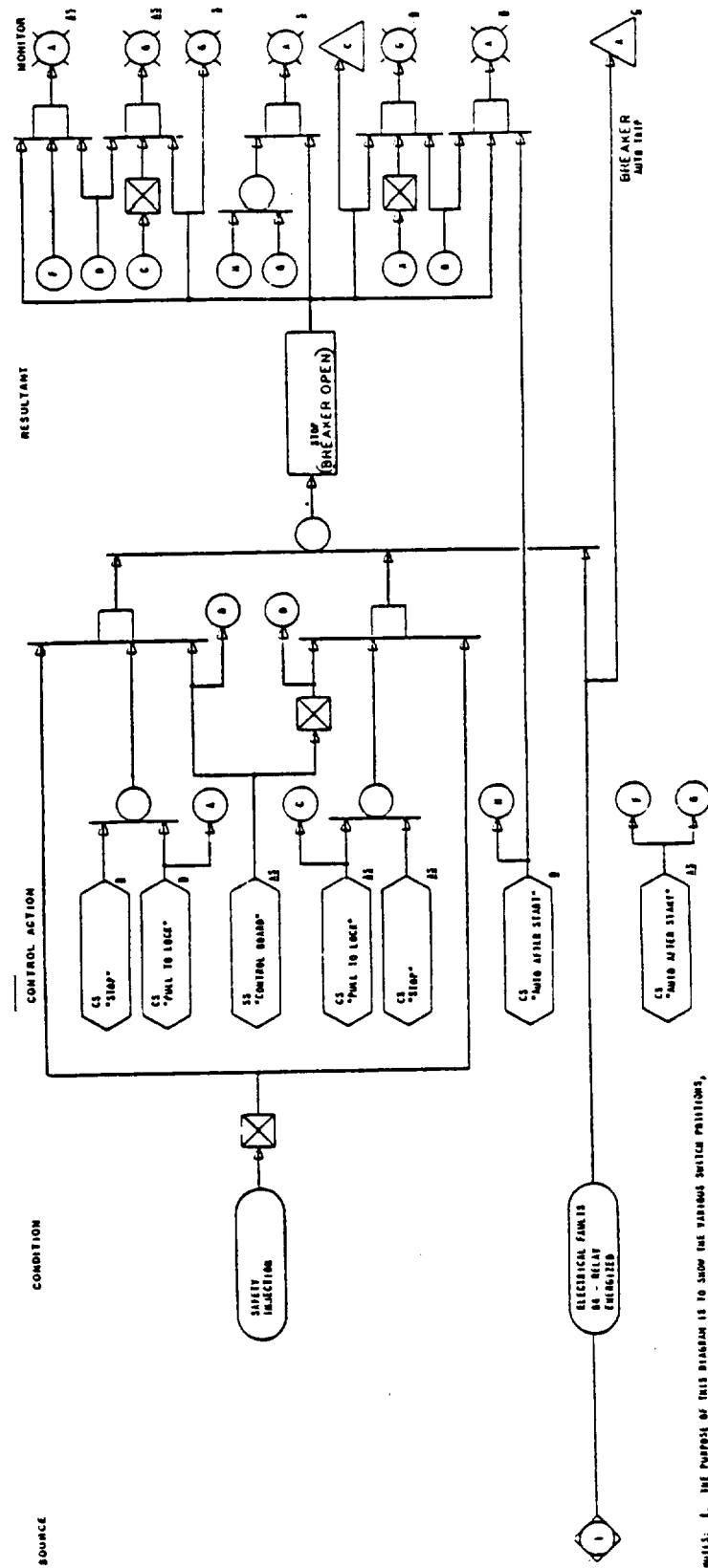
Figure 7.4-1
SWITCHING LOGIC, SHEET 1, FOR TRANSFER BETWEEN MAIN CONTROL BOARD AND AUXILIARY SHUTDOWN PANEL
(FOR SWITCHGEAR (TYPICAL))



NOTES: 1. THE PURPOSE OF THIS DIAGRAM IS TO SHOW THE VARIOUS SWITCH POSITIONS, NOT THE OPERATION OF AN INDIVIDUAL PIECE OF EQUIPMENT.

NO704001

Figure 7.4-2
SWITCHING LOGIC, SHEET 2, FOR TRANSFER BETWEEN MAIN CONTROL BOARD AND AUXILIARY SHUTDOWN PANEL
[FOR SWITCHGEAR (TYPICAL)]



NOTE: 1. THE PURPOSE OF THIS DIAGRAM IS TO SHOW THE VARIOUS SWITCH POSITIONS, NOT THE OPERATION OF AN INDIVIDUAL PIECE OF EQUIPMENT.

NO704002

Intentionally Blank

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION

7.5.1 Description

Tables 7.5-1 and 7.5-2 list the information readouts provided to the operator to enable him to perform required manual safety functions and to determine the effect of manual actions taken following a reactor trip due to a Condition II, III, or IV event. Table 7.5-2 also contains the minimum set of parameters classified as Type A for Condition IV events as analyzed by Regulatory Guide 1.97. The tables list the information readouts required to maintain the plant in a hot-shutdown condition or to proceed to a cold shutdown within the limits of the Technical Specifications. Reactivity control after Condition II and III faults will be maintained by administrative sampling of the reactor coolant for boron to ensure that the concentration is sufficient to maintain the reactor subcritical.

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

After the March 1979 accident at Three Mile Island, the arrangement of controls and displays on the control boards was reviewed. As a result, some devices were relocated on these boards to improve operator efficiency and to minimize the chance of operator error. A lamp test system was added on the safety-related control boards in the main control room to verify system/component status. In addition, postaccident monitoring and control panels were installed for both units.

7.5.2 Analysis

For Condition II, III, and IV events (see Tables 7.5-1 and 7.5-2), sufficient duplication of information is provided to ensure that the minimum information required will be available. The information is part of the operational monitoring of the plant that is under operator surveillance during normal plant operation. This is functionally arranged on the control board to provide the operator with ready understanding and interpretation of plant conditions. Comparisons between duplicate information channels or between functionally related channels will enable the operator to readily identify a malfunction in a particular channel.

Refueling water storage tank (RWST) level is indicated by four and alarmed by two independent single-channel systems. Similarly, two channels of primary system pressure (wide range) are available for maintaining proper pressure-temperature relationships following a postulated Condition II or III event. One channel of steam generator water level (wide range) is provided for each steam generator; this duplicates level information from steam generator water level (narrow range) and ensures the availability of level information to the operator.

The remaining safety-related display instrumentation necessary for Condition II, III, or IV events is obtained through isolation amplifiers from the protection system. These protection channels are described in Section 7.2.

The readouts identified in the tables were selected on the basis of sufficiency and availability during and subsequent to an accident for which they are necessary. Thus, the occurrence of an accident does not render this information unavailable, and the status and reliability of the necessary information is known to the operator before, during, and after an accident. No special separation is required to ensure the availability of necessary and sufficient information. In fact, such separation could reduce the operator's ease of interpretation of data.

The status of all safety-related instrumentation bi-stables is monitored by status lights and annunciators. All containment isolation trip valves have their status monitored by lights on the main control board. All safety-related switchgear is monitored by indicating lights in the main control room.

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

1. Range and accuracy requirements are determined through the analyses of Condition II, III, or IV events, as described in Chapter 15. The display system meets the following requirements:
 - a. The range of the readouts extends over the maximum expected range of the variable being measured, as listed in column 4 of Tables 7.5-1 and 7.5-2.
 - b. The combined available indicated accuracies, shown in column 5 of Tables 7.5-1 and 7.5-2, are within the errors assumed in the safety analyses.
 - c. Power supply for the display instruments is described in Section 8.3.1.2 and complies with paragraph 5.4 of IEEE Std 308-1971.
 - d. Those channels determined to provide useful information in charting the course of events are recorded, as shown in column 6 of Tables 7.5-1 and 7.5-2.
2. The following information is displayed on the main control board safeguards sections by more than one seismically qualified indicator from separate channels powered by separate vital buses and wired by separate multiconductor cables:
 - a. Containment building pressure.
 - b. Containment sump level.
 - c. Containment sump temperature.
 - d. RWST level.
 - e. RWST temperature.
 - f. Service water reservoir level.
 - g. Service water pressure.
 - h. Safety injection accumulator level.

- i. Safety injection accumulator pressure.
- j. Safety injection hot leg flow (total).
- k. Safety injection cold leg flow (total).
- l. Pressurizer liquid temperature
- m. Reactor vessel level
- n. Degree of Subcooling
- o. Core Exit Thermocouples

The following information is displayed to the operator on the main control board by more than one seismically qualified indicator, from separate channels powered by separate vital buses, wired by separate multiconductor cables and including a seismic recorder:

- a. Steam generator level.
- b. Pressurizer level.
- c. Pressurizer pressure.
- d. Reactor coolant temperature (wide range).
- e. Condensate storage tank level (with alarm).

The auxiliary feedwater flow is displayed to the operator on or adjacent to the main control board by a seismically qualified indicator:

The following parameters have input to the plant computer for station logs and postaccident review. The information from one channel of each parameter will be retained by the computer for 1 week, following a safeguards actuation, for postaccident analysis:

- a. Steam generator level.
- b. Pressurizer level.
- c. Pressurizer pressure.
- d. Reactor coolant temperature.
- e. Containment building pressure.

In response to NUREG-0578, Class I seismically qualified postaccident monitoring control panels for both units were installed (PAMC-1 and PAMC-2). The panels provide controls for the hydrogen analyzer inlet and outlet valves, hydrogen recombiner inlet and outlet valves, reactor coolant system venting valves, postaccident hydrogen indication, containment sump isolation valves, reactor vessel level, and containment pressure and water levels. The panels, including panel-mounted equipment, have been specified to IEEE Std 323-1971 and IEEE

Std 344-1975 requirements. All devices and internal wiring meet color separation requirements specified in Chapter 8.

In compliance with Regulatory Guide 1.97, the following information is displayed on the NIS panels by two Class 1E seismically qualified indicators from separate channels powered by separate vital buses and wired by separate multi-conductor cables.

- a. Excore neutron flux - wide range (10^{-8} to 200% of full power)
- b. Excore neutron flux - source range (0.1 to 10^5 cps)

In addition, in compliance with Appendix R, the single channel display at the remote monitoring panels provides for adequate information display of neutron flux information in the event of a fire in the control room, emergency switchgear room, or cable vault and tunnel.

Table 7.5-1
MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE
TO THE OPERATOR CONDITION II AND III EVENTS

Parameter	Number of Channels			Range	Available Indicated Accuracy ^a	Indicator/Recorder	Purpose
	Available	Required					
1. T _{cold} or T _{hot} (measured, wide range)	1 T _{hot} , 1 T _{cold} per loop	1 in any operating loop		0 to 700°F	± 13.5°F	All channels are recorded	Ensure maintenance of proper cooldown rate and ensure maintenance of proper relationship between system pressure and temperature for NDTT considerations.
2. Pressurizer water level	3	1		0 to 100% Entire distance between taps	± 7.12%	All 3 channels indicated; 1 channel is selected for recording	Ensure maintenance of proper reactor coolant inventory.
3. Reactor coolant system pressure (wide range)	2	1		0 to 3000 psig	± 70.1 psig	Indicated	Ensure maintenance of proper relationship between system pressure and temperature for NDTT considerations.
4. Containment pressure (narrow range)	4	1		0 to 65 psia	± 1.6 psia	All 4 are indicated Recorder for 1 channel	Monitor containment pressure conditions to indicate the need for potential safeguards actuation.
5. Containment pressure (wide range)	2	1		0 to 180 psia	± 4.9 psia	Both are indicated	Monitor containment pressure conditions to indicate the need for potential safeguards actuation.
6. Steam-line pressure	3/steam line	1/steam line		0 to 1400 psig	± 37.7 psig	All required channels are indicated	Monitor steam generator pressure conditions during hot shutdown and cooldown, and for use in recovery from steam generator tube ruptures.
7. Steam generator water level (wide range)	1/steam generator	b		0 to 100% (+ 7 to - 41 ft from nominal full-load water level)	- 2.1 to +2.9% (cold)	All channels recorded	Ensure maintenance of reactor heat sink.

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowances (CSA) values for a mild environment.)

b. Minimum requirements: One level channel per steam generator (either wide or narrow range) with wide-range channels operable on at least two loops.

Table 7.5-1 (continued)

MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE
TO THE OPERATOR CONDITION II AND III EVENTS

Parameter	Number of Channels		Range	Available Indicated Accuracy ^a	Indicator/Recorder	Purpose
	Available	Required				
8. Steam generator water level (narrow range)	3/steam generator	b	0 to 100% (+ 7 to - 5 ft from nominal full-load water level)	-2.7% to +11.1%	All channels indicated; the channels used for control are recorded	Ensure maintenance of reactor heat sink.
9. Inadequate Core Cooling Monitor	2	1			All channels indicated	Ensure proper core subcooling.
9.1 Reactor vessel level					One channel recorded	
Upper range vessel level			60 to 120%	- 8.2 to + 3.7%		
Full range vessel level			0 to 120%	- 11.7 to + 5.5%		
Dynamic head vessel level			0 to 120%	- 7.4 to + 3.4°F		
9.2 Degree of subcooling			- 35°F (superheat) to 200°F (subcooled)	- 24.9 to +18.6°F		
9.3 Core exit thermocouples			40 to 2300°F	- 18.6 to + 24.9°F		
10. Pressurizer liquid temperature	2	1	100 to 700°F	not calculated	All channels indicated and monitored at the computer	Provide compensation temperature for pressurizer water level

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowances (CSA) values for a mild environment.)

b. Minimum requirements: One level channel per steam generator (either wide or narrow range) with wide-range channels operable on at least two loops.

Table 7.5-2
MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE
TO THE OPERATOR CONDITION IV EVENTS

Parameter	Number of Channels			Range	Available Indicated Accuracy ^a	Indicator/Recorder	Purpose
	Available	Required					
1. Containment pressure (narrow range) ^b	4	1		0 to 65 psia	± 1.6 psia	All 4 are indicated	Monitor post-LOCA containment pressure conditions.
2. Containment pressure (wide range) ^b	2	1		0 to 180 psia	- 7.1 to + 7.5 psia	Both are indicated, only 1 is recorded	Monitor post-LOCA containment pressure conditions.
3. RWST water level	4	2		0 to 100%	-2.4 to +2.5%	All are indicated; 2 are alarmed	Ensure that water is available to the safety injection system after a LOCA and determine when to shift from injection to recirculation mode.
4. Steam generator water level (narrow range) ^b	3/steam generator	c		0 to 100% (+ 7 to - 5 ft from nominal full-load level)	- 3.7 to + 14.4% ^d	All channels indicated; the channels used for control are recorded	Detect steam generator tube rupture; monitor steam generator water level following a steam-line break.
5. Steam generator water level (wide range)	1/steam generator	c		0 to 100% (+ 7 to - 41 ft from nominal full-load level)	- 19.4 to +7.5% ^d	All channels are recorded	Detect steam generator tube rupture; monitor steam generator water level following a steam-line break.
6. Steam-line pressure ^b	3/steam line	1/steam line		0 to 1400 psig	± 96.6 psig	All channels are indicated	Monitor steam-line pressures following steam generator tube rupture or steam-line break.

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for Post Design Basis Event (PDBE) environment, except RWST and ECST water level, which is not located in a harsh environment.)

b. Variable analyzed by Regulatory Guide 1.97 and classified as Type A for Condition IV events.

c. Minimum requirements: One level channel per steam generator (either wide or narrow range) with wide-range channels operable for two loops.

d. For the steam break, when the water level channel is exposed to a hostile environment, the accuracy required can be relaxed. The indication need only convey to the operator that water level in the steam generator not experiencing the break is somewhere between the narrow-range steam generator water level taps.

Table 7.5-2 (continued)

MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE
TO THE OPERATOR CONDITION IV EVENTS

Parameter	Number of Channels			Range	Available Indicated Accuracy ^a	Indicator/Recorder	Purpose
	Available	Required					
7. Pressurizer water level ^b	3	1	0 to 100% Entire distance between taps	- 14.0 to + 2.1%	All 3 are indicated and 1 is for recording	Indicate that water has returned to the pressurizer following cooldown after steam generator tube rupture or steam-line break.	
8. Containment sump level (wide range) ^b	2	1	0 to 11 ft 4 in	- 7.2 to + 8.0 in	Both channels are indicated	Monitor containment sump level during and following a LOCA or steam-line break.	
9. Inadequate Core Cooling Monitor	2	1			All channels indicated	Monitor core conditions to help ensure proper core subcooling.	
9.1 Reactor vessel level					One channel recorded		
Upper range vessel level			60 to 120%	not calculated			
Full range vessel level			0 to 120%	not calculated			
Dynamic head vessel level			0 to 120%	not calculated			
9.2 Degree of subcooling ^b			- 35°F (superheat) to 200°F (subcooled)	- 74.8 to + 52.3 °F			
9.3 Core exit thermocouples 606K 149IH16-HIV ^b			40 to 2300°F	- 22.2 to + 36.0°F (at 700°F) - 22.8 to + 44.9°F (at 1200°F)			
10. Reactor coolant system pressure (wide range) ^b	2	1	0 to 3000 psig	- 115.1 to + 138.6 psig	Loop A and C indication only, trended on PCS	Monitor post-LOCA RCS pressure.	
11. High head safety injection flow to cold leg (total) ^b	2	1	0 to 1000 gpm	- 108.4 to + 99.9 gpm	Indicated on control board and trended on PCS	Monitor post-LOCA total safety injection flow rate to RCS cold legs.	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for Post Design Basis Event (PDBE) environment, except RWST and ECST water level, which is not located in a harsh environment.)

b. Variable analyzed by Regulatory Guide 1.97 and classified as Type A for Condition IV events.

Table 7.5-2 (continued)

MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS AVAILABLE
TO THE OPERATOR CONDITION IV EVENTS

Parameter	Number of Channels		Range	Available Indicated Accuracy ^a	Indicator/Recorder	Purpose
	Available	Required				
12. Containment high range radiation monitor ^b	2	1	10^0 to 10^7 R/hr	$\pm 2.25 \times 10^6$ R/hr	All channels are recorded	Monitor post-LOCA containment radiation levels.
13. Source range neutron flux (Gamma-Metrics)	2	1	10^{-1} to 10^5 cps	± 5810 cps	Trended on PCS	Monitor post-LOCA core reactivity.
14. Power range neutron flux (Gamma-Metrics)	2	1	10^{-8} to $2 \times 10^2\%$ power	$\pm 11.6\%$ power	Trended on PCS	Monitor post-LOCA core reactivity
15. RCS hot leg temperature (wide range)	3	1	0 to 700°F	- 6.9 to + 20.1°F	All channels are recorded	Monitor reactor coolant temperature to help ensure core cooling is being accomplished.
16. RCS cold leg temperature (wide range)	3	1	0 to 700°F	- 6.9 to + 20.1°F	All channels are recorded	Monitor reactor coolant temperature to help ensure core cooling is being accomplished.
17. Containment hydrogen analyzer	2	1	0 to 10% H ₂	$\pm 1.45\%$ H ₂	All channels are recorded	Monitor post-LOCA containment hydrogen levels.
18. Emergency condensate storage tank level	2	1	0 to 100%	$\pm 2.7\%$	One channel recorded	Monitor ECST level to help ensure adequate water supply for auxiliary feedwater.
19. Containment isolation valve position	1/isolation valve	1/isolation valve	Open/Close	not calculated	Indication only	Monitor containment integrity.

