SOUTHERN COMPANY®

UFSAR Table of Contents

Chapter 1 — Introduction and General Description of the Plant

Chapter 2 — Site Characteristics

Chapter 3 — Design of Structures, Components, Equipment and Systems

Chapter 4 — Reactor

Chapter 5 — Reactor Coolant System and Connected Systems

Chapter 6 — Engineered Safety Features

Chapter 7 — Instrumentation and Controls

Chapter 8 — Electric Power

Chapter 9 — Auxiliary Systems

Chapter 10 — Steam and Power Conversion

Chapter 11 — Radioactive Waste Management

Chapter 12 — Radiation Protection

Chapter 13 — Conduct of Operation

Chapter 14 — Initial Test Program

Chapter 15 — Accident Analyses

Chapter 16 — Technical Specifications

Chapter 17 — Quality Assurance

Chapter 18 — Human Factors Engineering

Chapter 19 — Probabilistic Risk Assessment

UFSAR Formatting Legend

Color	Description
	Original Westinghouse AP1000 DCD Revision 19 content
	Departures from AP1000 DCD Revision 19 content
	Standard FSAR content
	Site-specific FSAR content
	Linked cross-references (chapters, appendices, sections, subsections, tables, figures, and references)

TABLE OF CONTENTS

Section	Title	Page
CHAPTER 7	INSTRUMENTATION AND CONTROLS	7.1-1
7.1	Introduction	7.1-1
7.1.1	The AP1000 Instrumentation and Control Architecture	7.1-2
7.1.2	Protection and Safety Monitoring System	7.1-4
7.1.2.1	Plant Protection Subsystems	7.1-4
7.1.2.2	Engineered Safety Features Coincidence Logic	7.1-5
7.1.2.3	Engineered Safety Features Actuation Subsystems	7.1-5
7.1.2.4	Reactor Trip Switchgear	7.1-5
7.1.2.5	Qualified Data Processing Subsystems	7.1-5
7.1.2.6	Main Control Room Multiplexers	7.1-5
7.1.2.7	Sensors	7.1-5
7.1.2.8	Communication Functions	7.1-6
7.1.2.9	Fault Tolerance, Maintenance, Test, and Bypass	7.1-6
7.1.2.10	Isolation Devices	7.1-6
7.1.2.11	Test Subsystem	7.1-7
7.1.2.12	Safety-Related Display Instrumentation	7.1-7
7.1.2.13	Auxiliary Supporting Systems	7.1-7
7.1.2.14	Verification and Validation	7.1-7
7.1.3	Plant Control System	7.1-8
7.1.3.1	Distributed Controllers	7.1-9
7.1.3.2	Signal Selector Algorithms	7.1-10
7.1.3.3	Operator Controls and Indication	7.1-10
7.1.3.4	Real-Time Data Network	7.1-11
7.1.3.5	Rod Control System	7.1-11
7.1.3.6	Rod Position Indication	7.1-11
7.1.3.7	Rod Drive Motor-Generator Sets	7.1-11
7.1.4	Identification of Safety Criteria	7.1-12
7.1.4.1	Conformance of the Safety System Instrumentation to Applicable Criteria	7.1-12
7.1.4.2	Conformance With Industry Standards	7.1-12
7.1.5	AP1000 Protective Functions	7.1-13
7.1.6	Combined License Information	7.1-13
7.1.7	References	7.1-13
7.2	Reactor Trip	7.2-1
7.2.1	Description	7.2-1
7.2.1.1	Functional Description	7.2-2
7.2.1.2	Design Basis for Reactor Trips	7.2-10
7.2.1.3	System Drawings	7.2-11
7.2.2	Analyses	7.2-12
7.2.2.1	Failure Modes and Effects Analysis (FMEA)	7.2-12
7.2.2.2	Conformance of the Reactor Trip Function to Applicable Criteria	7.2-12
7.2.3	Combined License Information	7.2-14
7.2.4	References	7.2-14
7.3	Engineered Safety Features	7.3-1
7.3.1	Description	7.3-1
7.3.1.1	Safeguards Actuation (S) Signal	7.3-2
7.3.1.2	Engineered Safety Feature Descriptions	7.3-3

TABLE OF CONTENTS (CONTINUED)

Section	Title	Page
	7.3.1.3 Blocks, Permissives, and Interlocks for Engineered Safety Features Actuation	7.3-18
	7.3.1.4 Bypasses of Engineered Safety Features Actuation	7.3-18
	7.3.1.5 Design Basis for Engineered Safety Features Actuation	7.3-18
	7.3.1.6 System Drawings	7.3-20
	7.3.2 Analysis for Engineered Safety Features Actuation	7.3-20
	7.3.2.1 Failure Modes and Effects Analyses	7.3-20
	7.3.2.2 Conformance of Engineered Safety Features to the Requirements of IEEE 603-1991	7.3-20
	7.3.3 Combined License Information	7.3-22
	7.3.4 References	7.3-22
7.4	Systems Required for Safe Shutdown	7.4-1
	7.4.1 Safe Shutdown	7.4-2
	7.4.1.1 Safe Shutdown Using Safety-Related Systems	7.4-2
	7.4.1.2 Safe Shutdown Using Safety-Related and Nonsafety-Related Systems	7.4-4
	7.4.1.3 Safe Shutdown Using Nonsafety-Related Systems	7.4-5
	7.4.2 Safe Shutdown Systems	7.4-8
	7.4.2.1 Passive Core Cooling System	7.4-8
	7.4.2.2 Passive Containment Cooling System	7.4-8
	7.4.2.3 Containment Isolation	7.4-8
	7.4.2.4 Reactor Coolant System Circulation	7.4-9
	7.4.2.5 Other Systems Required for Safe Shutdown	7.4-9
	7.4.3 Safe Shutdown from Outside the Main Control Room	7.4-9
	7.4.3.1 Description	7.4-9
	7.4.3.2 Analysis	7.4-11
	7.4.4 Combined License Information	7.4-12
	7.4.5 References	7.4-12
7.5	Safety-Related Display Information	7.5-1
	7.5.1 Introduction	7.5-1
	7.5.2 Variable Classifications and Requirements	7.5-1
	7.5.2.1 Variable Types	7.5-2
	7.5.2.2 Variable Categories	7.5-4
	7.5.3 Description of Variables	7.5-7
	7.5.3.1 Type A Variables	7.5-7
	7.5.3.2 Type B Variables	7.5-8
	7.5.3.3 Type C Variables	7.5-8
	7.5.3.4 Type D Variables	7.5-8
	7.5.3.5 Type E Variables	7.5-9
	7.5.3.6 Type F Variables	7.5-9
	7.5.4 Processing and Display Equipment	7.5-9
	7.5.5 Combined License Information	7.5-10
7.6	Interlock Systems Important to Safety	7.6-1
	7.6.1 Prevention of Overpressurization of Low-Pressure Systems	7.6-1
	7.6.1.1 Description of Normal Residual Heat Removal Isolation Valve Interlocks	7.6-1

TABLE OF CONTENTS (CONTINUED)

Section	Title	Page
	7.6.1.2 Analysis of Normal Residual Heat Removal Valve Interlocks	7.6-1
	7.6.2 Availability of Engineered Safety Features	7.6-2
	7.6.2.1 Passive Residual Heat Removal Heat Exchanger Inlet Isolation Valve	7.6-2
	7.6.2.2 Core Makeup Tank Cold Leg Balance Line Isolation Valves	7.6-3
	7.6.2.3 Interlocks for the Accumulator Isolation Valve and IRWST Discharge Valve	7.6-4
	7.6.2.4 Interlock for Containment Vacuum Relief Isolation Valves	7.6-5
	7.6.3 Combined License Information	7.6-6
7.7	Control and Instrumentation Systems	7.7-1
	7.7.1 Description	7.7-1
	7.7.1.1 Reactor Power Control System	7.7-2
	7.7.1.2 Rod Control System	7.7-4
	7.7.1.3 Control Rod Position Monitoring	7.7-5
	7.7.1.4 Control Rod Insertion Limits	7.7-6
	7.7.1.5 Control Rod Stops	7.7-7
	7.7.1.6 Pressurizer Pressure Control System	7.7-7
	7.7.1.7 Pressurizer Water Level Control System	7.7-8
	7.7.1.8 Feedwater Control System	7.7-8
	7.7.1.9 Steam Dump Control System	7.7-9
	7.7.1.10 Rapid Power Reduction System	7.7-11
	7.7.1.11 Diverse Actuation System	7.7-12
	7.7.1.12 Signal Selector Algorithm	7.7-16
	7.7.2 Analysis	7.7-17
	7.7.3 Combined License Information	7.7-18
APPENDIX 7A	INSTRUMENTATION AND CONTROLS LICENSING BASIS DOCUMENT CHANGES	7A-1
7A.1	WCAP-15775, AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report	7A-1
7A.2	WCAP-17179-P and WCAP-17179-NP, AP1000™ Component Interface Module Technical Report	7A-2
7A.3	WCAP-17184-P, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report	7A-3
7A.4	WCAP-16438-P and WCAP-16438-NP, FMEA of AP1000™ Protection and Safety Monitoring System	7A-4

LIST OF TABLES

Table Number	Title	Page
7.2-1	Reactor Trip Variables, Limits, Ranges, and Accuracies (Design Basis for Reactor Trip) (Nominal)	7.2-15
7.2-2	Reactor Trips	7.2-18
7.2-3	Reactor Trip Permissives and Interlocks	7.2-20
7.2-4	System-Level Manual Inputs to the Reactor Trip Functions	7.2-22
7.2-5	Figure 7.2-1 Cross References	7.2-23
7.3-1	Engineered Safety Features Actuation Signals	7.3-23
7.3-2	Interlocks for Engineered Safety Features Actuation System	7.3-32
7.3-3	System-Level Manual Input to the Engineered Safety Features Actuation System	7.3-36
7.3-4	Engineered Safety Features Actuation, Variables, Limits, Ranges, and Accuracies (Nominal)	7.3-38
7.4-1	Systems Required for Safe Shutdown	7.4-13
7.5-1	Post-Accident Monitoring System	7.5-11
7.5-2	Summary of Selection of Criteria	7.5-23
7.5-3	Summary of Qualification, Design, and Interface Requirements	7.5-24
7.5-4	Summary of Type A Variables	7.5-25
7.5-5	Summary of Type B Variables	7.5-26
7.5-6	Summary of Type C Variables	7.5-27
7.5-7	Summary of Type D Variables	7.5-28
7.5-8	Summary of Type E Variables	7.5-32
7.5-9	Summary of Type F Variables	7.5-33
7.5-201	Not Used	7.5-37
7.5-202	Not Used	7.5-37
7.7-1	Rod Control System Interlocks - Power Control Subsystem	7.7-19
7.7-2	Rod Control System Interlocks – Axial Offset Control Subsystem	7.7-20
7.7-3	Cross Reference Table for Defense-in-Depth Functions Supported by the Plant Control System	7.7-21

LIST OF FIGURES

Figure Number	Title	Page
7.1-1	Instrumentation and Control Architecture	7.1-15
7.1-2	Common Q Standard Process and AP1000 Project-Specific Documents	7.1-16
7.1-3–7.1-11	Not Used	7.1-17
7.2-1	(Sheet 1 of 21) Functional Diagram Index and Symbols	7.2-24
7.2-1	(Sheet 2 of 21) Functional Diagram Reactor Trip Functions	7.2-25
7.2-1	(Sheet 3 of 21) Functional Diagram Nuclear Startup Protection	7.2-26
7.2-1	(Sheet 4 of 21) Functional Diagram Nuclear Overpower Protection	7.2-27
7.2-1	(Sheet 5 of 21) Functional Diagram Core Heat Removal Protection and Reactor Coolant Pump Trip	7.2-28
7.2-1	(Sheet 6 of 21) Functional Diagram Primary Overpressure & Loss of Heat Sink Protection	7.2-29
7.2-1	(Sheet 7 of 21) Functional Diagram Loss of Heat Sink Protection	7.2-30
7.2-1	(Sheet 8 of 21) Functional Diagram Loss of Heat Sink Protection	7.2-31
7.2-1	(Sheet 9 of 21) Functional Diagram Steam Line Isolation	7.2-32
7.2-1	(Sheet 10 of 21) Functional Diagram Feedwater Isolation	7.2-33
7.2-1	(Sheet 11 of 21) Functional Diagram Safeguards Actuation	7.2-34
7.2-1	(Sheet 12 of 21) Functional Diagram Core Makeup Tank Actuation	7.2-35
7.2-1	(Sheet 13 of 21) Functional Diagram Containment and Other Protection	7.2-36
7.2-1	(Sheet 14 of 21) Functional Diagram Turbine Trip	7.2-37
7.2-1	(Sheet 15 of 21) Functional Diagram Automatic RCS Depressurization Valve Sequencing	7.2-38
7.2-1	(Sheet 16 of 21) Functional Diagram In-containment Refueling Water Storage Tank Actuations	7.2-39
7.2-1	(Sheet 17 of 21) Functional Diagram Passive Residual Heat Removal and Core Makeup Tank Isolation Valve Interlocks	7.2-40
7.2-1	(Sheet 18 of 21) Functional Diagram Normal Residual Heat Removal System Isolation Valve Interlocks	7.2-41
7.2-1	(Sheet 19 of 21) Functional Diagram Containment Vacuum Relief Protection	7.2-42
7.2-1	(Sheet 20 of 21) Functional Diagram Diverse Actuation System Logic Automatic Actuations	7.2-43
7.2-1	(Sheet 21 of 21) Functional Diagram Diverse Actuation System Logic, Manual Actuations	7.2-44

Chapter 7 Instrumentation and Controls

7.1 Introduction

The instrumentation and control systems presented in this chapter provide protection against unsafe reactor operation during steady-state and transient power operations. They initiate selected protective functions to mitigate the consequences of design basis events. This chapter relates the functional performance requirements, design bases, system descriptions, and safety evaluations for those systems. The safety evaluations show that the systems can be designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

Because of the rapid changes that are taking place in the digital computer and graphic display technologies employed in a modern human system interface, design certification of the AP1000 focuses upon the process used to design and implement instrumentation and control systems for the AP1000, rather than on the specific implementation. The design specifics provided here are included as an example for illustration.

Chapter 7 for the AP1000 has been written to describe the protection system hardware utilizing the Common Qualified Platform (Common Q) described in Reference 8 (which includes the NRC SER), and augmented by Reference 2. The I&C functional requirements of the AP600, which has received Design Certification, have been retained to the maximum extent compatible with the Common Q hardware and software.

The terminology used for Chapter 7 is intended to be independent of any product, but when this is not possible, Common Q terminology is used.

This chapter also discusses the instrumentation portions of the safety-related systems which function to achieve the system responses assumed in the accident analysis, and those needed to shutdown the plant. Section 7.1 describes the AP1000 instrumentation and control architecture, with specific emphasis on the protection and safety monitoring system. The plant control system is discussed briefly. Other systems are discussed in more detail in relevant sections or chapters. Section 7.2 discusses the reactor trip function, and Section 7.3 addresses the engineered safety features (ESF). Systems required for safe shutdown are discussed in Section 7.4 in support of other chapters. Safety-related display instrumentation is discussed in Section 7.5 and interlocks important to safety are presented in Section 7.6. Control systems and the diverse actuation system are discussed in Section 7.7.

Definitions

Terminology used in this chapter reflects an interdisciplinary approach to safety-related systems similar to that proposed in IEEE 603 (Reference 1).

Safety System – The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis events.

Protection and Safety Monitoring System – The aggregate of electrical and mechanical equipment which senses generating station conditions and generates the signals to actuate reactor trip and ESF, and which provides the equipment necessary to monitor plant safety-related functions during and following designated events.

Protective Function – Any one of the functions necessary to mitigate the consequences of a design basis event. Protective functions are initiated by the protection and safety monitoring system logic and will be accomplished by the trip and actuation subsystems. Examples of protective functions are reactor trip and engineered safety features (such as valve alignment and containment isolation).

Actuated Equipment – The assembly of prime movers and driven equipment used to accomplish a protective function (such as solenoids, shutdown rods, and valves).

Actuation Device – A component that directly controls the motive power for actuated equipment (such as circuit breakers, relays, and pilot valves).

Division – One of the four redundant segments of the safety system. A division includes its associated sensors, field wiring, cabinets, and electronics used to generate one of the redundant actuation signals for a protective function. It also includes the power source and actuation signals.

Channel – One of the several separate and redundant measurements of a single variable used by the protection and safety monitoring system in generating the signal to initiate a protective function. A channel can lose its identity when it is combined with other inputs in a division.

Degree of Redundancy – The number of redundant channels monitoring a single variable, or the number of redundant divisions which can initiate a given protective function or accomplish a given protective function. Redundancy is used to maintain protection capability when the safety-related system is degraded by a single random failure.

System-Level Actuation – Actuation of a sufficient number of actuation devices to effect a protective function.

Component-Level Actuation – Actuation of a single actuation device (component).

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network.

The lower portion of the figure includes the plant protection, control, and monitoring functions. At the lower right-hand side is the protection and safety monitoring system. It performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing (QDPS) functions. The I&C equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

The ESF coincidence logic performs system-level logic calculations, such as initiation of the passive residual heat removal system. It receives inputs from the plant protection subsystem bistables and the main control room.

The ESF actuation subsystems provide the capability for on-off control of individual safety-related plant loads. They receive inputs from the ESF coincidence logic, remote shutdown workstation and the main control room.

The plant control system performs nonsafety-related instrumentation and control functions using both discrete (on/off) and modulating (analog) type actuation devices.

The nonsafety-related real-time data network, which horizontally divides Figure 7.1-1, is a high speed, redundant communications network that links systems of importance to the operator. Safety-related systems are connected to the network through gateways and qualified isolation devices so that the safety-related functions are not compromised by failures elsewhere. Plant

protection, control, and monitoring systems feed real-time data into the network for use by the control room and the data display and processing system.

The upper portion of the figure depicts the control rooms and data display and processing system. The main control room is implemented as a set of compact operator consoles featuring color graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided.

The data display and processing (plant computer) system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains its input from the real-time data network and delivers its output over the network to other users.

WCAP-15775 (Reference 7) describes the diversity and defense-in-depth features of the AP1000 instrumentation and control architecture.

Protection and Safety Monitoring System

The protection and safety monitoring system provides detection of off-nominal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The protection and safety monitoring system controls safety-related components in the plant that are operated from the main control room or remote shutdown workstation. Secure development and operational environments for the protection and safety monitoring system are used during design as described in Reference 22.

In addition, the protection and safety monitoring system provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by Regulatory Guide 1.97.

Special Monitoring System

The special monitoring system does not perform any safety-related or defense-in-depth functions. The special monitoring system consists of specialized subsystems that interface with the instrumentation and control architecture to provide diagnostic and long-term monitoring functions.

The special monitoring system is the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system is composed of digital circuit boards, controls, indicators, power supplies and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service. The metal impact monitoring system is described in Subsection 4.4.6.4.

Plant Control System

The plant control system provides the functions necessary for normal operation of the plant from cold shutdown through full power. The plant control system controls nonsafety-related components in the plant that are operated from the main control room or remote shutdown workstation.

The plant control system contains nonsafety-related control and instrumentation equipment to change reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation. The plant control system is described in Subsections 7.1.3 and 7.7.1.

Diverse Actuation System

The diverse actuation system is a nonsafety-related, diverse system that provides an alternate means of initiating reactor trip and actuating selected engineered safety features, and providing plant information to the operator. The diverse actuation system is described in Subsection 7.7.1.11.

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for these centers. With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, protection and safety monitoring system, plant control system, data display and processing system).

The boundaries of the operation and control centers system for the main control room and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the plant protection and safety monitoring system processor and logic circuits, which interface with the reactor trip and ESF plant components; the plant control system processor and logic circuits, which interface with the nonsafety-related plant components; and the plant real-time data network, which provides plant parameters, plant component status, and alarms.

Data Display and Processing System

The data display and processing system provides the equipment used for processing data that result in nonsafety-related alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data logging and historical storage and retrieval, and providing operational support for plant personnel.

The data display and processing system also contains the real-time data network, which is a redundant data highway that links the elements of the AP1000 instrumentation and control architecture.

Incore Instrumentation System

The primary function of the incore instrumentation system is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system, as well as to optimize core performance. A secondary function of the incore instrumentation system is to provide the protection and safety monitoring system with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The incore instrument assemblies house both fixed incore flux detectors and core exit thermocouples. The incore instrumentation system is described in Subsection 4.4.6.1.

7.1.2 Protection and Safety Monitoring System

Reference 19, Section 2.1 provides an overview description of the protection and safety monitoring system.

7.1.2.1 Plant Protection Subsystems

Reference 19, Section 2.2 describes the plant protection subsystems.

7.1.2.1.1 Reactor Trip Functions

Reference 19, Section 1.1 describes the reactor trip functions.

7.1.2.1.2 Reactor Trip Switchgear Interface

Reference 19, Subsection 2.2.3.1.1 describes the reactor trip switchgear interface.

7.1.2.1.3 Manual Reactor Trip

Reference 19, Subsection 2.2.3.1.3 describes the manual reactor trip.

7.1.2.2 Engineered Safety Features Coincidence Logic

Reference 19, Subsection 2.2.3.2.1 describes the Engineered Safety Features Coincidence Logic.

7.1.2.3 Engineered Safety Features Actuation Subsystems

Reference 19, Subsection 2.2.3.2.2 describes the Engineered Safety Features Actuation Subsystems.

7.1.2.4 Reactor Trip Switchgear

Reference 19, Subsection 2.2.3.1.1 describes the reactor trip switchgear.

7.1.2.5 Qualified Data Processing Subsystems

Reference 19, Section 4.2 describes the Qualified Data Processing Subsystems (QDPS).

7.1.2.6 Main Control Room Multiplexers

The protection and safety monitoring system does not use multiplexers to provide a signal path between the protection system equipment and the main control room. Each division's safety display communicates with the protection system equipment via that division's communications network as shown in Figure 2-2 of Reference 19.

7.1.2.7 Sensors

The protection and safety monitoring system monitors key variables related to equipment mechanical limitations, and variables directly affecting the heat transfer capability of the reactor. Some limits, such as the overtemperature ΔT setpoint, are calculated in the plant protection subsystem from other parameters because direct measurement of the variable is not possible. This subsection provides a description of the sensors which monitor the variables for the protection and safety monitoring system. For convenience the discussions are grouped into the following three categories:

- Process sensors
- Nuclear instrumentation detectors
- Status inputs from field equipment

The inputs described are those required to generate the initiation signals for the protective functions. The use of each parameter is discussed in the sections that deal with each protective function. For example, reactor trip is discussed in Section 7.2 and ESF actuation is described in Section 7.3.

7.1.2.7.1 Process Sensors

The process sensors are devices which measure temperature, pressure, fluid flow, and fluid level. Process instrumentation excludes nuclear and radiation measurements.

Additional information on these process variables is included as part of the description of each process system provided in other chapters. The process variables measured by the protection and safety monitoring system are listed in Sections 7.2, 7.3, and 7.5.

7.1.2.7.2 Nuclear Instrumentation Detectors

Three types of neutron detectors are used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The intermediate range channels are capable of measuring overpower excursions up to 200 percent of full power.

The lowest range (source range) covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This generally is greater than two counts per second. The next range (intermediate range) covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps the higher portion of the intermediate range. The neutron detectors are installed in tubes located around the reactor vessel in the primary shield. Detector types for these three ranges are:

- Source range – proportional counter or pulse fission chamber
- Intermediate range – pulse fission chamber
- Power range – uncompensated ionization chamber

7.1.2.7.3 Equipment Status Inputs

Some inputs to the protection system are not measurements of process or nuclear variables, but are discrete indications of the status of certain equipment. Examples include manual switch positions, contact status inputs, and indications provided by valve limit switches.

7.1.2.8 Communication Functions

Reference 19, Section 3, and Reference 25 describe the communication functions.

7.1.2.9 Fault Tolerance, Maintenance, Test, and Bypass

Reference 19, Section 7 describes the fault tolerance features, and Section 6 describes the maintenance, test, and bypass features of the protection and safety monitoring system.

7.1.2.10 Isolation Devices

Isolation devices are used to maintain the electrical independence of divisions, and to prevent interaction between nonsafety-related systems and the safety-related system.

Isolation devices are incorporated into selected interconnections to maintain division independence. Isolation devices serve to prevent credible faults (such as open circuits, short circuits, or applied credible voltages) in one circuit from propagating to another circuit.

7.1.2.11 Test Subsystem

Reference 19, Section 6 describes the test subsystem.

7.1.2.12 Safety-Related Display Instrumentation

Safety-related display instrumentation provides the operator with information to determine the effect of automatic and manual actions taken following reactor trip due to a Condition II, III, or IV event as defined in Chapter 15. This instrumentation also provides for operator display of the information necessary to meet Regulatory Guide 1.97. A description of the equipment used to provide this function is provided in Subsection 7.1.2.5. A description of the data provided to the operator by this instrumentation is provided in Section 7.5.

7.1.2.13 Auxiliary Supporting Systems

The safety-related system equipment is supported by the supply of uninterruptible electrical power. This electrical power is supplied by the Class 1E dc and UPS system discussed in Chapter 8.

7.1.2.14 Verification and Validation

[*Adequacy of the hardware and software is demonstrated for the protection and safety monitoring system through a verification and validation (V&V) program. Details on the verification and validation program are provided in WCAP-16096-NP-A (Reference 9.*]* WCAP-16096-NP-A defines a software development process consistent with appropriate industry standards.

7.1.2.14.1 Design Process

[*WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:*

- *Conceptual phase (may also be referred to as design requirements phase)*
- *Requirements phase (may also be referred to as system definition phase)*
- *Design phase (may also be referred to as hardware and software development phase)*
- *Implementation phase (may also be referred to as hardware and software development phase)*
- *Test phase (may also be referred to as system integration and test phase)*
- *Installation and checkout phase (may also be referred to as installation phase)*

WCAP-16096-NP-A (Reference 9), WCAP-15927 (Reference 20), and NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]*

Reference 22 describes the process for ensuring that the design life cycle process for the protection and safety monitoring system meets the computer security requirements of IEEE 603 and Regulatory Guide 1.152.

The planning (or design requirements) phase documents are listed below. Figure 7.1-2 shows the relationship of the same documents.

*NRC Staff approval is required prior to implementing a change in this information.

Document 1: WNA-PN-00043-WAPP, NuStart/DOE Design Finalization Program"

Document 2: WNA-PQ-00201-WAPP, NuStart/DOE Design Finalization Program Project Quality Plan"

Document 3: WNA-PN-00045-WAPP, NuStart/DOE Design Finalization Protection and Safety Monitoring System Project Plan"

Document 4: WNA-PD-00042-WAPP, NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan"

Document 5: WCAP-16096-NP-A, "Software Program Manual for Common Q Systems"

Document 6: NABU-DP-00014-GEN, "Design Process for Common Q Safety Systems"

Document 7: WNA-PV-00009-GEN, "Verification & Validation Process for the Common Q Safety Systems"

Document 8: WNA-PT-00058-GEN, "Testing Process for Common Q Safety Systems"

Document 9: NABU-DP-00015-GEN, "Common Q Software Configuration Management Guidelines"

Document 10: 00000-ICE-3889, "Coding Standards & Guidelines for Common Q Systems"

Document 11: APP-PMS-GER-020, "Protection and Safety Monitoring System Concept Phase V&V Summary Report"

Document 12: APP-PMS-T5-001, "AP1000 Protection and Safety Monitoring System Test Plan"

Document 13: WCAP-15927, "Design Process for AP1000 Common Q Safety Systems"

Document 14: APP-GW-J0R-012, "AP1000™ Protection and Safety Monitoring System Computer Security Plan"

Document 15: APP-GW-GLR-143 (WCAP-17179), "AP1000™ Component Interface Module Technical Report," Revision 2 (as modified by changes provided in Appendix 7A)

7.1.2.14.2 Commercial Dedication

[*WCAP-16097-P-A (Reference 8) provides for the use of commercial off-the-shelf hardware and software through a commercial dedication process.*]* Control of the hardware and software during the operational and maintenance phase is the responsibility of the Combined License applicant as described in Subsection 13.5.3.

7.1.3 Plant Control System

The plant control system is a nonsafety-related system that provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions. The plant control system integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes for required normal and off-normal conditions. The plant control system also provides control of the nonsafety-related decay heat removal systems during shutdown. The plant control system accomplishes these functions through use of the following:

*NRC Staff approval is required prior to implementing a change in this information.

- Rod control
- Pressurizer pressure and level control
- Steam generator water level control
- Steam dump (turbine bypass) control
- Rapid power reduction

The plant control system provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes). The plant control system acts to maximize margins to plant safety limits and maximize the plant transient performance. The plant control system also provides the capability for manual control of plant systems and equipment. Redundant control logic is used in some applications to increase single-failure tolerance.

The plant control system includes the equipment from the process sensor input circuitry through to the modulating and nonmodulating control outputs as well as the digital signals to other plant systems. Modulating control devices include valve positioners, pump speed controllers, and the control rod equipment. Nonmodulating devices include motor starters for motor-operated valves and pumps, breakers for heaters, and solenoids for actuation of air-operated valves. The plant control system cabinets contain the process sensor inputs and the modulating and nonmodulating outputs. The plant control system also includes equipment to monitor and control the control rods.

The functions of the plant control system are performed by system assemblies including:

- Distributed controllers
- Signal selector algorithms
- Operator controls and indication
- Real-time data network
- Rod control system
- Rod position indication
- Rod drive motor-generator sets

7.1.3.1 Distributed Controllers

Each distributed controller processes inputs, performs system-level and component-level control calculations, provides capability for an operator interface to the controlled components, transmits control signals to discrete, modulating, and networked interfaced control components, and provides plant status and plant parameter information to the real-time data network.

The distributed controllers receive process inputs and implement the system-level logic and control algorithms appropriate for the plant operating mode. The distributed controllers receive process inputs from, and transmit process control outputs to, the actuated components. The distributed controller also transmits and receives process signals via the real-time data network. The real-time data network also provides for two-way communication between the distributed controllers and between the distributed controllers and the main control room and remote shutdown workstation.

Control functions are distributed across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers. The major control functions which are implemented in different distributed controllers include reactor power control, feedwater control, pressurizer control, and turbine control.

7.1.3.2 Signal Selector Algorithms

Signal selector algorithms provide the plant control system with the ability to obtain inputs from the protection and safety monitoring system. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals. Therefore, the control system does not cause an unsafe control action to occur even if one of four redundant protection channels is degraded by random failure simultaneous with another of the four channels bypassed for test or maintenance.

Each signal selector algorithm receives data from each of the redundant divisions of the protection and safety monitoring system. The data is received from each division through an isolation device.

The signal selector algorithms provide validated process values to the plant control system. They also provide the validation status; the average, the median, or an individual input value of the valid process values; the number of valid process values; an alarm (if one process value has been rejected); and another alarm (if the algorithm is not able to provide a valid process value).

For the logic values received from the protection and safety monitoring system, such as permissives, two-out-of-four (2/4) voting is used to provide a valid logic value to the plant control system.

The signal selection algorithm is executed in the PLS, and the results are not available to PMS or DAS. Therefore, PMS and DAS performance, controls, and displays are independent of the signal selector algorithm.

7.1.3.3 Operator Controls and Indication

The plant control operator interface is a set of soft control devices that replace conventional switch/light or potentiometer/meter assemblies used for operator interface with control systems. These soft control devices provide consistent operator interfaces for the plant control system. The soft controls are located on each operator workstation and the remote shutdown workstation. Each soft control device can control safety-related and nonsafety-related equipment.

The implementation of the soft controls is consistent with the following functional requirements:

- The soft control function does not affect the electrical or functional isolation of the safety-related and nonsafety-related equipment. This isolation is maintained upon a single failure of any equipment performing or supporting the soft control function.

- Failure of the operator displays does not prevent an operator from being able to safely shutdown the plant.

When the operator desires to operate a component, the graphical operator display which is indicating the component status is presented on the operator control console. This results in a message being sent to the soft control device. The soft control device then displays the appropriate control template. The operator then selects the desired control action on the template. After the operator verifies that the desired control action is properly selected, the operator then actuates the control action, causing the selected control action to be transmitted to the control device.

7.1.3.4 Real-Time Data Network

The real-time data network is a redundant data highway that supports both periodic and aperiodic data transfers of nonsafety-related signals and data. Periodic transfers consist of process data that is broadcast over the network at fixed intervals and is available to all destinations. Aperiodic data transfer is generally used for messages or file transfers.

The real-time data network provides communications among the distributed controllers, the plant protection and safety monitoring system gateways, the incore instrumentation, and the special monitoring system.

7.1.3.5 Rod Control System

The primary means of regulating the reactor power and power distribution is to position clusters of control rods in the reactor core using the rod control system.

The control rods are moved into and out of the reactor core by means of electromagnetic jacking mechanisms, called control rod drive mechanisms, located on the reactor vessel head. Each control rod drive mechanism consists of two gripper mechanisms, one stationary and one movable, that hold a notched driveline attached to the upper end of the control rod. The grippers and the lift armature are controlled by coils mounted external to the mechanism, concentric with the rod driveline. By controlling the sequence of energizing these coils, the mechanism can be made to step into, or out of, the reactor in increments. The rod control equipment provides this sequence control.

The control rods are arranged into symmetrical groups. The groups of control rods are divided into two categories: shutdown rods that are normally held fully withdrawn from the reactor, and control rods that are positioned to some intermediate insertion. In addition, there is a subcategory of control rods (low worth gray rods). If a rapid shutdown is necessary, the control, shutdown, and gray rods are dropped into the reactor by de-energizing their drive mechanisms.

Interlocks are provided to prevent the motion of the control rods outside of planned sequences.

7.1.3.6 Rod Position Indication

The position of each control rod is continuously monitored by the rod position indication system. This information is detected by the rod position detector assemblies. The signals from the detectors are processed by the data cabinets and transmitted to the distributed controllers. The distributed controllers further process the rod position information and transmit this information to the real-time data network.

7.1.3.7 Rod Drive Motor-Generator Sets

The rod drive motor-generator sets provide the power to the control rod drive mechanisms through the reactor trip switchgear. The rod drive motor-generator sets are included in the plant control system. The safety-related reactor trip switchgear is included in the plant protection and safety monitoring system.

There are two motor-generator sets with flywheels and one control cabinet. Each motor-generator is a three-phase induction motor, direct-coupled to a flywheel, and a synchronous alternator.

During normal operating conditions, both motor generator sets are operating in parallel and equally sharing the total load demand. Each motor-generator set is capable of supplying the entire load requirements when the other set is out of service.

7.1.4 Identification of Safety Criteria

7.1.4.1 Conformance of the Safety System Instrumentation to Applicable Criteria

The safety-related system instrumentation described in Subsection 7.1.1 is designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power. Applicable General Design Criteria are listed in Section 3.1, NRC Regulatory Guides in Subsection 1.9.1, and Branch Technical Positions in Subsection 1.9.2. Industry Standards are cited as references.

The instrumentation and control portion of the safety-related system meets the requirements of IEEE 603-1991 as discussed in WCAP-15776 (Reference 12). The topics are listed in the same order as they appear in Sections 4 through 8 of IEEE 603-1991. IEEE 603 provides the design bases of the instrumentation and control portion of the safety system. Other criteria related to the IEEE 603-1991 requirements are also identified.

7.1.4.2 Conformance With Industry Standards

The instrumentation and control systems are designed in accordance with guidance provided in applicable portions of the following standards. The portions of the standards which are considered to be applicable are the portions of the standards which apply to instrumentation and control systems performing protection and control functions in an industrial environment:

- IEEE 323-1974; “IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations”
- IEEE 344-1987; “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations”
- IEEE 379-2000; “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”
- IEEE 383-1974; “IEEE Standard for Type Test of Class IE Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations”
- IEEE 384-1981; “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”
- IEEE 420-1982; “IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations”
- IEEE 603-1991; “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
- IEEE 627-1980; “IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations”
- IEEE 1050-1996; “IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations”
- IEEE 1074-1995; “IEEE Standard for Developing Software Life Cycle Processes”
- EPRI TR-102323, Revision 1, “Guidelines for Electromagnetic Interference Testing in Power Plants”

7.1.5 AP1000 Protective Functions

Protective functions are those necessary to achieve the system responses assumed in the safety analyses, and those needed to shut down the plant safely. The protective functions are grouped into two classes, reactor trip and ESF actuation. The software associated with these functions is considered a basic component as defined in 10 CFR 21 (Reference 6).

Reactor trip is discussed in Section 7.2. ESF actuation is discussed in Section 7.3.

7.1.6 Combined License Information

7.1.6.1 The calculation of setpoints for protective functions consistent with the methodology presented in Reference 5 is addressed in WCAP-16361-P (Reference 17). Reference 5 is an AP600 document that describes a methodology that is applicable to AP1000. AP1000 has some slight differences in instrument spans.

The Setpoint Program described in Technical Specifications Section 5.5 provides the appropriate controls for update of the instrumentation setpoints following completion of the calculation of setpoints for protective functions and the reconciliation of the setpoints against the final design.

7.1.6.2 The I&C platform is addressed in APP-GW-GLR-017 (Reference 18).

7.1.7 References

1. IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

2. [*WCAP-17201-P, Revision 0, "AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15," February 2010.*]*

3. Not used.

4. Not used.

5. WCAP-14605 (Proprietary) and WCAP-14606 (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems, AP600," April 1996.

6. 10 CFR 21, "Reporting of Defects and Noncompliance."

7. WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Revision 4 (as modified by changes provided in Appendix 7A)

8. [*WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Revision 0, "Common Qualified Platform," May 2003.*]*

9. [*WCAP-16096-NP-A, Revision 01A, "Software Program Manual for Common Q Systems," December 2004.*]*

10. Not used.

11. Not used.

*NRC Staff approval is required prior to implementing a change in this information.

12. WCAP-15776, “Safety Criteria for the AP1000 Instrument and Control Systems,” April 2002.

13. Not used.

14. Not used.

15. IEEE 7-4.3.2-1993, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

16. Not used.

17. WCAP-16361-P (Proprietary) and WCAP-16361-NP (Non-Proprietary), “Westinghouse Setpoint Methodology for Protection Systems – AP1000,” February 2011.

18. APP-GW-GLR-017, AP1000 Standard Combined License Technical Report, “Resolution of Common Q NRC Items,” Westinghouse Electric Company LLC.

19. WCAP-16675-P (Proprietary) and WCAP-16675-NP (Non-Proprietary), “AP1000 Protection and Safety Monitoring System Architecture Technical Report,” Revision 5.

20. [*WCAP-15927, Revision 2 (Non-proprietary), “Design Process for AP1000 Common Q Safety Systems,” November 2008.*]*

21. Westinghouse Electric Company Quality Management System (QMS), Revision 5 (Non-Proprietary), October 1, 2002.

22. APP-GW-J0R-012, “AP1000 Protection and Safety Monitoring System Computer Security Plan,” Revision 4, Westinghouse Electric Company LLC.

23. WCAP-17184-P, “AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report,” Revision 2 (as modified by changes provided in UFSAR Appendix 7A).

24. [*WCAP-17179-P (Proprietary) and WCAP-17179-NP (Non-Proprietary), “AP1000 Component Interface Module Technical Report,” Revision 2 (as modified by changes provided in UFSAR Appendix 7A).*]*

25. WCAP-16674-P (Proprietary) and WCAP-16674-NP (Non-Proprietary), “AP1000 I&C Data Communication and Manual Control of Safety Systems and Components,” Revision 4.

*NRC Staff approval is required prior to implementing a change in this information.

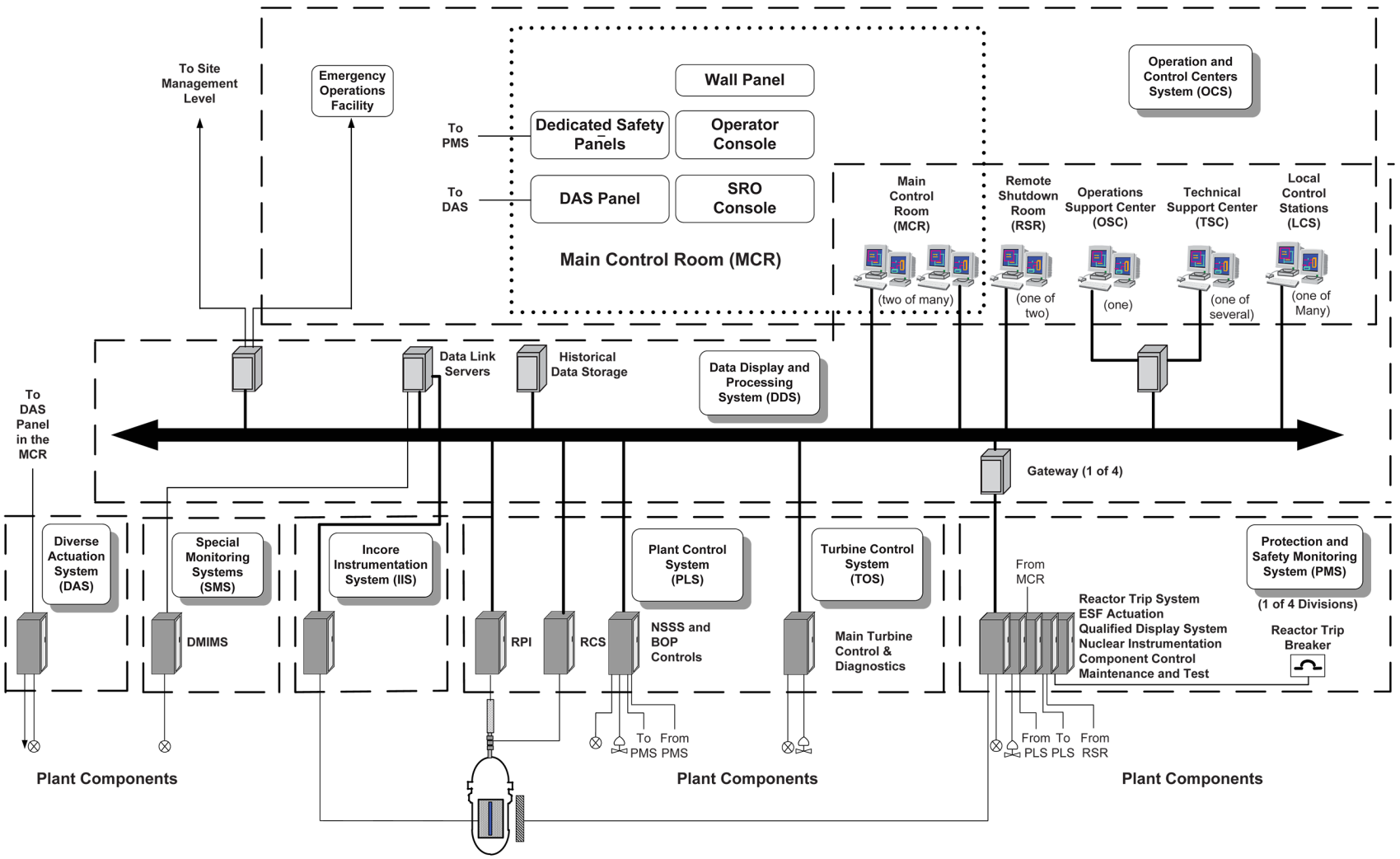


Figure 7.1-1
Instrumentation and Control Architecture

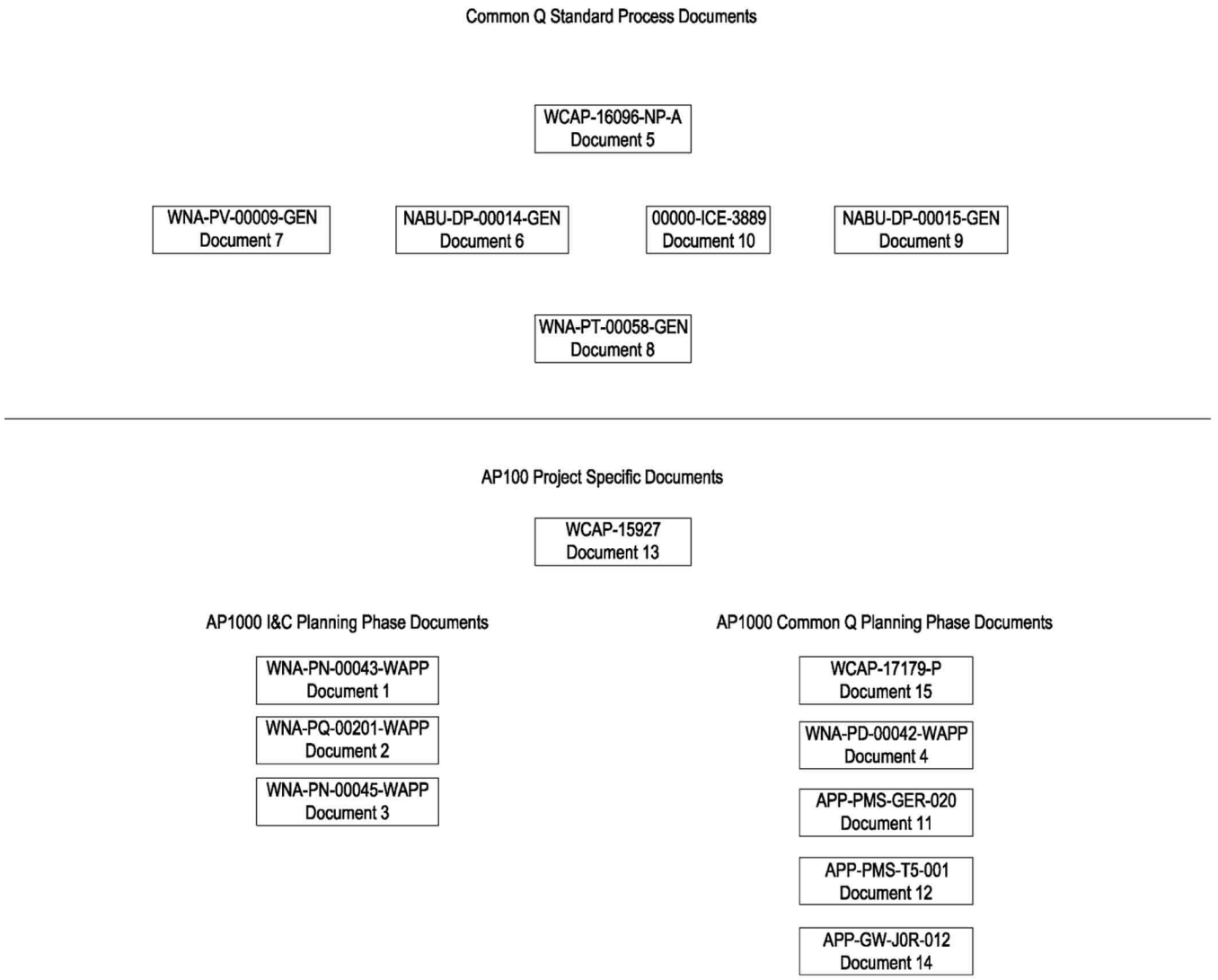


Figure 7.1-2
Common Q Standard Process and AP1000 Project-Specific Documents

Figures 7.1-3–7.1-11 Not Used

7.2 Reactor Trip

7.2.1 Description

Considerations, such as mechanical or hydraulic limitations on equipment or heat transfer requirements on the reactor core, define a safe operating region for the plant. Maneuvering of the plant within this safe operating region is permitted in response to normal power generation demands. The plant design provides margin to the safety limits so that an unsafe condition is not caused by the transients induced by normal operating changes. The plant control system attempts to keep the reactor operating away from any safety limit. Excursions toward a limit occur because of abnormal demands, malfunctions in the control system, or by severe transients induced by occurrence of a Condition II or III event, as discussed in Chapter 15. Hypothetical events (Condition IV) are analyzed with respect to plant safety limits. The safety system keeps the reactor within the safe region by shutting down the reactor whenever safety limits are approached. Reactor trip is a protective function performed by the protection and safety monitoring system when it anticipates an approach of a parameter to its safety limit. Reactor shutdown occurs when electrical power is removed from the rod drive mechanism coils, allowing the rods to fall by gravity into the reactor core.

Section 7.1 provides a description of the reactor trip equipment. The equipment involved is:

- Sensors and manual inputs
- Protection and safety monitoring system cabinets
- Reactor trip switchgear

The plant protection subsystems maintain surveillance of key process variables directly related to equipment mechanical limitations (such as pressure), and of variables which directly affect the heat transfer capability of the reactor (such as flow and temperature). Some limits, such as the overtemperature ΔT setpoint, are calculated in the protection and safety monitoring system from other parameters when direct measurement of the variable is not possible. Table 7.2-1 lists variables monitored for reactor trip.

