7.2 Reactor Trip

7.2.1 Description

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

The equipment involved in reactor trip is shown in simplified block diagram form in Figure 7.1-2. Section 7.1 provides a description of the equipment. The equipment involved is:

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

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

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

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

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

Bypasses of parameter channels used to generate reactor trip signals and of reactor trip actuation divisions are permitted as described in subsection 7.2.1.1.12. Single failure criterion is met even when one channel or division is bypassed. Bypassing two or more redundant channels or divisions is not allowed.

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

7.2.1.1 Functional Description

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

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

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

7.2.1.1.1 Nuclear Startup Trips

Source Range High Neutron Flux Trip

Source range high neutron flux trips the reactor when two of the four source range channels exceed the trip setpoint. This trip provides protection during reactor startup and plant shutdown. This function is delayed from actuating each time the source range detector's high voltage power is energized to prevent a spurious trip due to the short term instability of the processed source

range values. It may be manually blocked and the high voltage source range detector power supply de-energized when the intermediate range neutron flux is above the P-6 setpoint value. It is automatically blocked by the power range neutron flux interlock (P-10). The trip may be manually reset when neutron flux is between P-6 and P-10. The reset occurs automatically when the intermediate range flux decreases below P-6. The channels can be individually bypassed to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated in the main control room.

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

Intermediate Range High Neutron Flux Trip

Intermediate range high neutron flux trips the reactor when two of the four intermediate range channels exceed the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if the power range channels are above approximately 10-percent power (P-10). The trip is automatically reset when the power range channels indicate less than 10-percent power. The intermediate range channels, including detectors, are separate from the power range channels. The intermediate range channels can be individually bypassed to permit channel testing during plant shutdown or prior to startup. This bypass action is indicated in the main control room.

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

Power Range High Neutron Flux Trip (Low Setpoint)

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

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

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

7.2.1.1.2 Nuclear Overpower Trips

Power Range High Neutron Flux Trip (High Setpoint)

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

Power Range High Positive Flux Rate Reactor Trip

This trip protects the reactor when a sudden abnormal increase in power occurs in two out of the four power range channels. It provides protection against ejection accidents of low worth rods

from midpower. It is always active. A channel is tripped when rate-sensitive circuits in the channel detect rates of change in nuclear power above the setpoint value. The channel trip is latched such that the partial trip signal does not disappear when the rate of change in power goes below the setpoint value. Once latched, the channel can only be reset from the main control room by manual action. The reactor is tripped when two out of the four rate channels have tripped.

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

7.2.1.1.3 Core Heat Removal Trips

Overtemperature ΔT Reactor Trip

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

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

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

$$q_{\Delta T} = \rho(T_C, P_{ZR})[h(T_H, P_{ZR}) - h(T_C, P_{ZR})]/\Delta T^\circ$$

Where:

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

T_H = $[(1+\tau_3 s)/(1+\tau_4 s)]T_{HOT}$, where T_{HOT} is the measured hot leg temperature (lead/lag compensation applied to compensate for core-to-hot leg transit time)

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

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

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

s = Laplace transform operator

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

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

Where:

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

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

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

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

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

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

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

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

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

Overpower ΔT Trip

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

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

$q_{\Delta T} \geq OPDT_{SP} = K_4 - f_2(\Delta I)$,

Where:

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

K_4 = A preset bias

$F_2(\Delta I)$ = A function of the neutron flux difference between upper and lower ionization chamber flux signals; to correct, if necessary, for an adverse axial flux shape.

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

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

Reactor Trip on Low Pressurizer Pressure

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

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

Reactor Trip on Low Reactor Coolant Flow

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

Figure 7.2-1, sheet 5 shows the logic for this trip. The development of permissives P-10 and P-8 are shown in Figure 7.2-1, sheet 4.

Reactor Trip on Reactor Coolant Pump Underspeed

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

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

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

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

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

Reactor Coolant Pump Bearing Water Temperature

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

The reactor trip on high reactor coolant pump bearing water temperature in any single reactor coolant pump is automatically blocked when reactor power is below the P-10 permissive setpoint. This enhances reliability by preventing unnecessary reactor trips. The trip is automatically reset when reactor power is above the P-10 setpoint.

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

7.2.1.1.4 Primary Overpressure Trips

Pressurizer High Pressure Reactor Trip

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

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

High-3 Pressurizer Water Level Reactor Trip

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

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

7.2.1.1.5 Loss of Heat Sink Trip

Reactor Trip on Low Water Level in any Steam Generator

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

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

7.2.1.1.6 Feedwater Isolation Trip

High-2 Steam Generator Water Level in Any Steam Generator

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

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

7.2.1.1.7 Automatic Depressurization Systems Actuation Reactor Trip

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

Manual automatic depressurization system actuation is initiated from either of two sets of controls in the main control room. Operating either of the two sets of controls also sends a reactor trip signal to the reactor trip switchgear breakers. Outputs on the control sets, physically and

electrically separated, send their position status to the protection and safety monitoring system. These inputs de-energize the undervoltage trip attachments on the reactor trip breakers, causing them to trip open. Additional outputs interrupt power to the shunt trip interposing relays, actuating the shunt trip attachments on each reactor trip circuit breaker. These provide a backup to the undervoltage trip of the breakers.

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

7.2.1.1.8 Core Makeup Tank Injection Trip

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

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

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

7.2.1.1.9 Reactor Trip on Safeguards Actuation

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

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

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

7.2.1.1.10 Manual Reactor Trip

The manual reactor trip consists of 2 controls in the main control room, either of which trip all 8 of the reactor trip switchgear breakers. The reactor trip circuit breakers contain both undervoltage and shunt trip attachments. The shunt trip acts as a diverse backup to the undervoltage trip in the breakers. Contacts on each control, physically and electrically separated, are in series with the undervoltage trip attachment on the reactor trip breakers, the shunt trip attachment interposing relays, and the power outputs at the protection and safety monitoring system cabinet. Actuating either control interrupts power from the voting logic to the undervoltage trip attachments, releasing them. It also interrupts power to shunt trip interposing relays, actuating the shunt trip attachments. The breakers trip when either the shunt trip attachments are energized or the undervoltage trip attachments are de-energized. Actuating either manual trip control causes each breaker to trip by initiating both of these actions.

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

7.2.1.1.11 Reactor Trip System Interlocks

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

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

Source Range Block (One Control for each Division)

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

Intermediate Range Block (One Control for each Division)

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

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

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

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

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

7.2.1.1.12 Bypasses of Reactor Trip Functions

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

7.2.1.2 Design Basis for Reactor Trips

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

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

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

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

The variables monitored for reactor trips are:

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

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

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

The allowable values for the limiting safety-related system settings and the trip setpoint for reactor trips are in the technical specifications (Chapter 16).

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

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

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

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

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

During startup or shutdown, reactor trips are provided for three ranges of neutron flux (source, intermediate, and power range). The source range, intermediate range, and power range (low setpoint) trips are manually blocked when the appropriate power escalation permissives are present. The trips are automatically reset during power de-escalation. Subsection 7.2.1.1.1 describes these reactor trips. Their interlocks are described in subsection 7.2.1.1.11.

During testing or maintenance, functions are provided to bypass a channel monitoring a variable for reactor trip. Although no setpoints need to be changed for bypassing, the coincidence logic is automatically adjusted as described in subsection 7.2.1.1.12. The logic provides that the remaining redundant channels for that variable meet the single failure criterion. The two-out-of-four logic is automatically reinstated when the bypass is removed.

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

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

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

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

Redundancy provides confidence that reactor trips are generated on demand, even when the protection system is degraded by a single failure. Reactor trips are four-way redundant. The single failure criterion is met even if one channel is bypassed, as discussed in subsection 7.2.1.1.12. More than one bypass is not allowed.

7.2.1.3 System Drawings

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

7.2.2 Analyses

7.2.2.1 Failure Modes and Effects Analysis (FMEA)

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

7.2.2.2 Conformance of the Reactor Trip Function to Applicable Criteria

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

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

The protection and safety monitoring system initiates a reactor trip whenever a condition monitored by the system reaches a preset level. The reactor trips are listed in Table 7.2-2 and are discussed in subsection 7.2.1.1. The variables which are monitored for these trips are listed in

subsection 7.2.1.2.2. Table 7.2-1 lists the ranges, accuracies, and response times for these variables. The reactor trip setpoints are listed in the technical specifications, Chapter 16.

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

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

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

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

A single failure in the protection and safety monitoring system or the reactor trip actuation divisions does not prevent a reactor trip, even when a reactor trip channel is bypassed for test or maintenance. Conformance of the equipment to this requirement is discussed in WCAP-15776 (Reference 2). In addition to the redundancy of equipment, diversity of reactor trip functions is incorporated. Most Condition II, III, or IV events requiring a reactor trip are protected by trips from diverse parameters. For example, reactor trip, because of an uncontrolled rod cluster control assembly bank withdrawal at power, may occur on power range high neutron flux, overtemperature, overpower, pressurizer high pressure or pressurizer high water level. Reactor trip on complete loss of reactor coolant flow may occur on low flow or from the diverse parameter of low reactor coolant pump speed.

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

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

control system to work leads to more conservative results, that assumption is made. In this way, reactor trips do not depend on control system actions.

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

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

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

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

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

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

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

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

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

Operating bypasses for reactor trips are described in subsection 7.2.1.1.11.

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

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

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

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

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

The reactor is tripped by actuating one of two manual reactor trip controls from the main control room. The reactor is also tripped upon manual actuation of the automatic depressurization system, manual core makeup tank injection, or upon manual safeguards actuation. These reactor trips are described in subsections 7.2.1.1.7, 7.2.1.1.8, 7.2.1.1.9, and 7.2.1.1.10. Refer also to WCAP-15776 (Reference 2).

7.2.3 Combined License Information

The Combined License information requested in this subsection has been completely addressed in WCAP-16438-P (Reference 1) and WCAP-16592-P (Reference 4), and the applicable changes are incorporated into the DCD. No additional work is required by the Combined License applicant.

The following words represent the original Combined License Information Item commitment, which has been addressed as discussed above:

> Combined License applicants referencing the AP1000 certified design will provide an FMEA for the protection and safety monitoring system. The FMEA will include a Software Hazards Analysis. This FMEA will provide the basis for those Technical Specification Completion Times that rely on an FMEA for their basis.

7.2.4 References

1. WCAP-16438-P, WCAP-16438-NP, "FMEA of AP1000 Protection and Safety Monitoring System," Revision 1, June 2006.

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

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

4. WCAP-16592-P, WCAP-16592-NP, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System," Revision 0, June 2006.

Table 7.2-1 (Sheet 1 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES (DESIGN BASIS FOR REACTOR TRIP) (NOMINAL)

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

Table 7.2-1 (Sheet 2 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES (DESIGN BASIS FOR REACTOR TRIP) (NOMINAL)

Protective Functions	Variables	Range of Variables	Typical Accuracy[1]	Typical Response Time (Sec)[2]
Overpower ΔT			±4% of ΔT span	
	Cold leg temp. (T_{cold})	490° to 610°F		5.5
	Hot leg temp. (T_{hot})	530° to 650°F		5.5
	Neutron flux (difference between top and bottom power range detectors)	-60 to +60% (Δφ)		0.6
Pressurizer Low Pressure	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
Pressurizer High Pressure	Pressurizer pressure	1700 to 2500 psig	±3% of span	0.9
Pressurizer High Water Level	Pressurizer water level	0-100% of entire cylindrical portion of pressurizer	±5% of span	0.9
Low Reactor Coolant Flow	Coolant flow	0 to 120% of rated flow	±3% of span	0.9
Low Reactor Coolant Pump Speed	Pump speed	0 to 120% of rated speed	±1% of span	0.7
Low Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±22% of span	0.9
High Steam Generator Water Level	Steam generator water level	0-100% of span (narrow range taps)	±13% of span	0.9
Reactor Coolant Pump High Bearing Water Temperature	Reactor coolant pump bearing water temperature	70°-450°F	±2% of span	5.5

Table 7.2-1 (Sheet 3 of 3)

REACTOR TRIP VARIABLES, LIMITS, RANGES, AND ACCURACIES (DESIGN BASIS FOR REACTOR TRIP) (NOMINAL)

Protective Functions	Variables	Range of Variables	Typical Accuracy(1)	Typical Response Time (Sec)(2)
Automatic or Manual Safeguards Actuation	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Manual Reactor Trip	Control status	N/A	N/A	N/A
Automatic or Manual Depressurization System Actuation	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4
Automatic or Manual Core Makeup Tank Injection	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4	See Table 7.3-4

Notes:

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

Table 7.2-2 (Sheet 1 of 2)

REACTOR TRIPS

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

Table 7.2-2 (Sheet 2 of 2)

REACTOR TRIPS

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

Notes:

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

---- No permissive or interlock.

