7.7 Control and Instrumentation Systems

The function of the AP1000 control systems is to establish and maintain the plant operating conditions within prescribed limits. The control system improves plant safety by minimizing the number of situations for which some protective response is initiated and relieves the operator from routine tasks.

The AP1000 control systems share a common hardware design and implementation philosophy. They are also functionally integrated to enhance responsiveness during plant transients. Specific design requirements are imposed that limit the impact of individual equipment failures. (See subsection 7.1.3).

The control systems regulate the operating conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following:

Reactor Coolant System Temperature - The control systems function to maintain the reactor coolant system temperature at or near a programmed value. This value is a function of plant load or other operating conditions. Steam conditions for the turbine depend on the temperature maintained in the reactor coolant. Reactor coolant system temperature is also used for controlling core reactivity.

Nuclear Power Distribution - Operating limits include the distribution of nuclear energy production within the core as well as its average value. The axial distribution of the nuclear power is controlled within prescribed limits.

Reactor Coolant System Pressure - The reactor coolant system is pressurized to prevent significant boiling at operating temperatures. This pressure is controlled within limits that prevent reductions which expose the fuel to possible departure from nucleate boiling or from increases that would challenge the reactor coolant system design pressure.

Pressurizer Water Level - To provide a sufficient buffer for plant transients, the reactor coolant system pressurizer contains a prescribed volume of water and steam which depends on plant load and operating temperature.

Steam Generator Water Level - The steam generator water level is maintained within limits to provide adequate energy removal capability and to avoid moisture carryover.

Steam Dump (Turbine Bypass) - For fast and large transients such as load rejections, an additional thermal load (designated steam dump or turbine bypass) functions until nuclear power is reduced. This steam dump is also used to maintain hot no-load or hot low-load conditions prior to turbine loading. It provides a means for plant cooldown.

7.7.1 Description

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

Reactor Power Control System - The reactor power control system coordinates the responses of the various reactivity control mechanisms. The system enables daily load follow operation with a minimum of manual control by the operator. Load regulation and frequency control are compatible with the reactor power control system operation. Axial nuclear power distribution control is also performed by the reactor power control system.

Rod Control System - The rod control system, in conjunction with the reactor power control system, maintains nuclear power and reactor coolant temperature, without challenges to the protection systems, during normal operating transients.

Pressurizer Pressure Control - The pressurizer pressure control system maintains or restores the pressurizer pressure to the nominal operating value following normal operating transients. The control system reacts to avoid challenges to the protection systems during these operating transients.

Pressurizer Water Level Control - The pressurizer water level control system establishes, and maintains or restores pressurizer water level to its programmed value. The required water level 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 level at a predetermined setpoint during steady-state operation. It also maintains the water level within operating limits during normal transient operation. The feedwater control system restores normal water level following a unit trip. The various modes of feedwater addition are automated to require a minimum of operator involvement.

Steam Dump Control - The steam dump control system reacts to prevent a reactor trip following a sudden loss of electrical load. The steam dump control system also removes stored energy and residual heat following a reactor trip so that the plant can be brought to equilibrium no-load conditions without actuation of the steam generator safety valves. The steam dump control system also provides for maintaining the plant at no-load or low-load conditions to facilitate a controlled cooldown of the plant.

Rapid Power Reduction - For large, rapid load rejections (turbine trip or grid disconnect from 50-percent power or greater) a rapid nuclear power cutback is implemented. This results in a reduction of thermal power to a level that can be handled by the steam dump system.

Defense-In-Depth Control - The plant control system provides control of systems performing defense-in-depth functions. Table 7.7-3 provides a listing of the defense-in-depth functions that are supported by the plant control system and provides a cross reference to the applicable information located in other sections of this document.

7.7.1.1 Reactor Power Control System

Automatic reactor power and power distribution control are the basic functions of the reactor power control system. They are achieved by varying the position of the control rods. Separate control rod banks are used to regulate reactor power and power distribution.

The reactor power control system enables the plant to respond to the following load change transients:

- Step load changes of plus or minus 10 percent
- Ramp load increases and decreases of 5 percent per minute
- Daily load follow operations with the following profile:
  - Power ramps from 100 percent to 50 percent in 2 hours
  - Power remains at 50 percent for 2 to 10 hours
  - Power ramps back up to 100 percent in 2 hours
  - Power remains at 100 percent for the remainder of the 24-hour cycle
- Grid frequency response (denoted load regulation) resulting in a maximum of 10-percent power change at 2 percent per minute

These capabilities are accomplished without a reactor trip or steam dump actuation. During daily load follow and load regulation transients, automatic control of axial offset is provided. The system restores coolant average temperature to a value which is within the programmed temperature band following a change in load. Manual control of either the power control rods (M banks) or the axial offset control rods (AO bank) is performed within the range of defined insertion limits.

The reactor power control system uses a different control strategy for the rods used to regulate core power (M banks) from the control strategy used to regulate axial offset (AO bank). Reactor coolant system boron concentration is adjusted by the operator to account for long-term core burnup. The adjustment also maintains the two gray M banks and both black M banks (M1 and M2) in a near fully withdrawn position, the first two moving gray M banks fully inserted, and the AO bank slightly inserted. During load follow or load regulation response transients, the power control and the axial offset control subsystems jointly function to control both core power and axial offset. The following two subsections provide a description of each control subsystem.

7.7.1.1.1 Power Control

The power control subsystem controls the reactor coolant average temperature by regulating the M control rod bank positions. The reactor coolant loop average temperatures are determined from hot and cold leg measurements in each reactor coolant loop. The average coolant temperature (T_{avg}) is computed for each loop, where:

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

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the highest of the lead/lag compensated T_{avg} measured temperatures from each of the reactor coolant loops constitutes the primary control signal. The programmed coolant temperature increases linearly with turbine load from the zero-power to the full-power condition.