Four redundant measurements, using four separate sensors, are made for each variable used for reactor trip. Analog signals are converted to digital form by analog-to-digital converters within the protection and safety monitoring system. Signal conditioning is applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated if one channel's measurement exceeds its predetermined or calculated limit. Processing of variables for reactor trip is identical in each of the four redundant divisions of the protection system. Each division sends its partial trip status to each of the other three divisions over isolated data links. Each division is capable of generating a reactor trip signal if two or more of the redundant channels of a single variable are in the partial trip state.

The reactor trip signal from each of the four divisions of the protection and safety monitoring system is sent to the corresponding reactor trip switchgear breakers.

Each of the four reactor trip actuation divisions consists of two reactor trip circuit breakers. The reactor is tripped when two or more actuation divisions output a reactor trip signal. This automatic trip demand initiates the following two actions. It deenergizes the under-voltage trip attachments on the reactor trip breakers, and it energizes the shunt trip devices on the reactor trip breakers. Either action causes the breakers to trip. Opening the appropriate trip breakers removes power to the rod drive mechanism coils, allowing the rods to fall into the core. This rapid negative reactivity insertion causes the reactor to shutdown.

Bypasses of parameter channels used to generate reactor trip signals and of reactor trip actuation divisions are permitted as described in Subsection 7.2.1.1.13. Single failure criterion is met even when one channel or division is bypassed. Bypassing two or more redundant channels or divisions is not allowed.

Subsection 7.2.1.1 provides a description of each of the reactor trip functions. Figure 7.2-1 shows the functional diagrams for reactor trips, as well as functional diagrams for other related plant functions. Figure 7.2-1 sheets are derived from the APP-PMS-J1 drawings and the references shown on Figure 7.2-1 sheets are tied to these parent drawings and not the sheets. Table 7.2-5 provides a cross reference to match the APP-PMS-J1 drawing to its corresponding Figure 7.2-1 sheet.

7.2.1.1 Functional Description

The following subsections describe the specific reactor trip functions and are grouped according to the following 11 conditions:

- Subsection 7.2.1.1.1 Nuclear Startup Trips
- Subsection 7.2.1.1.2 Nuclear Overpower Trips
- Subsection 7.2.1.1.3 Core Heat Removal Trips
- Subsection 7.2.1.1.4 Primary Overpressure Trips
- Subsection 7.2.1.1.5 Loss of Heat Sink Trips
- Subsection 7.2.1.1.6 Feedwater Isolation Trip
- Subsection 7.2.1.1.7 Automatic Depressurization Systems Actuation Reactor Trip
- Subsection 7.2.1.1.8 Core Makeup Tank Injection Trip
- Subsection 7.2.1.1.9 Reactor Trip on Passive Residual Heat Removal Actuation
- Subsection 7.2.1.1.10 Reactor Trip on Safeguards Actuation
- Subsection 7.2.1.1.11 Manual Reactor Trip

Table 7.2-2 lists the reactor trips and summarizes the coincidence logic to trip. Table 7.2-3 provides the interlocks for each trip. Table 7.2-4, lists system level manual inputs to reactor trip functions.

7.2.1.1.1 Nuclear Startup Trips

Source Range High Neutron Flux Trip

Source range high neutron flux trips the reactor when two of the four source range channels exceed the trip setpoint. This trip provides protection during reactor startup and plant shutdown. This function is delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious trip due to the short term instability of the processed source range values. This trip function may be manually blocked and the high voltage source range detector power supply de-energized when the intermediate range neutron flux is above the P-6 setpoint value. It is automatically blocked by the power range neutron flux interlock (P-10). The trip may be manually reset when neutron flux is between P-6 and P-10. The reset occurs automatically when the intermediate range flux decreases below P-6. The channels can be individually bypassed to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated in the main control room.

Figure 7.2-1, sheet 3 shows the logic for this trip. This sheet also shows the development of permissive P-6 while P-10 is shown in Figure 7.2-1, sheet 4.

Intermediate Range High Neutron Flux Trip

Intermediate range high neutron flux trips the reactor when two of the four intermediate range channels exceed the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if the power range channels are above approximately 10-percent power (P-10).

The trip is automatically reset when the power range channels indicate less than 10-percent power. The intermediate range channels, including detectors, are separate from the power range channels. The intermediate range channels can be individually bypassed to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated in the main control room.

Figure 7.2-1, sheet 3 shows the logic for this trip. The development of permissive P-10 is shown in Figure 7.2-1, sheet 4.

Power Range High Neutron Flux Trip (Low Setpoint)

Power range high neutron flux (low setpoint) trips the reactor when two of the four power range channels exceed the trip setpoint.

The trip, which provides protection during startup, can be manually blocked when the power range channels are above approximately 10-percent power (P-10). The trip is automatically reset when the power range channels indicate less than 10-percent power.

Figure 7.2-1, sheet 3 shows the logic for this trip. The development of permissive P-10 is shown on Figure 7.2-1, sheet 4.

7.2.1.1.2 Nuclear Overpower Trips

Power Range High Neutron Flux Trip (High Setpoint)

Power range high neutron flux (high setpoint) trips the plant when two of the four power range channels exceed the trip setpoint. It provides protection against excessive core power generation during normal operation and is always active. Figure 7.2-1, sheet 4 shows the logic for this trip.

Power Range High Positive Flux Rate Reactor Trip

This trip protects the reactor when a sudden abnormal increase in power occurs in two out of the four power range channels. It provides protection against ejection accidents of low worth rods from midpower. It is always active. A channel is tripped when rate-sensitive circuits in the channel detect rates of change in nuclear power above the setpoint value. The channel trip is latched such that the partial trip signal does not disappear when the rate of change in power goes below the setpoint value. Once latched, the channel can only be reset from the main control room by manual action. The reactor is tripped when two out of the four rate channels have tripped.

Figure 7.2-1, sheet 4 shows the logic for this trip.

7.2.1.1.3 Core Heat Removal Trips

Overtemperature ΔT Reactor Trip

The overtemperature ΔT trip provides core protection to prevent departure from nucleate boiling for combinations of pressure, power, coolant temperature, and axial power distribution. The protection is provided if the transient is slow with respect to piping transient delays from the core to the temperature detectors and pressure is within the range between the high and low pressure reactor trips. This setpoint includes corrections for changes in density and heat capacity of water with temperature and dynamic compensation for piping delays from the core to the loop temperature detectors. With normal axial power distribution, this reactor trip limit is always below the core safety limit. If axial peaks are greater than design, as indicated by the difference between upper and lower power range nuclear detectors, the reactor trip limit is automatically reduced. Two hot leg temperature measurements per loop are combined with individual cold leg temperature measurements to form four ΔT power signals, $q_{\Delta T}$.

The ΔT power signal, $q_{\Delta T,}$ is the calculated core power based on the properties of compressed water at the measured hot leg T_H, cold leg temperature, T_C, and pressurizer pressure, P_{PZR}:

$q_{\Delta T}$ = $f(T_H, T_C, P_{PZR})$

$q_{\Delta T}$ = $\rho(T_C, P_{ZR})[h(T_H, P_{ZR}) – h(T_C, P_{ZR}) – C]/\Delta T°$

Where:

T_C = $(1+\tau_1 s)/[(1+\tau_2 s)(1+\tau_3 s)]T_{COLD}$, where T_{COLD} is the measured cold leg temperature (lead/lag compensation with time constants τ_1, τ_2, and τ_3 applied to compensate for cold leg-to-core transit time)

T_H = $(1+\tau_4 s)/[(1+\tau_5 s)(1+\tau_6 s)]T_{HOT}$, where T_{HOT} is the measured hot leg temperature (lead/lag compensation with time constants τ_4, τ_5, and τ_6 applied to compensate for core-to-hot leg transit time)

$\rho(T_C,P_{PZR})$ = density of water at cold leg temperature in the cold leg (T_C) and pressurizer pressure, P_{PZR}

$h(T,P_{PZR})$ = enthalpy of water at the specified temperature (T_H or T_C) and pressurizer pressure P_{PZR}

ΔT° = a conversion factor, such that the value of $q_{\Delta T}$ is 100 percent at normal rated thermal power

C = a bias coefficient that permits zeroing $q_{\Delta T}$ at zero power (to compensate for small errors in RTD calibration)

s = Laplace transform operator

The ΔT setpoint for the overtemperature trip is continuously calculated, with one set of temperature measurements per loop by interpolating from tabulated core safety limits, with correction, (if needed) for adverse axial power distribution.

$OT\Delta T_{SP}$ = $OT\Delta T_{SP}^{\circ} - f_1(\Delta I)$

Where:

$f_1(\Delta I)$ = the penalty associated with an adverse axial power distribution

$OT\Delta T_{SP}^{\circ}$ = the core DNB thermal design limit with design axial power distribution

$OT\Delta T_{SP}^{\circ}$ = $f(P_{PZR}, TC)$. The function, f(P,T), is determined by interpolation from specified tables of allowable core thermal power as a function of core inlet temperature at various pressures.

P_{PZR} and T_C, pressurizer pressure and cold leg temperature, are as defined previously.

A reactor trip is initiated if $q_{\Delta T} \geq OT\Delta T_{SP}$ in two of the four divisions.

Two separate ionization chambers supply the upper and lower flux signal for each overtemperature ΔT channel.

Increases in ΔI beyond a predefined deadband results in a decrease in trip setpoint.

The required one pressurizer pressure parameter per loop is obtained from four separate sensors connected to pressure taps at the top of the pressurizer.

Figure 7.2-1, sheet 5, shows the logic for the overtemperature ΔT trip function.

A more detailed description of the Overtemperature ΔT reactor trip is provided in Reference 5.

Overpower ΔT Trip

The Overpower ΔT reactor trip provides confidence of fuel integrity during overpower conditions, limits the required range for overtemperature ΔT protection, and provides a backup to the power range high neutron flux trip.

A reactor trip is initiated if the ΔT power signal, $q_{\Delta T}$, exceeds the setpoint in two of the four divisions; that is, if:

$$q_{\Delta T} \geq OP\Delta T_{SP} = C_{OP}^{\circ} - f_2(\Delta I),$$

Where:

$q_{\Delta T}$ is the same ΔT power signal used for the Overtemperature ΔT reactor trip

C_{OP}° = A preset bias

$f_2(\Delta I)$ = A function of the neutron flux difference between upper and lower ionization chamber flux signals; to correct, if necessary, for an adverse axial flux shape.

Increases in ΔI beyond a predefined deadband results in a decrease in trip setpoint.

The source of temperature and neutron flux information is identical to that of the overtemperature ΔT trip, and the resultant ΔT setpoint is compared to the same measured ΔT power signal. Figure 7.2-1, sheet 5, shows the logic for this trip function.

A more detailed description of the Overpower ΔT reactor trip is provided in Reference 5.

Reactor Trip on Low Pressurizer Pressure

This trip protects against low pressure, which could lead to departure from nucleate boiling. The parameter sensed is reactor coolant pressure as measured in the pressurizer. This trip is automatically blocked when reactor power is below the P-10 permissive setpoint to allow control rod testing during cold, depressurized conditions. The trip is automatically reset when reactor power is above the P-10 setpoint.

Figure 7.2-1, sheet 5, shows the logic for this trip. The development of the P-10 permissive is shown in Figure 7.2-1, sheet 4.

Reactor Trip on Low Reactor Coolant Flow

This trip protects against departure from nucleate boiling in the event of low reactor coolant flow. Flow in each hot leg is measured at the hot leg elbow. The trip on low flow in the hot legs is automatically blocked when reactor power is below the P-10 permissive setpoint. This enhances reliability by preventing unnecessary reactor trips. The trip function is automatically reset when reactor power is above the P-10 setpoint.

Figure 7.2-1, sheet 5 shows the logic for this trip. The development of permissive P-10 is shown in Figure 7.2-1, sheet 4.

Reactor Trip on Reactor Coolant Pump Underspeed

This trip protects the reactor core from departure from nucleate boiling in the event of a loss of flow in more than one loop. This protection is provided by tripping the reactor when the speed on two out of the four reactor coolant pumps falls below the setpoint. Loss of flow in more than one loop could be caused by a voltage or frequency transient in the plant power supply such as would occur during a station blackout. It could be caused by inadvertent opening of more than one reactor coolant pump circuit breaker. There is one speed detector mounted on each reactor coolant pump. The trip is automatically blocked when reactor power is below the P-10 permissive setpoint to enhance reliability by preventing unnecessary reactor trips. The trip is automatically reset when reactor power is above the P-10 setpoint.

Figure 7.2-1, sheet 5, shows the logic for this trip. The development of P-10 is shown in Figure 7.2-1, sheet 4.

Reactor coolant pump speed is detected by a probe mounted on the reactor coolant pump frame. The speed signal is transmitted to the protection and safety monitoring system to provide the input to the trip logic function.

The reactor coolant pump underspeed trip provides a direct measurement of the parameter of interest. It permits the plant to ride through many postulated voltage or frequency dip transients without reactor trip if safety limits are not violated. Selection of the underspeed trip setpoint and time response provide for the timely initiation of reactor trip during the complete loss of flow accident and the limiting frequency decay event, consistent with the analysis results reported in Chapter 15.

The reactor coolant pump speed detectors perform their protective function (during the complete loss of flow accident and the limiting frequency decay event) in an environment (temperature, humidity, pressure, chemical, and radiation) that is not changed by the event. Therefore, it is not necessary to impose environmental qualification requirements on these detectors more restrictive than those imposed for use under rated conditions. The reactor coolant pump speed detectors are qualified for use under rated conditions with their performance verified by operation in the plant. The reactor coolant pump speed detectors are qualified to the most limiting vibrations experienced by pump operation.

Reactor Trip on High Reactor Coolant Pump Bearing Water Temperature

This trip is an anticipatory trip based on the expectation of a complete loss of reactor coolant flow if cooling water is lost to any of the reactor coolant pumps. This trip occurs before the reactor coolant pumps are tripped on the same measurement.

Figure 7.2-1, sheet 5, shows the logic for this trip.

7.2.1.1.4 Primary Overpressure Trips

Pressurizer High Pressure Reactor Trip

This trip protects the reactor coolant system against system overpressure. The same sensors used for the pressurizer low pressure reactor trip are used for the high pressure trip except that separate setpoints are used. The high pressurizer pressure protection trips the reactor when two out of the four pressurizer pressure channels exceed the trip setpoint. There are no interlocks or permissives associated with this trip function.

Figure 7.2-1, sheet 6, shows the logic for this trip.

High-3 Pressurizer Water Level Reactor Trip

This trip is provided as backup to the high pressurizer pressure reactor trip and serves to prevent water relief through the pressurizer safety valves. The high-3 pressurizer water level protection trips the reactor when two out of the four pressurizer water level channels exceed the trip setpoint. The level signal is compensated for both reference leg temperature and system pressure. The trip is automatically blocked when reactor power is below the P-10 permissive setpoint. This permits control rod testing with the plant cold and the pressurizer water solid. The trip is automatically reset when reactor power is above the P-10 setpoint.

Figure 7.2-1, sheet 6, shows the logic for the trip. The development of P-10 is shown in Figure 7.2-1, sheet 4.

7.2.1.1.5 Loss of Heat Sink Trip

Reactor Trip on Low Water Level in any Steam Generator

This trip protects the reactor from loss of heat sink in the event of a loss of feedwater to the steam generators. The reactor is tripped when two out of the four water level sensors in any steam generator produce signals below the setpoint value.

Figure 7.2-1, sheet 7, shows the logic for the trip. There are no interlocks or permissives associated with this trip.

7.2.1.1.6 Feedwater Isolation Trip

High-2 Steam Generator Water Level in Any Steam Generator

This function is an anticipatory trip based on the expectation that a reactor trip would occur after steam generator feedwater is isolated. The plant control system uses a lower steam generator water level setpoint, High-1, to close the feedwater control valves. This provides an interval for operator action to prevent total isolation of the steam generator and a reactor trip before the High-2 setpoint is exceeded. The trip on High-2 steam generator water level may be manually blocked below the P-11 permissive setpoint to allow control rod testing. The trip is automatically reset when the pressurizer pressure is above the P-11 setpoint.

Figure 7.2-1, sheet 10, shows the logic for this trip function.

7.2.1.1.7 Automatic Depressurization Systems Actuation Reactor Trip

A reactor trip is initiated if an automatic depressurization system actuation occurs either automatically or manually. This provides a reactor trip if the system is depressurized and a trip is not initiated from another source. The automatic depressurization system actuation function is discussed in Subsection 7.3.1.2.4.

Manual automatic depressurization system actuation is initiated from either of two sets of controls in the main control room. Operating either of the two sets of controls also sends a reactor trip signal to the reactor trip switchgear breakers. Outputs on the control sets, physically and electrically separated, send their position status to the protection and safety monitoring system. These inputs de-energize the undervoltage trip attachments on the reactor trip breakers, causing them to trip open. Additional outputs interrupt power to the shunt trip interposing relays, actuating the shunt trip attachments on each reactor trip circuit breaker. These provide a backup to the undervoltage trip of the breakers.

Figure 7.2-1, sheet 15 shows the logic for this trip function. There are no interlocks or bypasses associated with this trip.

7.2.1.1.8 Core Makeup Tank Injection Trip

A reactor trip is initiated if core makeup injection occurs either automatically or manually. Since core makeup tank injection results in a trip of the reactor coolant pumps, providing a reactor trip upon core makeup tank injection maximizes the margin to DNB at all power levels. The core makeup tank injection function is discussed in Subsection 7.3.1.2.3.

Manual core makeup tank injection is initiated from either of two controls in the main control room. Operating either of the two controls also sends a reactor trip signal to the reactor trip switchgear breakers. Outputs on each control, physically and electrically separated, send their position status to the protection and safety monitoring system. These inputs de-energize the undervoltage trip attachments on the reactor trip breakers, causing them to trip open. Additional outputs on each control interrupt power to the shunt trip interposing relays, actuating the shunt trip attachments on each reactor trip circuit breaker. These provide a backup to the undervoltage trip of the breakers.

Figure 7.2-1, sheets 2 and 12 show the logic for this trip function. There are no interlocks or bypasses associated with this trip.

7.2.1.1.9 Reactor Trip on Passive Residual Heat Removal System Actuation

A reactor trip is initiated when the passive residual heat removal (PRHR) system's discharge valves come off their fully shut seat, allowing flow through the PRHR heat exchanger (PRHR HX). This reactor trip will prevent the fuel design limits from being exceeded in the event the PRHR HX is inadvertently aligned to allow flow when the reactor is being operated at power conditions. The PRHR HX alignment is discussed in Subsection 7.3.1.2.7.

Figure 7.2-1, sheets 2 and 4 show the logic for this trip function. There are no interlocks or bypasses associated with this trip.

7.2.1.1.10 Reactor Trip on Safeguards Actuation

A reactor trip is initiated with any signal that causes a safeguards actuation. This reactor trip occurs whether the safeguards actuation is commanded automatically or manually. The means for actuating safeguards automatically are described in Section 7.3. This trip protects the core against a loss of reactor coolant or a steam line rupture.

Manual safeguards actuation is initiated from either of two controls in the main control room. Operating either of the two controls also sends a reactor trip signal to the reactor trip switchgear breakers. Outputs on each control, physically and electrically separated, send their position status to the protection and safety monitoring system. These inputs de-energize the undervoltage trip attachments on the reactor trip breakers, causing them to trip open. Additional outputs on each control interrupt power to the shunt trip interposing relays, actuating the shunt trip attachments on each reactor trip circuit breaker. These provide a backup to the undervoltage trip of the breakers.

Figure 7.2-1, sheets 2 and 11, show the logic for this trip function. There are no interlocks or bypasses associated with this trip.

7.2.1.1.11 Manual Reactor Trip

The manual reactor trip consists of 2 controls in the main control room, either of which trip all 8 of the reactor trip switchgear breakers. The reactor trip circuit breakers contain both undervoltage and shunt trip attachments. The shunt trip acts as a diverse backup to the undervoltage trip in the breakers. Contacts on each control, physically and electrically separated, are in series with the undervoltage trip attachment on the reactor trip breakers, the shunt trip attachment interposing

relays, and the power outputs at the protection and safety monitoring system cabinet. Actuating either control interrupts power from the voting logic to the undervoltage trip attachments, releasing them. It also interrupts power to shunt trip interposing relays, actuating the shunt trip attachments. The breakers trip when either the shunt trip attachments are energized or the undervoltage trip attachments are de-energized. Actuating either manual trip control causes each breaker to trip by initiating both of these actions.

Figure 7.2-1, sheets 2 and 13, show the logic for the manual trip. There are no interlocks or bypasses associated with this trip.

7.2.1.1.12 Reactor Trip System Interlocks

The interlocks used in the reactor trip functions are designated as P-xx permissives. Table 7.2-3 provides a listing of these interlocks. These permissives are implemented at the channel level rather than at the logic level because plant availability has been determined to be improved using this technique of integrating permissives into each channel.

Manual blocks to reactor trip are listed on Table 7.2-4 and are described in the following subsections. The source, intermediate, power (low setpoint), and steam generator water level manual blocks, when used in conjunction with the applicable permissives, are implemented during startup.

Source Range Block (One Control for each Division)

The source range reactor trip may be manually blocked upon the occurrence of the P-6 permissive and is automatically reset when the permissive condition is not met. The channel is automatically blocked upon the occurrence of the P-10 permissive with the block automatically removed when the P-10 condition is not met. Figure 7.2-1, sheet 3, shows these blocks.

Intermediate Range Block (One Control for each Division)

The intermediate range reactor trip may be manually blocked upon the occurrence of the P-10 permissive and is automatically reset when the permissive condition is not met. Figure 7.2-1, sheet 3, shows this block.

Power Range (Low Setpoint) Block (One Control for each Division)

The power range low setpoint reactor trip may be manually blocked upon the occurrence of the P-10 permissive and is automatically reset when the permissive condition is not met. Figure 7.2-1, sheet 3, shows this block.

Steam Generator High-2 Water Level Block (One Control for each Division)

The steam generator High-2 reactor trip may be manually blocked upon the occurrence of the P-11 permissive. This trip function is automatically reset when the permissive condition is not met. Figure 7.2-1, sheets 9, 10, and 11, illustrates the functional logic relating to this function.

7.2.1.1.13 Bypasses of Reactor Trip Functions

Each channel used in reactor trip can be bypassed, as discussed in Subsection 7.1.2.9, except for reactor trips resulting from manual initiations. One channel can be bypassed for an indefinite period of time with the normal two-out-of-four trip logic automatically reverting to a two-out-of-three trip logic. Bypassing two or more channels is not allowed.

7.2.1.2 Design Basis for Reactor Trips

This section provides the design bases information on the reactor trip function, including the information required by Section 4 of IEEE-603-1991. Reactor trip is a protective function generated as part of the protection and safety monitoring system. Those design bases relating to the equipment that initiates and accomplishes reactor trips are contained in WCAP-15776 (Reference 2). The design bases presented here concern the variables monitored for reactor trips, the minimum performance requirements in generating the trips, and the requirements placed on reactor trips during various reactor operating modes.

7.2.1.2.1 Design Basis: Generating Station Conditions Requiring Reactor Trip (Paragraph 4.1 of IEEE-603-1991)

The generating station conditions requiring protective actions are analyzed in Chapter 15. Conditions that result in a reactor trip are listed in Table 15.0-6. This table correlates the accident conditions (II, III, or IV events) to each reactor trip.

7.2.1.2.2 Design Basis: Variables, Levels, Ranges, and Accuracies Used in Reactor Trip Functions (Paragraphs 4.1, 4.2, and 4.4 of IEEE-603-1991)

The variables monitored for reactor trips are:

- Neutron flux
- Reactor coolant pump bearing water temperature
- Pressurizer pressure
- Water level in the pressurizer
- Reactor coolant flow in each loop
- Speed of each reactor coolant pump
- Water level in each steam generator
- Cold leg temperature (T_{cold}) in each loop
- Hot leg temperature (T_{hot}) in each loop
- Status of each manual reactor trip control
- Status of PRHR HX discharge valves

The ranges, accuracies, and response times for each variable are listed on Table 7.2-1.

A discussion on levels that require reactor trip is contained in Subsection 7.2.1.1.

The reactor trip setpoints are maintained by the setpoint program, which is described in the technical specifications (Chapter 16).

7.2.1.2.3 Design Basis: Spatially Dependent Parameters Used in Reactor Trip (Paragraph 4.6 of IEEE-603-1991)

The hot and cold leg temperature signals required for input to the protection and control functions are obtained using thermowell-mounted RTDs installed in each reactor coolant loop. The hot leg temperature measurement in each loop is accomplished using six fast-response, narrow-range RTDs each in its own thermowell; three thermowells are RTDs for each of the two divisions monitoring that hot leg. The three thermowells for each division are mounted approximately 120 degrees apart in the cross-sectional plane of the piping, to obtain a representative temperature sample. The temperatures measured by the three RTDs are different due to hot leg temperature streaming and vary as a function of thermal power. Therefore, these signals are averaged using electronic weighting to generate a hot leg average temperature. Provisions are incorporated into the process electronics to

allow for operation with only two RTDs in service. The two RTD measurements can be biased to compensate for the loss of the third RTD.

Radially varying cold leg temperature is not a concern since the resistance temperature detectors are located downstream of the reactor coolant pumps. The pumps provide mixing of the coolant so that radial temperature variations do not exist.

Radial neutron flux is not a spatially dependent concern because of core radial symmetry. Axial variation in neutron flux is used for calculations involving overtemperature and overpower ΔT. Excore detectors furnish this axially-dependent information to the overtemperature and overpower calculators. See Subsection 7.2.1.1.3.

7.2.1.2.4 Design Basis: Operational Limits for Variables in Various Reactor Operating Modes (Paragraph 4.3 of IEEE-603-1991)

During startup or shutdown, reactor trips are provided for three ranges of neutron flux (source, intermediate, and power range). The source range, intermediate range, and power range (low setpoint) trips are manually blocked when the appropriate power escalation permissives are present. The trips are automatically reset during power de-escalation. Subsection 7.2.1.1.1 describes these reactor trips. Their interlocks are described in Subsection 7.2.1.1.12.

During testing or maintenance, functions are provided to bypass a channel monitoring a variable for reactor trip. Although no setpoints need to be changed for bypassing, the coincidence logic is automatically adjusted as described in Subsection 7.2.1.1.13. The logic provides that the remaining redundant channels for that variable meet the single failure criterion. The two-out-of-four logic is automatically reinstated when the bypass is removed.

7.2.1.2.5 Design Basis: Reactor Trips for Malfunctions, Accidents, Natural Phenomena, or Credible Events (Paragraph 4.7 and 4.8 of IEEE-603-1991)

There are no reactor trip functions that directly shutdown the reactor on occurrence of either natural phenomena (such as seismic flood or wind) or internal events (such as fire or pipe whip). The operator can trip the reactor at any time by actuating the manual reactor trip.

Functional diversity is used to determine the reactor trips for accident conditions. Generally, two or more reactor trips occur for the transients analyzed in the accident analyses.

For example, protection is provided for the complete loss of coolant flow event by low reactor coolant pump speed and by low coolant flow reactor trips. Complete reliance is not made on a single reactor trip terminating a given event. Table 15.0-6 lists the reactor trips and the conditions which normally result in each trip.

Redundancy provides confidence that reactor trips are generated on demand, even when the protection system is degraded by a single failure. Reactor trips are four-way redundant. The single failure criterion is met even if one channel is bypassed, as discussed in Subsection 7.2.1.1.13. More than one bypass is not allowed.

7.2.1.3 System Drawings

Functional diagrams of the reactor trip function are provided in Figure 7.2-1.

7.2.2 Analyses

7.2.2.1 Failure Modes and Effects Analysis (FMEA)

A failure modes and effects analysis was performed on the AP1000 protection and safety monitoring system. Through the process of examining the feasible failure modes, it was concluded that the AP1000 protection system maintains safety functions during single point failures. The AP1000 failure modes and effects analysis is documented in Reference 1. The Common Q failure modes and effects analysis is documented in Reference 3 and also concludes that the protection system maintains safety functions during single point failures.

7.2.2.2 Conformance of the Reactor Trip Function to Applicable Criteria

Reactor trip is a protective function generated by the AP1000 protection and safety monitoring system. Requirements addressing equipment in the protection and safety monitoring system are presented in WCAP-15776 (Reference 2). The discussions presented in this subsection address only the functional aspects of reactor trip.

7.2.2.2.1 Conformance to the General Functional Requirements for Reactor Trip (Section 5 of IEEE-603-1991, GDC-13, GDC-20)

The protection and safety monitoring system initiates a reactor trip whenever a condition monitored by the system reaches a preset level. The reactor trips are listed in Table 7.2-2 and are discussed in Subsection 7.2.1.1. The variables which are monitored for these trips are listed in Subsection 7.2.1.2.2. Table 7.2-1 lists the ranges, accuracies, and response times for these variables. The reactor trip setpoints are listed in the technical specifications, Chapter 16.

As discussed in WCAP-15776 (Reference 2), the setpoints set into the protection and safety monitoring system equipment provide a margin to the safety limits which are assumed in the accident analyses. The safety limits are based on mechanical or hydraulic limitations of equipment or on heat transfer characteristics of the reactor core. While most setpoints used for reactor trip are fixed, there are continuously calculated setpoints for the overtemperature and overpower ΔT trips. Setpoints for reactor trip are selected on the basis of engineering design and safety studies. The setpoints provide a margin to allow for uncertainties and instrument errors.

The overtemperature and overpower conditions are not directly measurable quantities. However, the process variables that determine overtemperature and overpower conditions are sensed and evaluated. Small isolated changes in various process variables may not individually result in reaching a core safety limit. However, the combined variations over time may cause the overtemperature or overpower limit to be exceeded. The design concept for reactor trips takes cognizance of this situation by providing reactor trips associated with individual process variables in addition to the overtemperature and overpower ΔT safety limit trips. Process variable trips prevent reactor operation when a monitored value reaches a core or safety limit. Overtemperature and overpower ΔT trips provide protection for slow transients. Other trips, such as low flow or high flux, trip the reactor for rapid changes in flow or flux respectively.

Table 15.0-6 summarizes events which normally result in reactor trips.

7.2.2.2.2 Conformance to the Single Failure Criterion for Reactor Trip (Paragraph 5.1 of IEEE 603-1991, IEEE 379-2000)

A single failure in the protection and safety monitoring system or the reactor trip actuation divisions does not prevent a reactor trip, even when a reactor trip channel is bypassed for test or maintenance. Conformance of the equipment to this requirement is discussed in WCAP-15776 (Reference 2). In

addition to the redundancy of equipment, diversity of reactor trip functions is incorporated. Most Condition II, III, or IV events requiring a reactor trip are protected by trips from diverse parameters. For example, reactor trip, because of an uncontrolled rod cluster control assembly bank withdrawal at power, may occur on power range high neutron flux, overtemperature, overpower, pressurizer high pressure or pressurizer high water level. Reactor trip on complete loss of reactor coolant flow may occur on low flow or from the diverse parameter of low reactor coolant pump speed.

7.2.2.2.3 Conformance to the Requirements Covering Control and Reactor Trip Interactions (Paragraphs 5.6 and 6.3 of IEEE 603-1991, GDC-24)

The AP1000 is designed to permit maneuvering of the plant in response to normal power generation demands without causing a reactor trip. The plant control system attempts to keep the reactor operating away from any safety limit. However, the selection of the reactor trip setpoints does not take credit for such control actions. The accident analyses in Chapter 15 assume that the plant is at normal operation commensurate with the operating mode at the onset of the accident. If a control system action leads to more conservative results, that assumption is made. If failure of a control system to work leads to more conservative results, that assumption is made. In this way, reactor trips do not depend on control system actions.

As stated in Subsection 7.7.1.12, it is considered advantageous to use certain protection data for control functions. Isolation devices are incorporated into the protection system to prevent control system failures from degrading the performance of the protection system.

Failures in a protection channel monitoring a variable that is also used for control do not result in control system actions requiring protection by the redundant channels monitoring that variable. This is discussed in WCAP-15776 (Reference 2).

7.2.2.2.4 Conformance to Requirements on the Derivation of System Inputs for Reactor Trip (Paragraph 6.4 of IEEE 603-1991)

To the extent feasible, inputs used for reactor trip are derived from signals that are direct measurements of the desired variables. Two exceptions exist, overtemperature and overpower, which cannot be directly measured. The process variables that do affect these parameters can be measured and they are used to continuously calculate the setpoints.

The overtemperature ΔT trip setpoint is calculated from pressurizer pressure, reactor coolant temperature, and nuclear axial power shape. The setpoint is compared against the measured ΔT power signal.

Overpower ΔT is calculated from reactor coolant temperature and the nuclear axial power shape in the core. This value is compared against the measured ΔT power signal.

The overtemperature and overpower ΔT trips are described in Subsection 7.2.1.1.3.

7.2.2.2.5 Conformance to Requirements on Bypassing of Reactor Trip Functions (Paragraph 5.8, 5.9, 6.6, and 6.7 of IEEE 603-1991)

With the exception of the manual reactor trips, reactor trip channels and the reactor trip actuation divisions are permitted to be bypassed as described in WCAP-15776 (Reference 2).

Operating bypasses for reactor trips are described in Subsection 7.2.1.1.13.

7.2.2.2.6 Conformance to Requirements on Multiple Setpoints Used for Reactor Trips (Paragraph 6.8.2 of IEEE 603-1991)

For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the protection and safety monitoring system hardware and software are designed to provide positive means or administrative control to ensure that the more restrictive trip setpoint is used. The hardware and software used to prevent improper use of less restrictive trip settings are considered part of the protection and safety monitoring system.

7.2.2.2.7 Conformance to the Requirement for Completion of Reactor Trip Once Initiated (Paragraph 5.2 of IEEE 603-1991, Regulatory Guide 1.62)

Once initiated, reactor trips proceed to completion. Return to operation requires deliberate operator action to reset the reactor trip circuit breakers that are opened by the reactor trip signal. The circuit breakers cannot be closed while the reactor trip signals are present from the respective protection and safety monitoring system division. A manual control is provided in the main control room to reset (close) the reactor trip breakers when all reactor trip signals have been cleared. The reset feature is not a safety function. Refer also to WCAP-15776 (Reference 2).

7.2.2.2.8 Conformance to the Requirement to Provide for Manual Initiation of Reactor Trip (Paragraph 6.2 of IEEE 603-1991, Regulatory Guide 1.62)

The reactor is tripped by actuating one of two manual reactor trip controls from the main control room. The reactor is also tripped upon manual actuation of the automatic depressurization system, manual core makeup tank injection, or upon manual safeguards actuation. These reactor trips are described in Subsections 7.2.1.1.7, 7.2.1.1.8, 7.2.1.1.10, and 7.2.1.1.11. Refer also to WCAP-15776 (Reference 2).

7.2.3 Combined License Information

The FMEA for the protection and safety monitoring system is addressed in WCAP-16438-P (Reference 1) and WCAP-16592-P (Reference 4).

7.2.4 References

1. WCAP-16438-P (Proprietary), WCAP-16438-NP (Non-Proprietary), “FMEA of AP1000 Protection and Safety Monitoring System,” Revision 3 (as modified by changes provided in UFSAR Appendix 7A).

2. WCAP-15776, “Safety Criteria for the AP1000 Instrument and Control Systems,” April 2002.

3. WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Appendix 3, Rev. 0, “Common Qualified Platform, Digital Plant Protection System,” May 2003.

4. WCAP-16592-P (Proprietary), WCAP-16592-NP (Non-Proprietary), “Software Hazards Analysis of AP1000 Protection and Safety Monitoring System,” Revision 2.

5. APP-GW-GLR-137, “Bases of Digital Overpower and Overtemperature Reactor Trips,” Revision 1.

Table 7.2-1 (Sheet 1 of 3)
Reactor Trip Variables, Limits, Ranges, and Accuracies
(Design Basis for Reactor Trip)
(Nominal)

Protective Functions	Variable	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Source Range High Neutron Flux	Neutron flux	6 decades of neutron flux: 1 to 10^6 counts per second	±10% of span	0.6
Intermediate Range High Neutron Flux	Neutron flux	8 decades of neutron flux overlapping source range by 2 decades and including 100% power	±10% of span	0.6
Power Range Neutron Flux (Low Setpoint)	Neutron flux	1 to 120% of full power	±5% of span	0.6
Power Range Neutron Flux (High-Setpoint)	Neutron flux	1 to 120% of full power	±5% of span	0.6
Power Range High Positive Flux Rate	Neutron flux	1 to 120% of full power	±1% of span	0.6 (step input of 20% full power)
Overtemperature ΔT			±5% of ΔT span	
	Cold leg temp. (T_{cold})	490° to 610°F		5.5
	Hot leg temp. (T_{hot})	530° to 650°F		5.5
	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δφ)		0.6
Overpower ΔT			±4% of ΔT span	
	Cold leg temp. (T_{cold})	490° to 610°F		5.5
	Hot leg temp. (T_{hot})	530° to 650°F		5.5
	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δφ)		0.6

Table 7.2-1 (Sheet 2 of 3)
Reactor Trip Variables, Limits, Ranges, and Accuracies
(Design Basis for Reactor Trip)
(Nominal)

Protective Functions	Variable	Range of Variables	Typical Accuracy[1]	Typical Response Time (Sec)[2]
Pressurizer Low Pressure	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
Pressurizer High Pressure	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
Pressurizer High Water Level	Pressurizer water level	0-100% of entire cylindrical portion of pressurizer	±5% of span	0.9
Low Reactor Coolant Flow	Coolant flow	0 to 120% of rated flow	±3% of span	0.9
Low Reactor Coolant Pump Speed	Pump speed	0 to 120% of rated speed	±1% of span	0.7
Low Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±22% of span	0.9
High Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±13% of span	0.9
Reactor Coolant Pump High Bearing Water Temperature	Reactor coolant pump bearing water temperature	70°-450°F	±2% of span	5.5

Table 7.2-1 (Sheet 3 of 3)
Reactor Trip Variables, Limits, Ranges, and Accuracies
(Design Basis for Reactor Trip)
(Nominal)

Protective Functions	Variable	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Automatic or Manual Safeguards Actuation	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Manual Reactor Trip	Control status	N/A	N/A	N/A
Automatic or Manual Depressurization System Actuation	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Automatic or Manual Core Makeup Tank Injection	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Automatic or Manual PRHR Actuation	PRHR discharge valve position	Valve closed/valve not-closed	N/A	1.25

Notes:
1. Measurement uncertainty typical of actual applications. Harsh environment allowances have been included where applicable.
2. Delay from the time that the process variable exceeds the setpoint until the time that the control rods are free to fall into the core (includes reactor trip breaker opening delay and control rod drive mechanism gripper release delay).

Table 7.2-2 (Sheet 1 of 2)
Reactor Trips

Reactor Trip[1]	No. of Channels	Division Trip Logic	Bypass Logic	Permissives and Interlocks (See Table 7.2-3)
Source Range High Neutron Flux Reactor Trip	4	2/4	Yes[2]	P-6, P-10
Intermediate Range High Neutron Flux Reactor Trip	4	2/4	Yes[2]	P-10
Power Range High Neutron Flux (Low Setpoint) Trip	4	2/4	Yes[2]	P-10
Power Range High Neutron Flux (High Setpoint) Trip	4	2/4	Yes[2]	----
High Positive Flux Rate Trip	4	2/4	Yes[2]	----
Reactor Coolant Pump Bearing Water Temperature	16 (4/pump)	2/4 in any single pump	Yes[2]	----
Overtemperature ΔT	4 (2/loop)	2/4	Yes[2]	----
Overpower ΔT	4 (2/loop)	2/4	Yes[2]	----
Pressurizer Low Pressure Trip	4	2/4	Yes[2]	P-10
Pressurizer High Pressure Trip	4	2/4	Yes[2]	----
High-3 Pressurizer Water Level Trip	4	2/4	Yes[2]	P-10
Low Reactor Coolant Flow	8 (4/hot leg)	2/4 in either hot leg	Yes[2]	P-10
Reactor Coolant Pump Underspeed	4 (1/pump)	2/4	Yes[2]	P-10
Low Steam Generator Water Level	4/steam generator	2/4 in any steam generator	Yes[2]	----
High-2 Steam Generator Water Level	4/steam generator	2/4 in any steam generator	Yes[2]	P-11

Table 7.2-2 (Sheet 2 of 2)
Reactor Trips

Reactor Trip[1]	No. of Channels	Division Trip Logic	Bypass Logic	Permissives and Interlocks (See Table 7.2-3)
Automatic Safeguards Actuation	4	2/4	Yes[2]	—
Automatic Depressurization System Actuation	4	2/4	Yes[2]	—
Automatic Core Makeup Tank Injection	4	2/4	Yes[2]	—
PRHR Actuation	4	2/4	Yes[2]	—
Manual Safeguards Actuation	2 controls	1/2 controls	No	—
Manual Depressurization System Actuation	4 controls	2/4 controls	No	—
Manual Core Makeup Tank Injection	2 controls	1/2 controls	No	—
Manual Reactor Trip	2 controls	1/2 controls	No	—

Notes:
1. Reactor Trip divisions are also bypassed with the logic as defined in 2. below.
2. Bypass Logic = 2/4 with no bypasses; 2/3 with 1 bypass; more than one bypass is not allowed.

— No permissive or interlock.

Table 7.2-3 (Sheet 1 of 2)
Reactor Trip Permissives and Interlocks

Designation	Derivation	Function
P-6	Intermediate range neutron flux above setpoint	Allows manual block of source range reactor trip
$\overline{\text{P-6}}$	Intermediate range neutron flux below setpoint	Automatically resets source range reactor trip
P-10	Power range nuclear power above setpoint	(a) Allows manual block of power range (low setpoint) reactor trip (b) Allows manual block of intermediate range reactor trip (c) Automatically blocks source range reactor trip (back-up to P-6) (d) Allows reactor trip on low coolant flow (e) Allows reactor trip on low reactor coolant pump speed (f) Allows reactor trip on high pressurizer water level (g) Allows reactor trip on low pressurizer pressure

Table 7.2-3 (Sheet 2 of 2)
Reactor Trip Permissives and Interlocks

$\overline{\text{P-10}}$	Power range nuclear power below setpoint	(a) Prevents the block of power range (low setpoint) reactor trip (b) Prevents the block of intermediate range reactor trip (c) Permits manual reset of each source range channel reactor trip (d) Blocks reactor trip on low coolant flow (e) Blocks reactor trip on low reactor coolant pump speed (f) Blocks reactor trip on high pressurizer water level (g) Blocks reactor trip on low pressurizer pressure
P-11	Pressurizer pressure below setpoint	Allows manual block of High-2 steam generator water level reactor trip
$\overline{\text{P-11}}$	Pressurizer pressure above setpoint	Automatically resets High-2 steam generator water level reactor trip

Table 7.2-4
System-Level Manual Inputs to the Reactor Trip Functions

Manual Control	To Divisions				Figure 7.2-1 Sheet
Manual Reactor Trip Control #1	A	B	C	D	13
Manual Reactor Trip Control #2	A	B	C	D	13
Source Range High Neutron Flux Block, Division A	A				3
Source Range High Neutron Flux Block, Division B		B			3
Source Range High Neutron Flux Block, Division C			C		3
Source Range High Neutron Flux Block, Division D				D	3
Intermediate Range High Neutron Flux Block, Division A	A				3
Intermediate Range High Neutron Flux Block, Division B		B			3
Intermediate Range High Neutron Flux Block, Division C			C		3
Intermediate Range High Neutron Flux Block, Division D				D	3
Power Range High Neutron Flux Block (Low Setpoint), Division A	A				3
Power Range High Neutron Flux Block (Low Setpoint), Division B		B			3
Power Range High Neutron Flux Block (Low Setpoint), Division C			C		3
Power Range High Neutron Flux Block (Low Setpoint), Division D				D	3
Manual Safeguards Actuation Control #1	A	B	C	D	11
Manual Safeguards Actuation Control #2	A	B	C	D	11
Manual Core Makeup Tank Injection Control #1	A	B	C	D	12
Manual Core Makeup Tank Injection Control #2	A	B	C	D	12
Manual Depressurization System Stages 1, 2 & 3 Actuation Controls #1 & 2	A	B	C	D	15
Manual Depressurization System Stages 1, 2 & 3 Actuation Controls #3 & 4	A	B	C	D	15
Steam Line/Feedwater Isolation and Safeguards Block, Division A	A				9
Steam Line/Feedwater Isolation and Safeguards Block, Division B		B			9
Steam Line/Feedwater Isolation and Safeguards Block, Division C			C		9
Steam Line/Feedwater Isolation and Safeguards Block, Division D				D	9

Note:
Controls are located in the main control room except as noted on the applicable sheet of Figure 7.2-1.