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for Post Design Basis Event (PDBE) environment, except RWST and ECST water level, which is not located in a harsh environment.)

b. Variable analyzed by Regulatory Guide 1.97 and classified as Type A for Condition IV events.

Table 7.5-3
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
NUCLEAR INSTRUMENTATION						
1. Source range						
a. Count rate	2	10 ⁰ to 10 ⁶ counts/sec	± 7% of the linear full-scale analog voltage ^b	Both channels indicated; either may be selected for recording	Control board	One 2-pen recorder is used to record any of the 8 nuclear channels (2 source range, 2 intermediate range, and 4 power range)
b. Start-up rate	2	- 0.5 to 5.0 decades/min	± 7% of the linear full-scale analog voltage ^b	Both channels indicated	Control board	
2. Intermediate range						
a. Flux level	2	10 ⁻¹¹ to 10 ⁻³ amps 8 decades of neutron flux (corresponds to 0-to-full-scale analog voltage) overlapping the source range by 2 decades	± 7% of the linear full-scale analog voltage and ± 3% of the linear full-scale voltage in the range of 10 ⁻⁴ to 10 ⁻³ A ^b	Both channels indicated; either may be selected for recording	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
NUCLEAR INSTRUMENTATION (continued)						
2. Intermediate range (continued)						
b. Start-up rate	2	- 0.5 to 5.0 decades/min	± 7% of the linear full-scale analog voltage ^b	Both channels indicated	Control board	
3. Power range						
a. Uncalibrated ion chamber current (top and bottom uncompensa ted ion chambers)	4	0 to 120% of full-power current	± 1.2% of full power current	All 8 current signals indicated	NIS racks in control room	
b. Upper and lower ion chamber current difference	4	- 30 to + 30%	± 3% of full power ^b	Diagonally opposed; any 2 of the 4 channels may be selected for recording at the same time using recorder in item 1	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
NUCLEAR INSTRUMENTATION (continued)						
3. Power range (continued)						
c. Average flux of the top and bottom, ion chamber	4	0 to 120% of full power	± 3% of full power for indication ± 2% for recording ^b	All 4 channels indicated; any 2 of the 4 channels may be recorded using recorder in item 1 above	Control board	
d. Average flux of the top and bottom ion chambers	4	0 to 200% of full power	± 2% of full power to 120% ± 6% of full power to 200% ^b	All 4 channels recorded	Control board	
e. Flux difference on the top and bottom ion chambers	4	- 30 to + 30%	± 4% ^b	All 4 channels indicated	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
REACTOR COOLANT SYSTEM						
1. T_{avg} (measured)	1/loop	530° to 630°F	±3.64°F	The 1 channel is indicated	Control board	
2. ΔT (measured)	1/loop	0 to 150% of full-power ΔT	± 5.2% of full-power ΔT	The 1 channel is indicated; one loop's channel is selected for recording	Control board	
a. T_{cold} or T_{hot} (measured, wide range)	1- T_{hot} and 1- T_{cold} per loop	0 to 700°F	± 13.5°F	Both channels recorded	Control board	
3. Overpower ΔT setpoint	1/loop	0 to 150% of full-power ΔT	± 5.7% of full-power ΔT	The 1 channel is indicated; one loop's channel is selected for recording	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
REACTOR COOLANT SYSTEM (continued)						
4. Overtemperature ΔT setpoint	1/loop	0 to 150% of full-power ΔT	± 8.4 (F(ΔI) < 0) ± 6.7 (F(ΔI) = 0) ± 9.0 (F(ΔI) > 0)	All channels indicated; one channel is selected for recording	Control board	
5. Pressurizer pressure	5	1700 to 2500 psig	± 25.3 psig	All channels indicated	Control board	
6. Pressurizer level	3	0 to 100% Entire distance between taps	± 7.12%	All channels indicated; one channel is selected for recording	Control board	Two-pen recorder used, second pen records reference level signal.
7. Primary coolant flow	3/loop	0 to 120% of rated flow	± 3.5 Foxboro transmitters ± 3.5 Rosemount transmitters at 100% flow	All channels indicated	Control board	
8. Reactor coolant pump amperes	1/loop	0 to 1500A	not calculated	All channels indicated	Control board	One channel for each bus.
9. Reactor coolant system pressure (wide range)	2	0 to 3000 psig	± 70.1 psig	All channels indicated	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
REACTOR COOLANT SYSTEM (continued)						
10. Pressurizer liquid temperature	2	100 to 700°F	not calculated	All channels indicated and monitored at the computer	Control board	
REACTOR CONTROL SYSTEM						
1. Demanded rod speed	1	0 to 76 step/min	± 1.5 step/min ^b	The 1 channel is indicated	Control board	
2. Median T _{avg}	1	530° to 630°F	$\pm 3.64^\circ\text{F}$	The 1 channel is indicated and recorded	Control board	The median of the 3-loop average temperatures are passed to the indicator and recorder.
3. T _{reference}	1	530° to 630°F	$\pm 4^\circ\text{F}$ ^b	The 1 channel is indicated and recorded	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
 TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
REACTOR CONTROL SYSTEM (continued)						
4. Control rod position						
a. Number of steps of demand rod withdrawal	1/group	0 to 235 steps	± 1 step ^b	Each group is indicated during rod motion	Control board	If system not available, borate and sample accordingly. These signals are used in conjunction with the measured position signals (4c) to detect deviation of any individual rod from the demanded position. A deviation will actuate an alarm and annunciator.
b. Rod measured position	1 for each rod	0 to 235 steps	$\pm 5\%$ of full scale between 10-90% ^b	Each rod position is indicated	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/Recorder	Location	Notes
REACTOR CONTROL SYSTEM (continued)						
5. Control rod bank demand position	4	0 to 100% withdrawn (0 to 230 steps)	$\pm 2.5\%$ of total bank travel ^b	All 4 control rod bank positions are recorded along with the low-low limit alarm for each bank	Control board	1. One channel for each control rod. 2. An alarm and annunciator are actuated when the last rod control bank to be withdrawn reaches the withdrawal limit, when any rod control bank reaches the low insertion limit, and when any rod control bank reaches the low-low insertion limit.
CONTAINMENT SYSTEM						
Containment pressure (narrow range)	4	0 to 65 psia	± 1.6 psia	All 4 channels indicated	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/Recorder	Location	Notes
FEEDWATER AND STEAM SYSTEMS						
1. Auxiliary feedwater water flow	1/steam generator	0 to 500 gpm	± 15 gpm	All channels indicated	Control board	One channel to measure the flow to each steam generator.
2. Steam generator level (narrow range)	3/steam generator	+ 7 to - 5 ft from nominal full-load level	-0.3 to +1.3 ft	All channels indicated; the channels used for control are recorded	Control board	
3. Steam generator level (wide range)	1/steam generator	+ 7 to - 41 ft from nominal full-load level	- 1.3 to + 1.7 ft (cold)	All channels recorded	Control board	
4. Main feedwater flow	2/steam generator	0 to 5×10^6 lbm/hr	$\pm 1.46 \times 10^5$ lbm/hr	All channels indicated; the channels used for control are recorded	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/Recorder	Location	Notes
FEEDWATER AND STEAM SYSTEMS (continued)						
5. Magnitude of signal controlling main and bypass feedwater control valves	1/main 1/bypass	0 to 100% of valve opening	$\pm 1.5\%$ ^b	All channels indicated	Control board	1. One channel for each main and bypass feed-water control valve. 2. OPEN/SHUT indication is provided in the control room for each main feed- water control valve.
6. Steam flow	2/steam generator	0 to 5×10^6 lbm/hr	$\pm 2.04 \times 10^5$ lbm/hr	All channels indicated; the channels used for control are recorded	Control board	Accuracy is equipment capability; however, absolute accuracy depends on applicant calibration against feedwater flow.
7. Steam line pressure	3/steam line	0 to 1400 psig	± 37.7 psig	All channels indicated	Control board	

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

Table 7.5-3 (continued)
CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

Parameter	Number of Channels Available	Range	Available Indicated Accuracy ^a	Indicator/ Recorder	Location	Notes
FEEDWATER AND STEAM SYSTEMS (continued)						
8. Steam dump demand signal	1	0 to 100% maximum demand to valves	± 1.5% ^b	The one channel is indicated	Control board	OPEN/SHUT indication is provided in the control room for each steam dump valve.
9. Turbine impulse chamber pressure	2	0 to 120% full power	± 4.2% full power ^b	Both channels indicated	Control board	OPEN/SHUT indication is provided in the control room for each turbine stop valve.
10. Area monitoring (Aux. Building ambient temperature)	18	0 to 200°F	± 8.5°F	Each channel indicated	Control room	Main annunciator alarm on high temperature in any monitored area.

a. Includes channel accuracy and environmental effects. (Accuracies are based on Channel Statistical Allowance (CSA) values for a mild environment.)

b. An original Westinghouse estimation of indication accuracy - not a CSA calculation.

7.6 ALL OTHER SYSTEMS REQUIRED FOR SAFETY

Electrical schematic diagrams for all other systems required for safety, as described in Section 7.6.1, were included in reports NA-TR-1001 and NA-TR-1002, *Safety Related Electrical Schematics*, dated May 10, 1973, which were submitted to the Atomic Energy Commission (AEC), on May 18, 1973, as separate documents. A logic diagram for the loop stop valves has been included in the FSAR as Figure 7.6-1. Logic diagrams for the main control room ventilation duct isolation are included in report NA-TR-1001, dated May 10, 1973.

7.6.1 Instrumentation and Control Power Supplies

Chapter 8 provides a description and analysis of the instrumentation and control power supplies, consisting of the vital bus and dc power systems.

7.6.2 Residual Heat Removal System Inlet MOV Interlocks

7.6.2.1 Description

There are two motor-operated gate valves in series in the inlet line from the reactor coolant system to the residual heat removal (RHR) system. They are normally closed and are only open for residual heat removal after system pressure is reduced below approximately 450 psig and system temperature has been reduced below approximately 350°F. (See Chapter 5 for details of the RHR system.) Each of these valves is interlocked with a pressure signal to prevent its being opened whenever the system pressure exceeds 418 psig. The upstream valve is interlocked from one protection channel. The other valve is interlocked from a second protection channel. Both protection channels use Rosemount 1153 pressure transmitters which are environmentally qualified.

7.6.2.2 Analysis

Based on the scope definitions presented in Reference 1 (IEEE Std 279-1971) and Reference 2 (IEEE Std 338-1971), these criteria do not apply to the RHR isolation valve interlocks; however, to meet AEC requirements and because of the possible severity of the consequences of loss of function, the requirements of IEEE Std 279-1971 are applied with the following comments:

1. For the purpose of applying IEEE Std 279-1971, to this circuit, the following definitions are used:
 - a. Protection System—The two valves in series in the line and all components of their interlocking and closure circuits.
 - b. Protective Action - The maintenance of RHR system isolation from the reactor coolant system at reactor coolant system pressures above RHR design pressure.

2. IEEE Std 279-1971, Paragraph 4.10: The requirement for online test and calibration capability is applicable only to the actuation signal and not to the isolation valves, which are required to remain closed during power operation.
3. IEEE Std 279-1971, Paragraph 4.15: This requirement does not apply because the setpoints are independent of the mode of operation and are not changed.

Environmental qualification of the valves and wiring is discussed in Section 3.11.

7.6.3 Reactor Coolant System Loop Isolation Valve Interlocks

7.6.3.1 Description

The purpose of these interlocks is to ensure that an accidental start-up of an unborated and/or cold, isolated reactor coolant loop results only in a relatively slow reactivity insertion rate.

The interlocks perform a protective function. Therefore, there are:

1. Two independent limit switches to indicate that a valve is fully opened.
2. Two independent switches to indicate that a valve is fully closed.
3. Two differential pressure switches in each line that bypasses a cold-leg loop isolation valve. This is the line that contains the relief line isolation valve (valve 4 in Figure 7.6-2). It should be noted that flow through the relief line isolation valves indicates that (1) the valves in the line are open, (2) the line is not blocked, and (3) the pump is running.

7.6.3.2 Analysis

Section 15.2.6 presents an analysis of the start-up of an inactive reactor coolant loop with the loop isolation valves initially closed. The start-up of an inactive reactor coolant loop accident analysis does not credit the loop stop valve interlocks.

Based on the scope definitions presented in References 1 and 2, these criteria do not apply to the reactor coolant system loop isolation valve interlocks; however, to ensure continuous availability of the function provided by these interlocks, the requirements of IEEE Std 279-1971, are applied.

Only those interlocks and alarms relating to core protection are described. Those required for reactor coolant pump protection are not part of the protection system and need not meet the protection system criteria of Reference 1.

In addition to the interlocks, an alarm is provided to indicate that the bypass valve (valve 3 in Figure 7.6-2) is not closed when the power is above P-8. This will alarm whenever the reactor is at a power level where all loops are required to be in service and the bypass valve is not fully closed. An alarm is used because, if the bypass valve is opened at full power, the core flow reduction is of the order of 2% to 5% and does not result in an immediate DNB problem.

7.6.4 Main Control Room, Relay Room, and Emergency Switchgear Room Air Conditioning, Heating, and Ventilation System Instrumentation and Controls

7.6.4.1 Description

The system design, flow diagram, and instrumentation application for the main control room and relay room air conditioning, heating, and ventilation system are included in Section 9.4.1. Temperature controls are provided to maintain the return air from the main control room and relay room at a predetermined temperature, as sensed by the temperature transmitters. During LOCA conditions, the control and relay rooms are isolated from the outside atmosphere. A differential pressure indicator mounted on the ventilation panel, located in the main control room, is provided to determine that the pressure in the control room is being maintained slightly above the atmospheric pressure following a LOCA. A separate indicator mounted at the auxiliary shutdown panel for each unit shows that the pressure in the relay room is also being maintained slightly above atmospheric.

There are no areas other than those described above where safety-related control and electrical equipment require a controlled environment (temperature, humidity, and air particulate) for proper operation. Schematic drawings for equipment supporting the areas described were included in the *Safety Related Electrical Schematics*, Volume II, Tab 9, submitted to the AEC on May 18, 1973.

7.6.4.2 Analysis

The control room ventilation system outdoor air inlet has two dampers in series, powered from the same source as the fan and controlled by switches in the control room. Similarly, the dual dampers for the switchgear room ventilation inlet are powered from the same sources as its fan and are controlled by switches at the auxiliary control panel.

7.6.5 Refueling Interlocks

Electrical interlocks (i.e., limit switches) for reducing the possibility of damage to the fuel during fuel-handling operations are provided, as well as mechanical stops, which provide the primary means of preventing fuel-handling accidents. For example, safety aspects of the manipulator crane fuel-handling operation depend on the use of electrical interlocks and mechanical stops, as discussed in Section 9.1.4.4.4. The electrical interlocks for this manipulator crane fuel-handling operation are not specifically designed to the requirements of IEEE Std 279-1971 because of the backup provided by the mechanical stops.

7.6.6 Accumulator Isolation Valve Control

The control diagram for the motor-operated isolation valve in the accumulator discharge is shown in Figure 7.6-3. The controls of the motor-operated isolation valves include automatic opening whenever reactor coolant system pressure exceeds a specified limit consistent with the assumptions of the accident analyses.

It is necessary with automatic opening of these valves with reactor coolant pressure to include an administratively controlled manual bypass circuit that must be actuated to allow for periodic testing of the system valves. This manual bypass will be overridden by a safety injection signal or a manual opening signal. Additional description is in Sections 6.3.2.2.7 and 6.3.5.5.1.

7.6.7 Pressurizer Relief Valve Flow Indication

The NRC clarifications to NUREG-0578 (contained in *Discussion of Lessons Learned Short-Term Requirements*, Position 2.1.3.a, Clarification 2, October 30, 1979) state that control room indication and alarm should be provided for the valve position of the Pressurizer power-operated relief valves (PORVs) PCV-1455C and 1456 and the safety valves SV-1551A, B, and C. These valves have been included in the North Anna response to USNRC Regulatory Guide 1.97 - *Post Accident Monitoring*.

In order to protect the Reactor Coolant System and meet NUREG-0578 / Regulatory Guide 1.97, *Post Accident Monitoring* requirements, an environmentally and seismically qualified Valve Monitoring System (VMS) has been installed to verify the CLOSED, NOT-CLOSED position of the safety valves during all modes of plant operation, except Mode 6 (Refueling). The PORVs use separate, environmentally and seismically qualified limit switches to monitor valve position in all modes of operation.

The VMS monitors safety valves using accelerometers and preamplifiers located inside the reactor containment. These accelerometers provide an input to the acoustical monitors in the Control Room. They provide reliable indication and alarms in the Main Control Room whenever any one of the three safety valves, (SV-1551A, B, and C) are not fully closed.

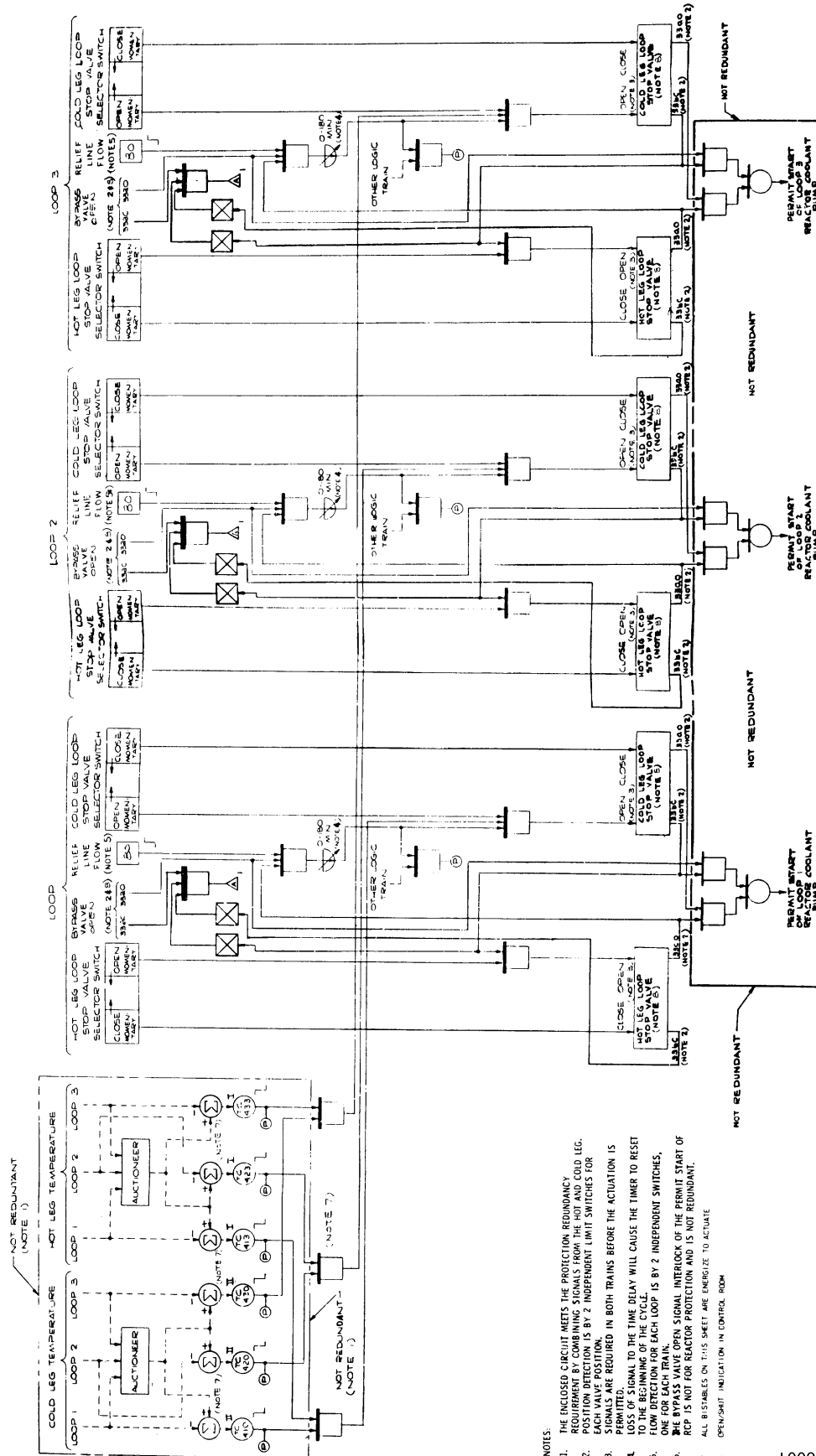
Pressurizer safety valves SV-1551A, B, and C have valve position indication in the Control Room derived from a qualified, single channel of acoustical monitoring, operating from a highly reliable power supply. For each safety valve, an active and passive qualified accelerometer has been attached to the outside of the discharge pipe and connected to preamplifiers installed inside a transient shield to maintain their environmental qualification. Either of these sensors can provide indication to alert the operator when flow is detected through a pressurizer safety valve. A panel, common to both Units 1 and 2, provides Operators with Control Room indication of the safety valves position. The power supply for the panel can be fed from either unit. A voltage relay provides automatic transfer on the loss of either unit's power supply. The panel is seismically supported and is located beside 1-EI-CB-08A.