The temperature input signals for the power control subsystem are fed from protection channels via isolation devices and the signal selector function.

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

The deviation of the reactor coolant temperature from the programmed value is the basic control variable for reactor power control. A deadband is included in the power control subsystem so that no rod motion is demanded if the temperature error is within the deadband. As the temperature error becomes greater, the demanded rod speed becomes greater.

Separate reactor control deadbands are used for each mode of control (load follow, load regulation, or base load). 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 provides for a linear ramp change in core power at the selected rate.

7.7.1.1.2 Axial Offset Control

The axial offset control subsystem controls the core axial offset (power difference between the top and bottom halves of the core) to a value that is within the desired control range for load follow and grid frequency change transients. This is accomplished by using control rod banks separate from those used for the reactor power control described in subsection 7.7.1.1.1. Measurements of

axial offset are input into the axial offset control subsystem and then compared to an axial offset control "window." This window is calculated from measurements of compensated excore nuclear flux, along with operator inputs for the desired axial offset target value and target bandwidth and the mode of control (load follow, load regulation, or base load). The nuclear flux signals are compensated by measurements of cold leg temperature to account for the effects of moderation of the neutron flux by the reactor vessel downcomer flow. If the plant is in a load regulation mode of control, then a "smoothing" compensation is applied to both the nuclear flux and the axial offset signals. This provides a time-weighted average nuclear flux and axial offset signal input to the axial offset controller to avoid rapid temporary changes from actuating axial offset control. When the axial offset error is outside the acceptable control window, the axial offset rods are actuated until the axial offset error is back inside the control window.

To minimize the potential for interactions between the power and the axial offset rod control subsystems, the power control subsystem takes precedence. If a demand signal exists for movement of the power control rods, then the axial offset rods are blocked from moving. Only when the temperature error is within the reactor power controller deadband and the associated rod banks have stopped are the axial offset rods allowed to move.

7.7.1.2 Rod Control System

The rod control system receives rod speed and direction signals from the power control and axial offset control subsystems. The portion of the rod control system associated with the power and axial offset control subsystems each operate their own sets of control rod banks as follows:

- The power control portion operates the MA, MB, MC, MD, M1 and M2 control rod banks.
- The axial offset control portion operates the AO control rod bank.

For power control, the rod speed demand signals vary over the range of 5 to 45 inches per minute (8 to 72 steps per minute), depending on the magnitude of the input signal. Manual control is provided to move a bank in or out at a prescribed fixed speed. In the automatic mode, the rods are withdrawn (or inserted) in a predetermined sequence within the limits imposed by the control interlocks as shown in Table 7.7-1.

For axial offset control, the rod speed demand signals are set to a fixed constant speed of approximately 5 inches per minute (8 steps per minute). Manual control is provided to move a bank in or out at a prescribed fixed speed. In the automatic mode, the rods are withdrawn (or inserted) within the limits imposed by the control interlocks, as shown in Table 7.7-2.

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

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

Power to the rod drive mechanisms is supplied by two motor-generator sets operating from two separate 480-volt, 3-phase busses. Each generator is the synchronous type, and is driven by a 200-horsepower induction motor. The ac power is distributed to the rod control system cabinets through the reactor trip switchgear.

The variable speed rod drive programmer used in the power control subsystem inserts small amounts of reactivity at low speed. This permits fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed for transients such as load rejections. A summary of the control rod assembly sequencing characteristics is given below:

- The control rod groups within the same bank are stepped so that the relative position of the groups do not differ by more than one step.

- The control rod banks are programmed so that withdrawal of the banks is sequenced in a prescribed order. The programmed insertion sequence is the opposite of the withdrawal sequence. That is, the last control bank withdrawn is the first control bank inserted.

- The control bank withdrawals are programmed so that, when the first bank reaches a preset position, the next bank begins to move out simultaneously with the first bank. This preset position is determined by the maximum allowable overlap between banks (approximately 50 to 100 steps). This withdrawal sequence continues until the reactor reaches the desired power level. The control bank insertion sequence is the opposite of the withdrawal sequence.

- Overlap between successive control banks is adjustable between 0 to 50 percent (0 to 135 steps), with an accuracy of ±1 step.

The constant rod speed used in the axial offset control subsystem provides a slow stable control of core axial offset. This is acceptable since axial offset changes for the design basis load follow transients generally occur over several hours and rapid response is not needed. The slow response of the axial offset control system also allows the rods used by the power control subsystem to counteract the core power reactivity changes that are induced by the axial offset rods.

7.7.1.3 Control Rod Position Monitoring

Digital Rod Position - The digital rod position indication system measures the position of each control rod assembly using a detector consisting of discrete coils mounted concentric with the rod drive pressure housing. The coils are located axially along the pressure housing and magnetically sense the entry and presence of the rod drive shaft through its center line.

Demand Position System - The demand position system counts the pulses generated in the rod control system to provide a digital readout of the demanded bank position. The demanded and measured rod position signals are displayed in the main control room. An alarm is generated whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm is set with appropriate allowance for instrument error and within sufficiently narrow limits to prevent exceeding core design hot channel factors.

Alarms are also generated if any shutdown rod is detected to have left its fully withdrawn position, or if any M bank control rods are detected at the bottom position, except as part of the normal insertion sequence.

7.7.1.4 Control Rod Insertion Limits

With the reactor critical, the normal indication of reactivity status in the core is the position of the control rod bank in relation to reactor power (as indicated by the ΔT power monitors). The ΔT power signal is used to calculate insertion limits for the banks. The following two alarms are provided for each bank.

- A "low" alarm and interlock alerts the operator of an approach to the rod insertion limits and acts to terminate automatic AO bank rod insertion (on reaching the AO bank "low" setpoint) or AO bank rod withdrawal (on reaching a M bank "low" setpoint). The operator terminates M bank insertion and reactor coolant system boron concentration changes by following appropriate plant procedures.

