CHAPTER 6

SPECIAL SAFETY SYSTEMS

CHAPTER OBJECTIVES:

At the end of this chapter, you will be able to describe the following features of the special safety systems:

1. The main functions and unique requirements of the special safety systems;
2. The functions, equipment and operation of shutdown systems number 1 and number 2;
3. The functions, equipment and operation of the emergency core cooling system;
4. The functions, equipment and operation of the containment system.

This chapter describes the basic design and operating practices used to ensure the safe operation of nuclear power plants, and in particular to prevent the release of unsafe amounts of radioactivity to the environment. It deals in detail with the four special safety systems that are used in CANDU generating units to ensure reactor safety.

6.1 SHUTDOWN SYSTEM REQUIREMENTS

The two reactor shutdown systems are designed in compliance with Regulatory Requirements for Shutdown Systems for CANDU Nuclear Power Plants, having the following characteristics:

- For events requiring prompt shutdown action, each shutdown system, acting alone, must ensure that
  - the reactor is rendered subcritical and maintained subcritical,
  - the reference dose limits are not exceeded, and
  - the integrity of the heat transport system is maintained (excluding any initiating LOCA). Emergency core cooling and containment functions may be credited as appropriate.
- For relevant events listed in Table 6.1 each shutdown system must ensure that fuel in the reactor, with no defects prior to the event, does not fail as a consequence of the event (excluding fuel in a ruptured channel).
- Each shutdown system is environmentally qualified to the most severe conditions under which it is required to function.
- Each shutdown system meets an unavailability target of less than 1×10^{-3}.
- The two shutdown systems incorporate the principles of redundancy, diversity, testability and separation throughout their design.
- The two shutdown systems are independent of the regulating and process systems.

For purposes of assessing the performance of shutdown system number 1, the following conservative requirements are used:

- For all relevant process failures (see Table 6.1), the shutdown system number 1, with the two most effective shutdown rods assumed unavailable, shall have sufficient speed and negative reactivity depth to reduce the reactor power to levels consistent with available fuel cooling.
- For an in-core loss-of-coolant event, the shutdown depth shall be adequate to shut down the reactor and maintain a shutdown state until operator action can be credited. In assessing shutdown depth the two most effective rods are assumed to be unavailable and any rods damaged by the event are not credited.

For purposes of assessing the performance of shutdown system number 2, the most effective poison injection nozzle is assumed unavailable. The remaining nozzles shall have sufficient speed and negative reactivity depth to reduce the reactor power to levels consistent with available fuel cooling for all process failures identified in Table 6.1

The reactor may not be operated at power, if either shutdown system number 1 or shutdown system number 2 is known to be unavailable.

Table 6.1. Coverage of Process Failures by Shutdown System Number 1 and Independently by Shutdown System Number 2.

No.	Process Failure	Trip Parameter	Alternative Trip Parameter
	Loss of Regulation from High Power:		
1.	Fast	High Rate Neutron Power	High Neutron Power/High Heat Transport Pressure
	Slow	High Neutron Power	High Heat Transport Pressure/Manual[1]
	Loss of Regulation from Decay Power Levels:		
2.	Pressurized/Pumps On		
	Fast	High Rate Neutron Power	High Heat Transport Pressure
	Slow	High Heat Transport Pressure	High Neutron Power[1] Manual[1]
3.	Pressurized/Pumps Off		
	Fast	High Rate Neutron Power	Low Gross Coolant Flow [2] [6]
	Slow	Low Gross Coolant Flow [2] [6]	High Heat Transport Pressure
4.	Reduced Pressure/Pumps Off		
	Fast	High Rate Neutron Power [2] [6]	Low Heat Transport Pressure/Low Gross Coolant Flow[2] [6]
	Slow	Low Gross Coolant Flow [2] [6]	Low Heat Transport Pressure [2] [6]/Manual[1]
5.	Reduced Pressure/Pumps On		
	Fast	High Rate Neutron Power	Low Heat Transport Pressure[2] [6]
	Slow	Low Heat Transport Pressure(2) (6)	Manual
6.	Loss of Class IV Power	Low Gross Coolant Flow[2]	High Heat Transport Pressure

Table 6.1. (Continued) Coverage of Process Failures by Shutdown System Number 1 and Independently by Shutdown System Number 2.