PORV position indication for PCV-1455C and 1456 have four environmentally and seismically qualified valve stem position limit switches, powered by diverse power supplies, to detect OPEN/CLOSED position of each valve. The limit switches are arranged in two sets of two per valve to provide channel redundant indication position lights in the Control Room. These limit switches have been seismically installed, external to the PORV.

7.6 REFERENCES

1. The Institute of Electrical and Electronic Engineers, Inc., *IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations*, IEEE Std 279-1971.
2. The Institute of Electrical and Electronics Engineers, Inc., *IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems*, IEEE Std 338-1971.

Figure 7.6-1
LOOP STOP VALVE INTERLOCKS

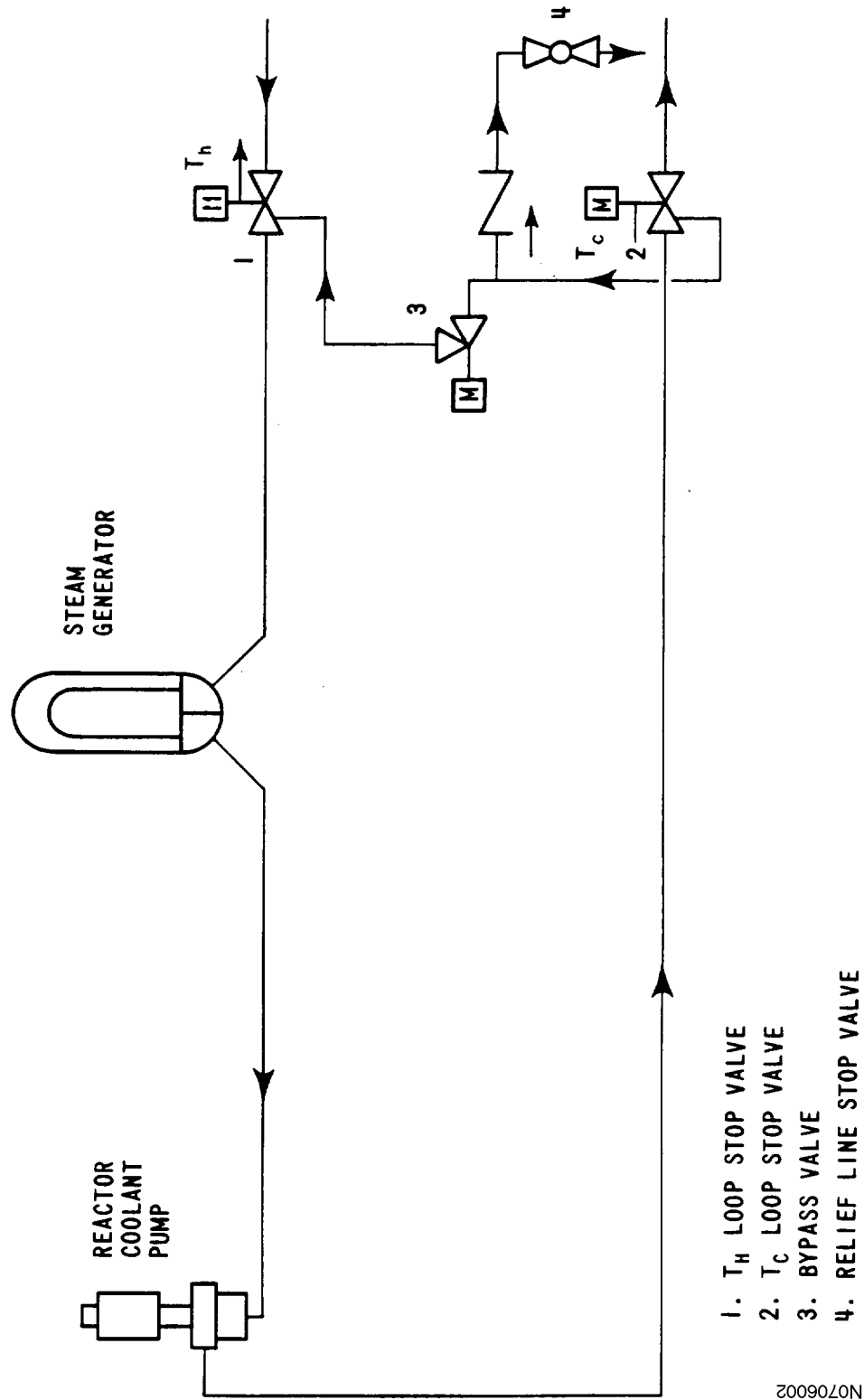


NOTES:

1. THE ENCLOSED CIRCUIT MEETS THE PROTECTION REDUNDANCY REQUIREMENTS FOR THE STOP VALVE INTERLOCKING SIGNALS FROM THE HOT AND COLD LEG. POSITION DETECTION IS BY 2 INDEPENDENT LIMIT SWITCHES FOR EACH VALVE POSITION.
2. SIGNALS ARE REQUIRED IN BOTH TRAINS BEFORE THE ACTUATION IS PERMITTED.
3. LOSS OF SIGNAL TO THE TIME DELAY WILL CAUSE THE TIMER TO RESET.
4. THE PERMIT START OF THE CYCLE DELAY WILL CAUSE THE TIMER TO RESET.
5. FLOW DETECTION FOR EACH LOOP IS BY 2 INDEPENDENT SWITCHES, ONE FOR EACH TRAIN.
6. THE BYPASS VALVE OPEN SIGNAL INTERLOCK OF THE PERMIT START OF RCP IS NOT FOR REACTOR PROTECTION AND IS NOT REDUNDANT.
7. ALL BISTABLES ON THIS SHEET ARE ENERGIZED TO ACTIVATE.
8. OPEN/SHUT INDICATION IN CONTROL ROOM.

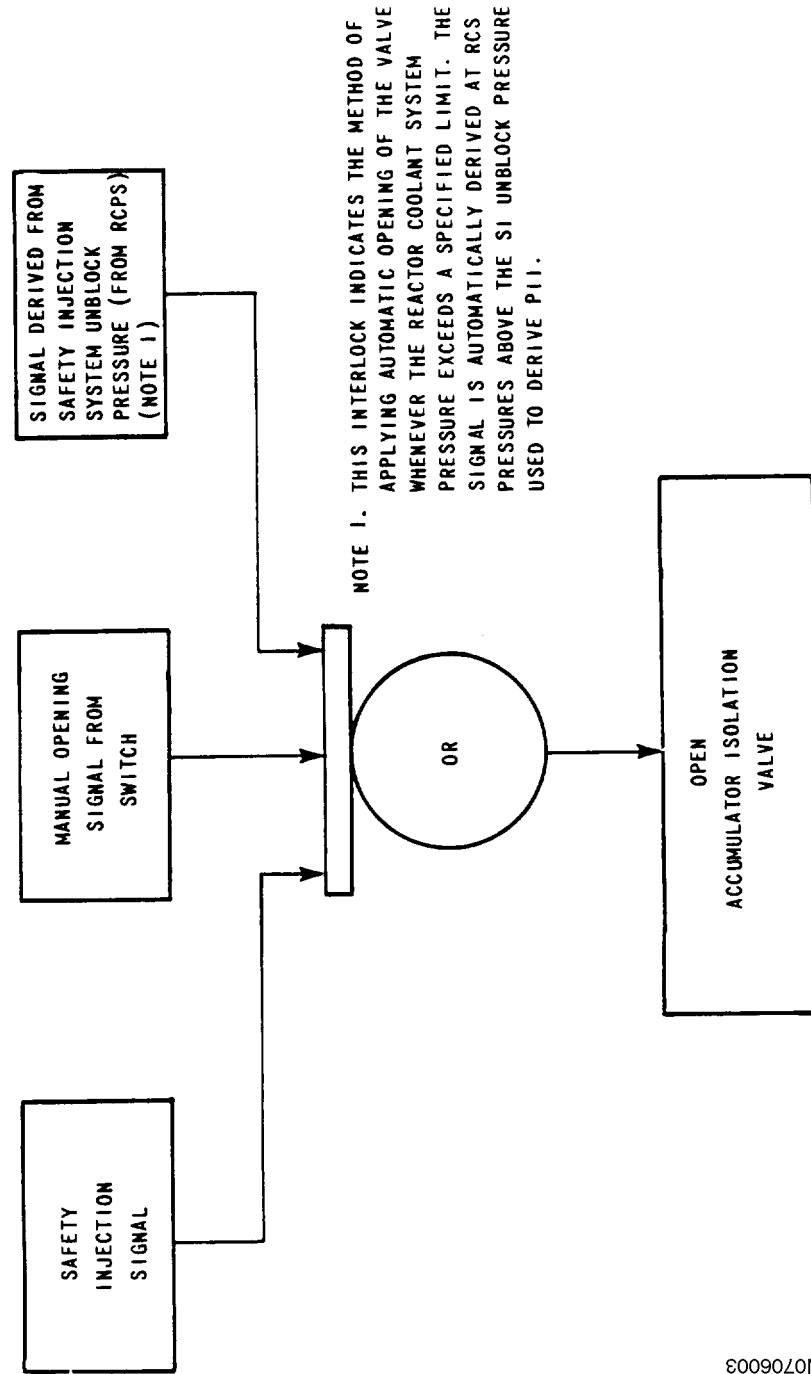
N0706001

Figure 7.6-2
TYPICAL REACTOR COOLANT SYSTEM LOOP WITH LOOP STOP VALVES



N0706002

Figure 7.6-3
FUNCTIONAL BLOCK DIAGRAM FOR OPENING ACCUMULATOR ISOLATION VALVE



N0706003

7.7 PLANT CONTROL SYSTEMS

The general design objectives of the plant control systems are the following:

1. To establish and maintain power equilibrium between the primary and secondary systems during steady-state unit operation.
2. To constrain operational transients to preclude unit trip and re-establish steady-state unit operation.
3. To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and enables the operator to assume manual control of the systems.

7.7.1 Description

The plant control systems described in this section perform the following functions:

1. *Reactor Control System*
 - a. Enables the nuclear plant to accept a step-load increase or decrease of 10% and a ramp increase or decrease of 5% per minute, within the load range of 15% to 100% without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.
 - b. Maintains reactor coolant average temperature (T_{avg}) within prescribed limits by creating the bank demand signals for moving groups of rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies the signals to pressurizer level control and steam dump control. These signals are derived in the Reactor Protection System sent to the reactor control system via circuit isolators.
2. *Rod Control System*
 - a. Provides for reactor power modulation by manual or automatic control of control rod banks in a preselected sequence and for manual operation of individual banks.
 - b. The rod control system includes systems for monitoring and indicating for the following purposes:
 - 1) To provide alarms to alert the operator if the required core reactivity shutdown margin is not available because of excessive control rod insertion.
 - 2) To display the control rod position.
 - 3) To provide alarms to alert the operator if control rod deviation exceeds a preset limit.
3. *Plant Control System Interlocks* (See Table 7.7-1.)

Prevent further withdrawal of the control banks when signal limits are approached that predict the approach of a DNBR limit or kilowatts per foot limit.

4. *Pressurizer Pressure Control*

Maintains or restores the pressurizer pressure to the design pressure ± 35 psi (which is well within reactor trip and relief and safety valve actuation setpoints limits) following normal operational transients that induce pressure changes by control (manual or automatic) of heaters and spray in the pressurizer. Also provides steam relief by controlling the power relief valves.

5. *Pressurizer Water-Level Control*

- a. Establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature. Level changes are caused by coolant density changes induced by loading, operational, and unloading transients. Level changes are also produced by charging flow control (manual or automatic) as well as by manual selection of letdown orifices.
- b. Maintains coolant level in the pressurizer within prescribed limits by controlling the charging system flowrate, thus providing control of the reactor coolant water inventory, and isolates the letdown on low level.

6. *Steam Generator Water-Level Control*

- a. Establishes and maintains the steam generator water level to within predetermined limits during normal operating transients.
- b. Provides capability to restores the steam generator water level to within predetermined limits at unit trip conditions. Regulates the feedwater flow rate such that during operational transients the heat sink for the reactor coolant system does not decrease below a minimum. Steam generator water inventory control is manual or automatic through the use of feedwater control valves.

7. *Steam Dump Control*

- a. Permits the nuclear plant to accept a sudden loss of load without incurring reactor trip. Steam is dumped to the condenser as necessary to accommodate excess power generation in the reactor during turbine load-reduction transients.
- b. Ensures that stored energy and residual heat are removed following a reactor trip, to bring the plant to equilibrium no-load conditions without the actuation of the steam generator safety valves.
- c. Maintains the plant at no-load conditions and permits manual temperature control.

8. *Incore Instrumentation*

Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

7.7.1.1 Reactor Control System

The reactor control system enables the nuclear plant to follow load changes automatically, including the acceptance of step-load increases or decreases of 10% and ramp increases or decreases of 5% per minute, within the load range of 15% to 100% without reactor trip, steam dump, or pressure relief, subject to possible xenon limitations. The system is also capable of restoring coolant average temperature to within the programmed temperature deadband following a change in load. Manual control rod operation may be performed at any time.

The reactor control system controls the reactor coolant average temperature by the regulation of control rod bank position. The reactor coolant loop average temperatures are determined from hot-leg and cold-leg measurements in each reactor coolant loop. These signals are derived in the reactor protection system sent to the reactor control system via circuit isolators. An average coolant temperature (T_{avg}) is computed for each loop, where:

$$T_{avg} = \frac{T_{hot} + T_{cold}}{2}$$

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the median value of the average measured temperatures (which is then processed through a lead-lag compensation unit) from each of the reactor coolant loops constitutes the primary control signal, as shown in general in Figure 7.7-1 and in more detail on the functional diagrams shown in Figure 7.7-2. The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full-power condition. The T_{avg} is also a signal to the pressurizer level control, steam dump control, and rod insertion limit monitoring.

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response.

7.7.1.2 Rod Control System

The rod control system receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 5 to 45 in/minute (8 to 72 steps/minute) depending on the magnitude of the error signal. The rod direction demand signal is determined by the positive or negative value of the error signal. Manual control is provided to move a control bank in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15% of rated load, the operator may select the AUTOMATIC mode, and rod motion is then controlled by the reactor control systems. A permissive interlock C-5 (see Table 7.7-1) derived from measurements of turbine impulse chamber pressure prevents automatic withdrawal when the turbine load is below 15%. In the AUTOMATIC mode, the rods are again withdrawn (or inserted) in a predetermined programmed

sequence by the automatic programming equipment. The manual and automatic controls are further interlocked with the control interlocks.

The shutdown banks are always in the fully withdrawn position during normal operation and are moved to this position at a constant speed by manual control before criticality. A reactor trip signal causes them to fall by gravity into the core. There are two shutdown banks.

The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All rod control cluster assemblies in a group are electrically paralleled to move simultaneously. There is individual position indication for each rod cluster control assembly.

Power to rod drive mechanisms is supplied by two motor-generator sets operating from two separate 480V, three-phase buses. Each generator is of the synchronous type and is driven by a 150-hp induction motor. The ac power is distributed to the rod control power cabinets through the two series connected reactor trip breakers.

The variable speed rod control system rod drive programmer affords the ability to insert small amounts of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed. A summary of the rod cluster control assembly sequencing characteristics is given below.

1. Two groups within the same bank are stepped such that the relative position of the groups will not differ by more than one step.
2. The control banks are programmed such that the withdrawal of the banks is sequenced in the following order: control bank A, control bank B, control bank C, and control bank D. The programmed insertion sequence is the opposite of the withdrawal sequence, that is, the last control bank withdrawn (bank D) is the first control bank inserted.
3. The control bank withdrawals are programmed such that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank. When the first bank reaches the top of the core, it stops, while the second bank continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the unit reaches the desired power. The control bank insertion sequence is the opposite.
4. Overlap between successive control banks is adjustable between 0% to 50% (0 and 115 steps), with an accuracy of ± 1 step.
5. Rod speeds for the control banks are capable of being controlled between a minimum of 8 steps/minute and a maximum of 72 steps/minute.

7.7.1.3 Plant Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

The nuclear instrumentation system is described in Reference 1.

The power range channels are important because of their use in monitoring power distribution in the core within specified safe limits. They are used to measure reactor power level, axial power imbalance, and radial power imbalance. These channels are capable of recording overpower excursions up to 200% of full power. Suitable alarms are derived from these signals, as described below.

Basic power range signals are as follows:

1. Total current from a power range detector (four such signals from separate detectors); these detectors are vertical and have an active length of 10 feet.
2. Current from the upper half of each power range detector (four such signals).
3. Current from the lower half of each power range detector (four such signals).

Derived from these basic signals are the following (including standard signal processing for calibration):

1. Indicated nuclear flux (four such).
2. Indicated axial flux imbalance, derived from upper-half flux minus lower-half flux (four such).

Alarm functions derived are as follows:

1. Deviation (maximum minus minimum of four) in indicated nuclear power.
2. Upper radial tilt (maximum to average of four) on upper-half currents.
3. Lower radial tilt (maximum to average of four) on lower-half currents.

Nuclear power and axial imbalance is selectable for recording as well. Indicators are provided on the control board for nuclear power and for axial power imbalance.

7.7.1.3.2 Rod Position Monitoring of Control Rods

The following separate systems are provided to sense and display control rod position:

1. Analog system—An analog signal is produced for each rod cluster control assembly by a linear variable transformer.

Direct continuous readout of every rod cluster control assembly position is presented to the operator by individual meter indications, without the need for operator selection or switching to determine rod position. A rod bottom (rod drop) alarm is provided.

