

TABLE OF CONTENTS

8.0	INSTRUMENTATION AND CONTROL SYSTEMS	8-1
8.1	Introduction	8-1
8.2	AP1000 Instrumentation and Control Overview	8-3
8.3	Reactor Trips	8-6
8.3.1	Introduction	8-6
8.3.1.1	Sensors.....	8-7
8.3.1.2	Reactor Trip Switchgear.....	8-8
8.3.2	Reactor Trip Descriptions.....	8-8
8.3.2.1	Nuclear Startup Trips	8-9
8.3.2.2	Nuclear Overpower Trips	8-10
8.3.2.3	Core Heat Removal Trips.....	8-10
8.3.2.4	Primary Overpressure Trips	8-12
8.3.2.5	Loss of Heat Sink Trip.....	8-12
8.3.2.6	Feedwater Isolation Trip.....	8-12
8.3.2.7	Automatic Depressurization System Actuation Trip	8-13
8.3.2.8	Core Makeup Tank Injection Trip	8-13
8.3.2.9	Reactor Trip on Passive Residual Heat Removal Actuation	8-13
8.3.2.10	Reactor Trip on Safeguards Actuation	8-13
8.3.2.11	Manual Trip	8-14
8.3.3	Reactor Trip System Interlocks	8-14
8.3.4	Bypasses of Reactor Trip Functions	8-15
8.4	Engineered Safety Features Actuation System	8-15
8.4.1	Introduction	8-15
8.4.2	Engineered Safety Features Actuation Descriptions.....	8-16
8.4.2.1	Safeguards Actuation (S) Signal	8-17
8.4.2.2	Containment Isolation	8-18
8.4.2.3	In-Containment Refueling Water Storage Tank Injection	8-18
8.4.2.4	Core Makeup Tank Injection	8-19
8.4.2.5	Automatic Depressurization System Actuation	8-19
8.4.2.6	Reactor Coolant Pump Trip.....	8-21
8.4.2.7	Main Feedwater Isolation	8-22
8.4.2.8	Passive Residual Heat Removal Heat Exchanger Alignment	8-23
8.4.2.9	Turbine Trip.....	8-24
8.4.2.10	Containment Recirculation.....	8-24
8.4.2.11	Steam Line Isolation	8-25
8.4.2.12	Steam Generator Blowdown System Isolation.....	8-26
8.4.2.13	Passive Containment Cooling Actuation	8-26
8.4.2.14	Startup Feedwater Isolation	8-27
8.4.2.15	Boron Dilution Block.....	8-27

8.4.2.16	Chemical and Volume Control System Isolation.....	8-28
8.4.2.17	Steam Dump Block.....	8-29
8.4.2.18	Main Control Room Isolation and Air Supply Initiation.....	8-29
8.4.2.19	Auxiliary Spray and Letdown Purification Line Isolation	8-30
8.4.2.20	Containment Air Filtration System Isolation.....	8-30
8.4.2.21	Normal Residual Heat Removal System Isolation	8-31
8.4.2.22	Refueling Cavity Isolation	8-31
8.4.2.23	Chemical and Volume Control System Letdown Isolation	8-31
8.4.2.24	Pressurizer Heater Block.....	8-31
8.4.2.25	Steam Generator Relief Isolation	8-32
8.4.2.26	Component Cooling Water System Containment Isolation	8-32
8.4.2.27	Containment Vacuum Relief.....	8-32
8.4.3	Blocks, Permissives, and Interlocks for Engineered Safety Features Actuation	8-33
8.4.4	Bypasses of Engineered Safety Features Actuation	8-33
8.5	Control Systems.....	8-33
8.5.1	Introduction.....	8-33
8.5.2	Control System Descriptions	8-34
8.5.3	Reactor Power Control System	8-36
8.5.3.1	Power Control.....	8-37
8.5.3.2	Axial Offset Control	8-38
8.5.4	Rod Control System	8-38
8.5.4.1	Control Rod Position Monitoring.....	8-40
8.5.4.2	Control Rod Insertion Limits	8-40
8.5.4.3	Control Rod Stops	8-41
8.5.5	Pressurizer Pressure Control System	8-41
8.5.6	Pressurizer Water Level Control System.....	8-41
8.5.7	Feedwater Control System.....	8-42
8.5.7.1	Feedwater Control.....	8-42
8.5.7.2	Startup Feedwater Control	8-43
8.5.8	Steam Dump Control System.....	8-43
8.5.8.1	Load Rejection Steam Dump Controller	8-44
8.5.8.2	Plant Trip Steam Dump Controller.....	8-45
8.5.8.3	Steam Header Pressure Controller	8-45
8.5.9	Rapid Power Reduction System.....	8-46
8.5.9.1	Rod Block Interlock	8-46
8.5.9.2	Rapid Power Reduction Rod Selection	8-47