- A "low-low" alarm alerts the operator to take immediate action to restore the M bank and AO bank within the appropriate limits by terminating M bank insertion or AO bank withdrawal (for "low-low" M bank alarm), or terminating AO bank insertion (for "low-low" AO bank alarm) that were not stopped by the "low" setpoint interlock.

The purpose of the control bank rod insertion alarms and interlocks is to provide warning to the operator of excessive rod insertion and to terminate the insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip. It also provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection. Insertion limits provide confidence that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power, the allowable rod insertion limits are decreased (the rods must be withdrawn further) with increasing power. The insertion limits for the M banks and the AO bank are calculated from the reactor power, as measured by the ΔT power monitor, according to the following equations:

$$Z^{M}_{LL} = A + B \cdot \Delta T + C \cdot Z_{AO} + D \cdot \Delta T \cdot Z_{AO}$$

$$Z^{AO}_{LL} = E$$

where:

Z^{M}_{LL} = Maximum permissible insertion limit for the affected M control bank

Z^{AO}_{LL} = Maximum permissible insertion limit for the affected AO control bank

Z_{AO} = Current AO bank position

ΔT = Average signal of valid ΔT measurements

A,B,C,D,E = Constants chosen to maintain $Z_{LL} \geq$ the actual limit based on physics calculations

The control rod bank demand position (Z) for the M banks and the AO bank is compared to the respective Z_{LL} as follows:

- If $Z - Z_{LL} \leq F$, a low alarm and interlock is actuated.
- If $Z - Z_{LL} \leq G$, a low-low alarm is actuated.

Since nuclear peaking factors can be aggravated by the opposite movement of the M banks and the AO bank, the interlocks on the AO bank are different, depending on whether the M bank or the AO bank insertion limit setpoint is actuated. If an M bank insertion limit is reached, this stops AO bank withdrawal and reduces the increases in the core peaking factor. If an AO bank insertion limit is reached, this stops AO bank insertion. If the M banks are fully withdrawn, AO bank automatic insertion is blocked.

7.7.1.5 Control Rod Stops

Rod stops are provided to prevent abnormal power conditions that could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

7.7.1.6 Pressurizer Pressure Control System

The primary system pressure is closely regulated during operation to prevent pressure from increasing to the point where an engineered safety features actuation is required to prevent overstressing the pressure boundary; or from decreasing to a condition where engineered safety features actuation is required to prevent the possibility of departure from nucleate boiling. Fine control of pressure to the desired setpoint is accomplished by regulating the power to a bank of heaters located in the pressurizer. Large decreases in pressure are accommodated by turning on additional heater banks and by the inherent flashing from the water mass in the pressurizer, which is at saturation. Large pressure increases are controlled by actuating pressurizer spray to condense steam.

Pressurizer pressure control is designed to provide stable and accurate control of pressure to its predetermined setpoint. Automatic pressure control is available from the point at which nominal pressure is established in the startup cycle to 100-percent power. During steady-state operating conditions, the pressurizer heater output is regulated to compensate for pressurizer heat loss and a small continuous pressurizer spray. During normal transient operation, the pressure is regulated to provide adequate margin to safety systems actuation or reactor trip. The pressurizer pressure control system is designed to minimize equipment duty (such as spray nozzle thermal cycling due to spray actuation) due to load regulation operation.

Small or slowly varying changes in pressure are regulated by modulation of the variable heater control. Reset (integral) action is included to maintain pressure at its setpoint. Decreases in pressure larger than that which can be accommodated by the variable heater control results in the

actuation of the backup heaters. The backup heaters are deactivated when the variable heaters alone are capable of restoring pressure. Large increases in the pressurizer water level also result in activation of the backup heaters. The purpose of this action is to avoid the accumulation of subcooled fluid in the pressurizer, thereby allowing flashing of the pressurizer fluid to limit the pressure decrease on any subsequent outsurge.

Pressure increases too fast to be handled by reducing the variable heater output result in spray actuation. Spray continues until pressure decreases to the point that the variable heaters alone can regulate pressure. For normal transients including a full-load rejection, the pressurizer pressure control system acts promptly to prevent reaching the high pressurizer pressure reactor trip setpoint.

7.7.1.7 Pressurizer Water Level Control System

The pressurizer water inventory, or level control, provides a reservoir for the reactor coolant system inventory changes that occur due to changes in reactor coolant system density. As the reactor coolant system temperature is increased from hot zero-load to full-load values, the reactor coolant system fluid expands. The pressurizer level is programmed to absorb this change. A deadband is provided around the pressurizer level programmed setpoint to intermittently control charging and letdown. When the pressurizer water level reaches the lower limit of the deadband, it actuates the charging system. The charging system continues to operate until the level is restored to a limit above the nominal program value. When the pressurizer water level reaches the upper limit of the deadband, it actuates letdown to the liquid waste processing system.

Pressurizer water level control provides stable and accurate control of pressurizer level within a prescribed deadband around the programmed setpoint value, as derived from the plant operating parameters. Automatic level control is supplied from the point in the startup cycle where the hot zero-load level is established through 100-percent power. The reference water level is also compensated for changes in operating temperature that result from such items as rod control deadband, or reduced T_{avg} return to power operation.

7.7.1.8 Feedwater Control System

The feedwater control system consists of those controllers and associated hardware whose primary function is to regulate the flow of feedwater into the steam generator. The feedwater control system consists of two separate subsystems. The feedwater control subsystem regulates the flow of feedwater into the steam generators via the main feedwater line. The startup feedwater control subsystem regulates the flow of feedwater into the steam generators via the startup feedwater line. Flow to the startup feedwater line may be supplied by either the main or startup feedwater pump. The following two subsections provide a description of each control subsystem.