2. Demand position system—The demand position system counts pulses generated in the rod drive control system to provide a digital readout of the demanded bank position.

The demand position and analog rod position indication systems are separate systems; each serves as backup for the other. Comparison by the reactor operator of the demand reading from the digital readout and the analog (actual) reading from the meter indications verifies proper operation of the rod control system. If doubt remains about the rod alignment, an incore map may be made as described in Section 7.7.1.9.3.

The rod position monitoring system is described in detail in Reference 2.

7.7.1.3.3 Control Bank Rod Insertion Monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the reactor coolant system loop delta T) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. The following two alarms are provided for each control bank:

1. The “low” alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the chemical and volume control system.
2. The “low-low” alarm alerts the operator to take action to add boron to the reactor coolant system by any one of several alternative methods.

The purpose of the control bank rod insertion monitor is to warn the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip; provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection; and limits rod insertion such that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power, the allowable rod insertion limits must be decreased (the rods must be withdrawn further) with increasing power. Two parameters that are proportional to power are used as inputs to the insertion monitor. These are the delta T between the hot leg and the cold leg, which is a direct function of reactor power, and T_{avg} which is programmed as a function of power. The rod insertion monitor uses parameters for each control rod bank as follows:

$$Z_{LL} = A(\Delta T) + B(T_{avg}) + C \quad (7.7-1)$$

where:

Z_{LL} = maximum permissible insertion limit for affected control bank

(ΔT) = median/high select ΔT of all loops

(T_{avg}) = median/high select T_{avg} of all loops

B = 0, A and C are maintained and revised by Engineering in the Core Operating Limits Report for Banks C and D.

The control rod bank demand position (Z) is compared to Z_{LL} as follows:

If $Z - Z_{LL} \leq D$, a low alarm is actuated.

If $Z - Z_{LL} \leq E$, a low-low alarm is actuated.

Since the highest values of T_{avg} and delta T are chosen by the median/Hi select feature in the event of a failure in a temperature channel, a conservatively high representation of power is used in the insertion limit calculations.

The actuation of the low alarm alerts the operator of an approach to reduced shutdown reactivity. Administrative procedures require the operator to add boron through the chemical and volume control system. The actuation of the low-low insertion limit alarm alerts the operator to initiate boration to restore shutdown margin in accordance with the plant procedures. The value of "E" is chosen so that the low-low alarm would normally be actuated before the insertion limit is reached. The value of "D" is chosen to allow the operator to follow normal boration procedures. Figure 7.7-3 shows a block diagram representation of the control rod bank insertion monitor. The monitor is shown in more detail on the functional diagrams shown in Figure 7.7-2. In addition to the rod insertion monitor for the control banks, an alarm system is provided to warn the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are established by the following:

1. Establishing the allowed rod reactivity insertion at full power consistent with the purposes given above.
2. Establishing the differential reactivity worth of the control rods when moved in normal sequence.
3. Establishing the change in reactivity with power level by relating power level to rod position.
4. Linearizing the resultant limit curve. All key nuclear parameters in this procedure are measured as part of the initial and periodic physics testing program.

Any unexpected change in the position of the control bank under automatic control, or a change in coolant temperature under manual control, provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, samples are taken periodically of coolant boron concentration. Variations in concentration during core life provide an additional check on the reactivity status of the reactor, including core depletion.

7.7.1.3.4 Rod Deviation Alarm

The demanded and measured rod position signals are displayed on the control board. They are also monitored by the plant computer, which provides a visual printout and an audible alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset

limit. The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot-channel factors.

Figure 7.7-4 is a block diagram of the rod deviation comparator and alarm system.

7.7.1.3.5 Rod Bottom Alarm

A rod bottom signal for the control rods bistable in the analog rod position system as described in Reference 2 is used to operate a control relay, which generates the ROD BOTTOM ROD DROP alarm.

7.7.1.4 Plant Control System Interlocks

The listing of the plant control system interlocks, along with the description of their derivations and functions, is presented in Table 7.7-1. It is noted that the designation numbers for these interlocks are preceded by “C.” The development of these logic functions is shown in the functional diagrams: C-1 (Figures 7.2-3 & 7.2-10); C-2 (Figure 7.2-10); C-3 (Figures 7.2-5 & 7.2-8); C-4 (Figures 7.2-5 & 7.2-8); C-5 (Figures 7.2-8 & 7.7-2); C-7 (Figure 7.7-5); C-8 (Figures 7.2-8 & 7.7-5); C-9 (Figure 7.7-5); C-11 (Figure 7.7-2); and C-20 (Figure 7.2-13).

7.7.1.4.1 Rod Stops

Rod stops are provided to prevent abnormal power conditions that could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

Rod stops are the C₁, C₂, C₃, C₄, and C₅ control interlocks identified in Table 7.7-1. The C₃ rod stop, derived from overtemperature delta T, and the C₄ rod stop, derived from overpower delta T, are also used for turbine runback, which is discussed below.

7.7.1.4.2 Automatic Turbine Load Runback

Automatic turbine load runback is initiated by an approach to an over-power or overtemperature condition. This will prevent high-power operation that might lead to an undesirable condition that, if reached, will be protected by reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower delta T signal. Two-out-of-three coincidence logic is used.

A rod stop and turbine runback are initiated when:

$$\Delta T > \Delta T_{\text{rod stop \& turbine runback}}$$

for both the overtemperature and the overpower condition.

For either condition in general:

$$\Delta T_{\text{rod stop \& turbine runback}} = \Delta T_{\text{setpoint}} - B_p \quad (7.7-2)$$

where:

B_p = a setpoint bias

where delta T setpoint refers to the overtemperature delta T reactor trip value and the overpower delta T reactor trip value for the two conditions.

The turbine runback is continued until delta T is equal to or less than delta $T_{\text{rod stop \& turbine runback}}$. This function serves to maintain an essentially constant margin to trip.

7.7.1.5 Pressurizer Pressure Control

The reactor coolant system pressure is controlled by using the heaters (in the water region) and the spray (in the steam region) of the pressurizer, plus steam relief for large positive pressure transients. Pressurizer pressure from one of the control system transmitters is used in conjunction with a reference pressure to develop a demand signal for a three mode controller providing for pressurizer proportional heater control, pressurizer backup heater control, spray valve control, and control of one of two PORVs.

Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer. The spray nozzle is located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

Pressure is raised by adding heat to the pressurizer via the pressurizer heaters. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct small pressure variations. These variations are due to heat losses, including heat losses from a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure controlled signal demands approximately 100% proportional heater power.

Two pressurizer power-operated relief valves limit system pressure for large positive pressure transients. During the low temperature solid water phase of reactor coolant system pressurization both PORVs are controlled by separate wide-range pressure transmitters and an auctioneered-low temperature signal from the wide-range reactor coolant system cold leg temperature devices. The PORVs will actuate if undesirable combinations of temperature and pressure develop. During power operations, one PORV is controlled by a pressurizer pressure transmitter and associated master controller. Actuation of this PORV is dependent on the master controller pressure setpoint and the length of time that pressurizer pressure is above the setpoint.

The second PORV is controlled, during power operations, from a separate pressurizer pressure transmitter and will actuate on a high-pressure signal.

A block diagram of the pressurizer pressure control system is shown in Figure 7.7-9.

7.7.1.6 Pressurizer Water-Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant changes due to reactor coolant temperature, the steam-water interface moves to absorb the variations with relatively small pressure disturbances.

The water inventory in the reactor coolant system is maintained by the chemical and volume control system. During normal plant operation, the charging flow varies to produce the flow demanded by the pressurizer water-level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the median temperature of the three loops average temperatures used for control. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

Manual control of pressurizer water level is available at all times.

A block diagram of the pressurizer water level control system is shown in Figure 7.7-10.

7.7.1.7 Steam Generator Water-Level Control

Each steam generator is equipped with a three-element feedwater flow control system that maintains a programmed water level as a function of turbine load. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water-level signal, the programmed level, and the pressure-compensated steam flow signal. Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual control of the feedwater control system is available at all times.

A block diagram of the steam generator water-level control system is shown in Figure 7.7-11.

7.7.1.8 Steam Dump Control

The steam dump system is designed to accept a 40% loss of net load without tripping the reactor.

The automatic steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed on the reactor coolant system. By bypassing the main steam directly to the condenser, an artificial load is maintained on the primary system. The

rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The North Anna plant can relieve the heat equivalent to 50% of rated load (40% by the steam dump system and 10% by the control rods). The steam dump steam flow capacity is 40% of full-load steam flow at full-load steam pressure.

If the difference between the reference T_{avg} (T_{ref}) based on turbine impulse chamber pressure and the lead/lag compensated median T_{avg} exceeds a predetermined amount and the interlock mentioned below is satisfied, a demand signal will actuate the steam dump to maintain the reactor coolant system temperature within control range until a new equilibrium condition is reached.

To prevent the actuation of steam dump on small-load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure. It is provided to unblock the dump valves when the rate of load rejection exceeds a preset value corresponding to a 10% step-load decrease or a sustained ramp-load decrease of 5% per minute.

A block diagram of the steam dump control system is shown in Figure 7.7-12.

7.7.1.8.1 Load Rejection Steam Dump Controller

This circuit prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is a difference between the lead/lag compensated median T_{avg} and the reference T_{avg} based on turbine impulse chamber pressure.

The T_{avg} signal is the same as that used in the reactor coolant system. The lead/lag compensation for the T_{avg} signal is to compensate for lags in the plant thermal response and in valve positioning. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase, thus generating an immediate demand signal for steam dump. Since control rods are available in this situation, steam dump terminates as the error comes within the maneuvering capability of the control rods.

7.7.1.8.2 Turbine Trip Steam Dump Controller

Following a turbine trip, as monitored by the turbine trip signal, the load rejection steam dump controller is defeated and the turbine trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the lead/lag compensated median T_{avg} and the no-load reference T_{avg} . When the error signal exceeds a predetermined setpoint, the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude, indicating that the reactor coolant system T_{avg} is being reduced toward the reference no-load value, the dump valves are modulated by the plant trip controller to regulate the rate of decay heat removal and thus gradually establish the equilibrium hot-shutdown condition.

The error signal determines whether a group of valves is to be tripped open or modulated open. In either case, they are modulated when the error is below the trip-open setpoints.

7.7.1.8.3 Steam Header Pressure Controller

The main steam header pressure is maintained by the steam generator pressure controller (manually selected) that controls the amount of steam flow to the condensers. This controller operates the steam dump valves to the condensers. The controller can automatically control the steam dump valves to maintain the desired steam header pressure, or the dump valves can be manually controlled in this mode.

7.7.1.9 Incore Instrumentation

The incore instrumentation system consists of Chromel-Alumel thermocouples at fixed core outlet positions and movable miniature neutron detectors that can be positioned at the center of selected fuel assemblies, anywhere along the length of the fuel assembly vertical axis. The basic system for the insertion of these detectors is shown in Figure 7.7-13. Sections 1 and 2 of Reference 3 outline the incore instrumentation system in more detail.

7.7.1.9.1 Thermocouples

The 51 Chromel-Alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies and terminate at the exit flow end of the fuel assemblies. The thermocouples are provided with a compression seal from conduit to head. The thermocouples are supported in guide tubes in the upper core support assembly.

7.7.1.9.2 Movable Neutron Flux Detector Drive System

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. See Reference 3 for neutron flux detector parameters. The stainless steel detector shell is welded to the leading end of helical wrap drive cable and to stainless-steel-sheathed coaxial cable. The retractable thimbles, into which the miniature detectors are driven, are pushed into the reactor core through conduits that extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table.

The thimbles are closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal line. During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal table is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of drive assemblies, 5-path rotary transfer operation selector assemblies, and 10-path rotary transfer selector assemblies, as shown in Figure 7.7-13. These assemblies are described in Reference 3. The drive system pushes hollow helical wrap drive cables into the core with the miniature

detectors attached to the leading ends of the cables and small-diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor that pushes a helical wrap drive cable and a detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

The leakage detection and gas purge provisions are discussed in Reference 3.

Manual isolation valves (one for each thimble) are provided for closing the thimbles. When closed, the valve forms a 2500-psig barrier. The manual isolation valves are not designed to isolate a thimble while a detector/drive cable is inserted into the thimble. The detector/drive cable must be retracted to a position above the isolation valve before closing the valve.

A small leak would probably not prevent access to the isolation valves; thus, a leaking thimble could be isolated during a hot shutdown. A large leak might require cold shutdown for access to the isolation valve.

7.7.1.9.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The control system consists of two sections, one physically mounted with the drive units, the other contained in the control room. Limit switches in each transfer device provide feedback of path selection operation. Each gearbox drives an encoder for position feedback. One five-path operation selector is provided for each drive unit to insert the detector in one of five functional modes of operation. A common path is provided to permit cross-calibration of the detectors.

A 10-path rotary transfer assembly is a transfer device that is used to route a detector into any one of up to 10 selectable paths.

The control room contains the necessary equipment for control, position indication, and flux recording for each detector. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting, and gain controls.

A “flux-mapping” consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from 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.

The thimbles are distributed nearly uniformly over the core with approximately the same number of thimbles in each quadrant. The number and location of these thimbles have been

chosen to permit the measurement of local to average peaking factors to an accuracy of $\pm 5\%$ (95% confidence). Measured nuclear peaking factors will be increased by 5% to allow for this accuracy. If the measured power peaking is larger than acceptable, reduced power required by Technical Specifications.

Operating plant experience has demonstrated the adequacy of the incore instrumentation in meeting the design bases stated.

7.7.1.10 Computer System

A plant computer system (PCS) is provided with each unit to assist the operator in the efficient operation of the plant. The computer's primary function is to provide the operator with additional information as to the condition of the nuclear steam supply system. It also has the capability to monitor inputs from the balance of plant systems and to alarm and log various off-normal conditions. There is no direct reactor control or protection action taken by the computer; therefore, the safety of the plant operation is not impaired by its loss.

In addition to the above operator support functions, the PCS also serves as the station's Emergency Response Facility Computer System, fulfilling the requirements of NUREG-0737, Supplement 1 and the guidance of NUREG-0696.

The following operator support and emergency response functions are performed by the PCS:

Operator Support

The PCS obtains data by scanning analog and digital sensors and processes this data to provide the operator with graphic displays, and indications, trends and logs of plant parameters and equipment status. It provides alarms for various off-normal conditions. It is also used for post-trip reviews, sequence of events recording, sensor calibration, and converting values into engineering units. Also included are reactor control and protection system supervision. Under this function are control rod cluster position deviation and deviation in redundant measurements monitoring. There are also calculations made under the nuclear steam supply system process supervision function. These calculations include reactor dynamic thermal output, steam generator total thermal output, unit net efficiency, RCS leak rate, and onsite incore data collection. Calculations performed by the PCS may be modified or added to the system from time to time under the control of an administrative procedure as operational and regulatory requirements change.

Emergency Response

The PCS host computer receives plant sensor inputs via the Validyne multiplexing system and processes this data for use in Emergency Response related indication, alarm, trending, recording, and display functions. Users of the system access this information from personal computer workstations that communicate with the host over the station's local area network and

the Corporate wide area network. Workstations dedicated to Emergency Response functions are located in the station's Main Control Room (MCR), Technical Support Center (TSC) and Local Emergency Operations Facility (LEOF) and off-site in the Corporate Emergency Operations Facility (CEOF) and Corporate Emergency Response Center (CERC). The PCS supports the following functions related to Emergency Response:

- SPDS (Safety Parameter Display System)
- NRC ERDS (Emergency Response Data System)
- MIDAS (Meteorological Information Dose Assessment System)
- Monitoring of certain Regulatory Guide 1.97 variables

7.7.1.11 Process Instrumentation

Much of the process instrumentation that has been provided is described in Section 7.2, and Section 7.3. The remaining portion of the process instrumentation that is not safety-related is shown on the system flow diagrams included in the appropriate sections of this report. System flow diagrams serve as piping and instrumentation diagrams (P&IDs) and illustrate the operations and processes of the various auxiliary systems. The instrument application portion of each auxiliary system section describes the process instrumentation provided for monitoring and automatically controlling that system.

The Westinghouse test program, designed to demonstrate that adequate physical separation exists between safety-related and non-safety-related portions of the 7300 Series process analog system, is described in Reference 4. The tests conclusively demonstrate that automatic actuation of the safety systems is ensured even if called on to function at a time when severe abnormal electrical conditions existed on system cabling in the balance of plant.

The lead/lag amplifier cards have been retrofitted to improve performance. This modification was to prevent the perturbation of the card output due to a step change in the power supply voltage.

7.7.1.12 Control Stations

The control room, located in the service building, contains all controls and instrumentation necessary to start up, operate, or shut down both units. All pertinent interrelated information required for the safe and reliable operation of the plant, including periods of transient and accident conditions, is presented there. If this area becomes inaccessible, the reactors can be brought to and maintained in a hot-shutdown condition at the auxiliary shutdown control panels located in the relay rooms below the main control room. The control room is shown in Figure 1.2-3 and Reference Drawing 1.

7.7.1.12.1 Design Basis

The main control room contains controls and instrumentation necessary for monitoring the operation of the reactors and turbine generators under normal and accident conditions. Continuous surveillance under all operating conditions and the postulated design-basis accident (DBA) conditions is provided by licensed operators.

The main control room has four independent communication systems. One system consists of standard commercial telephones (PBX system) using leased lines. 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 that interconnects the entire station and is supplied from the vital power system. In order to ensure that portable radios can be used following a fire in any area of the plant, an additional emergency communications system has been installed. This additional system is located in separate fire areas from the existing system and consists of repeaters, handsets, antennas, hand held radios, and associated equipment. The fourth system is sound powered, with telephone jacks and interconnecting wires at each major control point for test and maintenance purposes. Sound-powered telephones are installed at various stations throughout the plant. This system is accessible so that roving operators or service personnel may have easy communication with the main control room or one another. The sound-powered communication system does not rely on any power source, so it is available at all times. The communication systems are described in detail in Section 9.5.2.

Sufficient shielding, distance, and structural integrity are provided to ensure that control room personnel shall not be subjected to doses that in the aggregate would exceed suggested limits in 10 CFR 50 Appendix A, GDC 19 as revised for AST. All equipment in this area has been designed to minimize the possibility of a condition that could lead to inaccessibility or evacuation.

A 1-hour supply of breathing-quality air is available for the main control room from high-pressure air cylinders. After this air supply is depleted, an emergency ventilation system with HEPA/charcoal filters is available to supply breathing air indefinitely.

The auxiliary shutdown control panels, also highly protected, are designed with a minimum of simple control actions required to bring and maintain the reactor in a hot-shutdown condition. See Section 7.4 for details of the auxiliary shutdown control panels.

7.7.1.12.2 Design Description

The primary objectives of the main 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 main control room is arranged with consideration given to the fact that certain systems normally require more operator attention than do others. The main control board

is the central item in the main control room. The control board for Unit 1 is completely independent of the control board for Unit 2. Completely separate systems, circuits, instruments, power supplies, cabling panels, racks, and control boards are provided for Unit 2, except for certain shared auxiliary systems.

