7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

The general objectives of the non-safety instrumentation and control (I&C) systems are:

- To make sure the major process variables of the nuclear steam supply system (NSSS) are kept in pre-defined and allowed ranges during normal power operation.
- To limit the variation of process parameters during normal operation in such a way that the initial conditions for operation are met at the onset of design basis events (DBE) as assumed in the safety analyses.
- To minimize the need for protective actions and thus increase plant availability.
- To provide the reactor operator with monitoring instrumentation that indicates the required input and output control parameters of the systems and provide the operator with the capability of assuming manual control of the system.

7.7.1 DESCRIPTION

This section provides a description on the major non-safety I&C system used to implement non-safety functions.

The non-safety functions are categorized as follows:

- Operational I&C functions.
- Limitation I&C functions.

Operational I&C functions provide control of plant systems during normal operation. These functions are used to make sure the major process variables of the NSSS are kept in predefined and allowed ranges during normal power operation. These functions are described in Section 7.7.2.1 and Section 7.7.2.2.

Limitation I&C functions are functions that execute one or more of the following actions:

- Prevents plant disturbances from causing normal operating limits to be exceeded.
- Alerts the operator when normal operating limits have been exceeded.
- Prevents disturbances from leading to a DBE.

Limitation I&C functions are described in Section 7.7.2.3.

Some operational I&C functions have a minor direct influence on the process of nuclear power generation. These functions are presented in Section 7.7.2.4 and are listed in Table 7.7-1—Cross Reference of Non-Safety Controls.

7.7.1.1 I&C Systems Related to Core Control

The I&C systems that provide core-control functions are the reactor control, surveillance and limitation (RCSL) system, the process information and control system (PICS), and the control rod drive control system (CRDCS). The architecture of RCSL, PICS, and CRDCS are described in Section 7.1.

The RCSL system implements the automation level I&C functions related to core control. PICS interfaces with the RCSL system to provide the operator with control and monitoring capability of the core control functions.

The CRDCS controls the movement of the rod cluster control assemblies (RCCA) in the reactor pressure vessel (RPV) by providing sequenced control current to the stationary gripper, moveable gripper, and lift coils of the control rod drive mechanism (CRDM) to move its respective RCCA. The logic that generates the control current comes from the RCSL System. The CRDCS converts the demands from RCSL into rod movement current sequences supplied to the coils of the CRDM.

The CRDCS provides the interface to the operating coils of the CRDMs. The CRDCS controls and measures the current to each CRDM coil. There is a module in the CRDCS for each CRDM coil. This controls the amount of current applied, as well as provides the correct sequencing of coil currents for control rod movement in or out of the core. A detailed description of the CRDM and its associated operating coils is provided in Section 3.9.4.

The rod control unit of the CRDCS provides the interface with the RCSL system for control of the RCCAs. The RCSL system transmits the movement direction and speed of the RCCA to the rod control unit of the CRDCS. Each rod control unit generates the cycling sequence and rod speed for one RCCA, which is used as the input to the coil modules. A feedback signal from the rod control unit to the RCSL system provides information necessary for digital position indication of the RCCA based on the number of rod movement steps sent to the RCCA. Adjustments to boron concentration levels in the reactor coolant system (RCS) provide another means of core control. Boron addition and dilution demand signals are generated by RCSL and are sent to the chemical and volume control system (CVCS). Boron concentration adjustments are addressed in Section 9.3.4.

The operational I&C functions related to core control are described in Section 7.7.2.1. The limitation I&C functions related to core control are described in Section 7.7.2.3.1 through Section 7.7.2.3.10.

7.7.1.2 I&C Systems Related to Plant Control

The I&C systems that provide control of plant parameters are the process automation system (PAS) and the PICS. The PAS implements the automation level I&C functions related to the control of the plant parameters. The architecture of PAS is described in Section 7.1. The PICS interfaces with PAS to provide operator control and monitoring capability of plant parameters.

The operational I&C functions related to plant parameters are described in Section 7.7.2.2. The limitation I&C functions related to plant parameters are described in Section 7.7.2.3.11 through Section 7.7.2.3.14.

7.7.2 Design Basis Information

The design basis for the non-safety I&C systems are based on the functions described in this section.

7.7.2.1 Operational Core Control Functions

7.7.2.1.1 Principles of RCCA Control

A description of some of the principles of RCCA control is necessary to aid in the explanation of the core control functions.

Bank Descriptions

The RCCAs are divided into control banks that are used as control elements for the average coolant temperature (ACT) control function, axial offset (AO) control function, and the neutron flux control function. Shutdown banks are only used for negative reactivity insertion during a reactor trip. The 89 RCCAs have the same characteristics.

The bank composition is as follows:

- Control Bank D contains two sub-banks. Sub-bank D_1 contains 5 RCCAs and sub-bank D_2 contains 4 RCCAs.
- Control Bank C contains two sub-banks. Sub-bank C_1 contains 4 RCCAs and sub-bank C_2 contains 8 RCCAs.
- Control Bank B contains 12 RCCAs.
- Control Bank A contains 8 RCCAs.
- Shutdown Bank SA contains 20 RCCAs.
- Shutdown Bank SB contains 12 RCCAs.

- Shutdown Bank SC contains 16 RCCAs.

The bank name allocation is definable on a cycle by cycle basis. RCCA bank composition is subject to change based on the core operating limits report (COLR) requirements. The COLR is addressed in Chapter 16, Section 1.1.

Bank Sequence and Overlap

The rods move in the bank configuration for all cases except in the case of the partial trip (PT). In a PT, the sub-bank of rods that are dropped is a function of rod worth and relative position in the core.

The bank insertion and withdrawal sequence and overlap are defined by the control bank insertion limits. Control rod banks are withdrawn and inserted in a prescribed sequence and overlap. For withdrawal, the sequence is shutdown SA, shutdown SB, shutdown SC, control A, control B, control C, and control D. The insertion sequence is the reverse of the withdrawal sequence. The control bank rods move in a prescribed overlap that is specified in the COLR. This means that during bank withdrawal, control B will begin withdrawal before control A is fully withdrawn and likewise for control C and control D. Conversely, control C will begin insertion before control D is fully inserted and likewise for control B and control A.

7.7.2.1.2 Average Coolant Temperature Control

The ACT control function is designed to maintain a programmed average RCS average temperature (Tavg) by regulating core power. The ACT control is the predominant function of core control. The control logic is illustrated in Figure 7.7-1—Average Coolant Temperature Control Logic and consists of the following four main elements:

- The mismatch between turbine generator load and reactor power (i.e., power imbalance feed forward).
- The formation of the ACT control setpoint based on power level.
- The difference between the measured average RCS temperature and the desired average temperature (i.e., temperature error).
- The relationship between the sum of the two error signals and the resulting rod movement actuation requests.

The ACT setpoint serves as an input to determine the temperature error. The setpoint follows the ACT versus the power relationship as shown in Figure 4.4-7.

The ACT control function consists of two main error signal channels which are summed to provide a total error input signal to the rod speed control program. The rod speed program is shown in Figure 7.7-2—Rod Speed Control Program. The rods that are used to perform this function are designated as control bank rods that move into or out of the core in a prescribed manner, referred to as sequence and overlap that is followed during insertion or withdrawal. The signal output of the rod speed program is a digital pulse that determines both rod stepping speed and direction (i.e., insertion or withdrawal). The two error channels are:

- Average temperature error - Difference between the 2nd highest (auctioneered) measured loop Tavg and the ACT setpoint.
- Power imbalance feed-forward error - Mismatch between turbine generator load and reactor power.

The power imbalance feed-forward error signal and the temperature error signal are combined additively to produce a total error signal. This total error signal is the output that determines whether the control rods need to be inserted or withdrawn and the speed at which the movement needs to occur. If the total error is negative, rods are withdrawn. If the total error is positive, rods are inserted. The rod speed control program determines the rod movement as a function of total temperature error. Likewise when rod movement is prohibited and the total error is positive a boron addition batch will be performed, and when rod movement is prohibited and the total error is negative a dilution batch will be performed.

If the total error exceeds a high level setpoint any ongoing turbine power increase or decrease will be placed on hold until the total error is less than the reset value (within the capability of the rods and boron addition and dilution systems).

This function uses the rod banks (i.e., first priority) and boron addition and dilution batches (i.e., second priority) as final control elements. The ACT has to be controlled even if bank movement is not allowed due to AO control limits.