Table 7.2-3 (Sheet 1 of 2)

REACTOR TRIP PERMISSIVES AND INTERLOCKS

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

Table 7.2-3 (Sheet 2 of 2)

REACTOR TRIP PERMISSIVES AND INTERLOCKS

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

Table 7.2-4

SYSTEM-LEVEL MANUAL INPUTS TO THE REACTOR TRIP FUNCTIONS

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

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

Table 7.2-5

FIGURE 7.2-1 CROSS REFERENCES

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

[Page Intentionally Left Blank]

LOGIC SYMBOLS

SYMBOLS	LOGIC FUNCTION	DESCRIPTION
	OR	A FUNCTION WHICH PRODUCES AN OUTPUT ONLY WHEN ONE INPUT (OR MORE) EXISTS.
	NOT	A FUNCTION WHICH PRODUCES AN OUTPUT ONLY WHEN THE INPUT DOES NOT EXIST.
	AND	A FUNCTION WHICH PRODUCES AN OUTPUT ONLY WHEN EVERY INPUT EXISTS.
2/3	COINCIDENCE 2 OUT OF 3 SHOWN	A FUNCTION WHICH PRODUCES AN OUTPUT WHEN THE PRESCRIBED NUMBER (OR MORE) OF SIGNAL INPUTS EXIST (EXAMPLE : 2 OR MORE INPUTS MUST EXIST FOR AN OUTPUT).
2/4 BYP	COINCIDENCE BYPASS GATE 2 OUT OF 4 SHOWN	A FUNCTION WHICH PRODUCES AN OUTPUT WHEN THE PRESCRIBED NUMBER (OR MORE) OF SIGNAL INPUTS EXIST. THIS GATE ALSO RECEIVES SIGNALS INDICATING CHANNELS BYPASSED. THESE BYPASS SIGNALS MODIFY THE COINCIDENCE OPERATION OF THIS DEVICE AS DEPICTED IN THE TABLE BELOW.

COINCIDENCE GATE TYPE	NUMBER OF CHANNELS BYPASSED				
	0	1			
2/4	2/4	2/3			
2/3	2/3	1/2			

A.I.	MEMORY	A FUNCTION WHICH RETAINS THE CONDITION OF OUTPUT CORRESPONDING TO THE LAST ACTUATED INPUT.
TROL IGIC PUT A.O.	ANALOG GATE	A FUNCTION WHICH PERMITS AN ANALOG SIGNAL TO PASS IN AN ISOLATED CALCULATION IF THE CONTROL LOGIC INPUT EXISTS. IF THE CONTROL LOGIC INPUT DOES NOT EXIST, THE ANALOG OUTPUT IS ZERO.
	ADJUSTABLE TIME DELAY ACTUATING	A FUNCTION WHICH PRODUCES AN OUTPUT FOLLOWING A DEFINITE INTENTIONAL TIME DELAY AFTER RECEIVING AN INPUT.
	ADJUSTABLE TIME DELAY DE-ACTUATING	A FUNCTION WHICH PRODUCES AN OUTPUT COINCIDENT WITH THE INPUT AND MAINTAINS THE OUTPUT FOR A DEFINITE INTENTIONAL TIME DELAY AFTER THE INPUT IS REMOVED.
T S	ONE SHOT	**A FUNCTION THAT PRODUCES A TRUE OUTPUT FOR A DEFINITE INTENTIONAL TIME PERIOD OF T SECONDS AFTER THE INPUT BECOMES TRUE. THE OUTPUT RETURNS TO FALSE AFTER T SECONDS REGARDLESS OF THE TIME DURATION OF THE TRUE STATE OF THE INPUT.**

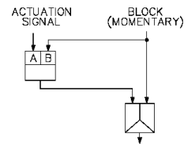
LOGIC SYMBOLS

S R OR R S — **SET/RESET MEMORY** — **A FUNCTION THAT PRODUCES A TRUE OUTPUT WHEN THE SET INPUT IS TRUE WHILE AT THE SAME TIME THE RESET INPUT IS FALSE. WHEN THE RESET INPUT IS TRUE THE OUTPUT IS UNCONDITIONALLY FALSE. TRANSITION TABLE:**

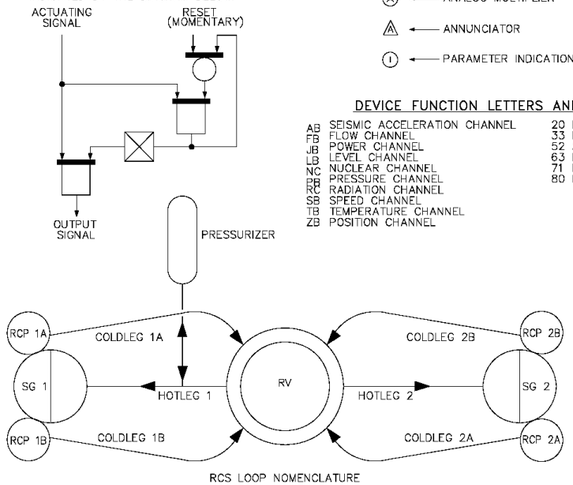
S 0 1 1 1 0 0 0 1
R 0 0 1 0 0 1 0 1
O 0 1 0 1 1 1 0 0 0

L R OR R L — MEMORY WITH ACTUATION BLOCK — A FUNCTION WITH MEMORY AND ACTUATION SIGNAL BLOCK LOGIC FUNCTIONS AS INDICATED BY THE DIAGRAM BELOW.

L 0 1 1 1 0 1 0 0 0 1
R 0 0 1 0 0 0 0 0 1 0 1
O 0 1 0 0 0 1 1 0 0 0



A B — ACTUATION BLOCK — A FUNCTION HAVING AN ACTUATION SIGNAL BLOCK LOGIC FUNCTION SO THAT THE OUTPUT SIGNAL MAY BE REMOVED BY THE MANUAL BLOCK (RESET) CONTROL EVEN THOUGH THE INPUT ACTUATE SIGNAL IS PRESENT, AS INDICATED BY THE DIAGRAM BELOW.



RCS LOOP NOMENCLATURE

FOR SIGNALS DERIVED FROM SENSORS IN THE HOT LEG AND COLD LEG (SUCH AS T_{AVG}) THE FOLLOWING NOTATION WILL BE USED.

DEFINITION	LOOP
HOT LEG 1 & COLD LEG 1A	LOOP 1A
HOT LEG 1 & COLD LEG 1B	LOOP 1B
HOT LEG 2 & COLD LEG 2A	LOOP 2A
HOT LEG 2 & COLD LEG 2B	LOOP 2B

ADDITIONAL SYMBOLS

PB	ELECTRONIC BISTABLE
	OUTPUT INDICATOR
	BISTABLE OUTPUT IS A LOGIC "1" WHEN THE MEASURED PARAMETER IS GREATER THAN THE SETPOINT VALUE.
	BISTABLE OUTPUT IS A LOGIC "1" WHEN THE MEASURED PARAMETER IS LESS THAN THE SETPOINT VALUE.
	BISTABLE OUTPUT IS A LOGIC "1" WHEN THE MEASURED PARAMETER DEVIATES FROM THE NORMAL VALUE BY MORE THAN THE SETPOINT AMOUNTS.
OR OR	SAME AS ABOVE EXCEPT WITH AN AUTOMATICALLY ADJUSTED SETPOINT
OR OR	SAME AS ABOVE EXCEPT WITH REQUIRED HYSTERESIS
27	ELECTRO-MECHANICAL BISTABLE
	OUTPUT INDICATOR (SAME AS EXPLAINED ABOVE)
	LOGIC INFORMATIOM TRANSMISSION
	ANALOG INFORMATION TRANSMISSION
	REDUNDANCY DEMARCATION
	ARRAY INFORMATION TRANSMISSION
S	ANALOG SUMMER
⊗	ANALOG MULTIPLIER
A	ANNUNCIATOR
I	PARAMETER INDICATION

DEVICE FUNCTION LETTERS AND NUMBERS

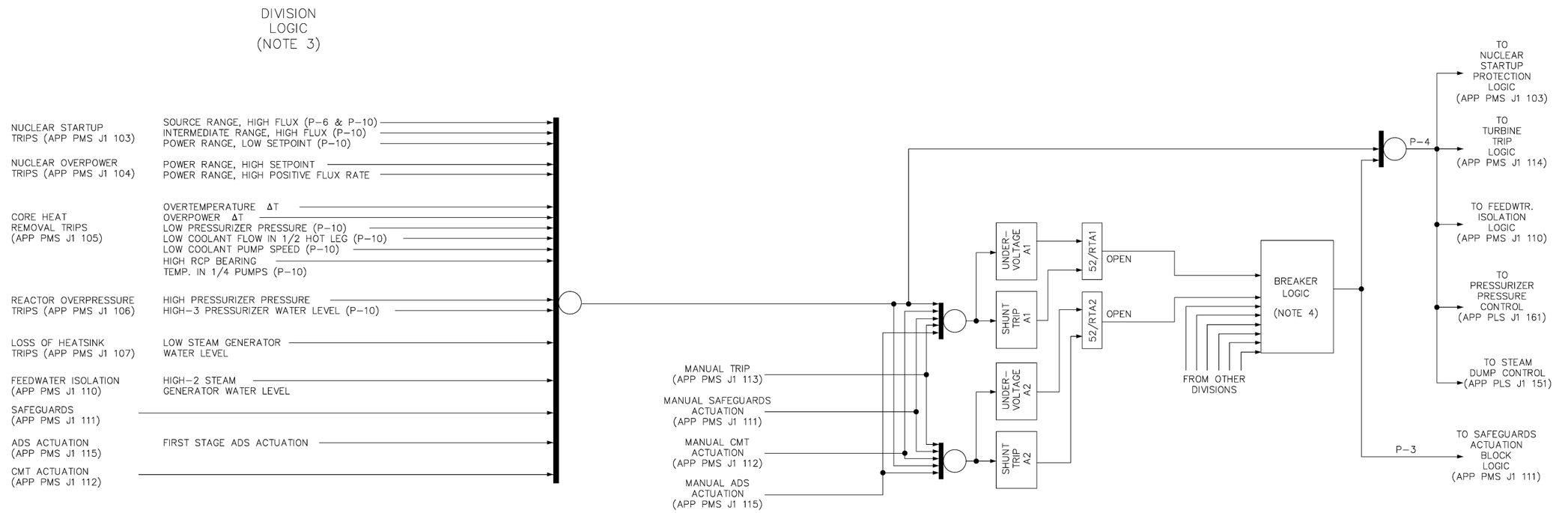
AB	SEISMIC ACCELERATION CHANNEL	20	ELECTRIC OPERATED VALVE
FB	FLOW CHANNEL	33	POSITION SWITCH
JB	POWER CHANNEL	52	AC CIRCUIT BREAKER
LB	LEVEL CHANNEL	63	PRESSURE SWITCH
NC	NUCLEAR CHANNEL	71	LEVEL SWITCH
PB	PRESSURE CHANNEL	80	FLOW SWITCH
RC	RADIATION CHANNEL		
SB	SPEED CHANNEL		
TB	TEMPERATURE CHANNEL		
ZB	POSITION CHANNEL		

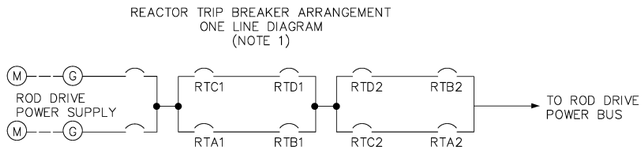
GENERAL NOTES:

1. IN THE LOGIC CIRCUITS, THE INDICATED ACTUATION OF A SYSTEM OR DEVICE OCCURS WHEN A LOGIC "1" SIGNAL IS PRESENT.
2. EXCEPT WHERE INDICATED OTHERWISE THE FOLLOWING IS TRUE: ALL LOGIC CIRCUITS ARE EITHER TWOFOLD OR FOURFOLD REDUNDANT. EVERY TWOFOLD REDUNDANT LOGIC CIRCUIT SHOWN HAS A DUPLICATE LOCATED IN A SEPARATE CABINET. EVERY FOURFOLD REDUNDANT CIRCUIT SHOWN HAS THREE ADDITIONAL IDENTICAL LOGIC CIRCUITS LOCATED IN SEPARATE CABINETS. MANUAL CONTROLS DO NOT HAVE REDUNDANT ACTUATORS, BUT DO HAVE REDUNDANT CONTACTS WHERE LOGIC IS REDUNDANT.
3. WHENEVER A PROCESS SIGNAL IS USED FOR MONITORING OR CONTROL AND IS DERIVED FROM A PROTECTION CHANNEL, ISOLATION MUST BE PROVIDED.
4. THIS SET OF DRAWINGS AND THE ASSOCIATED REACTOR CONTROL AND PROTECTION SYSTEM FUNCTIONAL REQUIREMENTS DOCUMENTS ILLUSTRATE THE FUNCTIONAL REQUIREMENTS OF THE REACTOR CONTROL AND PROTECTION SYSTEM, INCLUDING ENGINEERED SAFEGUARDS. THESE DRAWINGS SHOULD NOT BE USED WITHOUT THE ASSOCIATED FUNCTIONAL REQUIREMENTS DOCUMENT AND THEY DO NOT REPRESENT ACTUAL HARDWARE IMPLEMENTATION.
5. COMBINATION OF PROTECTION FUNCTIONS IS PERMITTED PROVIDED:
   A. THE COMBINATION DOES NOT DEGRADE THE RELIABILITY OF THE COMBINED FUNCTION.
   B. THE COMBINED FUNCTIONS SHARE COMMON SENSOR INPUTS.
6. THE ALARM SHOWN ON SIGNAL SELECTORS REPRESENTS ALARMING OF SIGNAL REJECTION.