The design criteria for maintaining separation and independence of the systems associated with Unit 1 from those of Unit 2 in the main control room are the observance of a minimum physical separation of 4 ft. 0 in. for the independent systems. The shared systems are considered as part of Unit 1 and the following criteria apply:

1. The design criteria for maintaining separation and independence of all safety-related redundant systems, instruments, power supplies, and cabling that share a common panel or control board are to provide a spacing of 12 inches or a physical barrier between the redundant components. Studies of the main control room and control boards were made to arrive at the optimum arrangement for the operation of the station while meeting the criteria for separation.
2. All redundant systems located in separate panels, racks, or control boards in the control area are separated by either a space of 12 inches between redundant components or physical barriers.

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 which is immediately needed in cases of emergency, are either mounted on the bench console or vertical 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 main control room where their use simplifies the control of certain auxiliary systems or for systems that require less frequent operator attention such as turbine supervisory, 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 alarms are initiated automatically by the radiation monitoring system on high-radiation levels. Audible alarms also sound in appropriate areas through the station if high-radiation conditions are present.

Design specifications for the equipment in the main control room specify no loss of protective function over the temperature range from 40°F to 120°F. Thus, there is a wide margin

between design limits and the normal operating environment for control room equipment. If only one of the four control room cooling units remains operable, the common control room temperature will level off under 90°F. The electronic equipment was tested at the factory for the design temperature range of 40°F to 110°F. Qualification testing has demonstrated that the instrumentation remains operable to 120°F, as there is a possible calibration shift above this range. The 120°F limit establishes the maximum temperature at which plant shutdown is required. As the control room latent heat is negligible, humidity is not a factor. A double failure (both conditioning systems 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 shut down the reactor. Onsite testing proved 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 the operation of safety functions at elevated ambient temperatures to 120°F for control room equipment and in full postaccident environment for required equipment in the containment.

Detailed results of some of these tests are proprietary to the supplier, but are on file at the supplier and available for audit by qualified parties.

A reliable source of electrical power, described in Section 8.3, is provided to ensure continual operation of vital unit and station instrumentation. Emergency lighting is also provided.

7.7.1.13 Control Room Availability

The main control room is designed to be available at all times. Safe occupancy of the main control room during an abnormal condition is provided for in the design of the service building. Two carbon dioxide monitors have been installed to verify carbon dioxide levels in the control rooms are at accepted habitability limits. One monitor is installed in Unit 1 control room and one is installed in Unit 2 control room. Adequate shielding and air conditioning are used to maintain tolerable radiation and air temperature levels in the main 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 are isolated as required. Outside air is automatically isolated upon an SI signal. Makeup air, under emergency conditions, is immediately available from a compressed breathing-air bank and, on exhaustion, from emergency ventilating units supplying air through HEPA and charcoal filters to remove particulates and iodine, respectively. With all outside air makeup shut off, the quality of the air will be maintained with the compressed air bank or the filtered emergency ventilation with an emergency ventilation fan/filter operating in recirculation.

Incorporated in the control room design are provisions to limit the possibility and potential magnitude of a fire.

If a fire should occur in the main control room, it is expected to be only minor in magnitude so that it could be readily extinguished by underfloor gas flooding or a hand fire extinguisher. Smoke and vapors can be removed by the ventilation system during normal operations. If venting is undesirable in any emergency, breathing apparatus is available for use. The main control room and auxiliary shutdown control panels are protected from outside fire, smoke, or airborne radioactivity by sealed penetrations, weather-stripped doors, absence of windows, and by the positive air pressure maintained in the area during normal and emergency operations.

7.7.1.13.1 Auxiliary Shutdown Control Panels

The probability of the main control room becoming inaccessible as a result of fire or other causes is considered extremely small. However, if the operator must leave the main 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 shutdown control panels. Each reactor unit can be brought to and maintained in a hot-shutdown condition from the auxiliary shutdown control panels, which are provided with the following 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 on the auxiliary shutdown control panels. The auxiliary shutdown control panel instrumentation measurement range is shown in Table 7.7-2. This equipment is sufficient to safely maintain the unit or units for an extended period of time in a hot-standby condition.

Each auxiliary shutdown control panel has the following equipment:

1. No. 2 auxiliary feedwater pump turbine steam supply valve control switches.
2. No. 3A auxiliary feedwater pump motor start-stop control switch.
3. No. 3B auxiliary feedwater pump motor start-stop control switch.
4. Pneumatic hand-control valves—auxiliary feed pump discharge open-close control stations (Reference 3).
5. Steam generator 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. Nos. 2A and 2B boric acid pump motor start-stop control switches (Unit 1).
10. Nos. 2C and 2D boric acid pump motor start-stop control switches (Unit 2).
11. Motor-operated valves—auxiliary feedwater pump discharge open-close control switch (Reference 4).
12. Transfer switches for all the above valve and pump motors.
13. Status lights for all the above pump motors and valve positions.
14. Charging flow indicator.
15. T_{avg} indicator for each loop.
16. Condensate storage tank level indicator.
17. Pressurizer pressure indicators.
18. Pressurizer level indicators.
19. Pressurizer heater control switch.
20. Sound-powered telephone between auxiliary shutdown control panels and all areas, including the following:
 - a. Switchgear room.
 - b. Emergency switchgear room.
 - c. Auxiliary building at the Emergency boration line motor-operated valve.
 - d. Auxiliary feedwater pumphouse
21. Power relief valves (PCV-MS101-A, B, C) (3) hand-indicating control station with transfer capability.
22. Indication of pressure difference between the turbine building and the relay room.
23. Charging flow manual station.
24. Controls for letdown isolation valves.
25. Steam pressure for each steam generator.
26. Auxiliary feedwater pump discharge pressure.
27. Relay room emergency ventilation for control and damper position indication.

7.7.1.13.2 Auxiliary Monitoring Panels

Two additional monitoring panels have been added in the fuel building. These provide instrumentation to be used in conjunction with the auxiliary shutdown control panel to safely shut down the reactor in accordance with 10 CFR 50 Appendix R (Section 9.5.1).

Auxiliary monitoring panel 2-EI-CB-97A supplies Unit 1 and 2 indication of the following parameters:

- Pressurizer level
- Pressurizer pressure
- Reactor coolant system hot leg temperature

This panel can be powered from either the Unit 1 or the Unit 2 emergency power system.

Auxiliary monitoring panel 1-EI-CB-203 supplies Unit 1 and 2 indication of the following parameters:

- Steam generator wide range level
- Reactor coolant system cold leg temperature
- Wide and source range excore neutron flux

Redundant steam generator wide range level and reactor coolant cold leg temperature indicators are supplied to provide greater system reliability.

Power for the steam generator wide range level and the reactor coolant system cold leg temperature instrumentation for Unit 1 is supplied by the Unit 2 emergency power system. Conversely, the steam generator wide range level and the reactor coolant system cold leg temperature instrumentation for Unit 2 is supplied by the Unit 1 emergency power system. This was done to ensure that power will be available to the instrumentation of the affected unit following a fire in that units emergency switchgear room, cable tunnel, or cable vault.

The Unit 1 excore neutron flux monitor system is normally supplied from the Unit 1 emergency power system. A transfer switch on the Unit 2 emergency switchgear room isolation panel is used to transfer power for one train of the system from the Unit 1 to the Unit 2 emergency power system. The Unit 2 excore neutron flux monitor system is powered in a similar manner.

7.7.1.13.3 Pump Operation at Emergency Switchgear

The provisions of 10 CFR 50 Appendix R on alternative and dedicated shutdown capability include requirements for achieving cold shutdown conditions within 72 hours. In order to reach cold shutdown one pump from the service water system, one pump from the component cooling water system, and one pump from the residual heat removal system are required for each reactor unit in operation. These pumps are normally controlled from the control room.

In the event of a control room evacuation the capability to isolate damaged control circuits and to operate the pumps in these systems from the emergency switchgear room has been incorporated by the installation of a transfer switch and a control switch on each pumps breaker compartment at the switchgear.

7.7.1.13.4 System Evaluation

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

7.7.1.14 ATWS Mitigation System Description

The anticipated Transient Without Scram (ATWS) Mitigation System (AMSAC) is a diverse control system which initiates turbine trip and auxiliary feedwater system flow upon detection of an ATWS type event. An ATWS event is described as a postulated operational occurrence or a transient such as a loss of feedwater, loss of condenser vacuum, or other design basis event coincident with a failure of the reactor protection system to shut down or scram the reactor. The AMSAC is diverse from the reactor protection system from field sensor output to, but not including, the actuation devices, except for the reactor trip via the motor generator set input breakers which is a diverse actuation device.

The AMSAC initiates a reactor trip, turbine trip, and auxiliary feedwater flow (pumps start) upon detection of steam generator level less than its setpoint on any two out of three level channels on any two out of three steam generators, with turbine load greater than setpoint, permissive C-20 satisfied.

The AMSAC generic design specified in Reference 5 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 5 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 5 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. 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 those 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 normal feedwater ATWS event have shown that for a C-20 setpoint corresponding to 50% rated thermal power, the voiding that

would occur without AMSAC was still less than that expected for the full power case with AMSAC (Reference 6).

Therefore the current North Anna AMSAC design meets its design basis, provided AMSAC is armed at $\leq 40\%$ turbine load (nominal) or $\leq 50\%$ rated thermal power.

The steam generator level signals are wired from isolated outputs in the Westinghouse solid state protection racks. The steam generator level signals are from the narrow range channels I, II, and III of each steam generator. The turbine load signals are wired from the redundant turbine impulse chamber pressure channels III and IV.

The input signals are wired to three programmable logic controllers (PLC) located in the AMSAC panel. These signals are isolated with class 1E qualified devices in the 7300 System to provide signals to the PLCs. One PLC is dedicated to each steam generator. The two turbine impulse chamber pressure signals are wired to each PLC. The PLCs perform timing, logic functions, and provide outputs to the various loads. The outputs to safety-related circuits are wired through safety-related qualified class 1E isolation relays. The AMSAC panel is located in the Instrument Rack Room. The AMSAC panel is powered from the TSC Uninterruptible Power Supply (UPS), using a new breaker in UPS Distribution Subpanel A.

The AMSAC is initiated when the turbine load is greater than setpoint and a complete loss of feedwater is detected. Loss of feedwater is the condition of any two of the three level transmitters in any 2 out of 3 steam generators less than or equal to setpoint of narrow range level span. The PLCs perform a time delay to allow the existing Reactor Protection System (RPS) to respond first.

In the event of an ATWS and the expiration of the time delay, the main turbine will be tripped, all three auxiliary feedwater pumps will receive signals to start, the steam generator blowdown isolation and sample isolation valves will receive automatic close signals, and the breakers which supply power for each rod control motor-generator set will be provided trip signals.

ATWS mitigation by AMSAC is automatically blocked below the setpoint power by permissive (C-20) that is derived from the First Stage Pressure (FSP) transmitters. This automatic block will be defeated for approximately 360 seconds following a decrease of FSP below its setpoint. This time delay will be required for the instance wherein an ATWS event occurs and the turbine load reduces causing FSP to drop. The ATWS mitigating actions, AMSAC, will still be initiated automatically if a loss of heat sink (steam generator inventory loss) occurs within the 360-second time delay.

7.7.2 Analysis

The plant control systems are designed to ensure high reliability in any anticipated operational occurrences. Equipment used in these systems is designed and constructed to maintain a high level of reliability.

Proper positioning of the control rods is monitored in the control room by bank arrangements of the individual rod position indicators for each rod cluster control assembly. A rod deviation alarm alerts the operator of a deviation of one rod cluster control assembly from the other rods in that bank position. There are also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the control room for each full-length rod cluster control assembly. Four ex-core long ion chambers also detect asymmetrical flux distribution indicative of rod misalignment.

Overall reactivity control is achieved by the combination of soluble boron and rod cluster control assemblies. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short-term reactivity control for power changes is accomplished by the plant control system that automatically moves rod cluster control assemblies. This system uses input signals including neutron flux, coolant temperature, and turbine load.

The plant control systems will prevent an undesirable condition in the operation of the plant that, if reached, will be protected by reactor trip. The description and analysis of this protection is covered in Section 7.2. Worst-case failure modes of the plant control systems are postulated in the analysis of off-design operational transients and accidents covered in Chapter 15, such as the following:

1. Uncontrolled rod cluster control assembly withdrawal from a subcritical condition.
2. Uncontrolled rod cluster control assembly withdrawal at power.
3. Rod cluster control assembly misalignment.
4. Loss of external electrical load and/or turbine trip.
5. Loss of all ac power to the station auxiliaries (station blackout).
6. Excessive heat removal because of feedwater system malfunctions.
7. Excessive load increase.
8. Accidental depressurization of the reactor coolant system.

These analyses show that a reactor trip setpoint is reached in time to protect the health and safety of the public under these postulated incidents and that the resulting coolant temperatures produce a DNBR well above the DNBR Design Limit. Thus, there will be no cladding damage and no release of fission products to the reactor coolant system under the assumption of these postulated worst-case failure modes of the plant control system.

7.7.2.1 Separation of Protection and Control Systems

In some cases, it is advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Accordingly, this

postulated failure mode meets the requirements of General Design Criterion 24 (1971 criteria). Test results have shown that a short circuit, open circuit, or the application of 120V ac or 140V dc on the isolated output portion of the circuit (i.e., the nonprotective side of the circuit) will not affect the input (protective) side of the circuit.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action, and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action even when degraded by a second random failure. This meets the applicable requirements of Section 4.7 of IEEE Std 279-1971. An exception to these requirements is justified in Section 7.2.2.3.5.

The pressurizer pressure channels needed to derive the control signals are physically isolated from the pressure channels used to derive protection signals.

Channels of the nuclear instrumentation that are used in the protective system are combined to provide nonprotective functions such as signals to indicating or recording devices; the required signals are derived through isolation amplifiers. These isolation amplifiers 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 protection side of the circuit. As such, failures on the nonprotective side of the system will not affect the individual protection channels.

7.7.2.2 Reactivity Control Considerations

Reactor shutdown with control rods is completely independent of the control functions since the trip breakers interrupt power to the rod drive mechanisms regardless of existing control signals. The design is such that the system can withstand accidental withdrawal of control groups or unplanned dilution of soluble boron without exceeding acceptable fuel design limits. Thus, the design meets the applicable requirements of General Design Criterion 25 (1971 criteria).

No single electrical or mechanical failure in the rod control system could cause the accidental withdrawal of a single rod cluster control assembly from the partially inserted bank at full-power operation. The operator could deliberately withdraw a single rod cluster control assembly in the control bank; this feature is necessary in order to retrieve a rod, should one be accidentally dropped. In the extremely unlikely event of simultaneous electrical failures that could result in single withdrawal, rod deviation would be displayed on the plant annunciator, and the rod position indicators would indicate the relative positions of the rods in the bank. The withdrawal of a single rod cluster control assembly by operator action, whether deliberate or by a combination of errors, would result in the activation of the same alarm and the same visual indications.

Each bank of control and shutdown rods in the system is divided into two groups of four mechanisms each. The rods comprising a group operate in parallel through multiplexing thyristors. The two groups in a bank move sequentially such that the first group is always within one step of the second group in the bank. A definite schedule of actuation or deactuation of the

stationary gripper, movable gripper, and lift coils of a mechanism is required to withdraw the rod cluster control assembly attached to the mechanism. Since the four stationary gripper, movable gripper, and lift coils associated with the rod cluster control assemblies of a rod group are driven in parallel, any single failure that could cause rod withdrawal would affect a minimum of one group of rod cluster control assemblies. Mechanical failures are in the direction of insertion, or immobility.

The identified multiple failure involving the least number of components consists of open-circuit failure of the proper 2 out of 16 wires connected to the gate of the lift coil thyristors. The probability of open-wire (or terminal) failure is $0.016 \times 10^{-6}/\text{hr}$ by MIL-HBD-217A. These wire failures would have to be accompanied by the failure or disregard of the indications mentioned above. The probability of this occurrence is therefore too low to have any significance.

To erroneously withdraw a single rod cluster control assembly, the operator would have to improperly set the bank selector switch, the lift coil disconnect switches, and the in-hold-out switch. In addition, the three indications would have to be disregarded or ineffective. Such a series of errors would require a complete lack of understanding and administrative control. A probability number cannot be assigned to a series of errors such as this. Such a number would be highly subjective.

The rod position indication system provides direct visual displays of each control rod assembly position. The plant computer alarms for the deviation of rods from their banks. In addition, a rod insertion limit monitor provides an audible and visual alarm to warn the operator of an approach to an abnormal condition due to dilution. The low-low insertion limit alarm alerts the operator to initiate boration to restore shutdown margin in accordance with the plant procedures. The facility reactivity control systems are such that acceptable fuel damage limits will not be exceeded even in the event of a single malfunction of either system.

An important feature of the control rod system is that insertion is provided by gravity fall of the rods.

In all analyses involving reactor trip, the single, highest-worth rod cluster control assembly is postulated to remain untripped in its full-out position.

One means of detecting a stuck control rod assembly is available from the actual rod position information displayed on the control board. The control board position readouts, one for each full-length rod, give the plant operator the actual position of the rod in steps. The indications are grouped by banks (e.g., control bank A, control bank B) to indicate to the operator the deviation of one rod with respect to other rods in a bank. This serves as a means to identify rod deviation.

The plant computer monitors the actual position of all rods. Should a rod be misaligned from the other rods in that bank and approach limits specified in the Technical Specifications, the rod deviation alarm is actuated.

Misaligned rod cluster control assemblies are also detected and alarmed in the control room via the nuclear instrumentation flux tilt monitoring system, which is independent of the plant computer.

Isolated signals derived from the nuclear instrumentation system are compared with one another to determine if a preset amount of deviation of average power has occurred. Should such a deviation occur, the comparator output will operate a bi-stable unit to actuate a control board annunciator. This alarm will alert the operator to a power imbalance caused by a misaligned rod. By the use of individual rod position readouts, the operator can determine the deviating control rod and take corrective action. Thus, the design of the plant control systems meets the applicable requirements of General Design Criterion 25 (1971 criteria).

The rod system can compensate for xenon burnout reactivity transients over the allowed range of rod travel. Xenon burnout transients of larger magnitude must be accommodated by boration or by reactor trip (which eliminates the burnout). The boron system can compensate for all xenon burnout reactivity transients without exception.

The boron system is not needed to compensate for the reactivity effects of fuel and water temperature changes accompanying power level changes.

The rod system can compensate for the reactivity effects of fuel and water temperature changes accompanying power level changes over the full range from full load to no load at the design maximum load uprate. Automatic control of the rods is, however, limited to the range of approximately 15% to 100% of rating for reasons unrelated to reactivity or reactor safety.

The boron system (by the use of administrative measures) will maintain the reactor in the cold-shutdown state irrespective of the disposition of the control rods. The overall reactivity control achieved by the combination of soluble boron and rod cluster control assemblies meets the applicable requirements of General Design Criterion 26 (1971 criteria).

7.7.2.3 Step-Load Changes Without Steam Dump

The plant control system restores equilibrium conditions, without a trip, following a $\pm 10\%$ step change in load demand, over the 15% to 100% power range for automatic control. The steam dump controller is not armed for load decreases less than or equal to 10%. A load demand greater than full power is prohibited by the turbine control load limit devices.

The plant control system minimizes the reactor coolant average temperature deviation during the transient within a given value and restores average temperature to the programmed setpoint. Excessive pressurizer pressure variations are prevented by using spray, heaters, and power relief valves in the pressurizer.

The control system will limit nuclear power overshoot to acceptable values following a 10% increase in load to 100%.

7.7.2.4 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 plant. The function of the control system is to maintain the coolant average temperature as a function of turbine-generator load.