ACT Control using Boron Addition and Dilution

If an AO limit is encountered the system will automatically switch to boron addition and dilution batches as the method to perform the ACT function.

When control bank D reaches a reference position, this control automatically switches from controlling ACT using control bank movement as a first priority to boron addition and dilution batches as the first priority. The reference position is specified in the COLR. In this mode, boron addition and dilution is the preferred temperature control but control will automatically revert to control bank movement if the temperature error signal reaches the error signal limit established for rod control.

When Tavg is less than the ACT setpoint and rod movement is restricted, it is necessary to dilute to restore Tavg. The dilution batches are of XD gallons at a rate of YD gallons per minute that are followed by ZD minutes waiting time between the completion of one batch and the initiation of a subsequent dilution batch. Each of these constants, XD, YD, and ZD, are set by the operator and are expected to change frequently depending on core burnup.

When Tavg is greater than the ACT setpoint and rod movement is restricted, it is necessary to borate to restore Tavg. The boron addition batches are of XB gallons at a rate of YB gallons per minute that are followed by ZB minutes waiting time between the completion of one batch and the initiation of a subsequent boron addition batch. Each of these constants, XB, YB, and ZB, are set by the operator and are expected to change frequently depending on core burnup.

The transition between the neutron flux control function to the ACT control function occurs at 25 percent reactor power.

7.7.2.1.3 Neutron Flux Control

The neutron flux control function is designed to control reactor power (i.e., neutron flux) during startup and shutdown operations, while the secondary pressure is controlled with the turbine bypass system (TBS). This function simplifies the constant power operation and facilitates the operator tasks during the startup of the turbine and the synchronization of the generator with the grid.

In the neutron flux control mode, the control bank movements operate in the same way as under the ACT control (i.e., in sequence and overlap). This function is used below 25 percent reactor power when the secondary steam pressure is controlled with the turbine bypass valves. At higher powers the ACT control function is used instead of the neutron flux control function.

The neutron flux control setpoint can be adjusted manually by the operator using the PICS.

When the reactor is at hot shutdown with all the banks inserted, the operator begins the first stage of the startup by withdrawing the shutdown and control banks until the reactor is critical. The withdrawal sequence requires that the shutdown banks are pulled to their all rods out (ARO) position before control banks are pulled. Control banks are then withdrawn in sequence and overlap as described in Section 7.7.2.1.1.

During startup (i.e., after exceeding a low reactor power permissive P5) and shutdown operation, the reactor power (i.e., neutron flux) can be controlled in conjunction with the main steam (MS) pressure control using the turbine bypass valves. The neutron flux control function blocks turbine synchronization at power levels less than a setpoint on increasing reactor power and blocks power reductions below a setpoint until the turbine is tripped on decreasing reactor power.

The neutron flux control acts on the rod control banks in the same way as the ACT control function. The neutron flux deviation is appropriately amplified to give an output signal corresponding to that from the ACT control.

7.7.2.1.4 Axial Offset Control

The AO control function is designed to maintain core axial power within analyzed limits. AO is a measure of the axial power distribution in the core. Extreme shifts in power distributions have an adverse impact on accident analysis results. The AO limitation function described in Section 7.7.2.3.2 is also designed to maintain core axial power within analyzed limits.

Since the reactor is taken critical at a control bank D position near the core mid plane, unrestricted rod withdrawal could result in a core power profile that is shifted towards the top of the core (AO is positive).

The AO control strategy can be considered as a two phase process. In the first phase the AO control strategy implements restrictions on rod motion to attempt to control AO within a limited band about an optimum AO path to full power. The second phase of the AO control strategy takes more drastic measures to prevent the AO from remaining outside of the allowable AO limit.

During power ascension, automatic rod withdrawal is blocked when AO exceeds the first phase positive AO band limit and boron dilution becomes the only acceptable means of performing ACT control. When the first phase negative AO limit is exceeded automatic boron dilution is blocked and the only acceptable means of performing ACT control is automatic rod withdrawal. During power ascension when AO exceeds the second phase AO band limits (i.e., positive or negative), all automatic dilutions, rod withdrawal, and power increases are blocked.

During reactor down powers, the process is reversed. Automatic rod insertion is blocked when AO exceeds the first phase negative AO band limit and boron addition is the only acceptable means of performing ACT control. When the first phase positive AO band limit is exceeded automatic boron addition is blocked and the only acceptable means of performing ACT control is automatic rod insertion. During reactor down powers when AO exceeds the second phase AO band limits (i.e., positive or negative), all automatic boron addition, rod insertions, and power decreases are blocked.

Two further restrictions are placed on rod insertions:

- Automatic rod insertions are blocked below the core mid-plane.
- Rod insertions are blocked to make sure that control bank insertion limits as a function of reactor power, described in the COLR, are not violated.

7.7.2.2 Operational Plant Control Functions

7.7.2.2.1 RCS Pressure Control

The RCS pressure control maintains the RCS pressure within allowable limits during Mode 1 through Mode 5. When in the automatic control mode, the RCS pressure control maintains the primary pressure at a setpoint value in steady-state operation and within an allowable range around its setpoint (i.e., control band) during transients, including startup and cooldown operations. Figure 7.7-3—RCS Pressure Setpoints indicates the control band relative to other RCS pressure setpoints.

When the automatic heatup and cooldown mode is selected, the RCS pressure control has an automatically generated temperature dependent setpoint. The automatic heatup and cooldown mode is selected during plant Mode 2 and Mode 3. The primary pressure is required to stay in an allowable range around the automatically generated setpoint. If the pressure drifts from the limits of the setpoint, the Max2 sliding pressure limitation function described in Section 7.7.2.3.11 is actuated. If the pressure progresses further from the temperature dependent setpoint to the high pressure (HP) or low pressure (LP) locking setpoints, the automatic heatup and cooldown is interrupted, and an alarm is sent to PICS.

RCS pressure control is performed by actuating pressurizer (PZR) heaters or PZR normal spray.

A manual control mode allows manual setpoint control, and manual control of the actuators.

7.7.2.2.2 Pressurizer Level Control

The PZR level control provides:

- Sufficient RCS water inventory for cooling and for proper control of RCS pressure.
- A sufficient steam volume in the PZR to accommodate in-surges in the PZR from the RCS without causing an excessive pressure increase for normal operating transients. There is also sufficient water mass to accommodate out-surges from the PZR to the RCS without causing an excessive pressure decrease.

The function of the PZR level control is to maintain the PZR level at a setpoint value in steady-state operation and within the allowable range around its setpoints during normal operational situations, including startup and cooldown. When in automatic control mode, PZR level control channel makes sure that the PZR level remains within given limits (i.e., control band) around the setpoint. Figure 7.7-4—Pressurizer Level Setpoints indicates the control band relative to other PZR level setpoints.

The PZR level control monitors the PZR level for deviations from its setpoint during Mode 1 through Mode 4, and based on mode changes, actuates different control valves at the pressure reducing stations located in the CVCS letdown lines.

A manual control mode allows manual setpoint control and manual control of the pressure reducing valve actuators.

7.7.2.2.3 RCS Loop Level Control

The RCS loop level control function provides an automatic and continuous control of the RCS water inventory during mid-loop operation. In case of primary system inventory changes, the control function limits the resulting mid-loop operation level deviations within the specified control band.

The loop level control function provides an automatic control of RCS water inventory by continuously monitoring the RCS loop level and controlling the coolant letdown flowrate.

RCS loop level control is maintained by a closed-loop control I&C function, which is put in service manually at cold shutdown conditions.

RCS loop level control is manually activated at cold shutdown conditions. Control actions are only effective when an HP charging pump is in operation and the VCT bypass line is not opened.

7.7.2.2.4 Steam Generator Level Control

The steam generator (SG) water level control automatically maintains SG level by matching feedwater flow to steam demand. The level can also be controlled manually.

This SG level control I&C function provide the following:

- Sufficient water level for heat removal from the primary to secondary side.
- Minimizes moisture carryover to the turbine.

The SG level control I&C function maintains the SG level at a setpoint value in steady-state operation during heatup and cooldown (Mode 1 through Mode 4), and within allowable limits (called the control band) during normal operational transients. Figure 7.7-5—Steam Generator Level Setpoints illustrates the control band relative to other SG level setpoints.

This function acts on the following valves in the main feedwater system (MFWS) to control SG water level:

- Full load control valve (FLCV).