Figure 7.2-1 (Sheet 1 of 20)

Functional Diagram Index and Symbols



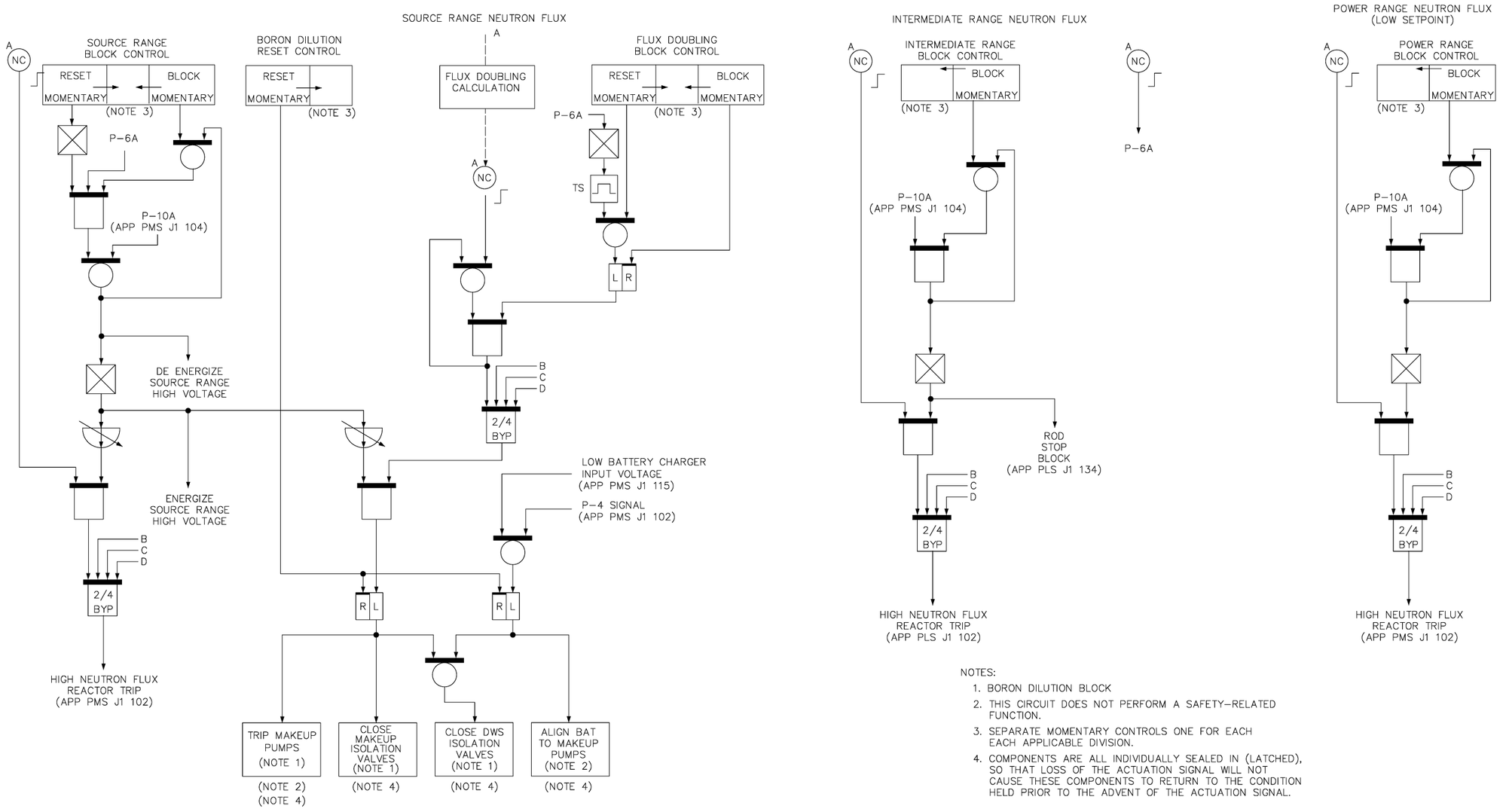


NOTES:

1. TRIPPING ANY TWO OR MORE BREAKER SETS, BOTH 1 AND 2 BREAKERS DE–ENERGIZE THE ROD DRIVES. THE FULL LENGTH CONTROL RODS AND SHUTDOWN RODS ARE THEREBY RELEASED FOR GRAVITY INSERTION INTO THE REACTOR CORE.
2. DELETED.
3. THIS CIRCUITRY IS FOURFOLD REDUNDANT. ONLY ONE DIVISION IS SHOWN WHICH IS TYPICAL OF THE OTHER DIVISIONS.
4. REACTOR TRIP LOGIC PRODUCES A TRUE (LOGIC "1") OUTPUT IF THE FOLLOWING BREAKER OPEN STATUS CONDITIONS ARE MET:
   [(A1+B1) . (C1+D1)] + [(A2+C2) . (B2+D2)]

Figure 7.2-1 (Sheet 2 of 20)

Functional Diagram
Reactor Trip Functions

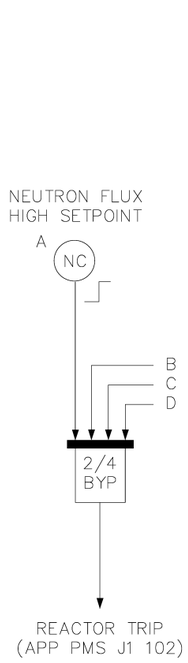


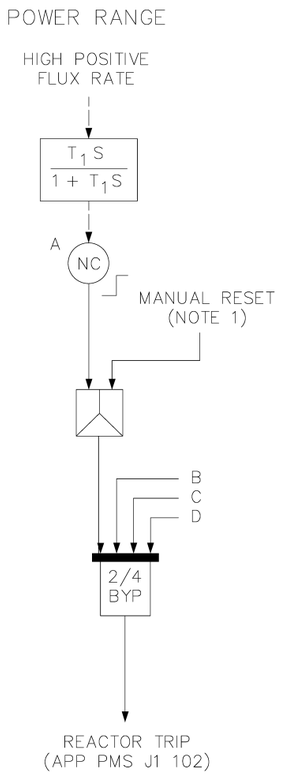
NOTES:

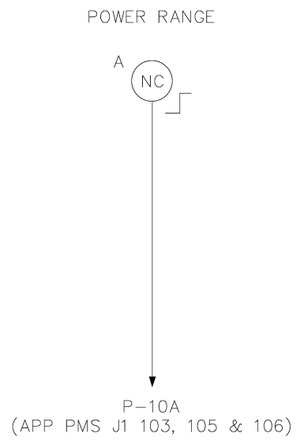
1. BORON DILUTION BLOCK
2. THIS CIRCUIT DOES NOT PERFORM A SAFETY–RELATED FUNCTION.
3. SEPARATE MOMENTARY CONTROLS ONE FOR EACH EACH APPLICABLE DIVISION.
4. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.

Figure 7.2-1 (Sheet 3 of 20)

Functional Diagram
Nuclear Startup Protection







NOTES:

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

Figure 7.2-1 (Sheet 4 of 20)

