7.4 EMERGENCY CORE COOLING CONTROL AND INSTRUMENTATION

7.4.1 Safety Objective

The controls and instrumentation for the Emergency Core Cooling Systems initiate appropriate responses from the various cooling systems so that the fuel is adequately cooled under abnormal or accident conditions. The cooling provided by the systems restricts the release of radioactive materials from the fuel by limiting the extent of fuel damage following situations in which reactor coolant is lost from the nuclear system.

Even after the reactor is shut down from power operation by the full insertion of all control rods, heat continues to be generated in the fuel as radioactive fission products decay. An excessive loss of reactor coolant allows the fuel temperature to rise, cladding to melt, and fission products in the fuel to be released. If the temperatures in the reactor rise to a sufficiently high value, a metal (zirconium) water reaction occurs which releases energy. Such a reaction increases the pressure inside the nuclear system and the primary containment. This threatens the integrity of the barriers, which are relied upon to prevent the uncontrolled release of radioactive materials. The controls and instrumentation for Emergency Core Cooling Systems prevent such a sequence of events by actuating core cooling systems in time to limit fuel temperatures to acceptable levels (less than 2200°F).

7.4.2 Safety Design Basis

1. Controls and instrumentation shall (with precision and reliability) automatically initiate and control the Emergency Core Cooling Systems to allow removal of heat from the reactor core in time to prevent cladding temperatures in excess of 2200°F so that fuel and core deformation do not limit effective cooling of the core.

2. Controls and instrumentation shall (with precision and reliability) initiate and control the Emergency Core Cooling Systems with sufficient timeliness to prevent more than a small fraction of the core from heating to a temperature at which a gross release of fission products occurs.

3. To meet the precision requirements of safety design bases 1 and 2, the controls and instrumentation for the Emergency Core Cooling Systems shall respond to conditions that indicate the potential inadequacy of core cooling, regardless of the physical location of the defect causing the inadequacy.

4. To place limits on the degree to which safety is dependent on operator judgment in time of stress, the following safety design bases are specified:

a. Appropriate responses of the Emergency Core Cooling Systems shall be initiated automatically by control systems when positive precise action is immediately required, so that no decision or manipulation of controls beyond the capacity of plant operations personnel is demanded.

b. Intelligence of the responses of the Emergency Core Cooling Systems shall be provided to the operator by control room instrumentation, so that faults in the actuation of safety equipment can be diagnosed.

c. Facilities for manual actuation of the Emergency Core Cooling Systems shall be provided in the control room, so that operator action is possible, yet reserved for the remedy of a deficiency in the automatic actuation of the safety equipment or for control over the long-term effects of an abnormal or accident condition.

5. To meet the reliability requirements of safety design bases 1 and 2, the following safety design bases are specified:

a. No single failure, maintenance, calibration, or test operation shall prevent the integrated operations of the Emergency Core Cooling Systems from providing adequate core cooling.

b. No protective device which causes interruption of performance or availability of the Emergency Core Cooling Systems shall be automatic, unless there is a high probability that continued use would make complete failure imminent. Instead, such protective devices shall indicate off-standard conditions for operator decision and action.

c. Any installed means of manually interrupting the availability of the Emergency Core Cooling Systems shall be under administrative control.

d. The power supplies for the controls and instrumentation for the Emergency Core Cooling Systems shall be chosen so that core cooling can be accomplished concurrently with a loss of normal auxiliary AC power.

e. The physical events that accompany a loss-of-coolant accident shall not interfere with the ability of the controls and instrumentation of the Emergency Core Cooling Systems to function properly.

f. Earthquake ground motion shall not impair the ability of essential controls and instrumentation of the Emergency Core Cooling Systems to function properly.

6. To provide the operator with the means to verify the availability of the Emergency Core Cooling Systems, it shall be possible to test the responses of the controls and instrumentation to conditions representative of abnormal or accident situations.

7.4.3 Descriptions

7.4.3.1 Identification

The controls and instrumentation for the Emergency Core Cooling Systems are identified as that equipment required for the initiation and control of the following:

a. High Pressure Coolant Injection System (HPCI),

b. Automatic Depressurization System,

c. Core Spray System, and

d. Low Pressure Coolant Injection System (LPCI) (an operating mode of the Residual Heat Removal System).

The equipment involved in the control of these systems includes automatic injection valves, turbine pump controls, electric pump controls, relief valve controls, and the switches, contacts, and relays that make up sensory logic channels. Testable check valves and certain automatic isolation valves are not included in this description because they are described in Subsection 7.3, "Primary Containment Isolation System."

To ensure the functional capabilities of the Emergency Core Cooling Systems during and after earthquake ground motions, the controls and instrumentation for each of the systems are designed as Class I equipment as described in Appendix C. This meets safety design basis 5f.

Backup controls are provided for the ECCS, as indicated in Figures 6.4-1, 6.4-3, and 6.4-5, 7.4-6b Sheets 1 through 5, and Section 7.18.

7.4.3.2 High Pressure Coolant Injection System (HPCI) Control and Instrumentation

7.4.3.2.1 Identification and Physical Arrangement

When actuated, the HPCI system pumps water from either the condensate supply header or the pressure suppression chamber to the reactor vessel via the feedwater pipelines. The HPCI includes one turbine which drives both main and booster pumps, one DC motor-driven auxiliary oil pump, one gland seal condenser DC condensate pump, one gland seal condenser DC blower, automatic valves, control

devices for this equipment, sensors, and logic circuitry. The arrangement of equipment and control devices is shown in Figures 6.4-1, 6.4-3, 6.4-5, and 7.4-6b Sheets 1 through 5.

Pressure and level transmitters used in the HPCI are located on racks in the Reactor Building. The only operating component for the HPCI that is located inside the primary containment is one of the two HPCI turbine steam supply pipeline isolation valves. The rest of the HPCI control and instrumentation components are located outside the primary containment. Cables connect the sensors to control circuitry in the Auxiliary Instrument and Main Control Room. The system is arranged to allow full-flow functional testing during normal reactor power operation. Test controls are arranged so that the injection flow path will be automatically re-aligned to the reactor vessel should a HPCI initiation signal be received while testing. The HPCI flow controller could be in either AUTO or MANUAL during testing with the flow adjusted to less than full design flow rate. Operator action would be required to adjust the flow back to the design flow rate. The HPCI System is designed to meet the intent of the IEEE proposed criteria for Nuclear Power Plant Protection Systems (IEEE-279-1971).

7.4.3.2.2 HPCI Initiation Signals and Logic

Reactor vessel low-water level and primary containment (drywell) high pressure are the two functions, either of which can automatically start the HPCI. Reactor vessel low-water level is an indication that reactor coolant is being lost and that the fuel is in danger of being overheated. Primary containment high pressure is an indication that a breach of the nuclear system process barrier has occurred inside the drywell.

The logic scheme used for the initiating functions is a dual trip system arrangement. Each trip system receives initiation signals from two independent sensor channels for each monitored variable. Either trip system can start the HPCI. The trip systems are powered from reliable DC buses.

The reactor vessel low-water level setting for HPCI initiation is selected high enough above the active fuel to start the HPCI in time, both to prevent excessive fuel clad temperature and to prevent more than a small fraction of the core from reaching the temperature at which gross fuel failure occurs. The water level setting is far enough below normal levels that spurious HPCI startups are avoided. The primary containment high-pressure setting is selected to be as low as possible without including spurious HPCI startup.

7.4.3.2.3 HPCI Initiating Instrumentation

Reactor vessel low-water level is monitored by four level transmitters that sense the difference between the pressure due to a constant reference column of water and the pressure due to the actual height of water in the vessel. Two pipelines, attached

to taps above and below the water level on the reactor vessel, are required for the differential pressure measurement for each pair of transmitters. The pipelines terminate outside the primary containment and inside the Reactor Building; they are physically separated from each other and tap off the reactor vessel at widely separated points. These same pipelines are also used for pressure and water level instruments for other systems. The level transmitters for the HPCI are arranged in pairs, each pair sensing level from different pipelines. One transmitter in each pair provides an input to trip system A, the other to trip system B. This arrangement assures that no single event can prevent HPCI initiation from reactor vessel low-water level. Cables from the level transmitters lead to the auxiliary instrument room.