- Low load control valve (LLCV).
- Very low load control valve (VLLCV).

The system can be operated in the following modes:

- Automatic control mode which controls SG water level within given limits of a setpoint. Automatic control mode is the normal mode of operation.
- Manual control mode.

7.7.2.2.5 Main Steam Pressure Control

The purpose of the MS pressure control function is to provide MS overpressure control and limitation in case of load reduction due to load steps, load ramps, or load rejection. MS pressure is controlled by automatically modulating the turbine bypass valves.

During normal power operation, this function is realized by maintaining a floating MS pressure setpoint above the measured MS pressure. As the measured pressure changes, the setpoint changes accordingly. However, a limitation is placed on the rate of change of the setpoint so that if the measured pressure increases at a rate greater than the limitation of the floating setpoint, the turbine bypass valves will be opened. The turbine bypass valves close and are prevented from opening on high condenser backpressure or high hot well level.

During plant heatup and cooldown operations, the operator can adjust a target pressure setpoint which is adapted with a limited temperature gradient. Based on the target pressure setpoint, the turbine bypass valves control MS pressure and thus reactor coolant temperature. Locking logic is provided to interrupt the automatic heatup or cooldown process when RCS parameters deviate from their setpoint thresholds.

When partial cooldown is initiated, the MS pressure setpoint follows a specific partial cooldown setpoint which has priority over all other setpoints and locking signals.

Following a reactor trip, in order to avoid primary overcooling, the MS pressure setpoint is immediately set to a fixed maximum pressure setpoint.

7.7.2.3 Limitation I&C Functions

7.7.2.3.1 Loss of one Reactor Coolant Pump Limitation

This limitation function is designed to avoid the low reactor coolant flowrate (i.e., one loop) reactor trip function described in Section 7.2.

This function initiates a PT and a turbine load reduction when two RCS loop flow values of the same loop drop below the setpoint value and the P3 permissive is validated.

7.7.2.3.2 Axial Offset Limitation

The objective of this limitation is to survey the axial power imbalance and make sure that the axial power distribution is within the parameters assumed in the safety analysis to limit the consequences at high power levels of accidents for which a top-peaked core power distribution is penalizing. The limited parameter is the AO value calculated from the self powered neutron detectors. The AO operating range is bounded by positive and negative thresholds. This function generates alarms and the blocking of the generator power increase.

This limitation function is inhibited below a low level of power.

The calculated AO is compared with thresholds derived from reactor power. When the threshold is met an action occurs to block the increase of generator power.

7.7.2.3.3 Reactor Power Limitation with Respect to Feedwater Flow Rate

This limitation function limits the reactor power with respect to the feedwater flowrate. The limitation function is designed to correct plant conditions before a protective action due to low SG level occurs. The loss of one or more main feedwater (MFW) pumps leads to a large imbalance between power generation in the reactor and heat transfer to the main heat sink. Operational I&C will detect the failure of one pump and start a standby pump, if available, within a few seconds, thus allowing normal operation to continue.

This limitation function can handle the following three events:

- Loss of one MFW pump.
- Loss of all MFW pumps.
- Imbalance of feedwater flowrate and reactor power during startup phase.

Loss of One MFW Pump

This limitation function deals with the loss of one MFW pump by initiating a PT and a turbine load reduction. An imbalance between MFW flowrate and a nominal MFW flowrate (according to feedwater temperature and reactor power) activates a PT and a generator power reduction to a power level corresponding to operation with two MFW pumps.

Loss of All MFW Pumps

A low MFW flowrate combined with a high reactor power level is the criteria for the detection of the loss of all MFW pumps. In this case the limitation function will initiate a non-safety-related reactor trip, activate turbine trip, and close all FW FLCVs. The reactor trip signal resets this actuation.

Imbalance of Feedwater Flowrate and Reactor Power During Startup Phase

Indications of a low enough feedwater flowrate and a high enough reactor power leads to blocking the withdrawal of any RCCA. This prevents an increase of the reactor power without an increase of the MFW flowrate during the startup phase.

7.7.2.3.4 Reactor Power Limitation with respect to Generator Power

This limitation function limits reactor power after loss of generator load events. The objective is to limit the energy level of the primary system in case of load rejections or turbine trip in order to avoid reaching the RT criteria. This will be done by initiating a PT. The target reactor power level is determined by:

- The maximum of generator power.
- The minimum PT target power.

In case of turbine trip or load rejection to house load, the plant is first stabilized at minimum PT target power while heat removal is performed via the turbine bypass valves. A further controlled reduction to the minimum load reactor power will then be done by ACT control.

7.7.2.3.5 Reactor Power Limitation with respect to Thermal Power

The reactor power limitation with respect to thermal power function is designed to maintain reactor power below 100 percent rated thermal power. This function provides the capability to adjust turbine power and indirectly reactor power due to cooling tower temperature changes that affect overall plant efficiencies. The reactor power signal is selected from the highest of the following:

- Continuous secondary calorimetric calculation (i.e., above 25 percent power).
- Median select excore power range indication of reactor power.
- Median select RCS enthalpy indication of reactor power.

The control logic compares the mismatch between main turbine and generator load and the highest of the previously listed power signals and takes actions when reactor power exceeds 100 percent. There are two thresholds. The intent of the first is to alert the operator and take action to prevent further power increase. The intent of the second threshold is to reduce power to 100 percent.

7.7.2.3.6 Rod Drop Limitation

The objective of this limitation function is to detect the spurious drop of RCCA(s) and to reduce the turbine generator power level to match the reactor power reduction due to the dropped RCCAs.

This limitation function is designed to avoid reactivity compensation by core control functions after the RCCA(s) drop and to avoid the low departure from nucleate boiling (DNBR) and high linear power density (HLPD) protective actuations after one or more RCCAs drop into the core.

Rod drop is detected in the protection system (PS) based on the RCCA position measurements. In each PS division a quarter of the RCCAs are monitored. Four (i.e., one per PS division) RCCA drop detection logic signals are acquired in RCSL and voted one out of four.

The other criterion indicating an RCCA drop is derived from the decrease of the reactor power level (i.e., neutron flux from power range detectors). The derivative of the four nuclear power signals are compared with a low threshold and voted one out of four.

The limitation will be actuated if both criteria coincide and no intended PT has been initiated by other limitation functions.

7.7.2.3.7 Intermediate Range High Neutron Flux Limitation

This limitation function is designed to avoid the high neutron flux (i.e., intermediate range) and low doubling time (i.e., intermediate range) reactor trips when an excessive reactivity increase occurs during reactor startup from a subcritical or a low power startup condition. At the limitation criteria the withdrawal of any RCCA is blocked.

Each RCSL division receives four binary limitation signals (i.e., one per PS division). Each limitation signal from the PS combines the following criteria:

- Low doubling time IR limitation threshold.
- High neutron flux IR limitation threshold.
- Manual inhibition above a low power level (permissive P6).

If these criteria are met in a PS division, a vote signal is sent from that PS division to RCSL. If two out of four vote signals are received by RCSL from the PS, the following actions are performed:

- RCCA withdrawal is blocked.
- Alarm on PICS.

7.7.2.3.8 High Linear Power Density Limitation

There are three sub-functions to the HLPD limitation function. The three sub-functions are:

- Block function.
- Reduction function.
- PT function.

The HLPD limitation sub-functions are designed to avoid a reactor trip on HLPD for each transient that leads to an uncontrolled increase of the linear power density of the reactor core. This function initiates a PT and a fast turbine load reduction.

For the block and reduction sub-functions, a calculation of the linear power density (LPD) in the lower and upper portions of the core is performed in RCSL. In each sub-function the calculated LPD values for the upper and lower portions of the core are compared to threshold levels for each portion of the core. The self-powered neutron detectors (SPND) provide input for the calculation of the LPD values in RCSL.

The threshold levels for the block sub-function are above the threshold levels for the reduction sub-function, and therefore, the block sub-function actuates before the reduction sub-function.

Violation of the block sub-function threshold levels results in the following actions:

- Block dilution signal (for lower core half threshold level violation only).
- RCCA bank withdrawal blocking signal.
- Generator power increase blocking signal.
- Block lead control bank insertion (for lower core half threshold level violation only).

Violation of the reduction sub-function threshold levels results in the following actions:

- Reduce generator power signal.
- Insert lead control bank (for upper core half threshold level violation only).