7.7.1.8.1 Feedwater Control

The feedwater control subsystem maintains a programmed water level in the shell side of the steam generator during steady-state operation, and limits the water level shrink and swell during normal plant transients. This prevents an undesirable reactor trip actuation. Indication is provided for monitoring system operation. Alarms and indications are provided to alert the plant operator of control system malfunctions or abnormal operating conditions.

Two modes of feedwater control are incorporated in the feedwater control subsystem. In the high-power control mode, the feedwater flow is regulated in response to changes in steam flow and proportional plus integral (PI)-compensated steam generator narrow range water level deviation from setpoint. In the low-power control mode, the feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated steam generator narrow range water level deviation from setpoint. A separate low range feedwater flow measurement is used in the low-power feedwater control mode.

The transition from the low to the high-power control mode is initiated on the basis of the filtered high range feedwater flow signal. The transition point is set at a feedwater flow corresponding to a power at which reliable steam flow indication is expected. The transition point is also low enough to allow effective feedforward control using wide range water level, and to allow feedwater flow indication within the upper limit of the low range feedwater flow measurement. If 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.

The feedwater valve lift required to provide the demanded feedwater flow is computed on the basis of the estimated ΔP available across the feedwater control valve, and the C_V characteristic of the valve. This compensation improves the response to changes in system ΔP, such as following the loss of one feedwater pump during high-power operation.

A high steam generator water level signal reduces the feedwater flow demand signal and closes the feedwater control valves.

7.7.1.8.2 Startup Feedwater Control

During no-load or very low power conditions, the main feedwater control subsystem is not intended to be used for automatic control of the steam generator water level. The startup feedwater control subsystem performs this function.

The startup feedwater control subsystem maintains a programmed water level in the shell side of the steam generator during low power (below approximately 10 percent of plant rated thermal power), no-load, and plant heatup and cooldown modes. During low feedwater flow demand, feedwater is controlled by the startup feedwater control subsystem. Transition between the main and startup feedwater line is automatically controlled based on flow measurements within the respective lines. The startup feedwater control subsystem is also automatically actuated on signals which indicate a loss of water inventory or heat sink in the secondary side of the steam generator and will attempt to recover the inventory loss and return the steam generator water level to the programmed value. If the startup feedwater control subsystem cannot recover the inventory deficit, reactor cooling is initiated by the passive residual heat removal system.

The startup feedwater control subsystem regulates the flow of feedwater in a manner which is similar to the way (main) feedwater is controlled in the low-power control mode. Feedwater flow is regulated in response to changes in steam generator wide-range water level and PI-compensated

steam generator narrow range water level deviation from setpoint. Tracking is provided to allow a smooth transition between control modes and between manual and automatic control.

The startup feedwater control valve lift required to provide the demanded startup feedwater flow is computed on the basis of the estimated ΔP available across the startup feedwater control valve, and the C_V characteristic of the valve. This compensation improves the response to changes in system ΔP, such as during plant heatup or cooldown where the steam pressure can change drastically.

7.7.1.9 Steam Dump Control System

The AP1000 is designed to sustain a 100-percent load rejection, or a turbine trip from 100-percent power, without generating a reactor trip, requiring atmospheric steam relief, or actuating a pressurizer or steam generator safety valve. The automatic steam dump control system, in conjunction with other control systems, is provided to accommodate this abnormal load rejection and to reduce the effects of the transient imposed on the reactor coolant system. By bypassing main steam to the condenser, an artificial load is maintained on the primary system. This artificial load makes up the difference between the reactor power and the turbine load for load rejections and turbine trips. It also removes latent and decay heat following a reactor trip.

The steam dump system is sized to pass 40 percent of nominal steam flow. This capacity, in conjunction with the performance of the reactor power control system, is sufficient to handle reactor trips from any power level, turbine trips from 50-percent power or less, and load rejections equivalent to a step load decrease of 50 percent or less of rated load. For turbine trips initiated above 50-percent power, or load rejections greater than the equivalent of a 50-percent step, the steam dump operates in conjunction with the rapid power reduction system described in subsection 7.7.1.10 to meet the performance described in the previous paragraph.

The steam dump control system has two main modes of operation:

- The T_{avg} mode uses the difference between measured auctioneered loop T_{avg} and a reference temperature derived from turbine first-stage impulse pressure, to generate a steam dump demand signal. This mode is largely used for at-power transients requiring steam dump, such as load rejections and turbine trips (where the load rejection T_{avg} mode is used) and reactor trips (where the plant trip T_{avg} mode is used). The load rejection controller is discussed in subsection 7.7.1.9.1. The plant trip controller is discussed in subsection 7.7.1.9.2.

- The pressure mode uses the difference between measured steam header pressure and a pressure setpoint to generate a steam dump demand signal. This mode is used for low-power conditions (up through turbine synchronization) and for plant cooldown. It is described in subsection 7.7.1.9.3.

Process variable input signals to the steam dump control system are fed from protection channels via isolation devices and the signal selector function. Each input (T_{avg}, turbine load, steam header pressure, and wide-range steam generator water level) is obtained from multiple transmitters of the same parameter. The signal selector rejects any signal which is bad in comparison with the remaining transmitter outputs and allows only valid measurements to be used by the control

system. This makes the steam dump system tolerant of single transmitter failures or input signal failures and eliminates interaction between the control and the protection system.

To prevent actuation of steam dump on small load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure. It unblocks the dump valves when the rate of a load rejection exceeds a preset value corresponding to a 10-percent step load decrease or a sustained ramp load decrease of greater than 5 percent per minute.

The steam dump system valves also receive a signal to close on a low wide-range steam generator water level signal. Isolating steam dump on low wide-range water level improves the plant performance to anticipated transients without reactor scram events modeled in the AP1000 Probabilistic Risk Assessment.

7.7.1.9.1 Load Rejection Steam Dump Controller

This controller prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is a difference between the lead-lag compensated selected T_{avg} and the selected reference T_{avg} (designated T_{ref}), based on turbine impulse chamber pressure.