No.	Process Failure	Trip Parameter	Alternative Trip Parameter
	Loss of Coolant Into Containment:		
7.	Large	High Rate Neutron Power	High Neutron Power/High reactor building Pressure
8.	Intermediate	High Neutron Power	High reactor building Pressure
9.	Small		
	With Regulation	High reactor building Pressure	Low Heat Transport Pressure[2]/Low Pressurizer Level
	With Regulation - Pressurizer Isolated	High reactor building Pressure	Low Heat Transport Pressure
	Without Regulation	High reactor building Pressure	High Neutron Power
10.	Very Small		
	With Regulation	Low Heat Transport Pressure[2]	Low Pressurizer Level/ Manual
	With Regulation- Pressurizer Isolated	Low Heat Transport Pressure[2]	Manual
	Without Regulation	High Neutron Power	Manual[1]
11.	Loss-of-Coolant Into Calandria		
	With Regulation	Low Heat Transport Pressure[2] Moderator High Level	Low Pressurizer Level/ Manual[1]
	With Regulation - Pressurizer Isolated	Low Heat Transport Pressure(2) Moderator High Level	Manual[1]
	Without Regulation	High Neutron Power Moderator High Level	Manual[1]

Table 6.1. (Continued) Coverage of Process Failures by Shutdown System No. 1 and Independently by Shutdown System No. 2

No.	Process Failure	Trip Parameter	Alternative Trip Parameter
	Secondary Side Failures:		
12.	Steam Main Break with Feed Pumps On		
	Inside Containment	High reactor building Pressure	Low steam generator Level [1] /Low steam generator Feedline Pressure[5] / Low Heat Transport Pressure
	Outside Containment	Low steam generator Level	Low Heat Transport Pressure[1][4] /Low steam generator Feedline Pressure[1][4] /Manual[1]
13.	Steam Main Break with Feed Pumps Off		
	Inside Containment	High reactor building Pressure	Low steam generator Feedline Pressure[1][4] / Low steam generator Level[1]
	Outside Containment	Low steam generator Feedline Pressure[4][3]	Low steam generator Level/ High Heat Transport Pressure(1)
14.	Feedline Break Upstream of Check Valves	Low steam generator Feedline Pressure[4][1]	Low steam generator Level, High Heat Transport Pressure, Manual
	Downstream of Check Valves	High reactor building Pressure	Low steam generator Level/ Low steam generator Feedline Pressure[1][4] / High Heat Transport Pressure[3][1] /Manual[1]

Table 6.1. (Continued) Coverage of Process Failures by Shutdown System Number 1 and Independently by Shutdown System Number 2.

No.	Process Failure	Trip Parameter	Alternative Trip Parameter
15.	Loss of Feedwater Control (e.g., Closure of Feedwater Valves to a steam generator)	Low steam generator Level	High Heat Transport Pressure[3][1] /Manual[3]
16.	Feedwater Pumps Trip	Low Steam generator Level	High Heat Transport Pressure [3][1] / Low steam generator Feedline Pressure [1][4]
17.	Loss of Moderator Cooling	High Moderator Level	Manual
18.	Moderator Pipe Break	Low Moderator Level	Manual/High Neutron Power

Notes:

(1) Alternative trip parameters which provide trip coverage over a limited range of event scale (e.g , break size).

(2) The low coolant flow and low heat transport system pressure trips are conditioned out on log power < 0.3 percent.

(3) If 4 percent feedwater flow is available after trip.

(4) The low steam generator feedline pressure trip is conditioned out when log power < 10 percent.

(5) Feedline pressure may precede steam generator low level.

(6) Trip acts as high power trip in effect since power is increasing - this instigates a trip by removing the conditioned-out state.

6.2 SHUTDOWN SYSTEM NUMBER 1

The primary method of quickly terminating reactor operation when certain parameters enter an unacceptable range, is the release of the spring-assisted gravity-drop shutdown rods of shutdown system number 1. Shutdown system number 1 employs a logic system having three independent channels, designated D, E and F, which detect the requirement for reactor trip and de-energize direct current clutches to release the shutdown rods into the moderator region of the reactor core.

Reactor and Process Measurements

The design philosophy is based on triplicated measurements of each variable, with protective action initiated when any two of the three trip channels are tripped. A single loop component or power supply failure will not incapacitate or spuriously invoke the operation of the safety system.

As indicated in Table 6.2 there are nine types of measured variables which can initiate a reactor trip through shutdown system number 1. The selection of variables is such that, to the maximum extent practicable, there are redundant sensing parameters for all categories of process failures identified. The reactor trip can also be manually initiated by the operator from the main control room or from the secondary control area. The nine measured variables are described separately below:

a. Neutron Power

Inconel in-core flux detectors are provided in each of channels D, E, and F for overpower or loss-of-regulation protection. The detectors are located in the vertical in-core flux detector assemblies. The detectors are of the straight individually replaceable type and are three lattice pitches long. A linear amplifier converts each detector current to a corresponding voltage signal.

Abnormal reactor operating conditions are accounted for by lowering the trip setpoint on all detectors by a predetermined amount. This is done through a safety system console.