For the PT sub-function, the actuator logic signals are generated in the PS and are inhibited below a low power level by permissive P2. Each division of the PS provides a vote input to the two out of four voting logic in RCSL. When two votes for the PT sub-function are received by RCSL, the following actions are performed:

- PT.
- Turbine load reduction.

7.7.2.3.9 Low Departure from Nucleate Boiling Limitation

There are three sub-functions to the low DNBR limitation function. The three sub-functions are:

- Block function.
- Reduction function.
- PT function.

These functions are designed to correct conditions to avoid the low DNBR protective functions as described in Section 7.2. The functions provide DNBR margin with respect to the DNB criterion.

For the block and reduction sub-functions, a calculation of the minimum DNBR value is performed in RCSL. The following are the inputs for the calculation of the minimum DNBR value in RCSL:

- Power density distribution of the hot channel which is derived from SPNDs.
- Average reactor inlet temperature.
- Average PZR pressure.
- Core flowrate derived from average RCP speed.

The threshold level for the block sub-function is above the threshold level for the reduction sub-function, and therefore, the block sub-function will actuate before the reduction function.

If the DNBR value drops below the threshold for the block sub-function, the following actions are performed:

- Alarm in the main control room (MCR).
- Block RCCA withdrawal.
- Block generator power increase.

If the DNBR value drops below the threshold for the reduction sub-function, the following actions are performed:

- Reduce generator power setpoint.
- Insert RCCAs.

The actuator logic signals for the low DNBR PT limitation sub-function are generated in the PS and are inhibited below a low power level by permissive P2. Each division of the PS provides a vote input to the two out of four voting logic in RCSL. When two votes for the low DNBR PT limitation function are received by RCSL, the following actions are performed:

- PT.
- Turbine load reduction.

7.7.2.3.10 RCS Dilution (Shutdown Condition) Limitation

This limitation function is designed to avoid the actuation of the antidilution in standard shutdown states protective function as described in Section 7.3. This function contains the following sub-functions:

- Limitation in case of low RCS boron concentration.
- Prevent dilution at shutdown.

In the first sub-function, the RCS boron concentration is calculated in the PS based on boron meter measurements and on charging flowrate measurements. This value is compared to the permissible shutdown state boron concentration. The low concentration limitation threshold is generated in the PS at a higher threshold than the antidilution at a shutdown condition state protection criterion. Four redundant limitation signals from the PS are transferred to RCSL. When the two out of four voting is fulfilled in RCSL, the following actions are initiated:

- Boron addition with maximum injection rate.
- Isolation of demineralized water injection lines of the reactor boron and water makeup system (RBWMS). Both demineralized water injection pumps are shut off and both control valves are closed with highest priority.

The second sub-function is activated when shutdown conditions are detected (reactor trip or no RCPs running). In this sub-function, boron concentration injected by RBWMS is measured. If the injected concentration is below the permissible value then the demineralized water injection lines will be isolated.

7.7.2.3.11 Reactor Coolant System Pressure Limitations

When the RCS pressure goes out of the normal operating range, the following RCS pressure limitation functions can be activated. These functions are designed to correct RCS pressure transients before a RT setpoint is reached, or to protect equipment. These functions have a more stringent action than the RCS pressure control function as described in Section 7.7.2.2.1. A graphical presentation of the RCS pressure limitation setpoints in relation to protective function setpoints and the control band is presented in Figure 7.7-3.

In case of postaccident operations, the operator is able to inhibit the activation of the RCS pressure limitation functions from PICS.

Max2 Pressure Function

The Max2 pressure function improves the availability of the plant by avoiding an RT on the Max2p setpoint (i.e., high PZR pressure). When the RCS pressure measurement reaches the setpoint, this function de-energizes the PZR heaters and actuates the normal spray. If the normal spray is not functional, auxiliary spray is actuated. The normal spray availability is determined based on RCP speed or the loop flowrate.

This function is operational in Mode 1 through Mode 3.

Max2 Sliding Pressure Function

The Max2 sliding pressure function improves plant availability by preventing a lock of the automatic heatup and cooldown on Max2p and limits the temperature differences between the PZR and RCS loops. The Max2 sliding pressure function is similar to the Max2 pressure function except this function has an automatically generated temperature dependent setpoint and is operational during the automatic heatup and cooldown.

When the pressure measurement reaches the setpoint, this function de-energizes the PZR heaters and actuates the normal spray. If the normal spray is not functional, the auxiliary spray is actuated. The normal spray availability is determined based on RCP speed or the loop flowrate.

Residual Heat Removal System Function

The RHRS function protects the RHRS equipment from overpressurization and prevents challenging the PZR safety relief valves (PSRV) during low temperature operation. The setpoint for the RHRS function is below the RHRS maximum pressure. This function is similar to the Max2 pressure function except the setpoint is temperature dependent and the function is operational during Mode 4 through Mode 6 when the P14 permissive has been acknowledged. The RHRS is normally connected to the RCS for decay heat removal when the P14 permissive process parameter setpoints are met and the P14 permissive has been acknowledged by the operator.

When primary pressure reaches the RHRS function setpoint, this function de-energizes the PZR heaters and actuates normal spray. If the normal spray is not working properly, the auxiliary spray is actuated. The unavailability of the normal spray is detected by RCP speed or the loop flowrate.

Reactor Coolant Pump Function

The reactor coolant pump (RCP) function avoids a RT on Min2p (i.e., low PZR pressure) during Mode 1. It also protects RCPs from cavitation and keeps pressure from falling below the Min3p setpoint for initiation of safety injection. The RCP function setpoint is temperature dependent and below the nominal operating pressure setpoint of the RCS pressure control function. The function is operational in Mode 1 through Mode 5.

When pressure reaches the RCP function setpoint, the function secures the PZR spray and energizes PZR heaters.

Reactor Pressure Vessel Brittle Fracture Function

At low RCS temperatures, the PSRVs opening setpoint is lowered to protect the RCS from overpressurization. The lowering of the PSRV opening setpoints is performed by the PS and is described in Section 7.3. The RPV brittle fracture function is implemented in the PAS to prevent pressure from reaching the electrically controlled PSRV open setpoints when in Mode 4 and Mode 5. The RPV brittle fracture setpoint is temperature dependent.

When the pressure measurement reaches the setpoint of the function, the RPV brittle fracture function stops the CVCS charging pumps, the medium head safety injection (MHSI) pumps, the extra borating system pumps, and de-energizes the PZR heaters. If the MHSI pumps are running due to a safety function actuation, the MHSI pumps will continue to run.

7.7.2.3.12 Pressurizer Level Limitations

The PZR level limitation functions are designed to backup the normal PZR level control function when the normal control function is outside of its normal control band. This process is achieved by performing actions that supplement the normal control function to return the RCS to the 100 percent power, level control band following a transient that caused the deviation. This improves the availability of the plant by correcting PZR level before reaching RT setpoints and other safety protective function setpoints. A graphical presentation of the PZR level limitation setpoints in relation to protective function setpoints and the control band is presented in Figure 7.7-4.

Max2 Level Function

The Max2 level function avoids overfilling the PZR and flooding the PZR spray nozzles. It improves the availability of the plant by correcting PZR level before reaching the Max1p RT setpoint (i.e., high PZR level) in Mode 1 and Mode 2. When the PZR level reaches the Max2 level setpoint, this function isolates the injection coming from the charging line and the auxiliary spray, thus limiting the increase of PZR level. When the PZR level returns below the Max2 level setpoint, the activating signal is withdrawn and the normal PZR spray is realigned for RCS pressure control. Furthermore, the charging line isolation valve and the auxiliary spray line isolation valve remain closed; however, the operator can manually reopen the valves. An alarm on PICS indicates that the Max2 level function has been actuated.

This function is operational in Mode 1 through Mode 4.

In case of postaccident operations, the operator is able to inhibit the activation of this function from PICS.

Δ Max Function

The Δ Max function improves the availability of the plant by correcting PZR level before reaching the RT setpoint on Max1p (i.e., high PZR level). This function acts before reaching the Max2 level setpoint. The Δ Max level setpoint corresponds to a certain percentage above the PZR level control function setpoint. When the PZR level reaches the Δ Max level setpoint, this function adjusts the letdown flowrate at the HP reducing stations of CVCS to the maximum flowrate limit. An alarm on PICS indicates that the Δ Max level function has been actuated. When the PZR level returns below the Δ Max level setpoint, the activating signal is withdrawn and the HP reducing station returns to automatic PZR level control.