8.5.10	Signal Selector Algorithm.....	8-47
8.6	Diverse Actuation System	8-48

LIST OF TABLES

8-1	Reactor Trip Variables, Limits, Ranges, and Accuracies	8-51
8-2	Reactor Trips	8-54
8-3	Reactor Trip Permissives and Interlocks.....	8-56
8-4	Engineered Safety Features Actuation Signals.....	8-58
8-5	Interlocks For Engineered Safety Features Actuation System	8-67
8-6	Engineered Safety Features Actuation, Variables, Limits, Ranges, and Accuracies (Nominal)	8-71
8-7	Rod Control System Interlocks – Power Control Subsystem	8-73
8-8	Rod Control System Interlocks – Axial Offset Control Subsystem	8-74

LIST OF FIGURES

Instrumentation and Control Architecture	Fig. 8-1
Advant Controller (Common Q)	Fig. 8-2
Protection and Safety Monitoring System.....	Fig. 8-3
Reactor Trip Logic	Fig. 8-4
Reactor Trip Switchgear Configuration.....	Fig. 8-5
Plant Control System.....	Fig. 8-6
Functional Diagram - Reactor Trip Functions	Fig. 8-7
Functional Diagram - Safeguards Actuation	Fig. 8-8
ESF Logic	Fig. 8-9

8.0 INSTRUMENTATION AND CONTROL SYSTEMS

Learning Objectives:

1. State the purposes of the following:
 - a. Protection and Safety Monitoring System,
 - b. Reactor Trip System,
 - c. Engineered Safety Features Actuation System,
 - d. Control Systems, and
 - e. Diverse Actuation System.
2. Describe the major differences between the instrumentation and control systems of the AP1000 design and those of currently operating Westinghouse plants.

8.1 Introduction

The instrumentation and control (I&C) 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 provides descriptions of these systems.

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.

The AP1000 was originally designed to permit the use of either the Westinghouse Eagle protection system hardware or the Common Qualified (Common Q) platform. Common Q was originally developed by ASEA Brown Boveri/Combustion Engineering (ABB/CE), and ABB still owns the rights to the software. The Common Q platform has been chosen by Westinghouse for the AP1000 design; this chapter describes protection system hardware applicable to the Common Q platform.

The Common Q platform is a computer-based system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform is to be loaded with plant-specific application software to implement various nuclear plant safety system applications. The common Q platform is currently in use at operating US nuclear facilities for such applications as digital rod position indication and post-accident monitoring.

The I&C functional requirements of the AP600, the forerunner of the AP1000, which has received Design Certification, have been retained to the maximum extent compatible with the Common Q hardware and software.

For nonsafety-related control systems the AP1000 design incorporates a version of Emerson Electric Company's Ovation expert control and information system designed specifically to automate power generation. The Ovation system controls power generation processes, provides operations and maintenance interfaces, and collects and distributes plant-wide information for process and power generation management.

This chapter also discusses the instrumentation portions of the safety-related systems which function to achieve the system responses assumed in the accident analyses, and those needed to shut down the plant.

Section 8.2 outlines the overall AP1000 instrumentation and control architecture. I&C functions are discussed in more detail in the remaining sections of the chapter: section 8.3 discusses the reactor trip function, section 8.4 addresses the engineered safety feature (ESF) actuation functions, section 8.5 discusses plant control systems, and section 8.6 describes the diverse actuation system.

Definitions

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 trips and ESF functions, 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 are accomplished by the trip and actuation subsystems. Examples of protective functions are reactor trips and engineered safety features actuations (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 a circuit breaker, relay, or pilot valve).

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 maintains 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).

8.2 AP1000 Instrumentation and Control Overview

Figure 8-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data 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 ESF actuation functions, and the Qualified Data Processing System (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, which reverts 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 those associated with 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, the 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 8-1, 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 the 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 inputs 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.

Protection and Safety Monitoring System

The protection and safety monitoring system provides detection of off-nominal conditions and actuations 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. Manual control is from the main control room or the remote shutdown workstation.

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

The protection and safety monitoring system incorporates the Common Q platform and the Advant Controller 160, which executes the protection algorithms for the Common Q application (Figure 8-2). The Common Q platform typically consists of the following major components, which for each division are located in a single cabinet:

- Processor modules,
- Input and output modules,
- Flat panel display system (operations and maintenance),
- Communications bus,
- High-speed link (fiber-optic) communications, and
- Qualified power supplies.

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. The sensors and their related signal-processing devices are mounted in pairs to maintain the impact monitoring function if a sensor fails in service.

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 the 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 systems utilize Emerson's Ovation expert distributed control and information system.

The plant control system is described in Section 8.5 and shown in Figure 8-6.

Diverse Actuation System

The diverse actuation system is a nonsafety-related, diverse system that provides an alternate means of initiating reactor trips, actuating selected engineered safety features, and providing plant information to the operator. The diverse actuation system is described in section 8.6.

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown workstation, the 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 (1) the plant protection and safety monitoring system processor and logic circuits, which interface with the reactor trip and ESF plant components; (2) the plant control system processor and logic circuits, which interface with the nonsafety-related plant components; and (3) 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 the 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.