The type of loss-of-regulation incident that determines the locations and trip setpoints for the in-core detectors is a slow uncontrolled power increase, starting from various initial flux shapes. The flux shapes used to design the neutron overpower trip are chosen to ensure coverage of any flux shape that could arise during normal maneuvering of the reactor or from any single device failure.

Test facilities are provided to check the trip circuit by adding a test current to the normal detector current on the amplifier input, and to check the insulation resistance of each detector. The detector outputs can be displayed on cathode ray tubes in the main control room and the secondary control area for purposes of monitoring the signals, at the command of the operator.

b. Rate of Logarithmic Neutron Power

This parameter uses ion chambers, located in separate housings on one side of the calandria. The ion chambers provide a current signal which is proportional to the thermal neutron flux. The output current from each ion chamber goes to an amplifier which produces linear and logarithmic neutron power, and rate logarithmic signals; the latter is used as a direct trip parameter.

c. Heat Transport System Flow

Heat transport system flow is measured in a number of feeders. Flow readings from half of these feeders are used for shutdown system Number 1 while the other half are used for shutdown system Number 2. The logic is arranged such that each trip channel has measurements from each coolant pass. The trip is conditioned out automatically at very low power or shutdown conditions.

The flow elements are installed in a horizontal run of the inlet feeder to the specified fuel channels. Flow transmitters are mounted on the three channelized instrument racks.

d. Heat Transport System Pressure

Heat transport system pressure is measured at three widely separated locations on each reactor outlet header. The pressure transmitters are mounted on channelized instrument racks. Regular loop testing is conducted from the main control room. Both high pressure and low pressure are used as trip signals. The low pressure trip is conditioned out automatically at low power level.

These pressure transmitters also provide the signal for the heat transport liquid relief valves.

e. Reactor Building Pressure

This parameter uses a triplicated measurement of the reactor building pressure. It is effective for primary and secondary side breaks within containment.

f. Pressurizer Level

Low pressurizer level is a trip parameter effective for small loss-of-coolant accidents. Triplicated level measurements (D, E, F) are provided on the pressurizer for this trip. The trip is conditioned out automatically at very low power levels to allow for draining the pressurizer during maintenance.

g. Steam Generator Level

The steam generator low level trip provides protection against secondary side failures. Triplicated level measurements (D, E and F) are provided on each steam generator. The trip is conditioned out automatically at low power level.

h. Steam Generator Feedline Pressure

Each channel monitors the pressure in each steam generator feedline between the feedwater control valve station and the steam generator. This trip parameter protects against secondary side failures which could result in the loss of the steam generators as a heat sink. The trip is conditioned out automatically at low power level.

j. Moderator Level

Moderator level is a trip parameter effective for loss of moderator cooling, moderator pipe breaks and channel failures (i.e., in-core loss-of-coolant accidents). Triplicated level measurements (D, E, F) are provided to measure the level on the calandria for trips on both low and high level.

Table 6.2. Shutdown System Number No. 1 Trip Parameters

Item	Trip Parameter	Detector
a.	Neutron Power	Vertical In-Core Detectors
b.	Rate Log Neutron Power	Ion Chambers
c.	Heat transport system Flow	Differential Pressure Transmitters
d.	Heat transport system Pressure	Pressure Transmitters
e.	Reactor building Pressure	Differential Pressure Transmitters
f.	Reactor building Pressure	Differential Pressure Transmitters
g.	Steam generator Level	Differential Pressure Transmitters on each steam generator
h.	Steam generator Feedline Pressure	Pressure Transmitters on Individual Feedlines
i.	Moderator Level	Differential Pressure Transmitters

Logic Processing and Testing

There are three independent channels, D, E and F, having completely independent and physically separated power supplies, trip parameter sensors, instrumentation, trip computers, and annunciation. Shutdown system number 1 uses general coincidence voting logic; i.e. the shutdown rods are dropped when any two of the three channels trip, regardless of the parameters causing the channel trips. A simplified block diagram of one channel is shown in Figure 6.3.

The trip system is monitored to provide a positive indication of the state of the trip logic, by verifying the correct operation of all contacts when each channel is tested.

The shutdown units are divided into two banks: each bank is supplied with redundant (90 V(dc) to 110 V(dc)) power supplies for the clutches. Each clutch coil is held energized by the contacts of a separate relay. The high volt-ampere rating of the clutch dictates this arrangement to ensure no relay contact overrating.

For each variable monitored, a test capability is provided by which a trip condition is simulated, establishing that the channel and parameter trip logic function as designed. The testing frequency is determined based on the target unavailability for each parameter.