Functional Diagram
Nuclear Overpower Protection

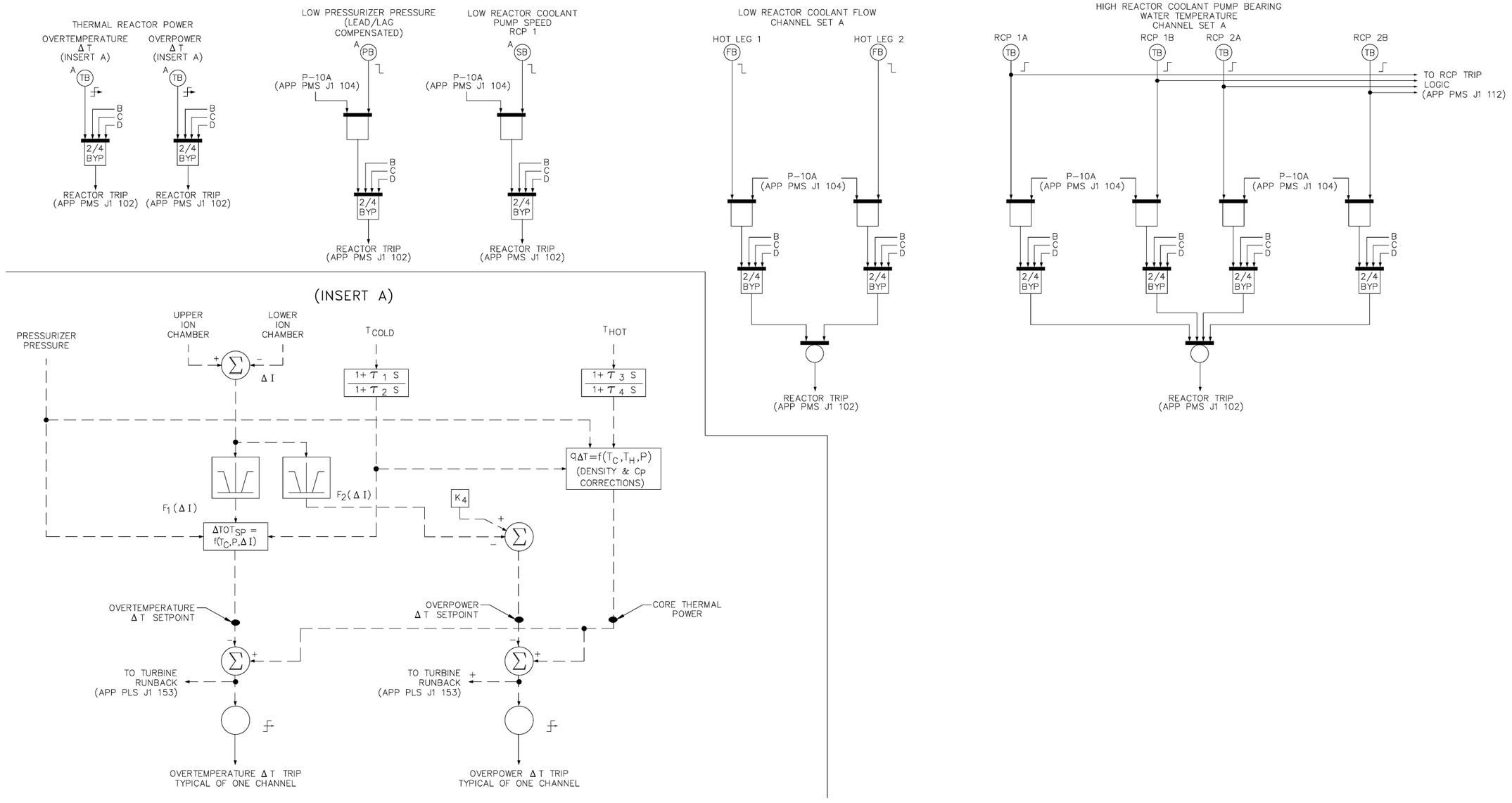
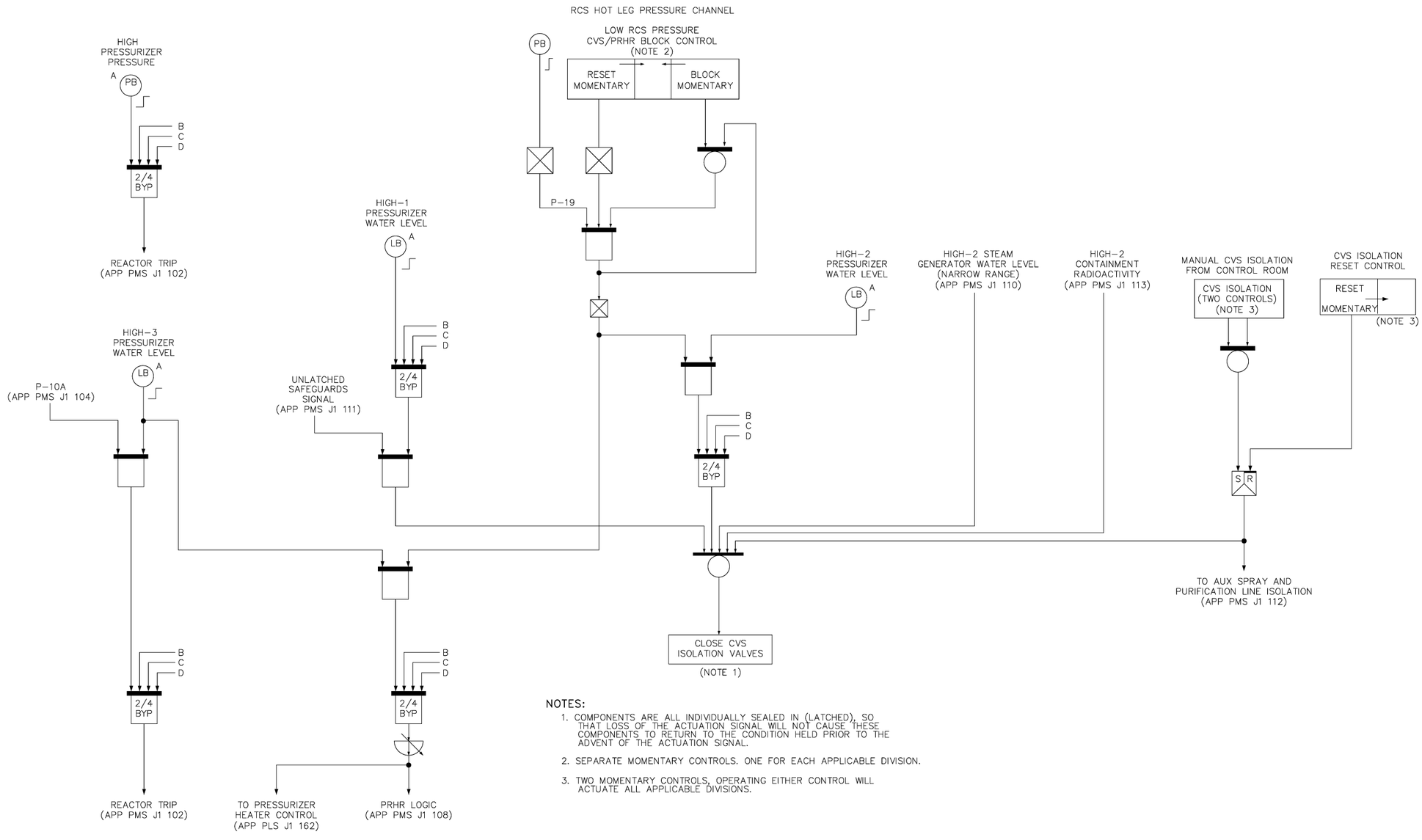


Figure 7.2-1 (Sheet 5 of 20)

Functional Diagram
Core Heat Removal Protection



NOTES:

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

Figure 7.2-1 (Sheet 6 of 20)

Functional Diagram
Primary Overpressure & Loss of Heat Sink Protection

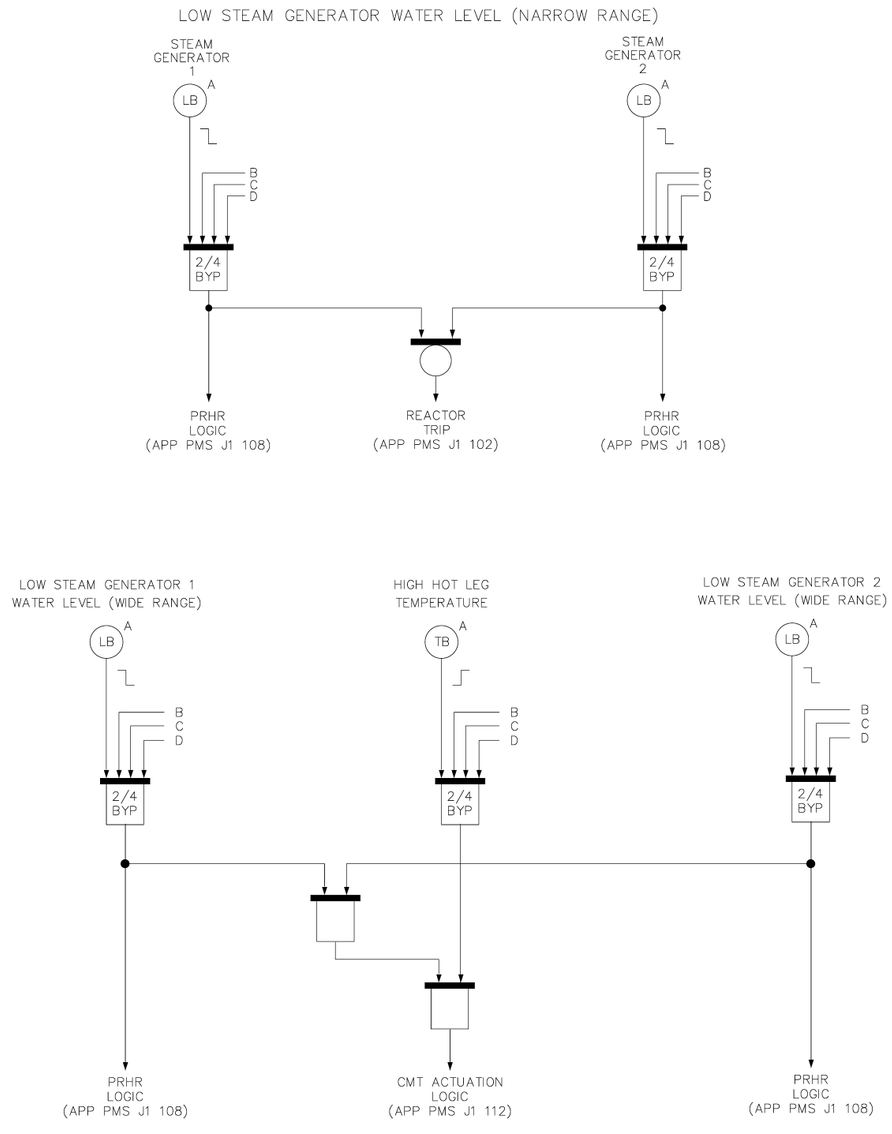
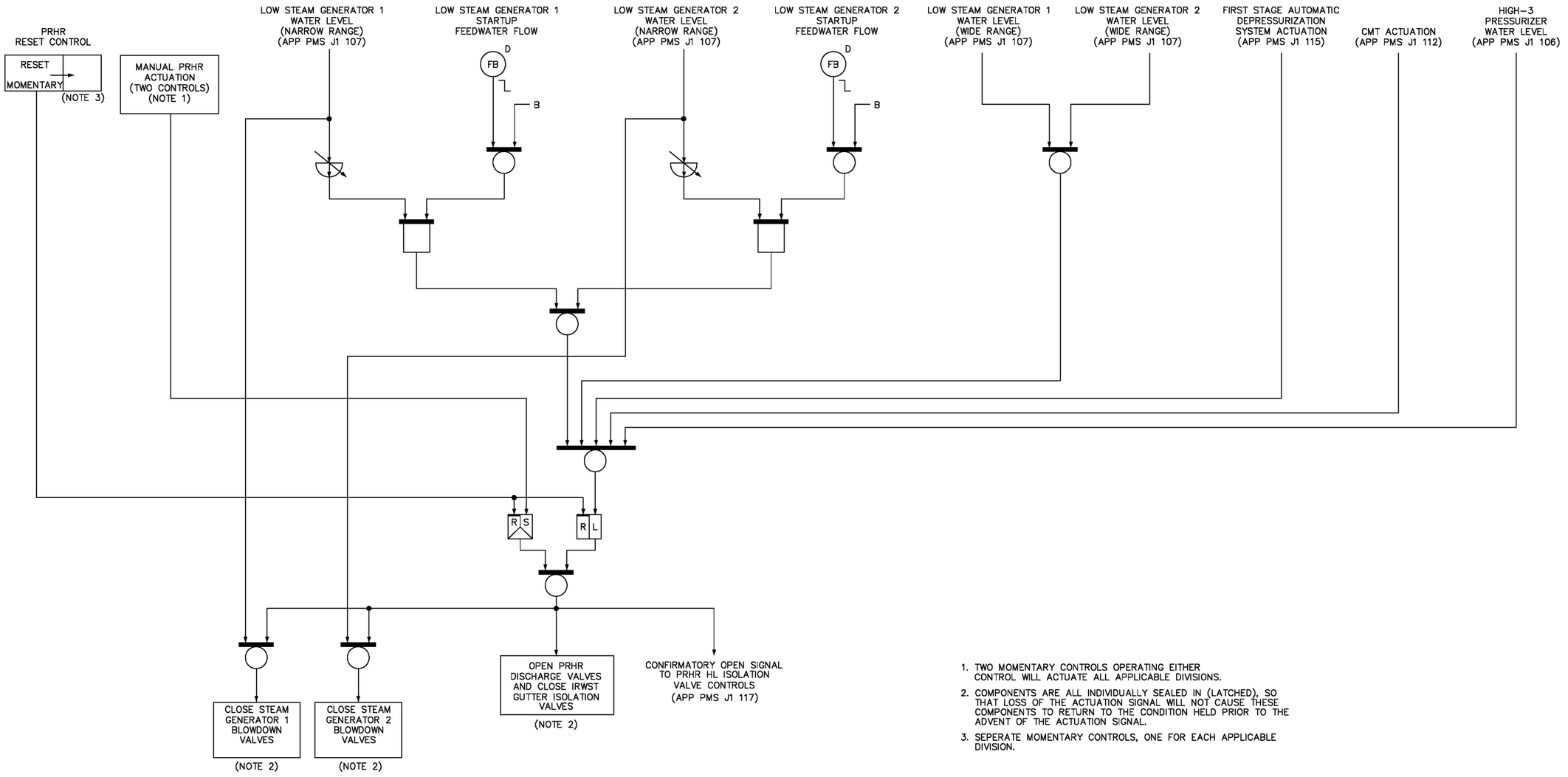


Figure 7.2-1 (Sheet 7 of 20)

Functional Diagram
Loss of Heat Sink Protection



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

Figure 7.2-1 (Sheet 8 of 20)