8.3 Reactor Trips

8.3.1 Introduction

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 the occurrence of a Condition II or III event, as discussed in Chapter 15 of the AP1000 Design Control Document (DCD). 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. A 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.

The equipment involved in generating reactor trips is shown in simplified block diagram form in Figure 8-3. The equipment involved includes:

- Sensors,
- Protection and safety monitoring system cabinets, and
- 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 8-1 lists variables monitored for reactor trips.

Figure 8-4 illustrates the development of a reactor trip. Four redundant measurements, from 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, Figure 8-5.

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 two actions: it de-energizes the undervoltage 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 shut down.

Bypasses of parameter channels used to generate reactor trip signals and of reactor trip actuation divisions are permitted as described in subsection 8.3.4. The 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 8.3.2 provides a description of each of the reactor trip functions. Figure 8-7 is a functional diagram of the reactor trips.

8.3.1.1 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, and
- 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 particular protective functions.

The process sensors are devices which measure temperature, pressure, fluid flow, and fluid level. Process instrumentation excludes nuclear and radiation measurements. Additional information on process variables is included as part of the descriptions of process systems provided in other sections.

Three types of neutron detectors monitor the leakage neutron flux, from a completely shutdown condition to 120 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, and
- Power range – uncompensated ionization chamber.

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

8.3.1.2 Reactor Trip Switchgear

The reactor trip switchgear (Figure 8-5) is used to initiate reactor shutdown. The reactor trip switchgear connects the electrical motive power, supplied from motor-generator sets, to the rod control system. The rod control system holds the control rods in position as long as electrical power is available. When the protection and safety monitoring system senses that established limits for safe operation of the plant have been, or are about to be, exceeded, a command is generated to de-energize the undervoltage trip devices and to energize the shunt trip devices in the reactor trip switchgear breakers. Either of these actions trips (opens) the breakers, interrupting the power to the rod control system. When power is removed, the control rods drop by gravity into the reactor core, initiating the shutdown process.

8.3.2 Reactor Trip Descriptions

The following subsections describe the specific reactor trip functions, which are grouped according to the following eleven conditions:

- Subsection 8.3.2.1 - Nuclear Startup Trips,
- Subsection 8.3.2.2 - Nuclear Overpower Trips,
- Subsection 8.3.2.3 - Core Heat Removal Trips,
- Subsection 8.3.2.4 - Primary Overpressure Trips,
- Subsection 8.3.2.5 - Loss of Heat Sink Trips,
- Subsection 8.3.2.6 - Feedwater Isolation Trip,
- Subsection 8.3.2.7 - Automatic Depressurization Systems Actuation Trip,
- Subsection 8.3.2.8 - Core Makeup Tank Injection Trip,
- Subsection 8.3.2.9 - Reactor Trip on Passive Residual Heat Removal Actuation,
- Subsection 8.3.2.10 - Reactor Trip on Safeguards Actuation, and
- Subsection 8.3.2.11 - Manual Reactor Trip.

Table 8-2 lists the reactor trips and summarizes the coincidence logic for each trip. Table 8-3 provides the interlocks for each trip.

8.3.2.1 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.

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.

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.

8.3.2.2 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.

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 rod 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.

8.3.2.3 Core Heat Removal Trips

Overtemperature ΔT Reactor Trip

The overtemperature ΔT trip provides core protection to prevent departure from nucleate boiling (DNB) 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 if pressure is within the range between the high and low pressure reactor trips. This setpoint includes corrections for changes in the 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 setpoint is automatically reduced according to the setpoint calculation equation.

Two hot leg temperature measurements per loop are combined with individual cold leg temperature measurements to form four ΔT power signals, $q_{\Delta T}$. $q_{\Delta T}$ is the calculated core power based on the properties of compressed water at the measured hot leg temperature (T_H), cold leg temperature (T_C), and pressurizer pressure (P_{PZR}). Hence, $q_{\Delta T} = f(T_H, T_C, P_{PZR})$.

The overtemperature trip setpoint, $OT \square T_{SP}$, is continuously calculated as a function of P_{PZR} , T_C , and axial flux difference (ΔI): $OT \square T_{SP} = f_1(P_{PZR}, T_C) - f_2(\Delta I)$, where $f_2(\Delta I)$ is the penalty associated with adverse axial power distribution. A reactor trip is initiated if $q_{\Delta T}$ exceeds $OT \square T_{SP}$ in at least two of the four divisions.

Two separate ionization chambers supply the upper and lower flux signals for each overtemperature ΔT channel. An increase in ΔI beyond a predefined deadband results in a decrease in the trip setpoint. The required four pressurizer pressure parameters, one per loop, are obtained from four separate sensors connected to pressure taps at the top of the pressurizer.

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, $q_{\Delta T}$ (the same as that used for the overtemperature ΔT trip), exceeds the setpoint in at least two of the four divisions. The setpoint is a calculated value which includes a penalty for adverse axial power distribution. The sources of temperature and neutron flux information for the overpower ΔT trip are identical to those of the overtemperature ΔT trip, and the resultant ΔT setpoint is compared to the same measured ΔT power signal.