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

7.7.2.5 Load Rejection Furnished by Steam Dump System

When a load rejection occurs, if the difference between the required temperature setpoint of the reactor coolant system and the actual average temperature exceeds a predetermined amount, a signal will actuate the steam dump to maintain the reactor coolant system temperature within the control range until a new equilibrium condition is reached.

The reactor power is reduced automatically at a rate consistent with the capability of the rod control system. The steam dump flow reduction is as fast as rod cluster control assemblies are capable of inserting negative reactivity.

The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is 40% of full-load steam flow at full-load steam pressure.

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

The dump valves are modulated by the reactor coolant average temperature signal. The required number of steam dump valves can be tripped quickly to stroke full open or modulate, depending upon the magnitude of the temperature error signal resulting from the loss of load.

7.7.2.6 Turbine Trip with Reactor Trip

Whenever the turbine-generator unit trips at an operating power level above 30% power, the reactor also trips. The thermal capacity of the reactor coolant system is greater than that of the secondary system, and because the full-load average temperature is greater than the no-load temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent the actuation of steam generator safety valves for a trip from full power. This heat sink is provided by

the combination of the controlled release of steam to the condenser and by the makeup of cold feedwater to the steam generators. The trip signal interfaces are shown in Figure 7.3-2.

The steam dump system is controlled from the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. The actuation of the steam dump is rapid, to prevent the actuation of the steam generator safety valves. With the 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 bypassed.

Following the turbine trip, the feedwater flow is cut off when the average coolant temperature decreases below a given temperature or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level while ensuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected) that controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers that are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and water level fall rapidly during the transient because of coolant contraction. The pressurizer water level is programmed so that the level following the turbine and reactor trip is above the low-level safety injection setpoint. If heaters become uncovered following the trip, they are de-energized and the chemical and volume control system will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

The steam dump and feedwater control systems are designed to prevent the average coolant temperature from falling below the programmed no-load temperature following the trip, to ensure adequate reactivity shutdown margin.

7.7 REFERENCES

1. J. B. Lipchak and R. A. Stokes, *Nuclear Instrumentation System*, WCAP-7669, 1971.
2. A. E. Blanchard, *Rod Position Monitoring*, WCAP-7571, 1971.
3. J. J. Loving, *Incore Instrumentation (Flux-Mapping System and Thermocouples)*, WCAP-7607, 1971.
4. R. M. Siroky and F. W. Marasco, *Westinghouse 7300 Series Process Control System Noise Tests*, 1976.
5. M. R. Adler, *AMSAC Generic Design Package*, WCAP-10858P-A, Rev. 1, July 1987.
6. Westinghouse Technical Bulletin ESBU-TB-08, *AMSAC C-20 Interlock Permissive*, November 26, 1997.

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.	11715-FE-27B	Arrangement: Main Control Room, Elevation 276'- 9", Units 1 & 2

Table 7.7-1
PLANT CONTROL SYSTEM INTERLOCKS

Designation	Derivation	Function
C-1	1/2 neutron flux (intermediate range) above setpoint	Blocks automatic and manual control rod withdrawal
C-2	1/4 neutron flux (power range) above setpoint	Blocks automatic and manual control rod withdrawal
C-3	2/3 overtemperature delta T above setpoint	Blocks automatic and manual control rod withdrawal Actuates turbine runback via load reference
C-4	2/3 overpower delta T above setpoint	Blocks automatic and manual control rod withdrawal Actuates turbine runback via load reference
C-5	1/1 turbine impulse chamber pressure below setpoint	Blocks automatic control rod withdrawal
C-7	1/1 time derivative (absolute value) of turbine impulse chamber pressure (decrease only) above setpoint	Makes steam dump valves available for either tripping or modulation
C-8	Turbine trip, 2/3 turbine auto stop oil pressure below setpoint	Blocks steam dump control via load rejection T_{avg} controller
	or	Makes steam dump valves available for either tripping or modulation
	4/4 turbine valves closed	
	No turbine trip, 2/3 turbine auto stop oil pressure above setpoint and 1/4 turbine-inlet line stop valves not closed	Blocks steam dump control via turbine trip T_{avg} controller
C-9	Any condenser pressure above setpoint, or Three circulation water pump breakers open	Blocks steam dump to condenser
C-11	1/1 bank D control rod position above setpoint	Blocks automatic rod withdrawal
C-20	First stage pressure transmitter	Blocks AMSAC below the first stage pressure setpoint

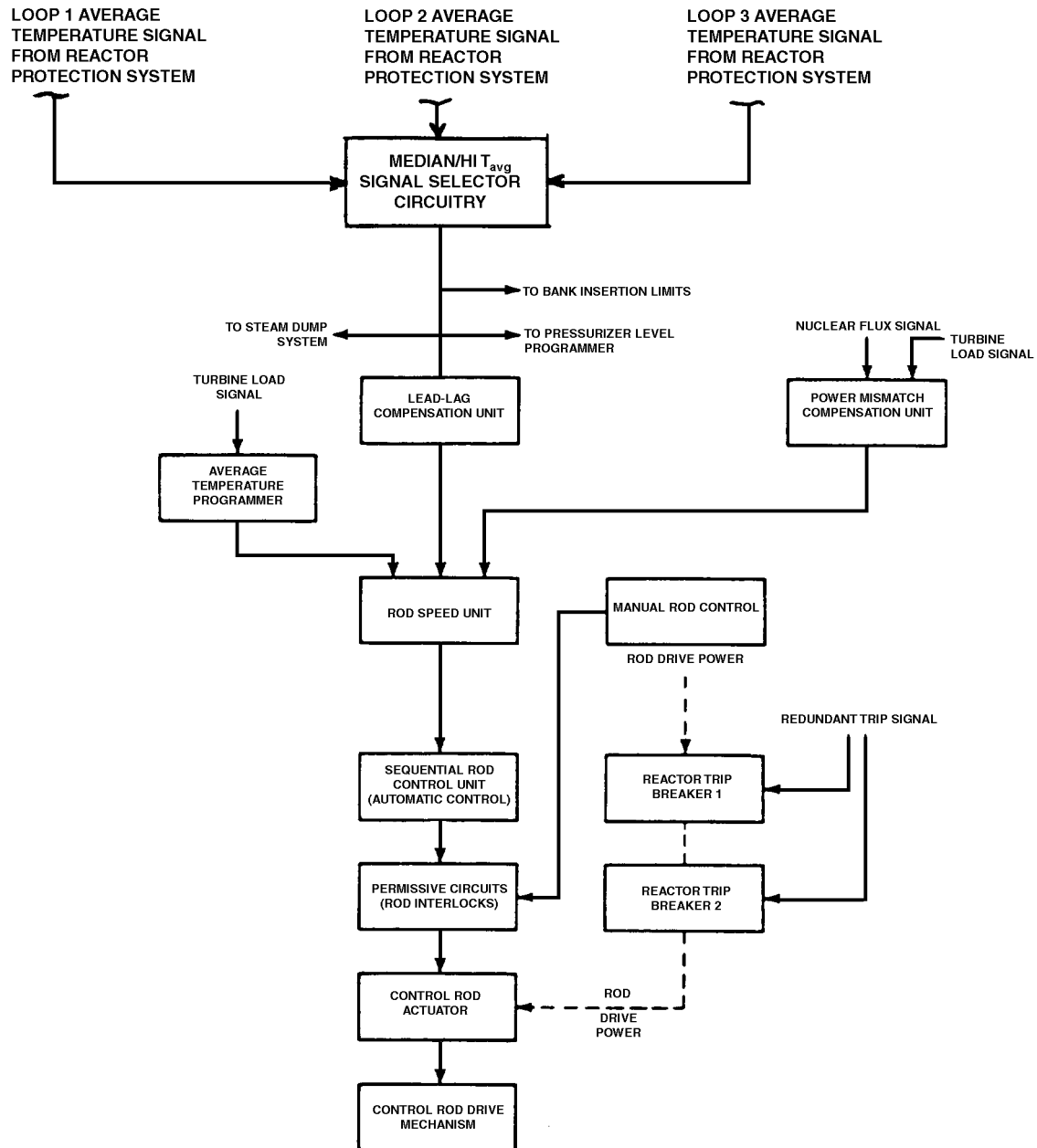
Table 7.7-2
AUXILIARY SHUTDOWN PANEL MONITORING INSTRUMENTATION^a

Instrument	Measurement Range
1. Reactor Coolant Temperature—Average	530-630°F
2. Pressurizer Pressure	1700-2500 psig
3. Pressurizer Level	0-100%
4. Auxiliary Feed Pump Discharge Header Pressure	500-1500 psig
5. Emergency Condensate Storage Tank Level	0-100%
6. Charging Flow	0-180 gpm
7. Main Steam Line Pressure	0-1400 psig
8. Steam Generator Level	0-100%
9. Relay Room Positive Ventilation	0-0.50 inches H ₂ O

a. Located at Elevation 254 in the Emergency Switchgear and Relay Room.

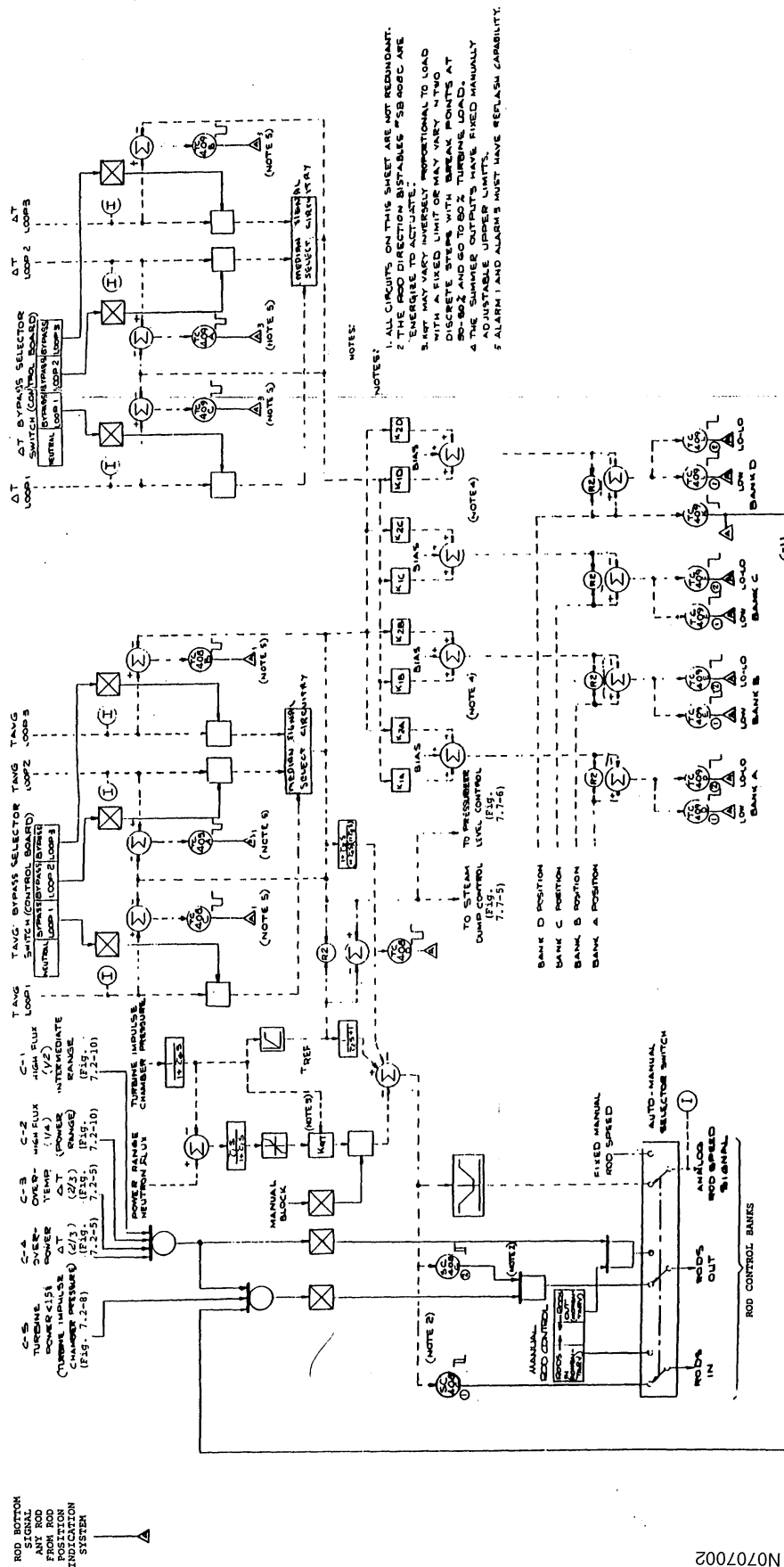
Figure 7.7-1
SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL SYSTEM

NOTES: 1. TEMPERATURES ARE MEASURED AT STEAM GENERATOR'S INLET AND OUTLET.



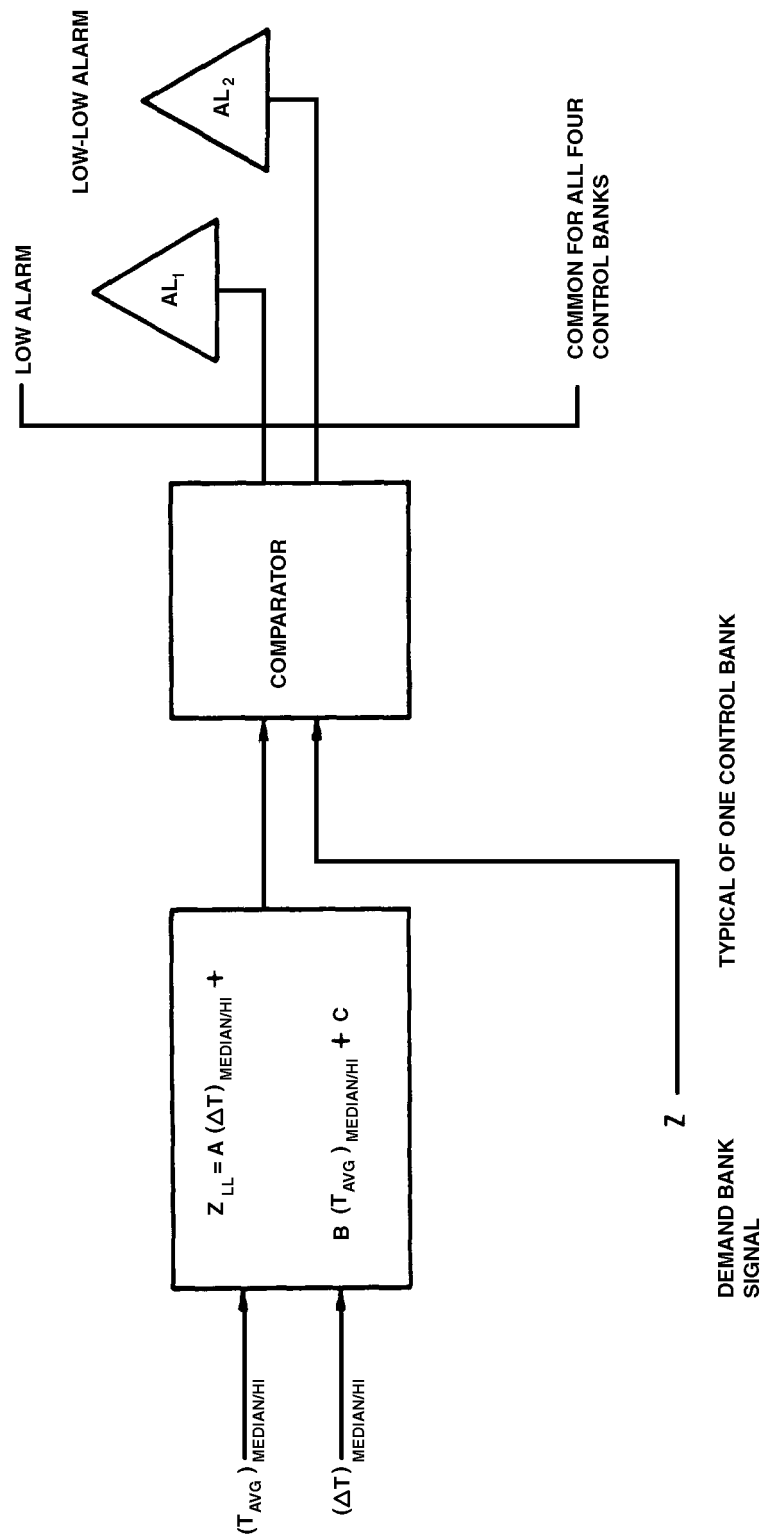
N0707001

Figure 7.7-2
ROD CONTROLS AND ROD BLOCKS



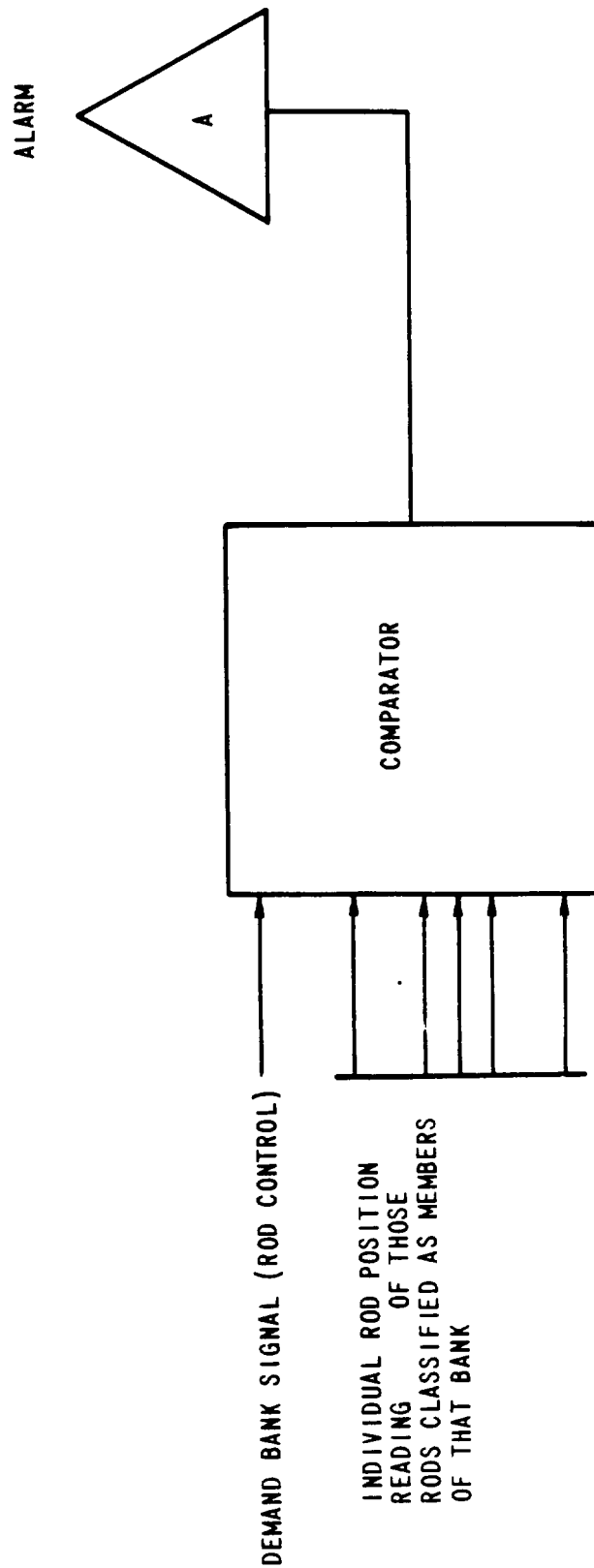
N0707002

Figure 7.7-3
CONTROL BANK ROD INSERTION MONITOR



NOTE: 1. ANALOG CIRCUITRY IS USED FOR THE COMPARATOR NETWORK
2. COMPARISON IS DONE FOR ALL CONTROL BANKS

Figure 7.7-4
ROD DEVIATION COMPARATOR



- NOTE:
1. DIGITAL OR ANALOG SIGNALS MAY BE USED FOR THE COMPARATOR COMPUTER INPUTS.
 2. THE COMPARATOR WILL ENERGIZE THE ALARM IF THERE EXISTS A POSITION DIFFERENCE GREATER THAN A PRESENT LIMIT BETWEEN ANY INDIVIDUAL ROD AND THE DEMAND BANK SIGNAL.
 3. COMPARISON IS INDIVIDUALLY DONE FOR ALL CONTROL BANKS.