Functional Diagram
Loss of Heat Sink Protection

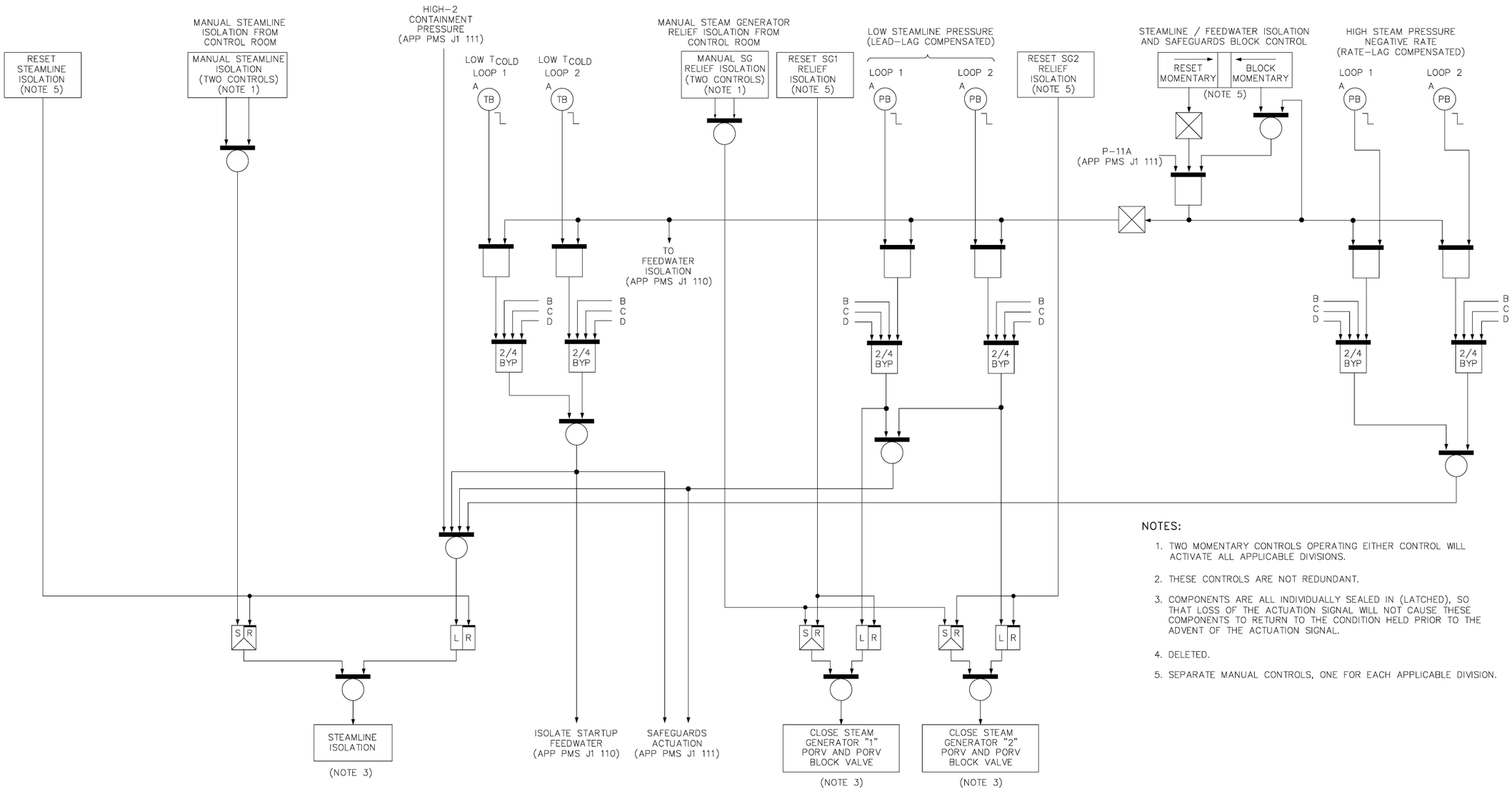


Figure 7.2-1 (Sheet 9 of 20)

Functional Diagram
Steamline Isolation

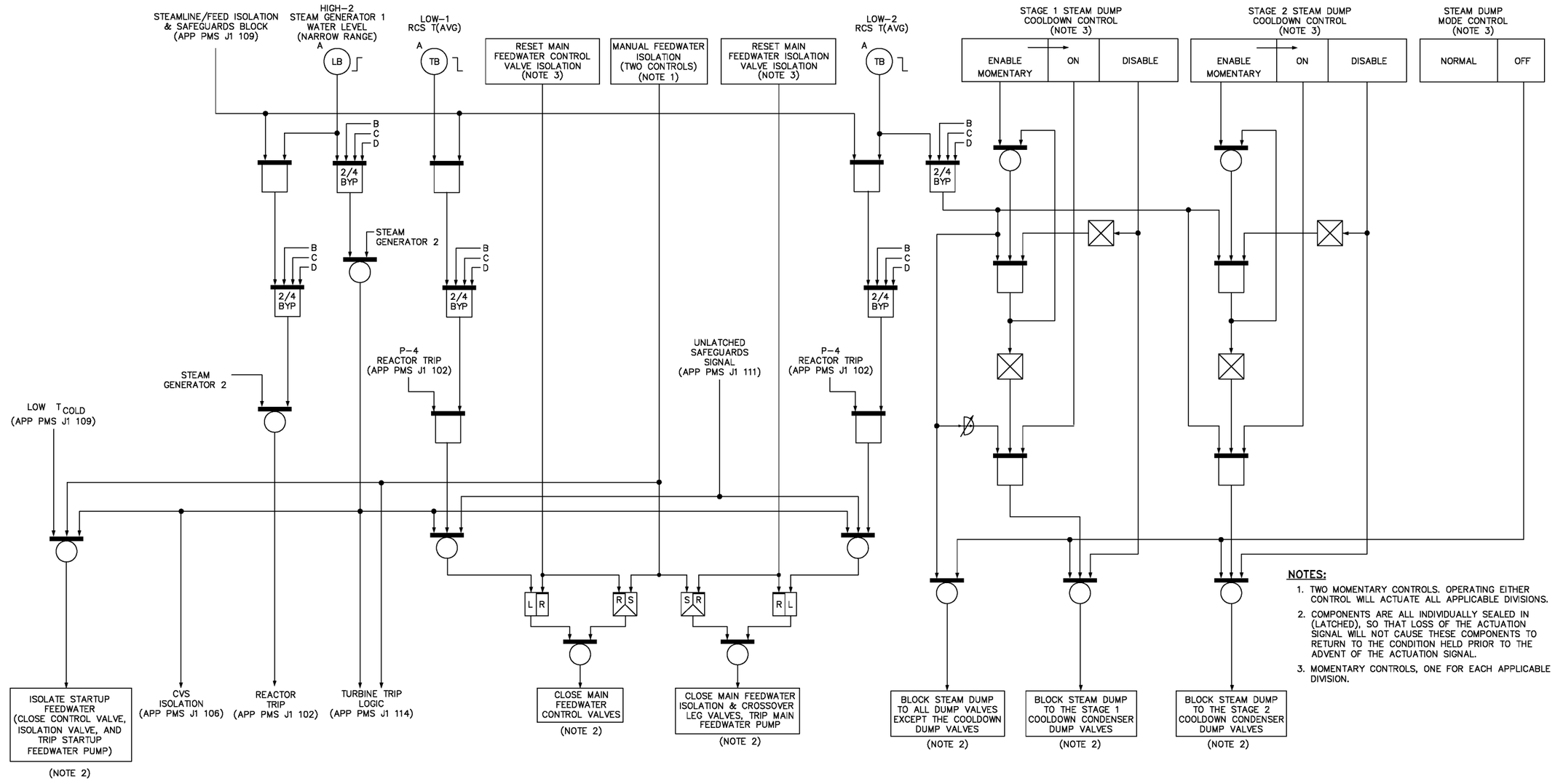
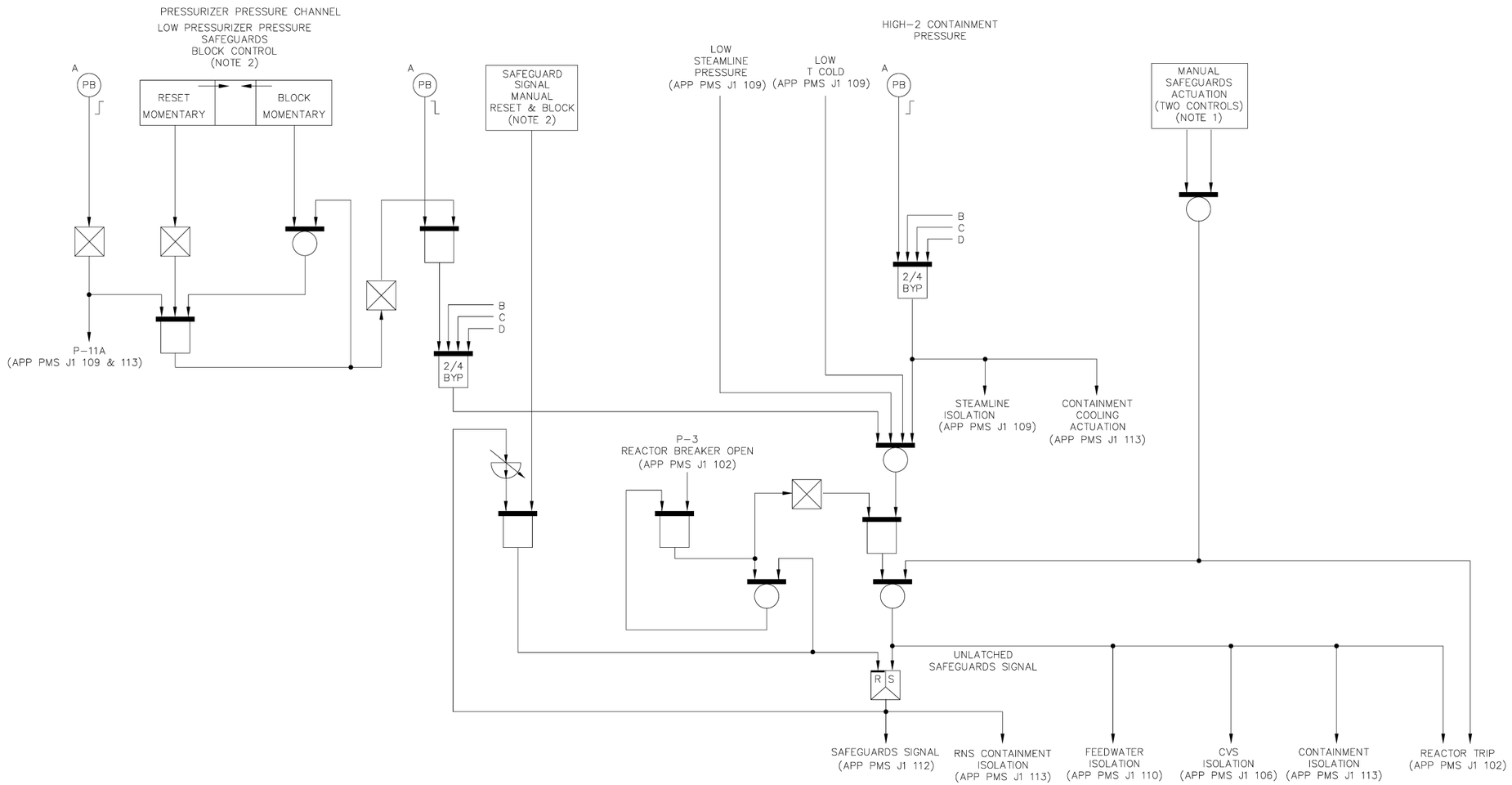


Figure 7.2-1 (Sheet 10 of 20)