This function is operational in Mode 1 through Mode 5 when RCS temperature is greater than approximately 140°F and an HP reducing station of the CVCS is in operation.

In case of postaccident operations, the operator is able to inhibit the activation of this function from PICS.

Δ Min Function

The Δ Min function improves the availability of the plant by correcting PZR level before reaching the RT setpoint on Min2p (i.e., low PZR pressure). This function acts before reaching the Min2 level setpoint. The Δ Min level setpoint corresponds to a certain percentage below the PZR level control function setpoint. When the PZR level reaches the Δ Min level setpoint, this function increases the water injection into the RCS to the maximum possible flowrate by starting a second CVCS pump and adjusting the HP reducing station to the minimum flowrate limit. An alarm on PICS indicates that the Δ Max level function has been actuated. When the PZR level returns above the Δ Min level setpoint, the activating signal is withdrawn and the HP reducing station returns to automatic PZR level control. The CVCS charging pumps continue to run, however, the operator has the capability to manually stop a pump.

This function is operational in Mode 1 through Mode 5 when RCS temperature is greater than approximately 140°F and a HP reducing station of the CVCS is in operation.

In case of postaccident operations, the operator is able to inhibit the activation of this function from PICS.

Min2 Level Function

The Min2 level function avoids emptying the PZR, thus avoids activating the emergency core cooling criteria. When the PZR level reaches the Min2 function level, this function isolates the CVCS letdown lines and thus limits the decrease of RCS water inventory. An alarm on PICS indicates that the Min2 level function has been actuated. When the PZR level returns above the Min2 level setpoint, the activating signal is withdrawn, but the CVCS letdown lines remain isolated; however, the operator has the capability to manually reopen the letdown lines.

This function is operational in Mode 1 through Mode 5 when RCS temperature is greater than approximately 140°F and an HP reducing station of the CVCS is in operation.

In case of postaccident operations, the operator is able to inhibit the activation of this function from PICS.

Min3 Level Function

The Min3 level function protects the PZR heaters from being uncovered and is designed to prevent severe damage to the PZR heaters and also a potential breach of the RCS. When the PZR level reaches the Min3 function level setpoint, the PZR heaters are de-energized. An alarm on PICS indicates that the Min3 level function has been actuated. When the PZR level returns above the Min3 level setpoint, the PZR heaters are automatically switched back to RCS pressure control.

This function is operational during all plant modes.

The Min3 level function cannot be inhibited.

7.7.2.3.13 Reactor Coolant System Loop Level Limitation

The RCS loop level limitation function continuously monitors the loop level during mid-loop operation.

The RCS loop level limitation function makes sure that the minimum and maximum admissible water levels are in the RCS loops in case of transients. This limitation function acts when an overshoot of the control band limit occurs. This function prevents the actuation of safety functions by the PS.

The RCS loop level limitation function considers the water level required to protect the low head safety injection (LHSI) pumps from cavitation during mid loop operation.

This limitation function also prevents inadvertent filling of the loops. Filling the loops interrupts the flow area for the purge gas in the loop and the necessary free water surface for removal of noble gas. This could endanger personnel working in the SG bowls, and could potentially discharge coolant to the containment via open SG manways.

The RCS loop level limitation function fully closes the LP and HP reducing station of the CVCS letdown line when the RCS water level falls below a dedicated threshold that is below the lower control band limit of the RCS loop level control function. This limitation function fully opens the LP reducing stations to increase the coolant letdown flowrate when the water level exceeds a dedicated threshold above the upper control band limit of the RCS loop level control function. Both the upper and lower thresholds of this function are constant.

The limitation function is automatically activated during the plant shutdown procedure when the operating range of the LHSI RHRS is reached.

The RCS loop level limitation function is disabled beyond its specified operating range in order to exclude the occurrence of inadvertent actuation signals.

7.7.2.3.14 Steam Generator Level Limitations

The SG level limitation functions are non-safety-related functions designed to correct SG level transients before a protective function setpoint is reached. A graphical presentation of the SG level limitation setpoints in relation to protective function setpoints and the control band is presented in Figure 7.7-5.

In the case of postaccident operations, the operator is able to inhibit the SG level limitation functions from PICS.

High SG Level Limitation Function

The high SG level limitation function avoids RT at MAX 1p and returns the SG level to its normal operating range. It has higher priority over the SG level control function described in Section 7.7.2.2.4.

This function is operable in Mode 1 through Mode 4.

The high SG level limitation function receives input from the narrow range SG level and the FLCV position. Two setpoints, MAX c1 and MAX c2, are set between the SG level control function setpoint and the safety setpoint MAX 1p, with MAX c2 higher than MAX c1. The LLCV and the FLCV in the MFWS are actuated depending on the SG level with respect to the MAX c1 and MAX c2 setpoints.

If SG level is greater than the MAX c1 setpoint, a close order is sent to the FLCV first. If the FLCV position is below a certain position and the SG level is still above the MAX c1 setpoint, then a close order is also sent to the LLCV. A close order to both the FLCV and the LLCV remain as long as the SG level is greater than the MAX c1 setpoint.

If the SG level is greater than the MAX c2 setpoint, close orders are immediately sent to both the FLCV and the LLCV regardless of their initial positions. When the water level is reduced to the intermediate region between MAX c2 and MAX c1, the close order is sent to the FLCV if it is not totally closed yet, while the LLCV would remain in its current position. When the FLCV is nearly closed, the LLCV will also be allowed to close.

The close orders to the FLCV and the LLCV will remain as long as the SG level is above the MAX c1 setpoint.

Low SG Level Limitation Function

The low SG level limitation function avoids RT at MIN 1p and returns the SG level to its normal operating range. This function has higher priority over the SG level control function described in Section 7.7.2.2.4.

This function is operable in Mode 1 through Mode 4.

This function receives input from SG Level NR and reactor power.

The low SG level limitation function defines a movable setpoint MIN c1, set at a constant distance below the SG level control function setpoint and above the safety setpoint MIN 1p. The MIN c1 setpoint is designed to be movable at a constant distance from the SG level control function setpoint to prevent undesired actuation of the low SG level safety function during SG level setpoint reduction before an RCP restart.

When the SG level is less than MIN c1 and reactor power is less than 20 percent, an open order is sent to the LLCV. SG level is controlled by the LLCV at this power level. The open order to the LLCV is maintained as long as the water level is less than the MIN c1 setpoint. Once the level increases above than MIN c1 setpoint, the control of the LLCV returns back to the automatic control mode.

When the SG level is less than MIN c1 and reactor power is greater than 20 percent, an open order is sent to the FLCV and the LLCV. The open orders are maintained to both valves as long as the water level is less than the MIN c1 setpoint. Once the level increases above than MIN c1 setpoint, the control of the FLCV and the LLCV return back to the automatic control mode.

Very Low Flow SG Level Limitation Function

The very low flow SG level limitation function deactivates the VLLCV electronic stop and returns the SG level to the normal operating range. It has higher priority over the SG level control function described in Section 7.7.2.2.4.

This function is operable in Mode 2 and Mode 3.

The very low flow SG level limitation function deactivates the VLLCV electronic stop which provides the minimum position limitation during the startup and shutdown phases. The FLCV and LLCV are manually closed during Mode 2 and Mode 3 and therefore the FLCV and LLCV are not controlled by this limitation function.

To prevent water hammer and thermal stratification phenomena on the SG feedwater nozzle, the VLLCV electronic stop guarantees a minimum continuous feedwater flowrate by preventing the VLLCV from closing below the minimum flow position. However, this could potentially cause a high water level in the SG.

When the SG level is greater than the MAX c1 setpoint, the VLLCV electronic stop is deactivated and close orders are sent to the VLLCV. Once the SG level drops below the MAX c1 setpoint, the VLLCV returns to the automatic control mode.

7.7.2.4 Non-Safety Control Systems Described in Other Sections

Table 7.7-1 provides a cross-reference to other sections of the final safety analysis report (FSAR) that contain information on I&C that support non-safety-related functions. The functions listed in Table 7.7-1 do not have direct influence on the process of nuclear power generation.

7.7.2.5 Safety Classification

The I&C systems described in Section 7.7.1.1 and Section 7.7.1.2 are non-safety related. The functions that these systems implement provide control of important parameters, but are not necessary to show protection against DBEs.