NO707004

Figure 7.7-7
PRESSURIZER HEATER CONTROL

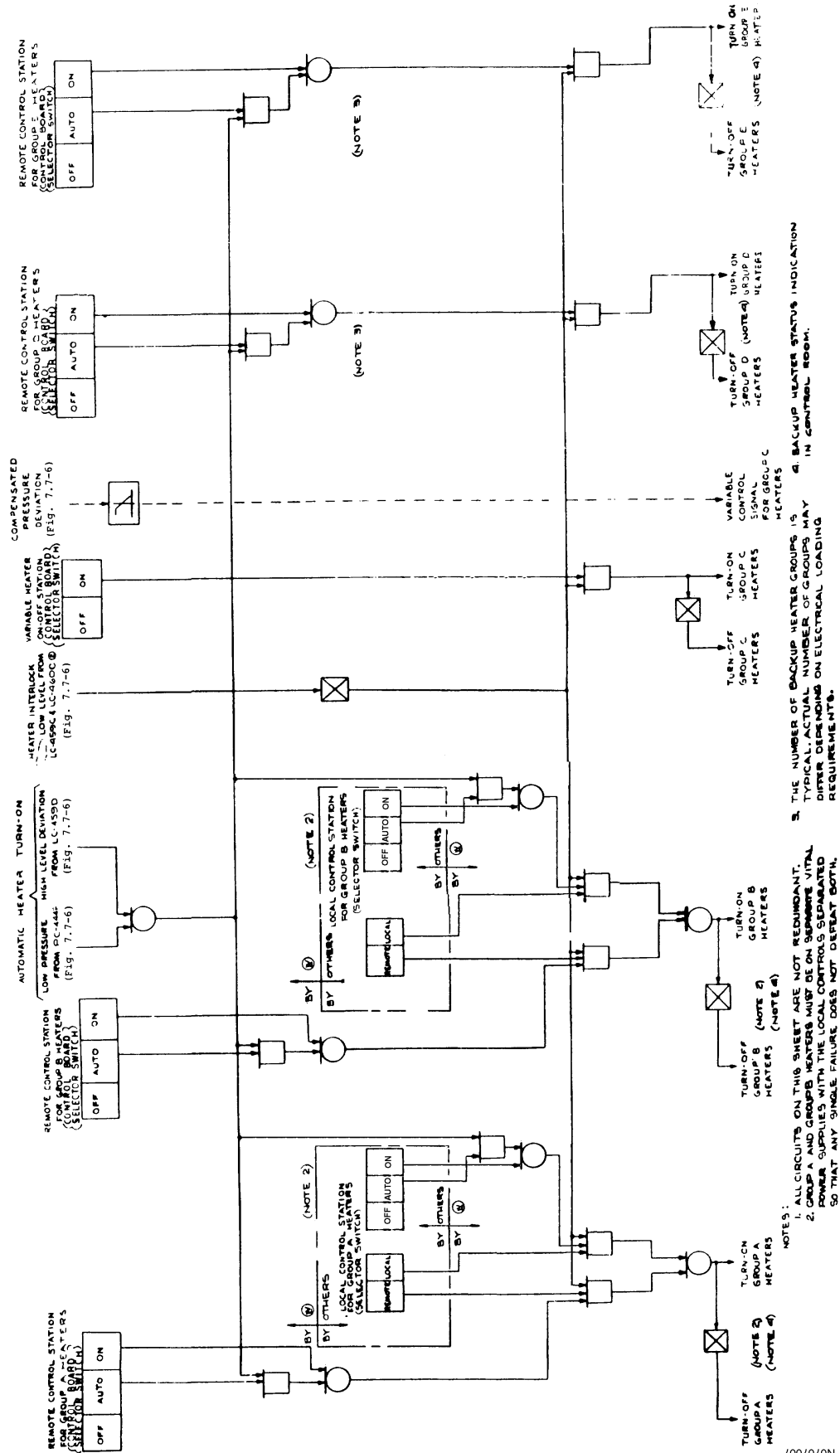
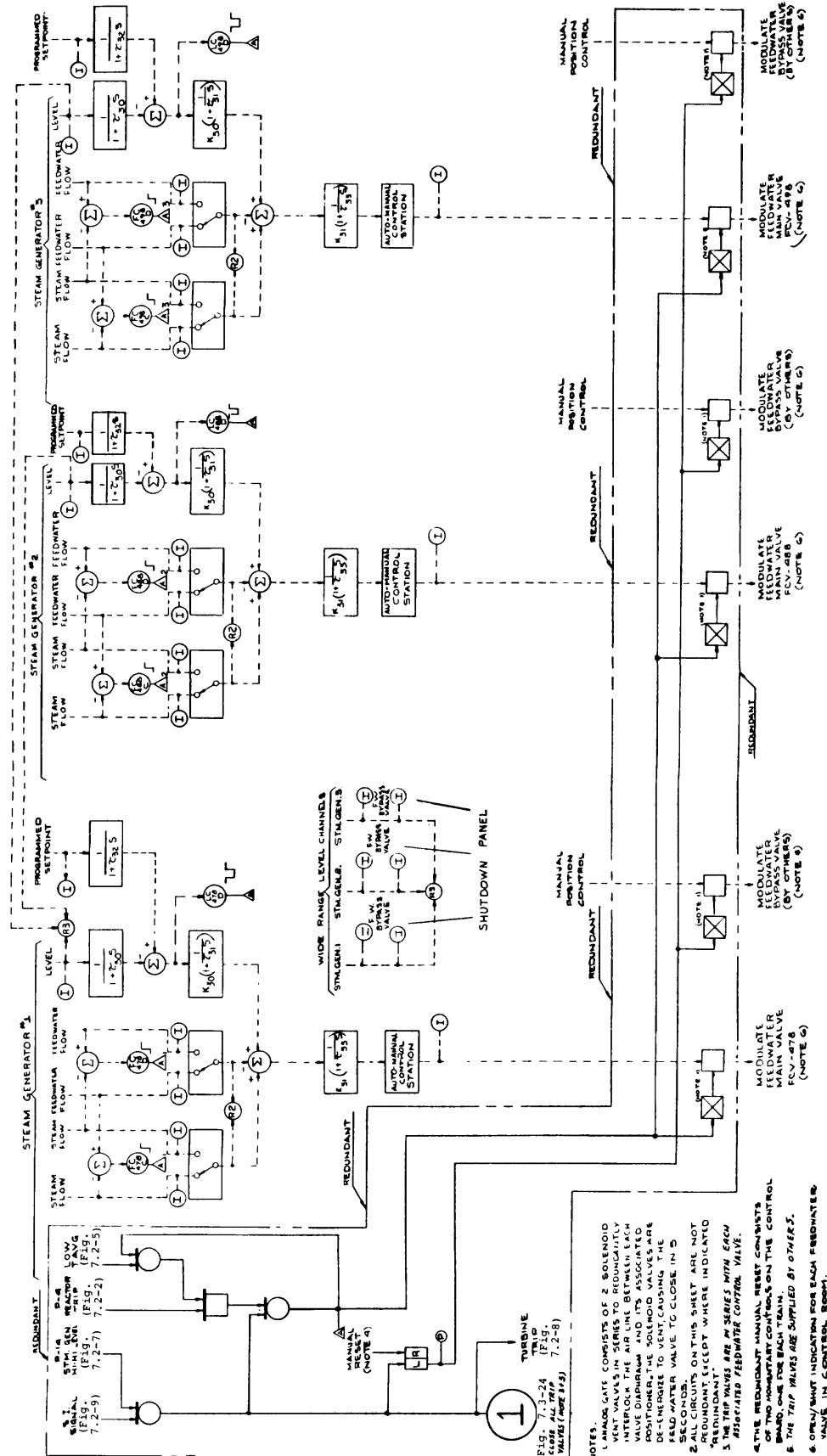