Functional Diagram
Feedwater Isolation

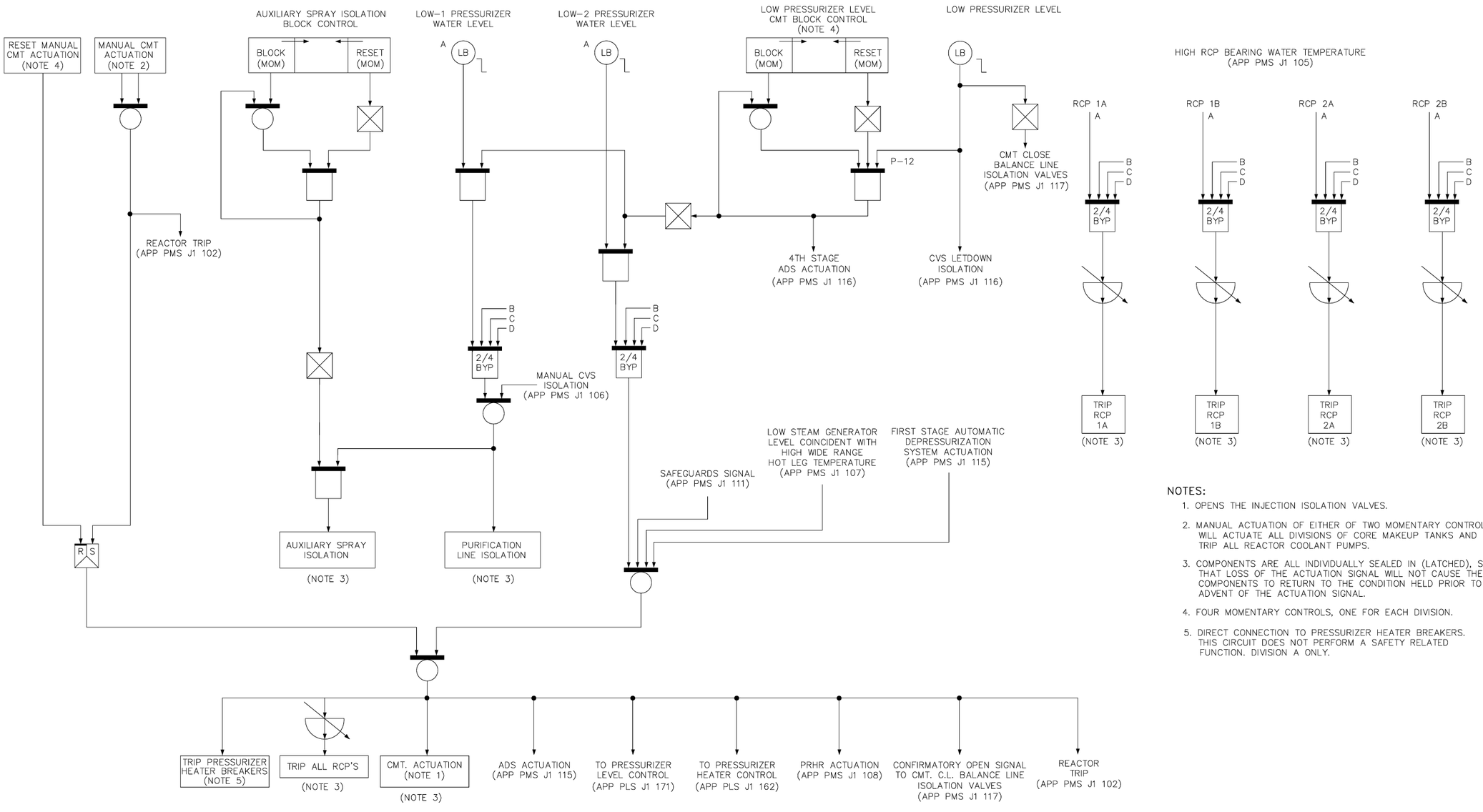


NOTES:

1. TWO MOMENTARY CONTROLS. OPERATING EITHER CONTROL WILL ACTUATE ALL APPLICABLE DIVISIONS.
2. SEPARATE MOMENTARY CONTROLS. ONE FOR EACH APPLICABLE DIVISION.

Figure 7.2-1 (Sheet 11 of 20)

Functional Diagram
Safeguards Actuation

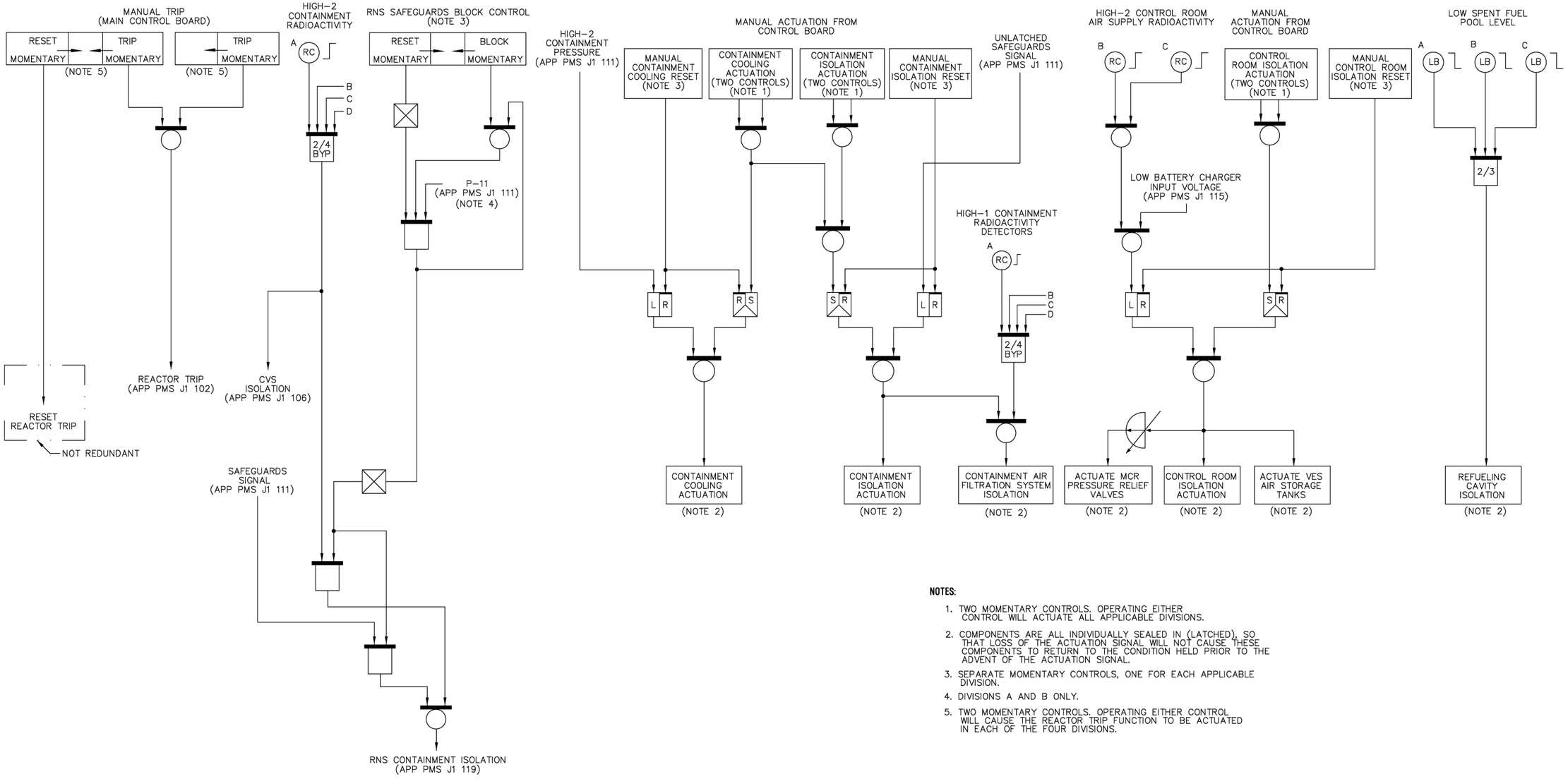


NOTES:

1. OPENS THE INJECTION ISOLATION VALVES.
2. MANUAL ACTUATION OF EITHER OF TWO MOMENTARY CONTROLS WILL ACTUATE ALL DIVISIONS OF CORE MAKEUP TANKS AND TRIP ALL REACTOR COOLANT PUMPS.
3. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
4. FOUR MOMENTARY CONTROLS, ONE FOR EACH DIVISION.
5. DIRECT CONNECTION TO PRESSURIZER HEATER BREAKERS. THIS CIRCUIT DOES NOT PERFORM A SAFETY RELATED FUNCTION. DIVISION A ONLY.

Figure 7.2-1 (Sheet 12 of 20)

Functional Diagram
Core Makeup Tank Actuation and Reactor Coolant Pump Trip

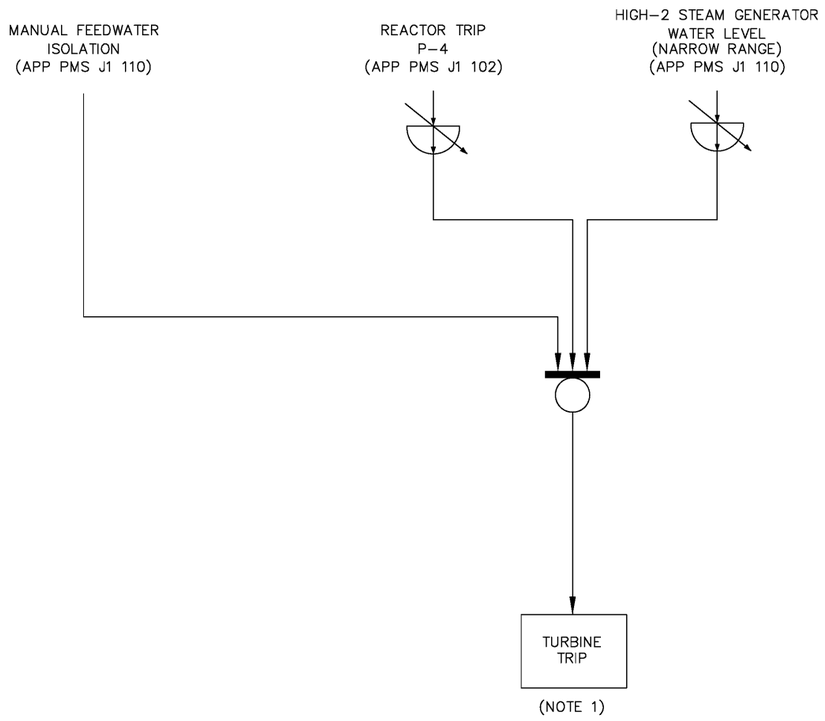


NOTES:

1. TWO MOMENTARY CONTROLS. OPERATING EITHER CONTROL WILL ACTUATE ALL APPLICABLE DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. SEPARATE MOMENTARY CONTROLS, ONE FOR EACH APPLICABLE DIVISION.
4. DIVISIONS A AND B ONLY.
5. TWO MOMENTARY CONTROLS. OPERATING EITHER CONTROL WILL CAUSE THE REACTOR TRIP FUNCTION TO BE ACTUATED IN EACH OF THE FOUR DIVISIONS.

Figure 7.2-1 (Sheet 13 of 20)

Functional Diagram
Containment and Other Protection

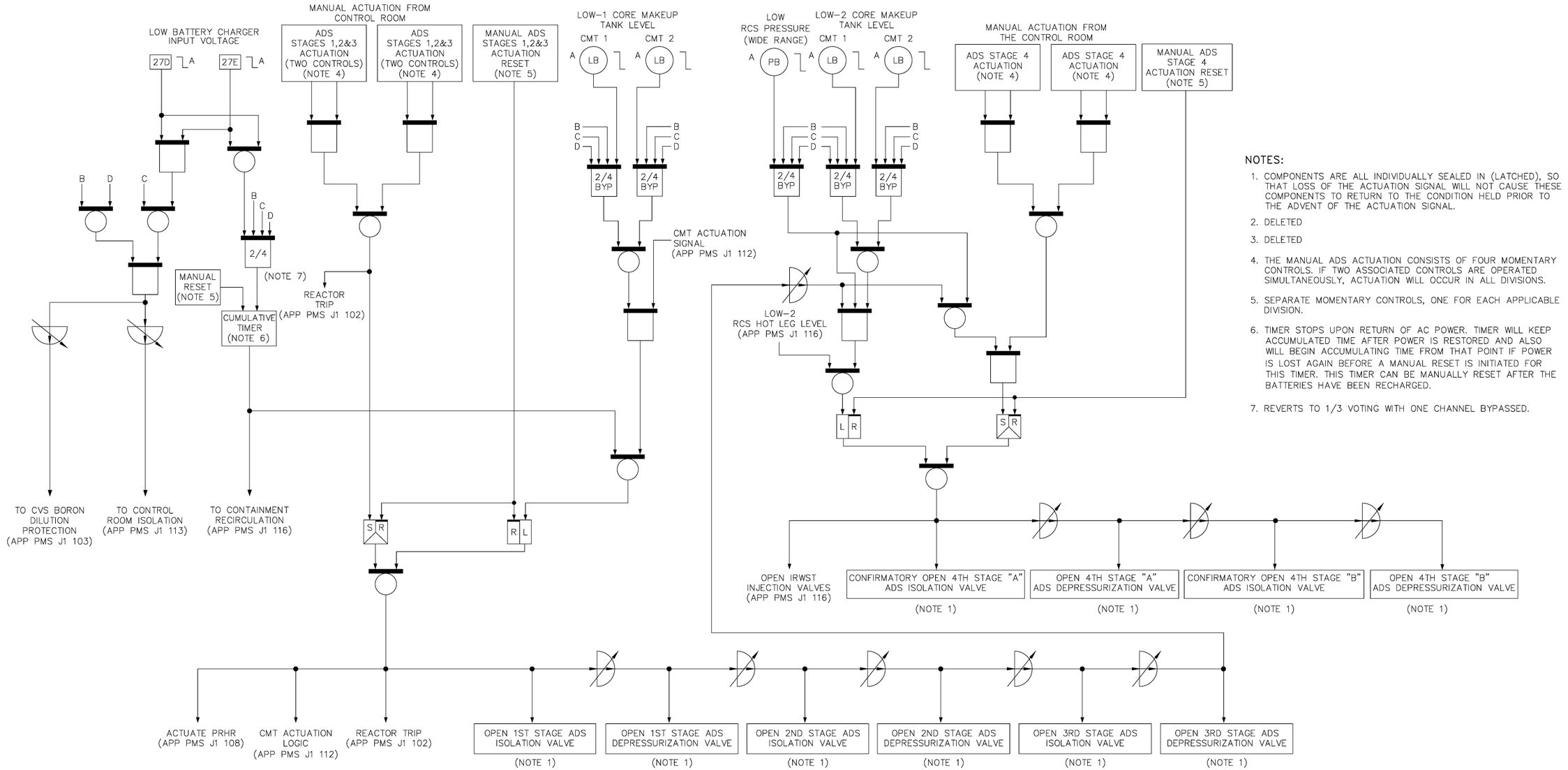


NOTES:

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

Figure 7.2-1 (Sheet 14 of 20)

Functional Diagram
Turbine Trip

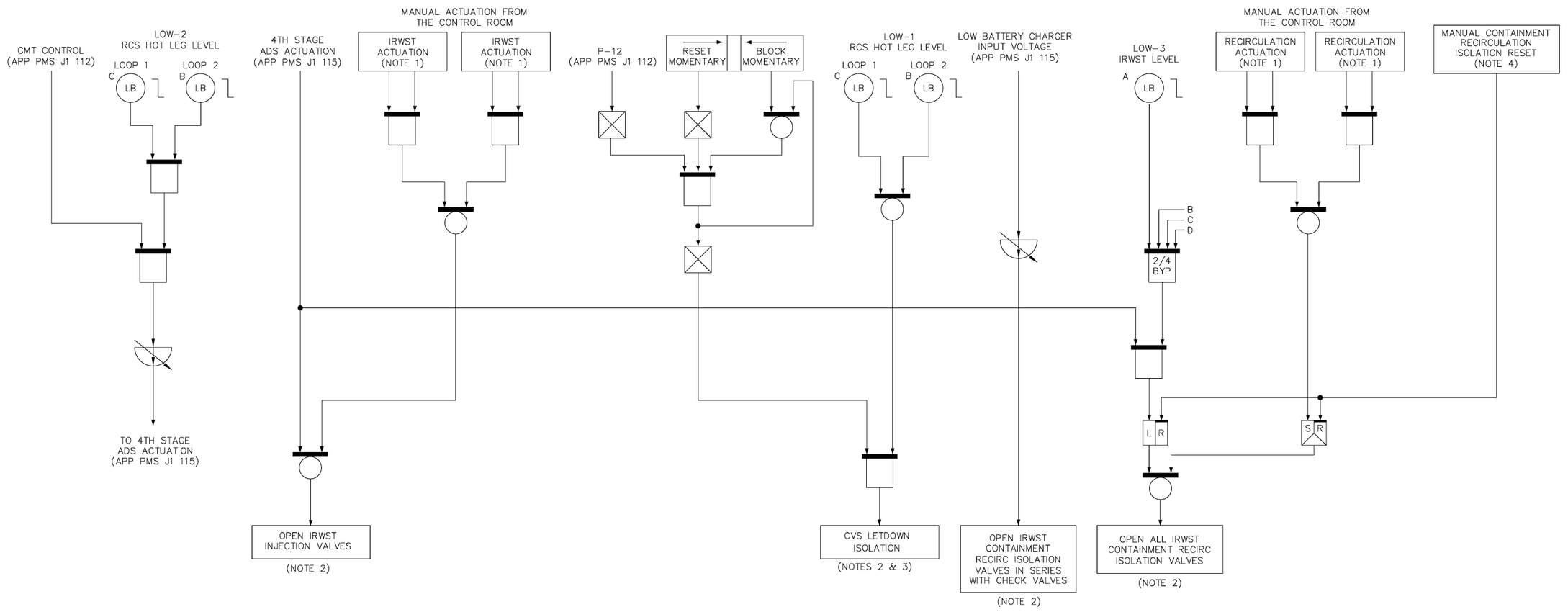


NOTES:

1. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
2. DELETED
3. DELETED
4. THE MANUAL ADS ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL DIVISIONS.
5. SEPARATE MOMENTARY CONTROLS, ONE FOR EACH APPLICABLE DIVISION.
6. TIMER STOPS UPON RETURN OF AC POWER. TIMER WILL KEEP ACCUMULATED TIME AFTER POWER IS RESTORED AND ALSO WILL BEGIN ACCUMULATING TIME FROM THAT POINT IF POWER IS LOST AGAIN BEFORE A MANUAL RESET IS INITIATED FOR THIS TIMER. THIS TIMER CAN BE MANUALLY RESET AFTER THE BATTERIES HAVE BEEN RECHARGED.
7. REVERTS TO 1/3 VOTING WITH ONE CHANNEL BYPASSED.

Figure 7.2-1 (Sheet 15 of 20)

Functional Diagram
Automatic RCS Depressurization Valve Sequencing

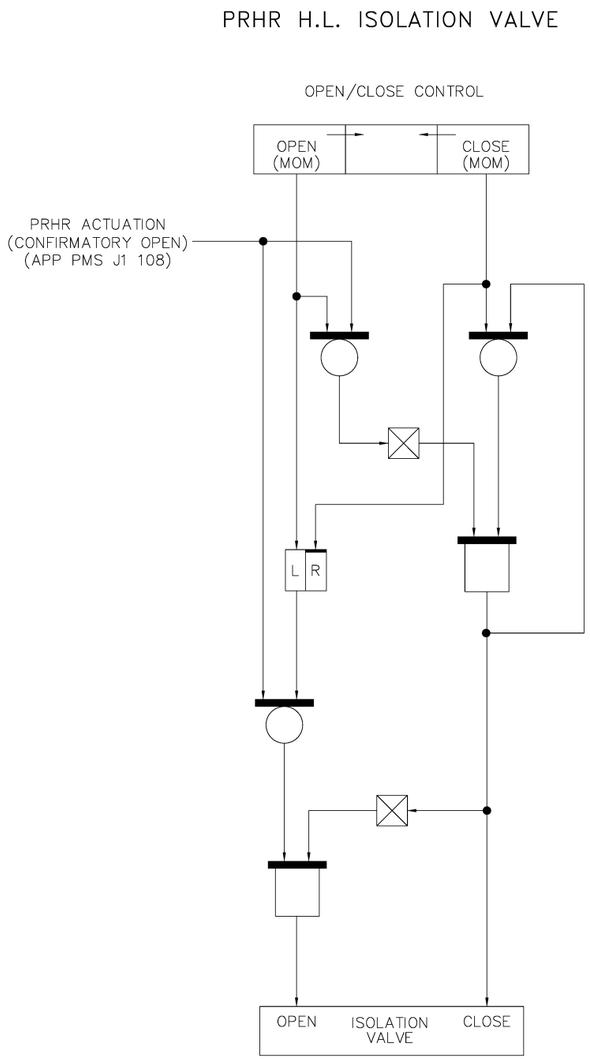


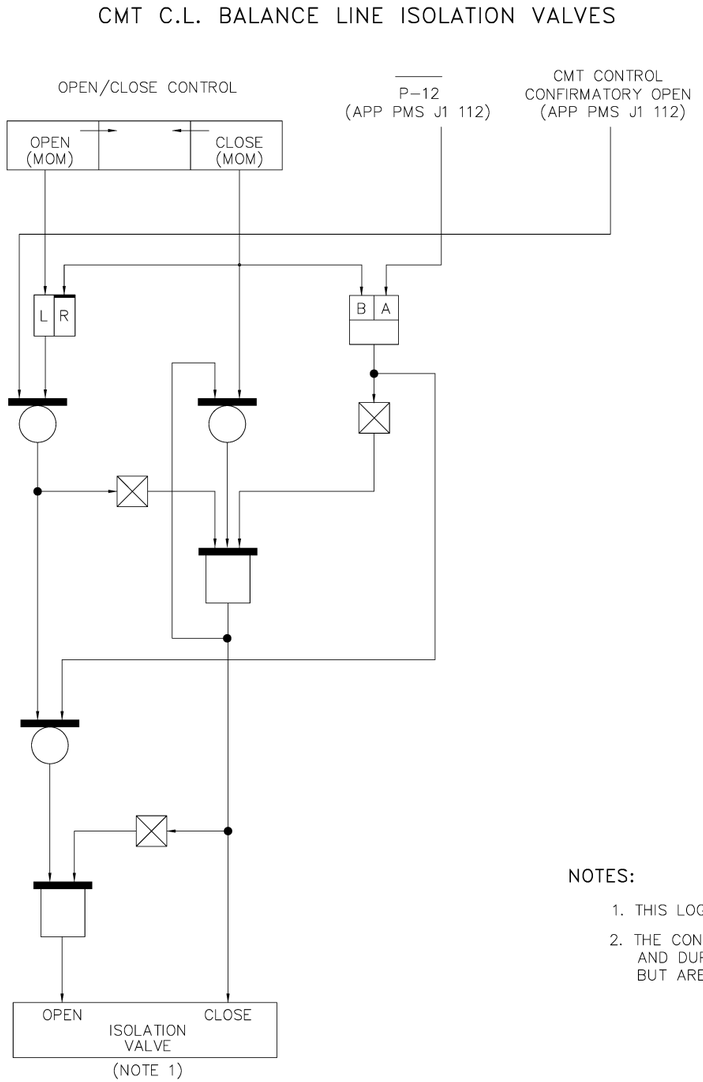
NOTES:

1. THE MANUAL ACTUATION CONSISTS OF FOUR MOMENTARY CONTROLS. IF TWO ASSOCIATED CONTROLS ARE OPERATED SIMULTANEOUSLY, ACTUATION WILL OCCUR IN ALL APPLICABLE DIVISIONS.
2. COMPONENTS ARE ALL INDIVIDUALLY SEALED IN (LATCHED), SO THAT LOSS OF THE ACTUATION SIGNAL WILL NOT CAUSE THESE COMPONENTS TO RETURN TO THE CONDITION HELD PRIOR TO THE ADVENT OF THE ACTUATION SIGNAL.
3. CVS LETDOWN ISOLATION ALSO OCCURS DURING CONTAINMENT ISOLATION. SEE APP PMS J1 113.
4. SEPERATE MOMENTARY CONTROLS, ONE FOR EACH APPLICABLE DIVISION.

Figure 7.2-1 (Sheet 16 of 20)

Functional Diagram
In-Containment Refueling Water Storage Tank Actuations





NOTES:

1. THIS LOGIC IS REPEATED FOR EACH VALVE.
2. THE CONTROLS ARE LOCATED IN THE MAIN CONTROL ROOM AND DUPLICATED AT THE REMOTE SHUTDOWN WORK STATION, BUT ARE NOT FUNCTIONAL AT BOTH LOCATIONS SIMULTANEOUSLY.