Shutdown Rod Withdrawal and Drop Test

Normal withdrawal is controlled by the regulating system. The shutdown rods are withdrawn as soon as the trip signal has been cleared and the trip has been reset by the operator. All shutdown rods are withdrawn simultaneously. Withdrawal of the shutdown rods is interrupted if control is switched to manual, or the flux power error is excessive, or the reactor is tripped. If the log-rate exceeds 7 percent per second, the withdrawal of the shutdown rods is also interrupted. The computer monitors the withdrawal time and, if it is greater than normal, the 'shutdown rod stuck' signal is generated.

An individual rod may be selected for manual control at any time for drop testing or drive.

Withdrawal of the rods by banks in the manual mode is possible when the automatic control is not available. The motor and drive circuits are electrically independent of the clutch circuits, ensuring effective separation of the regulating and safety functions.

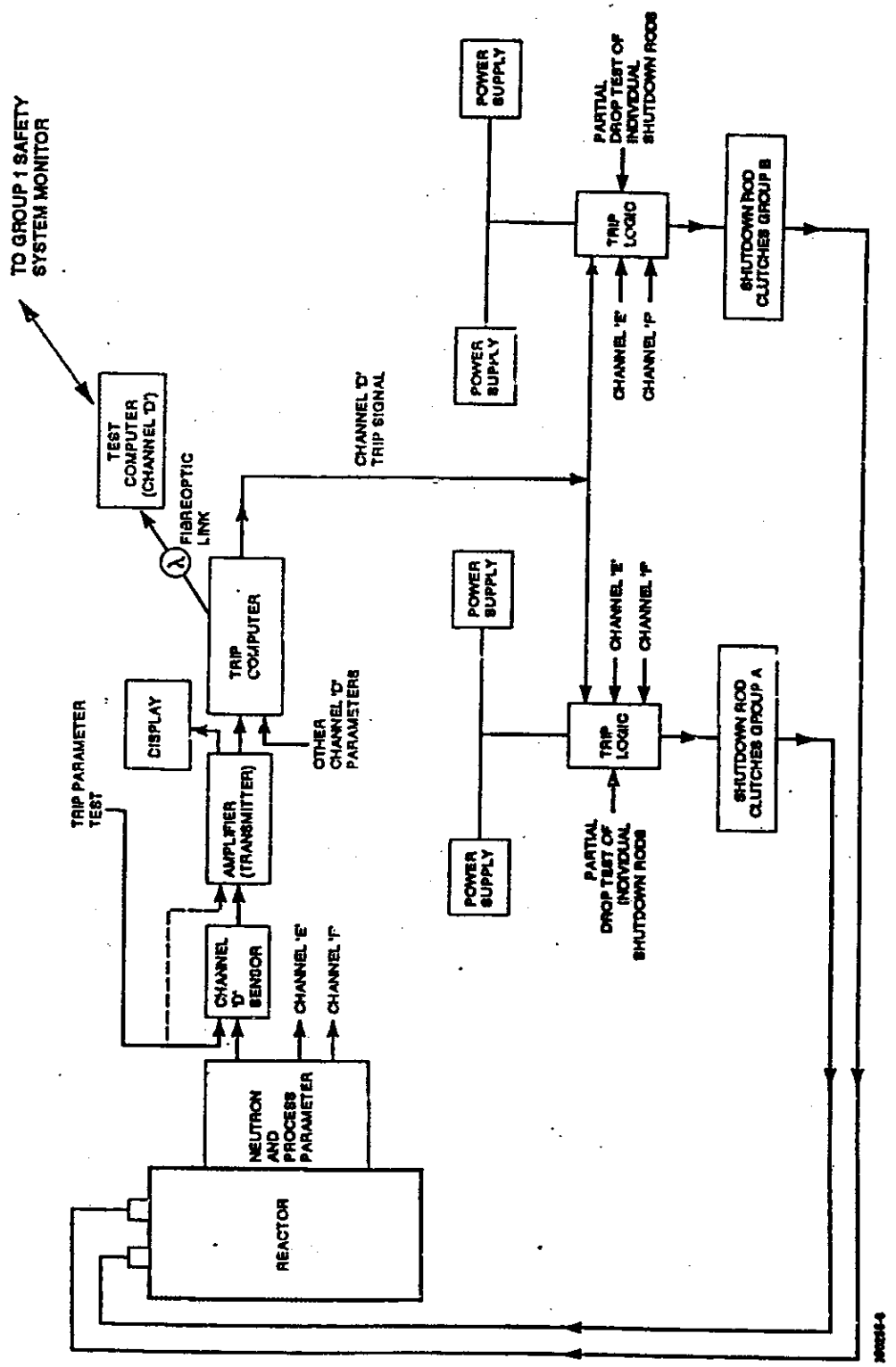

Figure 6.3. Shutdown System Number 1 - Block Diagram.