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.

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 block enhances reliability by preventing unnecessary reactor trips. The trip function is automatically reset when reactor power is above the P-10 setpoint.

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 of at least two out of the four reactor coolant pumps falls below the setpoint. A 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 the 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.

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.

8.3.2.4 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. The high pressurizer pressure protection trips the reactor when at least two out of the four pressurizer pressure channels exceed the trip setpoint. There are no interlocks or permissives associated with this trip function.

High-3 Pressurizer Water Level Reactor Trip

This trip is provided as a backup to the high pressurizer pressure reactor trip and serves to prevent water relief through the pressurizer safety valves. The high pressurizer water level protection trips the reactor when at least two out of the four pressurizer water level channels exceed the trip setpoint. Each 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.

8.3.2.5 Loss of Heat Sink Trip

Reactor Trip on Low Water Level in any Steam Generator

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

8.3.2.6 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.

8.3.2.7 Automatic Depressurization System Actuation Trip

A reactor trip is initiated if an automatic depressurization system actuation occurs either automatically or manually. This provides a reactor trip if the reactor coolant system is depressurized and a trip is not initiated from another source. The automatic depressurization system actuation function is discussed in subsection 8.4.2.5.

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 the reactor trip circuit breakers. These provide a backup to the undervoltage trip of the breakers.

8.3.2.8 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 8.4.2.4.

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 the reactor trip circuit breakers. These provide a backup to the undervoltage trip of the breakers.

8.3.2.9 Reactor Trip on Passive Residual Heat Removal Actuation

A reactor trip is initiated when the passive residual heat removal heat exchanger's (PRHRHX's) discharge valves come off their fully shut seats, allowing flow through the heat exchanger. This reactor trip will prevent the fuel design limits from being exceeded in the event that the PRHRHX is inadvertently aligned to allow flow when the reactor is being operated at power conditions. The PRHRHX alignment is discussed in subsection 8.4.2.8.

8.3.2.10 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 8.4. 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 the reactor trip circuit breakers. These provide a backup to the undervoltage trip of the breakers.

8.3.2.11 Manual Trip

The manual reactor trip consists of two controls in the main control room, either of which trip all eight 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. Contacts on each control, physically and electrically separated, are in series with the undervoltage trip attachments 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 the 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.

8.3.3 Reactor Trip System Interlocks

The interlocks which affect reactor trip functions are designated as P-xx permissives. Table 8-3 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 the technique of integrating permissives into each channel.

Manual blocks of reactor trips are described in this subsection. The source range, intermediate range, and power range (low setpoint) high flux trip manual blocks, and the low steam generator water level trip manual block, 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.

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.

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.

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.

8.3.4 Bypasses of Reactor Trip Functions

Each channel which affects reactor trips can be bypassed, 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 reverting to a two-out-of-three logic. Bypassing two or more channels is not allowed.

8.4 Engineered Safety Features Actuation System

8.4.1 Introduction

The AP1000 design provides instrumentation and controls to sense accident situations and to initiate engineered safety features (ESFs). 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.

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. A block diagram of the protection and safety monitoring system is provided in Figure 8-3.

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. The development of component actuation is illustrated in the ESF logic diagram of Figure 8-9.

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.) Monitored variables are listed in Table 8-6. 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 actuation to be generated. When a 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 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 components.

Subsection 8.4.2 provides a functional description of the signals and initiating logic for each of the engineered safety features actuations. Figure 8-8 presents the functional diagram for safeguards actuation.

Table 8-4 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 Chapters 6 and 15 of the AP1000 DCD. However, not all the functions listed in Table 8-4 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.

8.4.2 Engineered Safety Features Actuation Descriptions

Each of the following subsections provides a functional description of the signals and initiating logic for a particular engineered safety features actuation. Table 8-4 lists the signals and summarizes the coincidence logic used to generate the safeguards actuation signal or initiate each engineered safety feature. Table 8-5 describes the permissives and interlocks relating to the engineered safety features.

8.4.2.1 Safeguards Actuation (S) Signal

A safeguards actuation (S) signal is involved in the initiation logic of many of the engineered safety features actuations discussed in subsection 8.4.2. In addition, as described in section 8.3, 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 trips the reactor and generates a safeguards actuation signal.

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

Separate momentary controls are provided, each of which manually resets the safeguards actuation signal in a single division. The manual reset of a safeguards actuation signal, in coincidence with the reactor trip breaker open permissive (P-3), blocks the safeguards actuation signal. The absence of P-3 automatically resets the blocking function. The safeguards actuation signal can be 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.

8.4.2.2 Containment Isolation

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

1. Automatic or manual safeguards actuation signal (subsection 8.4.2.1)
2. Manual initiation
3. Manual actuation of passive containment cooling (subsection 8.4.2.13)

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.

A manual reset is provided to block the automatic actuation signal for containment isolation. A separate momentary control is 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 involve interlock or permissive inputs.

8.4.2.3 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 8.4.2.5)
2. Coincidence of both loop 1 and loop 2 hot leg levels below the 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 8.4.2.5.