The T_{avg} input signals are the same as those used in the reactor power control system, although a signal selector algorithm in a separate controller is employed. The lead-lag compensation for the T_{avg} signal compensates for lags in the plant thermal response and in valve positioning. The lead-lag compensation in the T_{ref} signal is used to compensate for hangup effects noted in the turbine impulse pressure measurement on turbine trips and grid disconnects. It allows for a decrease in gain in the steam dump controller, thereby increasing stability. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase. This generates an immediate demand signal for steam dump. Following the initial steam dump opening, the reactor power control system in conjunction with the rod control system commands the control rods to insert in a controlled manner to reduce the reactor power to match turbine load. On a load rejection resulting in a turbine runback, the steam dump terminates when the reactor power matches the turbine load and the temperature error is within the maneuvering capability of the control rods. On a turbine trip or grid disconnect, the steam dump modulates closed in response to the control rods reducing nuclear power to approximately 15-percent load. At this point, rod insertion stops and the plant stabilizes in preparation for a turbine/generator restart and/or grid synchronization with the steam dumps partially open.

7.7.1.9.2 Plant Trip Steam Dump Controller

Following a reactor trip, the load rejection steam dump controller is defeated and the plant trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal for steam dump is the error signal between the lead-lag compensated auctioneered T_{avg} and the no-load reference T_{avg}. When the error signal exceeds a predetermined setpoint, the steam dump valves are opened in a prescribed sequence. As the error signal reduces in magnitude, indicating that the reactor coolant system T_{avg} is being reduced toward the reference no-load value, the dump valves are modulated by the plant trip controller. This regulates the rate of removal of decay heat and establishes the equilibrium hot shutdown condition.

7.7.1.9.3 Steam Header Pressure Controller

Decay heat removal between hot standby and residual heat removal system cut-in conditions is maintained by the steam header pressure controller. This controller uses the difference between steam header pressure and a pressure setpoint to control the steam flow to the condensers. Reset action is used to eliminate steady-state error. This controller uses the same steam dump valves as the load rejection and plant trip controllers described in subsections 7.7.1.9.1 and 7.7.1.9.2. The steam header pressure control mode is manually selected by the operator. The pressure setpoint is manually adjusted by the operator based on the desired reactor coolant system temperature. In addition, the controller has a feature that allows automatically controlled plant cooldowns at a chosen rate (within limits). The operator can enter the desired cooldown rate and the desired target reactor coolant system temperature. The control system then dumps the required steam to achieve the setpoint cooldown rate and stops at the target setpoint.

7.7.1.10 Rapid Power Reduction System

The rapid power reduction system rapidly reduces the nuclear power to a level capable of being handled by the steam dump system for a large load rejection (greater than 50-percent power reduction at a rapid rate). Upon the detection of a large and rapid turbine power reduction (via a rate/lag circuit, similar to that used for steam dump control), the circuit provides a signal demanding the release of a preselected number of control rods. The dropping of these preselected rods causes the reactor power to rapidly reduce to approximately 50-percent power.

The large load rejection also actuates the steam dump system and the reactor power control system via a primary-to-secondary power mismatch signal. Following the initiation of the load rejection, the power control rods insert in a controlled manner due to the mismatch between the programmed reference average coolant temperature (based on turbine impulse chamber pressure) and the compensated average coolant temperature measured in the reactor coolant loops. In a similar manner, the load rejection steam dump controller controls the steam dump valves to prevent a large increase in reactor coolant temperature. Following the release of the preselected control rods, the power control system continues to insert the remaining control group control rods to reduce power (by temperature control channel trying to match T_{avg} to T_{ref}). Following the initial opening, the steam dump valves modulate closed based upon the (T_{avg} - T_{ref}) signal.

Controlled rod insertion and steam dump modulation continue until power is reduced to approximately 15-percent power. At this time, the rod motion ceases and the plant stabilizes with steam dump maintained to match the steam flow to the thermal load. The operators can then switch to pressure mode of control on the steam dump control system, recover the released control rods, and establish normal rod control. A normal power escalation is then performed through the following actions: resynchronize the turbine/generator, if necessary, perform turbine loading until the steam dumps close, reset the steam dump controller, place the plant back into automatic, and return to the desired power level.

7.7.1.10.1 Rod Block Interlock

To avoid the potential for a withdrawal of the normally functioning power control rods following the rod release by the rapid power reduction system, a rod withdrawal block is actuated. Actuation

occurs by the reduction of reactor power (P-17) after the initiation of the rapid power reduction system as discussed in subsection 7.2.1.1.11. The rod withdrawal block does not adversely impact the performance of the rapid power reduction system. The demand of the power control subsystem is a continuous rod insertion. Rod withdrawal during the power reduction phase is not required.

7.7.1.10.2 Rapid Power Reduction Rod Selection

The number of rods needed to obtain this power reduction is dependent on the core burnup during the fuel cycle. In addition, if a large load rejection (grid disconnect) is initiated at a part-power condition (50-percent to 100-percent power), then a reduced number of control rods need to be released. Therefore, a means is provided to have the control system select which rods will be released by the rapid power reduction system.

The selection of the rods that are released during the rapid power reduction is based on a thermal power measurement. The thermal power is integrated over time to arrive at a core burnup. Depending on the core burnup and the plant power level, the choice of the control rods to be released by the rapid power reduction system is determined. Capability is provided for the operator to correct the integrated burnup periodically based upon a more detailed burnup calculation.

7.7.1.11 Diverse Actuation System

The diverse actuation system is a nonsafety-related system that provides a diverse backup to the protection system. This backup is included to support the aggressive AP1000 risk goals by reducing the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control systems.

The protection and safety monitoring system is designed to prevent common mode failures. However, in the low probability case where a common mode failure does occur, the diverse actuation system provides diverse protection. The specific functions performed by the diverse actuation system are selected based on the PRA evaluation. The diverse actuation system functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with the event probability.