A partial drop test facility is provided in the clutch circuit to allow the operation of each shutdown rod to be checked during reactor operation. There is a time delay relay for each shutdown rod, which is set during commissioning, to de-energize the clutch relay for sufficient time to allow the shutdown rod to drop a defined distance. The position of the shutdown rod after the test is recorded to determine whether there has been any change in the shutdown unit performance.

Equipment Layout

The shutdown unit drive mechanisms are located on the reactivity mechanism deck. This permits controlled access to the clutches, motors, potentiometers, gearboxes and winches for removal or for maintenance one at a time.

There are separate cables and junction boxes for the clutch circuits and the motor drive circuits, to maintain separation between the regulating and shutdown system channels.

The trip computers and other trip logic for each channel of shutdown system number 1 are located in the main control area.

All of the reactor measuring devices on shutdown system number 1 are field-mounted in a manner which minimizes the possibility of common-mode failures with the devices used for shutdown system number 2 and for the regulating system. The connecting cables are routed to the shutdown system number 1 trip logic equipment in the main control area, in three separate channelized cable runs.

Instrumentation and Power Supplies

All the information required on the tripping parameters and the status and operation of the system is available for display on video display units in the main control room.

Separately channeled Group 1, Class II power supplies are provided for each channel of shutdown system number 1.

The direct current clutches, operated from rectified, redundant Class III power, release on loss of power.

A reactor trip occurs on a loss of power to two or more channels. Power loss to a channel results in an irrational signal to the trip computer, and a channel trip.

When a parameter reaches the trip level, the system indicates an alarm state until the operator resets. The status of all trip parameters is sent to the plant display system through a fiber-optic link for annunciation and event sequencing. During upset conditions, the time and sequence of various parameters exceeding their limits can be printed out on demand.

Trip Computers

The trip logic and trip testing for both shutdown systems make use of trip and test computers in the main and secondary control areas and video display units and console in the main control room

Figure 6.3 shows how the trip computers and test computers are used in the trip logic for shutdown system number 1. Figure 6.4 shows the configuration of fully computerized shutdown systems. Links shown in dotted lines are normally disabled; external interlocks ensure that only one trip channel can receive information at any given time.

One trip computer per channel is used in each shutdown system. The trip computers replace all analog trip comparators, all programmable digital comparators and relay logic which was used in previous plants. The final two out of three voting continues to be done using relays.

Video Display Units

The video display units provide significant improvement over panel meters for the following reasons:

- Multiple process signals for the same trip parameter (e.g., levels in various steam generators) are grouped under similar scales and headings, making it easy to find desired measurements.
- Numeric display of measurements give a high degree of reading accuracy.
- Graphical barcharts allow quick evaluation of measurements relative to setpoints and other similar signals.
- Margin-to-trip indication is provided.
- The trip condition of each signal is highlighted, supplementing the window alarms and giving more detail as to which measurement caused the trip.
- Messages are used to identify abnormal conditions such as conditioning status, irrational measurements, etc. Similar information from the annunciation system may not persist due to flooding of alarm messages during plant upsets.

The video display unit receives all necessary information from the trip computer via a unidirectional serial data link. Uni-directional data transmission is used to prevent video display unit faults from propagating back to the trip computer. The fiber-optic link ensures electrical isolation and immunity to electromagnetic interference.

The system performs, under operator control via the safety system monitor computers, the periodic testing of trip logic. It will report to the operator all relevant test results and produce a permanent printed record. Suitable interlocks ensure that only one channel in a shutdown system can be under test at one time. If abnormal conditions occur during a test, the system will automatically cancel the test.