Primary containment pressure is monitored by four pressure transmitters which are mounted on instrument racks outside the drywell, but inside the Reactor Building. Cables are routed from the transmitters to the auxiliary instrument room. Pipes that terminate in the Reactor Building allow the transmitters to communicate with the drywell interior. The transmitters are grouped in pairs and electrically connected so that no single event can prevent the initiation of the HPCI due to primary containment high pressure.

7.4.3.2.4 HPCI Turbine and Turbine Auxiliaries Control

The HPCI controls automatically start the HPCI from the receipt of a reactor vessel low-water-level signal or primary containment high-pressure signal and bring the system to its design flow rate within 30 seconds (see Section 6.5 for value assumed in Emergency Core Cooling System analyses).

The controls then function to provide design makeup water flow to the reactor vessel until a high reactor water level trip is received at which time HPCI shuts down. The controls are arranged to allow remote-manual startup, operation, and shutdown.

HPCI flow is compared against the flow controller setting and turbine speed adjusted accordingly to achieve design flow. The flow signal used for automatic control of the turbine is derived from a differential pressure measurement across an orifice type flow element in the HPCI discharge line. The HPCI Lube Oil System furnishes hydraulic pressure to the turbine stop and control valves by a DC powered auxiliary oil pump during startup and a turbine shaft driven oil pump as turbine speed increases.

Upon receipt of an initiation signal, the auxiliary oil pump starts and other automatic actions (e.g., steam admission valve opens) occur. Operation of the auxiliary oil pump provides lube oil pressure sufficient to begin opening the turbine stop and control valves. Because there is no HPCI flow at this point, the flow controller will be asking the turbine speed governor for full demand. When sufficient oil pressure is available to open the turbine stop valve, a limit switch on the valve starts the turbine

speed governor ramp generator function. This action takes the turbine control valve in the close direction until turbine speed begins reopening the valve so that the ramp function is followed. Once the ramp output exceeds the flow controller demand, the flow controller takes over turbine speed control and maintains HPCI flow at the design flow rate over the design range of HPCI discharge pressure.

The turbine is automatically shut down by tripping the turbine stop valve closed if any of the following conditions are detected (reset capability has been provided):

a. Auto isolation signal,

b. High turbine exhaust pressure,

c. Low pump suction pressure,

d. Low turbine steam supply pressure

e. Reactor vessel high-water level,

f. Turbine mechanical overspeed.

High turbine exhaust pressure indicates a condition that threatens the physical integrity of the exhaust pipeline. Low pump suction pressure warns that cavitation and lack of cooling could cause damage to the booster and/or main pump which could place the HPCI System out of service. A turbine trip is initiated for these conditions so that, if the causes of the abnormal conditions can be found and corrected, the system can be quickly restored to service. The turbine will automatically reset when these conditions are cleared. The turbine will then automatically restart if the required initiation signals are present. The trip settings are selected far enough from normal values so that a spurious turbine trip is unlikely, but not so close that damage occurs before the turbine is shut down. Turbine overspeed is detected by a standard turbine overspeed mechanical-hydraulic device which automatically resets after the turbine trip. Two pressure switches are used to detect high turbine exhaust pressure; either switch can initiate turbine shutdown. One pressure switch is used to detect low HPCI pump suction pressure.

High-water level in the reactor vessel indicates that the HPCI has performed satisfactorily in providing makeup water to the reactor vessel. Further increase in level could result in HPCI turbine damage caused by gross carryover of moisture. The reactor vessel high-water-level setting which trips the turbine is near the top of the steam separators and is sufficient to prevent gross moisture carryover to the main steam line and then to the HPCI turbine. The two level transmitters that sense differential pressure feed analog trip units that are arranged to require that both analog trip units trip (coincidence) to initiate a turbine shutdown. The turbine will automatically restart on a low-water-level signal.

The controls are arranged for automatic or manual control. Upon receipt of an HPCI initiation signal, the auxiliary oil pump starts and provides hydraulic pressure to open the turbine stop valve and the turbine control valve. As the turbine gains speed, the shaft-driven oil pump begins to supply hydraulic pressure. After about 1/2 minute during an automatic turbine startup, the pressure supplied by the shaft-driven oil pump is sufficient, and the auxiliary oil pump automatically stops upon receipt of a high oil pressure signal. Should the shaft-driven oil pump malfunction, causing oil pressure to drop, the auxiliary oil pump restarts.

Operation of the gland seal condenser components--gland seal condenser condensate pump (DC), gland seal condenser blower (DC), and gland seal condenser water level instrumentation--capable of preventing outleakage from the turbine shaft seals. Startup of this equipment is automatic. Failure of this equipment will not prevent the HPCI from providing water to the reactor vessel.

7.4.3.2.5 HPCI Valve Control

All automatic valves in the HPCI System are equipped with remote-manual test capability, so that the entire system can be operated locally, with the exception of the inboard steam line isolation valve, or from the Main Control Room. Motor-operated valves are provided with appropriate torque switches or limit switches to turn off the motors when the full-closed positions are reached. Certain valves are automatically closed on isolation or turbine trip signals. All essential components of the HPCI controls operate from a reliable DC power source.

To ensure that the HPCI can be brought to design flow rate within 30 seconds from the receipt of the initiation signal, the following maximum operating times for essential HPCI valves are provided by the valve operation mechanisms.

HPCI turbine steam supply valve	30 seconds
HPCI pump discharge valves	30 seconds
HPCI pump minimum flow bypass valve	15 seconds

The operating time for both the pump discharge valves and minimum flow bypass valve is the time for the valve to travel from the fully closed to the fully open position, or vice versa. The operating time for the steam admission valve is the time to travel from fully closed to opened sufficiently to provide adequate steam flow to allow the HPCI system to deliver required flow to the vessel.

The two HPCI steam supply line isolation valves are intended to isolate the HPCI steam line in the event of a break in that line; the operating time requirements for them are based on isolation specifications. These are described in Subsection 7.3, "Primary Containment Isolation System." A normally closed, DC motor-operated

isolation valve is located in the turbine steam supply pipeline just upstream of the turbine stop valve. Upon receipt of an HPCI initiation signal, this valve opens and remains open until closed by operator action from the control room.

Two normally open isolation valves are provided in the steam supply line to the turbine. The valve inside the drywell is controlled by an AC motor fed from a reactor MOV board. The valve outside the drywell is controlled by a DC motor. An electrically operated valve with automatic isolation function is in parallel with the outside containment isolation valve for start up after isolation purposes. The valves automatically close upon receipt of an HPCI turbine steam line high-flow signal, an HPCI turbine steam supply low-pressure signal, high steam line space temperature, or high turbine exhaust (diaphragm) rupture disc pressure. The instrumentation for isolation is described in Subsection 7.3, "Primary Containment Isolation System."

Three pump suction valves are provided in the HPCI. One valve lines up pump suction from the condensate supply header, the other two from the pressure suppression chamber. The condensate supply header is the preferred source. All three valves are operated by DC motors. Although the condensate storage tank suction valve is normally open, an HPCI initiation signal opens it if it is closed. If the level in the condensate supply header falls below a preselected value, the pressure suppression chamber suction valves automatically open. When the pressure suppression chamber valves are both fully open, the condensate supply header suction valve automatically closes. Two level switches are used to detect the condensate supply header level. Either switch can cause the pressure suppression chamber suction valves to open. The pressure suppression chamber suction valves also automatically open and the condensate supply header suction valve closes if a high-water level is detected in the pressure suppression chamber. Two level switches monitor the pressure suppression chamber water level. Either switch can initiate opening of the pressure suppression chamber suction valves. If open, the pressure suppression chamber suction valves automatically close upon receipt of the signals that initiate HPCI steam line isolation.

Two DC motor-operated HPCI pump discharge valves in the pump discharge pipeline are provided. One valve is used for maintenance purposes and remains in the open position during standby conditions. The other valve is normally closed. Both valves receive an open signal upon receipt of a HPCI initiation signal. The valves remain open upon receipt of a turbine trip signal until closed by operator action in the control room.

To prevent the pump from being damaged by overheating at reduced HPCI pump discharge flow, pump discharge minimum flow bypass is provided to route the water discharged from the pump back to the pressure suppression chamber. The bypass is controlled by an automatic, DC motor-operated valve. If a HPCI initiation signal is present, the minimum flow bypass valve will open until HPCI flow increases at which time the valve will close. A flow switch that measures the pressure difference

across a flow element in the HPCI pump discharge pipeline provides the signals used for automatic operation of the minimum flow bypass valve. There is also an interlock provided to shut the minimum flow bypass whenever the turbine is tripped. This is necessary to prevent drainage from the condensate supply header into the pressure suppression pool. In the event that the trip signal is reset and a valid HPCI initiation signal is present, the minimum flow bypass valve will reopen. However, the condensate drainage into the pressure suppression pool will be quite small and provides ample time for the operator to close the valve before pressure suppression pool level is affected.