The functional logic for the diverse actuation system is shown in Figure 7.2-1, sheets 19 and 20.

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 microprocessor-based subsystems. Input signals are received from the sensors by an input signal conditioning block, which consists of one or more electronic modules. This block converts the signals to standardized levels, provides a barrier against electromagnetic and radio frequency interference, and presents the resulting

signal to the input signal conversion block. The conversion block continuously performs analog to digital signal conversions and stores the value for use by the signal processing block.

The signal processing block polls the various inputs under the control of a software-based algorithm, evaluates the input signals against stored setpoints, executes the programmed 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 microprocessor 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.

Diversity is achieved by the use of a different architecture, different hardware implementations and different software from that of the protection and safety monitoring system.

The diverse design uses standard input modules designed for use with small industrial computer systems. It also uses a microprocessor board different from those used in the protection system.

Software diversity is achieved by running different operating systems and programming in different languages.

The diverse automatic actuations are:

- Trip rods via the motor generator set, trip turbine, initiate the passive residual heat removal, actuate core makeup tanks, and trip the reactor coolant pumps on low wide-range steam generator water level

- Open the passive heat removal discharge isolation valves and close the in-containment refueling water storage tank gutter isolation valves on high hot leg temperature

- Trip rods via the motor generator set, trip turbine, actuate the core makeup tanks, and trip the reactor coolant pumps on low pressurizer water level

- Isolate selected containment penetrations and start passive containment cooling water flow on high containment temperature

The selection of setpoints and time responses determine that the automatic functions do not actuate unless the protection and safety monitoring system has failed to actuate to control plant conditions. Capability is provided for testing and calibrating the channels of the diverse actuation system.

Manual Actuation Function

[*The manual actuation function of the diverse actuation system is implemented by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the control room multiplexers, the protection and safety monitoring system cabinets, and the diverse actuation system automatic logic.*]*

The diverse manual functions are:

- Reactor and turbine trip
- Passive containment cooling actuation
- Core makeup tank actuation and reactor coolant pump trip
- Open stage 1 automatic depressurization system valves
- Open stage 2 automatic depressurization system valves
- Open stage 3 automatic depressurization system valves
- Open stage 4 automatic depressurization system valves
- Open the passive residual heat removal discharge isolation valves and close the in-containment refueling water storage tank gutter isolation valves
- Selected containment penetration isolation
- Containment hydrogen igniter actuation
- Initiate in-containment refueling water storage tank injection
- Initiate containment recirculation
- Initiate in-containment refueling water storage tank drain to containment

Actuation Logic Function

There are two actuation logic modes, automatic and manual. The automatic actuation logic mode functions to logically combine the automatic signals from the two redundant automatic subsystems in a two-out-of-two basis. The combined signal operates a power switch with an output drive capability that is compatible, in voltage and current capacity, with the requirements of the final actuation devices. The two-out-of-two logic is implemented by connecting the outputs in series. The manual actuation mode operates in parallel to independently actuate the final devices.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual, two out of two redundancy reduces the probability of inadvertent actuation.

The diverse actuation system is designed so that, once actuated, each mitigation action goes to completion. Any subsequent return to operation requires deliberate operator action.

Indication

To support the diverse manual actuations, sensor outputs are displayed in the main control room in a manner that is diverse from the protection system display functions. The indications that are provided from at least two sensors per function are:

- Steam generator water level – for reactor trip and passive residual heat removal actuations, and for overfill prevention by manual actuation of the automatic depressurization system valves
- Hot leg temperature – for passive residual heat removal actuation
- Core exit temperature – for automatic depressurization system actuation and subsequent initiation of in-containment refueling water storage tank injection and also containment hydrogen igniter actuation
- Pressurizer level – for core makeup tank actuation and reactor coolant pump trip
- Containment temperature – for containment isolation and passive containment cooling system actuation

Isolation

The diverse actuation system uses sensors that are separate from those being used by the protection and safety monitoring system and the plant control system. This prohibits failures from propagating to the other plant systems through the use of shared sensors.

There is signal isolation between the two subsystems within the diverse actuation system, one for each input and output path. These isolators are characterized by a high common mode voltage withstand capability to provide the necessary isolation against faults. The configuration is set up such that the isolation devices are capable of protecting against fault propagation between the diverse actuation system subsystems.

Actuation interfaces are shared between the diverse actuation system and the protection and safety monitoring system. The diverse actuation system actuation devices are isolated from the protection and safety monitoring system actuation devices, so as to avoid adverse interactions between the two systems. The actuation devices of each system are capable of independent operation that is not affected by the operation of the other. The diverse actuation system is designed to actuate components only in a manner that initiates the safety function. This type of interface also prevents the failure of an actuation device in one system from propagating a failure into the other system.

The diverse actuation system and the protection and safety monitoring system use independent and separate uninterruptible power supplies.

Operability, Availability, and Testing

The diverse actuation system is designed to provide protection under all plant operating conditions in which the reactor vessel head is in place and non-Class 1E UPS power is available. The automatic actuation processors, in each of the two redundant automatic subsystems of the diverse actuation system, are provided with the capability for channel calibration and testing while the plant is operating. To prevent inadvertent DAS actuations during online calibration, testing activities or maintenance, the normal activation function is bypassed. Testing of the diverse actuation system is performed on a periodic basis.

Equipment Qualification and Quality Standards

The diverse actuation system is located in a controlled environment, but is capable of functioning during and after normal and abnormal events and conditions that include:

- Wide temperature range of 40° to 120°F
- Noncondensing relative humidity up to 95 percent
- Radio frequency and electromagnetic interference

The diverse actuation system processor cabinets are located in the portion of the Annex Building that is a Seismic Category II structure. The diverse actuation system equipment, including actuated devices, is designed and tested in accordance with industry standards. The adequacy of the hardware and software is demonstrated through the verification and validation program discussed in subsection 7.1.2.14. This program provides for the use of commercial off-the-shelf hardware and software. As the diverse actuation system performs many of the protection functions associated within the ATWS systems used in existing plants, the diverse actuation system is designed to meet the quality guidelines established by Generic Letter 85-06, "Quality Assurance Guidelines for ATWS Equipment that is not Safety-Related."