7.7.2.6 Effects of Control System Operation Upon Accidents

The effects of non-safety control system action and inaction on the transient response of the plant for accidents and AOOs are considered in the safety analysis addressed in Chapter 15.

The non-safety control functions make sure that the major process variables of the NSSS are kept in predefined and allowed ranges during normal power operation and AOOs, but the proper operation of the non-safety control functions is not necessary to provide protection against accidents.

7.7.2.7 Effects of Control System Failures

The effects of control system failures are minimized by the features described in this section.

Functions assigned to RCSL and PAS are redundant in more than one division. The failure of a function in one division is backed up by a redundant function in another division. The redundant functions and their associated equipment, including support systems are independent of each other. Independence is achieved by the following:

- Redundant functions are allocated to physically separated divisions.
- Electrical isolation between divisions.
- Erroneous signals or messages from one faulty division do not impair the functionality of the remaining divisions.

The primary source of power to the RCSL and PAS is provided by a battery backed source. The secondary power source is from a separate battery backed source fed from a different power bus. Upon loss of the primary source of power to PAS or RCSL, the secondary power source automatically and without interruption, maintains power. In case of a total loss of power to the plant, the battery source permits continued operation of the plant controls for a two hour period.

Segregation of functions is provided by allocating functions related to core control in the RCSL and functions related to RCS parameters in the PAS. Failures of components in one non-safety system do not effect the functioning of the other non-safety system.

Data communication between the non-safety systems and other I&C systems is electrically isolated.

Control system failures are considered as event initiators in the safety analysis described in Chapter 15.

7.7.2.8 Environmental Control System

Environmental controls are provided to protect equipment from environmental extremes. Heating, ventilation, and air conditioning (HVAC) is provided to maintain ambient conditions in a range acceptable for proper operation of I&C equipment. Section 9.4 provides details on HVAC functions that maintain ambient temperature control where I&C equipment is located.

7.7.2.9 Independence

Electrical isolation and communication independence between safety and non-safety systems is provided by components of the safety I&C systems. Electrical isolation and communication independence is further described in Section 7.1.

7.7.2.10 Interactions between Safety and Non Safety I&C Systems

The non-safety control systems use signal selection algorithms to calculate a process representation value which is then used by the non-safety control system to take action. The calculated value reflects all the input signals and not a specific signal value. This technique provides fewer challenges to safety-related I&C systems due to non-safety control system failure.

7.7.2.11 Defense in Depth and Diversity

A methodology used to evaluate the adequacy of I&C design with respect to diversity and defense-in-depth is presented in the AREVA Instrumentation and Controls Diversity and Defense-in-Depth Methodology Topical Report (Reference 1). Non-safety functions that are designed to provide diverse protective functions are described in Section 7.8.

7.7.2.12 Potential for Inadvertent Actuation

The non-safety control systems and functions are designed to limit the potential for inadvertent actuation and challenges to the safety systems. Many of the limitation I&C functions described in Section 7.7.2.3 are designed to achieve optimum plant availability. These types of limitation functions act before protection functions, and thus restore normal operating conditions without challenging the protection thresholds for the most frequent accident conditions. The limitation thresholds are set before protection thresholds (as close as possible to them), but with a margin taking into account the counter-measure response time. After exceeding a limitation threshold, rapid corrective actions are automatically initiated. The typical limitation function action is the RCCA dropping called the PT which leads to a fast power decrease.

7.7.2.13 Control of Access

Physical access to I&C cabinets is restricted to authorized personnel. Unauthorized electronic access to system software via network connections is prevented by administrative controls. The loading of software and parameter changes via maintenance equipment is only possible in accordance with clearly defined procedures.

7.7.3 Analysis

The control systems described in Section 7.7.1.1 and Section 7.7.2.1 are those used for normal operation that are not relied upon to perform safety functions following AOOs or accidents, but these systems control plant processes having a significant impact on plant safety.

The plant control systems attempt to prevent an undesirable condition in the operation of the plant that, if reached, is protected by the PS. The description and analysis of this protection is covered in Section 7.2 and Section 7.3. Worst-case credible failures of the plant control systems are postulated in the analysis of operational transients and accidents covered in Chapter 15.

How these control systems comply with the acceptance criteria and conform to guidelines set forth in NUREG-0800 (Reference 2) is described in Section 7.1.

7.7.4 References

1. ANP-10284, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007.

2. NUREG-0800, Standard Review Plan, Section 7.7, “Control Systems,” Revision 5, March 2007.

Table 7.7-1—Cross Reference of Non-Safety I&C Controls

System	Non Safety Control Function(s)	FSAR Section(s)
Fuel Storage and Handling	Provides a means for handling fuel assemblies.	9.1
Essential Service Water System	Cooling of the Severe Accident Heat Removal System.	9.2.1
Component Cooling Water System	• Cooling of non-safety related components and heat exchangers. • Cooling of the Severe Accident Heat Removal System.	9.2.2
Operational Chilled Water System	Cooling source for non safety loads of HVAC.	9.2.9
Compressed Air System	Provides compressed air to non safety components.	9.3.1
Chemical Volume and Control System	• Reactor coolant water purification and clean up. • RCP sealing water supply. • Provide auxiliary spray to PZR.	9.3.4
Air Conditioning, Heating, Cooling and Ventilation Systems	Provide ambient air cooling for non-safety related systems and components.	9.4
Fire Protection Systems	Detects and suppresses fires.	9.5.1
Turbine Generator	Converts the thermal energy supplied by the main steam supply system into electrical energy.	10.2
Liquid Waste Management Systems	Receive and process radioactive liquid wastes from various systems.	11.2
Gaseous Waste Management Systems	Receive and process radioactive gaseous wastes from various systems.	11.3
Solid Waste Management Systems	Receive and process radioactive solid wastes from various systems.	11.4