Figure 7.2-1 (Sheet 17 of 20)

Functional Diagram
Passive Residual Heat Removal and
Core Makeup Tank Isolation Valve Interlocks

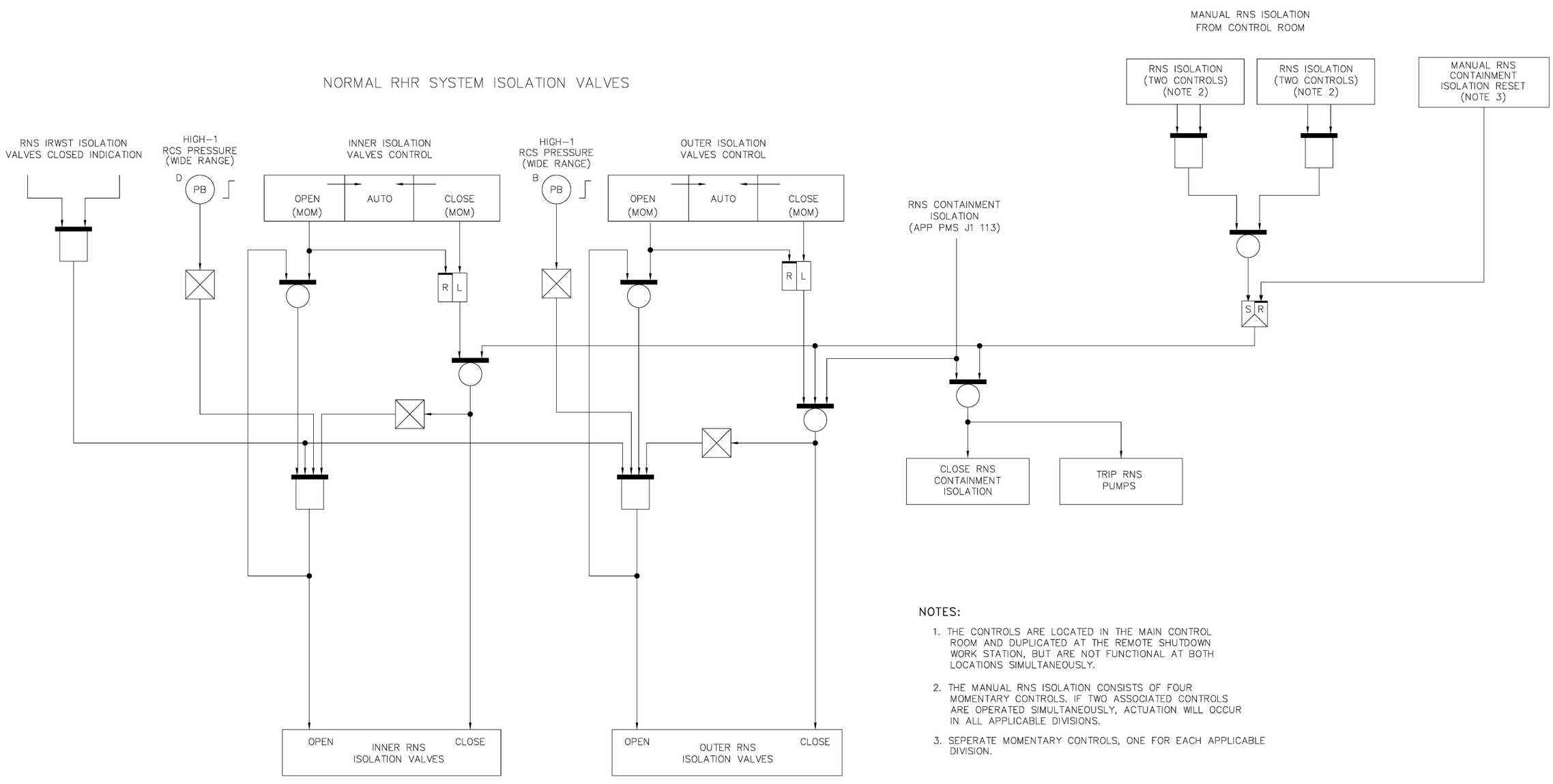


Figure 7.2-1 (Sheet 18 of 20)

Functional Diagram
Normal Residual Heat Removal System Isolation Valve Interlocks

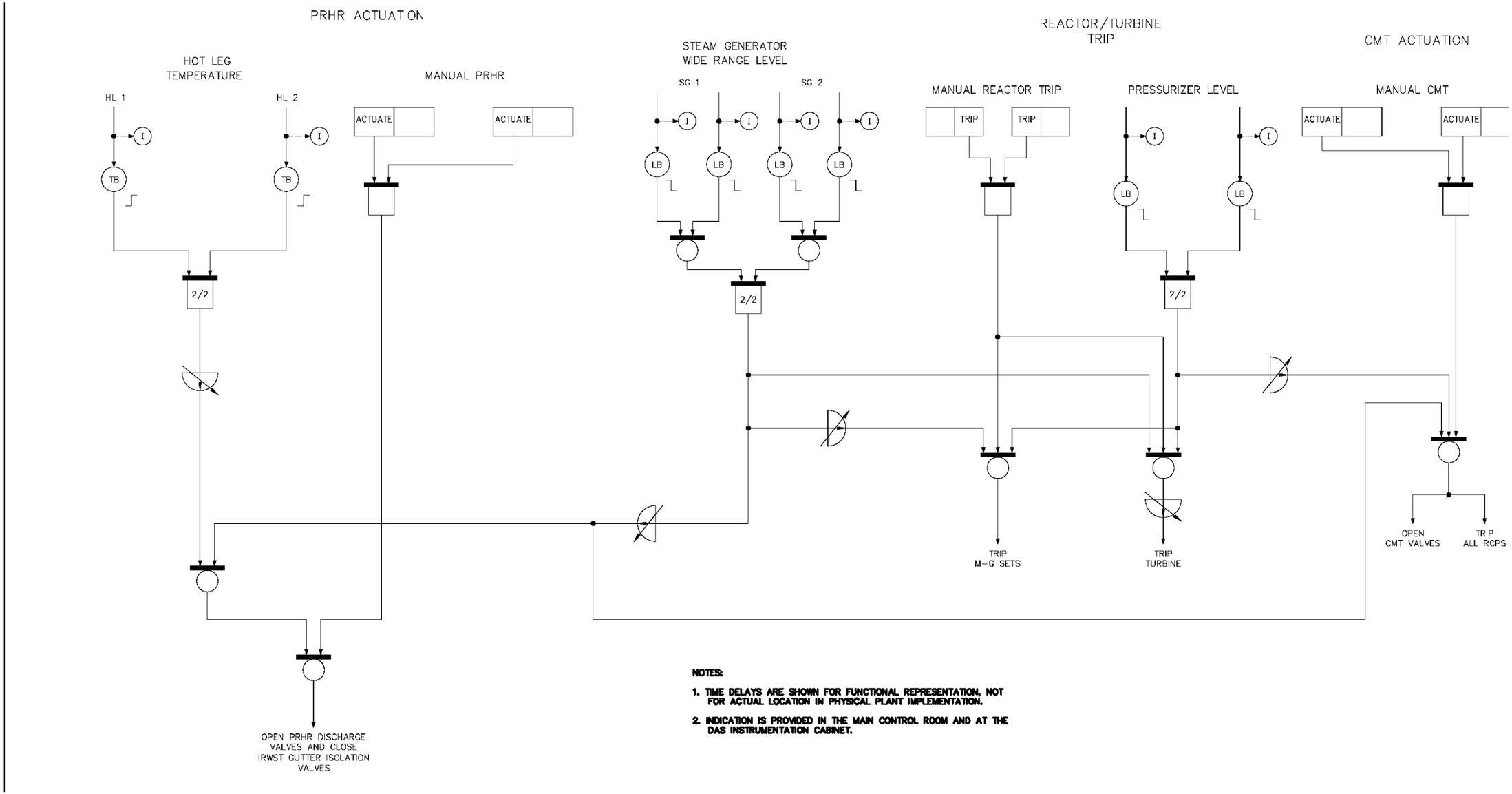
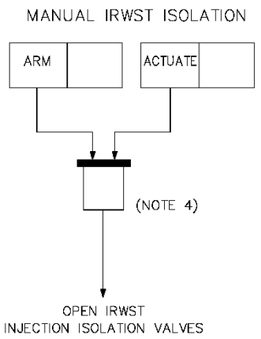
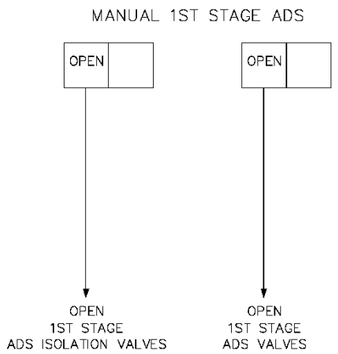
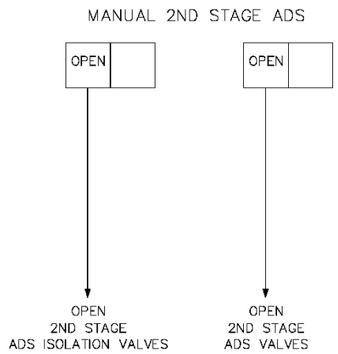


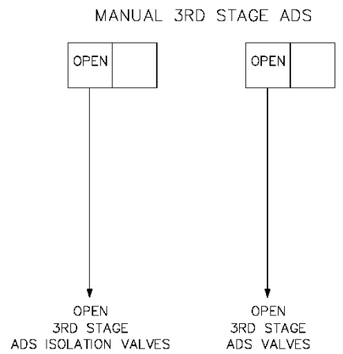
Figure 7.2-1 (Sheet 19 of 20)

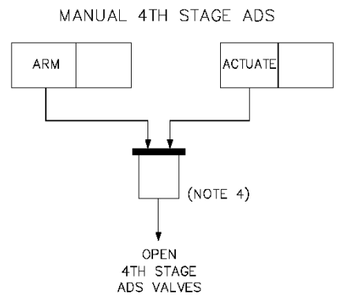
Functional Diagram
Diverse Actuation System Logic Automatic Actuations

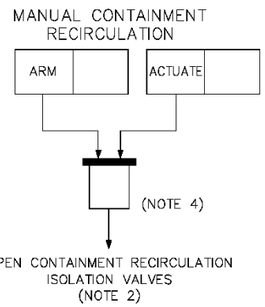


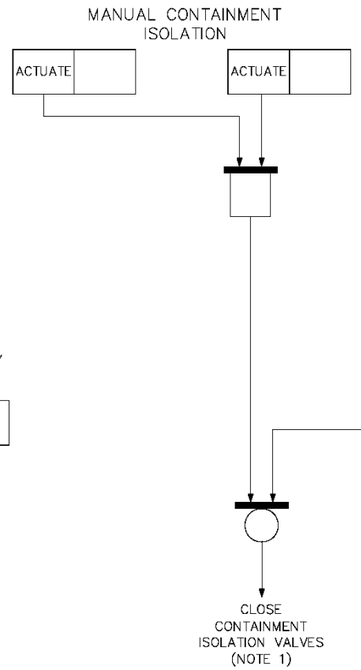


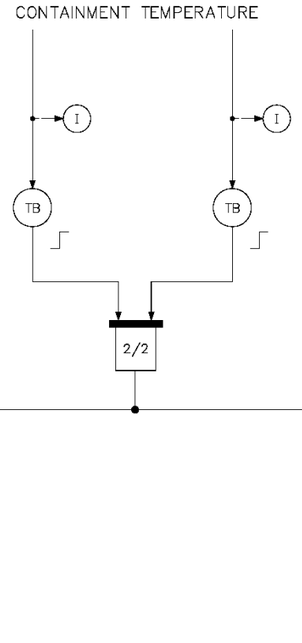


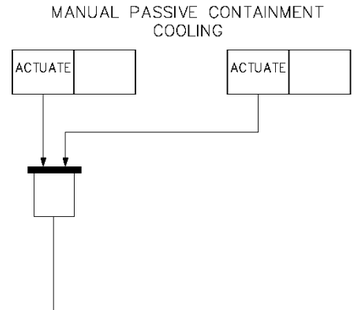


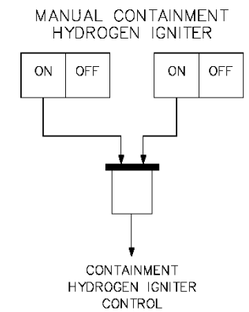


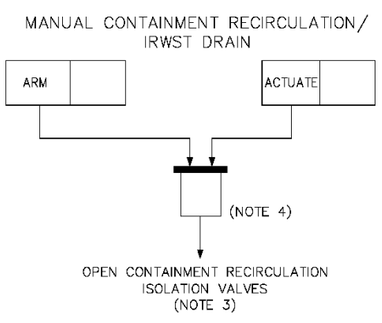


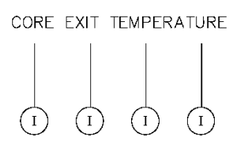












NOTES:

1. ISOLATION OF ONLY SELECTED CRITICAL CONTAINMENT PENETRATIONS.
2. OPENS ISOLATION VALVES IN SERIES WITH CHECK VALVES.
3. OPENS ISOLATION VALVES IN RECIRCULATION LINES WITHOUT CHECK VALVES.
4. LOGICAL "AND" FUNCTION PERFORMED BY SQUIB VALVE CONTROLLER.

Figure 7.2-1 (Sheet 20 of 20)

Functional Diagram
Diverse Actuation System Logic, Manual Actuations