To prevent the HPCI steam supply pipeline from filling up with water, a condensate drain pot, steam line drain with steam trap, and appropriate valves are provided in a drain pipeline arrangement just upstream of the turbine steam supply valve. The controls position valves so that during normal operation steam line drainage is routed to the main condenser. Upon receipt of an HPCI initiation signal, the turbine supply valve opens. The drainage path is isolated when the turbine steam supply valve is not fully closed. Excessive water collected in the condensate pot is controlled by a level control switch which opens the steam trap bypass level control valve to allow condensate to flow to the condenser. In the event that the condensing rate exceeds the blowdown rate, a level switch actuates to annunciate a high condensate pot level condition in the main control room and, at the same time, opens the HPCI steam line steam trap bypass valve to bypass the steam trap which is in series with the main condenser drain path. In Unit 1, excessive water collected in the condensate pot is drained to the condenser by a manual steam trap bypass valve. If a level switch actuates to annunciate a high condensate pot level condition in the main control room, the steam trap/drain pot arrangement must be manually drained using the steam trap bypass valve. Bypassing the steam trap reduces flow friction in the drain line and substantially increases flow to the condenser in order to return the condensate pot to its normal operating level.

During test operation, the HPCI pump discharge is routed to the condensate storage tanks. Two DC motor-operated test return throttle and block valves are installed in a test return line off the HPCI pump discharge line in order to route pump discharge flow back to the condensate storage tanks. The piping arrangement is shown in Figures 6.4-1, 6.4-3, and 6.4-5. Upon receipt of an HPCI initiation signal, the valves close and remain closed. The valves are automatically closed if either of the pressure suppression chamber suction valves are open. Numerous indications pertinent to the operation and condition of the HPCI are available to the control room operator. Figures 6.4-1, 6.4-3, and 6.4-5 show the control and logic of the various indications provided.

7.4.3.2.6 HPCI Environmental Considerations

The only HPCI control component located inside the primary containment that must remain functional in the environment resulting from a loss-of-coolant accident is the

control mechanism and motor for the inboard isolation valve on the HPCI turbine steam line. The environmental capabilities of this valve and motor are discussed in Subsection 7.3, "Primary Containment Isolation System." The HPCI control and instrumentation equipment located outside the primary containment is selected in consideration of the normal and accident environments in which it must operate.

7.4.3.3 Automatic Depressurization System (ADS) Control and Instrumentation

7.4.3.3.1 Identification and Physical Arrangement

Automatically controlled relief valves are installed on the main steam lines inside the primary containment. Six of the valves are dual purpose in that they will relieve pressure by normal mechanical action or by automatic action of an electro-pneumatic control system (see Subsection 4.4, "Nuclear System Pressure Relief System"). The relief by normal mechanical action is intended to prevent overpressurization of the nuclear system. The depressurization by automatic action of the control system is intended to reduce nuclear system pressure during a loss-of-coolant accident in which the HPCI fails, so that the relatively low-pressure core spray and LPCI systems can inject water into the reactor vessel. The ADS automatic control and instrumentation equipment for the main steam relief valves is described in this subsection. The controls and instrumentation for one of the main steam relief valves are discussed. Other main steam relief valves equipped for automatic depressurization are identical.

The control system consists physically of pressure and water level transmitters arranged in trip systems that control a solenoid-operated pilot air valve. The solenoid-operated pilot valve controls the pneumatic pressure applied to a diaphragm actuator which controls the main steam relief valve directly. An accumulator is included with the control equipment to store pneumatic energy for main steam relief valve operation. The accumulator is sized to hold five times the volume of air required for one valve operation following failure of the normal pneumatic supply to the accumulator. In addition, an emergency source of nitrogen is provided by the CAD system. Cables from the transmitters lead to the auxiliary instrument room where the logic arrangements are formed in cabinets. The electrical control circuitry is powered by direct current from the unit batteries. Both ADS initiation logic bus circuits are powered from a common source; however, one of the logic bus circuits is provided with an automatic transfer capability to an alternate power source so that the ADS automatic activation function will not be lost in the event of any single 250V DC power failure. See Table 6.5-3 for the Emergency Core Cooling Systems which are available for both recirculation suction and discharge breaks following an assumed single failure. Electrical elements in the control system energize to cause opening of the main steam relief valve. The automatic depressurization system is designed to meet the intent of the IEEE proposed criteria for Nuclear Power Plant Protection Systems (IEEE-279-1971).

7.4.3.3.2 Automatic Depressurization System Initiating Signals and Logic

The initiating signals for the Automatic Depressurization System are reactor vessel low-water level, and primary containment (drywell) high pressure or a sustained reactor vessel low-water level signal will provide the initiating signal after a time delay. The above initiation paths and a permissive signal verifying that the two core spray or at least one RHR pumps are running must be present to cause the main steam relief valves to open. This permissive signal is not required to start the ADS delay timers but must be present to actuate the main steam relief valves. However, verification that the two core spray or at least one RHR pumps are running is required for ADS actuation for Units 1, 2, and 3. Reactor vessel low-water-level indicates that the fuel is in danger of becoming overheated. This low water level would normally not occur unless the HPCI failed. Primary containment high pressure indicates that a breach in the nuclear system process barrier has occurred inside the drywell.

After receipt of the initiation signals, and after a 120 seconds delay provided by timers, the solenoid-operated pilot air valve is energized, providing that at least one LPCI pump or the appropriate two core spray pumps are running, allowing pneumatic pressure from the accumulator to act on the diaphragm actuator. Pump discharge pressure switches are used to sense that the core spray or LPCI pumps are running. The diaphragm actuator is an integral part of the main steam relief valve and expands to hold the main steam relief valve open. Lights in the control room inform the control room operator whenever the solenoid-operated pilot valve is energized, indicating that the main steam relief valve is open or being opened.

A two-position switch is provided in the control room for the control of the main steam relief valves. The two positions are "open" and "auto." In the open position, the switch energizes the solenoid-operated pilot valve, which allows pneumatic pressure to be applied to the diaphragm actuator of the main steam relief valve. This allows the control room operator to take action independent of the automatic system. The main steam relief valves can be manually opened to provide a controlled nuclear system cooldown under conditions where the normal heat sink is not available. Manual reset circuits and key-lock inhibit switches are provided for the reactor vessel low-water level and primary containment high-pressure initiating signals. By manually resetting the ADS initiating signals, the delay timers are recycled. By manually turning the key-lock inhibit switches to inhibit position, the ADS initiating signals are blocked preventing automatic opening of the main steam relief valves. This action is however, annunciated on the control room annunciators. The operator can use the reset switches to delay automatic opening of the main steam relief valves or use the key-lock inhibit switches to prevent the opening of the main steam relief valves indefinitely if such actions are deemed prudent throughout the cooldown period. If at any time the circuits are not reset or the key-lock inhibit switches are not engaged, blowdown will start and will continue unless the circuits are manually reset to recycle the timers or the key-lock inhibit switches are engaged.

Each trip system can initiate automatic depressurization when the logic in that trip system is satisfied. The logic of each trip system includes a timer that delays the opening of the main steam relief valve. This allows time for the operator to decide whether it is prudent to further postpone automatic depressurization.

Automatic Depressurization System Instrumentation and settings are listed in Table 7.4-2. The wiring for the trip systems is routed in separate conduits to reduce the probability that a single event will prevent automatic opening of a main steam relief valve.

The reactor vessel low-water-level initiation setting for the Automatic Depressurization System is selected to open the main steam relief valves to depressurize the reactor vessel in time to allow adequate cooling of the fuel by the Core Spray and LPCI Systems following a loss-of-coolant accident in which the other makeup systems (feedwater, RCICS, HPCI) fail to maintain vessel water level. The primary containment high-pressure setting is selected to be as low as possible without inducing spurious initiation of the Automatic Depressurization System.