7.7.1.12 Signal Selector Algorithm

The plant control system for the AP1000 derives some of its control inputs from signals that are also used in the protection and safety monitoring system. The advantages of this design are:

- The nonsafety-related plant systems are controlled from the same measurements which provide protection. This permits the control system to function in a manner which maintains margin between operating conditions and safety limits, and reduces the likelihood of spurious trips.

- Reducing the number of redundant measurements for any single process variable reduces the overall plant complexity at critical pressure boundary penetrations. This leads to a reduction in separation requirements within the containment, as well as to a decrease in plant cost and maintenance requirements.

To obtain these advantages, measures are taken to provide the independence of the protection and control systems. The criteria for these measures are contained in IEEE 603-1991, Section 5.6.3. Isolation devices are provided to guard the protection system against possible electrical faults in the control system.

To avoid a single component failure or spurious signal causing an inadvertent plant trip while a channel is in test or maintenance, the protection and safety monitoring system uses the bypass logic discussed in subsection 7.1.2.9. This necessitates a different mechanism for achieving the functional independence of control and protection.

Functional independence of control and protection is obtained by signal selector algorithms. The purpose of the signal selector algorithm is to prevent a failed signal, caused by the failure of a protection channel, from initiating a control action that could lead to a plant condition requiring that protective action. The signal selector function provides this capability by comparing the redundant signals and automatically eliminating an aberrant signal from use in the control system. This capability exists for bypassed sensors or for sensors whose signals have diverged from the expected error tolerance.

The operation of the signal selector algorithm is described in subsection 7.1.3.2.

7.7.2 Analysis

The control system is capable of maneuvering the plant through certain reference transients. This maneuvering is done without the need for manual intervention and without violating plant protection or component limits. The plant control systems provide high reliability during these anticipated operational occurrences and meet the following objectives:

- The capability to accept 10-percent step load decreases from an initial power level between 100-percent and 25-percent of full power, and step load increase of 10-percent from an initial power level between 15-percent and 90-percent of full power without reactor trip or steam dump actuation.

- The capability to accept ramp load changes at 5-percent power per minute while operating in the range of 15-percent to 100-percent of full power without reactor trip or steam dump system actuation, subject to core power distribution limits.

- The capability to accept the design full-load rejection without reactor trip.

- The capability to accept a turbine trip from full-power operation without reactor trip. This capability is provided with the normally available systems (such as steam dump and feedwater control).

- The capability to follow the design basis network load follow pattern for 90-percent of the fuel cycle. The design basis load follow pattern is defined as the daily (24-hour period) cycle consisting of 10 to 18 hours of operation at 100-percent power, followed by a 2-hour linear ramp to 50-percent power, followed by 2 to 10 hours of operation at 50-percent power and then a 2-hour linear ramp back to 100-percent power.

- The capability to satisfy a 20-percent power increase or decrease within 10 minutes.

- The capability of handling grid frequency changes equivalent to 10-percent peak-to-peak power changes at a two percent per minute rate. This capability is provided over a 15- to 100-percent power range throughout the plant operating life. A total of 35 peak-to-peak swings per day are allowed.

The control system permits maneuvering the plant through the transients without actuation of the following:

- Steam generator safety valves
- Steam generator power operated relief valves
- Pressurizer safety valves

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

7.7.3 Combined License Information

This section has no requirement for information to be provided in support of the Combined License application.

Table 7.7-1

ROD CONTROL SYSTEM INTERLOCKS - POWER CONTROL SUBSYSTEM

Designation	Derivation	Function
C-1	2/4 neutron flux (intermediate range) above setpoint	Blocks automatic and manual control rod withdrawal
C-2	2/4 neutron flux (power range) above setpoint	Blocks automatic and manual control rod withdrawal
C-3	Margin to overtemperature ΔT (output of signal selector) below setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
C-4	Margin to overpower ΔT (output of signal selector) below setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
C-5	Turbine impulse chamber pressure (output of signal selector) below setpoint (blocked if in low-power rod control mode)	Blocks automatic control rod withdrawal
		Defeats remote load dispatching (if remote load dispatching is used)
C-11	1/1M bank control rod position above setpoint	Blocks automatic rod withdrawal
C-16	Reactor coolant system T_{avg} or (T_{avg} minus T_{ref}) signal (output of signal selector) below setpoint	Stops automatic turbine loading until condition clears
P-17	2/4 negative flux rate below setpoint	Blocks automatic rod withdrawal

Table 7.7-2

ROD CONTROL SYSTEM INTERLOCKS - AXIAL OFFSET CONTROL SUBSYSTEM

Designation	Derivation	Function
C-1	2/4 neutron flux (intermediate range) above setpoint	Blocks automatic and manual axial offset control rod withdrawal
C-2	2/4 neutron flux (power range) above setpoint	Blocks automatic and manual axial offset control rod withdrawal
C-5	Turbine impulse chamber pressure (output of signal selector) below setpoint	Blocks automatic axial offset control rod withdrawal and insertion
C-15	1/1 bank AO control rod position below setpoint	Blocks automatic axial offset control rod insertion
C-17	1/1M bank control rod position below setpoint	Blocks automatic axial offset control rod withdrawal
C-18	1/1M bank control rod position above setpoint	Blocks automatic axial offset control rod insertion
---	Power control rods moving in	Blocks automatic axial offset control rod insertion and withdrawal
---	Power control rods moving out	Blocks automatic axial offset control rod insertion and withdrawal
---	Power control rods in manual	Blocks automatic axial offset control rod insertion and withdrawal
P-17	2/4 negative flux rate below setpoint	Blocks automatic axial offset control rod withdrawal