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 8.4.2.4, this core makeup tank

actuation function can be manually blocked when the pressurizer water level is below the P-12 setpoint.

8.4.2.4 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 8.4.2.1)
2. Automatic or manual actuation of the first stage of the automatic depressurization system (subsection 8.4.2.5)
3. Low-2 pressurizer level
4. Low wide range steam generator level coincident with High hot leg temperature
5. Manual initiation

Each of conditions 1 through 5 initiates a block of the pressurizer heaters, trips the reactor and reactor coolant pumps, initiates alignment of the core makeup tank isolation valves for passive injection to the reactor coolant system, and provides 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.

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 levels 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_H) setpoint.

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

8.4.2.5 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 8.4.2.4) 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, aligns 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 signaled 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 signaled to open following a preset time delay after the first-stage depressurization valves have been signaled to open. The second-stage depressurization valves are signaled to open following a preset time delay after the second-stage isolation valves have been signaled to open, similar to stage one.

Similar to the second stage, the third-stage isolation valves are signaled to open following a preset time delay after the second-stage depressurization valves have been signaled to open. The third-stage depressurization valves are signaled to open following a preset time delay after the third-stage isolation valves have been signaled 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 (a nonsafety-related function) following a preset time delay after the first-stage depressurization valves have been signaled 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 have been signaled 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 valves is provided following a preset time delay after the substage-A depressurization valves have been signaled 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 8.4.2.3.

A signal to initiate the opening sequence of the fourth stage is also generated upon the occurrence of the coincidence of 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 8.4.2.3, 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 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 8.4.2.1.

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.

8.4.2.6 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 8.4.2.1)

2. Automatic or manual actuation of the first stage of the automatic depressurization system (subsection 8.4.2.5)
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 8.4.2.4)
6. High reactor coolant pump bearing water temperature

Once a signal to trip the reactor coolant pumps is generated, the actual tripping of the pumps 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 levels 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_H) 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 those used in the high reactor coolant pump bearing water temperature reactor trip (subsection 8.3.2.3), but with the inclusion of a preset time delay.

8.4.2.7 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 8.4.2.1)
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 trips the turbine and isolates the main feedwater supply. This action also initiates isolation of startup feedwater (subsection 8.4.2.14).

Condition 3 is derived from the 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 8.4.2.14), and isolates the chemical and volume control system.

Condition 4 results from the 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 the 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 the 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 8.4.2.17.

8.4.2.8 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 8.4.2.4)
2. First-stage automatic depressurization system actuation (subsection 8.4.2.5)
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. Any of these conditions overrides any closure signal to this valve and also closes the blowdown isolation valves for 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 from 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 aligns the passive residual heat removal heat exchanger and thereby initiates heat removal by this path.

8.4.2.9 Turbine Trip

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

1. Reactor trip (Table 8-2, interlock P-4)
2. High-2 steam generator narrow range water level
3. Manual feedwater isolation (subsection 8.4.2.7)

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

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

8.4.2.10 Containment Recirculation

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

1. Low-3 in-containment refueling water storage tank water level coincident with fourth-stage automatic depressurization system actuation (subsection 8.4.2.5)
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.

Either of conditions 1 and 2 results 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 actuation 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 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.

8.4.2.11 Steam Line Isolation

A signal to isolate the steam lines 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 their associated bypass valves. In addition to manual system-level steam line isolation, the steam line isolation valves can be closed individually via the nonsafety-related 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. Each 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 any two of the four reactor coolant system cold leg temperatures below the Low T_C setpoint in either 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 by either Condition 3 or 5, or by Condition 4.

8.4.2.12 Steam Generator Blowdown System Isolation

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

1. Passive residual heat removal heat exchanger alignment signal (subsection 8.4.2.8)
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 for the affected steam generator.

8.4.2.13 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 8.4.2.2) and isolation of the containment air filtration system (subsection 8.4.2.20).

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. A separate momentary control is provided for resetting each division.

8.4.2.14 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 8.4.2.7)
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 any two of the four reactor coolant system cold leg temperatures below the Low setpoint in either 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 the 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 the 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).

8.4.2.15 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 8-2, 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 nonsafety 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 is from a borated source that does 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 T1, compared to a similar average taken for time period T2 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 the 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 detectors' 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 charger for division A or C coincident with an undervoltage to the battery charger for division B or D.

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

8.4.2.16 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 8.4.2.1) 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 the 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 8.4.2.19).

Condition 6 results from the 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).

8.4.2.17 Steam Dump Block

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

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

Condition 1 results from the 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.

8.4.2.18 Main Control Room Isolation and Air Supply Initiation

Signals to initiate isolation of the main control room, to initiate the emergency air supply to the control room, and to open the control room pressure relief isolation valves are generated from any 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 charger for division A or C coincident with an undervoltage to the battery charger for division B or D.

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

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

8.4.2.19 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 allows the operators to use the auxiliary spray to rapidly depressurize the reactor coolant system. The operator can also manually initiate auxiliary spray isolation.