7.4.3.3.3 Automatic Depressurization System Initiating Instrumentation

The pressure and level transmitters used to initiate the Automatic Depressurization System are common to each main steam relief valve control circuitry. Reactor vessel low-water level is detected by six transmitters that measure differential pressure. Primary containment high pressure is detected by four pressure transmitters. Some of the transmitters used for these two initiating functions are the same ones used for the LPCI and Core Spray System. The primary containment high-pressure signals are arranged to seal into the control circuitry, they must be manually reset to clear.

Two timers are used in the control circuitry for each main steam relief valve. The delay time setting before the Automatic Depressurization System is actuated is chosen to be long enough so that the HPCI has time to start, yet not so long that the Core Spray System and LPCI are unable to adequately cool the fuel if the HPCI fails to start. An alarm in the control room is tripped when either of the timers is operating. Resetting the Automatic Depressurization System initiating signals recycles the timers.

The requirement that at least one of the LPCI pumps or two core spray pumps be running before automatic depressurization starts insures that cooling will be available to the core after the system pressure is lowered.

7.4.3.3.4 Automatic Depressurization System Alarms

A single-train acoustic monitoring system has been installed to provide unambiguous main control room indication of main steam relief valve position (open or closed) and alarm. The acoustic monitoring system detects steam flow in the main steam relief valve discharge pipeline by using an accelerometer which is physically attached to the discharge tailpipe downstream. The accelerometers transmit conditioned signals back to a common electronics module located in the main control room. For each valve, the electronic module inserts a selective gain into the signal and provides a relative indication of steam flow through a series of ten indicating lights. A control room alarm initiates when the fifth light is illuminated.

A main steam relief valve discharge tailpipe temperature monitoring system is provided to detect and provide indication of relief status. A temperature element is installed in a thermowell in the main steam relief valve discharge tailpipe downstream of the valve discharge flange. The temperature element is connected to a multipoint recorder in the control room which provides a means of detecting main steam relief valve leakage during normal plant operation. When the temperature in any main steam relief valve discharge tailpipe exceeds a preset value, an alarm condition is indicated on the recorder in the control room. The temperature recorders installed in Units 2 and 3 have the capability to selectively raise the high temperature alarm setpoint on a per channel basis. Additionally, these recorders provide an interface to the plant process computer which has the capability to display and trend the discharge tailpipe temperatures. In addition to providing a leakage indication, the main steam relief valve discharge tailpipe temperature monitoring instrumentation provides an alternate main control room indication of main steam relief valve position.

A common "MAIN STEAM RELIEF VALVE OPEN" annunciator exists in the control room with inputs from all 13 acoustic monitors. The acoustic monitor system satisfies the requirements for main steam relief valve position indication.

A key-lock inhibit switch is in-line with each ADS initiating logic channel. When a key-lock inhibit switch is in the inhibit position, an alarm is sounded in the control room to inform the operators that ADS has been inhibited.

As relays and plant process sensors within each ADS initiating logic channel are activated, control room alarms are sounded to inform the operators of a pending ADS event. These alarms include: (1) RHR or CS pump running ADS blowdown permissive, (2) reactor water level low ADS blowdown permissive, (3) ADS high drywell pressure seal-in, (4) ADS auxiliary blowdown relays energized, and (5) ADS blowdown timers initiated.

Other control room annunciations are available to inform the operators of abnormal plant conditions or test conditions under which the ADS function is reduced or

compromised. These alarms include: (1) ADS main steam relief valve accumulator low control air pressure, (2) backup control panel selector switch in the emergency position, ADS blowdown system control power failure, (3) ADS blowdown system in test status, and (4) ADS blowdown system test switches misaligned. Any of these would indicate a potential degraded ability of the ADS main steam relief valves.

7.4.3.3.5 Automatic Depressurization System Environmental Considerations

The signal cables, solenoid valves, and main steam relief valve operators are the only items of the control and instrumentation equipment of the Automatic Depressurization System that are located inside the primary containment and must remain functional in the environment resulting from a loss-of- coolant accident. These items are selected with capabilities that permit proper operation in the most severe environment resulting from a design basis loss-of-coolant accident. Gamma and neutron radiation is also considered in the selection of these items. Other equipment, located outside the drywell, is selected in consideration of the normal and accident environments in which it must operate.

7.4.3.4 Core Spray System Control and Instrumentation

7.4.3.4.1 Identification and Physical Arrangement

The Core Spray System consists of two independent spray loops, as shown in Figures 6.4-2, 6.4-4, and 6.4-6. Each loop is capable of supplying sufficient cooling water to the reactor vessel to adequately cool the core by spraying following a design basis loss-of-coolant accident. The two spray loops are physically and electrically separated so that no single physical event makes both loops inoperable. Each loop includes two AC motor-driven 50 percent-capacity pumps, appropriate valves, and the piping to route water from the pressure suppression pool to the reactor vessel. The controls and instrumentation for the Core Spray System include the sensors, relays, wiring, and valve-operating mechanisms used to start, operate, and test the system. Except for the check valve in each spray loop, which is inside the primary containment, the sensors and valve-closing mechanisms for the Core Spray System are located in the Reactor Building. The check valves are described in Section 6.0, "Emergency Core Cooling Systems." Cables from the sensors are routed to the Auxiliary Instrument Room where the control circuitry is assembled in electrical panels. The core spray pumps for each unit are powered from different AC buses that are capable of receiving standby power. The power supply for automatic valves is Class 1E and feeds from the same bus structure as the core spray pumps. Control power for each of the core spray loops comes from separate DC buses. The electrical equipment in the Auxiliary Instrument Room for one core spray loop is located in a separate cabinet from that used for the electrical equipment for the other loop. The CS System is designed to meet the intent of the IEEE proposed criteria for Nuclear Power Plant Protection Systems (IEEE-279-1971).

7.4.3.4.2 Core Spray System Initiating Signals and Logic

Trip settings are given in Table 7.4-3. The overall operation of the system following the receipt of an initiating signal is as follows:

a. Test bypass valves are closed and interlocked to prevent opening.

b. If normal AC power is available, the four core spray pumps start one at a time, in order, at 0.2, 7, 14, and 21 seconds.

c. If normal AC power is not available, the four core spray pumps start seven seconds after standby power becomes available. (The LPCI pumps start as soon as standby power is available.)

d. When reactor vessel pressure drops to 450 psig (See Section 6.5 for value utilized in the Emergency Core Cooling System analysis), the core spray inboard injection valve opens allowing water to be sprayed on the core once core spray discharge pressure overcomes RPV pressure.

e. When adequate pump discharge flow is indicated, the pump low-flow bypass valves shut, directing full flow into the reactor vessel.

Two initiating functions are used for the Core Spray System: reactor vessel low-water-level, and primary containment (drywell) high pressure plus low reactor vessel pressure (450 psig). Either initiation signal can start the system. The development of these accident signals is discussed further in Section 7.4.3.4.7.

Reactor vessel low-water level indicates that the core is in danger of being overheated due to the loss of coolant. Drywell high pressure plus low reactor vessel pressure indicate that a breach of the nuclear system process barrier has occurred inside the drywell. The reactor vessel low- water-level, primary containment high pressure and low reactor vessel pressure settings, and the instruments that provide the initiating signals are selected and arranged so as to assure adequate cooling for the design basis loss-of-coolant accident without inducing spurious system startups.

7.4.3.4.3 Core Spray System Pump Control

The circuitry provides for detection of normal power availability, so that all pumps are automatically started in sequence. Each pump can be manually controlled by a control room remote switch or by the automatic control system. A pressure transducer on the discharge pipeline from each set of core spray pumps provides a signal to an indicator in the control room to indicate the successful startup of the pumps. If a core spray initiation signal is received when normal AC power is not available, the core spray pumps start, after a seven-second time delay, to allow the

start of the LPCI pumps to avoid overloading the source of standby power. If one core spray pump fails to start owing to a loss of normal or diesel generator bus voltage, the companion core spray pump motor in the affected core spray loop will not start either in order to avoid a pump run out condition which occurs when only one pump is operating to inject water into the reactor vessel. The core spray pump motors are provided with overload and undervoltage protection. Overload relays are applied so as to maintain power as long as possible without immediate damage to the motors or emergency power system. Undervoltage trips are provided with time delays sufficient to permit power transfer from auxiliary transformers to startup transformer source without tripping the pump power supply breaker open. Undervoltage protection is locked out if an accident signal is present and the shutdown boards are being powered by the diesel-generators.

Flow-measuring instrumentation is provided in each of the core spray pump discharge lines. The instrumentation provides flow indication in the control room.