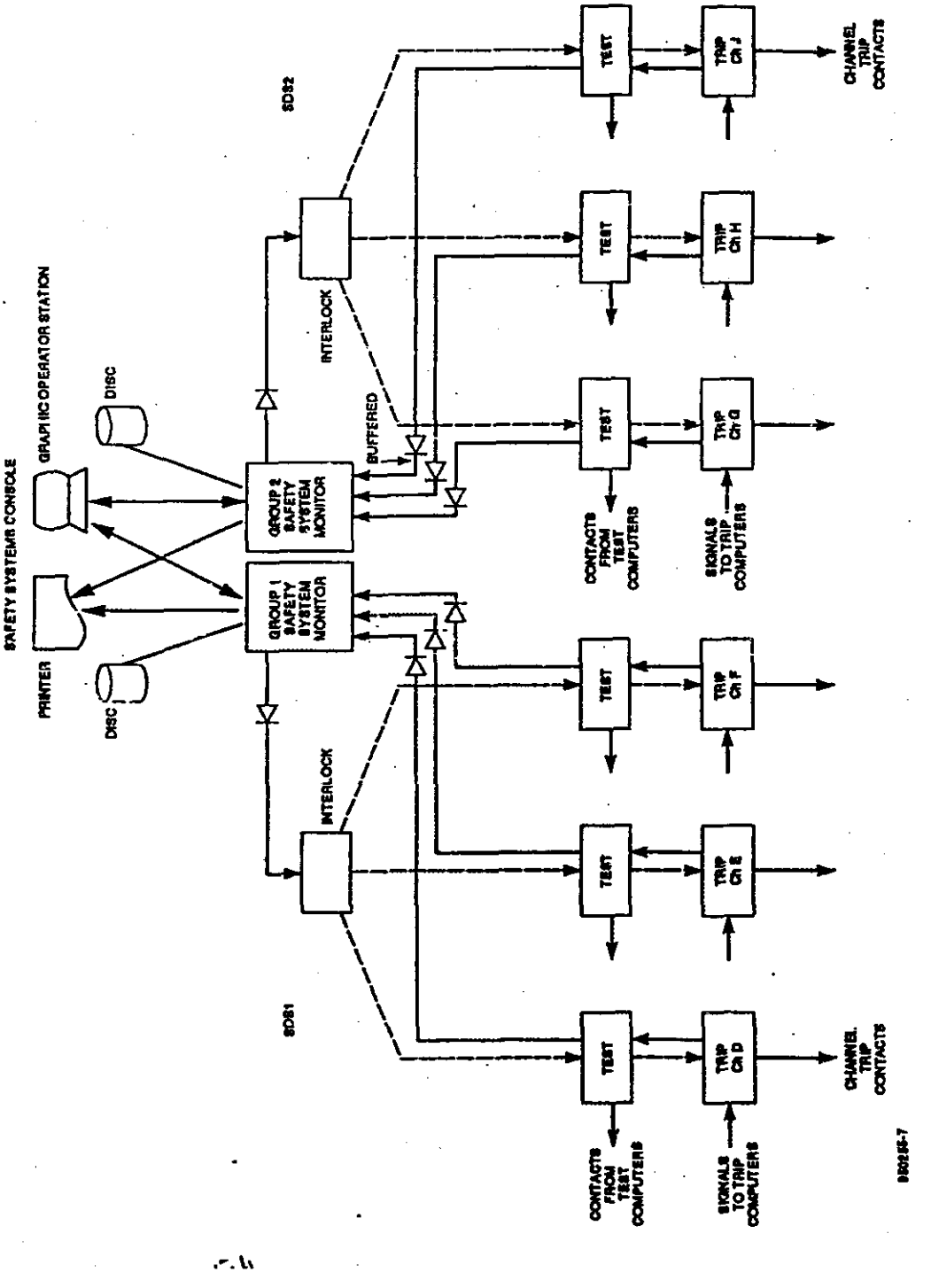

Figure 6.4. Configuration of Fully Computerized Shutdown Systems.

Design Evaluation

The required shutdown system number 1 reactivity insertion time is less than or equal to two seconds.

The variation of the dynamic reactivity worth of shutdown rods with distance inserted is shown schematically in Figure 6.5. The calculations are made with a three-dimensional two-energy group neutron kinetics code, with reactor model that includes the effect of the calandria notch region, nominal zone controller insertion and all adjuster rods fully inserted.

In general, changes in lattice properties and their influence on shutdown margin are negligible throughout the life of the plant. The most reactive condition occurs when the fuel is fresh and approximately 10 mk of positive static reactivity appears after shutdown because of the cooling of the fuel. However, depleted/natural uranium is usually used for the initial case load.

The effectiveness of shutdown system number 1 is evaluated on the basis of the two most effective shutdown rods being unavailable.

The required unavailability of shutdown system number is $1x10^{-3}$ or less on the following basis: any two of the shutdown rods fail to operate as designed and each trip parameter provides two-out-of-three trip signals. No credit is taken in the unavailability analysis for trip signals from alternative trip parameters.

Operation

The tripped condition or unavailability of shutdown system number 1 (more than two shutdown rods not fully withdrawn) inhibits moderator poison removal, and adjuster and mechanical control absorber withdrawal, and isolates the moderator system D_2O supply lines to prevent addition of pure D_2O to a poisoned moderator. The tripped condition of shutdown system number 2 inhibits withdrawal of the shutdown rods.

6.3 SHUTDOWN SYSTEM NUMBER 2

Shutdown system number 2 is the second method of quickly terminating reactor operation when certain parameters enter an unacceptable range. This is via the rapid injection of concentrated gadolinium nitrate solution into the moderator through horizontal nozzle assemblies. Shutdown system number 2 employs a logic system with three independent channels which sense the requirement for shutdown and signal the opening of fast-acting valves which release high pressure helium to inject the gadolinium poison into the moderator.