Figure 7.7-8
FEEDWATER CONTROL AND ISOLATION



N0707008

Figure 7.7-9
BLOCK DIAGRAM OF PRESSURIZER PRESSURE CONTROL SYSTEM

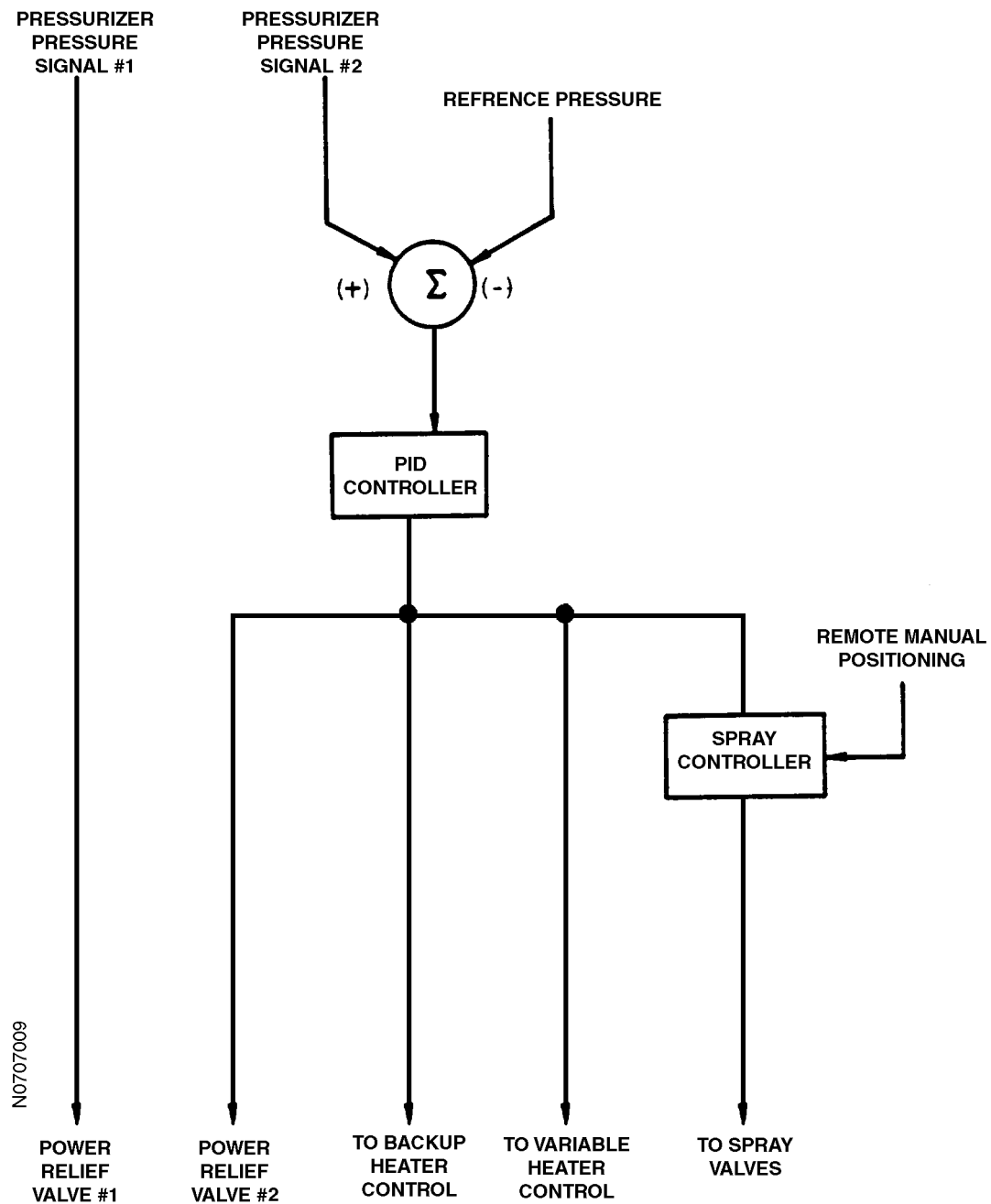


Figure 7.7-10
BLOCK DIAGRAM OF PRESSURIZER LEVEL CONTROL SYSTEM

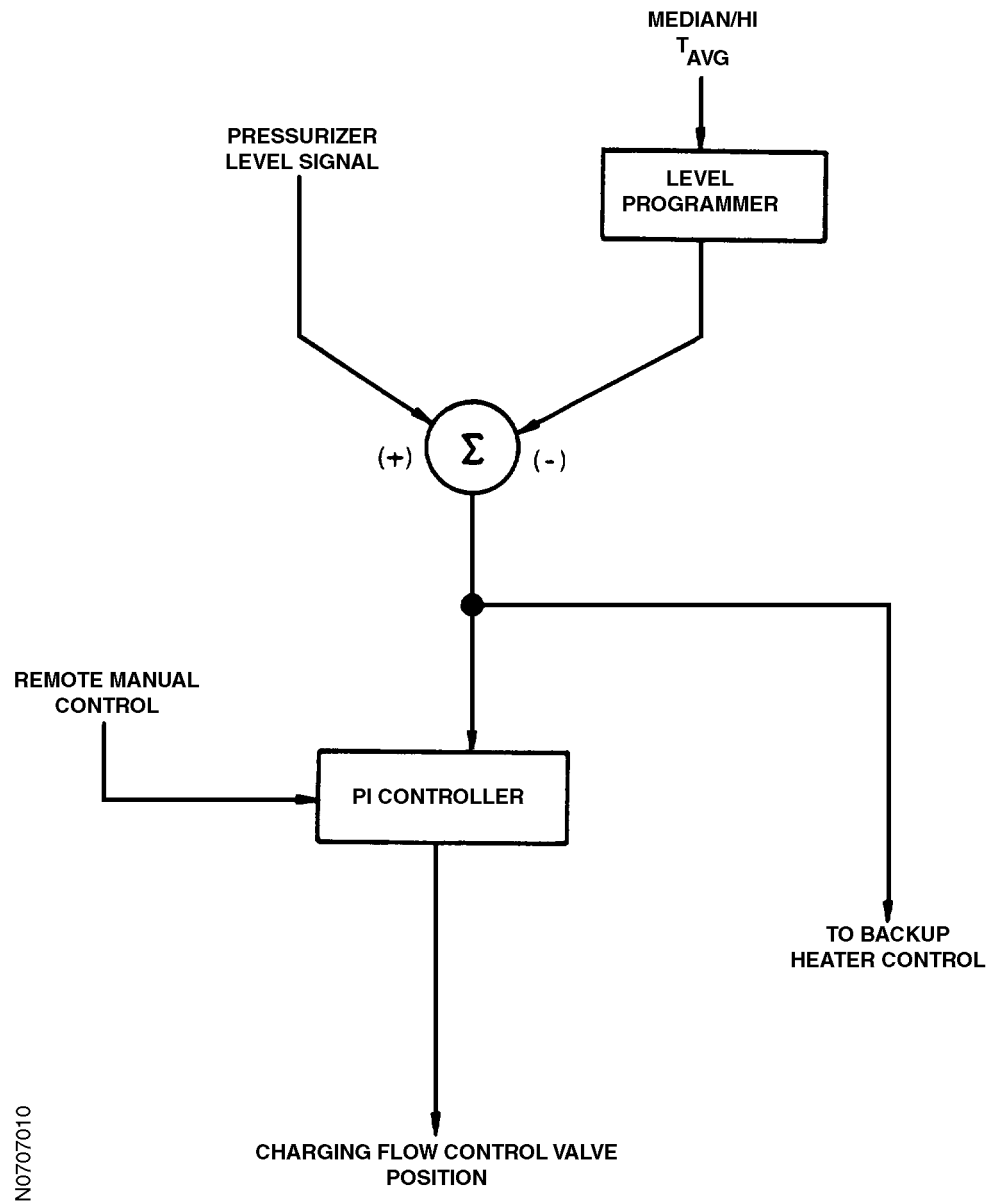


Figure 7.7-11
BLOCK DIAGRAM OF STEAM GENERATOR WATER LEVEL CONTROL SYSTEM

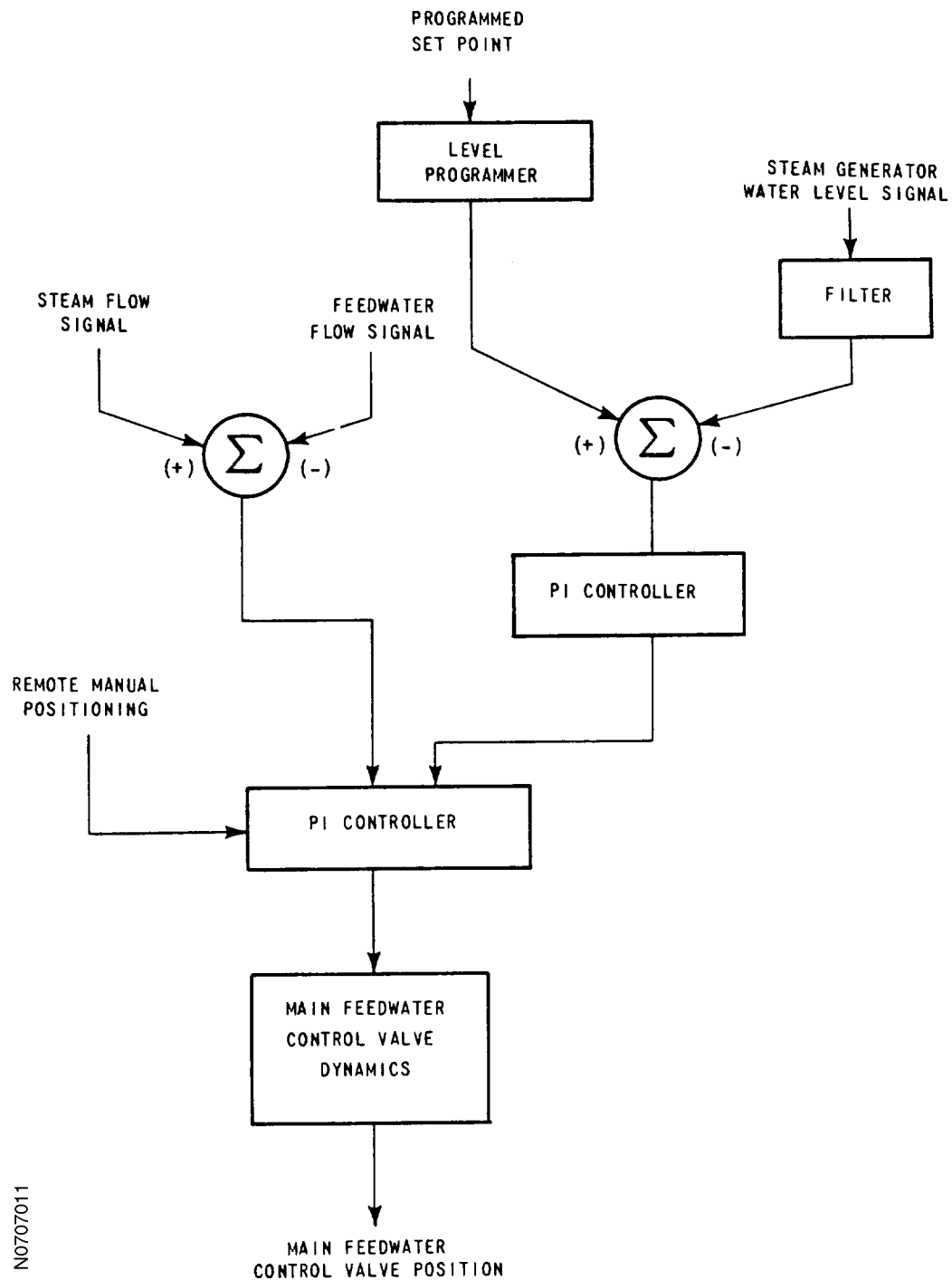


Figure 7.7-12
BLOCK DIAGRAM OF STEAM DUMP CONTROL SYSTEM

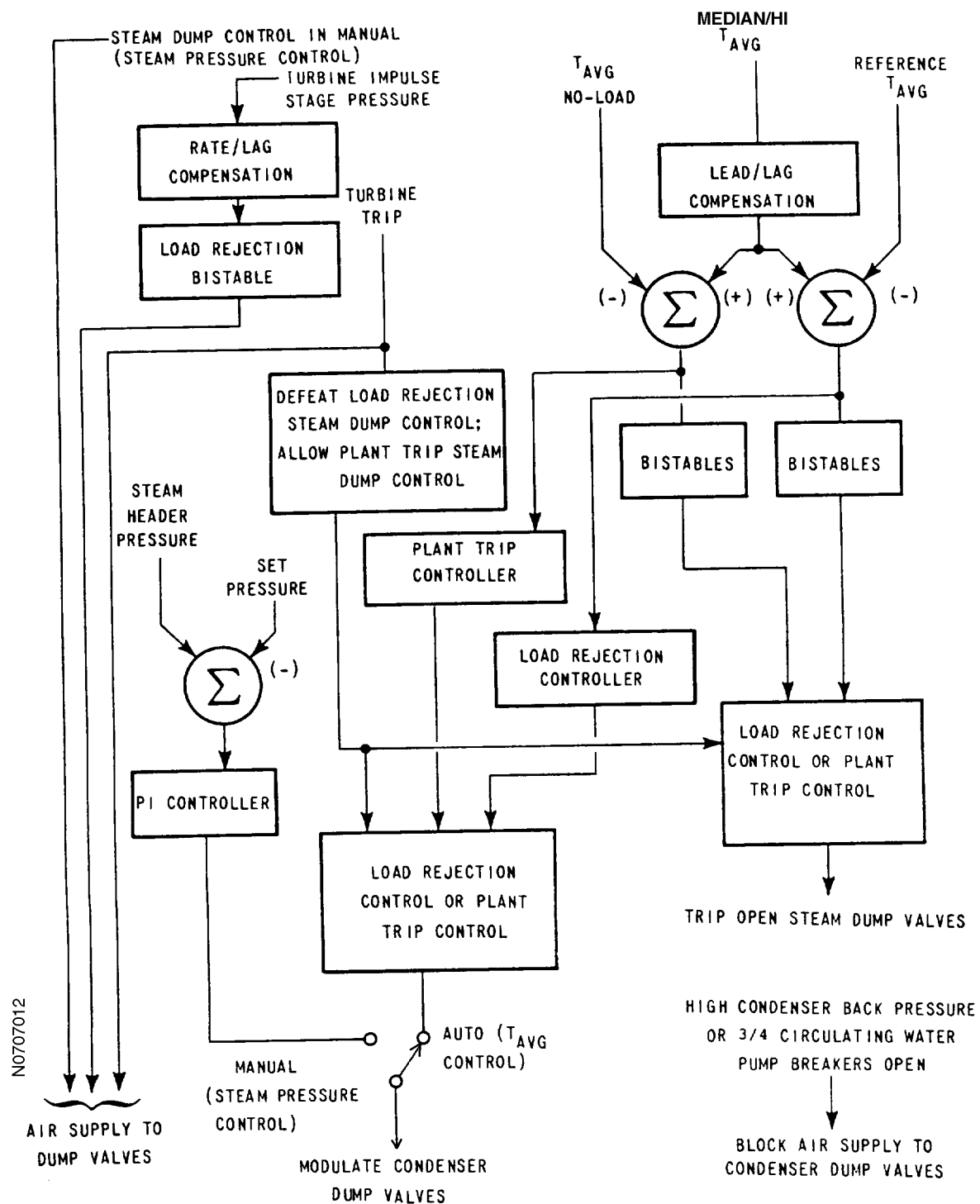
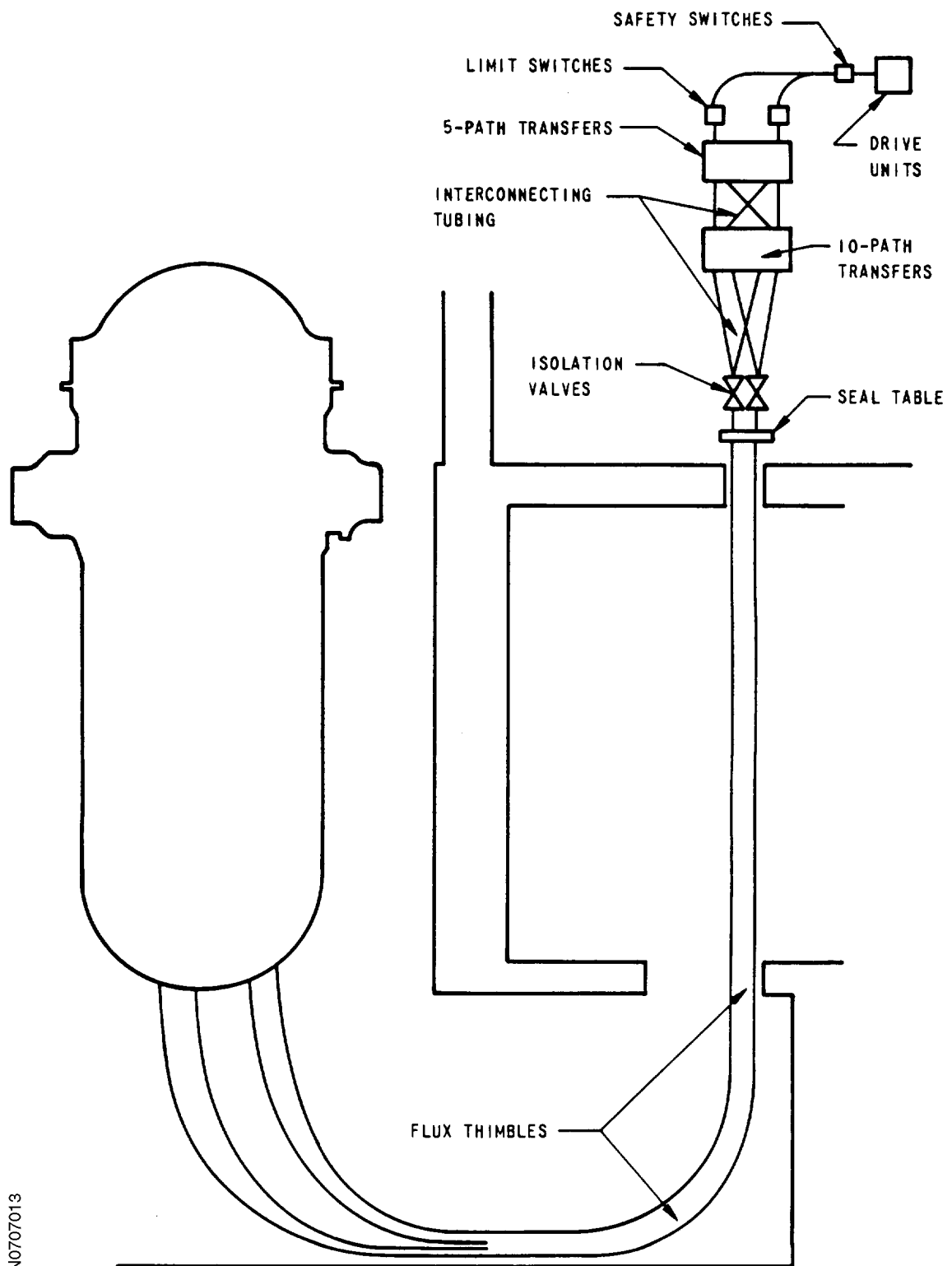


Figure 7.7-13
BASIC FLUX-MAPPING SYSTEM



Intentionally Blank

7.8 EMERGENCY RESPONSE TO ACCIDENTS

In order to provide improved management of accidents, the Emergency Response Facilities have been installed in accordance with Supplement 1 to NUREG-0737, NUREG-0696 and within the requirements set forth in NUREG-0700. The Emergency Response Facilities (ERF) which have been installed include:

- Technical Support Center (TSC)
- Emergency Control Center (ECC)
- Operations Support Center (OSC)
- Local Emergency Operations Facility (LEOF)
- Corporate Emergency Response Center (CERC)
- Center Emergency Operation Facility (CEOF)
- The Safety Parameter Display System (SPDS)

Although the Safety Parameter Display System is not a facility, it is an integral part of the ERF and will be treated as such.

The Emergency Response Facilities provide the following services:

- Keep the reactor operators informed of the plant's safety status.
- Relieve the reactor operators of peripheral duties not directly related to plant safety.
- Provide technical assistance to the reactor operators.
- Provide a coordinated response to the accident.
- Keep observers out of the control room.
- Provide communications between onsite and offsite emergency response organizations.
- Centralize control of recommendations for offsite actions.
- Provide relevant plant data to the NRC for analysis.

Personnel assigned to staff the Emergency Response Facilities are trained to follow emergency procedures in a timely manner. Emergency Planning is described in Section 13.3.

Activation of the Emergency Facilities is initiated by the Emergency Plan Implementary Procedures (EPIP):

EPIP-1.01	<i>Emergency Manager Controlling Procedures</i>
EPIP-1.02	<i>Response to Notification of Unusual Event</i>
EPIP-1.03	<i>Response to Notification of Alert</i>
EPIP-1.04	<i>Response to Notification of Site Area Emergency</i>
EPIP-1.05	<i>Response to Notification of General Emergency</i>

The following EPIPs provide the instruction to direct personnel to set the Emergency Response Facilities equipment into operation:

EPIP-3.01	<i>Activation of the Technical Support Center</i>
EPIP-3.02	<i>Activation of the Operational Support Center</i>
EPIP-3.03	<i>Activation of the Emergency Operation Facility</i>

7.9 INADEQUATE CORE COOLING MONITOR (ICCM) SYSTEM

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

7.9.1 Design Bases

The Inadequate Core Cooling Monitor (ICCM) system is designed by Westinghouse and Combustion Engineering, and meets all the requirements of Regulatory Guide 1.97 (Reference 2). The ICCM consists of the following three redundant subsystems that share common redundant calculator devices and continuous control room displays: Core Exit Thermocouple (CET) System, Core Cooling Monitor (CCM) System, and Reactor Vessel Level Instrumentation System (RVLIS).

The system provides means for acquiring data only, and performs no operational unit control. The system readily detects and displays conditions of inadequate core cooling.

The safety-grade signal inputs, calculator devices and displays are qualified to IEEE Std 323-1974 (Reference 3) and IEEE Std 344-1975 (Reference 4).

The system is safety-related, Class 1E. The RVLIS is a Seismic Class I System. All piping tubing, and conduit are seismically supported. All equipment has seismically-qualified mounting supports and the redundant electronics, including the microprocessor, are housed in seismically-qualified equipment cabinets.

System data are given in Table 7.9-1.

The system is designed and constructed in accordance with General Design Criteria 14, 15, 16, 30 and 55 of Appendix A to 10 CFR, Part 50. All components and materials used in the design are consistent with original station design criteria, except that compression type fittings, besides being used for the connection at the instruments, are also used in the RVLIS tubing connecting the reactor vessel head vent valve to the high-volume sensors. These fittings, which meet system design pressures and temperatures, are necessary to prevent damaging the tubing when the reactor vessel head is removed during refueling.

7.9.2 Design Description

7.9.2.1 Core Exit Thermocouple (CET) System—Subsystem of ICCM System

The Core Exit Thermocouple System uses inputs from up to 50 of the 51 incore thermocouples (51st available as spare) to calculate and display temperature of the reactor coolant as it exits the core. Refer to Figures 4.4-20 (Unit 1) and 4.4-21 (Unit 2) for the locations of thermocouples that have been abandoned in place.

The CET system consists of Type K, ungrounded, stainless steel sheathed thermocouples. Refer to UFSAR Section 7.7.1.9.1 for description of the quantity and design of the thermocouples.

Safety-related thermocouples from each channel (25 for Train A and 25 for Train B) are wired to the redundant ICCM calculators in the annunciator room via the electrical penetrations and Station Multiplexer System.

The cold junction compensation is performed internally at the remote multiplexer (MUX) installed in the cable vault area.

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

7.9.2.2 Reactor Vessel Level Instrumentation Systems (RVLIS)—Subsystem of ICCM 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 (except mode 6).

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 function 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.

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. To do this, it is necessary to tap into the reactor coolant system at the reactor vessel head, seal table, and the resistance temperature detector bypass piping of the hot legs of two reactor coolant system loops. Filled, sealed capillary impulse lines are used from the reactor coolant system to the transmitters. Each capillary line is sealed at the reactor coolant system end with a sensor bellow. A hydraulic isolator provides isolation of each sensing line outside of the containment. Reactor coolant system pressure, hot-leg temperatures and impulse line temperatures will be monitored and used to compensate for fluid density variations occurring during operating conditions.

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. This d/p cell 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. This d/p cell provides an indication of reactor core and internals pressure drop for any combination of operating RCPs. 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. This d/p cell provides an indication of reactor vessel level from the bottom of the reactor vessel to the top of the reactor during natural circulation conditions.

Temperature measurements of the impulse lines together with the reactor coolant temperature measurements (hot leg RTDs) and wide range RCS pressure, are employed to compensate the d/p transmitter 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 containment 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.

7.9.2.3 Core Cooling Monitor System—Subsystem of ICCM System

The Core Cooling or Subcooled Margin Monitor System uses various parameters to calculate saturated 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 perform calculations which determine the equivalent saturated temperature (T_{sat}) based on reactor wide range pressure. This (T_{sat}) value is used to determine the subcooled margin for the average of the five highest core exit thermocouples temperature.

7.9 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 Std 323-1974, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, 1974.
4. IEEE Std 344-1975, *Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*, 1975.

Table 7.9-1

INADEQUATE CORE COOLING MONITOR (ICCM) SYSTEM DATA

I. ICCM Display	
1. Type/Location	Flat Plasma Graphic/Vertical Main Control Board
2. Operator Interface/Location	4 - Button Keypad/Main Control Board Benchboard
3. Redundancy	Yes
4. Information Displayed	<ul style="list-style-type: none"> • DATA LINK FAILURE message indicates the data link from the system microprocessor to the display has failed • Incore thermocouple display graphics • Core Cooling display graphics • RVLIS display graphics
5. Display Update Rate	Every two seconds
II. Calculator	
1. Type	Microprocessor (16 Bit)
2. Location	Annunciator Room
3. Operator Interface	Local Display Panel with switches or portable maintenance terminal
4. Redundancy	Yes
5. Alarm	Control board annunciation on system malfunction
III. Reactor Vessel Level Instrumentation System (RVLIS) - Subsystem of ICCM System	
1. Redundancy	Yes
2. System Input Sensors (Per Channel)	<ul style="list-style-type: none"> • 3 - Reactor Coolant Pump Breaker contacts • 3 - RVLIS Hydraulic Isolator contacts • 3 - RVLIS d/p transmitter signals • 5 to 7 - RVLIS capillary RTDs (quantity varies per unit/channel) • 2 - Hot Legs RTDs • 1 - RCS Wide Range Pressure

Table 7.9-1 (continued)

INADEQUATE CORE COOLING MONITOR (ICCM) SYSTEM DATA

Reactor Vessel Level Instrumentation System (RVLIS) - Subsystem of ICCM System (continued)	
III.	
3. Display Graphics Available (Per Channel)	<ul style="list-style-type: none"> • Reactor Coolant Status - ON/OFF • Vessel level trending for the preceding 30 minutes showing static head (full range level) with a range of 0-120% level, dynamic head with a range of 0-120% full dP, and data quality based on the number of sensors used in the computations • Graphics layout of complete RVLIS process, including RVLIS status, RCS wide range pressure, and hot leg temperature • Instantaneous vessel level conditions for dynamic head full dP, and full and upper range level in ranges between 0 and 120% • RVLIS diagnostic information.
IV.	Core Cooling Monitor System - Subsystem of ICCM
1. Redundancy	Yes
2. System Input Sensors (per channel)	<ul style="list-style-type: none"> • 25 - Incore thermocouples ^a • 2 - Hot leg RTDs • 1 - RCS wide range pressure
3. Display Graphics Available (per channel)	<ul style="list-style-type: none"> • Pressure - Temperature (P-T) graph showing the saturation temperature curve and the over pressure and over temperature regions and current RCS coolant conditions plus trending of coolant conditions for previous 30 minutes. The P-T curve vertical axis range is 0 to 3000 psig wide range pressure and the horizontal axis range is 0 to 700°F of the average of the five highest incore thermocouples. Also displayed digitally are the input parameters and margin-to-saturation.
4. Alarm	Control board annunciation on approach-to-saturation temperature

a. Refer to Figures 4.4-20 (Unit 1) and 4.4-21 (Unit 2) for the locations of thermocouples that have been abandoned in place.

Table 7.9-1 (continued)

INADEQUATE CORE COOLING MONITOR (ICCM) SYSTEM DATA

V. Core Exit Thermocouple (CET) Monitoring System - Subsystem of ICCM	
1. Redundancy	Yes
2. System Input Sensors (per channel)	<ul style="list-style-type: none"> • 25 - Type K Core Exit thermocouples ^a (1 spare train B thermocouple available)
3. Display Graphics Available (per channel)	<ul style="list-style-type: none"> • Full core map showing temperature at each thermocouple location for that channel • Core map showing the maximum, minimum and average temperature for that channel for each quadrant and the subcooled temperature • Tabulation of each thermocouple for that channel by quadrant, location, and temperature • Trending curve of the average of the five highest CETs per core for past 30 minutes, including a graph of the data quality based on the number of thermocouples used in the computations. Also listed are the subcooling temperature and the CET temperature based on the average of the five highest thermocouples per core • CET diagnostic information • Thermocouple range of all displays is 0-2,300°F

a. Refer to Figures 4.4-20 (Unit 1) and 4.4-21 (Unit 2) for the locations of thermocouples that have been abandoned in place.

Intentionally Blank