Table 7.2-5
Figure 7.2-1 Cross References

APP-PMS-J1 Drawing Number	Figure 7.2-1 Sheet Number
APP-PMS-J1-101	1
APP-PMS-J1-102	2
APP-PMS-J1-103	3
APP-PMS-J1-104	4
APP-PMS-J1-105	5
APP-PMS-J1-106	6
APP-PMS-J1-107	7
APP-PMS-J1-108	8
APP-PMS-J1-109	9
APP-PMS-J1-110	10
APP-PMS-J1-111	11
APP-PMS-J1-112	12
APP-PMS-J1-113	13
APP-PMS-J1-114	14
APP-PMS-J1-115	15
APP-PMS-J1-116	16
APP-PMS-J1-117	17
APP-PMS-J1-119	18
APP-PMS-J1-120	19
APP-DAS-J1-102	20
APP-DAS-J1-103	21

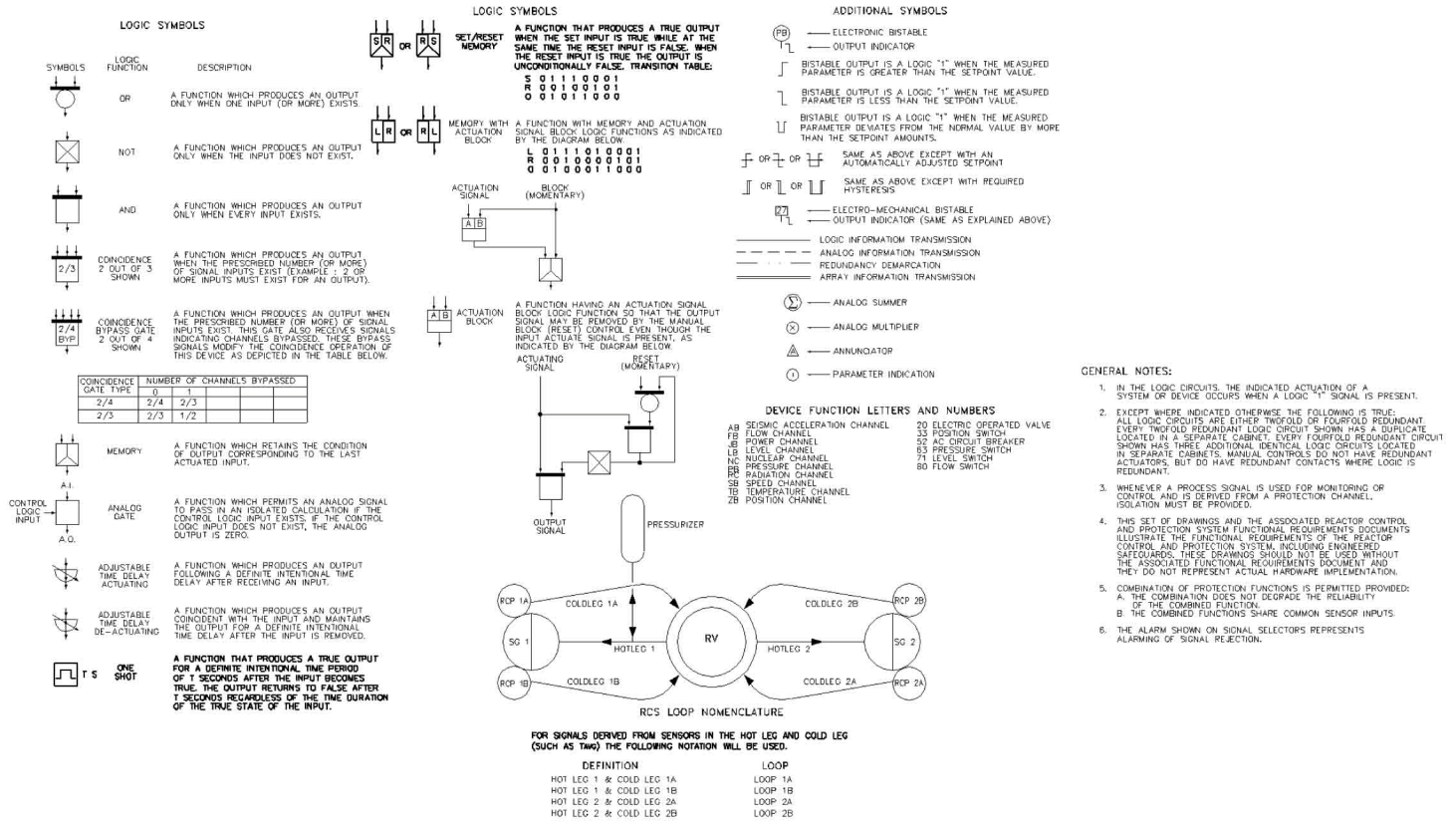


Figure 7.2-1 (Sheet 1 of 21)
Functional Diagram
Index and Symbols

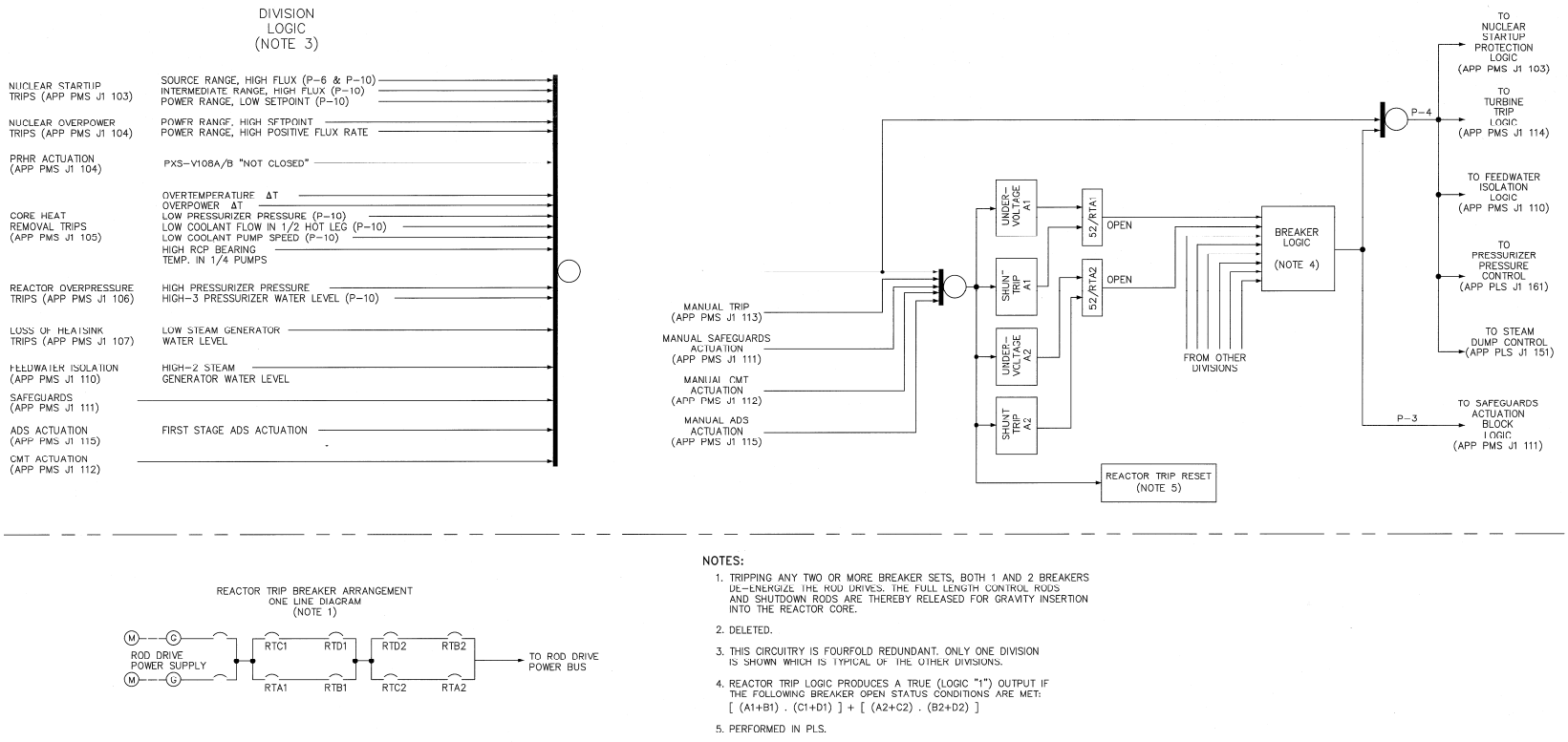


Figure 7.2-1 (Sheet 2 of 21)
Functional Diagram
Reactor Trip Functions

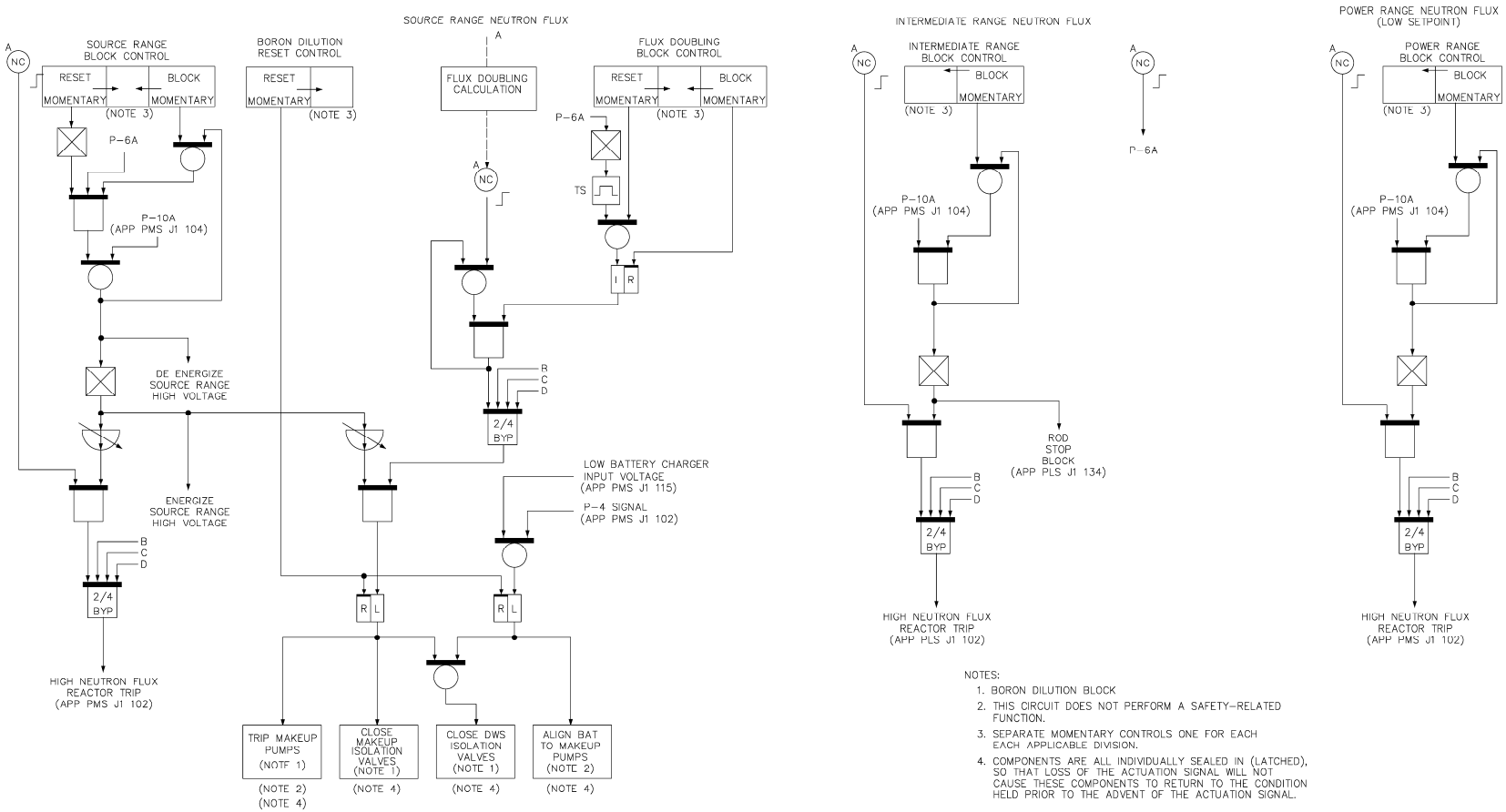
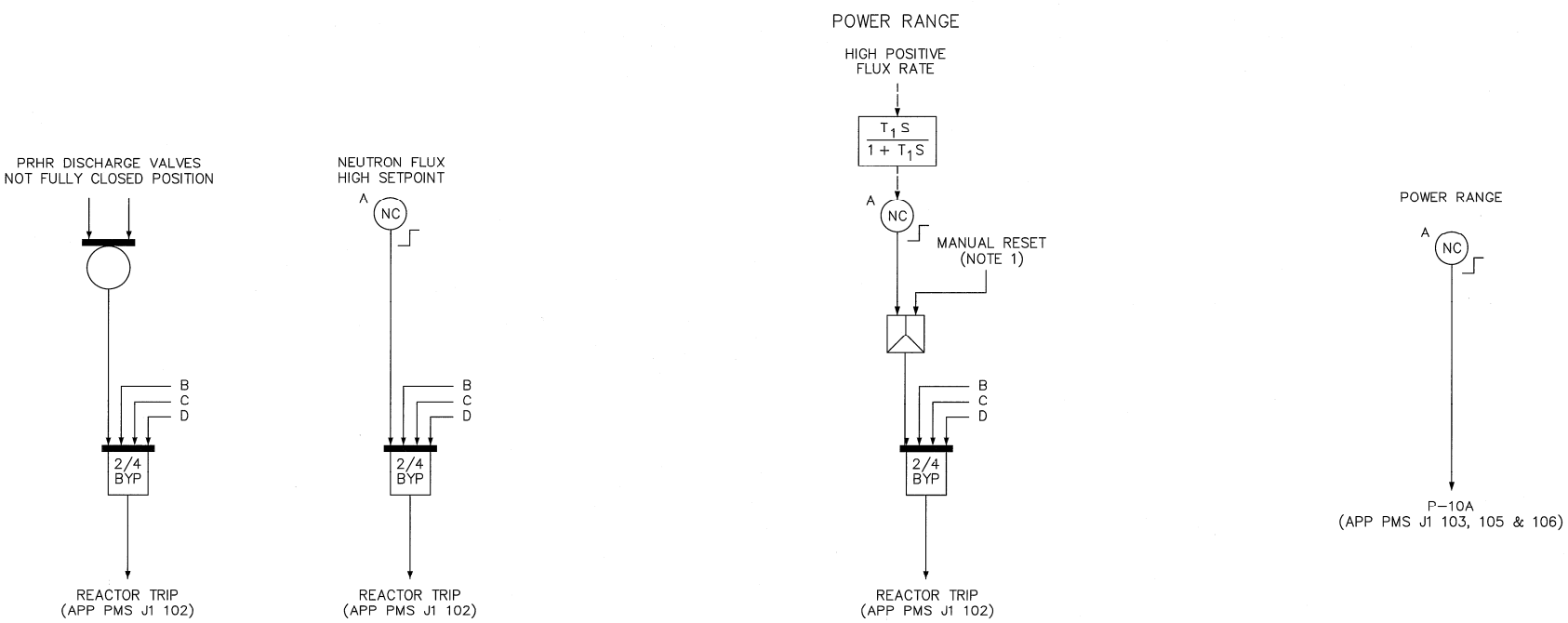


Figure 7.2-1 (Sheet 3 of 21)
Functional Diagram
Nuclear Startup Protection



NOTES:

1. FOUR MOMENTARY CONTROLS, ONE FOR EACH DIVISION.
2. DELETED.

Figure 7.2-1 (Sheet 4 of 21)
Functional Diagram
Nuclear Overpower Protection

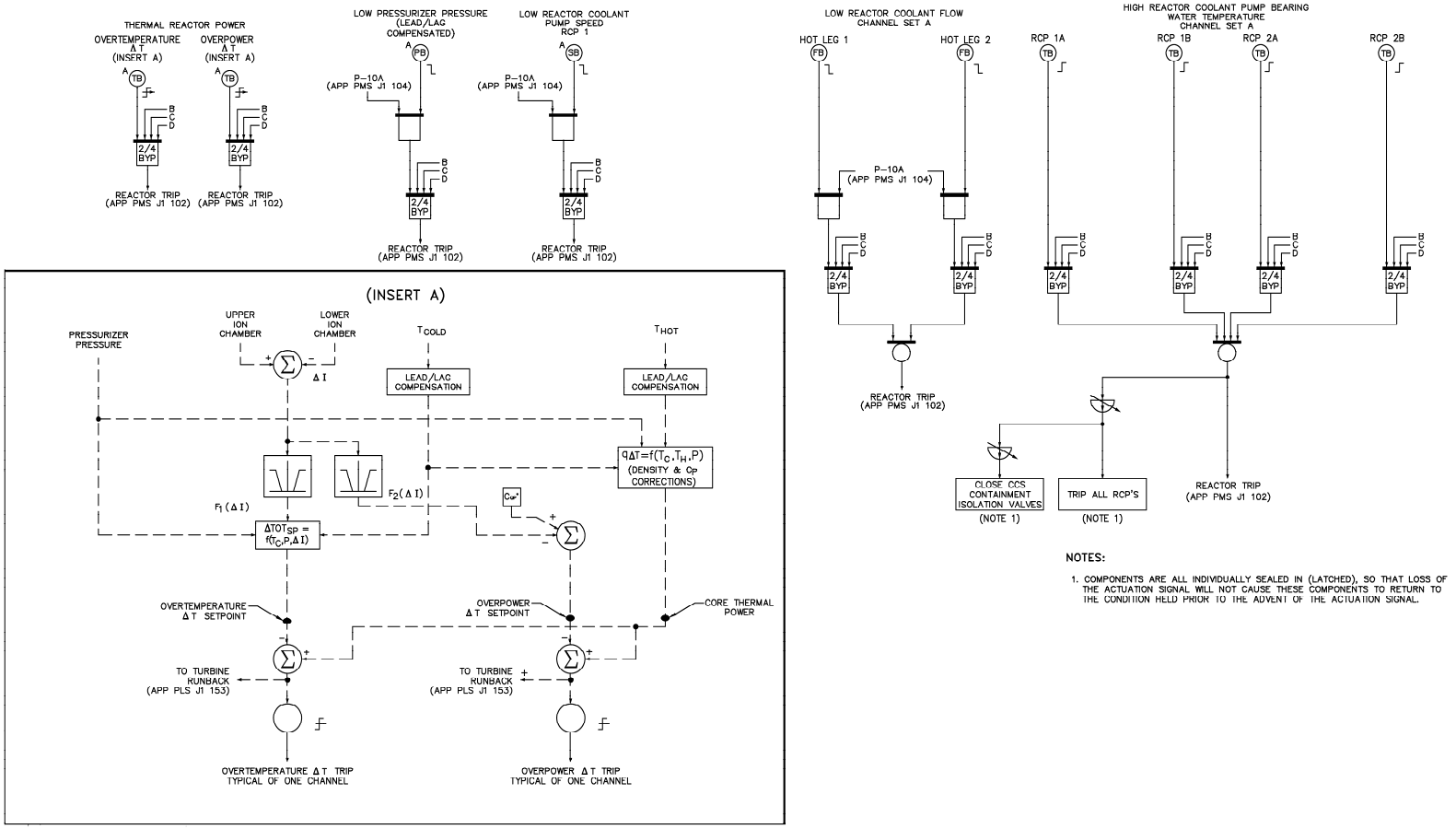


Figure 7.2-1 (Sheet 5 of 21)
Functional Diagram
Core Heat Removal Protection
and Reactor Coolant Pump Trip

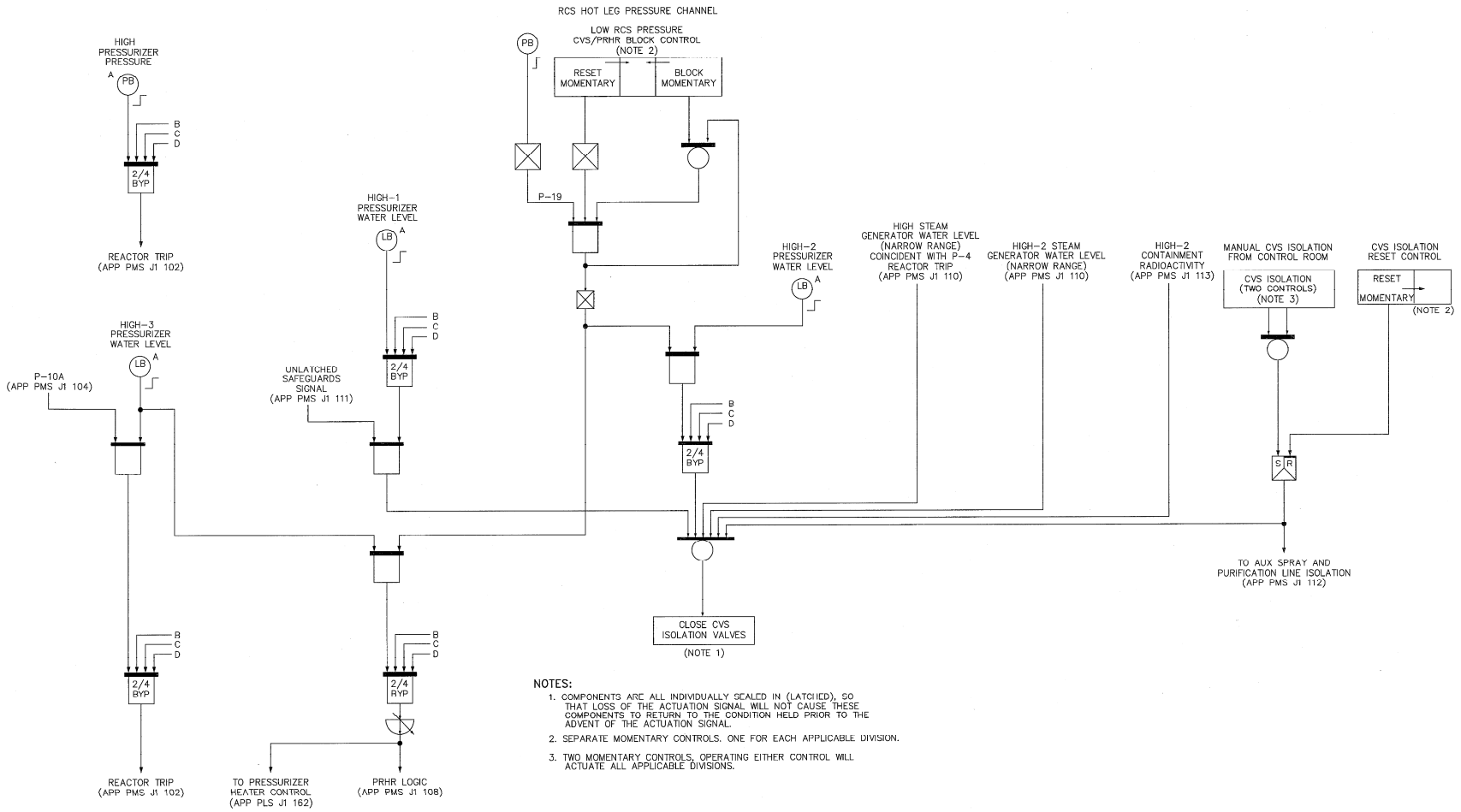


Figure 7.2-1 (Sheet 6 of 21)
Functional Diagram
Primary Overpressure & Loss of Heat Sink Protection

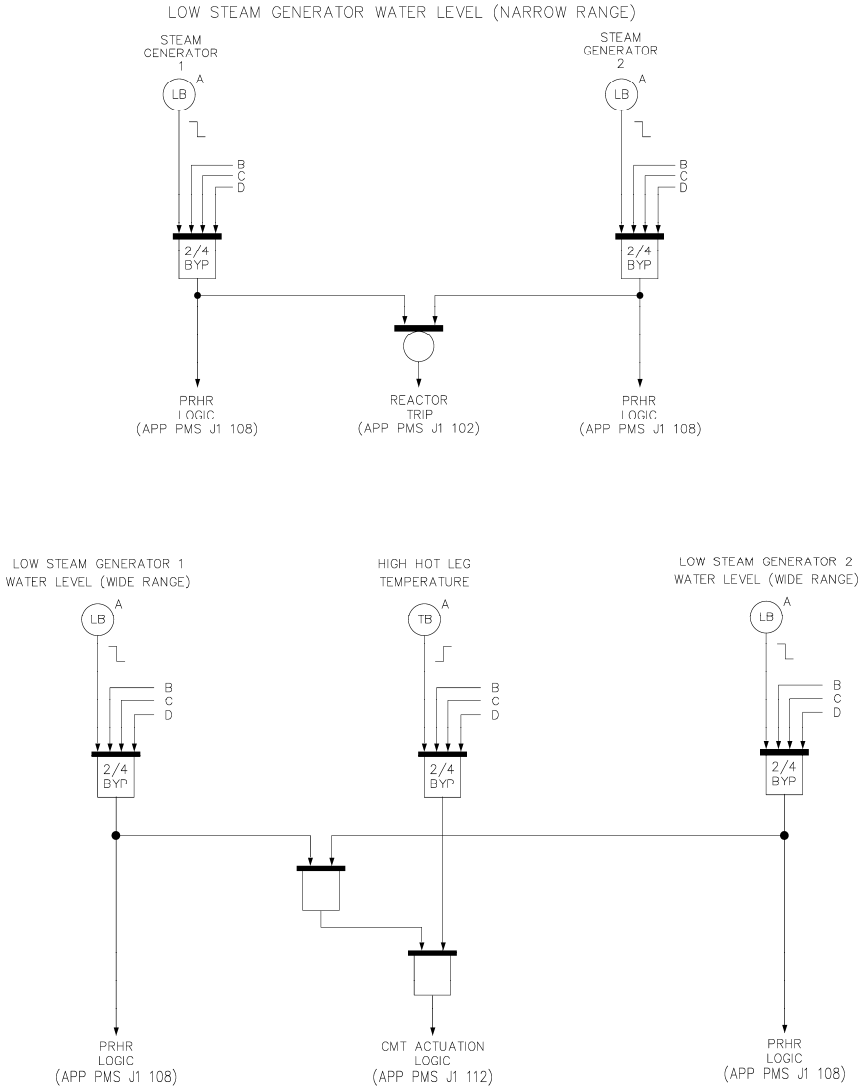


Figure 7.2-1 (Sheet 7 of 21)
Functional Diagram
Loss of Heat Sink Protection

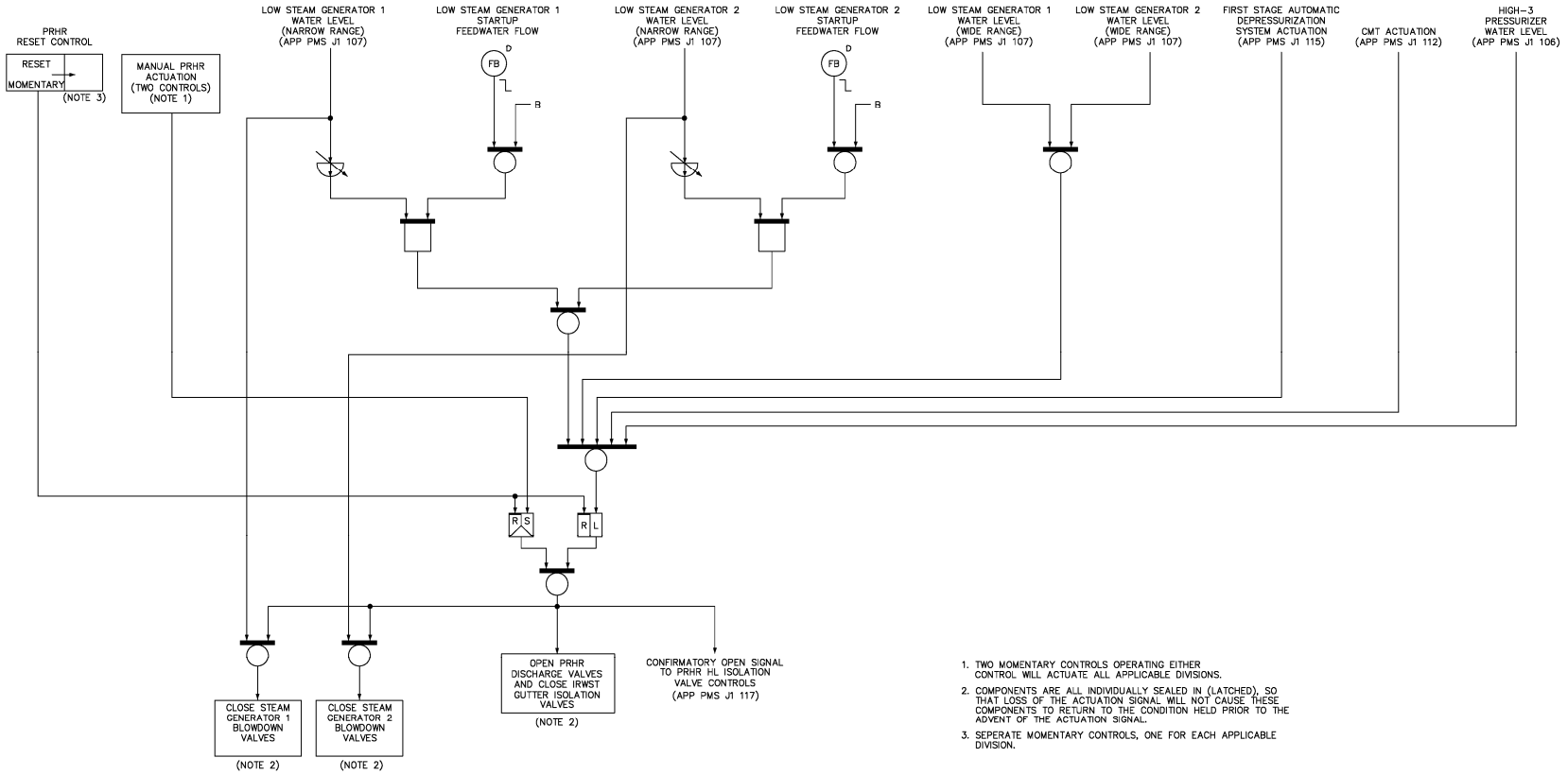


Figure 7.2-1 (Sheet 8 of 21)
Functional Diagram
Loss of Heat Sink Protection

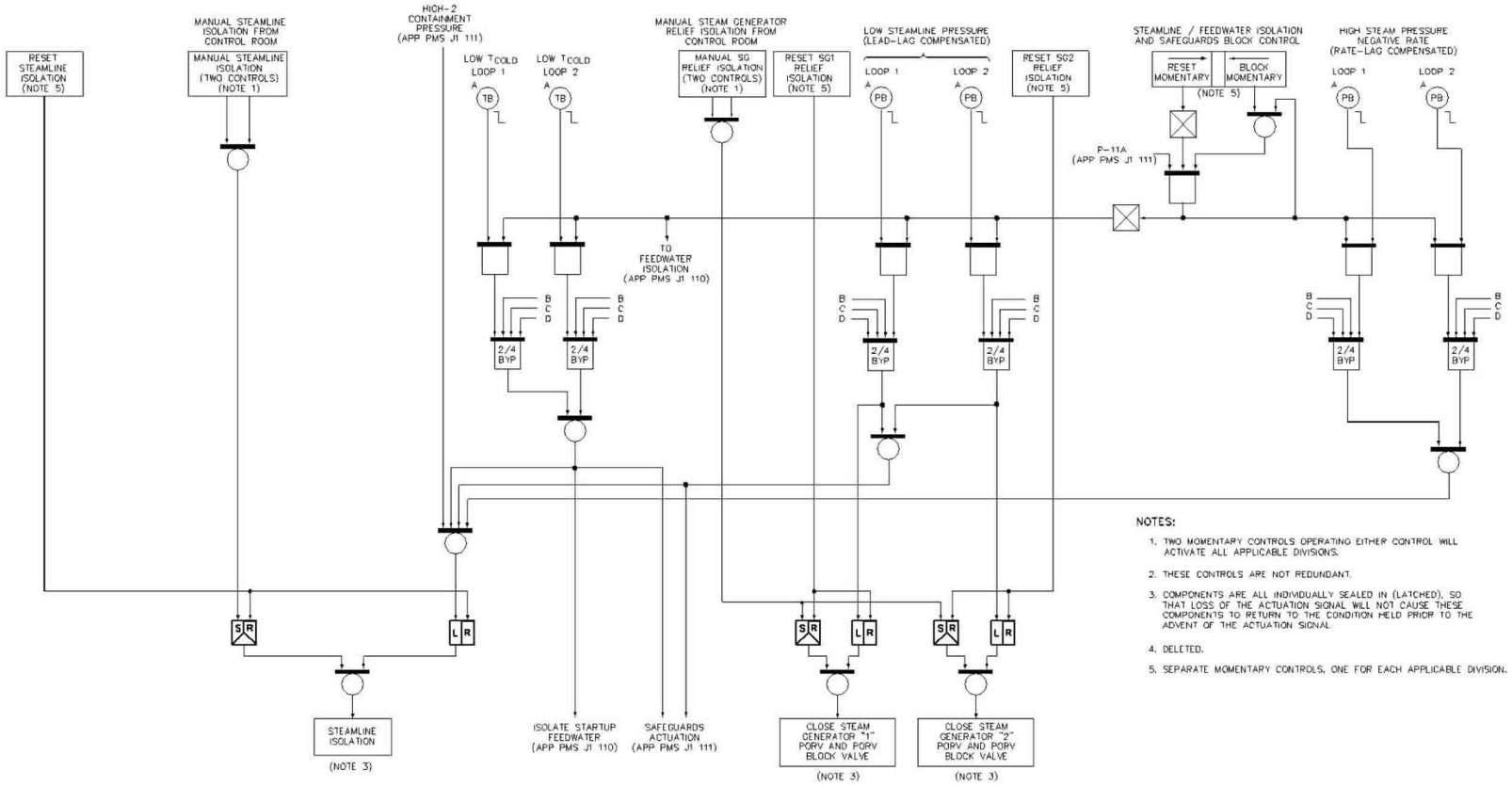


Figure 7.2-1 (Sheet 9 of 21)
Functional Diagram
Steam Line Isolation

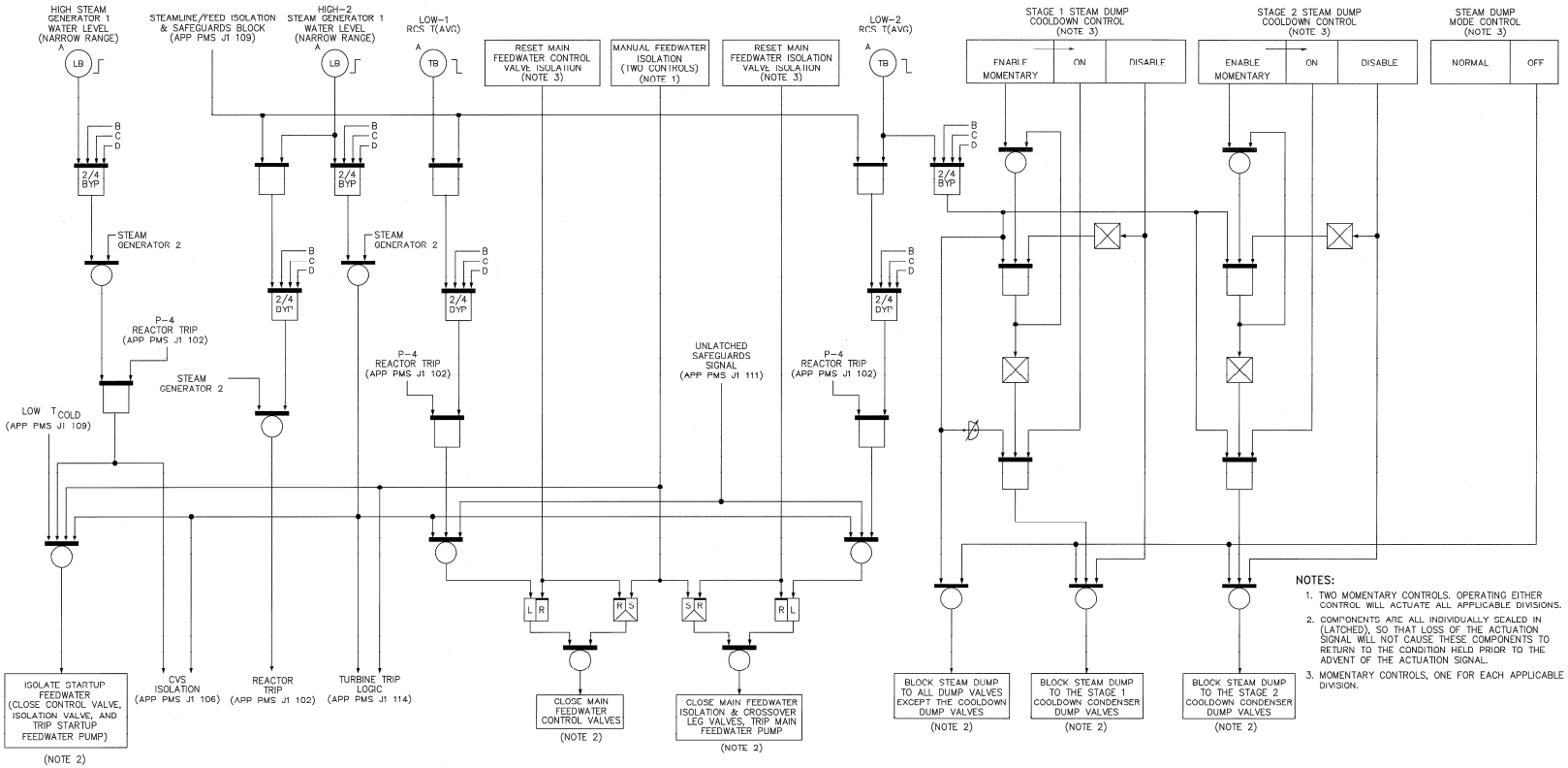


Figure 7.2-1 (Sheet 10 of 21)
Functional Diagram
Feedwater Isolation

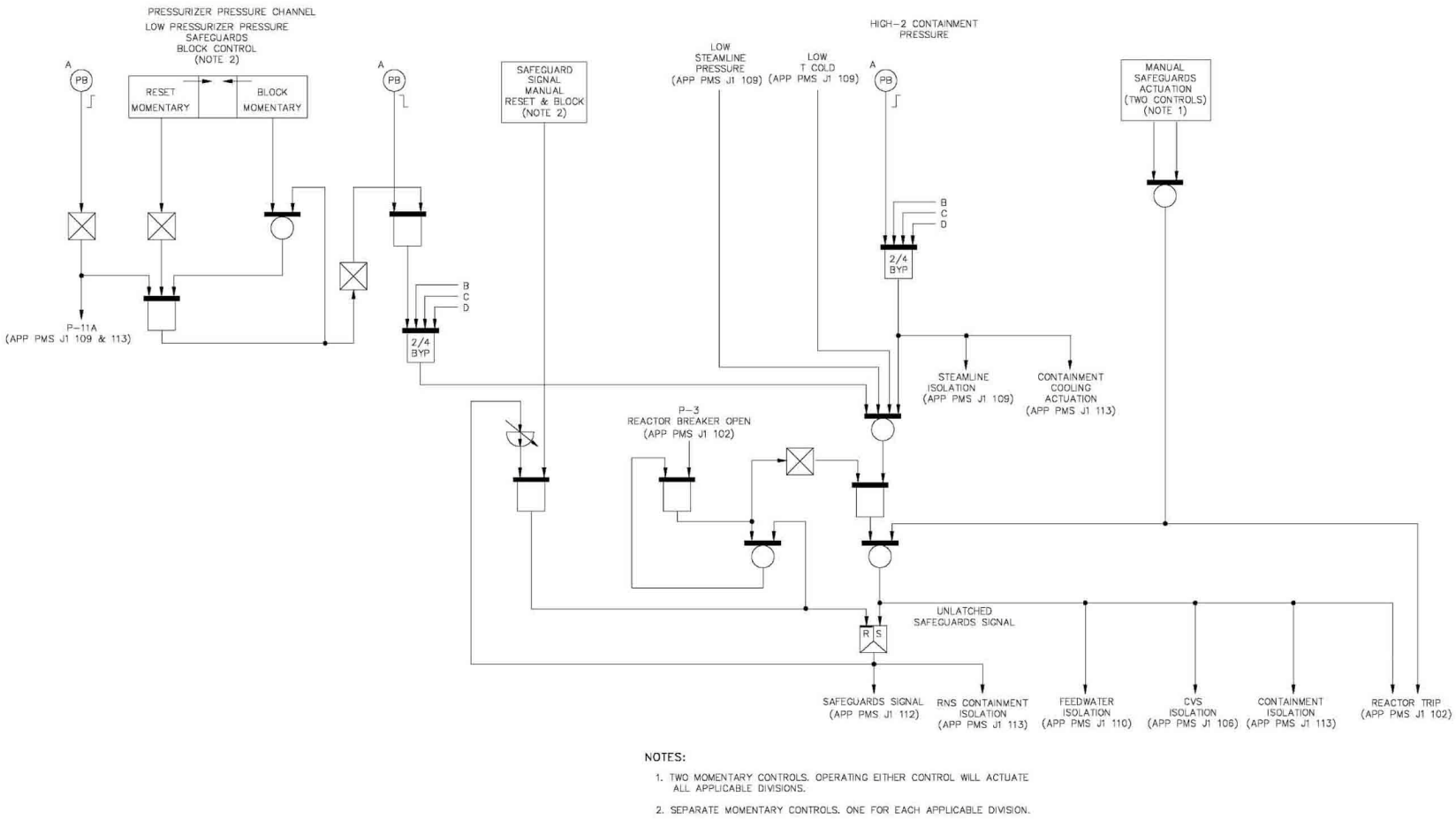


Figure 7.2-1 (Sheet 11 of 21)
Functional Diagram
Safeguards Actuation

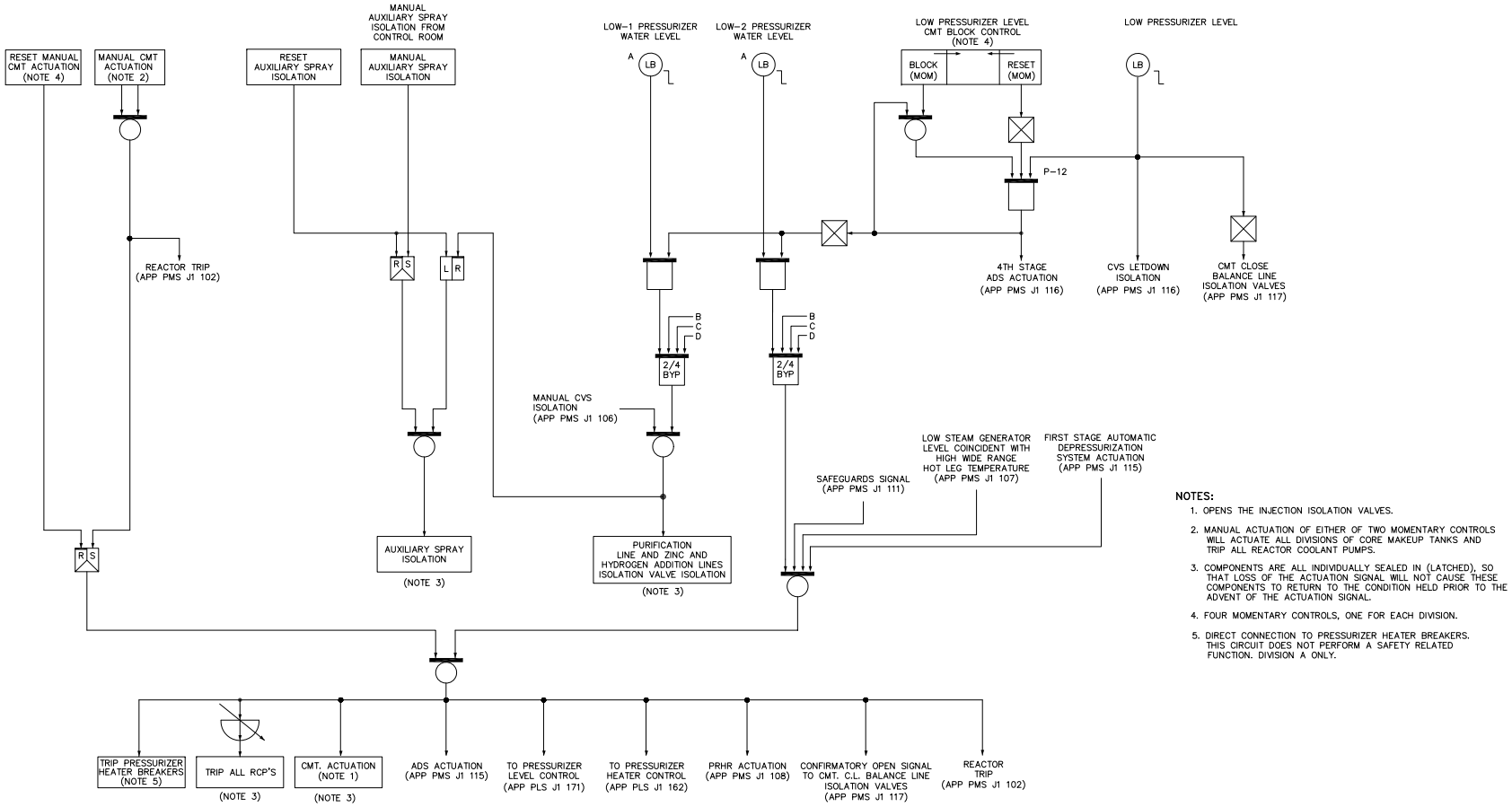


Figure 7.2-1 (Sheet 12 of 21)
Functional Diagram
Core Makeup Tank Actuation

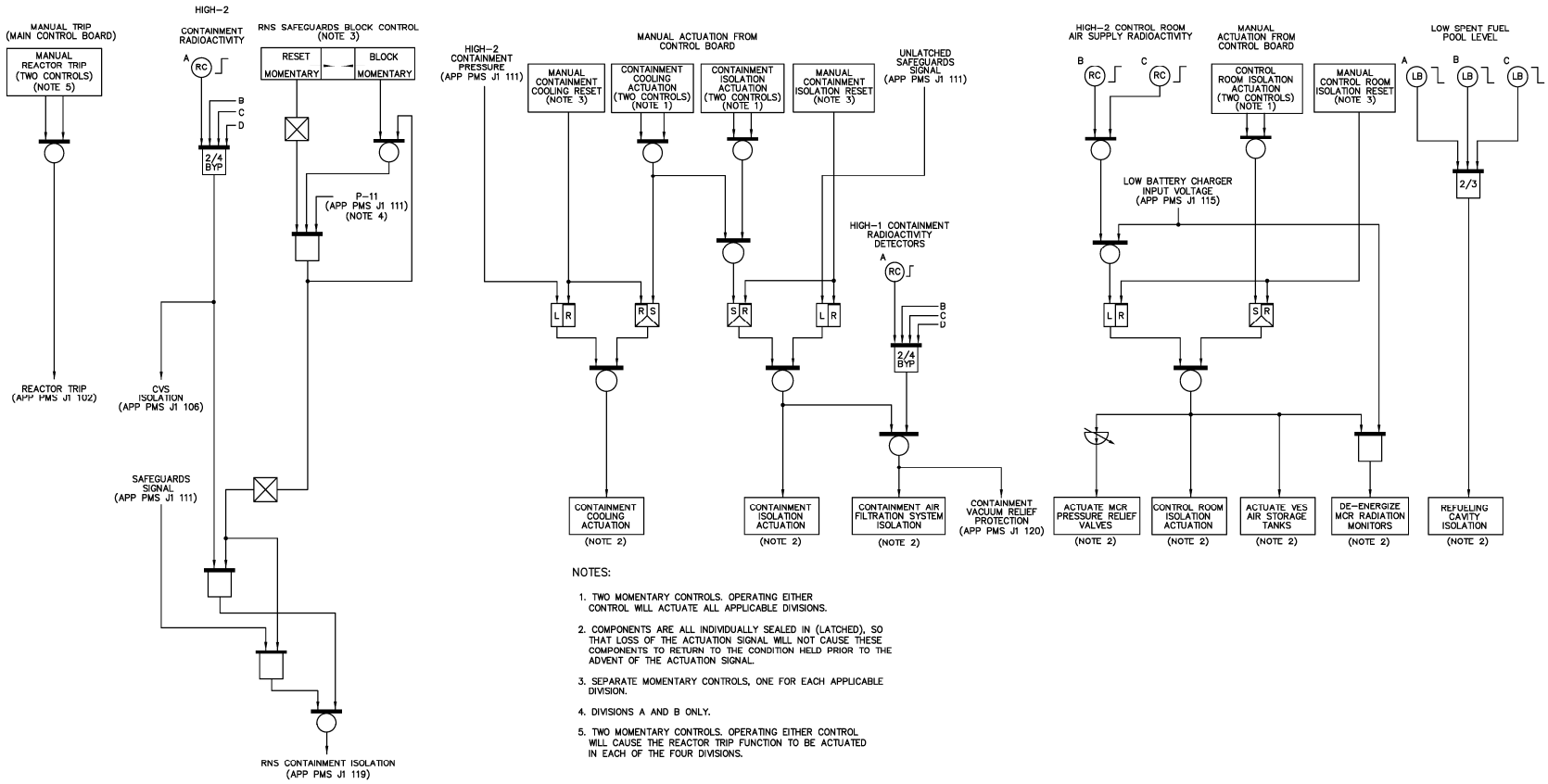
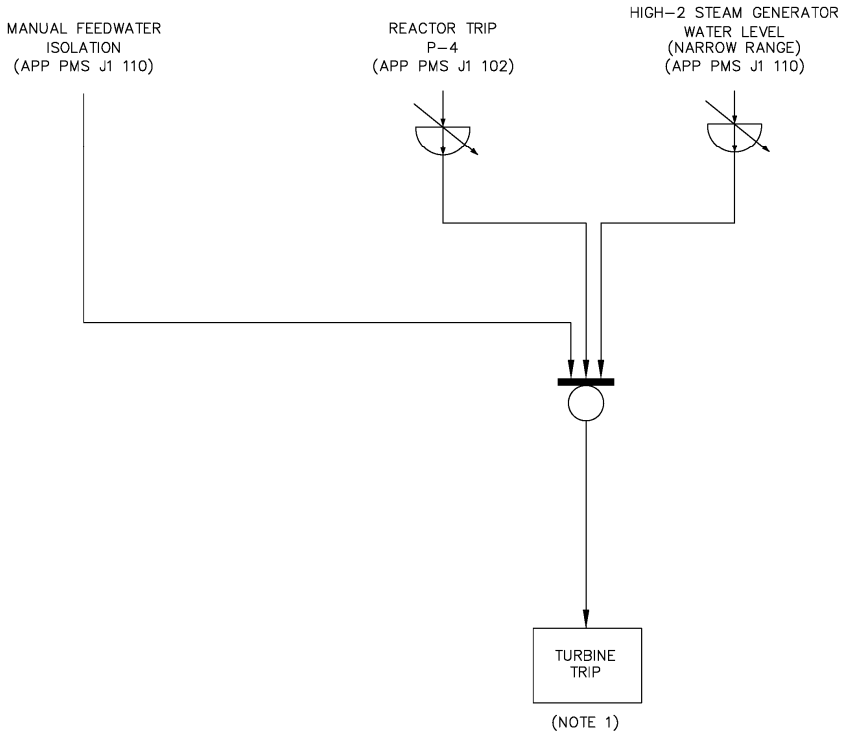


Figure 7.2-1 (Sheet 13 of 21)
Functional Diagram
Containment and Other Protection



NOTES:

1. COMPONENTS ARE INDIVIDUALLY SEALED IN (LATCHED) SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.

Figure 7.2-1 (Sheet 14 of 21)
Functional Diagram
Turbine Trip

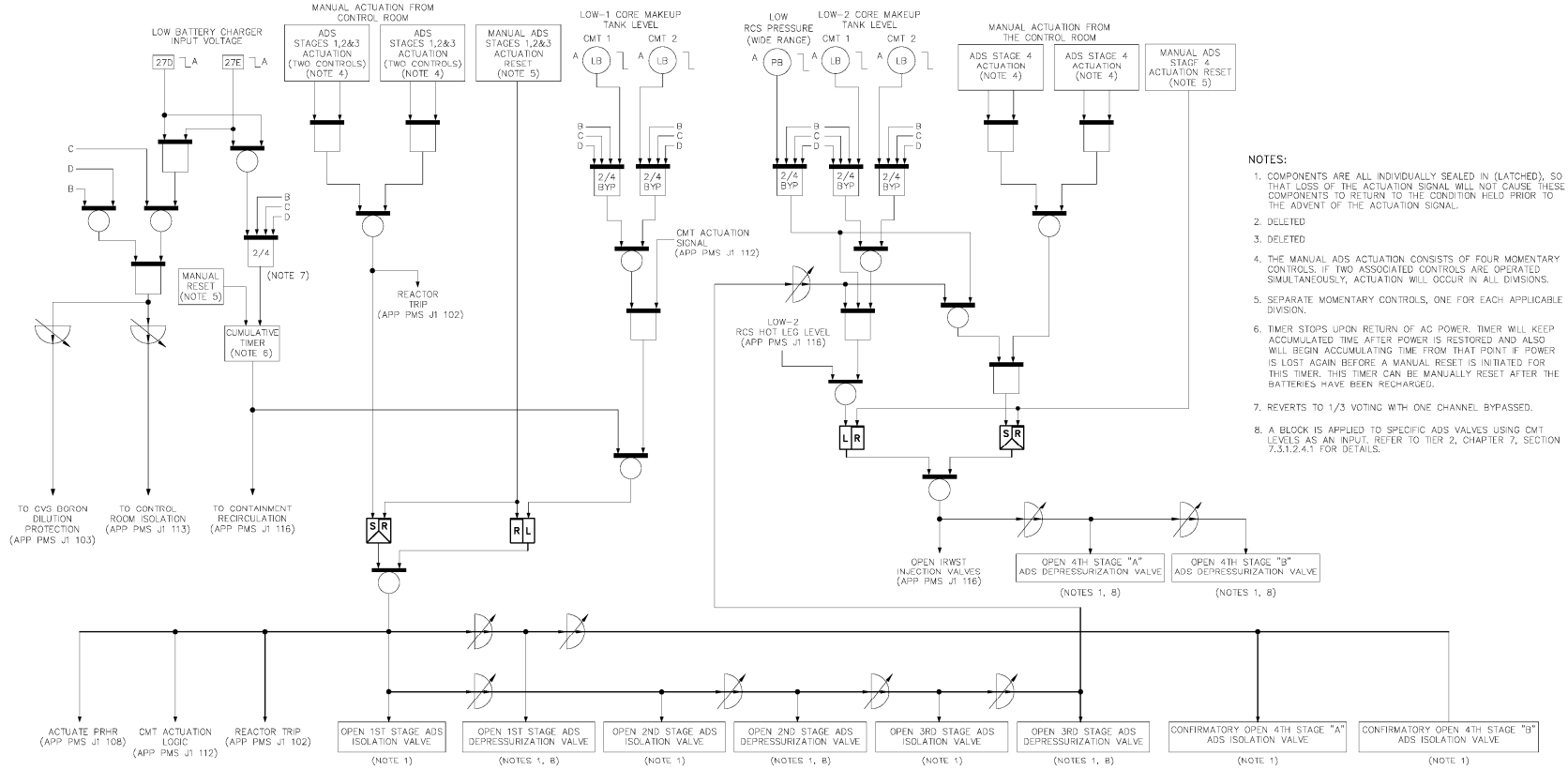
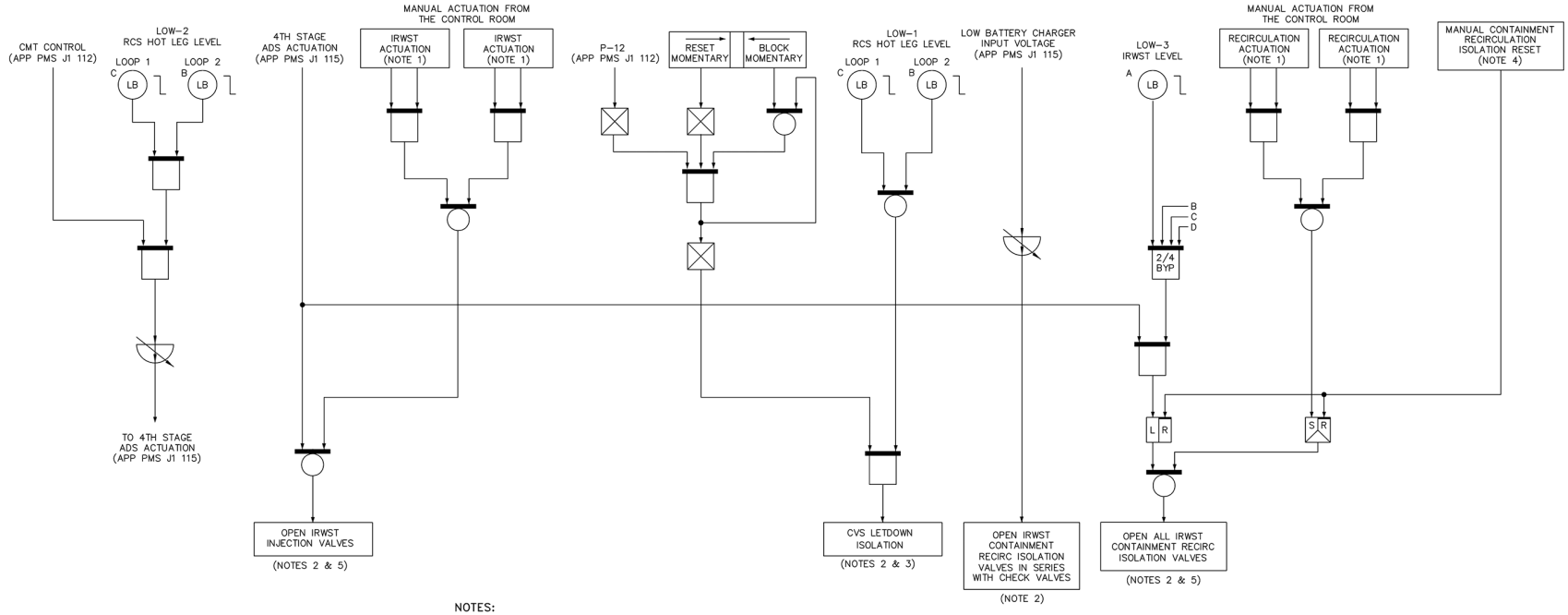


Figure 7.2-1 (Sheet 15 of 21)
Functional Diagram
Automatic RCS Depressurization Valve Sequencing



NOTES:

1. THE MANUAL ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL APPLICABLE DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. CVS LETDOWN ISOLATION ALSO OCCURS DURING CONTAINMENT ISOLATION. SEE APP PMS J1 113.
4. SEPARATE MOMENTARY CONTROLS, ONE FOR EACH APPLICABLE DIVISION.
5. FOR REDUNDANT COMPONENTS IN A PARALLEL CONFIGURATION, BOTH COMPONENTS USE DIFFERENT TIME DELAYS TO HELP PREVENT ACTUATING THEM SIMULTANEOUSLY.

Figure 7.2-1 (Sheet 16 of 21)
Functional Diagram
In-containment Refueling Water Storage Tank Actuations

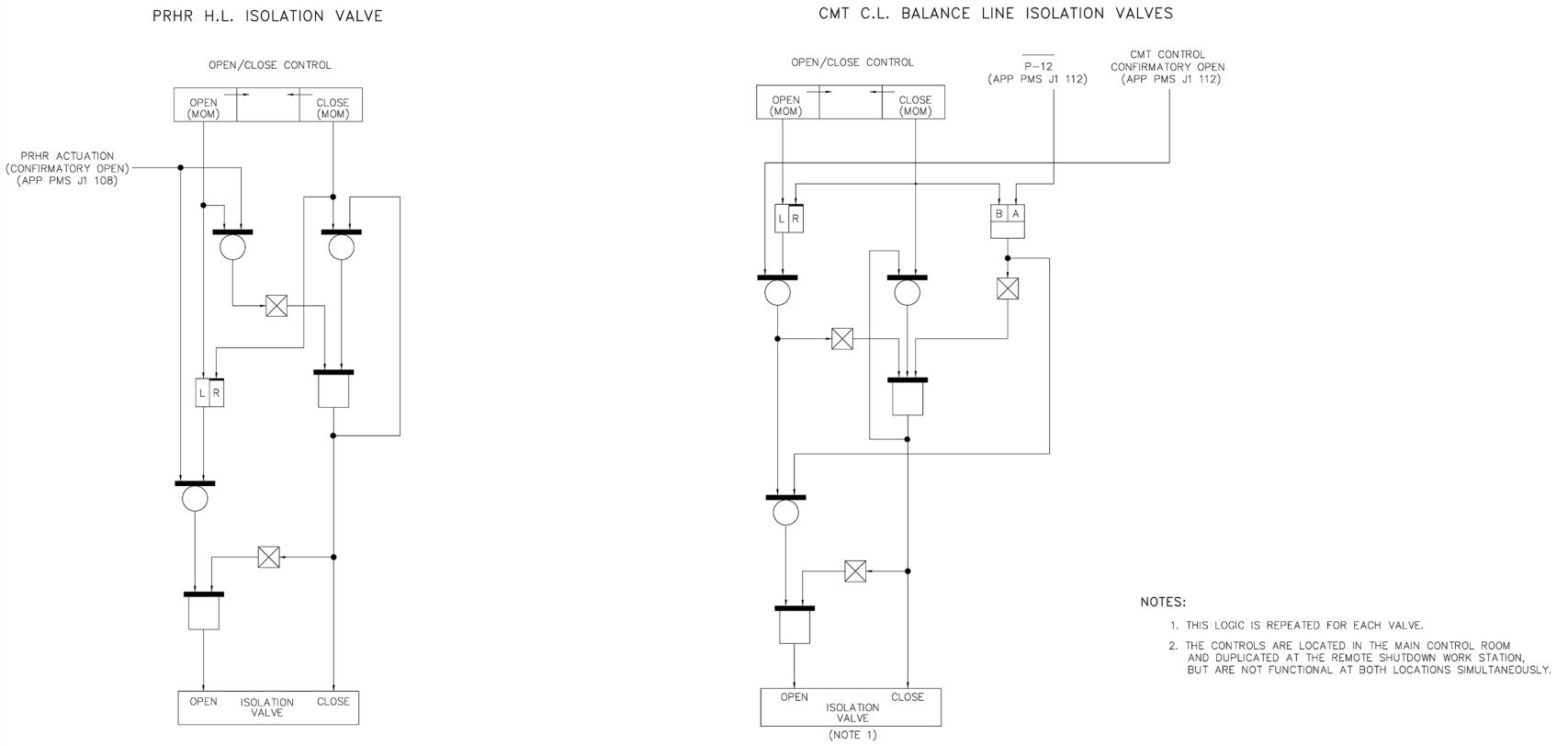


Figure 7.2-1 (Sheet 17 of 21)
Functional Diagram
Passive Residual Heat Removal and
Core Makeup Tank Isolation Valve Interlocks

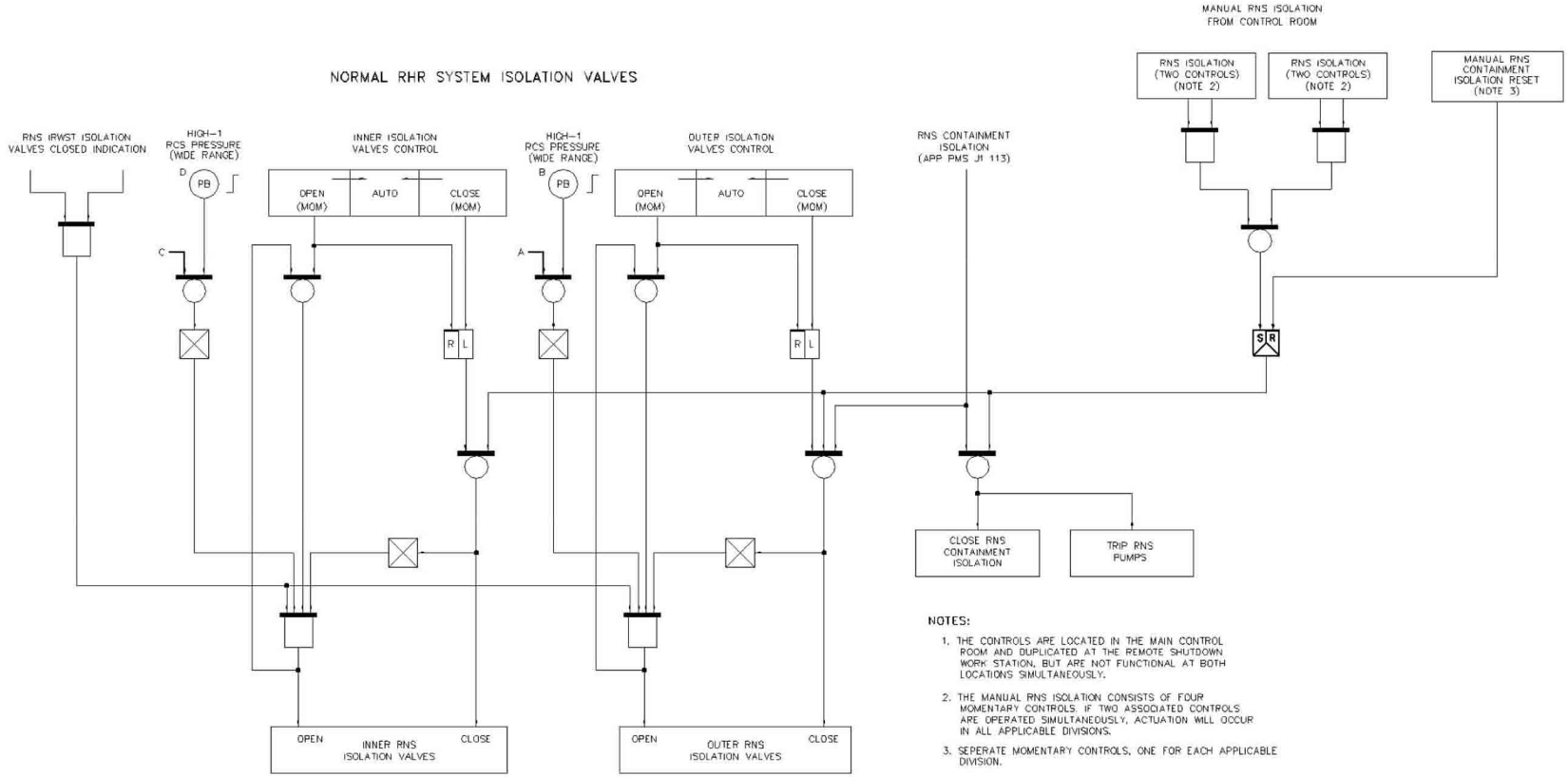
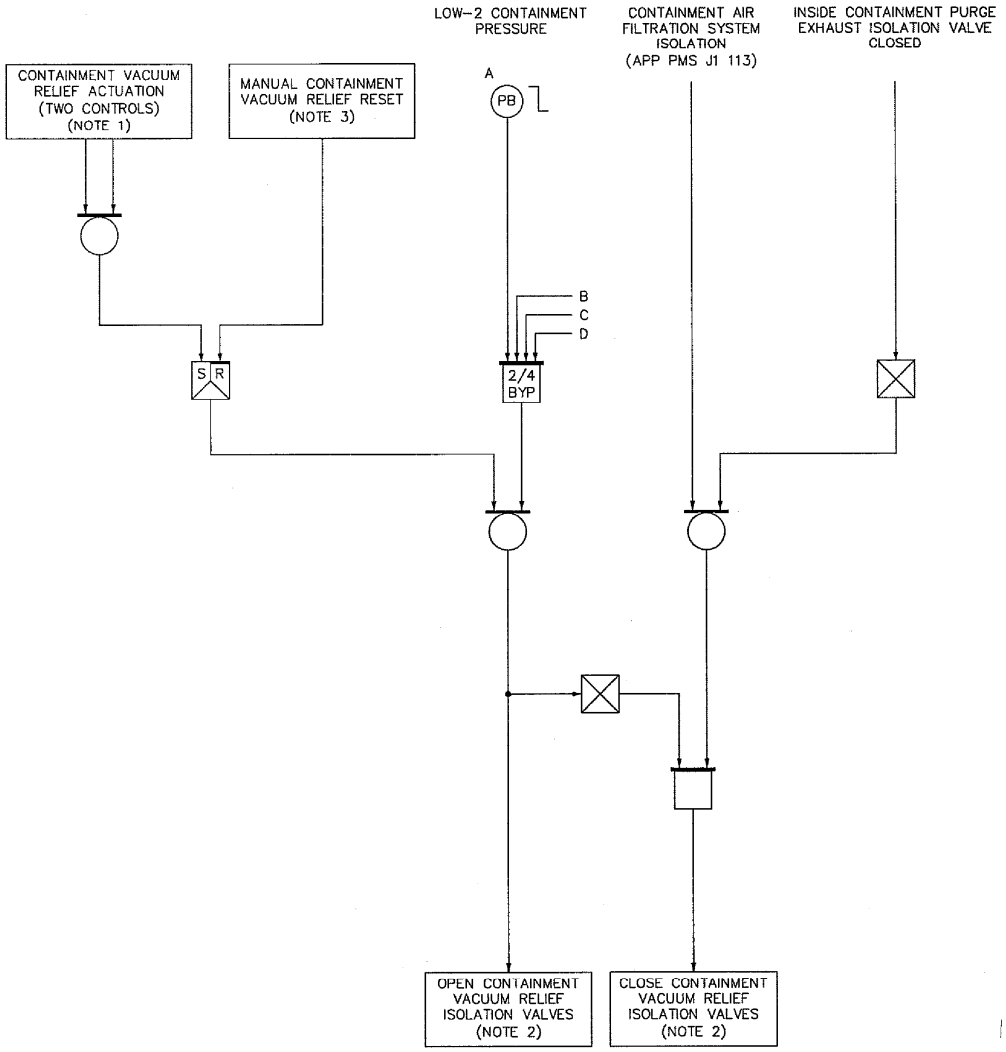


Figure 7.2-1 (Sheet 18 of 21)
Functional Diagram
Normal Residual Heat Removal System Isolation Valve Interlocks



NOTES:

1. TWO MOMENTARY CONTROLS. OPERATING EITHER CONTROL WILL ACTUATE ALL APPLICABLE DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. SEPARATE MOMENTARY CONTROLS, ONE FOR EACH APPLICABLE DIVISION.

Figure 7.2-1 (Sheet 19 of 21)
Functional Diagram
Containment Vacuum Relief Protection

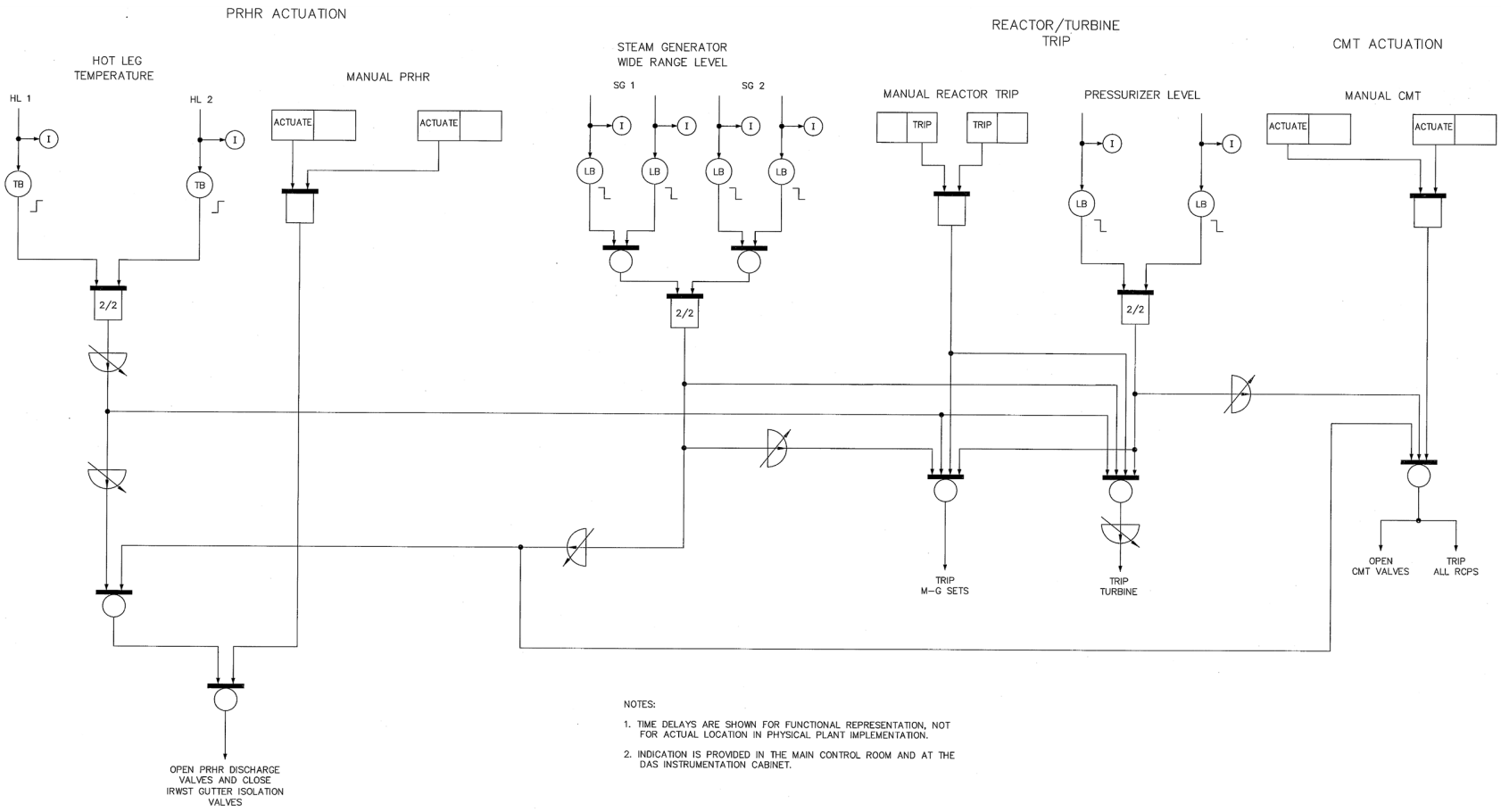


Figure 7.2-1 (Sheet 20 of 21)
Functional Diagram
Diverse Actuation System Logic Automatic Actuations

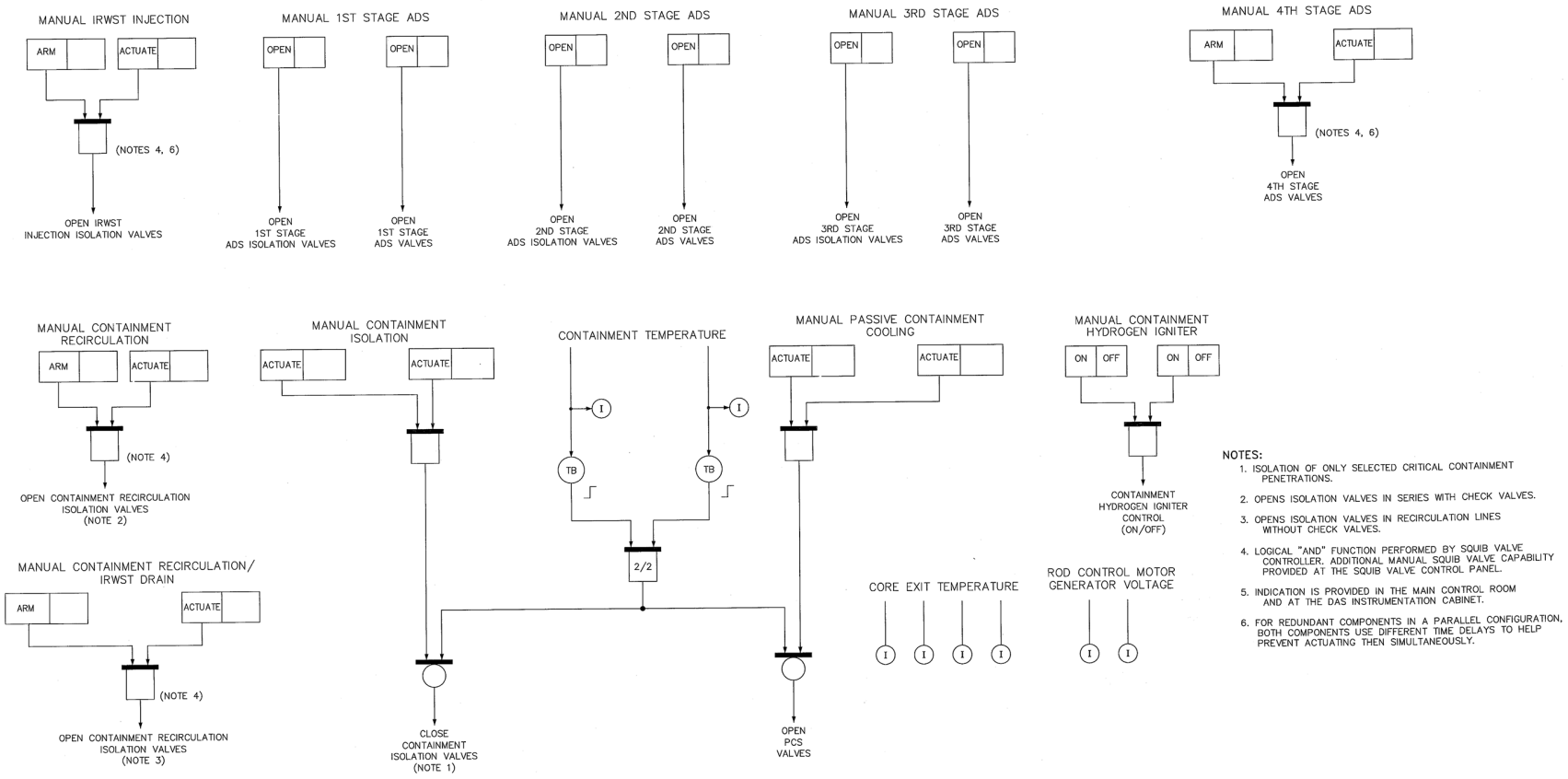


Figure 7.2-1 (Sheet 21 of 21)
Functional Diagram
Diverse Actuation System Logic, Manual Actuations

7.3 Engineered Safety Features

AP1000 provides instrumentation and controls to sense accident situations and initiate engineered safety features (ESF). The occurrence of a limiting fault, such as a loss of coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more of the engineered safety features. This combination of events prevents or mitigates damage to the core and reactor coolant system components, and provides containment integrity.

7.3.1 Description

The protection and safety monitoring system is actuated when safety system setpoints are reached for selected plant parameters. The selected combination of process parameter setpoint violations is indicative of primary or secondary system boundary ruptures. Once the required logic combination is generated, the protection and safety monitoring system equipment sends the signals to actuate appropriate engineered safety features components.

The following paragraphs summarize the major functional elements of the protection and safety monitoring system that are involved in generating an actuation signal to an engineered safety features component.

Four sensors normally monitor each variable used for an engineered safety feature actuation. (These sensors may monitor the same variable for a reactor trip function.) Analog measurements are converted to digital form by analog-to-digital converters within each of the four divisions of the protection and safety monitoring system. Following required signal conditioning or processing, the measurements are compared against the setpoints for the engineered safety feature to be generated. When the measurement exceeds the setpoint, the output of the comparison results in a channel partial trip condition. The partial trip information is transmitted to the ESF coincidence logic to form the signals that result in an engineered safety features actuation. The voting logic is performed twice within each division. Each voting logic element generates an actuation signal if the required coincidence of partial trips exists at its inputs.

The signals are combined within each division of ESF coincidence logic to generate a system-level signal. System-level manual actions are also processed by the logic in each division.

The system-level signals are then broken down to the individual actuation signals to actuate each component associated with a system-level engineered safety feature. For example, a single safeguards actuation signal must trip the reactor and the reactor coolant pumps, align core makeup tank and in-containment refueling water storage tank valves, and initiate containment isolation. The interposing logic accomplishes this function and also performs necessary interlocking so that components are properly aligned for safety. Component-level manual actions are also processed by this interposing logic. The power interface transforms the low level signals to voltages and currents commensurate with the actuation devices they operate. The actuation devices, in turn, control motive power to the final engineered safety feature component.

Subsection 7.3.1.2 provides a functional description of the signals and initiating logic for each of the engineered safety features. Figure 7.2-1 presents the functional diagrams for engineered safety features actuation.

Table 7.3-1 summarizes the signals and initiating logic for each of the engineered safety features initiated by the protection and safety monitoring system. Most of the functions provide protection against design basis events which are analyzed in Chapter 6 and Chapter 15. However, not all the functions listed in Table 7.3-1 are necessary to meet the assumptions used in performing the safety analysis. For example, the design provides features which provide automatic actuations which are not required for performing the safety analysis. In addition, some functions are provided to support

assumptions used in the probabilistic risk assessment, but are not used to mitigate a design basis accident. Only those functions which meet the 10 CFR 50.36(c)(2)(ii) criteria are included in the AP1000 DCD, Section 16.1, Technical Specifications. This accounts for any difference between functions listed in Table 7.3-1 and functions which are included in the Technical Specifications.

7.3.1.1 Safeguards Actuation (S) Signal

A safeguards actuation (S) signal is used in the initiation logic of many of the engineered safety features discussed in Subsection 7.3.1.2. In addition, as described in Section 7.2, the safeguards actuation signal also initiates a reactor trip. The variables that are monitored and used to generate a safeguards actuation signal are typically those that provide indication of a significant plant transient that requires a response by several engineered safety features.

The safeguards actuation signal is generated from any of the following initiating conditions:

1. Low pressurizer pressure
2. Low lead-lag compensated steam line pressure
3. Low cold leg temperature
4. High-2 containment pressure
5. Manual initiation

Condition 1 results from the coincidence of pressurizer pressure below the Low setpoint in any two of the four divisions.

Condition 2 results from the coincidence of two of the four divisions of compensated steam line pressure below the Low setpoint in either of the two steam lines. The steam line pressure signal is lead-lag compensated to improve system response.

Condition 3 results from the coincidence of two of the four divisions of reactor coolant system cold leg temperature below the Low setpoint in any loop.

Condition 4 results from the coincidence of two of the four divisions of containment pressure above the High-2 setpoint.

Condition 5 consists of two momentary controls. Manual actuation of either of the two controls will trip the reactor and generate a safeguards actuation signal.

To permit startup and cooldown, the safeguards actuation signals generated from low pressurizer pressure, low steam line pressure, or low reactor coolant inlet temperature can be manually blocked when pressurizer pressure is below the P-11 setpoint. The signal is automatically unblocked when the pressurizer pressure is above the P-11 setpoint.

Separate momentary controls are provided, each of which will manually reset the safeguards actuation signal in a single division. Manual reset of a safeguards actuation signal in coincidence with reactor trip breaker open (P-3) blocks the safeguards actuation signal. Absence of P-3 automatically resets the blocking function. The safeguards actuation signal is manually reset based on a preset delay following initiation. Resetting the signal does not reposition any safeguards actuated equipment, since individual components are required to latch in and seal on the safeguards actuation signal.

The logic relating to the development of the safeguards actuation signal is illustrated in Figure 7.2-1, sheets 9 and 11.

7.3.1.2 Engineered Safety Feature Descriptions

The following subsections provide a functional description of the signals and initiating logic for each engineered safety feature. Table 7.3-1 lists the signals and summarizes the coincidence logic used to generate the safeguards actuation signal or initiate each engineered safety feature. Table 7.3-2 describes the permissives and interlocks relating to the engineered safety features. Table 7.3-3 lists the system-level manual input to the engineered safety features.

7.3.1.2.1 Containment Isolation

A signal to actuate containment isolation is generated from any of the following conditions:

1. Automatic or manual safeguards actuation signal (Subsection 7.3.1.1)
2. Manual initiation
3. Manual actuation of passive containment cooling (Subsection 7.3.1.2.12)

Conditions 1 and 3 are discussed in other subsections as noted.

Condition 2 consists of the manual actuation of either of two momentary controls in the main control room. Either control actuates all divisions and closes the nonessential fluid system paths from the containment.

Manual reset is provided to block the automatic actuation signal for containment isolation. Separate momentary controls are provided for resetting each division.

No other interlocks or permissive signals apply directly to the containment isolation function. Automatic actuation originates from a safeguards actuation (S) signal that does contain interlock and permissive inputs.

The functional logic that actuates containment isolation is illustrated in Figure 7.2-1, sheets 11 and 13.

7.3.1.2.2 In-Containment Refueling Water Storage Tank Injection

Signals to align the in-containment refueling water storage tank for injection are generated from the following conditions:

1. Actuation of the fourth stage of the automatic depressurization system (Subsection 7.3.1.2.4)

2. Coincidence loop 1 and loop 2 hot leg levels below Low-2 setpoint for a duration exceeding an adjustable time delay

3. Manual initiation

Each of the above conditions opens the in-containment refueling water storage tank injection valves, thereby providing a flow path to the reactor coolant system.

In addition to initiating in-containment refueling water storage tank injection, condition 2 also initiates the opening sequence of the fourth stage of the automatic depressurization system. This is discussed in Subsection 7.3.1.2.4.

Condition 3 consists of two sets of two momentary controls. Manual actuation of both controls of either of the two control sets generates signals that open the in-containment refueling water storage tank injection valves. A two-control simultaneous actuation prevents inadvertent actuation.

In-containment refueling water storage tank injection on Low-2 hot leg level is automatically blocked when the pressurizer water level is above the P-12 setpoint. This reduces the probability of a spurious injection. This block is removed when the core makeup tank actuation on low pressurizer level function is manually blocked to allow mid-loop operation. As described in Subsection 7.3.1.2.3, this core makeup tank actuation function can be manually blocked when the pressurizer water level is below the P-12 setpoint.

The functional logic relating to in-containment refueling water storage tank injection is illustrated in Figure 7.2-1, sheets 12 and 16.

7.3.1.2.3 Core Makeup Tank Injection

Signals to align the core makeup tanks for injection are generated from the following conditions:

1. Automatic or manual safeguards actuation (Subsection 7.3.1.1)

2. Automatic or manual actuation of the first stage of the automatic depressurization system (Subsection 7.3.1.2.4)

3. Low-2 pressurizer level

4. Low wide range steam generator level coincident with High hot leg temperature

5. Manual initiation

Conditions 1 through 5 initiate a block of the pressurizer heaters; trip the reactor and reactor coolant pumps; initiate alignment of the core makeup tank isolation valves for passive injection to the reactor coolant system; and provide a confirmatory open signal to the cold leg balance line isolation valves. The balance line isolation valves are normally open but can be closed by the operator. The confirmatory open signal automatically overrides any bypass features that are provided to allow the cold leg balance line isolation valves to be closed for short periods of time. The motive force for core makeup tank injection is provided by density differences between the fluids in the cold leg balance line and the core makeup tank water.

Condition 3 results from the coincidence of pressurizer level below the Low-2 setpoint in any two of the four divisions. This function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This function is automatically unblocked when the pressurizer water level is above the P-12 setpoint.

Condition 4 is derived from a coincidence of:

- Both steam generator 1 and steam generator 2 wide range level below the Low setpoint (derived from two of the four wide range level measurement divisions for each steam generator), and

- Two of the four divisions of hot leg temperature above the High (T_{hot}) setpoint

Condition 5 consists of two momentary controls. Manual actuation of either of the two controls will align the core makeup tanks for injection.

The functional logic relating to core makeup tank injection is illustrated in Figure 7.2-1, sheets 7, 12 and 15.

7.3.1.2.4 Automatic Depressurization System Actuation

A signal to actuate the first stage of the automatic depressurization system is generated from any of the following conditions:

1. Core makeup tank injection alignment signal (Subsection 7.3.1.2.3) coincident with core makeup tank level less than the Low-1 setpoint in either core makeup tank in two of the four divisions

2. Extended loss of ac power sources (low Class 1E battery charger input voltage)

3. Manual initiation

Any actuation of the first stage of the automatic depressurization system also trips the reactor and reactor coolant pumps, align the core makeup tanks for injection, and actuates the passive residual heat removal heat exchanger.

The automatic depressurization system is arranged to sequentially open four parallel stages of valves. Each of the first three stages consists of two parallel paths with each path containing an isolation valve and a depressurization valve. The first three stages are connected to the pressurizer and discharge into the in-containment refueling water storage tank. The fourth stage paths are connected to the hot legs of the reactor coolant system and discharge to containment.

The first stage isolation valves open on any actuation of the first stage of the automatic depressurization system. The first stage depressurization valves are opened following a preset time delay after the isolation valves are sent a signal to open. No interlocks or permissive signals apply directly to the first stage depressurization. However, some safeguards actuation signals, from which the core makeup tank injection actuation signal is derived, do contain interlock and permissive inputs.

The second stage isolation valves are sent a signal to open following a preset time delay after the first stage isolation valves are sent a signal to open. The second stage depressurization valves are sent a signal to open following a preset time delay after the second stage isolation valves are sent a signal to open, similar to stage one.

Similar to the second stage, the third stage isolation valves are sent a signal to open following a preset time delay after the second stage depressurization valves are sent a signal to open. The third stage depressurization valves are sent a signal to open following a preset time delay after the third stage isolation valves are sent a signal to open.

The fourth stage of the automatic depressurization system consists of four parallel paths. Each of these paths consists of a normally open isolation valve and a depressurization valve. The four paths are divided into two redundant groups with two paths in each group. Within each group, one path is designated to be substage A and the second path is designated to be substage B.

The fourth stage isolation valves receive a confirmatory open signal (nonsafety-related function) following a preset time delay after the first stage depressurization valves are sent a signal to open.

The fourth stage is actuated upon the coincidence of a Low-2 core makeup tank level and Low reactor coolant system pressure following a preset time delay after the third stage depressurization valves are sent a signal to open. The Low-2 core makeup tank level input is based on the core makeup tank level being less than the Low-2 setpoint in two of the four divisions in either core makeup tank. Upon a fourth stage actuation signal, the substage-A depressurization valves are opened following a preset time delay. The signal to open the substage-B depressurization valve is provided following a preset time delay after the substage-A depressurization valves are sent a signal

to open. The net effect is to provide a controlled depressurization of the reactor coolant system. In addition to initiating this controlled depressurization sequence, the fourth stage actuation signal also provides a signal that aligns the in-containment refueling water storage tank for injection, as discussed in Subsection 7.3.1.2.2.

A signal to initiate the opening sequence of the fourth stage is also generated upon the occurrence of coincidence loop 1 and loop 2 hot leg levels below the Low-2 setpoint for a duration exceeding an adjustable time delay. This signal also initiates in-containment refueling water storage tank injection. As discussed in Subsection 7.3.1.2.2, this signal is automatically blocked when the pressurizer water level is above the P-12 setpoint. This reduces the probability of a spurious signal. The block is removed when the core makeup tanks actuation on low pressurizer level function is manually blocked to allow mid-loop operation.

The fourth stage can also be manually initiated. In this case the manual initiation signal is interlocked to prevent actuation until either the reactor coolant system pressure has decreased below a preset setpoint, or until the signals which control the opening sequence of the first, second, and third stage valves have been generated. As discussed above, the signals to the first, second, and third stage valves are generated based on preset time delays.

The core makeup tank injection alignment signal, which is part of condition 1, is latched-in upon its occurrence. A deliberate operator action is required to reset this latch. This feature is provided so that an automatic depressurization system actuation signal is not cleared by the reset of the safeguards actuation signal as discussed in Subsection 7.3.1.1.

Condition 2 results from the loss of all ac power for a period of time that approaches the 24-hour Class 1E dc battery capability to activate the automatic depressurization system valves. The timed output holds upon restoration of ac power and is manually reset after the batteries are recharged. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by either of the two sensors connected to two of the four battery chargers.

Condition 3 is achieved via either of two sets of two momentary controls. If both controls of either set are operated simultaneously, actuation of the automatic depressurization system occurs. A two-control simultaneous actuation prevents inadvertent actuation.

The functional logic relating to automatic depressurization operation is illustrated in Figure 7.2-1, sheet 15.

7.3.1.2.4.1 Block to Prevent ADS Spurious Actuation

A number of measures have been taken to reduce the likelihood of spurious actuation of ESF functions in the AP1000 Protection and Safety Monitoring System (PMS) design. Special attention has been given to prevention of spurious Automatic Depressurization System (ADS) valve action, since a spurious actuation could result in a release of reactor coolant to containment. In order to prevent such spurious actuations, an ADS blocking device is provided that is independent of PMS failure modes. Each division of the PMS contains an independent blocking device that prevents the following ADS Stage 1-4 valves from actuating unless there is a confirmatory process condition separate from the PMS ADS actuation logic:

ADS Stage 1: Depressurization Valve for Stage 1A Valve Set and Depressurization Valve for Stage 1B Valve Set

ADS Stage 2: Depressurization Valve for Stage 2A Valve Set and Depressurization Valve for Stage 2B Valve Set

ADS Stage 3: Depressurization Valve for Stage 3A Valve Set and Depressurization Valve for Stage 3B Valve Set

ADS Stage 4: Block “ARM” or “FIRE” signal for all squib valves

Independence

The ADS blocking device is a Class 1E module physically located within each of the PMS divisions. The blocking device is diverse from the PMS hardware and software that is used to create the automatic ADS actuation signal, which provides the input to the component interface modules for the ADS valves. There are no inter-divisional connections between the blocking devices nor will there be any coincidence voting.

Clearing of the ADS Block

The ADS block device uses Core Makeup Tank (CMT) level to automatically clear this block. The ADS block in each division uses a level signal input from a level sensor on each CMT that clears the block if either signal indicates a CMT is draining. The use of two CMT level sensors in each ADS block device provides for a device that does not adversely affect the reliability of ADS to actuate when it is required. Switches, one for each division, are provided in the Main Control Room (MCR) to allow the operators to manually clear the ADS blocks.

7.3.1.2.5 Reactor Coolant Pump Trip

A signal to trip reactor coolant pumps is generated from any one of the following conditions:

1. Automatic or manual safeguards actuation signal (Subsection 7.3.1.1)
2. Automatic or manual actuation of the first stage of the automatic depressurization system (Subsection 7.3.1.2.4)
3. Low-2 pressurizer level
4. Low wide range steam generator level coincident with High hot leg temperature
5. Manual initiation of core makeup tank injection (Subsection 7.3.1.2.3)
6. High reactor coolant pump bearing water temperature

Once a signal to trip the reactor coolant pump is generated, the actual tripping of the pump is delayed by a preset time delay.

Condition 3 results from the coincidence of pressurizer level below the Low-2 setpoint in any two of the four divisions. This function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This function is automatically unblocked when the pressurizer water level is above the P-12 setpoint.

Condition 4 is derived from a coincidence of:

- Both steam generator 1 and steam generator 2 wide range level below the Low setpoint (derived from two of the four wide range level measurement divisions for each steam generator), and

- Two of the four divisions of hot leg temperature above the High (T_{hot}) setpoint

Condition 6 is derived from a coincidence of two of the four divisions of high reactor coolant pump bearing water temperature for any reactor coolant pump. All of the reactor coolant pumps are tripped simultaneously if Condition 6 is met for the bearing water temperature of any reactor coolant pump. This function is included for equipment protection. The high temperature setpoint and dynamic compensation are the same as used in the high reactor coolant pump bearing water temperature reactor trip (Subsection 7.2.1.1.3) but with the inclusion of preset time delay.

The functional logic relating to the tripping of the reactor coolant pumps is illustrated in Figure 7.2-1, sheets 5, 7, 12, and 15.

7.3.1.2.6 Main Feedwater Isolation

Signals to isolate the main feedwater supply to the steam generators are generated from any of the following conditions:

1. Automatic or manual safeguards actuation (Subsection 7.3.1.1)
2. Manual initiation
3. High-2 steam generator narrow range water level
4. Low-1 reactor coolant system average temperature coincident with P-4 permissive
5. Low-2 reactor coolant system average temperature coincident with P-4 permissive

Conditions 1, 2, and 3 isolate the main feedwater supply by tripping the main feedwater pumps and closing the main feedwater control, isolation and crossover valves. These conditions also initiate a turbine trip.

Condition 2 consists of two momentary controls. Manual actuation of either of the two controls will trip the turbine and isolate the main feedwater supply. This action also initiates isolation of startup feedwater (Subsection 7.3.1.2.13).

Condition 3 is derived from a coincidence of two of the four divisions of narrow range steam generator water level above the High-2 setpoint for either steam generator. In addition to tripping the turbine and isolating the main feedwater supply, condition 3 also initiates a reactor trip, isolates the startup feedwater supply (Subsection 7.3.1.2.13), and isolates the chemical volume control system.

Condition 4 results from a coincidence of two of the four divisions of reactor loop average temperature (T_{avg}) below the Low-1 setpoint coincident with the P-4 permissive (reactor trip). This condition results in the closure of the main feedwater control valves. The feedwater isolation resulting from this condition may be manually blocked when the pressurizer pressure is below the P-11 setpoint. The block is automatically removed when the pressurizer pressure is above the P-11 setpoint.

Condition 5 results from a coincidence of two of the four divisions of reactor loop average temperature (T_{avg}) below the Low-2 setpoint coincident with the P-4 permissive (reactor trip). This condition results in the tripping of the main feedwater pumps and closure of the main feedwater isolation and crossover valves. The feedwater isolation resulting from this condition may be manually blocked when the pressurizer pressure is below the P-11 setpoint. The block is automatically removed when the pressurizer pressure is above the P-11 setpoint.

Condition 5 also blocks the steam dump valves and becomes an interlock to the steam dump interlock selector switch. This is discussed in Subsection 7.3.1.2.16.

The functional logic relating to the isolation of the main feedwater is illustrated in Figure 7.2-1, sheet 10.

7.3.1.2.7 Passive Residual Heat Removal Heat Exchanger Alignment

A signal to align the passive heat removal heat exchanger to passively remove core heat is generated from any of the following conditions:

1. Core makeup tank injection alignment signal (Subsection 7.3.1.2.3)
2. First stage automatic depressurization system actuation (Subsection 7.3.1.2.4)
3. Low wide range steam generator level
4. Low narrow range steam generator level coincident with Low startup feedwater flow
5. High-3 pressurizer water level
6. Manual initiation

Each of these conditions opens the passive residual heat removal discharge isolation valves, closes the in-containment refueling water storage tank gutter isolation valves, and provides a confirmatory open signal to the inlet isolation valve. The inlet isolation valve is normally open but can be closed by the operator. These conditions override any closure signal to this valve and also close the blowdown isolation valves in both steam generators.

Condition 3 results from the coincidence of two of the four divisions of wide range steam generator level below the Low setpoint in either of the two steam generators.

Condition 4 results from the coincidence of two of the four divisions of narrow range steam generator level below the Low setpoint, after a preset time delay, coincident with a Low startup feedwater flow in a particular steam generator. This function is provided for each of the two steam generators. The low narrow range steam generator level also isolates blowdown in the affected steam generator.

Condition 5 results from the coincidence of pressurizer level above the High-3 setpoint in any two of four divisions. This function can be manually blocked when the reactor coolant system pressure is below the P-19 permissive setpoint to permit pressurizer water solid conditions with the plant cold. This function is automatically unblocked when reactor coolant system pressure is above the P-19 setpoint. In addition to actuating the passive residual heat removal heat exchanger, condition 5 initiates a block of the pressurizer heaters.

Condition 6 consists of two momentary controls. Manual actuation of either of the two controls will align the passive residual heat removal heat exchanger initiating heat removal by this path.

The functional logic relating to alignment of the passive residual heat removal heat exchanger is illustrated in Figure 7.2-1, sheet 8.

7.3.1.2.8 Turbine Trip

A signal to initiate turbine trip is generated from any of the following conditions:

1. Reactor trip (Table 7.3-2, interlock P-4)
2. High-2 steam generator narrow-range water level
3. Manual feedwater isolation (Subsection 7.3.1.2.6)

Each of these conditions initiates a turbine trip to prevent or terminate an excessive cooldown of the reactor or minimizes the potential for equipment damage caused by loss of steam supply to the turbine.