The standby AC power system is designed such that automatic restart of the core spray pumps, after manual shedding of same, is not available unless the initiating signal is removed (see Subsection 8.5).

7.4.3.4.4 Core Spray System Valve Control

Except where specified otherwise, the remainder of the description of the Core Spray System refers to one spray loop. The second core spray loop is identical. All motor-operated valves are equipped with torque and limit switches to turn off the valve motor when the valve reaches the limits of movement and to provide control room indication of valve position. Each automatic valve can be operated from the control room. Valve motors are protected by overload devices.

Upon receipt of an initiation signal, the test bypass valve closes if it is open and is interlocked closed. The outboard injection valve (normally open but will open if it is closed) and the inboard injection valve will open provided all conditions necessary to inject are satisfied. The reactor pressure permissive setpoint for injection valve opening is selected low enough such that low pressure portions of the Core Spray System can not be overpressurized and yet high enough to open the inboard injection valve in time to provide adequate core cooling. Four pressure transmitters are used to monitor nuclear system pressure; these transmitters supply four analog trip units. Two analog trip units are used to monitor reactor pressure in a one-out-of-two logic arrangement which enables the injection valves' low pressure permissive. The full stroke operating times of the motor-operated valves are selected to be rapid enough to assure proper delivery of water to the reactor vessel in a design basis accident. The full stroke operating times are as follows:

Test bypass valve	30 seconds
Pump suction valve	standard closure rate
Pump discharge valves	33 seconds
Minimum flow bypass valves	15 seconds

The standard closure rate is based on isolating a 12-inch line in 60 seconds. Conversion to actual closing time can be made on this basis using the size of the line being isolated. A flow switch on the discharge of each set of pumps provides a signal to operate the minimum flow bypass line valve for each pump set. When core spray flow into the reactor pressure vessel reaches a predetermined setpoint, the minimum flow bypass valve closes and all flow is directed into the sparger at this time.

7.4.3.4.5 Core Spray System Alarms and Indications

Core Spray System discharge pressure is monitored by a pressure switch which has a process tap just upstream of the normally closed inboard injection valve. If excessive pressure beyond that expected in the standby configuration is present, the pressure switch will actuate a Main Control Room annunciator to alert the operator to this condition so that corrective actions may be carried out.

A detection system is also provided to confirm the integrity of the core spray piping between the inside of the reactor vessel and the core shroud. A differential pressure switch measures the pressure difference between the bottom of the core and the inside of the core spray sparger pipe just outside the reactor vessel. If the core spray sparger piping is sound, this pressure difference will be the pressure drop across the core. If integrity is lost, this pressure difference will change, initiating an alarm in the control room. An increase in the normal pressure drop initiates an alarm in the control room. The pressure in each core spray pump suction and discharge line is monitored by locally mounted pressure gauges. The discharge pressure gauges are used for determining pump performance. Temporary pressure gauges are furnished during surveillance testing to measure the suction pressure of each pump for pump performance purposes because existing gauges do not provide sufficient accuracy.

7.4.3.4.6 Core Spray System Environmental Considerations

There are no control and instrumentation components for the Core Spray System located inside the primary containment that must operate in the environment resulting from a loss-of-coolant accident. All components of the Core Spray System

that are required for system operation are outside the drywell and are selected in consideration of the normal and accident environments in which they must operate.

7.4.3.4.7 Core Spray System and Accident Signal Initiation

The Core Spray System is initiated by sensors and relays based on low reactor vessel water level (Level 1 setpoint) or high drywell pressure coincident with low reactor pressure. These same sensors and relays are used to initiate the Common Accident Signal, as shown on Figures 7.4-5d, 7.4-5l and 7.4-7i. The Core Spray System initiation signal starts the core spray pumps and actuates core spray valves in the unit sensing the low water level or abnormal pressures, as discussed in Sections 7.4.3.4.3 and 7.4.3.4.4. The sensor/relay outputs are also used as inputs to the RHR (LPCI) initiation circuitry and for Units 1 and 2 only, initiate the ECCS preferred pump logic to trip the opposite unit's running RHR and Core Spray pumps.

The low reactor vessel water level or high drywell pressure coincident with low reactor pressure signals are also used to generate a Common Accident Signal, which affects the operation of components associated with all three units. The Common Accident Signal performs the following functions:

a) sends a signal to start all eight Unit 1/2 and Unit 3 diesel generators,
b) trips the diesel generator output breakers (if closed),
c) defeats selected diesel generator protective trips,
d) blocks the 4kV Shutdown Board auto transfer logic,
e) trips and blocks the fire pumps A, B, and C auto start logic,
f) starts the RHRSW (aligned to EECW) pumps,
g) blocks subsequent RHRSW (aligned to EECW) pump start signal (if already running),
h) blocks the 4kV degraded voltage trips,
i) trips the RHRSW pumps A2 and C2,
j) trips the RCW pump 1D.

The low reactor vessel water level or high drywell pressure coincident with low reactor pressure signal also inputs to the 480V load shed logic in the unit where the signal originated. When this signal occurs, coincident with diesel generator voltage available, non-essential 480V loads are shed.

The Pre-Accident Signal is generated by low reactor vessel water level (Level 1 setpoint) or high drywell pressure signals, and again affects the operation of components associated with all three units. The Pre-Accident Signal sends a signal to start all eight Unit 1/2 and Unit 3 diesel generators. This feature anticipates an event and starts all eight diesels so that they are ready for electrical loading when required by the load sequencing logic.

Following an initiation of a Common Accident Signal (CAS) on either Units 1, 2, or 3 (which trips all eight diesel breakers), subsequent accident signal trips of the diesel breakers are blocked. A second diesel breaker trip on a "unit priority" basis is provided to ensure that during combinations of spurious and real accident signals, the diesel supplied buses are stripped prior to starting the RHR pumps and other ECCS loads. This diesel breaker re-trip will only occur if a spurious accident signal or a real accident signal from the other unit has previously tripped the diesel breakers. Inputs from the RHR initiation circuitry (shown on Figures 7.4-7b, 7.4-7i, and 7.4-7p indicating low reactor vessel water level or high drywell pressure coincident with low reactor pressure), combined with an existing CAS trip signal, will re-trip the diesel breakers on the unit where the RHR initiation signal originated. The other unit's diesels will be unaffected by this second trip. Thus each unit is given priority over the block of subsequent CAS diesel breaker trips for its diesels. This diesel breaker "Unit Priority Re-Trip" ensures that the diesel buses are stripped prior to starting the RHR pumps, Core Spray pumps and other required loads. Section 8.5 provides a discussion and evaluation of the CAS signals to the diesel generator breakers and the Unit Priority Re-Trip signal.

For Units 1 and 2 only, the RHR and Core Spray pumps for both units are powered from the same 4kV shutdown boards (see Chapter 8). If the ECCS loads for both Units 1 and 2 were allowed to start during combinations of real and spurious accident signals, the combined Unit 1/2 ECCS pumps would overload the 4kV shutdown boards and their associated diesel generators on a loss of offsite power, or the 4kV shutdown buses if normal power were available. Therefore, during combinations of real and spurious accident signals the Unit 1/2 ECCS preferred pump logic will assign the Unit 1 ECCS loads to the Division I 4kV shutdown boards and the Unit 2 ECCS loads to the Division II 4kV shutdown boards. The Unit 1/2 ECCS preferred pump logic will allow the Unit 1 Division I RHR and Core Spray pumps (1A and 1C) to start and load on the Division I 4kV shutdown boards, and the Unit 2 Division II pumps (2B and 2D) will load on the Division II 4kV shutdown boards. This will ensure that the shared Unit 1/2 4kV shutdown boards are not overloaded while still maintaining the minimum number of required ECCS injection subsystems described in Table 6.5-3.

If an accident signal was initiated in only one unit (Units 1 or 2) and any RHR or Core Spray pumps were already running in the opposite non-accident unit (e.g. for shutdown cooling), the Core Spray system will initiate the preferred pump logic to trip all of the non-accident unit’s running RHR and Core Spray pumps. This ensures that any running RHR or Core Spray pumps in the non-accident unit would be tripped, unloading the Unit 1/2 4kV shutdown boards prior to the accident unit starting all of its ECCS pumps (both divisions) on an accident signal, with or without a loss of offsite power.