Figure 7.7-1—Average Coolant Temperature Control Logic

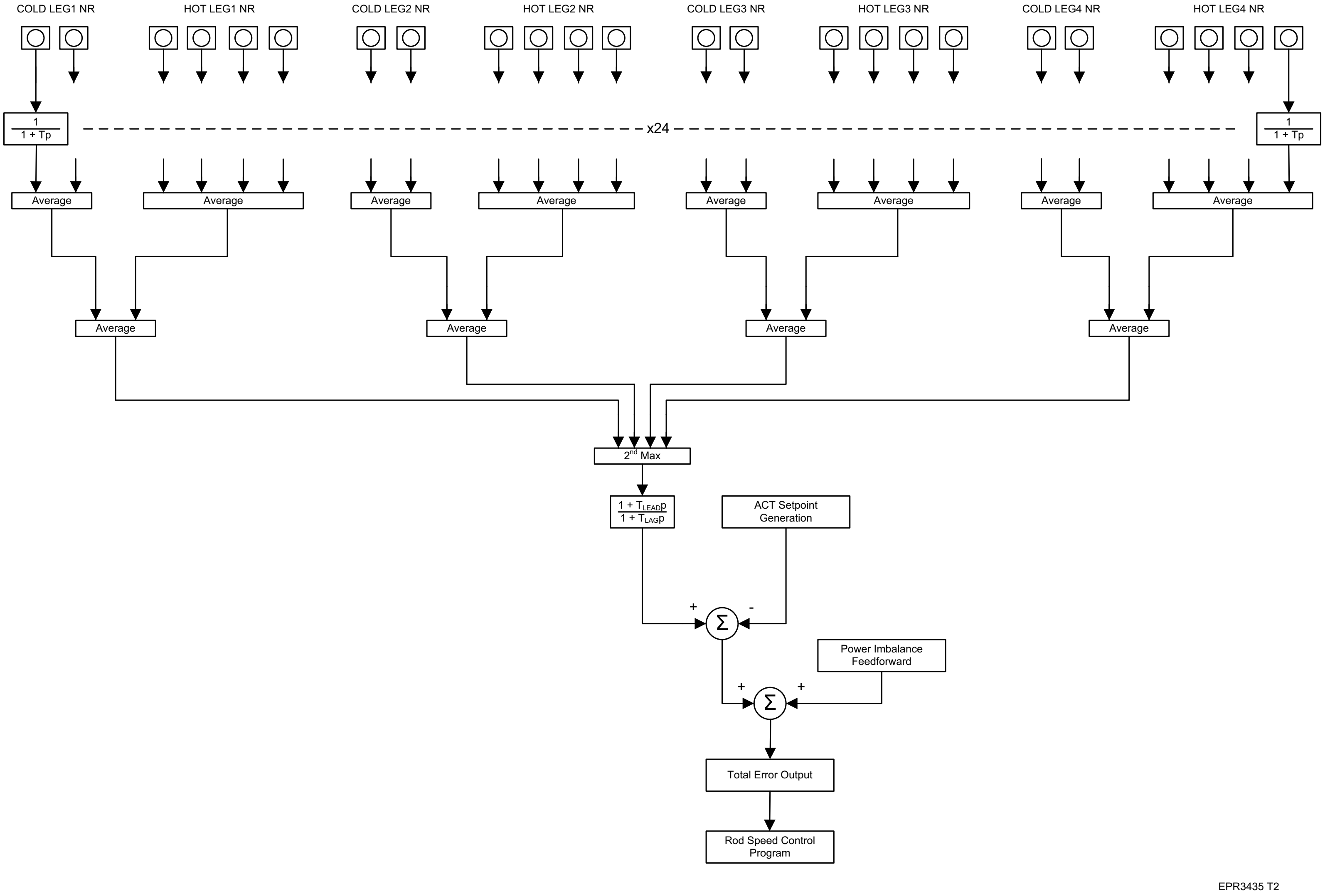


Figure 7.7-2—Rod Speed Control Program

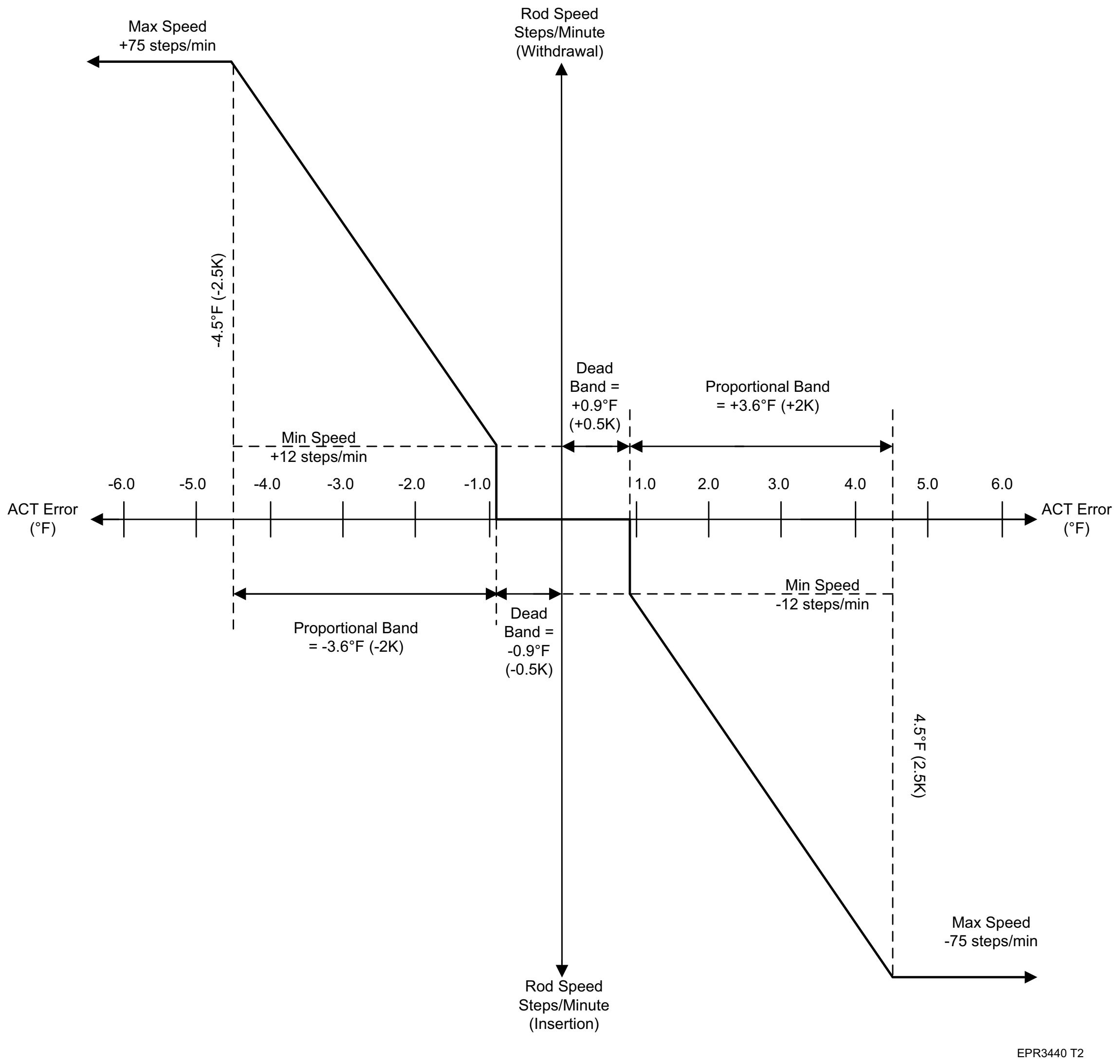


Figure 7.7-3—RCS Pressure Setpoints

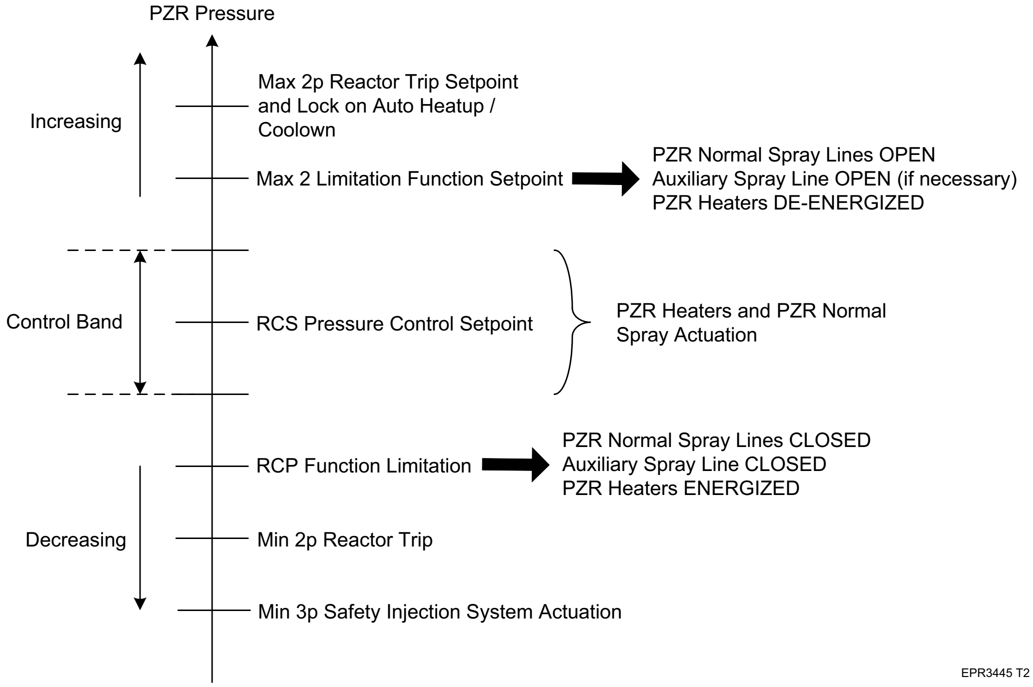
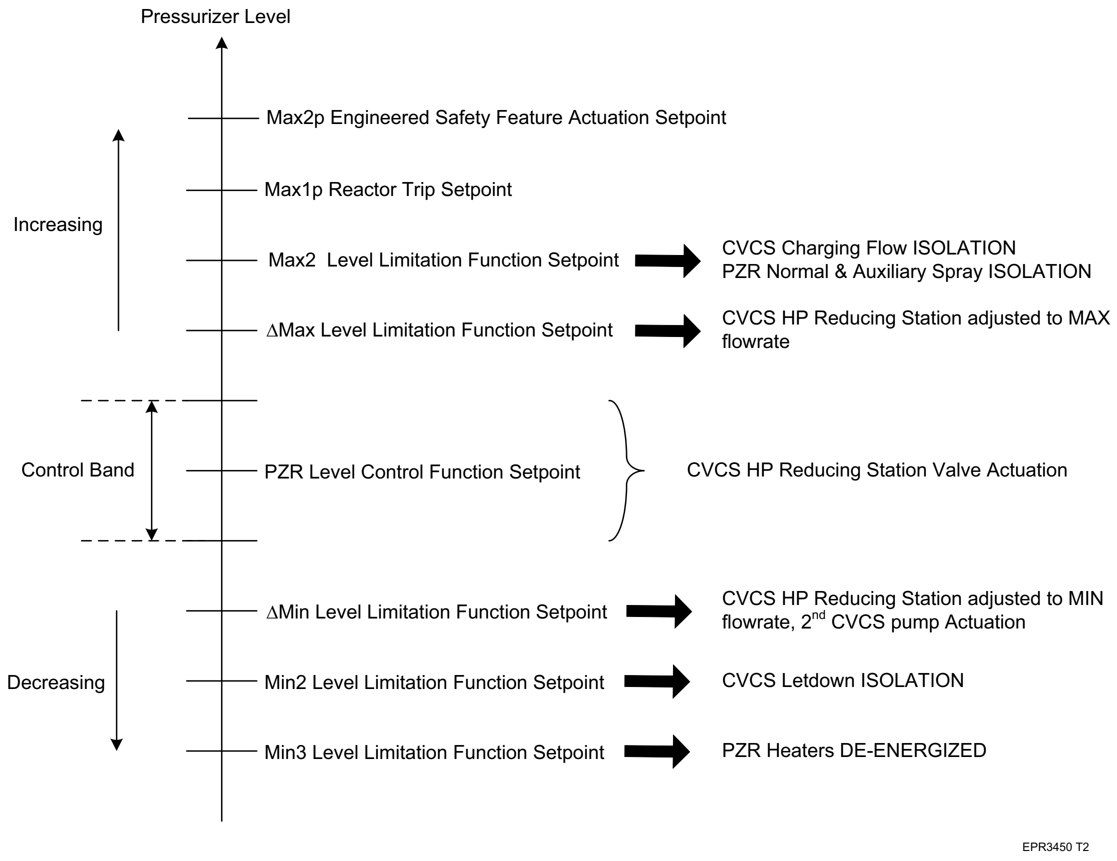