Condition 2 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High-2 setpoint for either steam generator.

The functional logic relating to the tripping of the turbine is illustrated in Figure 7.2-1, sheet 14.

7.3.1.2.9 Containment Recirculation

Signals to align the containment recirculation isolation valves are generated from the following conditions:

1. Low-3 in-containment refueling water storage tank water level in coincidence with fourth stage automatic depressurization system actuation (Subsection 7.3.1.2.4)

2. Manual initiation

3. Extended loss of ac power sources

There are four parallel containment recirculation paths provided to permit the recirculation of the water provided by the in-containment refueling water storage tank. Two of these paths are provided with two isolation valves in series while the remaining two paths are provided with a single isolation valve in series with a check valve.

Conditions 1 and 2 result in the opening of all isolation valves in all four parallel paths. Condition 3 results in the opening of the two isolation valves that are in series with the check valves.

Condition 1 results from the coincidence of two of the four divisions of in-containment refueling water storage tank water level below the Low-3 setpoint, coincident with an automatic fourth stage automatic depressurization system signal.

Condition 2 consists of two sets of two momentary controls. Manual actuation of both controls of either of the two control sets initiates recirculation in all four parallel paths. A two-control simultaneous actuation prevents inadvertent actuation.

Condition 3 results from the loss of all ac power for a period of time that approaches the 24-hour Class 1E dc battery capability to activate the in-containment refueling water storage tank containment recirculation isolation valves. The timed output holds on restoration of ac power and is manually reset after the batteries are recharged. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by either of the two sensors connected to two of the four battery chargers.

The functional logic relating to activation of the containment recirculation isolation valves is illustrated in Figure 7.2-1, sheets 15 and 16.

7.3.1.2.10 Steam Line Isolation

A signal to isolate the steam line is generated from any one of the following conditions:

1. Manual initiation
2. High-2 containment pressure
3. Low lead-lag compensated steam line pressure
4. High steam line pressure negative rate
5. Low cold leg temperature

The steam line isolation signal closes the main steam line isolation valves and the stop and bypass valves. In addition to manual system-level steam line isolation, steam line isolation valves can be closed individually via the non-safety plant control system.

Condition 1 consists of two momentary controls. Manual actuation of either of the two controls initiates steam line isolation for both steam generators.

Condition 2 results from the coincidence of two of the four divisions of containment pressure above the High-2 setpoint.

Condition 3 results from the coincidence of two of the four divisions of compensated steam line pressure below the Low setpoint. The steam line pressure signal is lead-lag compensated to improve system response. If the pressure is below this setpoint, in either steam line, both main steam lines are isolated.

Condition 4 results from the coincidence in either steam line of two of the four divisions of rate-lag compensated steam line pressure exceeding the High negative rate setpoint.

Condition 5 results from the coincidence of reactor coolant system cold leg temperature below the Low T_{cold} setpoint in any loop.

Steam line isolation for conditions 3 and 5 may be manually blocked when pressurizer pressure is below the P-11 setpoint and is automatically unblocked when pressurizer pressure is above P-11. Steam line isolation on condition 4 is automatically blocked when pressurizer pressure is above P-11 and is automatically unblocked on the manual blocking of the steam line isolation for conditions 3 and 5. Under all plant conditions, steam line isolation is automatically provided on either Condition 3 or 5, or Condition 4.

The functional logic relating to main steam isolation is illustrated in Figure 7.2-1, sheet 9.

7.3.1.2.11 Steam Generator Blowdown System Isolation

Signals to close the isolation valves of the steam generator blowdown system in both steam generators are generated from the following conditions:

1. Passive residual heat removal heat exchanger alignment signal (Subsection 7.3.1.2.7)
2. Low narrow range steam generator level

Condition 2 results from the coincidence of two of the four divisions of narrow range steam generator level below the Low setpoint. This condition only closes the blowdown system isolation valves of the affected steam generator.

The functional logic relating to steam generator blowdown isolation is illustrated in Figure 7.2-1, sheets 7 and 8.

7.3.1.2.12 Passive Containment Cooling Actuation

A signal to actuate the passive containment cooling system is generated from either of the following conditions:

1. Manual initiation
2. High-2 containment pressure

The passive containment cooling actuation signal opens valves that initiate gravity flow of cooling water from the passive containment cooling system water storage tank to the top of the containment shell. The evaporation of the water on the containment shell provides the passive cooling.

Condition 1 consists of two momentary controls. Manual actuation of either of the two controls results in manual actuation of the passive containment cooling system. This action also initiates containment isolation (Subsection 7.3.1.2.1) and isolation of the containment air filtration system (Subsection 7.3.1.2.19).

Condition 2 results from a coincidence of two of the four divisions of containment pressure above the High-2 setpoint. Manual reset is provided to block this actuation signal for passive containment cooling. Separate momentary controls are provided for resetting each division.

The functional logic relating to actuation of the passive containment cooling system is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.13 Startup Feedwater Isolation

Signals to isolate the startup feedwater supply to the steam generators are generated from either of the following conditions:

1. Low cold leg temperature
2. High-2 steam generator narrow range water level
3. Manual actuation of main feedwater isolation (Subsection 7.3.1.2.6)
4. High steam generator narrow range water level (coincident with P-4 permissive)

Any of these conditions isolates the startup feedwater supply by tripping the startup feedwater pumps and closing the startup feedwater isolation and control valves.

Condition 1 results from the coincidence of reactor coolant system cold leg temperature below the Low T_{cold} setpoint in any loop. Startup feedwater isolation on this condition may be manually blocked when the pressurizer pressure is below the P-11 setpoint. This function is automatically unblocked when the pressurizer pressure is above the P-11 setpoint.

Condition 2 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High-2 setpoint for either steam generator.

Condition 3 is discussed in other subsections as noted.

Condition 4 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High setpoint for either steam generator coincident with the P-4 permissive (reactor trip).

The functional logic relating to the isolation of the startup feedwater is illustrated in Figure 7.2-1, sheets 9 and 10.

7.3.1.2.14 Boron Dilution Block

Signals to block boron dilution are generated from any of the following conditions:

1. Excessive increasing rate of source range flux doubling signal
2. Loss of ac power sources (low Class 1E battery charger input voltage)
3. Reactor trip (Table 7.3-2, interlock P-4)

In the event of an excessive increasing rate of source range flux doubling signal, the block of boron dilution is accomplished by closing the chemical and volume control system makeup isolation valves and closing the makeup pump suction valves to the demineralized water storage tanks. This signal also provides a non-safety trip of the makeup pumps. These actions terminate the supply of potentially unborated water to the reactor coolant system as quickly as possible.

In the event of a loss of ac power sources or a reactor trip (as indicated by P-4), the block of boron dilution is accomplished by closing the makeup pump suction valves to the demineralized water storage tanks and aligning the boric acid tank to the suction of the makeup pumps. This permits makeup as needed but ensures that it will be from a borated source that will not reduce the available shutdown margin in the reactor core.

Condition 1 is an average of the source range count rate, sampled at least N times over the most recent time period T_1, compared to a similar average taken at time period T_2 earlier. If the ratio of the current average count rate to the earlier average count rate is greater than a preset value, a partial trip is generated in the division. On a coincidence of excessively increasing source range neutron flux in two of the four divisions, boron dilution is blocked. The Flux Doubling function is also delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious dilution block due to the short term instability of the processed source range values. This source range flux doubling signal may be manually blocked to permit plant startup and normal power operation. It is automatically reinstated when reactor power is decreased below the P-6 power level during shutdown.

Condition 2 results from the loss of ac power. A short, preset time delay is provided to prevent actuation upon momentary power fluctuations; however, actuation occurs before ac power is restored by the onsite diesel generators. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by each of the two sensors connected to two of the four battery chargers. The two-out-of-four logic is based on an undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.

Condition 3 results from a reactor trip as indicated by the P-4 interlock.

The functional logic relating to the boron dilution block is illustrated in Figure 7.2-1, sheets 3 and 15.

7.3.1.2.15 Chemical and Volume Control System Isolation

A signal to close the isolation valves of the chemical and volume control system is generated from any of the following conditions:

1. High-2 pressurizer level
2. High-2 steam generator narrow range water level
3. Automatic or manual safeguards actuation signal (Subsection 7.3.1.1) coincident with High-1 pressurizer level
4. High-2 containment radioactivity
5. Manual initiation
6. High steam generator narrow range water level (coincident with P-4 permissive)

Condition 1 results from the coincidence of pressurizer level above the High-2 setpoint in any two of the four divisions. This function can be manually blocked when the reactor coolant system pressure is below the P-19 permissive setpoint to permit pressurizer water solid conditions with the plant cold and to permit pressurizer level makeup during plant cooldowns. This function is automatically unblocked when reactor coolant system pressure is above the P-19 setpoint.

Condition 2 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High-2 setpoint for either steam generator.

Condition 3 results from the coincidence of two of the four divisions of pressurizer level above the High-1 setpoint, coincident with an automatic or manual safeguards actuation.

Condition 4 results from the coincidence of containment radioactivity above the High-2 setpoint in any two of the four divisions.

Condition 5 consists of two momentary controls. This action also initiates auxiliary spray and letdown purification line isolation (Subsection 7.3.1.2.18).

Condition 6 results from a coincidence of two of the four divisions of narrow range steam generator water level above the High setpoint for either steam generator coincident with the P-4 permissive (reactor trip).

The functional logic relating to chemical and volume control system isolation is illustrated in Figure 7.2-1, sheets 6 and 11.

7.3.1.2.16 Steam Dump Block

Signals to block steam dump (turbine bypass) are generated from either of the following conditions:

1. Low-2 reactor coolant system average temperature
2. Manual initiation

Condition 1 results from a coincidence of two of the four divisions of reactor loop average temperature (T_{avg}) below the Low-2 setpoint. This blocks the opening of the steam dump valves. This signal also becomes an input to the steam dump interlock selector switch for unblocking the steam dump valves used for plant cooldown.

Condition 2 consists of three sets of controls. The first set of two controls selects whether the steam dump system has its normal manual and automatic operating modes available or is turned off. The second set of two controls enables or disables the operations of the Stage 1 cooldown steam dump valves if the reactor coolant average temperature (T_{avg}) is below the Low-2 setpoint. The third set of two controls enables or disables the operation of the Stage 2 cooldown steam dump valves.

The functional logic relating to the steam dump block is illustrated in Figure 7.2-1, sheet 10.

7.3.1.2.17 Control Room Isolation and Air Supply Initiation

Signals to initiate isolation of the main control room, to initiate the air supply, and to open the control room pressure relief isolation valves are generated from either of the following conditions:

1. High-2 control room air supply radioactivity level
2. Loss of ac power sources (low Class 1E battery charger input voltage)
3. Manual initiation

Condition 1 is the occurrence one of two control room air supply radioactivity monitors detecting a radioactivity level above the High-2 setpoint.

Condition 2 results from the loss of all ac power sources. A preset time delay is provided to permit the restoration of ac power from the offsite sources or from the onsite diesel generators before initiation. The loss of all ac power is detected by undervoltage sensors that are connected to the input of each of the four Class 1E battery chargers. Two sensors are connected to each of the four battery charger inputs. The loss of ac power signal is based on the detection of an undervoltage condition by each of the two sensors connected to two of the four battery chargers. The two-out-of-four logic is based on an undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.

In addition, the loss of all ac power sources coincident with main control room isolation will de-energize the main control room radiation monitors in order to conserve the battery capacity.

Condition 3 consists of two momentary controls. Manual actuation of either of the two controls will result in control room isolation and air supply initiation.

The functional logic relating to control room isolation and air supply initiation is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.18 Auxiliary Spray and Letdown Purification Line Isolation

A signal to isolate the auxiliary spray and letdown purification lines is generated upon the coincidence of pressurizer level below the Low-1 setpoint in any two of four divisions. This helps to maintain reactor coolant system inventory. This function can be manually blocked when the pressurizer water level is below the P-12 setpoint. This function is automatically unblocked when the pressurizer water level is above the P-12 setpoint. The automatic auxiliary spray isolation signal can be reset by the operator, after actuation of the auxiliary spray isolation valve, by using the reset control. This will allow the operators to use the auxiliary spray to rapidly depressurize the reactor coolant system. The operator can also manually initiate auxiliary spray isolation. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 12.

The auxiliary spray and letdown purification line isolation signal is also generated upon manual actuation of chemical and volume control system isolation (Subsection 7.3.1.2.15).

7.3.1.2.19 Containment Air Filtration System Isolation

A signal to isolate the containment air filtration system is generated from any of the following conditions:

1. Automatic or manual safeguards actuation signal (Subsection 7.3.1.1)
2. Manual actuation of containment isolation (Subsection 7.3.1.2.1)
3. Manual actuation of passive containment cooling (Subsection 7.3.1.2.12)
4. High-1 containment radioactivity

Conditions 1, 2, and 3 are discussed in other subsections as noted.

Condition 4 results from the coincidence of containment radioactivity above the High-1 setpoint in any two of the four divisions.

The manual reset which is provided to block the automatic actuation signal for containment isolation (Subsection 7.3.1.2.1) also resets the containment air filtration system isolation signal generated as a result of condition 1.

No other interlocks or permissive signals apply directly to the containment air filtration system isolation function. Automatic actuation originates from a safeguards actuation (S) signal that does contain interlock and permissive inputs.

The functional logic relating to air filtration system isolation is illustrated in Figure 7.2-1, sheets 11 and 13.

7.3.1.2.20 Normal Residual Heat Removal System Isolation

Signals for isolating the normal residual heat removal system lines are generated from any of the following conditions:

1. Automatic or manual safeguards actuation signal (Subsection 7.3.1.1)
2. High-2 containment radioactivity
3. Manual initiation

The isolation signal generated as a result of Condition 1 can be manually reset to block the isolation of the normal heat removal system lines. This is done to permit the normal residual heat removal system to operate after the occurrence of a safeguards actuation signal. Separate momentary controls are provided for resetting each division.

Condition 2 results from the coincidence of containment radioactivity above the High-2 setpoint in any two of the four divisions.

These actuation signals can be manually blocked when pressurizer pressure is below the P-11 permissive setpoint and are automatically unblocked when pressurizer pressure is above the P-11 setpoint.

Condition 3 consists of two sets of two momentary controls. Manual actuation of both controls of either of two control sets initiates closure of RNS isolation valves. A two-control simultaneous actuation prevents inadvertent actuation.

The functional logic relating to normal residual heat removal system isolation is illustrated in Figure 7.2-1, sheets 13 and 18.

7.3.1.2.21 Refueling Cavity Isolation

A signal for isolating the spent fuel pool cooling system lines is generated upon the coincidence of spent fuel pool level below the Low setpoint in two of three divisions. This helps to maintain the water inventory in the refueling cavity due to line leakage. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 13.

7.3.1.2.22 Chemical and Volume Control System Letdown Isolation

A signal to isolate the letdown valves of the chemical and volume control system is generated upon the occurrence of a Low-1 hot leg level in either of the two hot leg loops. This helps to maintain reactor coolant system inventory during mid-loop operation. This signal may be manually blocked by the operator when pressurizer level is above the P-12 setpoint. The functional logic relating to this is illustrated in Figure 7.2-1, sheet 16. These letdown valves are also closed by the containment isolation function as described in Subsection 7.3.1.2.1.

7.3.1.2.23 Pressurizer Heater Trip

Signals for disabling the operation of the pressurizer heaters are generated from any of the following conditions:

1. Core makeup tank injection alignment signal (Subsection 7.3.1.2.3)
2. High-3 pressurizer water level

Division A of the protection and safety monitoring system provides actuation signals to five load center circuit breakers which provide the power feed to five pressurizer heater electrical control centers. When these five power feed breakers are opened, the electrical power is removed from the pressurizer heaters. In addition, Division C of the protection and safety monitoring system provides a separate signal to the plant control system. This separate signal is used to command the plant control system to open the molded-case circuit breakers which provide a power feed to each individual pressurizer heater. This arrangement provides for complete disabling of the pressurizer heaters, even if a single component failure occurs. Pressurizer heater trip on condition 2 may be manually blocked when wide range RCS pressure is below the P-19 setpoint.

The functional logic relating to the pressurizer heater block is illustrated in Figure 7.2-1, sheets 6 and 12.

7.3.1.2.24 Steam Generator Relief Isolation

A signal for closing the steam generator power operated relief valves and their block valves is generated from any of the following conditions:

1. Manual initiation
2. Low lead-lag compensated steam line pressure

Condition 2 results from the coincidence of two of the four divisions of compensated steam line pressure below the Low setpoint. The steam line pressure signal is lead-lag compensated to improve system response. The signal closes the steam generator power-operated relief valve and the associated block valve for the affected steam generator. Steam generator relief isolation for condition 2 may be manually blocked when pressurizer pressure is below the P-11 setpoint and is automatically unblocked when pressurizer pressure is above P-11.

The functional logic relating to steam generator relief isolation is illustrated in Figure 7.2-1, sheet 9.

7.3.1.2.25 Component Cooling System Containment Isolation Valve Closure

A signal to close the component cooling system containment isolation valves is derived from a coincidence of two of the four divisions of high reactor coolant pump bearing water temperature for any reactor coolant pump. The high temperature setpoint and dynamic compensation are the same as used in the high reactor coolant pump bearing water temperature reactor coolant pump trip (Subsection 7.3.1.2.5, condition 6), but with the inclusion of preset time delay.

The functional logic relating to the tripping of the reactor pumps is illustrated in Figure 7.2-1, Sheet 5.

7.3.1.2.26 Containment Vacuum Relief

A signal for opening the containment vacuum relief valves is generated from the following conditions:

- Low-2 containment pressure
- Manual initiation

Condition 1 results from the incidence of containment pressure reaching the Low-2 setpoint in any two of the four divisions.

Condition 2 consists of two momentary controls. Manual actuation of either of the two controls will result in opening of the containment vacuum relief valves.

Either signal will actuate two motor-operated containment isolation valves to break the containment vacuum.

The functional logic relating to containment vacuum relief is illustrated in Figure 7.2-1, Sheet 19.

7.3.1.3 Blocks, Permissives, and Interlocks for Engineered Safety Features Actuation

The interlocks used for engineered safety features actuation are designated as "P-xx" permissives and are listed in Table 7.3-2.

7.3.1.4 Bypasses of Engineered Safety Features Actuation

The channels used in engineered safety features actuation that can be manually bypassed are indicated in Table 7.3-1. A description of this bypass capability is provided in Subsection 7.1.2.9. The actuation logic is not bypassed for test. During tests, the actuation logic is fully tested by blocking the actuation logic output before it results in component actuation.

7.3.1.5 Design Basis for Engineered Safety Features Actuation

The following subsections provide the design bases information for engineered safety features actuation, including the information required by Section 4 of IEEE 603-1991. Engineered safety features are initiated by the protection and safety monitoring system. Those design bases relating to the equipment that initiates and accomplishes engineered safety features are given in WCAP-15776 (Reference 1). The design bases presented here concern the variables monitored for engineered safety features actuation and the minimum performance requirements in generating the actuation signals.

7.3.1.5.1 Design Basis: Generating Station Conditions Requiring Engineered Safety Features Actuation (Paragraph 4.1 of IEEE 603-1991)

The generating station conditions requiring protective action are identified in Table 15.0-6, which summarizes the engineered safety features as they relate to the Condition II, III, or IV events analyzed in Chapter 15.

7.3.1.5.2 Design Basis: Variables, Ranges, Accuracies, and Typical Response Times Used in Engineered Safety Features Actuation (Paragraphs 4.1, 4.2, and 4.4 of IEEE 603-1991)

The variables monitored for engineered safety features actuation are:

- Pressurizer pressure
- Pressurizer water level
- Reactor coolant temperature (T_{hot} and T_{cold}) in each loop
- Containment pressure
- Containment radioactivity level
- Steam line pressure in each steam line
- Water level in each steam generator (narrow and wide ranges)
- Source range neutron flux

- Core makeup tank level
- Reactor coolant level in each of the two hot legs
- Loss of ac power sources (low Class 1E battery charger input voltage)
- In-containment refueling water storage tank level
- Main control room supply air radioactivity level
- Reactor coolant pump bearing water temperature
- Startup feedwater flow
- Spent fuel pool level
- Reactor coolant pressure in each of the two hot legs

Subsections 7.3.1.1 and 7.3.1.2 discuss levels that result in engineered safety features actuation. The engineered safety features actuation and trip setpoints are maintained by the setpoint program, which is described in the technical specifications (Chapter 16).

Ranges, accuracies, and response times for the variables used in engineered safety features actuation are listed in Table 7.3-4. The time response is the maximum allowable time period for an actuation signal to reach the necessary components. It is based on following a step change in the applicable process parameter from 5 percent below to 5 percent above (or vice versa) the actuation setpoint with externally adjustable time delays set to OFF.

7.3.1.5.3 Design Basis: Spatially Dependent Variables Used for Engineered Safety Features Actuation (Paragraph 4.6 of IEEE 603-1991)

Spatially dependent variables are discussed in Subsection 7.2.1.2.3.

7.3.1.5.4 Design Basis: Limits for Engineered Safety Features Parameters in Various Reactor Operating Modes (Paragraph 4.3 of IEEE 603-1991)

During startup or shutdown, various engineered safety features actuation can be manually blocked. These functions are listed in Table 7.3-1.

During testing or maintenance of the protection and safety monitoring system, certain channels used for engineered safety features may be bypassed. Although no setpoints are changed for bypassing, the logic is automatically adjusted, as described in Subsection 7.3.1.4. The safeguards channels that can be bypassed in the protection and safety monitoring system are listed in Table 7.3-1.

7.3.1.5.5 Design Basis: Engineered Safety Features for Malfunctions, Accidents, Natural Phenomena, or Credible Events (Paragraph 4.7 and 4.8 of IEEE 603-1991)

The accidents that the various engineered safety features are designed to mitigate are detailed in Chapter 6 and Chapter 15. Table 15.0-6 contains a summary listing of the engineered safety features actuated for various Condition II, III, or IV events. It relies on provisions made to protect equipment against damage from natural phenomena and credible internal events. Consequently, there are no engineered safety features actuated by the protection and safety monitoring system to mitigate the consequences of events such as fires.

Functional diversity is used in determining the actuation signals for engineered safety features. For example, a safeguards actuation signal is generated from high containment pressure, low pressurizer pressure, and low compensated steam line pressure. Engineered safety features are not normally actuated by a single signal. The extent of this diversity is seen from the initiating signals presented in Subsections 7.3.1.1 and 7.3.1.2. Table 7.3-1 also lists the engineered safety features signals and the conditions that result from their actuation.

Redundancy provides confidence that engineered safety features are actuated on demand, even when the protection and safety monitoring system is degraded by a single random failure. The single-failure criterion is met even when engineered safety features channels are bypassed.

7.3.1.6 System Drawings

Functional diagrams are provided in Figure 7.2-1.

7.3.2 Analysis for Engineered Safety Features Actuation

7.3.2.1 Failure Modes and Effects Analyses

The AP1000 failure modes and effects analysis (Reference 1 of Section 7.2) examines failures of the protection and safety monitoring system. This analysis concludes that the protection system maintains safety functions during single point failures.

7.3.2.2 Conformance of Engineered Safety Features to the Requirements of IEEE 603-1991

The discussions presented in this subsection address only the functional aspects of actuating engineered safety features. Requirements addressing equipment in the protection and safety monitoring system are presented in WCAP-15776 (Reference 1).

7.3.2.2.1 Conformance to the General Functional Requirements for Engineered Safety Features Actuation (Section 5 of IEEE 603-1991)

The protection and safety monitoring system automatically generates an actuation signal for an engineered safety feature whenever a monitored condition reaches a preset value. The specific engineered safety features actuation functions are listed in Table 7.3-1 and are discussed in Subsection 7.3.1.2.

Table 7.3-4 lists the ranges, accuracies, and response times of the parameters monitored. The engineered safety features, in conjunction with a reactor trip, protect against damage to the core and reactor coolant system components, as well as maintain containment integrity following a Condition II, III, or IV event. Table 15.0-6 summarizes the events that normally result in the initiation of engineered safety features. The setpoints that actuate engineered safety features are listed in the technical specifications (Chapter 16).

7.3.2.2.2 Conformance to the Single Failure Criterion for Engineered Safety Features Actuation (Paragraph 5.1 of IEEE 603-1991)

A single failure in the protection and safety monitoring system does not prevent an actuation of the engineered safety features when the monitored condition reaches the preset value that requires the initiation of an actuation signal. The single failure criterion is met even when one division of the ESF coincidence logic is being tested, as discussed in Subsection 7.1.2.9, or when there is a bypass condition in connection with test or maintenance of the protection and safety monitoring system.

7.3.2.2.3 Conformance to the Requirements for Channel Independence of the Engineered Safety Features Actuation (Paragraph 5.6.1 of IEEE 603-1991)

A discussion of channel independence is presented in WCAP-15776 (Reference 1). The signals to initiate division A of the engineered safety features are electrically isolated from the signals to initiate the redundant divisions (B, C, and D). Divisions of the safeguards actuation system are electrically

independent and redundant, as are the power supplies for the divisions up to and including the final actuated equipment.

7.3.2.2.4 Conformance to the Requirements Governing Control and Protection System Interaction of the Engineered Safety Features Actuation (Paragraphs 5.6.3.1, 5.6.3.3, and 6.3.1 of IEEE 603-1991)

Discussions on this subject are presented in WCAP-15776 (Reference 1).

7.3.2.2.5 Derivation of System Input for Engineered Safety Features Actuation (Paragraph 6.4 of IEEE 603-1991)

To the extent feasible and practical, the protection and safety monitoring system inputs used to actuate engineered safety features are derived from signals that are direct measures of the desired parameters. The parameters are listed in Table 7.3-4.

7.3.2.2.6 Capability for Sensor Checks and Equipment Test and Calibration of the Engineered Safety Features Actuation (Paragraphs 5.7 and 6.5 of IEEE 603-1991)

The discussion of system testability provided in Section 7.1 is applicable to the sensors, signal processing, and actuation logic that initiate engineered safety features actuation.

The testing program meets Regulatory Guide 1.22 as discussed in WCAP-15776 (Reference 1). The program is as follows:

- Prior to initial plant operations, engineered safety features tests are conducted.
- Subsequent to initial startup, engineered safety features tests are conducted during each regularly scheduled refueling outage.
- During operation of the reactor, the protection and safety monitoring system is tested as described in Subsection 7.1.2.11. In addition, the engineered safety features final actuators, whose operation is compatible with continued plant operation, are tested periodically at power.
- Continuity of the wiring is verified for devices that cannot be tested at power without damaging or upsetting the plant. Operability of the final actuated equipment is demonstrated at shutdown.

During reactor operation, the basis for acceptability of engineered safety features actuation is the successful completion of the overlapping tests performed on the protection and safety monitoring system. Process indications are used to verify operability of sensors.

7.3.2.2.7 Conformance to Requirements on Bypassing Engineered Safety Features Actuation Functions (Paragraph 5.8, 5.9, 6.6, and 6.7 of IEEE 603-1991)

Discussions on bypassing are provided in WCAP-15776 (Reference 1) and Subsection 7.3.1.4.

7.3.2.2.8 Conformance to the Requirement for Completion of Engineered Safety Features Actuation Once Initiated (Paragraph 5.2 of IEEE 603-1991)

Once initiated, engineered safety features proceed to completion.

Equipment actuated on a safeguards actuation signal cannot be returned to its previous position for a predetermined time period following initiation of the safeguards actuation signal. A block of the automatic safeguards signal is permitted at this time, if the reactor is tripped. This interlock is shown in Figure 7.2-1, sheet 11.

Resetting a system-level safeguards signal does not terminate any safeguards function. Rather, it permits the operator to individually reposition equipment. Equipment cannot be reset until the system-level signal is reset.

7.3.2.2.9 Conformance to the Requirement to Provide Manual Initiation at the System-Level for All Safeguards Actuation (Paragraph 6.2 of IEEE 603-1991)

Manual initiation at the system-level exists for the engineered safety features actuation. These system-level manual initiations are discussed in Subsections 7.3.1.1 and 7.3.1.2.

As a minimum, two controls are provided for each system-level manual initiation so that the protective function can be manually initiated at the system-level, despite a single random failure in one control. In certain applications, such as automatic depressurization, two pairs of controls are provided. One pair must be actuated simultaneously. This reduces the likelihood of inadvertent actuation while providing a design that meets the single failure criterion.

7.3.3 Combined License Information

This section contained no requirement for information.

7.3.4 References

1. WCAP-15776, “Safety Criteria for the AP1000 Instrument and Control Systems,” April 2002.

Table 7.3-1 (Sheet 1 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
1. Safeguards Actuation Signal (Figure 7.2-1, Sheets 9 and 11)			
a. Low pressurizer pressure	4	2/4-BYP[1]	Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3 Manual block permitted below P-11 Automatically unblocked above P-11
b. Low lead-lag compensated steam line pressure	4/steam line	2/4-BYP[1] in either steam line	Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3 Manual block permitted below P-11 Automatically unblocked above P-11
c. Low cold leg temperature (Low T_{cold})	4/loop	2/4-BYP[1] either loop[6]	Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3 Manual block permitted below P-11 Automatically unblocked above P-11
d. High-2 containment pressure	4	2/4-BYP[1]	Can be manually blocked on presence of P-3 Block automatically removed on absence of P-3
e. Manual safeguards initiation	2 controls	1/2 controls	None
2. Containment Isolation (Figure 7.2-1 Sheets 11 and 13)			
a. Automatic or manual safeguards actuation signal	(See items 1a through 1e)		
b. Manual initiation	2 controls	1/2 controls	None
c. Manual initiation of passive containment cooling	(See item 10a)		

Table 7.3-1 (Sheet 2 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
3. Automatic Depressurization System (Figure 7.2-1, Sheet 15) **(Initiate Stages 1, 2, and 3)**			
a. Core makeup tank injection coincident with	(See items 6a through 6e)		
Core makeup tank level less than Low-1 setpoint	4/tank	2/4-BYP[1] either tank[2]	None
b. Extended undervoltage to Class 1E battery chargers(8)	2/charger	1/2 per charger and 2/4 chargers	None
c. Stages 1, 2, and 3 manual initiation	4 controls	2/4 controls[3]	None
(Initiate Stage 4)			
d. Stage 4 manual initiation coincident with one of the following two conditions:	4 controls	2/4 controls[3]	None
Low reactor coolant system pressure or	4	2/4 BYP[1]	None
3rd stage depressurization			
e. Core makeup tank level less than Low-2 setpoint coincident with	4/tank	2/4 BYP[1] either tank[2]	None
Low reactor coolant system pressure and coincident with	4	2/4 BYP[1]	None
3rd stage depressurization			
f. Coincident loop 1 and loop 2 Low-2 hot leg level (after delay)	1 per loop	2/2	Manual unblock permitted below P-12 Automatically blocked above P-12

Table 7.3-1 (Sheet 3 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
4. Main Feedwater Isolation (Figure 7.2-1, Sheet 10) (Closure of Control Valves)			
a. Safeguards actuation signal (automatic or manual)	(See items 1a through 1e)		
b. Manual initiation	2 controls	1/2 controls	None
c. High-2 steam generator narrow range level	4/steam generator	2/4-BYP[1] in either steam generator	None
d. Low reactor coolant temperature (Low-1 T_{avg}) coincident with	2/loop	2/4 -BYP[1]	Manual block permitted below P-11 Automatically unblocked above P-11
Reactor trip (P-4)	1/division	2/4	None
(Trip of Main Feedwater Pumps and Closure of Isolation and Crossover Valves)			
a. Safeguards actuation signal (automatic or manual)	(See items 1a through 1e)		
b. Manual initiation	2 controls	1/2 controls	None
c. High-2 steam generator narrow range level	4/steam generator	2/4-BYP[1] in either steam generator	None
d. Low reactor coolant temperature (Low-2 T_{avg}) coincident with	2/loop	2/4-BYP1	Manual block permitted below P-11 Automatically unblocked above P-11
Reactor trip (P-4)	1/division	2/4	None
5. Reactor Coolant Pump Trip (Figure 7.2-1, Sheets 5, 7, 12, and 15) **(Trips All Reactor Coolant Pumps)**			
a. Safeguards actuation signal (automatic or manual)	(See items 1a through 1e)		
b. Automatic reactor coolant system depressurization (first stage)	(See items 3a through 3c)		
c. Low-2 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-12 Automatically unblocked above P-12

Table 7.3-1 (Sheet 4 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
d. Low wide range steam generator water level coincident with	4/steam generator	2/4-BYP[1] in both steam generators	None
High hot leg temperature (High T_{hot})[(8)]	2/loop	2/4-BYP[1]	None
e. Manual core makeup tank initiation	(See item 6e)		
f. High reactor coolant pump bearing water temperature	4/pump	2/4-BYP[1] in affected pump	None
6. Core Makeup Tank Injection (Figure 7.2-1, Sheets 7, 12 and 15)			
a. Safeguards actuation signal (automatic or manual)	(See items 1a through 1e)		
b. Automatic reactor coolant system depressurization (first stage)	(See items 3a through 3c)		
c. Low-2 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-12 Automatically unblocked above P-12
d. Low wide range steam generator water level coincident with	4/steam generator	2/4-BYP[1] in both steam generators	None
High hot leg temperature (High T_{hot})[(8)]	2/loop	2/4-BYP[1]	None
e. Manual initiation	2 controls	1/2 controls	None
7. Turbine Trip (Figure 7.2-1, Sheet 14)			
a. Manual feedwater isolation	(See item 4b)		
b. Reactor trip (P-4)	1/division	2/4	None
c. High-2 steam generator narrow range level	4/steam generator	2/4-BYP[1] in either steam generator	None
8. Steam Line Isolation (Figure 7.2-1, Sheet 9)			
a. Manual initiation	2 controls	1/2 controls	None

Table 7.3-1 (Sheet 5 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
b. High-2 containment pressure	4	2/4-BYP[1]	None
c. Low lead-lag compensated steam line pressure[4]	4/steam line	2/4-BYP[1] in either steam line	Manual block permitted below P-11 Automatically unblocked above P-11
d. High steam line negative pressure rate	4/steam line	2/4-BYP[1] in either steam line[7]	Manual unblock permitted below P-11 Automatically blocked above P-11
e. Low cold leg temperature (Low T_{cold})	4/loop	2/4-BYP[1] either loop[6]	Manual block permitted below P-11 Automatically unblocked above P-11
9. Steam Generator Blowdown System Isolation (Figure 7.2-1 Sheets 7 and 8)			
a. Passive residual heat removal heat exchanger actuation	(See items 12a through 12f)		
b. Low narrow range steam generator water level	4/steam generator	2/4 BYP[1] in either steam generator	None
10. Passive Containment Cooling Actuation (Figure 7.2-1, Sheet 13)			
a. Manual initiation	2 controls	1/2 controls	None
b. High-2 containment pressure	4	2/4-BYP[1]	None
11. Startup Feedwater Isolation (Figure 7.2-1, Sheets 9 and 10)			
a. Low cold leg temperature (Low T_{cold})	4/loop	2/4-BYP[1] either loop[6]	Manual block permitted below P-11 Automatically unblocked above P-11
b. High-2 steam generator narrow range water level	4/steam generator	2/4-BYP[1] in either steam generator	None
c. Manual initiation of main feedwater isolation		(See item 4b)	
d. High steam generator narrow range level coincident with	4/steam generator	2/4-BYP[1] in either steam generator	None
Reactor trip (P-4)	1/division	2/4	None

Table 7.3-1 (Sheet 6 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
12. Passive Residual Heat Removal (Figure 7.2-1, Sheet 8)			
a. Manual initiation	2 controls	1/2 controls	None
b. Low narrow range steam generator water level coincident with	4/steam generator	2/4-BYP[1] in either steam generator	None
Low startup feedwater flow	2/feedwater line	1/2 in either feedwater line	None
c. Low steam generator wide range water level	4/steam generator	2/4-BYP[1] in either steam generator	None
d. Core makeup tank injection	(See Items 6a through 6e)		
e. Automatic reactor coolant system depressurization (first stage)	(See items 3a through 3c)		
f. High-3 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-19 Automatically unblocked above P-19
13. Block of Boron Dilution (Figure 7.2-1, Sheets 3 and 15)			
a. Flux doubling calculation	4	2/4-BYP[1]	Manual block permitted when critical or intentionally approaching criticality Automatically unblocked below P-6
b. Undervoltage to Class 1E battery chargers(8)	2/charger	2/2 per charger and 2/4 chargers[5]	None
c. Reactor trip (P-4)	1/division	2/4	None
14. Chemical Volume Control System Isolation (See Figure 7.2-1, Sheets 6 and 11)			
a. High-2 pressurizer water level	4	2/4-BYP[1]	Automatically unblocked above P-19 Manual block permitted below P-19
b. High-2 steam generator narrow range level	4/steam generator	2/4-BYP[1] in either steam generator	None
c. Automatic or manual safeguards actuation signal coincident with	(See items 1a through 1e)		

Table 7.3-1 (Sheet 7 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
High-1 pressurizer water level	4	2/4-BYP[1]	None
d. High-2 containment radioactivity	4	2/4-BYP[1]	None
e. Manual initiation	2 controls	1/2 controls	None
f. Flux doubling calculation	4	2/4-BYP[1]	Manual block permitted when critical or intentionally approaching criticality Automatically unblocked below P-6
g. High steam generator narrow range level coincident with	4/steam generator	2/4-BYP[1] in either steam generator	None
Reactor trip (P-4)	1/division	2/4	None
15. Steam Dump Block (Figure 7.2-1, Sheet 10)[(8)]			
a. Low reactor coolant temperature (Low-2 T_{avg})	2/loop	2/4-BYP[1]	None
b. Mode control	2 controls	1/division	None
c. Manual stage 1 cooldown control	2 controls	1/division	None
d. Manual stage 2 cooldown control	2 controls	1/division	None
16. Main Control Room Isolation and Air Supply Initiation (Figure 7.2-1, Sheet 13)			
a. High-2 control room supply air radiation	2	1/2	None
b. Undervoltage to Class 1E battery chargers[(8)]	2/charger	2/2 per charger and 2/4 chargers[5]	None
c. Manual initiation[(8)]	2 controls	1/2 controls	None
17. Auxiliary Spray and Purification Line Isolation (Figure 7.2-1, Sheet 12)			
a. Low-1 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-12 Automatically unblocked above P-12
b. Manual initiation of chemical and volume control system isolation	(See item 14e)		

Table 7.3-1 (Sheet 8 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
c. Manual initiation of auxiliary spray isolation	1	1/1	None
18. Containment Air Filtration System Isolation (Figure 7.2-1, Sheets 11 and 13)			
a. Containment isolation	(See items 2a through 2c)		
b. High-1 containment radioactivity	4	2/4-BYP[1]	None
c. N/A	2	N/A	For containment vacuum relief valves only – close on inside containment purge isolation valve not closed
19. Normal Residual Heat Removal System Isolation (Figure 7.2-1, Sheets 13 and 18)			
a. Automatic or manual safeguards actuation signal	(See items 1a through 1e)		
b. High-2 containment radioactivity	4	2/4-BYP[1]	Manual block permitted below P-11 Automatically unblocked above P-11
c. Manual initiation	4 controls	2/4 controls[3]	None
20. Refueling Cavity Isolation (Figure 7.2-1, Sheet 13)			
a. Low spent fuel pool level	3	2/3	None
21. Open In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valves (Figure 7.2-1, Sheets 12 and 16)			
a. Automatic reactor coolant system depressurization (fourth stage)	(See items 3d and 3e)		
b. Manual initiation	4 controls	2/4 controls[3]	None
22. Open Containment Recirculation Valves In Series with Check Valves (Figure 7.2-1, Sheet 15 and 16)			
a. Extended undervoltage to Class 1E battery chargers[(8)]	2/charger	1/2 per charger and 2/4 chargers	None
23. Open All Containment Recirculation Valves (Figure 7.2-1, Sheet 16)			
a. Automatic reactor coolant system depressurization (fourth stage) coincident with		(See items 3d through 3f)	
Low IRWST level (Low-3 setpoint)	4	2/4-BYP[1]	None
b. Manual initiation	4 controls	2/4 controls[3]	None
24. Chemical and Volume Control System Letdown Isolation (Figure 7.2-1, Sheet 16)			
a. Low-1 hot leg level	1 per loop	1/2	Manual block permitted above P-12 Automatically unblocked below P-12
25. Pressurizer Heater Trip (Figure 7.2-1, Sheets 6 and 12)			
a. Core makeup tank injection	(See items 6a through 6e)		
b. High-3 pressurizer level	4	2/4-BYP[1]	Manual block permitted below P-19 Automatically unblocked above P-19
26. Steam Generator Relief Isolation (Figure 7.2-1, Sheet 9)			

Table 7.3-1 (Sheet 9 of 9)
Engineered Safety Features Actuation Signals

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
a. Manual initiation	2 controls	1/2 controls	None
b. Low lead-lag compensated steam line pressure[4]	4/steam line	2/4-BYP[1] in either steam line	Manual block permitted below P-11 Automatically unblocked above P-11
27. Close Component Cooling System Containment Isolation Valves (Figure 7.2-1, Sheet 5)			
a. High reactor coolant pump bearing water temperature	4/pump	2/4-BYP[1] in affected pump	None
28. Containment Vacuum Relief (Figure 7.2-1, Sheet 19)			
a. Low-2 containment pressure	4	2/4-BYP[1]	None
b. Manual initiation	2 controls	1/2 controls	None

Notes:

1. 2/4-BYP indicates bypass logic. The logic is 2 out of 4 with no bypasses and 2 out of 3 with one bypass.
2. Any two channels from either tank not in same division.
3. Two associated controls must be actuated simultaneously.
4. Also, closes power-operated relief block valve of respective steam generator.
5. The two-out-of-four logic is based on undervoltage to the battery chargers for divisions A or C coincident with an undervoltage to the battery chargers for divisions B or D.
6. Any two channels from either loop not in same division.
7. Any two channels from either line not in same division.
8. This function does not meet the 10 CFR 50.36(c)(2)(ii) criteria and is not included in the Technical Specifications.

Table 7.3-2 (Sheet 1 of 4)
Interlocks for Engineered Safety Features Actuation System

Designation	Derivation	Function
P-3	Reactor trip breaker open	Permits manual reset of safeguards actuation signal to block automatic safeguards actuation
$\overline{\text{P-3}}$	Reactor trip breakers closed	Automatically resets the manual block of automatic safeguards actuation
P-4	Reactor trip initiated or reactor trip breakers open	(a) Isolates main feedwater if coincident with low reactor coolant temperature (b) Trips turbine (c) Blocks boron dilution
$\overline{\text{P-4}}$	No reactor trip initiated and reactor trip breakers closed	Removes demand for isolation of main feedwater, turbine trip and boron dilution block
P-6	Intermediate range neutron flux channels above setpoint	None
$\overline{\text{P-6}}$	Intermediate range neutron flux channels below setpoint	Automatically resets the manual block of flux doubling actuation of the boron dilution block
P-11	Pressurizer pressure below setpoint	(a) Permits manual block of safeguards actuation on low pressurizer pressure, low compensated steam line pressure, or low reactor coolant inlet temperature (b) Permits manual block of steam line isolation on low reactor coolant inlet temperature (c) Permits manual block of steam line isolation and steam generator power-operated relief valve block valve closure on low compensated steam line pressure (d) Coincident with manual actions of (b) or (c), automatically unblocks steam line isolation on high negative steam line pressure rate (e) Permits manual block of main feedwater isolation on low reactor coolant temperature

Table 7.3-2 (Sheet 2 of 4)
Interlocks for Engineered Safety Features Actuation System

Designation	Derivation	Function
P-11 (continued)	Pressurizer pressure below setpoint	(f) Permits manual block of startup feedwater isolation on low reactor coolant inlet temperature (g) Permits manual block of steam dump block on low reactor coolant temperature (h) Permits manual block of normal residual heat removal system isolation on high containment radioactivity.
$\overline{\text{P-11}}$	Pressurizer pressure above setpoint	(a) Prevents manual block of safeguards actuation on low pressurizer pressure, low compensated steam line pressure, or low reactor coolant inlet temperature (b) Prevents manual block of steam line isolation on low reactor coolant inlet temperature (c) Prevents manual block of steam line isolation and steam generator power-operated relief valve block valve closure on low compensated steam line pressure (d) Automatic block of steam line isolation on high negative steam line pressure rate (e) Prevents manual block of feedwater isolation on low reactor coolant temperature (f) Prevents manual block of startup feedwater isolation on low reactor coolant inlet temperature (g) Prevents manual block of normal residual heat removal system isolation on high containment radioactivity

Table 7.3-2 (Sheet 3 of 4)
Interlocks for Engineered Safety Features Actuation System

Designation	Derivation	Function
P-12	Pressurizer level below setpoint	(a) Permits manual block of core makeup tank actuation on low pressurizer level to allow mid-loop operation (b) Permits manual block of reactor coolant pump trip on low pressurizer level to allow mid-loop operation (c) Permits manual block of auxiliary spray and purification line isolation, and zinc and hydrogen addition isolation valves isolation on low pressurizer level to allow mid-loop operation (d) Coincident with manual action of (a), automatically unblocks fourth stage automatic depressurization system initiation on low hot leg level to provide protection during mid-loop operation. (e) Automatically unblocks chemical and volume control system letdown isolation on Low-1 hot leg level
$\overline{\text{P-12}}$	Pressurizer level above setpoint	(a) Prevents manual block of core makeup tank actuation on low pressurizer level (b) Prevents manual block of reactor coolant pump trip on low pressurizer level (c) Prevents manual block of auxiliary spray and purification line isolation, and zinc and hydrogen addition isolation valves isolation on low pressurizer level (d) Provides confirmatory open signal to the core makeup tank cold leg balance lines (e) Automatically blocks fourth stage automatic depressurization system initiation on low hot leg level to reduce the probability of spurious actuation. (f) Permits manual block of chemical and volume control system letdown isolation on Low-1 hot leg level

Table 7.3-2 (Sheet 4 of 4)
Interlocks for Engineered Safety Features Actuation System

Designation	Derivation	Function
P-19	Reactor coolant system pressure below setpoint	(a) Permits manual block of chemical and volume control system isolation on high pressurizer water level (b) Permits manual block of passive residual heat removal heat exchanger alignment on high pressurizer water level (c) Permits manual block of the pressurizer heater trip on high pressurizer water level
$\overline{\text{P-19}}$	Reactor coolant system pressure above setpoint	(a) Prevents manual block of chemical and volume control system isolation on high pressurizer water level (b) Prevents manual block of passive residual heat removal heat exchanger alignment on high pressurizer water level (c) Prevents manual block of the pressurizer heater trip on high pressurizer water level

Table 7.3-3 (Sheet 1 of 2)
System-Level Manual Input to the
Engineered Safety Features Actuation System

Manual Control	To Divisions				Figure 7.2-1 Sheet
Manual safeguards actuation #1	A	B	C	D	11
Manual safeguards actuation #2	A	B	C	D	11
Manual chemical and volume control system isolation #1	A		C	D	6
Manual chemical and volume control system isolation #2	A		C	D	6
Manual passive residual heat removal heat exchanger alignment #1	A	B		D	8
Manual passive residual heat removal heat exchanger alignment #2	A	B		D	8
Manual steam line isolation #1		B		D	9
Manual steam line isolation #2		B		D	9
Manual steam generator relief isolation #1		B		D	9
Manual steam generator relief isolation #2		B		D	9
Steam/feedwater isolation and safeguards block control #1	A				9
Steam/feedwater isolation and safeguards block control #2		B			9
Steam/feedwater isolation and safeguards block control #3			C		9
Steam/feedwater isolation and safeguards block control #4				D	9
Manual feedwater isolation #1		B		D	10
Manual feedwater isolation #2		B		D	10
Manual steam dump mode control #1		B			10
Manual steam dump mode control #2				D	10
Manual Stage 1 steam dump cooldown control #1		B			10
Manual Stage 1 steam dump cooldown control #2				D	10
Manual Stage 2 steam dump cooldown control #1		B			10
Manual Stage 2 steam dump cooldown control #2				D	10
Pressurizer pressure safeguards block control #1	A				11
Pressurizer pressure safeguards block control #2		B			11
Pressurizer pressure safeguards block control #3			C		11
Pressurizer pressure safeguards block control #4				D	11
Manual auxiliary spray isolation			C		12
Manual core makeup tank injection actuation #1	A	B	C	D	12
Manual core makeup tank injection actuation #2	A	B	C	D	12
Core makeup tank injection actuation block control #1	A				12
Core makeup tank injection actuation block control #2		B			12
Core makeup tank injection actuation block control #3			C		12
Core makeup tank injection actuation block control #4				D	12
Manual passive containment cooling actuation #1	A	B	C	D	13
Manual passive containment cooling actuation #2	A	B	C	D	13
Manual passive containment isolation actuation #1	A	B	C	D	13
Manual passive containment isolation actuation #2	A	B	C	D	13
Manual depressurization system stages 1, 2, and 3 actuation #1 & #2	A	B	C	D	15

Table 7.3-3 (Sheet 2 of 2)
System-Level Manual Input to the
Engineered Safety Features Actuation System

Manual Control	To Divisions				Figure 7.2-1 Sheet
Manual depressurization system stages 1, 2, and 3 actuation #3 & #4	A	B	C	D	15
Manual depressurization system stage 4 actuation #1 & #2	A	B	C	D	15
Manual depressurization system stage 4 actuation #3 & #4	A	B	C	D	15
Manual IRWST injection actuation #1 & #2	A	B	C	D	16
Manual IRWST injection actuation #3 & #4	A	B	C	D	16
Manual containment recirculation actuation #1 & #2	A	B	C	D	16
Manual containment recirculation actuation #3 & #4	A	B	C	D	16
Manual control room isolation and air supply initiation #1	A	B	C	D	13
Manual control room isolation and air supply initiation #2	A	B	C	D	13
RCS pressure CVS/PRHR block control #1	A				6
RCS pressure CVS/PRHR block control #2		B			6
RCS pressure CVS/PRHR block control #3			C		6
RCS pressure CVS/PRHR block control #4				D	6
Normal residual heat removal system isolation safeguards block control #1	A				13
Normal residual heat removal system isolation safeguards block control #2		B			13
Boron dilution block control #1	A				3
Boron dilution block control #2		B			3
Boron dilution block control #3			C		3
Boron dilution block control #4				D	3
Manual RNS isolation #1 & #3	A	B		D	18
Manual RNS isolation #2 & #4	A	B		D	18
CVS letdown isolation block control #1	A				16
CVS letdown isolation block control #2				D	16
Manual containment vacuum relief actuation #1	A		C		19
Manual containment vacuum relief actuation #2	A		C		19

Table 7.3-4 (Sheet 1 of 2)
Engineered Safety Features Actuation, Variables, Limits, Ranges, and Accuracies (Nominal)

Variable	Range of Variable	Typical Accuracy[1]	Typical Response Time (Sec)[2]
Pressurizer pressure	1700 to 2500 psig	±14% of span	1.0
Steam line pressure	500 to 1300 psig	±3% of span (Normal environment) ±10% of span (Adverse environment)	1.0
Steam line negative pressure rate	0 to 1300 psig	±0.2% of span	1.0
Cold leg temperature (T_{cold})	490 to 610°F	±3% of span	5.5
Hot leg temperature (T_{hot})	530 to 650°F	±2% of span	5.5
Containment pressure	-5 to 10 psig	±3% of span	1.0
Reactor coolant system hot leg level	0 to 100% of span	±5% of span	1.0
In-containment refueling water storage tank level	0 to 100% of span	±6% of span	1.0
Undervoltage on input of 1E battery charger	0 to 500 V	±2% of setpoint	1.5
Steam generator narrow range water level	0 to 100% of span (narrow range taps)	±22% of span	1.0
Steam generator wide range water level	0 to 100% of span (wide range taps)	±32% of span	1.0
Core makeup tank narrow range upper water level	0 to 100% of span	±40% of span	1.0
Core makeup tank narrow range lower water level	0 to 100% of span	±40% of span	1.0
Reactor coolant pump bearing temperature	70 to 450°F	±2% of span	5.5
Spent fuel pool level	0 to 26 feet	±3% of span	1.0
Reactor coolant system wide range pressure	0 to 3300 psig	±3% of span	1.0

Table 7.3-4 (Sheet 2 of 2)
Engineered Safety Features Actuation, Variables, Limits, Ranges, and Accuracies (Nominal)

Variable	Range of Variable	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Pressurizer water level	0 to 100% of cylindrical portion of pressurizer	±10% of span	1.0
Startup feedwater flow	0 to 600 gpm	±7% of span	1.0
Neutron flux (flux doubling calculation)	1 to 10^6 c/sec	±30% of span	1.0(3)
Control room supply air radiation level	10^{-12} to 10^{-2} μ Ci/cc	±50% of setpoint	20
Containment radioactivity	10^0 to 10^7 R/hr	±50% of setpoint	20

Notes:

1. Measurement uncertainty typical of actual applications. Harsh environments allowance has been included where applicable.
2. Delay from the time that the process variable exceeds the setpoint until the time that an output is provided to the actuated device.
3. Response time depends on flux doubling calculation.