7.4.3.5. Low Pressure Coolant Injection Control and Instrumentation

7.4.3.5.1. Identification and Physical Arrangement

Low pressure coolant injection (LPCI) is an operating mode of the Residual Heat Removal System (RHRS) that uses pumps and piping which are parts of the RHRS. Because the LPCI system is designed to provide cooling water to the reactor vessel following the design basis loss-of-coolant accident, the controls and instrumentation for it are discussed here. Section 4.8, “Residual Heat Removal System,” describes the RHRS in detail.

The LPCI system for Units 1, 2, and 3 has been modified from the original design. This modification changed the low pressure coolant injection mode of the RHR by deleting automatic loop selection in case of a loss-of-coolant accident by permitting simultaneous injection into both recirculation loops with backup capabilities.

Figures 7.4-6a sheets 1, 2, and 3 and 7.4-6b sheets 1, 2, 3, 4, and 5 show the entire Residual Heat Removal System, including the equipment used for LPCI operation. The following list of equipment itemizes essential components for which control or instrumentation is required:

Four RHRS pumps,

Pump suction valves, and

LPCI-to-recirculation loop injection valves.

The instrumentation for LPCI operation provides inputs to the control circuitry for other valves in the Residual Heat Removal System. This is necessary to ensure that the water pumped from the pressure suppression chamber by the pumps is routed directly to a reactor recirculation loop. These interlocking features and the actions of the reactor recirculation loop valves are described in this subsection, because these actions are accomplished to facilitate LPCI operation.

LPCI operation uses two identical pump loops, each loop with two pumps in parallel. The two loops are arranged to discharge water into different reactor recirculation loops. In Unit 2, this cross connection is closed off by a valve that has been electrically disabled in the closed position. The Unit 3 cross connection is isolated by an electrically disabled valve in the closed position or by a locked-closed manual shutoff valve. The Unit 1 LPCI loop cross-tie valve is removed; and the corresponding cross connection is removed by a combination of a blind flange and cut, capped connections. Figures 7.4-6a sheets 1, 2, and 3, and 7.4-6b sheets 1, 2, 3, 4, and 5 show the location of instruments, control equipment, and LPCI components relative to the primary containment. Except for the LPCI testable check

valves and the reactor recirculation loop pumps and valves, the components pertinent to LPCI operation are located outside the primary containment.

The power for the pumps is supplied from AC buses that can receive standby AC power. Each of the four pumps derives its power from a different shutdown board. Motive power for the injection valves used during LPCI operation comes from a reactor MOV board, which receives standby AC power and can be automatically connected to alternate standby power sources. Control power for the LPCI components comes from the unit batteries. Redundant trip systems are powered from different batteries. The use of common buses for some of the LPCI components is acceptable because electrical isolation devices have been installed between the buses and the components.

LPCI is arranged for automatic operation and for remote-manual operation from the control room. The equipment provided for manual operation of the system allows the operator to take action independent of the automatic controls in the event of a loss-of-coolant accident. The LPCI System is designed to meet the intent of the IEEE proposed criteria for Nuclear Power Plant Protection Systems (IEEE-279-1971).

7.4.3.5.2. LPCI Initiating Signals and Logic

The overall operating sequence for LPCI following the receipt of an initiation signal is as follows:

a. If normal AC power is available, the four pumps start one at a time, in order, at 0.2, 7, 14, and 21 seconds, taking suction from the pressure suppression chamber. The valves in the suction paths to the pressure suppression chamber are normally maintained open so that no automatic action is required to line up suction.

b. If normal AC power is not available, the four pumps start simultaneously, with no delay, as soon as the standby power source is available.

c. Valves in the containment cooling system are automatically closed so that the water pumped from the pressure suppression chamber is routed properly.

d. The Residual Heat Removal System service water pumps may be manually tripped (if running) because they are not needed for LPCI operation. If normal AC power is not available, the pumps are tripped by undervoltage. Pumps required to supply EECW are restarted automatically.

e. When nuclear system pressure has dropped to 450 psig (see Section 6.5 for analytical limit assumed in Emergency Core Cooling System analyses), the LPCI injection valves to both recirculation loops automatically open, allowing the LPCI

pumps to inject water into the pressure vessel as the reactor pressure drops below the pump shutoff head.

f. The LPCI system then delivers water to the reactor vessel via the recirculation loop to provide core cooling by flooding.

g. Recirculation pump discharge valves in both reactor loops automatically close when reactor pressure decreases to 230 psig (see Section 6.5 for analytical limit assumed in Emergency Core Cooling System analyses).

In the descriptions of LPCI controls and instrumentation that follow, Figures 7.4-6a sheets 1, 2, and 3 and 7.4-6b sheets 1, 2, 3, 4, and 5 can be used to determine the physical locations of sensors. Instrumentation and settings are given in Table 7.4-4.

Two automatic initiation functions are provided for the LPCI: reactor vessel low-water level, and primary containment (drywell) high pressure plus low reactor vessel pressure (450 psig). Reactor vessel low-water level indicates that the fuel is in danger of being overheated because of an insufficient coolant inventory. Primary containment high pressure plus low reactor vessel pressure is indicative of a break of the nuclear system process barrier inside the drywell.

Either initiation signal can start the system. Each of the initiating signals is sensed by four independent detectors arranged in a one-out-of-two-twice logic, as shown in Figures 7.4-7b, 7.4-7i, and 7.4-7p. The instruments used to detect reactor vessel low-water level, primary containment high pressure and low reactor vessel pressure are the same ones used to initiate the other ECCS. Once an initiation signal is received by the LPCI control circuitry, the signal is sealed in until manually reset. The seal-in feature is shown in Figures 7.4-7b, 7.4-7i, and 7.4-7p.

For Units 1 and 2 only, the RHR and Core Spray pumps for both units are powered from the same 4kV shutdown boards (see Chapter 8). If the ECCS loads for both Units 1 and 2 were allowed to start during combinations of real and spurious accident signals, the combined Unit 1/2 ECCS pumps would overload the 4kV shutdown boards and their associated diesel generators on a loss of offsite power, and the 4kV shutdown buses if normal power were available. Therefore, during combinations of real and spurious accident signals the Unit 1/2 ECCS preferred pump logic will assign the Unit 1 ECCS loads to the Division I 4kV shutdown boards and the Unit 2 ECCS loads to the Division II 4kV shutdown boards. The Unit 1/2 ECCS preferred pump logic will allow the Unit 1 Division I RHR and Core Spray pumps (1A and 1C) to start and load on the Division I 4kV shutdown boards, and the Unit 2 Division II pumps (2B and 2D) will load on the Division II 4kV shutdown boards. This will ensure that the shared Unit 1/2 4kV shutdown boards are not overloaded while still maintaining the minimum number of required ECCS injection subsystems described in Table 6.5-3.

The Core Spray logic initiated Common Accident Signal and the LPCI logic initiated unit priority re-trip is required to ensure that the shared Unit 1/2 4KV shutdown boards are stripped prior to starting the RHR pumps, Core Spray pumps, and other required loads when the shutdown boards are being supplied by the diesel generators. With a real and spurious accident signal present, the Unit 1 initiated Unit priority re-trip signal will only re-trip the Division I diesel breakers while the Unit 2 initiated unit priority re-trip signal will only re-trip the Division II diesel breakers. This will ensure that a spurious unit priority re-trip signal will not re-trip all four Unit 1/2 diesel breakers, which would result in interrupting both division's RHR and Core Spray pumps supplying the opposite unit in a real accident.

If an accident signal was initiated in only one unit (Units 1 or 2) and any RHR or Core Spray pumps were already running in the opposite non-accident unit (e.g. for shutdown cooling), the RHR system will initiate the preferred pump logic to trip all of the non-accident unit's running RHR and Core Spray pumps. This ensures that any running RHR or Core Spray pumps in the non-accident unit would be tripped, unloading the Unit 1/2 4kV shutdown boards prior to the accident unit starting all of its ECCS pumps (both divisions) on an accident signal, with or without a loss of offsite power.

7.4.3.5.3 LPCI Pump Mode Control

The reaction of the pumps to an initiation signal depends on the availability of power. If normal AC power is not available, the four main system pumps automatically start simultaneously after the standby power source (four diesel generators) is available, which takes about 10 seconds. (See Section 6.5 for analytical limit assumed in Emergency Core Cooling System analyses). If normal AC power is available, the four pumps start in a seven-second timed sequence (0.2, 7, 14, and 21 seconds) to prevent overloading the auxiliary power source.

The time delays are provided by timers, which are set as given in Table 7.4-4.