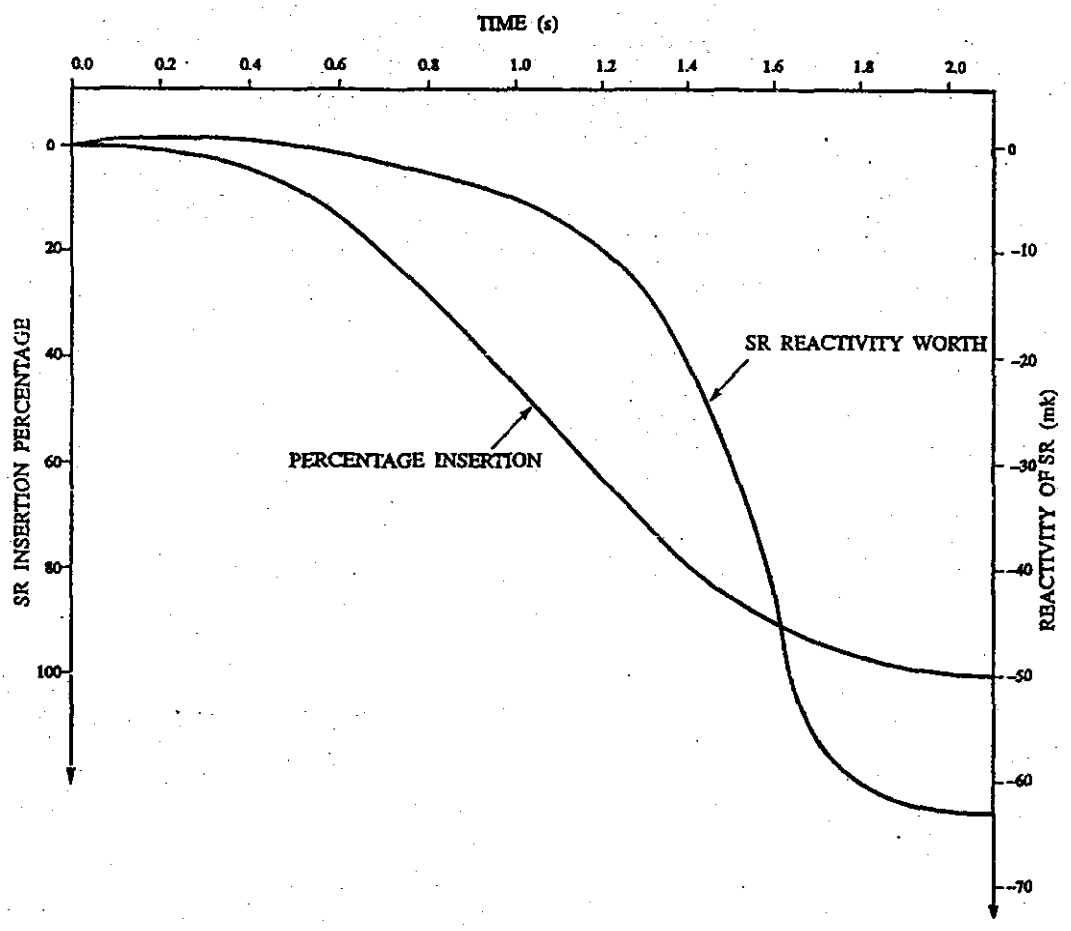

Figure 6.5. Shutdown Rod (SR) Insertion and Reactivity Worth.

Reactor and Process Measurements

The design philosophy is based on triplicating the measurement of each variable and initiating protective action when, for the same parameter, any two of the three exceed their setpoint (i.e., local coincidence logic). A single loop component or power supply failure will not incapacitate or spuriously invoke the operation of the safety system.

There are nine measured parameters which can initiate a reactor shutdown through shutdown system number 2, as shown in Table 6.3 The selection of parameters is such that, where practicable, there are redundant sensing parameters for all categories of process failures identified. Refer to Table 6.1. The system can also be manually tripped by the operator from the main control room or the secondary control area. The nine measured parameters are described separately in Table 6.3.

Table 6.3. Shutdown System Number 2 Trip Parameters and Detectors Used.

Item	Trip Parameter	Detector
a.	Neutron Power	Vertical In-Core Detectors
b.	Rate Log Neutron Power	Ion Chambers
c.	Heat transport system Flow	Differential Pressure Transmitter
d.	Heat transport system Pressure	Pressure Transmitter
e.	Reactor building Pressure	Differential Pressure Transmitter
f.	Reactor building Pressure	Differential Pressure Transmitter
g.	Steam generator Level	Differential Pressure Transmitter on each steam generator
h.	Steam generator Feedline Pressure	Pressure Transmitter on Individual Feedlines
i.	Moderator Level	Differential Pressure Transmitter

Neutron power

Horizontal in-core flux detector assemblies enter the calandria on the 'D' side of the reactor, refer to Figure 2.4. The detectors are divided between channels G, H and J, are three lattice pitches long, and are of the straight individually replaceable Inconel type. These detectors are separated from any regulating system and shutdown system number 1 detectors by virtue of the spatial separation and orientation of the assemblies.