The auxiliary spray and letdown purification line isolation signal is also generated upon manual actuation of chemical and volume control system isolation (subsection 8.4.2.16).

8.4.2.20 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 8.4.2.1)
2. Manual actuation of containment isolation (subsection 8.4.2.2)
3. Manual actuation of passive containment cooling (subsection 8.4.2.13)
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 8.4.2.2) 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 involve interlock and permissive inputs.

8.4.2.21 Normal Residual Heat Removal System Isolation

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

1. Automatic or manual safeguards actuation signal (subsection 8.4.2.1)
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. A separate momentary control is 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 the two control sets initiates closure of the RNS isolation valves. A two-control simultaneous actuation prevents inadvertent actuation.

8.4.2.22 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.

8.4.2.23 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 legs. This helps to maintain reactor coolant system inventory during mid-loop operation. The signal may be manually blocked by the operator when pressurizer level is above the P-12 setpoint. These letdown valves are also closed by the containment isolation function, as described in subsection 8.4.2.2.

8.4.2.24 Pressurizer Heater Block

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 8.4.2.4)
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 power to five pressurizer heater electrical control centers. When these five power-feed breakers are opened, all electrical power is removed from all 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 commands the plant control system to open each molded-case circuit breaker which provides power to an individual pressurizer heater. This arrangement provides for complete disabling of the pressurizer heaters, even if a single component failure occurs. The pressurizer heater trip on condition 2 may be manually blocked when wide range RCS pressure is below the P-19 setpoint.

8.4.2.25 Steam Generator Relief Isolation

A signal for closing the steam generator power-operated relief valves and their block valves is generated from either 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. Each 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 by 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.

8.4.2.26 Component Cooling Water System Containment Isolation

A signal to close the component cooling water system containment isolation valves is derived from the 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 8.4.2.6, condition 6), but with the inclusion of a preset time delay.

8.4.2.27 Containment Vacuum Relief

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

1. Low-2 containment pressure
2. 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 results in opening of the containment vacuum relief valves.

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

8.4.3 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 8-5.

8.4.4 Bypasses of Engineered Safety Features Actuation

The channels used in engineered safety features actuation that can be manually bypassed are indicated in Table 8-4. 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.

8.5 Control Systems

8.5.1 Introduction

The function of the AP1000 control systems is to establish and maintain the plant operating conditions within prescribed limits. The control systems improve 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.

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 adjusted to control 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 and 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 prescribed volumes of water and steam which depend 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 also maintains hot no-load or hot low-load conditions prior to turbine loading. It provides a means for plant cooldown.

8.5.2 Control System Descriptions

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 pressurizer water level at, or restores it to, its programmed value. The required water level operating region is programmed as a function of reactor coolant system temperature and power generation 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 levels at a predetermined setpoint during steady-state operation. It also maintains the water levels within operating limits during normal transient operation. The feedwater control system restores normal water levels 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 maintains 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 systems provide control of systems performing defense-in-depth functions.

Design Capability - The control systems are 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 increases of 10 percent from an initial power level between 15 percent and 90 percent of full power, without a 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 a reactor trip or steam dump system actuation, subject to core power distribution limits.
- The capability to accept the design full-load rejection without a reactor trip.
- The capability to accept a turbine trip from full-power operation without a 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, or
- Pressurizer safety valves.

In addition, these valves are not actuated during a normal plant trip.

8.5.3 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). The reactor coolant system boron concentration is adjusted by the operator to account for long-term core burnup. The adjustment also maintains two gray M banks and both black M banks (M1 and M2) in a nearly 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. Each of the following two subsections provides a description of one control subsystem.

8.5.3.1 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:

$$T_{avg} = (T_h + T_c) / 2$$

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the highest T_{avg} measured in one 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 each mode of control. If the plant is in a load-follow or load-regulation mode of operation, then the deadband is widened from that used for base-load 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 effects a linear ramp change in core power at the selected rate.

8.5.3.2 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 8.5.3.1. 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 rod positions are changed 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.

8.5.4 Rod Control System

The rod control system receives rod speed and direction signals from the power control and axial offset control subsystems. Portions of the rod control system operate specific 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 8-7.

For axial offset control, the rod speed demand signal is 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 8-8.

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 positions 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.

8.5.4.1 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 their center lines.

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.

8.5.4.2 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 an 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 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 a 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.

8.5.4.3 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.

8.5.5 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 of 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 at 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 those which can be accommodated by the variable heater control result 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 the 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.

8.5.6 Pressurizer Water Level Control System

The pressurizer water inventory, or level, 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, the pressurizer level control system 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, the pressurizer level control system 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 when 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.

8.5.7 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 generators. 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 lines. The startup feedwater control subsystem regulates the flow of feedwater into the steam generators via the startup feedwater lines. Flow to the startup feedwater lines may be supplied by a main feedwater pump or by the startup feedwater pumps. Each of the following two subsections provides a description of one of the control subsystems.