The timers provided in the LPCI circuitry for the main system pumps, as well as those used for the LPCI injection valves, are capable of adjustment over a range of 1.5 times the specified setting listed in Table 7.4-4.

Pressure indicators, installed in the pump discharge pipelines upstream of the pump discharge check valves, provide indication of proper pump operation following an initiation signal. Low pressure in a pump discharge pipeline indicates pump failure. The location of the pressure indicators relative to the discharge check valves prevents the operating-pump discharge pressure from concealing a pump failure.

To prevent pump damage due to overheating at no-flow, the control circuitry prevents a pump from starting unless a suction path is lined up. Limit switches on suction valves provide control room light indications that a suction lineup is in effect.

If suction valves change from their fully open position during pump operation, the limit switches trip the pump power supply breaker.

The main system pump motors are provided with overload and undervoltage protection. The overload relays are applied so as to maintain power on the motor as long as possible without harm to the motor or immediate damage to the emergency power system. Undervoltage trips are provided with time delays sufficient to permit power transfer from auxiliary transformers to startup transformer source without tripping the pump power supply breaker open.

The Standby AC Power System is designed such that automatic restart of the RHR pumps, after manual load shedding, is not available unless the original initiation signal is lost (see Subsection 8.5).

7.4.3.5.4 LPCI Valve Control

The automatic valves controlled by the LPCI control circuitry are equipped with appropriate torque and limit switches which turn off the valve-operating mechanisms whenever the valves reach the limits of travel. Seal-in and interlock features are provided to prevent improper valve positioning during automatic LPCI operation. The operating mechanisms for the valves are selected so that the LPCI operation is in time for the system to fulfill its objective of providing adequate core cooling following a design basis loss-of-coolant accident, except when the system is being tested. The time required for the valves pertinent to LPCI operation to travel from the fully closed to the fully open positions, or vice versa, is as follows:

LPCI injection valves	40 seconds
Reactor recirculation loop valves	36 seconds
Containment spray valves - drywell	30 seconds
Containment cooling valves - pressure suppression chamber	30 seconds
Residual Heat Removal System test line isolation valves	90 seconds

The pump suction valves to the pressure suppression pool are normally open. Upon receipt of an LPCI initiation signal, certain reactor shutdown cooling system valves and the RHRS test line valves automatically close. By closing these valves, the pump discharge is properly routed. Also included in this set of valves are the valves which, if not closed, would permit the pumps to take a suction from the reactor recirculation loops, a lineup that is used during normal shutdown cooling system

operation. The LPCI injection valves and RHR cross-tie valve are normally closed with the cross-tie valve being electrically disabled in the closed position for Unit 2. In Unit 3, either of the two available RHR loop cross-tie isolation valves can be placed in the closed position for loop isolation. The Unit 1 LPCI loop cross-tie valve is removed; and the corresponding cross connection is removed by a combination of a blind flange and cut, capped connections.

The LPCI is designed for automatic operation following a break in one of the reactor recirculating loops. The LPCI logic opens the injection valves to the recirculation loops and closes the recirculation pump discharge valves in the recirculation loops. No single failure or any single physical event can make all loops inoperable. See Subsections 6.4 and 4.8.

There is a requirement that reactor vessel pressure drop to a specified value before the valve logic will complete. There are four separate reactor pressure sensors for this function arranged in a one-out-of-two-twice logic. The injection valves will not open until reactor vessel pressure decreases to 450 psig (see Section 6.5 for analytical limit assumed in Emergency Core Cooling System analyses). LPCI flow then enters the vessel when the check valve opens, due to LPCI pressure being higher than reactor pressure. The recirculation discharge valves will not close until reactor vessel pressure decreases to 230 psig (see Section 6.5 for analytical limit assumed in Emergency Core Cooling System analyses).

A timer cancels the LPCI signals to the injection valves after a 5-minute delay time, which is long enough to permit satisfactory operation of the LPCI. The cancellation of the signals allows the operator to divert the water for other post-accident purposes. Cancellation of the signals does not cause the injection valves to move.

The manual controls in the control room allow the operator to open an LPCI injection valve only if nuclear system pressure is low or the other injection valve in the same pipeline is closed. These restrictions prevent overpressurization of low pressure piping. The same pressure switch used for the automatic opening of the valves is used in the manual circuit. Limit switches on both injection valves for each LPCI loop provide the valve position signals required for injection valve manual operation at high nuclear system pressures.

To protect the pumps from overheating at low flow rates, a minimum flow bypass pipeline, which routes water from the pump discharge to the pressure suppression chamber, is provided for each pair of pumps. A single motor-operated valve controls the condition of each bypass pipeline. Each minimum flow bypass valve automatically opens on sensing the low flow in the loop associated with the valve, and closes upon sufficient flow in the loop. Flow indications are derived from flow switches that sense the pressure differential across the length of each LPCI loop downstream of the cross-tie piping junction. Figures 7.4-6a sheets 1, 2, and 3 and 7.4-6b sheets 1, 2, 3, 4, and 5 show the location of the flow switches. If neither

pump in a pair is operating, but the pump suction valves are aligned for shutdown cooling, the minimum flow bypass valves are automatically closed. This is needed to avoid inadvertent blowdown of the reactor to the pressure suppression chamber during shutdown cooling.

480 Volt Reactor MOV Boards 2D and 2E which contain the power and control circuits for the RHR pump minimum flow bypass valves have not been environmentally qualified for operation following an RWCU line break outside primary containment. However, procedural controls have been established to ensure that if the RHR pumps start following an RWCU line break, operator action will prevent the pumps from continuing to run without adequate flow.

Electrical interlocks are installed between Division I RHR Shutdown Cooling Suction (SCS) Motor Operated Valves (MOVs) 2-FCV-74-2 and 2-FCV-74-13 and RHR Pressure Suppression Chamber (PSC) Isolation MOV 2-FCV-74-57. In addition, electrical interlocks are installed between Division II RHR SCS MOVs 2-FCV-74-25 and 2-FCV-74-36 and RHR PSC Isolation MOV 2-FCV-74-71. The interlocks are designed to prevent inadvertent draining of the reactor vessel by preventing the RHR SCS MOVs from opening if the RHR PSC Isolation MOV is open. The interlocks will also prevent the opening of the RHR PSC Isolation MOV if either of the RHR SCS MOVs are open.

The manual control circuitry for the recirculation loop valves is interlocked to prevent valve opening whenever an LPCI initiation signal is present.

The valves that allow the diversion of water for containment cooling are automatically closed upon receipt of an LPCI initiation signal. The manual controls for these valves are interlocked so that opening the valves by manual action is not possible unless primary containment (drywell) pressure is high, which indicates the need for containment cooling, and reactor vessel water level inside the core shroud is above the level equivalent to two-thirds the core height. Four switches are used to monitor drywell pressure for each loop set of valves. The signals are arranged in a one-out-of-two taken-twice logic so that at least two of the switches must register high to allow opening of the valves by manual action. The trip settings are selected to be as low as possible, yet provide indication of abnormally high drywell pressure. A single level switch is used to monitor water level inside the core shroud for each loop set of valves. A keylock switch in the control room allows a manual override of the two-thirds core height permissive contact for the containment cooling valves.

Sufficient temperature, flow, pressure, and valve position indications are available in the control room for the operator to accurately assess the LPCI operation. Valves (except for Units 2 and 3 RHR/LPCI System I and System II inboard isolation testable check valve, see Isolation Valves, Section 5.2.3.5) have indications of full-open and full-closed positions. Pumps have indications for pump running, pump

stopped, and pump tripped. Alarm and indication devices are shown in Figures 7.4-6a sheets 1, 2, and 3, 7.4-6b sheets 1, 2, 3, 4, and 5.

7.4.3.5.5 LPCI Environmental Considerations

The only control components pertinent to LPCI operation, located inside the primary containment, that must remain functional in the environment resulting from a loss-of-coolant accident are the cables and valve closing mechanisms for the recirculation loop isolation valves. The cables and valve operators are selected with environmental capabilities that assure valve closure under the environmental conditions resulting from a design basis loss-of-coolant accident. Gamma and neutron radiation is also considered in the selection of this equipment. Other equipment, located outside the drywell, is selected in consideration of the normal and accident environments in which it must operate.