PZR Pressure
Increasing
Max 2p Reactor Trip Setpoint and Lock on Auto Heatup / Coolown
Max 2 Limitation Function Setpoint
PZR Normal Spray Lines OPEN
Auxiliary Spray Line OPEN (if necessary)
PZR Heaters DE-ENERGIZED
Control Band
RCS Pressure Control Setpoint
PZR Heaters and PZR Normal Spray Actuation
RCP Function Limitation
PZR Normal Spray Lines CLOSED
Auxiliary Spray Line CLOSED
PZR Heaters ENERGIZED
Decreasing
Min 2p Reactor Trip
Min 3p Safety Injection System Actuation
EPR3445 T2

Figure 7.7-4—Pressurizer Level Setpoints


Pressurizer Level
Max2p Engineered Safety Feature Actuation Setpoint
Max1p Reactor Trip Setpoint
Increasing
Max2 Level Limitation Function Setpoint
CVCS Charging Flow ISOLATION
PZR Normal & Auxiliary Spray ISOLATION
ΔMax Level Limitation Function Setpoint
CVCS HP Reducing Station adjusted to MAX flowrate
Control Band
PZR Level Control Function Setpoint
CVCS HP Reducing Station Valve Actuation
ΔMin Level Limitation Function Setpoint
CVCS HP Reducing Station adjusted to MIN flowrate, 2nd CVCS pump Actuation
Decreasing
Min2 Level Limitation Function Setpoint
CVCS Letdown ISOLATION
Min3 Level Limitation Function Setpoint
PZR Heaters DE-ENERGIZED
EPR3450 T2

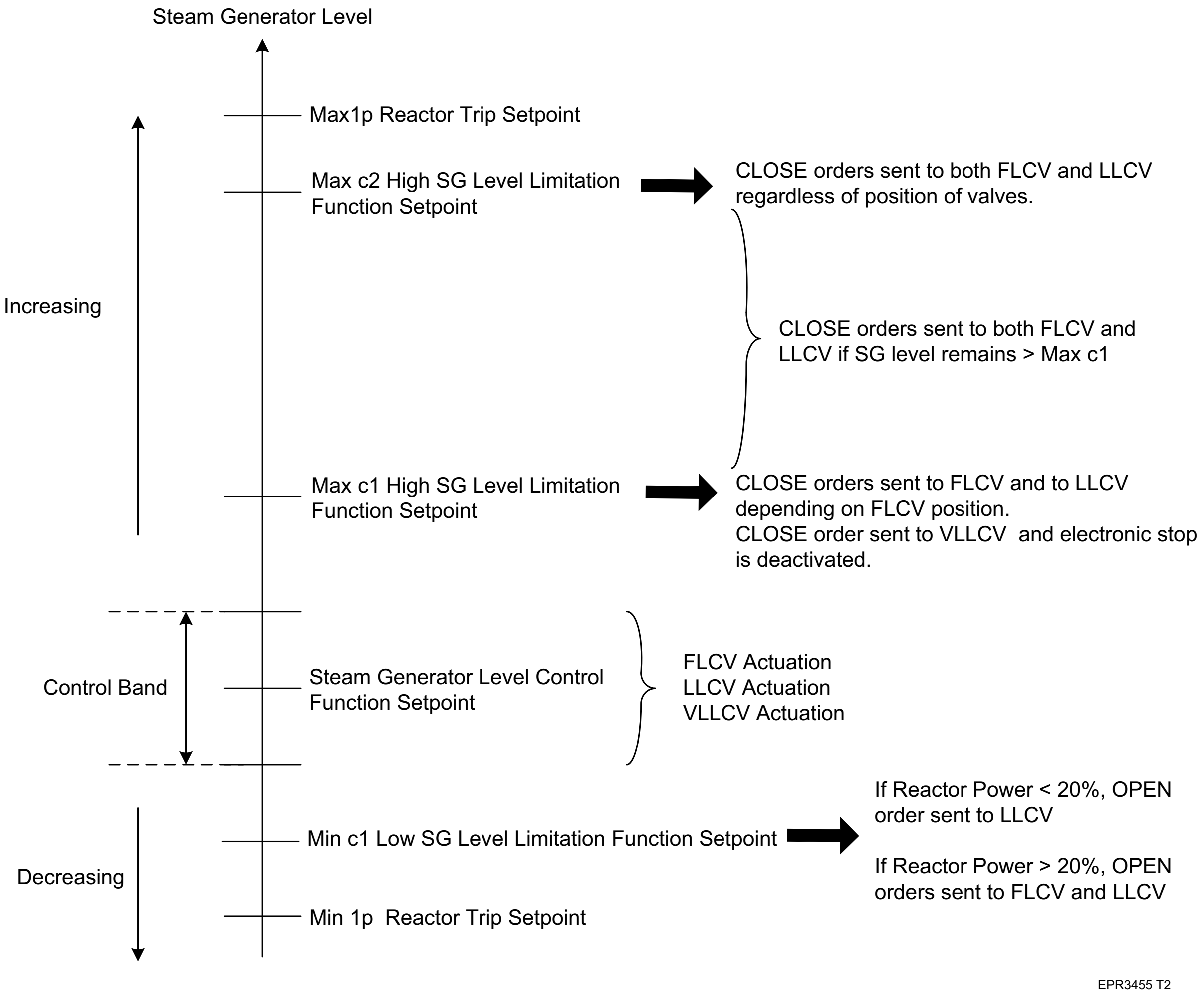

Steam Generator Level
Max1p Reactor Trip Setpoint
Max c2 High SG Level Limitation Function Setpoint
CLOSE orders sent to both FLCV and LLCV regardless of position of valves.
Increasing
CLOSE orders sent to both FLCV and LLCV if SG level remains > Max c1
Max c1 High SG Level Limitation Function Setpoint
CLOSE orders sent to FLCV and to LLCV depending on FLCV position.
CLOSE order sent to VLLCV and electronic stop is deactivated.
Control Band
Steam Generator Level Control Function Setpoint
FLCV Actuation
LLCV Actuation
VLLCV Actuation
If Reactor Power < 20%, OPEN order sent to LLCV
Min c1 Low SG Level Limitation Function Setpoint
If Reactor Power > 20%, OPEN orders sent to FLCV and LLCV
Decreasing
Min 1p Reactor Trip Setpoint
EPR3455 T2

Figure 7.7-5—Steam Generator Level Setpoints