Table 7.7-3 (Sheet 1 of 3)

CROSS REFERENCE TABLE FOR DEFENSE-IN-DEPTH FUNCTIONS SUPPORTED BY THE PLANT CONTROL SYSTEM

Supported System	Defense-in-Depth Function	DCD Section	DCD Figure
Component Cooling Water (CCS)	Provides cooling for normal residual heat removal system heat exchangers and pumps when the reactor coolant system pressure and temperature are below 450 psig and 350°F.	9.2.2.1.2.2 9.2.2.4.3	9.2.2-2
Component Cooling Water (CCS)	Provides cooling for the miniflow heat exchangers of the chemical and volume control system makeup pumps.	9.3.6.3.1	9.2.2-2
Component Cooling Water (CCS)	Provides cooling for the spent fuel pool heat exchangers for heat removal from the spent fuel pool.	9.2.2.1.2.3	9.2.2-2
Chemical and Volume Control (CVS)	Supply makeup and boration to the reactor coolant system.	9.3.6.7	9.3.6-1
Chemical and Volume Control (CVS)	Supply coolant to the pressurizer auxiliary spray line.	9.3.6.4.5	9.3.6-1
Standby Diesel and Auxiliary Boiler Fuel Oil (DOS)	Supply fuel to the onsite standby power diesel generators.	9.5.4	9.5.4-1
Main and Startup Feedwater (FWS)	Provide startup feedwater for heat removal from the reactor coolant system (startup feedwater).	10.4.9.1.2	10.4.7-1 10.3.2-1
Normal Residual Heat Removal (RNS)	Remove heat from the reactor coolant system during shutdown operation at reduced pressure and temperature.	5.4.7.1.2.1	5.4-7
Normal Residual Heat Removal (RNS)	Provide low temperature overpressure protection for the reactor coolant system.	5.4.7.1.2.5	5.4-7
Normal Residual Heat Removal (RNS)	Provide low-pressure makeup to the reactor coolant system and remove heat from the reactor coolant system following actuation of the automatic depressurization system.	5.4.7.1.2.4 5.4.7.4.4	5.4-7

Table 7.7-3 (Sheet 2 of 3)

CROSS REFERENCE TABLE FOR DEFENSE-IN-DEPTH FUNCTIONS SUPPORTED BY THE PLANT CONTROL SYSTEM

Supported System	Defense-in-Depth Function	DCD Section	DCD Figure
Spent Fuel Pool Cooling (SFS)	Provide for heat removal from the spent fuel stored in the spent fuel pool by pumping the water from the pool through a heat exchanger, and then returning the water to the pool.	9.1.3.2	9.1-8
Steam Generator (SGS)	Provide decay heat removal capability during shutdown operations by delivery of startup feedwater flow to the steam generator and venting of steam from the steam generators to the atmosphere via the power-operated relief valves.	10.4.9 10.3	10.4.7-1 10.3.2-1
Service Water (SWS)	Provide the capability for removing heat from the component cooling water system.	9.2.1.1.2	9.2.1-1
Service Water (SWS)	Provide the capability for removing heat from the spent fuel pool via the spent fuel cooling and component cooling water systems.	9.2.2 and Table 9.2.2-2	9.2.2-1 9.2.2-2
Service Water (SWS)	Provide the capability for decay heat removal at shutdown conditions through the normal residual heat removal and component cooling systems.	9.2.2 and Table 9.2.2-2	9.2.2-1 9.2.2-2
Nuclear Island Nonradioactive Ventilation (VBS)	Provide ventilation and cooling to the main control room envelope, Class 1E instrumentation and control rooms, Class 1E dc equipment rooms, and Class 1E battery rooms.	9.4.1	9.4.1-1 all sheets
Containment Hydrogen Control (VLS)	Provide hydrogen igniters to control hydrogen concentration in excess of the recombiner capability.	6.2.4	N/A
Central Chilled Water (VWS)	Provide chilled water to support the nuclear island nonradioactive ventilation system cooling of the main control room envelope, Class 1E instrumentation and control rooms, Class 1E dc equipment rooms, and the Class 1E battery rooms.	9.2.7	9.2.7-1 sheets 6 & 7
Central Chilled Water (VWS)	Provide chilled water to support the cooling functions of the compartment unit coolers for the normal residual heat removal system pump.	9.2.7	9.2.7-1 sheets 6 & 7

Table 7.7-3 (Sheet 3 of 3)

CROSS REFERENCE TABLE FOR DEFENSE-IN-DEPTH FUNCTIONS SUPPORTED BY THE PLANT CONTROL SYSTEM

Supported System	Defense-in-Depth Function	DCD Section	DCD Figure
Central Chilled Water (VWS)	Provide chilled water to support the cooling functions of the compartment unit coolers for the chemical and volume control system makeup pump.	9.2.7	9.2.7-1 sheets 6 & 7
Annex/Auxiliary Building Nonradioactive Heating and Ventilation (VXS)	Provide ventilation of the electrical switchgear rooms that contain the diesel bus switchgear. Provide ventilation of the equipment room that contains the switchgear room air-handling units.	9.4.2	9.4.2-1 sheets 3, 4, 5, and 6
Diesel Generator Building Heating and Ventilation (VZS)	Provide ventilation and cooling of the diesel generator building, and ventilation and heating of the diesel oil transfer module enclosure to support operation of the onsite standby power system.	9.4.10	9.4.10-1
Onsite Standby Power (ZOS)	Supply ac power to the Class 1E dc and UPS system.	8.3 and Table 8.3.1-2	8.3.1-2
Onsite Standby Power (ZOS)	Supply ac power to selected electrical components of the plant defense-in-depth, nonsafety-related systems.	8.3 and Table 8.3.1-2	8.3.1-2