7.4.4 Safety Evaluation

In Sections 14.0, "Plant Safety Analysis," and 6.0, "Emergency Core Cooling Systems," the individual and combined capabilities of the standby cooling systems are evaluated. The control equipment characteristics and trip settings described in this subsection were considered in the analysis of the performance of the Emergency Core Cooling Systems. For the entire range of nuclear process system break sizes, the cooling systems are effective both in preventing excessive fuel clad temperatures and in preventing more than a small fraction of the reactor core from reaching the temperature at which a gross release of fission products can occur. This conclusion is valid even with significant failures in individual cooling systems, because of the overlapping capabilities of the Emergency Core Cooling Systems. The controls and instrumentation for the Emergency Core Cooling Systems satisfy the precision and timeliness requirements of safety design bases 1 and 2.

Safety design basis 3 requires that instrumentation for the Emergency Core Cooling Systems respond to the potential inadequacy of core cooling regardless of the location of a breach in the nuclear system process barrier. The reactor vessel low-water level initiating function, which alone can actuate HPCI, LPCI, and core spray, meets this safety design basis, because a breach in the nuclear system process barrier inside or outside the primary containment is sensed by the low-water-level detectors.

Because of the isolation responses of the Primary Containment Isolation System to a breach of the nuclear system outside the containment, the use of the reactor vessel low-water-level signal as the only standby cooling system initiating function that is completely independent of breach location is satisfactory. The other major initiating function, primary containment high pressure plus low reactor vessel pressure, is provided because the Primary Containment Isolation System may not be able to isolate all nuclear system breaches inside the primary containment. The

primary containment high pressure plus low reactor vessel pressure initiating signal for the Emergency Core Cooling Systems provides a second reliable method for sensing losses of coolant that cannot necessarily be stopped by isolation valve action. This second initiating function is independent of the physical location of the breach within the drywell. Coincident failure of the Primary Containment Isolation System would be needed for nuclear system breaks outside the primary containment. Thus, safety design basis 3 is satisfied.

An evaluation of Emergency Core Cooling System controls shows that no operator action beyond the capacity of the operator is required to initiate the correct responses of the Emergency Core Cooling Systems.

The alarms and indications provided to the operator in the control room allow interpretation of any situation requiring Emergency Core Cooling System operations and verify the response of each system. Manual controls are illustrated on functional control diagrams. The control room operator can manually initiate every essential operation of the Emergency Core Cooling Systems.

Because the degree to which safety is dependent on operator judgment in time of stress, the operator's response has been appropriately limited by the design of Emergency Core Cooling System control equipment, safety design bases 4a, 4b, and 4c are satisfied.

The redundancy provided in the design of the control equipment for the Emergency Core Cooling Systems is consistent with the redundancy of the cooling systems themselves. The arrangement of the initiating signals, which come from common sensors, for the Emergency Core Cooling Systems is similar to that provided by the dual trip system arrangement of the Reactor Protection System. No failure of a single initiating sensor channel can prevent the start of the cooling systems. The number of control components provided in the design for individual cooling system components is consistent with the need for the controlled equipment. An evaluation of the control schemes for each Emergency Core Cooling System component shows that no single control failure can prevent the combined cooling systems from providing the core with adequate cooling. In performing this evaluation, the redundancy of components and cooling systems was considered. The functional control diagrams provided with the descriptions of cooling systems controls were used in assessing the functional effects of instrumentation failures. In the course of the evaluation, protection devices which can interrupt the planned operation of cooling system components were investigated for the results of their normal protective action as well as mal-operation on core cooling effectiveness. The only protection devices that can act to interrupt planned Emergency Core Cooling System operation are those that must act to prevent complete failure of the component or system. Examples of such devices are the HPCI turbine overspeed trip, HPCI steam line break isolation trip, pump trips on low suction pressure, and automatically controlled minimum flow bypass valves for pumps. In every case, the

action of a protective device cannot prevent other redundant cooling systems from providing adequate cooling to the core.

The location of controls where operation of Emergency Core Cooling Systems components can be adjusted or interrupted has been surveyed. Controls are located in areas under the surveillance of operations personnel. Control room override of local switches is provided (except when transferred to backup control). Other controls are located in the control room and are under the supervision of the control room operator.

The environmental capabilities of instrumentation for the Emergency Core Cooling Systems are discussed in the descriptions of the individual systems. Components that are located inside the primary containment, and which are essential to standby cooling system, performance are designed to operate in the environment resulting from a loss of coolant accident. See Subsection 1.5.

It is concluded from the previous paragraphs and the description of control equipment that safety design basis 5 is satisfied. The testing capabilities of the Emergency Core Cooling Systems, which are discussed in the following paragraph, satisfy design basis 6.

7.4.5 Inspection and Testing

Components required for HPCI, LPCI, and core spray are designed to allow functional testing during normal power operation. The inboard isolation check valves can only be tested during cold shutdown (MODE 4 or 5). Overall testing of these systems is described in Section 6.0, "Emergency Core Cooling Systems." During overall functional tests, the operability of the valves, pumps, turbines, and their control instrumentation can be checked. The ADS valves are subjected to tests during shutdown periods.

Logic circuitry used in the controls for the Emergency Core Cooling Systems can be individually checked by applying test or calibration signals to the sensors and observing trip system responses. Valve and pump operation from manual switches verifies the ability of breakers and valve-closing mechanisms to operate. The automatic control circuitry for the Emergency Core Cooling Systems is arranged to restore each of the cooling systems to normal operation if a loss-of-coolant accident occurs during a test operation, except for the RHR and core spray pump suction valves.

7.4.5.1 Periodic Testing Capability

Provisions are made for timely verification that each active or passive component in each of the engineered safeguard subsystems is capable of performing its intended function as an individual component and/or in conjunction with other components. In

fulfillment of this general objective, tests are provided to verify that the following specific conditions exist.

1. Each instrument channel functions independently of all others.

2. Sensing devices respond to process variables and provide channel trips at correct values.

3. Paralleled circuit elements can independently perform their intended function.

4. Series circuit elements are free from shorts that can abrogate their function.

5. Redundant instrument or logic channels are free from interconnecting shorts that could violate independence in the event of a single malfunction.

6. No element of the system is omitted from the test if it can in any way impair operability of the system. If the test is done in parts, the parts must be overlapping to a sufficient degree to assure operability of the entire system.

7. Each monitoring alarm or indication function is operable.

Test-Method guidelines include the following:

1. Provisions are made for testing without requiring shutdown or unscheduled power change as a condition of the test. Tests do not impair functional capability of the safeguards system (i.e., redundant subsystems are not both tested at the same time).

2. Testing is accomplished without disturbing the existing wiring, where possible. Pulling fuses is an acceptable practice. Second-party verification is used if wire lifting is necessary.

3. The use of clip leads is prohibited unless administrative controls are in place. Attachment of meter leads is acceptable if the temporary connections to the circuit are conspicuous.

4. Test jacks permanently wired to existing circuitry are considered acceptable, provided the connection points are so chosen that no portion of the installed protective wiring is untestable and that external equipment connected to the test jack is a conspicuous departure from normal conditions.

5. Permanently wired test lights are provided such that the installation is not capable of producing an unsafe failure through any malfunction of the lamp.

6. It is not necessary to exercise more than one accident-sensing sensor at a time to accomplish a specific test. Redundant permissive sensors, such as reactor low pressure, may also be individually exercised as required to permit complete testing of a specific part of the system. Provisions are made for frequent, periodic testing of the entire system for complete operation, unless operationally unfeasible. Provisions are made to permit total system testing when plant operating conditions permit.

7. Indications of action are positive and easily identifiable, such as:

   a. Annunciation without ambiguity,

   b. Observation of the relay actuation,

   c. Indicator lights,

   d. Pump motor shaft turning,

   e. Valve stem positions,

   f. Pressure gauges, and

   g. Flow indicators.

8. Application of test pressures to valved-out pressure sensors is an accepted method of exercising sensors. However, the installation allows such exercising without need of draining water-filled instruments and subsequent venting.

9. If any sensor is valved-out or otherwise removed from service during the test, if possible, positive indication is obtained that the sensor has been returned to service and will see changes in the process variable.

10. For Units 1 and 2, testing of Core Spray and LPCI System logic includes appropriate testing of the ECCS preferred pump logic and auto initiation inhibit to the other unit's Core Spray and LPCI. The inhibit is considered the contact in the auto initiating logic only (i.e., the permissive function of the inhibit). The test will consist of verifying continuity across the inhibit with a volt-ohmmeter.