7.4 Systems Required for Safe Shutdown

Systems to establish safe shutdown conditions perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a subcritical condition. Boration capability is provided to compensate for xenon decay and to maintain the required core shutdown margin. Second, these systems must provide residual heat removal capability to maintain adequate core cooling.

The designation of systems required for safe shutdown depends on identifying those systems that provide the following capabilities for maintaining a safe shutdown:

- Decay heat removal
- Reactor coolant system inventory control
- Reactor coolant system pressure control
- Reactivity control

There are two different safe shutdown conditions that are expected following a transient or accident condition. Short-term safe shutdown refers to the plant conditions from the start of an event until about 36 hours later. Long-term safe shutdown refers to the plant conditions after this 36-hour period.

The short-term safe shutdown conditions include maintaining the reactor subcritical, the reactor coolant average temperature less than or equal to no load temperature, and adequate coolant inventory and core cooling. These shutdown conditions shall be achieved following any of the design basis events using safety-related equipment. The specific safe shutdown condition achieved is a function of the particular accident sequence.

The long-term safe shutdown conditions are the same as the short-term conditions except that the coolant temperature shall be less than 420°F. This long-term condition must be achieved within 36 hours and maintained indefinitely using safety-related equipment.

There are no systems specifically and solely dedicated as safe shutdown systems. However, there are a number of plant systems that are available to establish and maintain safe shutdown conditions. Normally, in the event of a turbine or reactor trip, nonsafety-related plant systems automatically function to place the plant in short-term safe shutdown, as described in Subsection 7.4.1.2. During the short-term safe shutdown condition, an adequate heat sink is provided to remove reactor core residual heat and boration control is available. Redundancy of systems and components is provided to enable continued maintenance of the short-term safe shutdown condition. Additional redundant nonsafety-related systems are normally available to manually perform a plant depressurization and cooldown.

The engineered safety systems are designed to establish and maintain safe shutdown conditions for the plant. Nonsafety-related systems are not required for safe shutdown of the plant.

This section focuses on safety-related systems used to establish and maintain safe shutdown conditions. The discussion of safe shutdown does not include accident response and/or mitigation since the standard review plan for this section addresses safe shutdown not related to accident mitigation. However, safe shutdown conditions are also established and maintained by these safety-related systems following accident conditions. For example, the control rods are released to initially place the plant in a shutdown condition to mitigate the consequences of various accidents. The passive core cooling system, on the other hand, is used to provide core cooling in an accident, but it is also one of the principal systems used for safe shutdown. Only those specific engineered safety

systems listed in Table 7.4-1 are used to establish and maintain safe shutdown of the plant. These engineered safety systems automatically function to place the plant in a safe shutdown condition without operator action.

The instrumentation functions necessary for safe shutdown are available through instrumentation channels associated with the safety-related systems in the primary plant. These channels automatically actuate the protective functions provided by the safety-related systems. Manual actuation of the associated safety-related systems is also provided.

The instrumentation systems discussed in this section are those which are required during nonaccident conditions to align the safety-related systems and perform the specified safe shutdown functions.

The specific systems available for safe shutdown are discussed in Subsection 7.4.2 and are listed in Table 7.4-1.

Maintenance of safe shutdown conditions with these systems, and the associated instrumentation and controls, includes consideration of the accident consequences that might challenge safe shutdown conditions. The accident consequences that are germane are those that tend to degrade the capabilities for coolant circulation, boration, heat removal, and depressurization. Safe shutdown is achieved following any of the accidents analyzed in Chapter 15. The specific safe shutdown condition reached is a function of the particular accident sequence.

The instrumentation and controls discussed in Subsection 7.4.1 are used to control and/or monitor shutdown. These safety-related systems allow the maintenance of safe shutdown, even under accident conditions that tend toward a return to criticality or a loss of heat sink.

In addition to the operation of safety-related systems used for safe shutdown, as described in Subsection 7.4.1, the following are part of the safe shutdown provisions:

- The turbine is tripped. (This can be accomplished at the turbine as well as from the main control room.)
- The reactor is tripped. (This can be accomplished at the reactor trip switchgear as well as from the main control room.)
- Support of engineered safety systems actuation is provided by safety-related onsite dc power.

7.4.1 Safe Shutdown

7.4.1.1 Safe Shutdown Using Safety-Related Systems

The following describes the process that establishes safe shutdown conditions for the plant, using the safety-related systems, and no operator action. The reactor coolant system is assumed to be intact for this discussion of safe shutdown.

Since this discussion only considers the use of safety-related systems, offsite electrical power sources are assumed to be lost at the start of the event. This results in a loss of the reactor coolant pumps. Even though the reactor coolant pumps are tripped during the initiation of certain engineered safety system actuation, it is assumed that no engineered safety system actuation signal is generated for this initiating event. With loss of the reactor coolant pumps, reactor coolant system natural circulation flow initiates and transfers core heat to the steam generators. Since feedwater flow is lost, the existing steam generator water inventory provides initial decay heat removal capability.

The initial loss of main ac power results in the Class 1E dc batteries automatically supplying power to the Class 1E dc power distribution network and the four Class 1E 120 Vac instrumentation divisions via the inverters.

The initial response of the passive safety systems is to actuate the passive residual heat removal heat exchanger due to low steam generator water level. The passive residual heat removal heat exchanger removes decay heat from the core by transferring this heat to the in-containment refueling water storage tank.

The passive residual heat removal heat exchanger removes core decay heat, cooling the reactor coolant system. As reactor coolant system cooldown continues, the reactor coolant system pressure decreases due to contraction of the reactor coolant system inventory since the pressurizer heaters are de-energized. An engineered safety system actuation signal occurs when reactor coolant system pressure decreases below a setpoint. This actuates the core makeup tanks, if they had not been previously actuated due to low pressurizer level. The core makeup tanks provide borated water injection to the reactor coolant system.

The engineered safety system actuation signal generated on low pressurizer pressure also actuates containment isolation. This prevents loss of water inventory from containment and permits indefinite operation of the passive residual heat removal heat exchanger and the in-containment refueling water storage tank.

The in-containment refueling water storage tank starts to boil about one to two hours after passive residual heat removal operation is initiated. Once boiling occurs, the in-containment refueling water storage tank begins steaming to containment, transferring heat to the air flowing on the outside of the containment shell. As steaming to containment continues, containment pressure slowly increases. As containment pressure slowly increases, an engineered safety system actuation signal is generated on containment high pressure, resulting in the initiation of passive containment cooling. This provides water flow on the outside of the containment shell to improve the heat removal performance from containment through evaporative cooling to the outside air.

A gutter located at the operating deck elevation collects condensate from the inside of the containment shell. Valves located in drain lines from the gutter to the containment waste sump close on a passive residual heat removal heat exchanger actuation signal. This action diverts the condensate to the in-containment refueling water storage tank. The system indefinitely provides core decay heat removal in this configuration without a significant increase in the containment water level.

Once the reactor coolant system and the safety systems are in this configuration, the plant is in a stable shutdown condition. The reactor coolant system temperatures and pressures continue to slowly decrease. The passive residual heat removal heat exchanger cools the reactor coolant system to 420°F in 36 hours.

Operation in this configuration may be limited in time duration by reactor coolant system leakage. The core makeup tanks can only supply a limited amount of makeup in the event there is reactor coolant system leakage. Eventually the volume of the water in the core makeup tanks will decrease to the first stage automatic depressurization setpoint. The time to reach this setpoint depends upon the reactor coolant system leak rate and the reactor coolant cooldown.

The Class 1E dc batteries that power the automatic depressurization system valves provide power for at least 24 hours. There is a timer that measures the time that ac power sources are unavailable. This timer provides for automatic actuation of the automatic depressurization system before the Class 1E dc batteries are discharged. The emergency response guidelines direct the operator to assess the need for automatic depressurization before the timer completes its count (approximately 22 hours). The operator assessment includes consideration for a visible refueling water storage tank

level, full core makeup tanks, and a high and stable in-containment refueling water storage tank level. If automatic depressurization is not needed, the operator is directed to de-energize all loads on the Class 1E dc batteries. This action preserves the capability for the operator to initiate automatic depressurization at a later time.

The automatic depressurization system can be manually initiated by the operator at any time, but no operator action is needed to provide safe shutdown conditions. Once the automatic depressurization system sequence initiates, the plant automatically transitions to lower pressure and temperature conditions that establish and maintain long-term safe shutdown of the plant.

When the automatic depressurization system is actuated, the first stage depressurization valves open and the reactor coolant system depressurization starts. The second and third stage depressurization valves open in sequence, based on automatic timers that are started upon the actuation of the first stage depressurization valves. As reactor coolant inventory continues to be lost, the core makeup tanks continue to inject. If the volume of the water in the core makeup tanks decrease to the fourth stage automatic depressurization setpoint, the fourth stage depressurization valves open. The water and steam vented from the reactor coolant system initially flows into the in-containment refueling water storage tank and overflows into the refueling canal. Eventually this overflows into the reactor vessel cavity, where any moisture from the fourth stage automatic depressurization system valves also collects from discharge in the loop compartments. This overflow initiates the floodup of containment, along with condensate from the containment shell and other cool surfaces in containment.

As the reactor coolant system pressure decreases, the accumulators inject borated water into the reactor coolant system. After the fourth stage automatic depressurization system valves open, the reactor coolant system pressure is reduced sufficiently so that in-containment refueling water storage tank injection can begin as the core makeup tanks empty.

The drain down of the in-containment refueling water storage tank is relatively slow, depending on the injection rates and the reactor coolant system pressure. As the in-containment refueling water storage tank continues to inject, the containment floodup also continues and eventually the floodup volume is sufficient to initiate flow from the recirculation sump.

As the reactor coolant system voids during the cooldown and depressurization process, water flow through the passive residual heat removal heat exchanger is replaced by steam flow, which also provides core cooling. As the in-containment refueling water storage tank empties and uncovers the passive residual heat removal heat exchanger, heat transfer via this path decreases. Eventually, the passive residual heat removal heat exchanger is uncovered, heat removal by the passive residual heat removal heat exchanger stops, and decay heat is removed by automatic depressurization system venting.

The final long-term safe shutdown plant conditions are maintained with the reactor coolant system depressurized to about 10 psig at saturated conditions, venting steam through the automatic depressurization system valves to containment, with heat transferred to the outside atmosphere via the passive containment cooling system. With containment isolation established, the water inventory inside containment provides an indefinite cooling water supply for core decay heat removal.

7.4.1.2 Safe Shutdown Using Safety-Related and Nonsafety-Related Systems

This subsection describes situations where nonsafety-related features of the plant are used together with safety-related systems to establish safe shutdown conditions. As discussed in Subsection 7.4.1.1, the AP1000 can be placed in a safe shutdown condition and maintained there using safety-related systems and no operator actions. Section 6.3 provides additional discussion of these situations.

Following passive residual heat removal heat exchanger actuation, the in-containment refueling water storage tank heats up and starts to boil after several hours of operation. If normal steam generator heat removal is not re-established, the operators align the normal residual heat removal system to cool the in-containment refueling water storage tank. This operation prevents significant steaming to the containment.

In case the automatic depresurization system is actuated, the operators align the normal residual heat removal system to provide injection to the reactor coolant system. This action causes the core makeup tank level to remain above the fourth stage valve actuation setpoint and prevents significant steaming to and flooding of the containment.

7.4.1.3 Safe Shutdown Using Nonsafety-Related Systems

This subsection describes the process to establish and maintain safe shutdown conditions using the nonsafety-related systems. As discussed in Section 7.4, the review of the plant safe shutdown capability, including the capabilities provided by the nonsafety-related systems, does not include accident response or mitigation. The nonsafety-related systems normally used to support plant shutdown operations are expected to be available. Offsite power is also expected to be available to support safe shutdown operations, although the nonsafety-related systems can establish and maintain safe shutdown conditions using only onsite electrical power.

For the purposes of this discussion, the nonsafety-related system operation following a reactor trip is described. As assumed in the discussion in Subsection 7.4.1.1 on safe shutdown using safety-related systems, the reactor coolant system is assumed to be intact during plant safe shutdown operations.

The nonsafety-related systems and equipment used to establish and maintain safe shutdown conditions are the same systems and equipment that are operated during normal plant startup and shutdown evolutions. The safe shutdown capability using the safety-related systems, described in Subsection 7.4.1.1, is only expected to be used in the event that the nonsafety-related systems are not available.

The nonsafety-related systems operate to establish and maintain safe shutdown conditions by providing the safe shutdown functions described in Section 7.4, except that reactivity control is only needed for long-term safe shutdown. If offsite power is available, the operation of these nonsafety-related systems is automatic.

The nonsafety-related systems actuate to establish and maintain the short-term safe shutdown conditions. The systems can also establish and maintain long-term safe shutdown conditions within the time limits discussed in Section 7.4. The operational philosophy following any event is to maintain appropriate safe shutdown conditions based on the duration of the shutdown, until the plant is able to re-start.

Cold shutdown conditions would only be established if it becomes necessary for equipment repair or due to limitations of the nonsafety-related systems in maintaining safe shutdown conditions (such as feedwater system water inventory). This philosophy reduces unnecessary challenges to plant safety due to the transition from operating systems to infrequently-operated standby systems.

Normally, offsite electrical power is available and the nonsafety-related systems automatically maintain short-term safe shutdown conditions as follows:

- Reactor coolant system forced flow to the steam generators by the reactor coolant pumps
- Feedwater from the main or startup feedwater systems

- Heat removal by the steam generators to the main condenser using turbine bypass valves
- Condenser heat removal provided by the main circulating water system
- Reactor coolant system inventory and boration control by the chemical and volume control system
- Reactor coolant system pressure control using pressurizer heaters and normal spray

If offsite power is not available, the reactor coolant pumps, main feedwater pumps, and main circulating water pumps will not be operating. However, the nonsafety-related systems maintain short-term safe shutdown conditions without offsite electrical power as follows:

- Electrical power provided to the required nonsafety-related systems by the diesel-generators of the onsite standby power system
- Heat removal by the steam generators directly to the atmosphere through the power-operated relief valves
- Feedwater from the startup feedwater system
- Reactor coolant system flow to the steam generators via natural circulation
- Reactor coolant system inventory and boration control by the chemical and volume control system
- Reactor coolant system pressure control using pressurizer heaters and auxiliary spray

In case the main feedwater is unavailable, the initial response of the nonsafety-related systems following a reactor trip is to automatically actuate the startup feedwater system, on low steam generator water level, to provide decay heat removal. The steam generators can remove decay heat from the core by either forced or natural circulation in the reactor coolant system. If offsite electrical power is available, the reactor coolant pumps continue to provide forced circulation in the reactor coolant system and the circulating water system continues to operate to provide a heat sink for the steam discharged from the steam generators to the main condenser.

With offsite power and the main condenser available, the turbine bypass valves automatically actuate after the reactor trip to control reactor coolant system temperature, based on the pre-set steam generator pressure control set point that is normally established for standby turbine bypass valve operation. The main feedwater system or the startup feedwater system automatically maintains steam generator water level as the turbine bypass valves continue to throttle steam flow to match the decreasing core decay heat levels. The pressurizer heaters and spray automatically maintain reactor coolant system subcooling with pressure at normal reactor coolant system conditions.

The chemical and volume control system makeup pumps automatically actuate as required to provide borated makeup water to maintain pressurizer level in the programmed band for no-load conditions. The makeup source is the boric acid tank which provides long-term reactivity control. The makeup pumps are expected to operate infrequently during these conditions to compensate for normal reactor coolant system inventory losses such as valve leakage.

Operation of the nonsafety-related systems in this mode maintains short-term safe shutdown conditions and reactor coolant system temperature and pressure remain near no-load conditions. If it becomes necessary to perform a plant cooldown and depressurization to establish long-term safe shutdown conditions, the nonsafety-related systems are used, following the normal plant cooldown

procedures. Manual boration to the cold shutdown boron concentration is provided by the chemical and volume control system by initiating reactor coolant system letdown in combination with makeup pump operation. After the boration is completed and letdown is secured, the makeup pumps automatically maintain reactor coolant system inventory throughout the remainder of the cooldown process.

After the required boration is completed the turbine bypass valves are used to initiate the cooldown, with manual control of pressurizer heaters and spray to maintain the reactor coolant system pressure, temperature, and cooldown rate within the limits specified in the technical specifications. The main feedwater system automatically provides feedwater and maintains steam generator level throughout the cooldown process.

When the reactor coolant system temperature and pressure are reduced to within the capabilities of the normal residual heat removal system, at approximately 350°F and 400 psig, the system is manually aligned to the reactor coolant system and started to continue the cooldown process. The final long-term safe shutdown conditions established would be dependent upon the specific maintenance required.

The use of the nonsafety-related systems and equipment for both short-term and long-term safe shutdown also requires the operation of associated support systems. These normally operating support systems include component cooling water, chilled water, compressed air, area ventilation, and nonsafety-related instrumentation and control power. These systems are started as required following a loss of offsite power, once the nonsafety-related diesel-generators are started.

If offsite electrical power is unavailable, the nonsafety-related systems actuate to establish and maintain safe shutdown conditions. There are some differences in the decay heat discharge flow path and the reactor coolant system remains at a slightly higher temperature resulting from the natural circulation flow conditions. With the loss of offsite electrical power, the nonsafety-related diesel-generators provide electrical power for the required nonsafety-related equipment. However, the reactor coolant pumps, main feedwater pumps, and main circulating water pumps are not available. Therefore, core decay heat is transferred to the steam generators using natural circulation in the reactor coolant system, the startup feedwater pumps supply the steam generators, and the steam generators discharge directly to the atmosphere to remove decay heat.

When offsite electrical power is unavailable, reactor coolant temperature is automatically maintained by the steam generator atmospheric power-operated relief valves instead of the turbine bypass valves. The steam generator power-operated relief valves maintain a pre-set steam generator pressure by throttling the steam discharged directly from the steam generators to the atmosphere. The relief valve operation maintains a slightly higher steam generator pressure than the pressure maintained with turbine bypass valve standby operation, resulting in a slight increase in the reactor coolant system temperature. The automatic operation of the startup feedwater subsystem maintains steam generator inventory with the pumps powered from the diesel-generators. In addition, the direct discharge of steam to the atmosphere prevents condensate recovery, which limits the water inventory for the startup feedwater system.

Following a loss of offsite power, the reactor coolant system temperature is slightly higher than for a reactor trip when offsite electrical power is available, resulting from natural circulation flow and steam generator power-operated relief valve operation. Since the transition to natural circulation flow is relatively slow, the reactor coolant system pressure remains stable without operator action. Operator action is not required to maintain reactor coolant system pressure.

Without offsite electrical power, the pressurizer heaters are manually re-energized after the diesel-generators start. Without reactor coolant pump operation, normal pressurizer spray is unavailable to counteract system pressure increases. Therefore, auxiliary spray provided by the chemical and

volume control system makeup pumps is manually initiated to decrease reactor coolant system pressure, if necessary. The operation of the chemical and volume control system makeup pumps to maintain reactor coolant system inventory is similar to their operation when offsite power is available, except that the pumps are manually controlled and powered from the diesel-generators.

The nonsafety-related systems are normally expected to maintain short-term safe shutdown conditions when offsite power is not available. If it is required to establish long-term safe shutdown conditions for equipment maintenance, the cooldown would normally be delayed until offsite power is recovered.

However, the nonsafety-related systems can be used to perform a natural circulation cooldown, if necessary. When performing a natural circulation plant cooldown and depressurization, the operation of the nonsafety-related systems is similar to the normal cooldown operation except that they are powered from the diesel-generators. The primary difference in operation is the use of the steam generator power-operated relief valves to control the cooldown process.

7.4.2 Safe Shutdown Systems

To effect a safe shutdown, with safety-related systems, the plant is initially brought to a stable condition with heat removal provided by the passive residual heat removal heat exchanger. For safe shutdown conditions, control is possible from either the main control room or the remote shutdown workstation. To accomplish a safe shutdown, the functions required are: coolant circulation, boration, heat removal, and depressurization. The portions of the protection and safety monitoring system required to achieve the safe shutdown condition are described in Sections 7.2 and 7.3. The minimum systems required to maintain safe shutdown conditions under a nonaccident condition are listed and discussed in the following paragraphs.

7.4.2.1 Passive Core Cooling System

A description of the passive core cooling system and its operation is provided in Section 6.3. The passive residual heat removal heat exchanger, the core makeup tanks, the in-containment refueling water storage tank, the containment recirculation, and the automatic depressurization system actuate automatically. They can also be manually initiated. Actuation controls are located at the remote shutdown workstation as well as in the main control room.

The safety injection flow from the accumulators, initiates automatically by the reactor coolant system depressurization process. The operation of the accumulator is integrated with the automatic actuation of the other passive core cooling subsystems.

7.4.2.2 Passive Containment Cooling System

A description of the passive containment cooling system and its operation is provided in Subsection 6.2.2. The passive containment cooling system actuates automatically. It also can be manually initiated. Actuation controls are located at the remote shutdown workstation as well as in the main control room.

7.4.2.3 Containment Isolation

A description of containment isolation valves and their operation is provided in various subsections. Each system that has piping that penetrates the containment vessel and therefore, requires containment isolation valves is discussed in its own subsection. Most of these systems are nonsafety-related; however, the containment isolation valves and the associated piping are safety-related and automatically close on a safeguards actuation (S) signal. The containment isolation system is discussed in Subsection 6.2.3.

7.4.2.4 Reactor Coolant System Circulation

The preferred method of coolant circulation is forced circulation with the reactor coolant pumps supplying the driving head. Upon the loss of main ac power, or when the reactor coolant pumps are tripped during engineered safety system actuation, the reactor coolant pumps are not available. However, the reactor coolant system is designed to provide sufficient natural circulation to achieve safe shutdown conditions with the steam generators and passive residual heat removal heat exchanger removing decay heat. Natural circulation flow is verified by monitoring the reactor coolant system temperatures.

7.4.2.5 Other Systems Required for Safe Shutdown

The other safety-related equipment and systems used to maintain the plant in safe shutdown are identified in Table 7.4-1. They are also listed below, with a reference to the respective section or subsection which discusses their operation in more detail:

- Protection and safety monitoring system — Sections 7.2, 7.3, and 7.5
- Class 1E dc and UPS system — Subsection 8.3.2

These systems are either normally operating or they start automatically when required. The instrumentation for these systems is described in the particular section containing the system description.

The monitoring instrumentation available in the main control room for safe shutdown is safety-related and is part of the protection and safety monitoring system. The instrumentation available for safe shutdown monitoring is listed in Section 7.5.

7.4.3 Safe Shutdown from Outside the Main Control Room

7.4.3.1 Description

If temporary evacuation of the main control room is required because of some abnormal main control room condition, the operators can establish and maintain safe shutdown conditions for the plant from outside the main control room through the use of controls and monitoring located at the remote shutdown workstation. Safe shutdown is a stable plant condition that can be maintained for an extended period of time. In the event that access to the main control room is restricted, the plant is maintained in safe shutdown until the main control room can be re-entered.

7.4.3.1.1 Remote Shutdown Room/Remote Shutdown Workstation

Safe shutdown can be established and maintained from the remote shutdown room. The I&C equipment in the room is collectively referred to as the remote shutdown workstation. The workstation is designed to allow control of a shutdown following an evacuation of the control room, coincident with the loss of offsite power and a single active failure. No other design basis event is postulated. Subsection 9.5.1 provides a discussion of shutdown in the event of a fire. The design basis for the remote shutdown workstation does not require safety-related displays, alarms, and controls.

The remote shutdown workstation contains nonsafety controls, displays, and alarms for the safety-related equipment required to establish and maintain safe shutdown. Additionally, control of nonsafety-related components is available.

The remote shutdown workstation includes operator workstations that are similar to the operator workstations in the main control room and are designed to the same standards. The remote shutdown workstation also includes dedicated nonsafety controls that provide the minimum inventory of controls listed in Table 18.12.2-1. The dedicated nonsafety controls interface to the plant safety and monitoring system via qualified isolators within that system.

The operator workstations have the same capabilities as the reactor operator's workstation in the main control room. The displays and alarms listed in Table 18.12.2-1 are retrievable from the operator workstations. Subsection 18.12.3 provides more discussion on the remote shutdown workstation displays, alarms, and controls.

The remote shutdown workstation is provided for use only following an evacuation of the main control room. No actions are anticipated from the remote shutdown workstation during normal, routine shutdown, refueling, or maintenance operations.

The remote shutdown workstation has sufficient communication circuits to allow the operator to effectively establish safe shutdown conditions. As detailed in Subsection 9.5.2, communication is available between the following stations:

- Main control room
- Remote shutdown workstation
- Onsite technical support center
- Diesel generator local control station

Operator control capability at the remote shutdown workstation is normally disabled, and operator control functions are normally performed from workstations located inside the main control room; however, operator control capability can be transferred from the main control room workstations to the remote shutdown workstation if the control room requires evacuation. Procedures will instruct the operator to trip the reactor prior to evacuating the control room and transferring control to the remote shutdown workstation. This operator control transfer capability cannot be disabled by any single active failure coincident with the loss of offsite power.

The control transfer function is implemented by multiple transfer switches. Each individual transfer switch is associated with only a single safety-related or single nonsafety-related group. These switches are located behind an unlocked access panel. Entry into this access panel will result in alarms at the main control room and remote shutdown workstation. The access panel is located within a fire zone which is separate from the main control room. Actuation of these transfer switches results in additional alarms at the main control room and remote shutdown workstation, the activation of operator control capability from the remote workstation, and the deactivation of operator control capability from the main control room workstations. This deactivation of operator control capability includes deactivation of all operator control capability provided by the soft control devices described in Subsection 7.1.3.3 and deactivation of all operator control capability provided by dedicated switches. This includes deactivation of operator control capability using manual actuation functions provided by the diverse actuation system as described in Subsection 7.7.1.11. The manual reactor trip switches located in the main control room are not affected by this control transfer function. The operator displays, located in the main control room and on the remote shutdown workstation, are also not affected by this control transfer function. The displays on the remote shutdown workstation are operational during normal operation (from the main control room) so that they can be used with no delay if transfer to the remote shutdown workstation is required.

7.4.3.1.2 Controls at Other Locations

In addition to the controls and indicators provided at the remote shutdown workstation, the following controls are provided outside the main control room:

- Reactor trip capability at the reactor trip switchgear
- Turbine trip capability at the turbine
- Start/stop controls for the diesel generators, located at each diesel generator local control panel
- Local control at motor control centers and electrical switchgear.

7.4.3.1.3 Design Bases Information

According to GDC 19, the capability of establishing a shutdown condition and maintaining the station in a safe status in that mode is an essential function. The controls and indications necessary for this function are identified in Subsection 7.4.2. To provide the availability of the remote shutdown workstation after control room evacuation, the following design features are provided:

- The remote shutdown workstation conforms with the guidelines provided by ANSI 58.6 1996 (Reference 1).
- The remote shutdown workstation achieves and maintains safe shutdown conditions from full power conditions and maintains safe shutdown conditions thereafter.
- The remote shutdown workstation achieves safe shutdown when offsite power is available and when offsite power is not available.
- The remote shutdown workstation operates safety-related systems, independent from the main control room.
- The remote shutdown workstation is designed with redundancy. When a random event, such as a fire, or an allowable technical specification maintenance results in one safety-related division being unavailable, a single failure in a redundant division is not postulated. When a random event other than fire causes a main control room evacuation, a coincident single failure in the safety systems controlled from the remote shutdown workstation is considered.
- Access to the remote shutdown workstation is under administrative control.

7.4.3.2 Analysis

The analysis of the systems required for safe shutdown is provided in Subsection 7.4.1. The following discussion is limited to the remote shutdown workstation.

Conformance to NRC General Design Criteria

General Design Criterion 19 – The remote shutdown workstation provides adequate controls and indications located outside the main control room to establish and maintain the reactor and the reactor coolant system in a safe shutdown condition in the event that the main control room must be evacuated.

Conformance to NRC Regulatory Guides

Regulatory Guide 1.22 – The remote shutdown workstation is tested periodically during station operation.

Regulatory Guide 1.29 – The remote shutdown workstation is designed as seismic Category II to prevent compromising the function of safety-related devices during or after a safe shutdown earthquake.

Conformance to IEEE 603-1991

The remote shutdown workstation and the design features which provide for the transfer of control capability from the main control room to the remote shutdown workstation conform to applicable portions of IEEE 603-1991. The circuits which perform the control transfer function are designed so that a single failure does not prevent maintaining safe shutdown. This is accomplished by redundant components in the systems required for safe shutdown, using independent safety-related power divisions.

To prevent interaction between the redundant systems, the redundant control channels are wired independently and are separated from each other. Nonsafety-related circuits available for (but not required for) safe shutdown are electrically isolated from safety-related circuits.

7.4.4 Combined License Information

This section contained no requirement for information.

7.4.5 References

1. ANSI 58.6 1996, "Criteria for Remote Shutdown for Light Water Reactors."

Table 7.4-1
Systems Required for Safe Shutdown

Protection and Safety Monitoring System
Passive Core Cooling System
Passive Residual Heat Removal Heat Exchanger
Core Makeup Tanks
Accumulators
In-Containment Refueling Water Storage Tank
Containment Sump Recirculation
Automatic Depressurization Valves
Passive Containment Cooling System
Class 1E dc and UPS System
Containment Isolation Valves
Reactor System
Control Rods

7.5 Safety-Related Display Information

7.5.1 Introduction

An analysis is conducted to identify the appropriate variables and to establish the appropriate design bases and qualification criteria for instrumentation employed by the operator for monitoring conditions in the reactor coolant system, the secondary heat removal system, the containment, and the systems used for attaining a safe shutdown condition. This selection of monitored variables is based on the guidance provided in Regulatory Guide 1.97. The variables and instrument design criterion selected for the AP1000 is described in Subsections 7.5.2 and 7.5.3.

The safety-related display information is used by the operator to monitor and maintain the safety of the AP1000 throughout operating conditions that include anticipated operational occurrences and accident and post-accident conditions. The equipment which processes the safety-related display information and makes it available to the operator is discussed in Subsection 7.5.4.

7.5.2 Variable Classifications and Requirements

Accident monitoring instrumentation is necessary to permit the operator to take actions to address design basis accident situations and for unforeseen situations (should plant conditions evolve differently than predicted by the safety analyses, the control room operating staff has sufficient information to evaluate and monitor the course of the event). Additional instrumentation is needed to indicate to the operating staff whether the integrity of the fuel cladding, the reactor coolant pressure boundary, or the reactor containment has degraded beyond the prescribed limits defined in the plant safety analyses and other evaluations.

Six types of variables are classified to provide this instrumentation:

- Variables that provide information needed by the operator to perform manual actions associated with design basis accident events, for which no automatic control is provided and that are required for the safety systems to accomplish their safety function, are designated as Type A.

- Variables needed to assess that the plant critical safety functions are accomplished or maintained, as identified in the plant safety analysis and other evaluations, are designated as Type B.

- Variables used to monitor for the gross breach or the potential for gross breach of the fuel cladding, the reactor coolant pressure boundary, or the containment are designated as Type C.

- Variables needed to assess the operation of individual safety-related systems are designated as Type D.

- Variables used in determining the magnitude of the postulated releases and continually assessing releases of radioactive materials are designated as Type E.

- Variables that provide information to manually actuate and to monitor the performance of nonsafety-related systems to prevent unnecessary actuation of safety-related systems following plant events are designated as Type F.

The six classifications of variables are not mutually exclusive. When a variable is included in one or more of the six classifications, the equipment monitoring this variable meets the requirements of the highest category identified.

Three categories of design and qualification criteria are used. This classification is made to identify the importance of the information and to specify the requirements placed on the accident monitoring instrumentation. Category 1 instrumentation has the highest performance requirements and is used for information that cannot be lost. Category 2 and Category 3 instruments are of lesser importance in determining the state of the plant and do not require the same level of operational assurance.

The primary differences between category requirements are in qualification, application of single failure, power supply, and display requirements. Category 1 requires seismic and environmental qualification, the application of a single-failure criterion, use of emergency power, and an immediately accessible display. Category 2 requires environmental qualification commensurate with the required function. It may require emergency power, but does not require the single failure criterion or an immediately accessible display. Category 2 requires a rigorous performance verification for a single instrument channel. Category 3, which is high quality commercial grade, does not require qualification, single failure criterion, emergency power, or an immediately accessible display.

Table 7.5-1 summarizes the following information for each variable identified:

- Instrument range or status
- Type and category
- Environmental qualification
- Seismic qualification
- Number of required channels
- Power supply
- Qualified data processing system (QDPS) indication

Table 7.5-1 also provides variable data shown as "site specific."

7.5.2.1 Variable Types

Accident monitoring variables and information display channels are those that enable the control room operating staff to perform the functions defined by the Types A, B, C, D, E, and F classifications.

Type A

Type A variables provide the primary information to permit the control room operating staff to:

- Perform the diagnosis in the AP1000 emergency operating instructions

- Take the specified, preplanned, manually-controlled actions, for which automatic controls are not provided, and that are required for safety-related systems to mitigate design basis accidents

There are no specific preplanned, manually-controlled actions for safety-related systems to mitigate design basis events in the AP1000 design. This includes the diagnosis of plant conditions required to take preplanned manual action. Variables used for contingency actions and additional variables that might be utilized are Types B, C, D, E, and F.

Type B

Type B variables provide the control room operating staff with information to assess the process of accomplishing or maintaining critical integrity safety-related functions (that is, reactivity control, reactor coolant system integrity, reactor coolant system inventory control, reactor core cooling, heat sink maintenance, and reactor containment environment).

Type C

Type C variables provide the control room operating staff information to monitor:

- The extent to which variables that indicate the potential for causing a gross breach of a fission product barrier have exceeded the design basis values
- The in-core fuel cladding, the reactor coolant pressure boundary, or the primary reactor containment that may have been subject to gross breach

These variables include those required to initiate the early phases of an emergency plan. Excluded are those associated with monitoring of radiological release from the plant that are included in Type E.

Type C variables used to monitor the potential for breach of a fission product barrier have an extended range. The extended range is chosen to minimize the probability of instrument saturation even if conditions exceed those predicted by the safety analysis.

Although variables selected to fulfill Type C functions may rapidly approach the values that indicate an actual gross failure, it is the final steady-state value reached that is important. Therefore, a high degree of accuracy and a rapid response time are not necessary for Type C instrument channels.

Type D

Type D variables provide the control room operating staff with sufficient information to:

- Monitor the performance of plant safety-related systems used for mitigating the consequences of an accident and subsequent plant recovery to attain a safe shutdown condition, including verification of the automatic actuation of safety-related systems
- Take specified, preplanned, manually controlled actions using safety-related systems for establishing and maintaining a safe shutdown condition

Type E

Type E variables provide the control room operating staff with information to:

- Monitor the plant areas where access may be required to service equipment necessary to monitor or mitigate the consequences of an accident
- Estimate the magnitude of release of radioactive material through identified pathways and continually assess such releases
- Monitor radiation levels and radioactivity in the environment surrounding the plant
- Monitor the habitability of the main control room

Type F

Type F variables provide the information that allows the control room operating staff to:

- Take specified, preplanned, manually controlled actions using nonsafety-related systems to prevent the unnecessary actuation of safety-related systems

- Monitor the performance of plant nonsafety-related systems used for mitigating the consequences of an accident and subsequent plant recovery to establish shutdown conditions, including verification of the automatic actuation of nonsafety-related systems

- Operate other nonsafety-related systems normally used for plant cooldown and to maintain plant shutdown conditions

7.5.2.2 Variable Categories

The qualification requirements of the Types A, B, C, D, E, and F accident monitoring instrumentation are subdivided into three categories. Descriptions of the three categories are given below. Table 7.5-2 summarizes the selection criteria for Types A, B, C, D, E, and F variables into each of the three categories. Table 7.5-3 summarizes the design and qualification requirements of the three designated categories.

7.5.2.2.1 Category 1

Selection Criteria for Category 1

The selection criteria for Category 1 variables are subdivided according to the variable type. For Type A, those primary variables used for providing information for preplanned operator action, required for the safety-related systems to accomplish their safety function for design basis accidents, are designated as Category 1. For Type B, those primary variables used for monitoring the process of accomplishing or maintaining critical safety functions are designated Category 1. For Type C, those primary variables used for monitoring the potential for breach of a fission product barrier are designated as Category 1. There are no Types D, E, or F Category 1 variables.

Qualification Criteria for Category 1

The Category 1 instrumentation is seismically and environmentally qualified as described in Sections 3.10 and 3.11. Instrumentation continues to read within the required accuracy following, but not necessarily during, a seismic event.

Each instrumentation channel is qualified from the sensor up to, and including, the display. Subsection 7.5.2.2.4 details the extended range instrumentation qualification.

Design Criteria for Category 1

The following design criteria apply to Category 1:

- No single failure (within either the accident monitoring instrumentation, its auxiliary supporting features, or its power sources), concurrent with the failures that are a cause of or result from a specific accident, prevents the control room operating staff from receiving the required information. Where failure of one accident monitoring channel results in information ambiguity (that is, the redundant displays disagree), additional information is provided to allow the control room operating staff to analyze the actual conditions in the plant. This is accomplished by providing additional independent channels of information of the same variable (an identical channel), or by providing independent channels which monitor different variables which bear known relationships to the channels (a diverse channel(s)). Redundant or diverse channels are electrically independent and physically separated from each other and from equipment not classified as safety-related.

  If ambiguity does not result from failure of the channel, then a redundant or diverse channel is not provided.

- The instrumentation is energized from the uninterruptible power supply inverter subsystem from the Class 1E dc system.

- Servicing, testing, and calibration programs are specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the normal time interval between shutdowns, a capability for testing during power operation is provided.

- The design provides administrative control of the access for removing channels from service.

- The design provides administrative control of the access to setpoint adjustments, module calibration adjustments, and test points.

- The monitoring instrumentation design minimizes the development of conditions that cause displays to give anomalous indications that are potentially confusing to the control room operating staff.

- The instrumentation is designed to promote the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

- To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it is shown by analysis to provide unambiguous information.

- Periodic checking, testing, calibration, and calibration verification is performed.

- The range selected for the instrumentation encompasses the expected operating range of the monitored variable.

Information Processing and Display Interface Criteria for Category 1

The following interface criteria are implemented in the processing and displaying of the information:

- The control room operating staff has immediate access to the information from redundant or diverse channels in familiar units of measure. For example, degrees are used, not volts, for temperature readings. Where two or more instruments are needed to cover a particular range, overlapping instrument spans are provided.

- Continuous recording of these channels is provided following an accident until continuous recording of such information is not necessary. The term continuous recording does not exclude the use of discrete time sample data storage systems. This recording is available when required and does not need to be immediately accessible. The recording function is provided by the non-Class 1E data display and processing system.

7.5.2.2.2 Category 2

Selection Criteria for Category 2

The selection criteria for Category 2 variables are subdivided according to the variable type. For Types A, B, and C, some variables that provide backup information are designated Category 2. For Type D, those primary variables that are used for monitoring the performance of safety systems are designated as Category 2. For Type E, those primary parameters monitored for use in determining the magnitude of the release of radioactive materials and for continuously assessing such releases are designated as Category 2. For Type F, those primary parameters monitored for use in

implementing preplanned actions using nonsafety-related systems or for monitoring the status of nonsafety-related system operation are designated as Category 2.

Qualification Criteria for Category 2

Category 2 instrumentation is qualified from the sensor up to, and including, the channel isolation device for the environment in which it operates to serve its intended function.

Design Criteria for Category 2

The following design criteria apply to Category 2:

- Category 2 instrumentation that is required for operation of a safety-related component is energized from the Class 1E dc uninterruptible power supply system. Otherwise, the instrumentation is energized from the non-Class 1E dc uninterruptible power system.
- The out-of-service interval is based on the technical specification requirements on out-of-service for the system the instrument serves where applicable.
- Servicing, testing, and calibration programs are implemented to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the time interval between shutdowns, a capability for testing during power operation is provided.
- The design provides administrative control of the access for removing channels from service.
- The design provides administrative control of the access to setpoint adjustments, module calibration adjustments, and test points.
- The monitoring instrumentation design minimizes the potential for the development of conditions that cause displays to give anomalous indications that are potentially confusing to the control room operating staff.
- The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.
- To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information.
- Periodic checking, testing, calibration, and calibration verification is performed.
- The range selected for the instrumentation encompasses the expected operating range of the monitored variable.

Information Processing and Display Interface Criteria for Category 2

The instrumentation signal is processed for display on demand. Recording requirements are determined on a case-by-case basis.

7.5.2.2.3 Category 3

Selection Criteria for Category 3

The selection criteria for Category 3 variables are subdivided according to the variable type. Types B, C, D, E, and F variables which provide backup information are designated as Category 3.

Qualification Criteria for Category 3

The instrumentation is high quality, commercial grade which is not required to provide information when exposed to a post-accident adverse environment.

Design Criteria for Category 3

The following design criteria apply to Category 3:

- Servicing, testing, and calibration programs are implemented to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the normal time interval between plant shutdowns, a capability for testing during power operation is provided.
- The design provides administrative control of the access for removing channels from service.
- The design provides administrative control of the access to setpoint adjustments, module calibration adjustments, and test points.
- The monitoring instrumentation design minimizes the potential for the development of conditions that cause displays to give anomalous indications that are potentially confusing to the control room operating staff.
- The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.
- To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information.

Information Processing and Display Interface Criteria for Category 3

The instrumentation signal is processed for display on demand. Recording requirements are determined on a case-by-case basis.

7.5.2.2.4 Extended Range Instrumentation Qualification Criteria

The qualification environment for extended range instrumentation is based on the design basis accident events. The qualification value of the monitored variable is equal to the maximum range for the variable. The monitored variable is assumed to approach this peak by extrapolating the most severe initial ramp associated with the design basis accident events. The decay is considered proportional to the decay for this variable associated with the design basis accidents. No additional qualification margin is added to the extended range variable. Since extended variable ranges are nonmechanistically determined, extension of associated parameter levels is not justifiable and is, therefore, not implemented. For example, a sensor measuring containment pressure is qualified for the measured process variable range (that is, four times design pressure for steel containments), but the corresponding ambient temperature is not mechanistically linked to that pressure. Rather, the ambient temperature value is the bounding value for design basis accident events analyzed in Chapter 15. The extended range instrument provides information if conditions degrade beyond those postulated in the safety analysis.

7.5.3 Description of Variables

7.5.3.1 Type A Variables

Type A variables provide primary information to permit the control room operating staff to:

- Perform the diagnosis in the AP1000 emergency operating procedures.

- Take specified preplanned, manually-controlled actions, for which automatic controls are not provided, and that are required for safety-related systems to mitigate design basis accidents.

There are no specific preplanned, manually-controlled actions for safety-related systems to mitigate design basis events in the AP1000 design. This includes the diagnosis of plant conditions required to take preplanned manual action. Therefore, as reflected in Table 7.5-4, there are no Type A variables.

7.5.3.2 Type B Variables

Type B variables provide information to the control room operating staff to assess the process of accomplishing or maintaining critical safety functions, including the following:

- Reactivity control
- Reactor coolant system integrity
- Reactor coolant system inventory control
- Reactor core cooling
- Heat sink maintenance
- Containment environment.

Variables which provide the most direct indication (primary variable) to assess each of the six critical safety functions are designated as Category 1. Backup variables are designated as Category 2 or Category 3. These variables are listed in Table 7.5-5.

7.5.3.3 Type C Variables

Type C variables provide the control room operating staff with information to monitor the potential for breach or the actual gross breach of:

- Incore fuel cladding
- Reactor coolant system boundary
- Containment boundary.

Variables associated with monitoring radiological release from the plant are included in Type E.

Those Type C variables that provide the most direct measure of the potential for breach of one of the three fission product boundaries are designated as Category 1. Backup information that indicates potential for breach or actual breach is designated as Category 2 or Category 3. These variables are listed in Table 7.5-6.