8.5.7.1 Feedwater Control

The feedwater control subsystem maintains a programmed water level in the shell side of the steam generators 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 into the feedwater control subsystem. In the high-power control mode, the feedwater flow to each steam generator 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 feed-forward control using wide-range water level, and to allow a feedwater flow indication within

the upper limit of the low-range feedwater flow measurement. If the feedwater flow indication falls below the lower limit of the effective span of the low-range feedwater flow measurement, integration (reset) action of the low-power mode feedwater flow controller is inhibited. 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.

8.5.7.2 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 levels. The startup feedwater control subsystem performs this function.

The startup feedwater control subsystem maintains a programmed water level in the shell side of each steam generator during low-power (below approximately 10 percent of plant rated thermal power), no-load, and plant-heatup and -cooldown modes. With low feedwater flow demands, feedwater is controlled by the startup feedwater control subsystem. The transition between the main and startup feedwater lines is automatically controlled based on flow measurements within the respective lines. The startup feedwater control subsystem is also automatically actuated on signals which indicate a loss of water inventory or heat sink in the secondary side of a steam generator, and it attempts to recover the inventory loss and to return the steam generator water level(s) to the programmed value. If the startup feedwater control subsystem cannot recover the inventory deficit, core 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.

8.5.8 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, without requiring atmospheric steam relief, and without 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 8.5.9 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 the 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 operation, 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 8.5.8.1. The plant trip controller is discussed in subsection 8.5.8.2.
- The pressure mode uses the difference between the 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 cooldowns. It is described in subsection 8.5.8.3.

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 and input signal failures and eliminates interaction between the control and the protection systems.

To prevent actuation of the steam dump valves in response to 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 the steam dump on low wide-range water level improves the plant performance in response to anticipated-transient-without-reactor-scrum events, as modeled in the AP1000 Probabilistic Risk Assessment.

8.5.8.1 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 the difference between the lead-lag compensated selected T_{avg} and the selected reference T_{avg} (designated T_{ref}), which is 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 operation. 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 valves modulate 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 dump valves partially open.

8.5.8.2 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 valve opening 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 in the closed direction by the plant trip controller. This regulates the rate of removal of decay heat and establishes the equilibrium hot shutdown condition.

8.5.8.3 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 operates the same steam dump valves as those operated by the load rejection and plant trip controllers described in subsections 8.5.8.1 and 8.5.8.2. 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 an automatically controlled plant cooldown 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 opens the dump valves as necessary to achieve the setpoint cooldown rate and to stop at the target temperature setpoint.

8.5.9 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 (in accordance with the 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 valves maintained in positions to match the steam flow to the thermal load. The operators can then switch to the pressure mode of control of 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 dump valves close, reset the steam dump controller, place the plant back into automatic, and return to the desired power level.

8.5.9.1 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. 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.

8.5.9.2 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 are 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.

8.5.10 Signal Selector Algorithm

The plant control systems for the AP1000 derive some of their 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. Isolation devices are provided to guard the protection system against possible electrical faults in the control systems.

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 bypass logic. 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.

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 of the valid process values, the number of valid process values, an alarm if one process value has been rejected, and a second alarm if two process values have been rejected.

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.

8.6 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 in which 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 probabilistic risk assessment (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.

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 signals to the input signal conversion block. The conversion block continuously performs analog-to-digital signal conversions and stores the values 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 the DAS and the PMS is achieved by the use of different architectures, different hardware implementations, and different software, if any.

Software diversity between the DAS and the PMS is achieved through the use of different algorithms, logic, program architecture, executable operating systems, and executable software/logic.

The diverse automatic actuations are:

- Tripping rods via the motor-generator sets, tripping the turbine, initiating passive residual heat removal, actuating core makeup tanks, and tripping the reactor coolant pumps on low wide-range steam generator water level.
- Tripping rods via the motor-generator sets, tripping the turbine, opening the passive residual heat removal discharge isolation valves, and closing the in-containment refueling water storage tank gutter isolation valves on high hot leg temperature.
- Tripping rods via the motor-generator sets, tripping the turbine, actuating the core makeup tanks, and tripping the reactor coolant pumps on low pressurizer water level.
- Isolating selected containment penetrations and starting passive containment cooling water flow on high containment temperature.

The selected 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 both 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,
- Opening stage 1 automatic depressurization system valves,
- Opening stage 2 automatic depressurization system valves,
- Opening stage 3 automatic depressurization system valves,
- Opening stage 4 automatic depressurization system valves,
- Opening the passive residual heat removal discharge isolation valves and closing the in-containment refueling water storage tank gutter isolation valves,
- Selected containment penetration isolation,
- Containment hydrogen igniter actuation,
- Initiating in-containment refueling water storage tank injection,
- Initiating containment recirculation, and
- Initiating in-containment refueling water storage tank draining to containment.

In addition to the above functions, a redundant method of actuating the following components is provided at the DAS squib valve control cabinet:

- Opening stage 4 automatic depressurization system valves,
- Initiating in-containment refueling water storage tank injection,
- Initiating containment recirculation, and
- Initiating in-containment refueling water storage tank draining to containment.

Table 8-1 (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

Table 8-1 (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⁾
Overpower ΔT			$\pm 4\%$ 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	$\pm 3\%$ of span	0.9
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% ($\Delta\phi$)		0.6
Pressurizer Low Pressure	Pressurizer pressure	1700 to 2500 psig	$\pm 3\%$ of span	0.9
Pressurizer High Pressure	Pressurizer pressure	1700 to 2500 psig	$\pm 3\%$ of span	0.9
Pressurizer High Water Level	Pressurizer water level	0-100% of entire cylindrical portion of pressurizer	$\pm 5\%$ of span	0.9
Low Reactor Coolant Flow	Coolant flow	0 to 120% of rated flow	$\pm 3\%$ of span	0.9
Low Reactor Coolant Pump Speed	Pump speed	0 to 120% of rated speed	$\pm 1\%$ of span	0.7
Low Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	$\pm 22\%$ of span	0.9
High Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	$\pm 13\%$ of span	0.9
Reactor Coolant Pump High Bearing Water Temperature	Reactor coolant pump bearing water temperature	70°-450°F	$\pm 2\%$ of span	5.5

Table 8-1 (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 8-6	See Table 8-6	See Table 8-6	See Table 8-6
Manual Reactor Trip	Control status	N/A	N/A	N/A
Automatic or Manual Depressurization System Actuation	See Table 8-6	See Table 8-6	See Table 8-6	See Table 8-6
Automatic or Manual Core Makeup Tank Injection	See Table 8-6	See Table 8-6	See Table 8-6	See Table 8-6
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 8-2 (Sheet 1 of 2)

REACTOR TRIPS

Reactor Trip⁽¹⁾	No. of Channels	Division Trip Logic	Bypass Logic	Permissives and Interlocks (See Table 8-3)
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 8-2 (Sheet 2 of 2)

REACTOR TRIPS

Reactor Trip⁽¹⁾	No. of Channels	Division Trip Logic	Bypass Logic	Permissives and Interlocks (See Table 8-3)
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 8-3 (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
$\overline{P-6}$	Intermediate range neutron flux below setpoint	Automatically resets source range reactor trip
P-10	Power range nuclear power above setpoint	<ul style="list-style-type: none"> (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 8-3 (Sheet 2 of 2)

REACTOR TRIP PERMISSIVES AND INTERLOCKS

Designation	Derivation	Function
<u>P-10</u>	Power range nuclear power below setpoint	<ul style="list-style-type: none"> (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
<u>P-11</u>	Pressurizer pressure above setpoint	Automatically resets High-2 steam generator water level reactor trip

Table 8-4 (Sheet 1 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
1. Safeguards Actuation Signal			
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			
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 8-4 (Sheet 2 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
3. Automatic Depressurization System			
(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 8-4 (Sheet 3 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Division/ Controls	Actuation Logic	Permissives and Interlocks
4. Main Feedwater Isolation			
(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-BYP ¹	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			
(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 8-4 (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			
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			
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			
a. Manual initiation	2 controls	1/2 controls	None

Table 8-4 (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			
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			
a. Manual initiation	2 controls	1/2 controls	None
b. High-2 containment pressure	4	2/4-BYP ¹	None
11. Startup Feedwater Isolation			
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 8-4 (Sheet 6 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Division/ Controls	Actuation Logic	Permissives and Interlocks
12. Passive Residual Heat Removal			
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			
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			
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 8-4 (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 ⁽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			
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			
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 8-4 (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			
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			
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			
a. Low spent fuel pool level	3	2/3	None
21. Open In-Containment Refueling Water Storage Tank (IRWST) Injection Line Valves			
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			
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			
a. Automatic reactor coolant system depressurization (fourth stage) coincident with	(See items 3d through 3f)		

Table 8-4 (Sheet 9 of 9)

ENGINEERED SAFETY FEATURES ACTUATION SIGNALS

Actuation Signal	No. of Divisions/ Controls	Actuation Logic	Permissives and Interlocks
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			
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			
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			
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			
a. High reactor coolant pump bearing water temperature	4/pump	2/4-BYP ¹ in affected pump	None
28. Containment Vacuum Relief			
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 8-5 (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 8-5 (Sheet 2 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM		
Designation	Derivation	Function
P-11 (continued)	Pressurizer pressure below setpoint	<ul style="list-style-type: none"> (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.
<u>P-11</u>	Pressurizer pressure above setpoint	<ul style="list-style-type: none"> (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 8-5 (Sheet 3 of 4)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM		
Designation	Derivation	Function
P-12	Pressurizer level below setpoint	<ul style="list-style-type: none"> (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 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	<ul style="list-style-type: none"> (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 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 8-5 (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
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 8-6 (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 8-6 (Sheet 2 of 2)

**ENGINEERED SAFETY FEATURES ACTUATION,
VARIABLES, LIMITS, RANGES, AND ACCURACIES
(NOMINAL)**

Variables	Range of Variables	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.

Table 8-7

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 8-8

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