7.5.3.4 Type D Variables

Type D variables provide sufficient information to the control room operating staff to:

- Monitor the performance of plant safety-related systems used for mitigating the consequences of an accident and subsequent plant recovery to attain a safe shutdown condition, including verification of the automatic actuation of safety-related systems

- Take specified, preplanned, manually controlled actions using safety-related systems used for establishing and maintaining a safe shutdown condition

Primary Type D variables are designated as Category 2. Backup information is designated as Category 3. These variables are listed in Table 7.5-7.

7.5.3.5 Type E Variables

Type E variables provide the control room operating staff with information to:

- Monitor the plant areas where access may be required to service equipment to monitor or mitigate the consequences of an accident
- Estimate the magnitude of release of radioactive materials through identified pathways
- Monitor radiation levels and radioactivity in the environment surrounding the plant
- Monitor the habitability of the main control room

Primary Type E variables are designated as Category 2. Backup variables are designated as Category 3. These variables are listed in Table 7.5-8.

Table 7.5-8 also provides variable data shown as "site specific."

7.5.3.6 Type F Variables

Type F variables provide the control room operating staff with information to:

- Take preplanned manual actions using nonsafety-related systems to prevent unnecessary actuation of the safety-related systems
- Monitor the performance of the nonsafety-related systems used to mitigate the consequences of an accident
- Operate other nonsafety-related systems normally used for plant cooldown and to maintain plant shutdown conditions

Primary Type F variables are designated as Category 2. Backup variables are designated as Category 3. These variables are listed in Table 7.5-9.

7.5.4 Processing and Display Equipment

The AP1000 processing and display function is performed by equipment which is part of the protection and safety monitoring system, plant control system, and the data display and processing system. A description of each of these processing systems is provided in Section 7.1.

The protection and safety monitoring system provides signal conditioning, communications, and display functions for Category 1 variables and for Category 2 variables that are energized from the Class 1E dc uninterruptible power supply system. The plant control system and the data display and processing system provides signal conditioning, communications and display functions for Category 3 variables and for Category 2 variables that are energized from the non-Class 1E dc uninterruptible power system. The data display and processing system also provides an alternate display of the variables which are displayed by the protection and safety monitoring system. Electrical separation of the data display and processing system and the protection and safety monitoring system is maintained through the use of isolation devices in the interconnections connecting the two systems, as discussed in Subsection 7.1.2.10. The portion of the protection and safety monitoring system which is dedicated to providing the safety-related display function for post-accident monitoring is referred to as the qualified data processing subsystems and are discussed in Subsection 7.1.2.5.

The qualified data processing subsystems are divided into two separate electrical divisions. Each of the two electrical divisions is connected to a Class 1E dc uninterruptible power system with sufficient battery capacity to provide necessary electrical power for at least 72 hours. If all ac power sources are lost for a period of time that exceeds 72 hours, the power supply system will be energized from the ancillary diesel generator or from ac power sources which are brought to the site from other locations. See Section 8.3.

Instrumentation associated with primary variables that are energized from the Class 1E dc uninterruptible power supply system are powered from one of the two electrical divisions with 72 hour battery capacity. Instrumentation associated with other variables that are energized from the Class 1E dc uninterruptible power supply system are powered from one of four electrical divisions with 24 hour battery capacity. If a variable exists only to provide a backup to a primary variable, it may be powered by an electrical division with a 24 hour battery capacity. In such cases, provisions are provided to enable this variable to be powered by an alternate source if it is needed to resolve a discrepancy between two primary variables in the event that all ac power sources are lost for a period in excess of 24 hours.

Class 1E position indication signals for valves and electrical breakers may be powered by an electrical division with 24 hour battery capacity. This is necessary to make full use of all four Class 1E electrical divisions to enhance fire separation criteria. The power associated with the actuation signal for each of these valves or electrical breakers is provided by an electrical division with 24 hour battery capacity, so there is no need to provide position indication beyond this period. The operator will verify that the valves or electrical breakers have achieved the proper position for long-term stable plant operation before position indication is lost. Once the position indication is lost, there is no need for further monitoring since the operator does not have any remote capability for changing the position of these components.

Electrically operated valves, which have the electrical power removed to meet the single failure criterion, are provided with redundant valve position sensors. Each of the two position sensors is powered from a different non-Class 1E power source.

7.5.5 Combined License Information

The site specific variables are addressed in Subsection 7.5.2 and Table 7.5-1, and in Subsection 7.5.3.5 and Table 7.5-8.

Table 7.5-1 (Sheet 1 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
RCS wide range pressure	0-3300 psig	B1, B2, D2, C1, F2	Harsh	Yes	3 (Note 4)	1E	Yes	Located inside containment
RCS T_H (Wide Range)	50-700°F	B1, B2, D2, F2	Harsh	Yes	2	1E	Yes	Diverse Measurement: Core exit temperature
RCS T_C (Wide Range)	50-700°F	B1, B2, D2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
Steam generator water level (wide range)	0-100% of span	D2, F3	Harsh	Yes	1/steam generator	1E	Yes	
Steam generator water level (narrow range)	0-100% of span	D2, F2	Harsh	Yes	1/steam generator	1E	Yes	
Pressurizer level	0-100% of span	B1, D2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
Pressurizer reference leg temperature	50-420°F	B1, D2	Harsh	Yes	3 (Note 4)	1E	Yes	
Neutron flux	10^{-6}- 200% power	B1	Harsh	Yes	3 (Note 4)	1E	Yes	
Control rod position	0-267 steps	B3, D3	None	None	1/control rod	Non-1E	No	
Containment water level	El. 72 ft. to 110 ft. in discrete steps	B1, C1, F2	Harsh	Yes	3 (Note 4)	1E	Yes	

Table 7.5-1 (Sheet 2 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Core exit temperature	200-2300°F	B1, C1, F2	Harsh	Yes	2/quadrant per Division	1E	Yes	
PRHR HX inlet temperature	50-650°F	D3	None	None	1	Non-1E	No	Primary indication is RCS T_H
PRHR HX outlet temperature	50-500°F	B1, D2	Harsh	Yes	1	1E	Yes	Diverse variable to PRHR flow
PRHR flow	700-3000 gpm	B1, D2, F2	Harsh	Yes	2	1E	Yes	Diverse measurement: PRHR outlet temperature
IRWST water level	0-100% of span	B1, D2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
RCS subcooling (Note 6)	200°F Sub-cooling to 35°F super heat	B1, F2	Harsh	Yes	2	1E	Yes	Diverse measurement: Core exit temperature & wide range RCS pressure
Passive containment cooling water flow	0-150 gpm	B1, D2	Mild	Yes	1 (Note 1)	1E	Yes	
PCS storage tank water level	5-100% of tank height	B1, D2	Mild	Yes	2	1E	Yes	Diverse measurement: PCS flow
IRWST surface temperature	50-300°F	D3	None	None	1	Non-1E	No	
IRWST bottom temperature	50-300°F	D3	None	None	1	Non-1E	No	
Steam line pressure	0-1300 psig	F2	Harsh/ Mild (Note 8)	Yes	1/steam generator (Note 11)	1E	No	

Table 7.5-1 (Sheet 3 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Startup feedwater flow	0-600 gpm	F2	Mild	Yes	1/steam generator (Note 11)	1E	No	
Startup feedwater control valve status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Containment pressure	-5 to 10 psig	B1, C2, D2, F2	Mild	Yes	3 (Note 4)	1E	Yes	
Containment pressure (extended range)	0 to 240 psig	C1	Mild	Yes	3 (Note 4)	1E	Yes	
Containment area radiation (high range)	10^0-10^7 R	C1, E2, F2	Harsh	Yes	3 (Note 4)	1E	Yes	
Reactor vessel hot leg water level	0-100% of span	B2, B3	Harsh	Yes	1	1E	Yes	Two instruments are provided
Plant vent radiation level	(Note 3)	C2, E2	Mild	None	1	Non-1E	No	
Remotely operated containment isolation valve status	Open/ Closed	B1, D2	Harsh/mild	Yes	1/valve (Note 7)	1E	Yes	Separate divisions on series valves
Containment vacuum relief valves	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Boundary environs radiation		C3, E3	None	None	N/A	Non-1E	No	Conforms to Regulatory Guide 1.97, Revision 3
• Airborne Radiohalogens and Particulates (portable sampling with onsite analysis capability)	10^{-9} to 10^{-3} µCi/cc							
• Radiation (portable instrumentation)	10^{-3} to 10^4 R/hr, photons 10^{-3} to 10^4 rads/hr, beta and low-energy photons							
• Radioactivity (portable instrumentation)	Multichannel gamma ray spectrometer							

Table 7.5-1 (Sheet 4 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Hydrogen concentration	0-20%	C3	None	None	1	Non-1E	No	Three instruments are provided
Class 1E dc switchboard voltages	0-300 Vdc	D2	Mild	Yes	1/ switchboard	1E	Yes	
Diesel generator status	On/Off	F3	None	None	1/diesel generator	Non-1E	No	
Diesel generator load	0-6000 kW	F3	None	None	1/diesel generator	Non-1E	No	
Voltage for diesel-backed buses	0-8600V	F3	None	None	3/bus	Non-1E	No	
Power supply to diesel-backed buses	On/Off	F3	None	None	1/supply source/bus	Non-1E	No	
RCP bearing water temperature	70-450°F	F3	Mild	Yes	1/RCP (Note 10)	1E	Yes	
RCP breaker status	Open/ Closed	D2, F3	Mild	Yes	1/breaker (Note 11)	1E	No	
Reactor trip breaker status	Open/ Closed	D2	Mild	Yes	1/breaker (Note 11)	1E	No	
MCR air storage bottle pressure	0-5000 psig	D2	Mild	None	1	Non-1E	No	Two instruments are provided
Turbine stop valve status	Open/ Closed	D2	None (Note 12)	None	1/valve	Non-1E	No	
Turbine control valve status	Open/ Closed	D2	None (Note 12)	None	1/valve	Non-1E	No	
Pressurizer pressure	1700- 2500 psig	B1, D2	Harsh	Yes	3 (Note 4)	1E	Yes	
Pressurizer safety valve status	Open/ Closed	D2	Harsh	None	1/valve	Non-1E	No	
Pressurizer heater power (current)	0-800 amps	F3	None	None	1/group	Non-1E	No	

Table 7.5-1 (Sheet 5 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Steam generator PORV status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam generator PORV block valve status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam generator safety valve status	Open/ Closed	D2	Harsh	None	1/valve	Non-1E	No	
Main feedwater isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Main feedwater flow	0-9x10^6 lb/hr	F3	None	None	1/feedline	Non-1E	No	
Main feedwater control valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam generator blowdown isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Steam flow	0-9x10^6 lb/hr	F3	None	None	1/steam generator	Non-1E	No	
Main steam line isolation valve status	Open/ Closed	D2, F3	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Main steam line isolation bypass valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Main feedwater pump status	On/Off	D2, F3	Mild	None	1/pump	Non-1E	No	
Main to startup feedwater crossover valve status	Open/ Closed	D2, F3	Mild	None	1/valve	Non-1E	No	
Startup feed-water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Circulating water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Condenser backpressure	0-1 atm	F3	None	None	1	Non-1E	No	

Table 7.5-1 (Sheet 6 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Startup feedwater Isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Condenser steam dump valve status	Open/ Closed	D2, F3	Mild	None	1/valve	Non-1E	No	
Condensate storage tank water level	0-100% of span	F3	None	None	1	Non-1E	No	
PCS water storage tank isolation valve status (Non-MOV)	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
PCS water storage tank series isolation valve status (MOV)	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Containment temperature	32-400°F	D2, F3	Harsh	None	1	Non-1E	No	
CCS surge tank level	0-100% of span	F3	None	None	1	Non-1E	No	
CCS flow	0-15,000 gpm	F3	None	None	1	Non-1E	No	
CCS pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
CCS flow to RNS valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
CCS flow to RCPs valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
CCS pump inlet temperature	50-200°F	F3	None	None	1	Non-1E	No	
CCS heat exchanger outlet temperature	50-130°F	F3	None	None	1	Non-1E	No	
Containment fan cooler status	On/Off	F3	None	None	1/fan	Non-1E	No	

Table 7.5-1 (Sheet 7 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Water-cooled chiller status	On/Off	F3	None	None	1/chiller	Non-1E	No	
Water-cooled chilled water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Water-cooled chilled water valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Spent fuel pool pump flow	0-1500 gpm	F3	None	None	1/pump	Non-1E	No	
Spent fuel pool temperature	50-250°F	F3	None	None	1	Non-1E	No	
Spent fuel pool water level	0-100% of span	D2, F3	Mild	Yes	3 (Note 4)	1E	Yes	
SFS to SGS compartment valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
SFS to cont. sump valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
SFS floodup valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT discharge isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT inlet isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
CMT upper water level sensor	74.5% - 64% of Volume	D2, F2	Harsh	Yes	1/tank	1E	Yes	
CMT lower water level sensor	27% - 17% of Volume	D2, F2	Harsh	Yes	1/tank	1E	Yes	
IRWST injection isolation valve (Squib)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
IRWST line isolation valve status (MOV)	Open/ Closed	D3	None	None	1/valve	Non-1E	No	

Table 7.5-1 (Sheet 8 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
ADS: first, second and third stage valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
ADS fourth stage valve status (Non-MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
ADS fourth stage valve status (MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
PRHR HX inlet isolation valve status	Open/ Closed	D2	Harsh	Yes	1 (Note 7)	1E	Yes	
PRHR HX control valve status	Position	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
IRWST gutter bypass isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Accumulator pressure	100-800 psig	D2	Harsh	None	1/tank	Non-1E	No	
Accumulator isolation valve status	Open/ Closed	D3	None	None	1/valve	Non-1E	No	
Accumulator vent valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Pressurizer spray valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Auxiliary spray line isolation valve status	Open/ Closed	D2, F3	Harsh	Yes	1 (Note 7)	1E	Yes	
Purification stop valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 11)	1E	No	

Table 7.5-1 (Sheet 9 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Containment recirculation isolation valve status (Non-MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Containment recirculation isolation valve status (MOV)	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
Purification return line stop valve status	Open/ Closed	D2	Harsh	None	1	Non-1E	No	
Boric acid tank level	0-100%	F3	None	None	1	Non-1E	No	
Demineralized water isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Boric acid flow	0-175 gpm	F3	None	None	1	Non-1E	No	
Makeup blend valve status	Position	F3	None	None	1	Non-1E	No	
Makeup flow	0-175 gpm	F3	None	None	1	Non-1E	No	
Makeup pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Makeup flow control valve status	Position	F3	None	None	1	Non-1E	No	
Letdown flow	0-120 gpm	F3	None	None	1	Non-1E	No	
RNS hot leg suction isolation valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
RNS flow	0-3000 gpm	F3	None	None	1/pump	Non-1E	No	
RCS sampling line isolation valve status	Open/ Closed	E3	Harsh	None	1/valve	Non-1E	No	

Table 7.5-1 (Sheet 10 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
IRWST to RNS suction valve status	Open/ Closed	B1, F3	Harsh	Yes	1 (Note 7)	1E	Yes	
RNS discharge to IRWST valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
RNS pump status	On/Off	F3	None	None	1/pump	Non-1E	No	
Reactor vessel head vent valve status	Open/ Closed	D2	Harsh	Yes	1/valve (Note 7)	1E	Yes	
MCR return air isolation valve status	Open/ Closed	D2, F3	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR toilet exhaust isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR supply air isolation valve status	Open/ Closed	D2, F3	Mild	Yes	1/valve (Note 7)	1E	Yes	
MCR differential pressure	-1" to +1" wg	D2	Mild	Yes	2	1E	Yes	
MCR air delivery flowrate	0-80 cfm	D2	Mild	Yes	2	1E	Yes	
MCR pressure relief isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve	1E	Yes	
MCR air delivery isolation valve status	Open/ Closed	D2	Mild	Yes	1/valve (Note 7)	1E	Yes	
Instrument air header pressure	0-125 psig	F3	None	None	1	Non-1E	No	
Service water flow	0-10,000 gpm	F3	None	None	1/pump	Non-1E	No	
Service water pump status	On/Off	F3	None	None	1/pump	Non-1E	No	

Table 7.5-1 (Sheet 11 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Service water pump discharge valve status	Open/ Closed	F3	None	None	1/valve	Non-1E	No	
Service water pump discharge temperature	50-150°F	F3	None	None	1/pump	Non-1E	No	
Main control room supply air radiation	Note 5	E3, F3	Mild	Yes	2 (Note 9)	1E	No	
Plant vent air flow	0-110% design flow	E2	Mild	None	1	Non-1E	No	
Turbine island vent discharge radiation level	10^{-6} - 10^{+5} µCi/cc	C2, E2	Mild	None	1	Non-1E	No	
Steam generator blowdown discharge radiation	10^{-6} - 10^{-1} µCi/cc	C2	Mild	None	1	Non-1E	No	
Steam generator blowdown brine radiation level	10^{-6} - 10^{-1} µCi/cc	C2	Mild	None	1	Non-1E	No	
Main steam line radiation level	10^{-1} - 10^{3} µCi/cc	C2, E2	Mild	None	1/line	Non-1E	No	
Control support area radiation	10^{-1} - 10^{4} mR/hr	E3	None	None	1	Non-1E	No	
Meteorological parameters		E3	None	None		Non-1E	No	
• Wind Speed	0 – 100 mph (±0.5 mph)				2 (1@ 10 m and 1 @ 60 m)			Conforms to Regulatory Guide 1.97, Revision 3
• Wind Direction	0° – 540° (±2.43°)				2 (1@ 10 m and 1 @ 60 m)			
• Differential Temperature	-9.4°F to 19.4°F (±0.212°F)				1 (10 – 60 m)			

Table 7.5-1 (Sheet 12 of 12)
Post-Accident Monitoring System

Variable	Range/ Status	Type/ Category	Qualification		Number of Instruments Required	Power Supply	QDPS Indication (Note 2)	Remarks
			Environmental	Seismic				
Primary sampling station area radiation level	10^{-1} - 10^{7} mR/hr	E3	None	None	1	Non-1E	No	
VES passive air filtration flow	0-2000 cfm	E3	None	None	1	Non-1E	No	

Notes:

1. Total flow measurement is obtained from the sum of four branch flow devices.
2. The same information is available in the control support area via the monitor bus. Information available on the qualified data processing system is also available at the remote shutdown workstation.
3. Noble gas: 10^{-7} to 10^{5} µCi/cc
   Particulate: 10^{-12} to 10^{-7} µCi/cc
   Iodines: 10^{-11} to 10^{-6} µCi/cc
4. The number of instruments required after stable plant conditions is two. A third channel is available through temporary connections to resolve information ambiguity if necessary (See Subsection 7.5.4).
5. Noble gas: 10^{-7} to 10^{-1} µCi/cc
   Particulate: 10^{-12} to 10^{-7} µCi/cc
   Iodines: 10^{-11} to 10^{-5} µCi/cc
6. Degree of subcooling is calculated from RCS wide range pressure and core exit temperature.
7. This instrument is not required after 24 hours.
8. Two steam line pressure instruments per SG are located inside containment, and are qualified for a harsh environment. Two steam line pressure instruments per SG are located outside containment (not in MSIV compartment), and are qualified for a mild environment.
9. MCR supply air radiation monitoring is not required after MCR has been isolated.
10. This instrument is only required when non-safety power is available.
11. This instrument is not required if non-Class 1E UPS power is not available.
12. These devices are backup verification to qualified system status parameters. These devices are purchased to perform in their anticipated service environments for the plant conditions for which they must function.

Table 7.5-2
Summary of Selection of Criteria

Type	Category 1	Category 2	Category 3
A	Primary variables that are used for diagnosis or providing information necessary for operator action	Variables that provide backup information	None
B	Primary variables that are used for monitoring the process of accomplishing or maintaining critical safety functions	Variables that provide backup information	Variables that provide backup information
C	Primary variables that are used for monitoring the potential for breach of a fission product barrier	Variables that provide backup information	Variables that provide backup information
D	None	Primary variables used for monitoring the performance of plant safety-related systems	Variables that provide backup information and monitor the performance of plant safety-related systems
E	None	Primary variables to be monitored in determining the magnitude of the release of radioactive materials and for continuously assessing such releases.	Variables that provide backup information in determining the magnitude of the release of radioactive materials and for continuously assessing such releases
F	None	Primary variables to be monitored to implement preplanned manual actions using nonsafety-related systems	Variables that provide backup information and for monitoring the performance of nonsafety-related systems

Table 7.5-3
Summary of Qualification, Design, and Interface Requirements

	Category 1	Category 2	Category 3
Qualification			
Environmental	Yes	Yes	No
Seismic	Yes	As appropriate (See Subsection 7.5.2.2.2.)	No
Design			
Single failure	Yes	No	No
Power supply	Class 1E dc battery	Class 1E dc or Non-Class 1E dc battery onsite (As appropriate, see Subsection 7.5.2.2.2.)	Non-Class 1E
Channel out of service	Technical Specifications	As appropriate (See Subsection 7.5.2.2.2.)	No specific requirement
Interface			
Minimum indication	Immediately accessible	On demand	On demand
Recording	Yes	As required (See Subsection 7.5.2.2.2.)	As required (See Subsection 7.5.2.2.3.)

Table 7.5-4
Summary of Type A Variables

There are no Type A variables for AP1000.

Table 7.5-5
Summary of Type B Variables

Function Monitored	Variable	Type/Category
Reactivity Control	Neutron flux Control rod position	B1 B3
Reactor Coolant System Integrity	RCS wide range pressure RCS wide range T_{hot} RCS wide range T_{cold} Containment water level Containment pressure	B1 B1 B1 B1 B1
Reactor Coolant Inventory Control	Pressurizer level Pressurizer reference leg temperature Pressurizer pressure Reactor vessel - hot leg water level	B1 B1 B1 B3
Reactor Core Cooling	Core exit temperature RCS subcooling RCS wide range T_{hot} RCS wide range T_{cold} RCS wide range pressure Reactor vessel - hot leg water level	B1 B1 B2 B2 B2 B2
Heat Sink Maintenance	IRWST water level PRHR flow PRHR outlet temperature PCS storage tank water level Passive containment cooling water flow IRWST to RNS suction valve status	B1 B1 B1 B1 B1 B1
Containment Environment	Containment pressure Remotely operated containment isolation valve status	B1 B1

Table 7.5-6
Summary of Type C Variables

Function Monitored	Variable	Type/Category
Incore Fuel Clad	Core exit temperature	C1
RCS Boundary	RCS wide range pressure Containment pressure Containment water level Containment area high range radiation Turbine island vent discharge radiation level Steam generator blowdown discharge radiation level Steam generator blowdown brine radiation level Main steam line radiation level	C1 C2 C1 C1 C2 C2 C2 C2
Containment Boundary	Containment pressure (extended range) Plant vent radiation level Hydrogen concentration Boundary environs radiation	C1 C2 C3 C3

Table 7.5-7 (Sheet 1 of 4)
Summary of Type D Variables

System	Variable	Type/Category
Reactivity Control System	Reactor trip breaker status	D2
	Control rod position	D3
Pressurizer Level and Pressure Control	Pressurizer safety valve status	D2
	Pressurizer level	D2
	RCS wide range pressure	D2
	Pressurizer pressure	D2
	Reference leg temperature	D2
RCS Loops	RCS wide range T_{hot}	D2
	RCS wide range T_{cold}	D2
	RCP breaker status	D2
Secondary Pressure and Level Control	Steam generator PORV status	D2
	Steam generator PORV block valve status	D2
	Steam generator safety valve status	D2
	Main feedwater isolation valve status	D2
	Steam generator level (wide range)	D2
	Steam generator level (narrow range)	D2
	Steam generator blowdown isolation valve status	D2

Table 7.5-7 (Sheet 2 of 4)
Summary of Type D Variables

System	Variable	Type/Category
Secondary Pressure and Level Control (continued)	Main feedwater pump status	D2
	Main feedwater control valve status	D2
	Main steam line isolation valve status	D2
	Main steam line isolation bypass valve status	D2
Startup Feedwater	Startup feedwater control valve status	D2
	Startup feedwater isolation valve status	D2
	Main to startup feedwater crossover valve status	D2
Safeguards	Containment pressure	D2
	Accumulator pressure	D2
	Core makeup tank upper water level switch	D2
	Core makeup tank lower water level switch	D2
	IRWST/line isolation valve status (MOV)	D3
	IRWST/injection isolation valve status (Squib)	D2
	ADS first stage, second stage and third stage valve status	D2
	ADS fourth stage valve status (MOV)	D2
	ADS fourth stage valve status (non-MOV)	D2
	PRHR heat exchanger inlet isolation valve status	D3
	PRHR heat exchanger control valve status	D2
	Reactor vessel head vent valve status	D2
	CMT/discharge isolation valve status	D2
	CMT inlet isolation valve status	D2

Table 7.5-7 (Sheet 3 of 4)
Summary of Type D Variables

System	Variable	Type/Category
Safeguards (continued)	Accumulator/isolation valve status	D3
	PRHR flow	D2
	Containment recirculation isolation valve status (MOV)	D2
	Containment recirculation isolation valve status (non-MOV)	D2
	PRHR HX inlet temperature	D3
	PRHR HX outlet temperature	D2
	IRWST surface temperature	D3
	IRWST bottom temperature	D3
	IRWST water level	D2
	IRWST gutter bypass isolation valve status	D2
	Remotely operated containment isolation valve status	D2
Chemical and Volume Control	Auxiliary spray line isolation valve status	D2
	Purification stop valve status	D2
	Purification return line stop valve status	D2
	Demineralized water isolation valve status	D2
Normal Residual Heat Removal	RNS hot leg suction isolation valve status	D2
Electric Power	Class 1E dc switchboard voltage	D2
Spent Fuel Pool	Spent fuel pool water level	D2
	SFS refueling cavity drain to SGS compartment isolation valve status	D2
	SFS refueling cavity drain to containment sump isolation valve status	D2
	SFS containment floodup isolation valve status	D2

Table 7.5-7 (Sheet 4 of 4)
Summary of Type D Variables

System	Variable	Type/Category
Containment Cooling	Containment temperature	D2
	PCS water storage tank series isolation valve status (MOV)	D2
	PCS water storage tank isolation valve status (non-MOV)	D2
	Passive containment cooling water flow	D2
	PCS storage tank water level	D2
Containment Air Filtration	Containment vacuum relief valve status	D2
HVAC System Status	MCR return air isolation valve status	D2
	MCR toilet exhaust isolation valve status	D2
	MCR supply air isolation valve status	D2
	MCR air delivery isolation valve status	D2
	MCR pressure relief isolation valve status	D2
	MCR air storage bottle pressure	D2
	MCR differential pressure	D2
	MCR air delivery flowrate	D2
Main Steam	Turbine stop valve status	D2
	Turbine control valve status	D2
	Condenser steam dump valve status	D2

Table 7.5-8
Summary of Type E Variables

Function Monitored	Variable	Type/Category
Containment Radiation	Containment area high range radiation level	E2
Area Radiation	Control support area radiation level	E3
	Primary sampling station area radiation level	E3
Airborne Radioactivity Released from Plant	Turbine island vent discharge radiation level	E2
	Plant vent radiation level	E2
	Plant vent air flow	E2
	Main steam line radiation level	E2
	Boundary environs radiation	E3
	Main control room supply air radiation level	E3
Environs Radiation and Radioactivity	Plant Environs radiation levels and airborne radioactivity	E3
Meteorology	Wind speed, wind direction, and estimation of atmospheric stability (based on vertical temperature difference)	E3
Accident Sampling	Primary coolant	E3
	Containment air	E3
MCR Filtration Flow	MCR passive filtration induced flow rate	E3

Table 7.5-9 (Sheet 1 of 4)
Summary of Type F Variables

Variable	Type/Category
Monitoring for preplanned manual nonsafety-related system actions	
RCS wide range pressure	F2
RCS wide range T_{hot}	F2
RCS wide range T_{cold}	F2
Steam generator level (NR)	F2
Pressurizer level	F2
Containment pressure	F2
Steam line pressure	F2
Containment water level	F2
IRWST water level	F2
Startup feedwater flow	F2
Containment area high range radiation level	F2
Core exit temperature	F2
RCS subcooling	F2
PRHR flow	F2
Core makeup tank upper water level switch	F2
Core makeup tank lower water level switch	F2
Monitoring for nonsafety-related system performance	
Pressurizer heater power (current)	F3
Steam generator PORV status	F3
Steam generator PORV block valve status	F3

Table 7.5-9 (Sheet 2 of 4)
Summary of Type F Variables

Variable	Type/Category
Startup feedwater control valve status	F3
Main feedwater flow	F3
Steam generator level (WR)	F3
Steam flow	F3
Main steam line isolation valve status	F3
Main feedwater pump status	F3
Startup feedwater pump status	F3
Condenser steam dump valve status	F3
Condensate storage tank level	F3
Pressurizer spray valve status	F3
Auxiliary spray line isolation valve status	F3
Makeup flow	F3
Makeup pump status	F3
Letdown flow	F3
Circulating water pump status	F3
Condenser backpressure	F3
Accumulator vent valve status	F3

Table 7.5-9 (Sheet 3 of 4)
Summary of Type F Variables

Variable	Type/Category
Boric acid tank level	F3
Boric acid flow	F3
Makeup blend valve status	F3
Makeup flow control valve status	F3
RNS flow	F3
RNS pump status	F3
IRWST to RNS suction valve status	F3
RNS discharge to IRWST valve status	F3
CCS surge tank level	F3
CCS flow	F3
CCS pump status	F3
CCS flow to RNS valve status	F3
CCS flow to RCPs valve status	F3
CCS pump inlet temperature	F3
CCS heat exchanger outlet temperature	F3
Diesel generator status	F3
Diesel generator load	F3
Voltage for diesel-backed buses	F3
Power supply to diesel-backed buses	F3
RCP bearing water temperature	F3
RCP breaker status	F3
Containment fan cooler status	F3
Water-cooled chiller status	F3
Water-cooled chilled water pump status	F3
Water-cooled chilled water valve status	F3
Containment temperature	F3
Main control room supply air isolation valve status	F3
Main control room return air isolation valve status	F3
Main control room supply air radiation	F3
Service water flow	F3

Table 7.5-9 (Sheet 4 of 4)
Summary of Type F Variables

Variable	Type/Category
Service water pump status	F3
Service water pump discharge valve status	F3
Service water pump discharge temperature	F3
Instrument air header pressure	F3
Spent fuel pool pump flow	F3
Spent fuel pool temperature	F3
Spent fuel pool water level	F3
Main to startup feedwater crossover valve status	F3

Table 7.5-201
Not Used

Table 7.5-202
Not Used

7.6 Interlock Systems Important to Safety

This section discusses interlock systems which operate to reduce the probability of occurrence of specific events or to verify the state of a safety system. These include interlocks to prevent overpressurization of low-pressure systems and interlocks to verify availability of engineered safety features.

7.6.1 Prevention of Overpressurization of Low-Pressure Systems

7.6.1.1 Description of Normal Residual Heat Removal Isolation Valve Interlocks

An interlock is provided for the normally closed, motor-operated normal residual heat removal system (RNS) inner and outer suction isolation valves. The interlock prevents the suction valves for the normal residual heat removal system from being opened by operator action unless the reactor coolant system pressure is less than a preset pressure and both the suction and discharge valves for the in-containment refueling water storage tank are in a closed position.

There are two parallel sets of two motor-operated valves in series in the normal residual heat removal system pumps suction line from the reactor coolant system hot leg. The two valves nearest the reactor coolant system are designated as the inner isolation valves. The two valves nearest the normal residual heat removal system pumps are designated as the outer isolation valves. Logic for the outer valves is similar to that provided for the inner isolation valves, except that equipment diversity is provided by virtue of the fact that the pressure transmitters used for valve interlocks on the inner valves are diverse from the pressure transmitters used for the outer valve interlocks. Typically, this diversity is achieved by procuring wide range pressure transmitters either with similar measurement principles from different vendors, or with different measurement principles (from either the same or different vendors).

Each valve is interlocked so that it cannot be opened unless the reactor coolant system pressure is below a preset pressure. This interlock prevents the valve from being opened (from the main control room or the remote shutdown workstation) when the reactor coolant system pressure is above the normal residual heat removal system design pressure.

Figure 7.2-1, Sheet 18 illustrates the interlock logic that applies to these valves. The logic, shown on Sheet 18, is replicated twice, once for each parallel path. This interlock logic prevents the two series isolation valves from being opened while the reactor coolant system is pressurized above a set pressure.

The valves may be closed by operator action from the main control room at any time. To prevent an inadvertent closure of these valves, no auto-closure interlock that would close the valves on high reactor coolant system pressure is included.

The normal residual heat removal system relief valves provide adequate system pressure protection for conditions after the valves have been opened. (This is discussed in Subsection 5.2.2.1). Alarms are provided in the main control room and on the remote shutdown workstation to alert the operator if reactor coolant system pressure exceeds the normal residual heat removal system design pressure after the valves are opened.

7.6.1.2 Analysis of Normal Residual Heat Removal Valve Interlocks

IEEE 603-1991 and IEEE 338-1987 criteria do not apply to the normal residual heat removal isolation valve interlocks. Their function is not required during, or after, a design basis event. However, because of the possible severity of the consequences of loss of function, the requirements of IEEE 603-1991 are applied with the following comments:

- For the purpose of applying IEEE 603-1991, the protection system is the two parallel sets of two valves in series and the components of their interlock circuitry. The inner valve is powered by a separate power supply from the outer valve of each series combination.

- Online testability; IEEE 603-1991, Paragraph 5.7: The pressure interlock signals and logic are tested on line to the maximum extent possible without adversely affecting safety. This test includes the initiating signals for the interlocks from the protection and safety monitoring system cabinets.

- IEEE 603-1991, Paragraph 6.8.2: This requirement does not apply, as the setpoints are independent of mode of operation and are not changed.

7.6.2 Availability of Engineered Safety Features

7.6.2.1 Passive Residual Heat Removal Heat Exchanger Inlet Isolation Valve

The passive core cooling system passive residual heat removal heat exchanger inlet line includes a normally open motor-operated isolation valve that can be manually controlled from either the main control room or the remote shutdown workstation. The generation of the confirmatory open signal to this valve is described in Subsection 7.3.1.2.7.

The use of a confirmatory open signal to this valve provides a means to automatically override bypass features that are provided to allow this isolation valve to be closed for short periods of time. As a result of the confirmatory open signal, isolation of the passive residual heat removal heat exchanger inlet line, for short periods of time during modes of plant operation when the passive residual heat removal heat exchanger is required to be operable, is acceptable.

The operation of the valve is controlled by an actuation control circuit that functions in the following manner:

- The control circuit has an automatic operation function that is normally enabled. It allows the valve to automatically open upon receipt of the confirmatory open signal, in case the valve is closed.

- The control circuit has a valve open actuation function that opens the valve when a control switch on the operator workstation is manually actuated. Once the operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve close actuation function that closes the valve when a control switch on the operator workstation is manually actuated. This function is required when performing periodic operability testing of the passive residual heat removal heat exchanger discharge valves when the reactor is operating. Once the manual operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve maintain closed actuation function to provide an administratively controlled manual block of the automatic opening of the valve. This function allows the valve to be maintained closed if needed for leakage isolation. The maximum permissible time that a passive residual heat removal heat exchanger inlet isolation valve can be closed is specified in technical specifications. An alarm is actuated when the maintain closed function is instated.

The valve is interlocked so that:

- If the maintain closed actuation has not been manually initiated, it opens automatically on receipt of a confirmatory open signal with the control circuit in automatic control or during the manual valve close function.

- It cannot be manually closed when a confirmatory open signal is present.

During plant operation and shutdown, the passive residual heat removal heat exchanger inlet isolation valve is open. To prevent an inadvertent closure of the valve, redundant output cards are used in the protection and safety monitoring system cabinet. Power to this valve is normally locked out at power to prevent a fire-induced spurious closing.

Figure 7.2-1, sheet 17 illustrates the interlock logic which applies to the passive residual heat removal heat exchanger inlet isolation valve.

This normally open motor-operated valve has alarms, indicating valve mispositioning (with regard to their passive core cooling function). The alarm actuates in the main control room and the remote shutdown workstation.

An alarm actuates for the passive residual heat removal heat exchanger inlet isolation valve under the following conditions when the passive residual heat removal heat exchanger is required:

- Sensors on the motor operator for the valve indicate when the valve is not fully open.

- Redundant sensors on the valve stem indicate when the valve is not fully open.

7.6.2.2 Core Makeup Tank Cold Leg Balance Line Isolation Valves

Each core makeup tank has a cold leg balance line which is provided with a normally open, motor-operated, isolation valve. The balance line isolation valves, for each core makeup tank, may be manually controlled from either the main control room or the remote shutdown workstation. The generation of the confirmatory open signal to these valves is described in Subsection 7.3.1.2.3.

A confirmatory open signal to these valves automatically overrides any bypass features that are provided to allow the balance line isolation valve to be closed for short periods of time. As a result of the confirmatory open signal, isolation of the core makeup tank cold leg balance line to permit inservice testing of the core makeup tank discharge valves, is acceptable.

The operation of each valve is controlled by an actuation control circuit that functions in the following manner:

- The control circuit has an automatic operation function that automatically opens the valve upon receipt of the confirmatory open signal, in case the valve is closed.

- The control circuit has a valve open actuation function that opens the valve when a control switch on the operator workstation is manually actuated. Once the operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve close actuation function that closes the valve when a control switch on the operator workstation is manually actuated. This function is provided for performing periodic operability tests of the core makeup tank discharge valves when the reactor is operating. Once the manual operation is complete, the control circuit returns to automatic operation.

- The control circuit has a valve maintain closed actuation function to provide an administratively controlled manual block of the automatic opening of the valve when the pressurizer level is greater than the P-12 interlock. This function allows the valve to be maintained closed if needed for leakage isolation. The maximum permissible time that a core makeup tank cold leg balance line isolation valve can be closed is specified in technical specifications. An alarm is actuated when the maintain closed function is instated.

Each valve is interlocked so that:

- It receives a confirmatory open signal automatically whenever the pressurizer water level increases above the P-12 interlock.

- It cannot be manually closed when a confirmatory open signal is present.

During power and shutdown operations, the core makeup tank cold leg balance line isolation valve remains open. To prevent an inadvertent closure of the valve, redundant output cards are used in the protection and safety monitoring system cabinet. As a result, it is not necessary to lock out control circuit power.

Figure 7.2-1, sheet 17 illustrates the interlock logic which applies to the cold leg balance line isolation valves on each of the two core makeup tanks. The logic shown on sheet 17 is replicated for each core makeup tank.

These normally open motor-operated valves have alarms, indicating valve mispositioning (with regard to their passive core cooling function). The alarms actuate in the main control room and the remote shutdown workstation.

An alarm actuates for a core makeup tank cold leg balance line isolation valve under the following conditions when the core makeup tank is required to be operable:

- Sensors on the motor operator for the valve indicate when the valve is not fully open.

- Redundant position sensors indicate when the valve is not fully open.

7.6.2.3 Interlocks for the Accumulator Isolation Valve and IRWST Discharge Valve

The accumulator isolation and in-containment refueling water storage tank injection isolation valves are safety-related in order to retain their pressure boundary and remain in their open position. The accumulator isolation and in-containment refueling water storage tank injection valve operators are nonsafety-related since the valves are not required to change position to mitigate an accident. The Chapter 15 safety analyses assume that these valves are not subject to valve mispositioning (prior to an accident) or spurious closure (during an accident). Valve mispositioning and spurious closure are prevented by the following:

- The Technical Specifications, Section 16.1, require these valves to be open and power locked out whenever these injection paths are required to be available. The accumulators are required to be available when the reactor coolant system pressure is above 1000 psig. Both in-containment refueling water storage tank injection lines are required to be available in Modes 1, 2, 3, and 4. One in-containment refueling water storage tank injection line is required to be available in Mode 5 and in Mode 6.

- The Technical Specifications, Section 16.1, require verification that the motor-operated valves are open every 12 hours. They also require verification that power is removed every 31 days.

- With power locked out, redundant (nonsafety-related) valve position indication is provided in the main control room and remote shutdown workstation. Valve position indication and alarm are provided to alert the operator if these valves are mispositioned. These indications are powered by different nonsafety-related power supplies.

In addition, the valves have a confirmatory open signal during an accident (safeguards actuation signal for accumulator motor-operated valves and automatic depressurization system stage 4 signal for in-containment refueling water storage tank motor-operated valves). The valves also have an automatic open signal when their close permissives (P-11 for accumulator motor-operated valves and P-12 for in-containment refueling water storage tank motor-operated valves) clear during plant startup. The confirmatory open and the automatic open control signals are provided to the valve operator by the nonsafety-related plant control system.

7.6.2.4 Interlock for Containment Vacuum Relief Isolation Valves

The containment vacuum relief path includes normally closed motor-operated isolation valves, which are located outside the containment and open automatically to provide a flow path to allow atmospheric air into the containment to equalize a negative differential pressure across the containment vessel shell. These valves also perform a containment isolation function when vacuum relief is not required. An interlock ensures the availability of the engineered safety features for the vacuum relief isolation valves to perform their vacuum relief and containment isolation functions. The opening of these valves at any time other than the mitigation of a negative pressure condition or for required testing is controlled by the following:

- Section 16.1 of the Technical Specifications requires verification every 31 days that the containment purge isolation valves are closed except when open for pressure control, as low as reasonably achievable (ALARA), or air quality considerations.

- Section 16.1 of the Technical Specifications requires verification every 24 hours that the inside containment purge isolation valve VFS-PL-V009 is closed or that the purge exhaust path is fully open.

- Safety-related position indication is available in the main control room and in the remote shutdown workstation on the non-safety-related operator work stations for the containment vacuum relief isolation valves and for the containment purge exhaust containment isolation valves. An alarm is provided if these valves are incorrectly positioned.

There is also a valve interlock between the inside containment purge exhaust isolation valve and the vacuum relief isolation valves, which limits the potential release of radioactivity from the containment while the containment isolation valves are being closed. The purge and vacuum relief valve interlock automatically closes the vacuum relief isolation valves any time that the inside containment purge exhaust valve is not fully closed and a coincident vacuum relief actuation signal is not present. If a vacuum relief actuation signal is present, it takes priority over the valve closure interlock.

As discussed in Subsections 6.2.3.5 and 9.4.7.2.3, the vacuum relief subsystem is used to mitigate a condition where the atmospheric air pressure outside is higher than the reactor containment air pressure (so that a negative containment pressure condition exists). The valves can be opened either automatically or manually when an excessively low containment pressure exists to mitigate the event. The actuation signal includes a control interlock provided by the protection and safety monitoring system. The interlock is a part of the logic for the control of the valves shown on Figure 7.2-1 (Sheet 19 of 21).

7.6.3 Combined License Information

This section contained no requirement for information.

7.7 Control and Instrumentation Systems

The function of the AP1000 control systems is to establish and maintain the plant operating conditions within prescribed limits. The control system improves plant safety by minimizing the number of situations for which some protective response is initiated and relieves the operator from routine tasks.

The AP1000 control systems share a common hardware design and implementation philosophy. They are also functionally integrated to enhance responsiveness during plant transients. Specific design requirements are imposed that limit the impact of individual equipment failures. (See Subsection 7.1.3).

The control systems regulate the operating conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following:

Reactor Coolant System Temperature - The control systems function to maintain the reactor coolant system temperature at or near a programmed value. This value is a function of plant load or other operating conditions. Steam conditions for the turbine depend on the temperature maintained in the reactor coolant. Reactor coolant system temperature is also used for controlling core reactivity.

Nuclear Power Distribution - Operating limits include the distribution of nuclear energy production within the core as well as its average value. The axial distribution of the nuclear power is controlled within prescribed limits.

Reactor Coolant System Pressure - The reactor coolant system is pressurized to prevent significant boiling at operating temperatures. This pressure is controlled within limits that prevent reductions which expose the fuel to possible departure from nucleate boiling or from increases that would challenge the reactor coolant system design pressure.

Pressurizer Water Level - To provide a sufficient buffer for plant transients, the reactor coolant system pressurizer contains a prescribed volume of water and steam which depends on plant load and operating temperature.

Steam Generator Water Level - The steam generator water level is maintained within limits to provide adequate energy removal capability and to avoid moisture carryover.

Steam Dump (Turbine Bypass) - For fast and large transients such as load rejections, an additional thermal load (designated steam dump or turbine bypass) functions until nuclear power is reduced. This steam dump is also used to maintain hot no-load or hot low-load conditions prior to turbine loading. It provides a means for plant cooldown.

7.7.1 Description

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

Reactor Power Control System - The reactor power control system coordinates the responses of the various reactivity control mechanisms. The system enables daily load follow operation with a minimum of manual control by the operator. Load regulation and frequency control are compatible with the reactor power control system operation. Axial nuclear power distribution control is also performed by the reactor power control system.

Rod Control System - The rod control system, in conjunction with the reactor power control system, maintains nuclear power and reactor coolant temperature, without challenges to the protection systems, during normal operating transients.

Pressurizer Pressure Control - The pressurizer pressure control system maintains or restores the pressurizer pressure to the nominal operating value following normal operating transients. The control system reacts to avoid challenges to the protection systems during these operating transients.

Pressurizer Water Level Control - The pressurizer water level control system establishes, and maintains or restores pressurizer water level to its programmed operating region. The required water level operating region is programmed as a function of reactor coolant system temperature to minimize charging and letdown requirements. No challenges to the protection system result from normal operational transients.

Feedwater Control System - The feedwater control system maintains the steam generator water level at a predetermined setpoint during steady-state operation. It also maintains the water level within operating limits during normal transient operation. The feedwater control system restores normal water level following a unit trip. The various modes of feedwater addition are automated to require a minimum of operator involvement.

Steam Dump Control - The steam dump control system reacts to prevent a reactor trip following a sudden loss of electrical load. The steam dump control system also removes stored energy and residual heat following a reactor trip so that the plant can be brought to equilibrium no-load conditions without actuation of the steam generator safety valves. The steam dump control system also provides for maintaining the plant at no-load or low-load conditions to facilitate a controlled cooldown of the plant.

Rapid Power Reduction - For large, rapid load rejections (turbine trip or grid disconnect from 50-percent power or greater) a rapid nuclear power cutback is implemented. This results in a reduction of thermal power to a level that can be handled by the steam dump system.

Defense-In-Depth Control - The plant control system provides control of systems performing defense-in-depth functions. Table 7.7-3 provides a listing of the defense-in-depth functions that are supported by the plant control system and provides a cross reference to the applicable information located in other sections of this document.

7.7.1.1 Reactor Power Control System

Automatic reactor power and power distribution control are the basic functions of the reactor power control system. They are achieved by varying the position of the control rods. Separate control rod banks are used to regulate reactor power and power distribution.

The reactor power control system enables the plant to respond to the following load change transients:

- Step load changes of plus or minus 10 percent
- Ramp load increases and decreases of 5 percent per minute
- Daily load follow operations with the following profile:
  - Power ramps from 100 percent to 50 percent in 2 hours

  - Power remains at 50 percent for 2 to 10 hours
  - Power ramps back up to 100 percent in 2 hours
  - Power remains at 100 percent for the remainder of the 24-hour cycle
- Grid frequency response (denoted load regulation) resulting in a maximum of 10-percent power change at 2 percent per minute

These capabilities are accomplished without a reactor trip or steam dump actuation. During daily load follow and load regulation transients, automatic control of axial offset is provided. The system restores coolant average temperature to a value which is within the programmed temperature band following a change in load. Manual control of either the power control rods (M banks) or the axial offset control rods (AO bank) is performed within the range of defined insertion limits.

The reactor power control system uses a different control strategy for the rods used to regulate core power (M banks) from the control strategy used to regulate axial offset (AO bank). Reactor coolant system boron concentration is adjusted by the operator to account for long-term core burnup. The adjustment also maintains the two gray M banks and both black M banks (M1 and M2) in a near fully withdrawn position, the first two moving gray M banks fully inserted, and the AO bank slightly inserted. During load follow or load regulation response transients, the power control and the axial offset control subsystems jointly function to control both core power and axial offset. The following two subsections provide a description of each control subsystem.

7.7.1.1.1 Power Control

The power control subsystem controls the reactor coolant average temperature by regulating the M control rod bank positions. The reactor coolant loop average temperatures are determined from hot and cold leg measurements in each reactor coolant loop. The 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 highest of the T_{avg} measured temperatures from each of the reactor coolant loops constitutes the primary control signal. The programmed coolant temperature increases linearly with turbine load from the zero-power to the full-power condition.

The temperature input signals for the power control subsystem are fed from protection channels via isolation devices and the signal selector function.

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

The deviation of the reactor coolant temperature from the programmed value is the basic control variable for reactor power control. A deadband is included in the power control subsystem so that no rod motion is demanded if the temperature error is within the deadband. As the temperature error becomes greater, the demanded rod speed becomes greater.

Separate reactor control deadbands are used for various modes of control. If the plant is in a load regulation mode of operation, then the deadband is widened from that used for base load or load follow operation. This allows the core reactivity feedbacks to assist in stabilizing the plant at the conclusion of the maneuver and reduces the total control rod movement and subsequent wear on the control rods.

A different control strategy is used at low-power levels, principally when the turbine is off-line and the steam dump system is used to regulate coolant temperature. In this mode, nuclear power is controlled directly. For this mode, a nuclear power setpoint calculator allows the operator to enter a desired power level above or below the current power level along with a desired rate of change (limited to fixed predetermined maximum limits). The nuclear power setpoint calculator then supplies a changing setpoint that provides for a linear ramp change in core power at the selected rate.

7.7.1.1.2 Axial Offset Control

The axial offset control subsystem controls the core axial offset (power difference between the top and bottom halves of the core) to a value that is within the desired control range for load follow and grid frequency change transients. This is accomplished by using control rod banks separate from those used for the reactor power control described in Subsection 7.7.1.1.1. Measurements of axial offset are input into the axial offset control subsystem and then compared to an axial offset control "window." This window is calculated from measurements of compensated excore nuclear flux, along with operator inputs for the desired axial offset target value and target bandwidth and the mode of control (load follow, load regulation, or base load). The nuclear flux signals are compensated by measurements of cold leg temperature to account for the effects of moderation of the neutron flux by the reactor vessel downcomer flow. If the plant is in a load regulation mode of control, then lag compensation is applied to both the nuclear flux and the axial offset signals. This provides a smoothed nuclear flux and axial offset signal input to the axial offset controller to avoid unnecessary axial offset control. When the axial offset error is outside the acceptable control window, the axial offset rods are actuated until the axial offset error is back inside the control window.

To minimize the potential for interactions between the power and the axial offset rod control subsystems, the power control subsystem takes precedence. If a demand signal exists for movement of the power control rods, then the axial offset rods are blocked from moving. Only when the temperature error is within the reactor power controller deadband and the associated rod banks have stopped are the axial offset rods allowed to move.

7.7.1.2 Rod Control System

The rod control system receives rod speed and direction signals from the power control and axial offset control subsystems. The portion of the rod control system associated with the power and axial offset control subsystems each operate their own sets of control rod banks as follows:

- The power control portion operates the MA, MB, MC, MD, M1 and M2 control rod banks.
- The axial offset control portion operates the AO control rod bank.

For power control, the rod speed demand signals vary over the range of 5 to 45 inches per minute (8 to 72 steps per minute), depending on the magnitude of the input signal. Manual control is provided to move a bank in or out at a prescribed fixed speed. In the automatic mode, the rods are withdrawn (or inserted) in a predetermined sequence within the limits imposed by the control interlocks as shown in Table 7.7-1.

For axial offset control, the rod speed demand signals are set to a fixed constant speed of approximately 5 inches per minute (8 steps per minute). Manual control is provided to move a bank in

or out at a prescribed fixed speed. In the automatic mode, the rods are withdrawn (or inserted) within the limits imposed by the control interlocks, as shown in Table 7.7-2.

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

The power and axial offset control rod banks are the only rods that can be manipulated under automatic control. Each bank contains one or more groups of four control rod assemblies. Each control rod assembly in a group is electrically paralleled to move simultaneously. There is individual position indication for each control rod assembly.

Power to the rod drive mechanisms is supplied by two motor-generator sets operating from two separate 480-volt, 3-phase busses. Each generator is the synchronous type, and is driven by a 200-horsepower induction motor. The ac power is distributed to the rod control system cabinets through the reactor trip switchgear.

The variable speed rod drive programmer used in the power control subsystem inserts small amounts of reactivity at low speed. This permits fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed for transients such as load rejections. A summary of the control rod assembly sequencing characteristics is given below:

- The control rod groups within the same bank are stepped so that the relative position of the groups do not differ by more than one step.

- The control rod banks are programmed so that withdrawal of the banks is sequenced in a prescribed order. The programmed insertion sequence is the opposite of the withdrawal sequence. That is, the last control bank withdrawn is the first control bank inserted.

- The control bank withdrawals are programmed so that, when the first bank reaches a preset position, the next bank begins to move out simultaneously with the first bank. This preset position is determined by the maximum allowable overlap between banks (approximately 50 to 100 steps). This withdrawal sequence continues until the reactor reaches the desired power level. The control bank insertion sequence is the opposite of the withdrawal sequence.

- Overlap between successive control banks is adjustable between 0 to 50 percent (0 to 135 steps), with an accuracy of ±1 step.

The constant rod speed used in the axial offset control subsystem provides a slow stable control of core axial offset. This is acceptable since axial offset changes for the design basis load follow transients generally occur over several hours and rapid response is not needed. The slow response of the axial offset control system also allows the rods used by the power control subsystem to counteract the core power reactivity changes that are induced by the axial offset rods.

7.7.1.3 Control Rod Position Monitoring

Digital Rod Position - The digital rod position indication system measures the position of each control rod assembly using a detector consisting of discrete coils mounted concentric with the rod drive pressure housing. The coils are located axially along the pressure housing and magnetically sense the entry and presence of the rod drive shaft through its center line.

Demand Position System - The demand position system counts the pulses generated in the rod control system to provide a digital readout of the demanded bank position. The demanded and measured rod position signals are displayed in the main control room. An alarm is generated

whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm is set with appropriate allowance for instrument error and within sufficiently narrow limits to prevent exceeding core design hot channel factors.

Alarms are also generated if any shutdown rod is detected to have left its fully withdrawn position, or if any M bank control rods are detected at the bottom position, except as part of the normal insertion sequence.

7.7.1.4 Control Rod Insertion Limits

With the reactor critical, the normal indication of reactivity status in the core is the position of the control rod bank in relation to reactor power (as indicated by the ΔT power monitors). The ΔT power signal is used to calculate insertion limits for the banks. The following two alarms are provided for each bank.

- A "low" alarm alerts the operator of an approach to the M bank or AO bank insertion limits. Further approach is avoided by following appropriate plant procedure.
- A "low-low" alarm alerts the operator to take immediate action to restore margin to the M bank or AO bank insertion limits. Interlocks will terminate automatic AO bank withdrawal (to prevent further insertion of the M banks) or insertion (to avoid the AO bank insertion limits).

The purpose of the control bank rod insertion alarms and interlocks is to provide warning to the operator of excessive rod insertion and to terminate the insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip. It also provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection. Insertion limits provide confidence 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 are decreased (the rods must be withdrawn further) with increasing power. The insertion limits for the M banks and the AO bank are calculated from the reactor power, as measured by the ΔT power monitor, according to the following equations:

$$Z_{LL}^{M} = A + B \cdot \Delta T + C \cdot Z_{AO} + D \cdot \Delta T \cdot Z_{AO}$$

$$Z_{LL}^{AO} = E$$

where:

Z_{LL}^{M}	=	Maximum permissible insertion limit for the affected M control bank
Z_{LL}^{AO}	=	Maximum permissible insertion limit for the affected AO control bank
Z_{AO}	=	Current AO bank position
ΔT	=	Median value of the ΔT measurements
A,B,C,D,E	=	Constants chosen to maintain Z_{LL} ≥ the actual limit based on physics calculations

The control rod bank demand position (Z) for the M banks and the AO bank is compared to the respective Z_{LL} as follows:

- If $Z - Z_{LL} \leq F$, a low alarm is actuated.
- If $Z - Z_{LL} \leq G$, a low-low alarm and interlock is actuated.

Since nuclear peaking factors can be aggravated by the opposite movement of the M banks and the AO bank, the interlocks on the AO bank are different, depending on whether the M bank or the AO bank insertion limit setpoint is actuated. If an M bank insertion limit is reached, this stops AO bank withdrawal and reduces the increases in the core peaking factor. If an AO bank insertion limit is reached, this stops AO bank insertion. If the M banks are fully withdrawn, AO bank automatic insertion is blocked.

7.7.1.5 Control 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.

7.7.1.6 Pressurizer Pressure Control System

The primary system pressure is closely regulated during operation to prevent pressure from increasing to the point where an engineered safety features actuation is required to prevent overstressing the pressure boundary; or from decreasing to a condition where engineered safety features actuation is required to prevent the possibility of departure from nucleate boiling. Fine control of pressure to the desired setpoint is accomplished by regulating the power to a bank of heaters located in the pressurizer. Large decreases in pressure are accommodated by turning on additional heater banks and by the inherent flashing from the water mass in the pressurizer, which is at saturation. Large pressure increases are controlled by actuating pressurizer spray to condense steam.

Pressurizer pressure control is designed to provide stable and accurate control of pressure to its predetermined setpoint. Automatic pressure control is available from the point at which nominal pressure is established in the startup cycle to 100-percent power. During steady-state operating conditions, the pressurizer heater output is regulated to compensate for pressurizer heat loss and a small continuous pressurizer spray. During normal transient operation, the pressure is regulated to provide adequate margin to safety systems actuation or reactor trip. The pressurizer pressure control system is designed to minimize equipment duty (such as spray nozzle thermal cycling due to spray actuation) due to load regulation operation.

Small changes in pressure are regulated by modulation of the variable heater control. Reset (integral) action is included to maintain pressure at its setpoint. Decreases in pressure larger than that which can be accommodated by the variable heater control results in the actuation of the backup heaters. The backup heaters are deactivated when the variable heaters alone are capable of restoring pressure. Large increases in the pressurizer water level also result in activation of the backup heaters. The purpose of this action is to avoid the accumulation of subcooled fluid in the pressurizer, thereby allowing flashing of the pressurizer fluid to limit the pressure decrease on any subsequent outsurge.

Pressure increases too fast to be handled by reducing the variable heater output result in spray actuation. Spray continues until pressure decreases to the point that the variable heaters alone can regulate pressure. For normal transients including a full-load rejection, the pressurizer pressure control system acts promptly to prevent reaching the high pressurizer pressure reactor trip setpoint.

7.7.1.7 Pressurizer Water Level Control System

The pressurizer water inventory, or level control, provides a reservoir for the reactor coolant system inventory changes that occur due to changes in reactor coolant system density. As the reactor coolant system temperature is increased from hot zero-load to full-load values, the reactor coolant system fluid expands. The pressurizer level is programmed to absorb this change. A deadband is provided around the nominal pressurizer level program to intermittently control charging and letdown. When the pressurizer water level reaches the lower limit of the deadband, it actuates the charging system. The charging system continues to operate until the level is restored to a limit above the nominal program value. When the pressurizer water level reaches the upper limit of the deadband, it actuates letdown to the liquid waste processing system.

Pressurizer water level control provides stable and accurate control of pressurizer level within a prescribed deadband around the programmed setpoint value, as derived from the plant operating parameters. Automatic level control is supplied from the point in the startup cycle where the hot zero-load level is established through 100-percent power. The nominal water level program is also compensated for changes in operating temperature that occur during load regulation operations.

7.7.1.8 Feedwater Control System

The feedwater control system consists of those controllers and associated hardware whose primary function is to regulate the flow of feedwater into the steam generator. The feedwater control system consists of two separate subsystems. The feedwater control subsystem regulates the flow of feedwater into the steam generators via the main feedwater line. The startup feedwater control subsystem regulates the flow of feedwater into the steam generators via the startup feedwater line. Flow to the startup feedwater line may be supplied by either the main or startup feedwater pump. The following two subsections provide a description of each control subsystem.

7.7.1.8.1 Feedwater Control

The feedwater control subsystem maintains a programmed water level in the shell side of the steam generator during steady-state operation, and limits the water level shrink and swell during normal plant transients. This prevents an undesirable reactor trip actuation. Indication is provided for monitoring system operation. Alarms and indications are provided to alert the plant operator of control system malfunctions or abnormal operating conditions.

Two modes of feedwater control are incorporated in the feedwater control subsystem. In the high-power control mode, the feedwater flow is regulated in response to changes in steam flow and proportional plus integral (PI)-compensated steam generator narrow range water level deviation from setpoint. In the low-power control mode, the feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated steam generator narrow range water level deviation from setpoint.

The transition from the low to the high-power control mode is initiated on the basis of the filtered high range feedwater flow signal. The transition point is set at a feedwater flow corresponding to a power at which reliable steam flow indication is expected. The transition point is also low enough to allow effective feedforward control using wide range water level, and to allow feedwater flow indication within the upper limit of the low range feedwater flow measurement. Tracking is provided to allow a smooth transition between control modes and between manual and automatic control.

A high steam generator water level signal reduces the feedwater flow demand signal and closes the feedwater control valves.

7.7.1.8.2 Startup Feedwater Control

During no-load or very low power conditions, the main feedwater control subsystem is not intended to be used for automatic control of the steam generator water level. The startup feedwater control subsystem performs this function.

The startup feedwater control subsystem maintains a programmed water level in the shell side of the steam generator during low power (below approximately 10 percent of plant rated thermal power), no-load, and plant heatup and cooldown modes. During low feedwater flow demand, feedwater is controlled by the startup feedwater control subsystem. Transition between the main and startup feedwater line is automatically controlled based on flow measurements within the respective lines. The startup feedwater is also automatically actuated on signals which indicate a loss of water inventory or heat sink in the secondary side of the steam generator and will attempt to recover the inventory loss and return the steam generator water level to the programmed value. If the startup feedwater cannot recover the inventory deficit, reactor cooling is initiated by the passive residual heat removal system.

The startup feedwater control subsystem regulates the flow of feedwater in a manner which is similar to the way (main) feedwater is controlled in the low-power control mode. Feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated steam generator narrow range water level deviation from setpoint. Tracking is provided to allow a smooth transition between control modes and between manual and automatic control.

7.7.1.9 Steam Dump Control System

The AP1000 is designed to sustain a 100-percent load rejection, or a turbine trip from 100-percent power, without generating a reactor trip, requiring atmospheric steam relief, or actuating a pressurizer or steam generator safety valve. The automatic steam dump control system, in conjunction with other control systems, is provided to accommodate this abnormal load rejection and to reduce the effects of the transient imposed on the reactor coolant system. By bypassing main steam to the condenser, an artificial load is maintained on the primary system. This artificial load makes up the difference between the reactor power and the turbine load for load rejections and turbine trips. It also removes latent and decay heat following a reactor trip.

The steam dump system is sized to pass 40 percent of nominal steam flow. This capacity, in conjunction with the performance of the reactor power control system, is sufficient to handle reactor trips from any power level, turbine trips from 50-percent power or less, and load rejections equivalent to a step load decrease of 50 percent or less of rated load. For turbine trips initiated above 50-percent power, or load rejections greater than the equivalent of a 50-percent step, the steam dump operates in conjunction with the rapid power reduction system described in Subsection 7.7.1.10 to meet the performance described in the previous paragraph.

The steam dump control system has two main modes of operation:

- The T_{avg} mode uses the difference between measured auctioneered loop T_{avg} and a reference temperature derived from turbine first-stage impulse pressure, to generate a steam dump demand signal. This mode is largely used for at-power transients requiring steam dump, such as load rejections and turbine trips (where the load rejection T_{avg} mode is used) and reactor trips (where the plant trip T_{avg} mode is used). The load rejection controller is discussed in Subsection 7.7.1.9.1. The plant trip controller is discussed in Subsection 7.7.1.9.2.

- The pressure mode uses the difference between measured steam header pressure and a pressure setpoint to generate a steam dump demand signal. This mode is used for low-power conditions (up through turbine synchronization) and for plant cooldown. It is described in Subsection 7.7.1.9.3.

Process variable input signals to the steam dump control system are fed from protection channels via isolation devices and the signal selector function. Each input (T_{avg}, turbine load, steam header pressure, and wide-range steam generator water level) is obtained from multiple transmitters of the same parameter. The signal selector rejects any signal which is bad in comparison with the remaining transmitter outputs and allows only valid measurements to be used by the control system. This makes the steam dump system tolerant of single transmitter failures or input signal failures and eliminates interaction between the control and the protection system.

To prevent actuation of steam dump on small load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure. It unblocks the dump valves when the rate of a load rejection exceeds a preset value corresponding to a 10-percent step load decrease or a sustained ramp load decrease of greater than 5 percent per minute.

The steam dump system valves also receive a signal to close on a low wide-range steam generator water level signal. Isolating steam dump on low wide-range water level improves the plant performance to anticipated transients without reactor scram events modeled in the AP1000 Probabilistic Risk Assessment.

7.7.1.9.1 Load Rejection Steam Dump Controller

This controller 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 selected T_{avg} and the selected reference T_{avg} (designated T_{ref}), based on turbine impulse chamber pressure.

The T_{avg} input signals are the same as those used in the reactor power control system, although a signal selector algorithm in a separate controller is employed. The lead-lag compensation for the T_{avg} signal compensates for lags in the plant thermal response and in valve positioning. The lead-lag compensation in the T_{ref} signal is used to compensate for hangup effects noted in the turbine impulse pressure measurement on turbine trips and grid disconnects. It allows for a decrease in gain in the steam dump controller, thereby increasing stability. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase. This generates an immediate demand signal for steam dump. Following the initial steam dump opening, the reactor power control system in conjunction with the rod control system commands the control rods to insert in a controlled manner to reduce the reactor power to match turbine load. On a load rejection resulting in a turbine runback, the steam dump terminates when the reactor power matches the turbine load and the temperature error is within the maneuvering capability of the control rods. On a turbine trip or grid disconnect, the steam dump modulates closed in response to the control rods reducing nuclear power to approximately 15-percent load. At this point, rod insertion stops and the plant stabilizes in preparation for a turbine/generator restart and/or grid synchronization with the steam dumps partially open.

7.7.1.9.2 Plant Trip Steam Dump Controller

Following a reactor trip, the load rejection steam dump controller is defeated and the plant trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal for steam dump is the error signal between the lead-lag compensated auctioneered T_{avg} and the no-load reference T_{avg}. When the error signal exceeds a predetermined setpoint, the steam dump valves are opened 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. This regulates the rate of removal of decay heat and establishes the equilibrium hot shutdown condition.

7.7.1.9.3 Steam Header Pressure Controller

Decay heat removal between hot standby and residual heat removal system cut-in conditions is maintained by the steam header pressure controller. This controller uses the difference between steam header pressure and a pressure setpoint to control the steam flow to the condensers. Reset action is used to eliminate steady-state error. This controller uses the same steam dump valves as the load rejection and plant trip controllers described in Subsections 7.7.1.9.1 and 7.7.1.9.2. The steam header pressure control mode is manually selected by the operator. The pressure setpoint is manually adjusted by the operator based on the desired reactor coolant system temperature. In addition, the controller has a feature that allows automatically controlled plant cooldowns at a chosen rate (within limits). The operator can enter the desired cooldown rate and the desired target reactor coolant system temperature. The control system then dumps the required steam to achieve the setpoint cooldown rate and stops at the target setpoint.

7.7.1.10 Rapid Power Reduction System

The rapid power reduction system rapidly reduces the nuclear power to a level capable of being handled by the steam dump system for a large load rejection (greater than 50-percent power reduction at a rapid rate). Upon the detection of a large and rapid turbine power reduction (via a rate/lag circuit, similar to that used for steam dump control), the circuit provides a signal demanding the release of a preselected number of control rods. The dropping of these preselected rods causes the reactor power to rapidly reduce to approximately 50-percent power.

The large load rejection also actuates the steam dump system and the reactor power control system via a primary-to-secondary power mismatch signal. Following the initiation of the load rejection, the power control rods insert in a controlled manner due to the mismatch between the programmed reference average coolant temperature (based on turbine impulse chamber pressure) and the compensated average coolant temperature measured in the reactor coolant loops. In a similar manner, the load rejection steam dump controller controls the steam dump valves to prevent a large increase in reactor coolant temperature. Following the release of the preselected control rods, the power control system continues to insert the remaining control group control rods to reduce power (by temperature control channel trying to match T_{avg} to T_{ref}). Following the initial opening, the steam dump valves modulate closed based upon the (T_{avg} - T_{ref}) signal.

Controlled rod insertion and steam dump modulation continue until power is reduced to approximately 15-percent power. At this time, the rod motion ceases and the plant stabilizes with steam dump maintained to match the steam flow to the thermal load. The operators can then switch to pressure mode of control on the steam dump control system, recover the released control rods, and establish normal rod control. A normal power escalation is then performed through the following actions: resynchronize the turbine/generator, if necessary, perform turbine loading until the steam dumps close, reset the steam dump controller, place the plant back into automatic, and return to the desired power level.

7.7.1.10.1 Rod Block Interlock

To avoid the potential for a withdrawal of the normally functioning power control rods following the rod release by the rapid power reduction system, a rod withdrawal block is actuated. Actuation occurs by the reduction of reactor power (P-17) after the initiation of the rapid power reduction system as discussed in Subsection 7.2.1.1.11. The rod withdrawal block does not adversely impact the performance of the rapid power reduction system. The demand of the power control subsystem is a continuous rod insertion. Rod withdrawal during the power reduction phase is not required.

7.7.1.10.2 Rapid Power Reduction Rod Selection

The number of rods needed to obtain this power reduction is dependent on the core burnup during the fuel cycle. In addition, if a large load rejection (grid disconnect) is initiated at a part-power condition (50-percent to 100-percent power), then a reduced number of control rods need to be released. Therefore, a means is provided to alter which rods will be released by the rapid power reduction system. Following operator concurrence, suggested changes are implemented in the rod control logic cabinet.

The selection of the rods that are released during the rapid power reduction is based on a thermal power measurement. The thermal power is integrated over time to arrive at a core burnup. Depending on the core burnup and the plant power level, the choice of the control rods to be released by the rapid power reduction system is determined. Capability is provided for the operator to correct the integrated burnup periodically based upon a more detailed burnup calculation.

7.7.1.11 Diverse Actuation System

The diverse actuation system is a nonsafety-related system that provides a diverse backup to the protection system. This backup is included to support the aggressive AP1000 risk goals by reducing the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control systems.

The protection and safety monitoring system is designed to prevent common mode failures. However, in the low probability case where a common mode failure does occur, the diverse actuation system provides diverse protection. The specific functions performed by the diverse actuation system are selected based on the PRA evaluation. The diverse actuation system functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with the event probability.

The functional logic for the diverse actuation system is shown in Figure 7.2-1, sheets 20 and 21.

The DAS is developed using a planned design process, which provides for specific design documentation during the following life cycle stages:

- Design Requirements Phase
- System Definition Phase

These life cycle stages are completed by developing a number of specific design documents. The following documents are developed to address the Design Requirements and System Definition Phases:

- WCAP-17184-P, “AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report,” including Appendix A, “DAS Setpoint Methodology Description,” and Appendix B, “PRA Performance Requirements Associated with DAS Manual Actuation.”

  The DAS Technical Report identifies the DAS architecture and associated licensing basis at the functional design level. The overall DAS detailed design is not identified in the report. Select design details are identified only for the purpose of architectural completeness or licensing compliance. The content of this report is to cover SRP 7.8. Appendix A of the Technical Report describes the DAS setpoint methodology and provides a representative basis for DAS nominal trip setpoints. Appendix B addresses operator actions taken through DAS that are modeled in the “AP1000 Probabilistic Risk Assessment” (PRA). These manual actions are not required to mitigate design basis accidents but instead are modeled in the PRA to provide insights into

sequences that involve multiple failures. This appendix lists the operator actions used in the PRA for manual DAS actions from the control room DAS actuation panel.

- WCAP-15775, “AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report”

  Diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithms, or using different actuation means to provide different ways of responding to postulated plant conditions. NUREG/CR-6303 segregates the types of diversity into six different areas: human, design, software, functional, signal, and equipment. The “AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report” describes the type of diversity that exists among the four echelons of defense for AP1000 and identifies dependencies among the echelons.

A number of additional design process documents are submitted to the U.S. NRC for review and audit. They include the following:

1. “AP1000 Diverse Actuation System Logic Drawings”

2. “AP1000 Diverse Actuation System Sub-System Requirements”

3. “DAS Requirements Traceability Report”

Automatic Actuation Function

The automatic actuation signals provided by the diverse actuation system are generated in a functionally diverse manner from the protection system actuation signals. The common-mode failure of sensors of a similar design is also considered in the selection of these functions.

The automatic actuation function is accomplished by redundant logic subsystems. Input signals are received from the sensors by an input signal conditioning block, which consists of one or more electronic modules. This block converts the signals to standardized levels, provides a barrier against electromagnetic and radio frequency interference, and presents the resulting signal to the input signal conversion block. The conversion block continuously performs analog to digital signal conversions and stores the value for use by the signal processing block.

The signal processing block polls the various input signals, evaluates the input signals against stored setpoints, executes the logic when thresholds are exceeded, and issues actuation commands.

The resulting output signals are passed to the output signal conversion block, whose function is to convert logic states to parallel, low-level dc signals. These signals are passed to the output signal conditioning block. This block provides high-level signals capable of switching the traditional power plant loads, such as breakers and motor controls. It also provides a barrier against electromagnetic and radio frequency interference.

The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals. Diversity between DAS and PMS is achieved by the use of different architectures, different hardware implementations, and different software, if any.

Software diversity between the DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system, and executable software/logic.

The diverse automatic actuations are:

- Trip rods via the motor generator set, trip turbine, initiate the passive residual heat removal, actuate core makeup tanks, and trip the reactor coolant pumps on low wide-range steam generator water level

- Trip rods via the motor generator set, trip turbine, open the passive heat removal discharge isolation valves, and close the in-containment refueling water storage tank gutter isolation valves on high hot leg temperature

- Trip rods via the motor generator set, trip turbine, actuate the core makeup tanks, and trip the reactor coolant pumps on low pressurizer water level

- Isolate selected containment penetrations and start passive containment cooling water flow on high containment temperature

The selection of setpoints and time responses determine that the automatic functions do not actuate unless the protection and safety monitoring system has failed to actuate to control plant conditions. Capability is provided for testing and calibrating the channels of the diverse actuation system.

Manual Actuation Function

[*The manual actuation function of the diverse actuation system is implemented by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the protection and safety monitoring system cabinets, and the diverse actuation system automatic logic.*]*

The diverse manual functions are:

- Reactor and turbine trip

- Passive containment cooling actuation

- Core makeup tank actuation and reactor coolant pump trip

- Open stage 1 automatic depressurization system valves

- Open stage 2 automatic depressurization system valves

- Open stage 3 automatic depressurization system valves

- Open stage 4 automatic depressurization system valves

- Open the passive residual heat removal discharge isolation valves and close the in-containment refueling water storage tank gutter isolation valves

- Selected containment penetration isolation

- Containment hydrogen igniter actuation

- Initiate in-containment refueling water storage tank injection

- Initiate containment recirculation

- Initiate in-containment refueling water storage tank drain to containment

*NRC Staff approval is required prior to implementing a change in this information.

In addition to the above functions, a redundant method of actuating the following components is provided at the DAS squib valve control cabinet:

- Open stage 4 automatic depressurization system valves
- Initiate in-containment refueling water storage tank injection
- Initiate containment recirculation
- Initiate in-containment refueling water storage tank drain to containment

Actuation Logic Function

There are two actuation logic modes, automatic and manual. The automatic actuation logic mode functions to logically combine the automatic signals from the two redundant automatic subsystems in a two-out-of-two basis. The combined signal operates a power switch with an output drive capability that is compatible, in voltage and current capacity, with the requirements of the final actuation devices. The two-out-of-two logic is implemented by connecting the outputs in series. The manual actuation mode operates in parallel to independently actuate the final devices.

Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual, two out of two redundancy reduces the probability of inadvertent actuation.

The diverse actuation system is designed so that, once actuated, each mitigation action goes to completion. Any subsequent return to operation requires deliberate operator action.

Indication

To support the diverse manual actuations, sensor outputs are displayed in the main control room in a manner that is diverse from the protection system display functions. The instrument sensor output displayed in the main control room is repeated at the DAS instrumentation cabinet. The indications that are provided from at least two sensors per function are:

- Steam generator water level – for reactor trip and passive residual heat removal actuations, and for overfill prevention by manual actuation of the automatic depressurization system valves
- Hot leg temperature – for passive residual heat removal actuation and reactor trip
- Core exit temperature – for automatic depressurization system actuation and subsequent initiation of in-containment refueling water storage tank injection and also containment hydrogen igniter actuation
- Pressurizer level – for core makeup tank actuation and reactor coolant pump trip
- Containment temperature – for containment isolation and passive containment cooling system actuation
- Rod control motor generator voltage – for confirmation of reactor trip

Isolation

The diverse actuation system uses sensors that are separate from those being used by the protection and safety monitoring system and the plant control system. This prohibits failures from propagating to the other plant systems through the use of shared sensors.

There is signal isolation between the two subsystems within the diverse actuation system, one for each input and output path. These isolators are characterized by a high common mode voltage withstand capability to provide the necessary isolation against faults. The configuration is set up such that the isolation devices are capable of protecting against fault propagation between the diverse actuation system subsystems.

Actuation interfaces are shared between the diverse actuation system and the protection and safety monitoring system. The diverse actuation system actuation devices are isolated from the protection and safety monitoring system actuation devices, so as to avoid adverse interactions between the two systems. The actuation devices of each system are capable of independent operation that is not affected by the operation of the other. The diverse actuation system is designed to actuate components only in a manner that initiates the safety function. This type of interface also prevents the failure of an actuation device in one system from propagating a failure into the other system.

The diverse actuation system and the protection and safety monitoring system use independent and separate uninterruptible power supplies.

Operability, Availability, and Testing

The diverse actuation system is designed to provide protection under all plant operating conditions in which the reactor vessel head is in place and non-Class 1E UPS power is available. The automatic actuation processors, in each of the two redundant automatic subsystems of the diverse actuation system, are provided with the capability for channel calibration and testing while the plant is operating. To prevent inadvertent DAS actuations during online calibration, testing activities or maintenance, the normal activation function is bypassed. Testing of the diverse actuation system is performed on a periodic basis.

Equipment Qualification and Quality Standards

The diverse actuation system is located in a controlled environment, but is capable of functioning during and after normal and abnormal events and conditions that include:

- Wide temperature range of 40° to 120°F
- Noncondensing relative humidity up to 95 percent
- Radio frequency and electromagnetic interference

The diverse actuation system processor cabinets are located in the portion of the Annex Building that is a Seismic Category II structure. The diverse actuation system equipment, including actuated devices, is designed and tested in accordance with industry standards. The adequacy of the hardware and software (if any) is demonstrated through a diverse form of the verification and validation program discussed in Subsection 7.1.2.14. This program provides for the use of commercial off-the-shelf hardware and software. As the diverse actuation system performs many of the protection functions associated within the ATWS systems used in existing plants, the diverse actuation system is designed to meet the quality guidelines established by Generic Letter 85-06, "Quality Assurance Guidelines for ATWS Equipment that is not Safety-Related."

7.7.1.12 Signal Selector Algorithm

The plant control system for the AP1000 derives some of its control inputs from signals that are also used in the protection and safety monitoring system. The advantages of this design are:

- The nonsafety-related plant systems are controlled from the same measurements which provide protection. This permits the control system to function in a manner which maintains margin between operating conditions and safety limits, and reduces the likelihood of spurious trips.

- Reducing the number of redundant measurements for any single process variable reduces the overall plant complexity at critical pressure boundary penetrations. This leads to a reduction in separation requirements within the containment, as well as to a decrease in plant cost and maintenance requirements.

To obtain these advantages, measures are taken to provide the independence of the protection and control systems. The criteria for these measures are contained in IEEE 603-1991, Section 5.6.3. Isolation devices are provided to guard the protection system against possible electrical faults in the control system.

To avoid a single component failure or spurious signal causing an inadvertent plant trip while a channel is in test or maintenance, the protection and safety monitoring system uses the bypass logic discussed in Subsection 7.1.2.9. This necessitates a different mechanism for achieving the functional independence of control and protection.

Functional independence of control and protection is obtained by signal selector algorithms. The purpose of the signal selector algorithm is to prevent a failed signal, caused by the failure of a protection channel, from initiating a control action that could lead to a plant condition requiring that protective action. The signal selector function provides this capability by comparing the redundant signals and automatically eliminating an aberrant signal from use in the control system. This capability exists for bypassed sensors or for sensors whose signals have diverged from the expected error tolerance.

The operation of the signal selector algorithm is described in Subsection 7.1.3.2.

7.7.2 Analysis

The control system is capable of maneuvering the plant through certain reference transients. This maneuvering is done without the need for manual intervention and without violating plant protection or component limits. The plant control systems provide high reliability during these anticipated operational occurrences and meet the following objectives:

- The capability to accept 10-percent step load decreases from an initial power level between 100-percent and 25-percent of full power, and step load increase of 10-percent from an initial power level between 15-percent and 90-percent of full power without reactor trip or steam dump actuation.

- The capability to accept ramp load changes at 5-percent power per minute while operating in the range of 15-percent to 100-percent of full power without reactor trip or steam dump system actuation, subject to core power distribution limits.

- The capability to accept the design full-load rejection without reactor trip.

- The capability to accept a turbine trip from full-power operation without reactor trip. This capability is provided with the normally available systems (such as steam dump and feedwater control).

- The capability to follow the design basis network load follow pattern for 90-percent of the fuel cycle. The design basis load follow pattern is defined as the daily (24-hour period) cycle consisting of 10 to 18 hours of operation at 100-percent power, followed by a 2-hour linear ramp to 50-percent power, followed by 2 to 10 hours of operation at 50-percent power and then a 2-hour linear ramp back to 100-percent power.

- The capability to satisfy a 20-percent power increase or decrease within 10 minutes.

- The capability of handling grid frequency changes equivalent to 10-percent peak-to-peak power changes at a two percent per minute rate. This capability is provided over a 15- to 100-percent power range throughout the plant operating life. A total of 35 peak-to-peak swings per day are allowed.

The control system permits maneuvering the plant through the transients without actuation of the following:

- Steam generator safety valves

- Steam generator power operated relief valves

- Pressurizer safety valves

In addition, these valves are not actuated during a normal plant trip.

7.7.3 Combined License Information

This section contained no requirement for information.

Table 7.7-1
Rod Control System Interlocks - Power Control Subsystem

Designation	Derivation	Function
C-1	2/4 neutron flux (intermediate range) above setpoint	Blocks automatic and manual control rod withdrawal
C-2	2/4 neutron flux (power range) above setpoint	Blocks automatic and manual control rod withdrawal
C-3	Margin to overtemperature ΔT (output of signal selector) below setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
C-4	Margin to overpower ΔT (output of signal selector) below setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
C-5	Turbine impulse chamber pressure (output of signal selector) below setpoint (blocked if in low-power rod control mode)	Blocks automatic control rod withdrawal
		Defeats remote load dispatching (if remote load dispatching is used)
C-11	1/1M bank control rod position above setpoint	Blocks automatic rod withdrawal
C-16	Reactor coolant system T_{avg} or (T_{avg} minus T_{ref}) signal (output of signal selector) below setpoint	Stops automatic turbine loading until condition clears
P-17	2/4 negative flux rate below setpoint	Blocks automatic rod withdrawal

Table 7.7-2
Rod Control System Interlocks – Axial Offset Control Subsystem

Designation	Derivation	Function
C-1	2/4 neutron flux (intermediate range) above setpoint	Blocks automatic and manual axial offset control rod withdrawal
C-2	2/4 neutron flux (power range) above setpoint	Blocks automatic and manual axial offset control rod withdrawal
C-5	Turbine impulse chamber pressure (output of signal selector) below setpoint	Blocks automatic axial offset control rod withdrawal and insertion
C-15	1/1 bank AO control rod position below setpoint	Blocks automatic axial offset control rod insertion
C-17	1/1M bank control rod position below setpoint	Blocks automatic axial offset control rod withdrawal
C-18	1/1M bank control rod position above setpoint	Blocks automatic axial offset control rod insertion
---	Power control rods moving in	Blocks automatic axial offset control rod insertion and withdrawal
---	Power control rods moving out	Blocks automatic axial offset control rod insertion and withdrawal
---	Power control rods in manual	Blocks automatic axial offset control rod insertion and withdrawal
P-17	2/4 negative flux rate below setpoint	Blocks automatic axial offset control rod withdrawal

Table 7.7-3 (Sheet 1 of 3)
Cross Reference Table for Defense-in-Depth Functions
Supported by the Plant Control System

Supported System	Defense-in-Depth Function	DCD Section	DCD Figure
Component Cooling Water (CCS)	Provides cooling for normal residual heat removal system heat exchangers and pumps when the reactor coolant system pressure and temperature are below 450 psig and 350°F.	9.2.2.1.2.2 9.2.2.4.3	9.2.2-2
Component Cooling Water (CCS)	Provides cooling for the miniflow heat exchangers of the chemical and volume control system makeup pumps.	9.3.6.3.1	9.2.2-2
Component Cooling Water (CCS)	Provides cooling for the spent fuel pool heat exchangers for heat removal from the spent fuel pool.	9.2.2.1.2.3	9.2.2-2
Chemical and Volume Control (CVS)	Supply makeup and boration to the reactor coolant system.	9.3.6.7	9.3.6-1
Chemical and Volume Control (CVS)	Supply coolant to the pressurizer auxiliary spray line.	9.3.6.4.5	9.3.6-1
Standby Diesel Fuel Oil (DOS)	Supply fuel to the onsite standby power diesel generators.	9.5.4	9.5.4-1
Main and Startup Feedwater (FWS)	Provide startup feedwater for heat removal from the reactor coolant system (startup feedwater).	10.4.9.1.2	10.4.7-1 10.3.2-1
Normal Residual Heat Removal (RNS)	Remove heat from the reactor coolant system during shutdown operation at reduced pressure and temperature.	5.4.7.1.2.1	5.4-7
Normal Residual Heat Removal (RNS)	Provide low temperature overpressure protection for the reactor coolant system.	5.4.7.1.2.5	5.4-7
Normal Residual Heat Removal (RNS)	Provide low-pressure makeup to the reactor coolant system and remove heat from the reactor coolant system following actuation of the automatic depressurization system.	5.4.7.1.2.4 5.4.7.4.4	5.4-7

Table 7.7-3 (Sheet 2 of 3)
Cross Reference Table for Defense-in-Depth Functions
Supported by the Plant Control System

Supported System	Defense-in-Depth Function	DCD Section	DCD Figure
Spent Fuel Pool Cooling (SFS)	Provide for heat removal from the spent fuel stored in the spent fuel pool by pumping the water from the pool through a heat exchanger, and then returning the water to the pool.	9.1.3.2	9.1-8
Steam Generator (SGS)	Provide decay heat removal capability during shutdown operations by delivery of startup feedwater flow to the steam generator and venting of steam from the steam generators to the atmosphere via the power-operated relief valves.	10.4.9 10.3	10.4.7-1 10.3.2-1
Service Water (SWS)	Provide the capability for removing heat from the component cooling water system.	9.2.1.1.2	9.2.1-1
Service Water (SWS)	Provide the capability for removing heat from the spent fuel pool via the spent fuel cooling and component cooling water systems.	9.2.2 and Table 9.2.2-2	9.2.2-1 9.2.2-2
Service Water (SWS)	Provide the capability for decay heat removal at shutdown conditions through the normal residual heat removal and component cooling systems.	9.2.2 and Table 9.2.2-2	9.2.2-1 9.2.2-2
Nuclear Island Nonradioactive Ventilation (VBS)	Provide ventilation and cooling to the main control room envelope, Class 1E instrumentation and control rooms, Class 1E dc equipment rooms, and Class 1E battery rooms.	9.4.1	9.4.1-1 all sheets
Containment Hydrogen Control (VLS)	Provide hydrogen igniters to control hydrogen concentration in excess of the recombiner capability.	6.2.4	N/A
Central Chilled Water (VWS)	Provide chilled water to support the nuclear island nonradioactive ventilation system cooling of the main control room envelope, Class 1E instrumentation and control rooms, Class 1E dc equipment rooms, and the Class 1E battery rooms.	9.2.7	9.2.7-1 sheets 6 & 7
Central Chilled Water (VWS)	Provide chilled water to support the cooling functions of the compartment unit coolers for the normal residual heat removal system pump.	9.2.7	9.2.7-1 sheets 6 & 7

Table 7.7-3 (Sheet 3 of 3)
Cross Reference Table for Defense-in-Depth Functions
Supported by the Plant Control System

Supported System	Defense-in-Depth Function	DCD Section	DCD Figure
Central Chilled Water (VWS)	Provide chilled water to support the cooling functions of the compartment unit coolers for the chemical and volume control system makeup pump.	9.2.7	9.2.7-1 sheets 6 & 7
Annex/Auxiliary Building Nonradioactive Heating and Ventilation (VXS)	Provide ventilation of the electrical switchgear rooms that contain the diesel bus switchgear. Provide ventilation of the equipment room that contains the switchgear room air-handling units.	9.4.2	9.4.2-1 sheets 3, 4, 5, and 6
Diesel Generator Building Heating and Ventilation (VZS)	Provide ventilation and cooling of the diesel generator building, and ventilation and heating of the diesel oil transfer module enclosure to support operation of the onsite standby power system.	9.4.10	9.4.10-1
Onsite Standby Power (ZOS)	Supply ac power to the Class 1E dc and UPS system.	8.3 and Table 8.3.1-2	8.3.1-2
Onsite Standby Power (ZOS)	Supply ac power to selected electrical components of the plant defense-in-depth, nonsafety-related systems.	8.3 and Table 8.3.1-2	8.3.1-2

APPENDIX 7A INSTRUMENTATION AND CONTROLS LICENSING BASIS DOCUMENT CHANGES

Note: Revised text within the licensing basis documents is identified in this appendix with strikethrough font for deleted text, underlined font for new text, and three asterisks (* * *) where text is omitted for clarity.

7A.1 WCAP-15775, AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report

The UFSAR incorporates by reference Tier 2 document WCAP-15775, AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report. See Table 1.6-1. WCAP-15775, Revision 4, includes the following revisions and additions as indicated by strikethroughs and underlines.

- Revise the LIST OF ACRONYMS AND ABBREVIATIONS as follows:

* * *

ALS	Advanced Logic System

* * *

CIM	Component Interface Module

* * *

FPGA	Field Programmable Gate Array

- Revise Section 4.2, Determining Diversity – Guideline 2, under diversity aspect number 4, Human Diversity, as follows:

The design, verification, and validation programs for instrumentation and control systems, as described in described in WCAP-13383 (Reference 3) and CE-CES-195 (Reference 4), require and specify the use of independent review. ~~It is a requirement of the DAS that different people will be responsible for its design and fabrication, including verification and validation.~~ At the system level, different design and IV&V teams are used on the DAS and PMS systems.

The AP1000 Component Interface Module (CIM), provides the priority logic between PMS and plant control for component control. The AP1000 CIM Technical Report (Reference 9), identifies how diversity is maintained between the ALS-based DAS and the CIM.

The functionality of the CIM and DAS are different, and this reduces the chances that a common cause failure can be made in both designs. The FPGA Logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM, for the following lifecycle activities:

- Design Activities (i.e., different FPGA logic design teams for activities such as the preparation of design specifications and development of the application logic in the hardware descriptive language)
- Implementation Activities (i.e., different FPGA logic design teams for activities required to physically program the FPGA chip such as simulation, synthesis and “place and route” tasks)

- Black Box Test Activities (i.e., different IV&V test teams).

  Black Box Testing is the testing of a component or system in the target hardware without reference to the internal structure of the component or system. Testing focuses solely on the outputs generated in response to selected inputs and execution conditions.

- Revise Section 6, References, by adding Reference 9, as follows:

  9. WCAP-17179, Revision 2 (as modified by changes provided in Appendix 7A), "AP1000 Component Interface Module Technical Report"

7A.2 [*WCAP-17179-P and WCAP-17179-NP, AP1000™ Component Interface Module Technical Report*

The UFSAR incorporates by reference Tier 2 document WCAP-17179-P and WCAP-17179-NP, AP1000™ Component Interface Module Technical Report. See Table 1.6-1. WCAP-17179-P and WCAP-17179-NP, Revision 2, include the following revisions and additions as indicated by strikethroughs and underlines.*

- *Revise the DEFINITIONS as follows:*

Black Box Testing	*The testing of a component or system in the target hardware without reference to the internal structure of the component or system. Testing focuses solely on the outputs generated in response to selected inputs and execution conditions.*

- *Revise the REFERENCES as follows:*

  13. WCAP-15775, Revision ~~-~~4 (as modified by changes provided in Appendix 7A), "AP1000 Instrumentation and Control Defense-In-Depth and Diversity Report," Westinghouse Electric Company LLC.

  22. WCAP-17184-P (Proprietary), Revision ~~-1~~ 2 (as modified by changes provided in Appendix 7A), "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report," Westinghouse Electric Company LLC.

- *Revise Section 2.9.4, Human Diversity, as follows:*

  The purpose of human diversity is to reduce the chance of common errors in similar designs. [The functionality of the CIM and DAS are not similar, and this reduces the chances that a common error can be made in both designs. ~~For any functionality that is similar between the two designs, different designers were used for the CIM and DAS designs. In addition the different design teams and different test teams will be used to test the CIM and DAS designs.~~]~~[a,c]~~ The FPGA Logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM, for the following lifecycle activities:

  - *Design Activities (i.e., different FPGA logic design teams for activities such as the preparation of design specifications and development of the application logic in the hardware descriptive language)*

*NRC Staff approval is required prior to implementing a change in this information.

- *Implementation Activities (i.e., different FPGA logic design teams for activities required to physically program the FPGA chip such as simulation, synthesis and "place and route" tasks)*

- *Black Box Test Activities (i.e., different IV&V test teams).*]*

7A.3 WCAP-17184-P, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report

The UFSAR incorporates by reference Tier 2 document WCAP-17184-P, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report. See Table 1.6-1. WCAP-17184-P, Revision 2, includes the following revisions and additions as indicated by strikethroughs and underlines.

- Revise the DEFINITIONS section as follows:

  Black Box Testing

  The testing of a component or system in the target hardware without reference to the internal structure of the component or system. Testing focuses solely on the outputs generated in response to selected inputs and execution conditions.

- Revise the REFERENCES section as follows:

  20. APP-GW-GLR-143 (Proprietary), Revision ~~0~~ 2 (as modified by changes provided in UFSAR Appendix 7A), "AP1000 Component Interface Module Technical Report," Westinghouse Electric Company LLC.

- Revise Section 9.4, HUMAN DIVERSITY as follows:

  The design, verification, and validation programs for I&C systems, ~~[~~as described in WNA-PN-00056-WAPP, "NuStart/DOE Design Finalization Diverse Actuation System Project Plan" (Reference 14)~~]~~[a,c] and the DAS Design Process (Reference 15), require and specify the use of independent review. At the system level, different design and IV&V teams are used on the DAS and PMS systems. ~~It is a requirement of the DAS that different people (personnel not assigned to safety system engineering) will be responsible for its design and fabrication.~~

  ~~[~~The AP1000 Component Interface Module (CIM)~~, which~~ provides the priority logic between PMS and plant control for component control~~, is also provided by CS Innovations~~. The AP1000 CIM Technical Report (Reference 20), identifies how diversity is maintained between the ALS-based DAS and the CIM.~~]~~[a,c]

  The functionality of the CIM and DAS are different, and this reduces the chances that a common cause failure can be made in both designs. The FPGA Logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM, for the following lifecycle activities:

  - Design Activities (i.e., different FPGA logic design teams for activities such as the preparation of design specifications and development of the application logic in the hardware descriptive language)

*NRC Staff approval is required prior to implementing a change in this information.

- Implementation Activities (i.e., different FPGA logic design teams for activities required to physically program the FPGA chip such as simulation, synthesis and "place and route" tasks)

- Black Box Test Activities (i.e., different IV&V test teams)

7A.4 WCAP-16438-P and WCAP-16438-NP, FMEA of AP1000™ Protection and Safety Monitoring System

The UFSAR incorporates by reference Tier 2 document WCAP-16438-P and WCAP-16438-NP, FMEA of AP1000™ Protection and Safety Monitoring System. See Table 1.6-1. WCAP-16438-P and WCAP-16438-NP, Revision 3, include the following revisions and additions as indicated by strikethroughs and underlines.

- Revise the REFERENCES section as follows:

  6. WCAP-15775, Revision 4 (as modified by changes provided in UFSAR Appendix 7A), "AP1000™ Instrumentation and Control Defense-In-Depth and Diversity Report," Westinghouse Electric Company LLC.