The type of loss-of-regulation incident that determines the locations and trip setpoints for the in-core detectors is a slow uncontrolled power increase starting from various initial flux shapes.

The flux shapes used to design the neutron overpower trip are chosen to ensure coverage of any flux shape that could arise during normal maneuvering of the reactor or from any single device failure.

The output current of each detector goes to a linear amplifier. The design of these amplifiers is different from that used on shutdown system number 1.

Abnormal operating conditions. are accounted for by lowering the trip setpoint on all detectors by a predetermined ratio. This is done via channelized shutdown system number 2 console pushbuttons in which a single pushbutton reduces all detector setpoints in a specific channel.

Test facilities are provided to check the trip circuit by injection of a test current in parallel with the detector to the amplifier, and to check the insulation resistance of each detector. The detector outputs and trip setpoints can be displayed on video display units in the main control room and the secondary control room for purposes of monitoring the signals at the operator's command.

Rate of logarithmic neutron power

This parameter uses uncompensated ion chambers, located in separate housings attached to one side of the calandria. Lead shielding is provided between the inner end of the ion chambers and the outside of the calandria. The outer ends of the ion chamber tubes extend through the side wall of the reactor vault, where they are sealed by bellows.

The test shutter is the conventional piston-operated boral sleeve and has the capability of increasing the flux to the ion chambers by approximately 40 percent. The piston speed is adjustable to provide the necessary neutron rate signals. Shutter tests initiated from the main control room check a shutdown system number 1, a shutdown system number 2 and a regulating system ion chamber. Shutdown system number 1 and shutdown system number 2 ion chambers are on opposite sides of the reactor.

Heat transport system flow

Heat transport system flow is measured in a number of feeders. Flow readings from half of these feeders are used for shutdown system number 1 while the other half are used for shutdown system number 2. The logic is arranged such that each trip channel has measurements from each coolant pass. The trip is conditioned out automatically at very low power or shutdown conditions.

The flow elements are installed in a horizontal run of the inlet feeder to the specified fuel channels. Flow transmitters are mounted on the three channelized instrument racks.

Heat transport system pressure

Heat transport system pressure is measured at three widely separated locations on each reactor outlet header. The pressure-e transmitters are mounted on channelized instrument racks. Regular loop testing is conducted from the main control room. Both high pressure and low pressure are used as trip signals. The low pressure trip is conditioned out automatically at low power level.

Reactor building pressure

This parameter uses a triplicated measurement of the reactor building pressure. It is effective for primary and secondary side breaks within containment.

Reactor building pressure is normally held slightly negative with respect to atmospheric by the reactor building ventilation system. If the pressure rises above the setpoint, the reactor will be tripped.

Pressurizer level

Low pressurizer level is a trip parameter effective for small loss-of-coolant accidents. The trip is automatically conditioned out at very low power levels to allow for draining of the pressurizer during maintenance. Triplicated level-measuring loops G, H and J are provided from the pressurizer.

Steam generator level

The steam generator low level trip provides protection against secondary side failures. Triplicated level measurements (G, H and J) are provided on each of the steam generators. The trip is conditioned out automatically at low power level.

Steam generator feedline pressure

Channels G, H and J measure the pressure in the steam generator feedlines between the feedwater control valve and the steam generator. This trip parameter protects against secondary side failures which could result in the loss of the steam generators as a heat sink. The trip is conditioned out automatically at low power level.

Moderator level

The moderator level trip provides protection against pipe failure in the moderator system, loss of moderator cooling and channel failure (i.e. in-core loss-of-coolant accident). Triplicated level management (G, H, J) are provided on the calandria for both low and high level trips.

Logic Processing and Testing

There are three independent channels, G, H and J. Local coincidence is used, that is, for the same parameter, two-out-of-three exceeding their setpoint will initiate poison injection.

Figure 6.6 shows a simplified block diagram of one channel of the liquid poison injection system.

There are two alternate helium paths, each with injection valves and an interspace vent valve. Logic ensures that the interspace between the helium injection valves is depressurized to prevent spurious, partial injection, during testing.

For each variable monitored, a test capability is provided by which a trip condition is simulated establishing that the channel trip logic for that parameter functions as designed. In addition, trip parameter measurements are tested by a check for insulation resistance for the in-core flux detectors and by a monitoring and channelized cross-comparison process for process pressure measurements. Similar channelized measurements of routine pressure fluctuations are cross-compared using the monitoring computer to determine if any one of the transmitters is not responding properly to variation in the measured variables.

Testing frequencies are determined on the basis of target unavailability for each parameter.

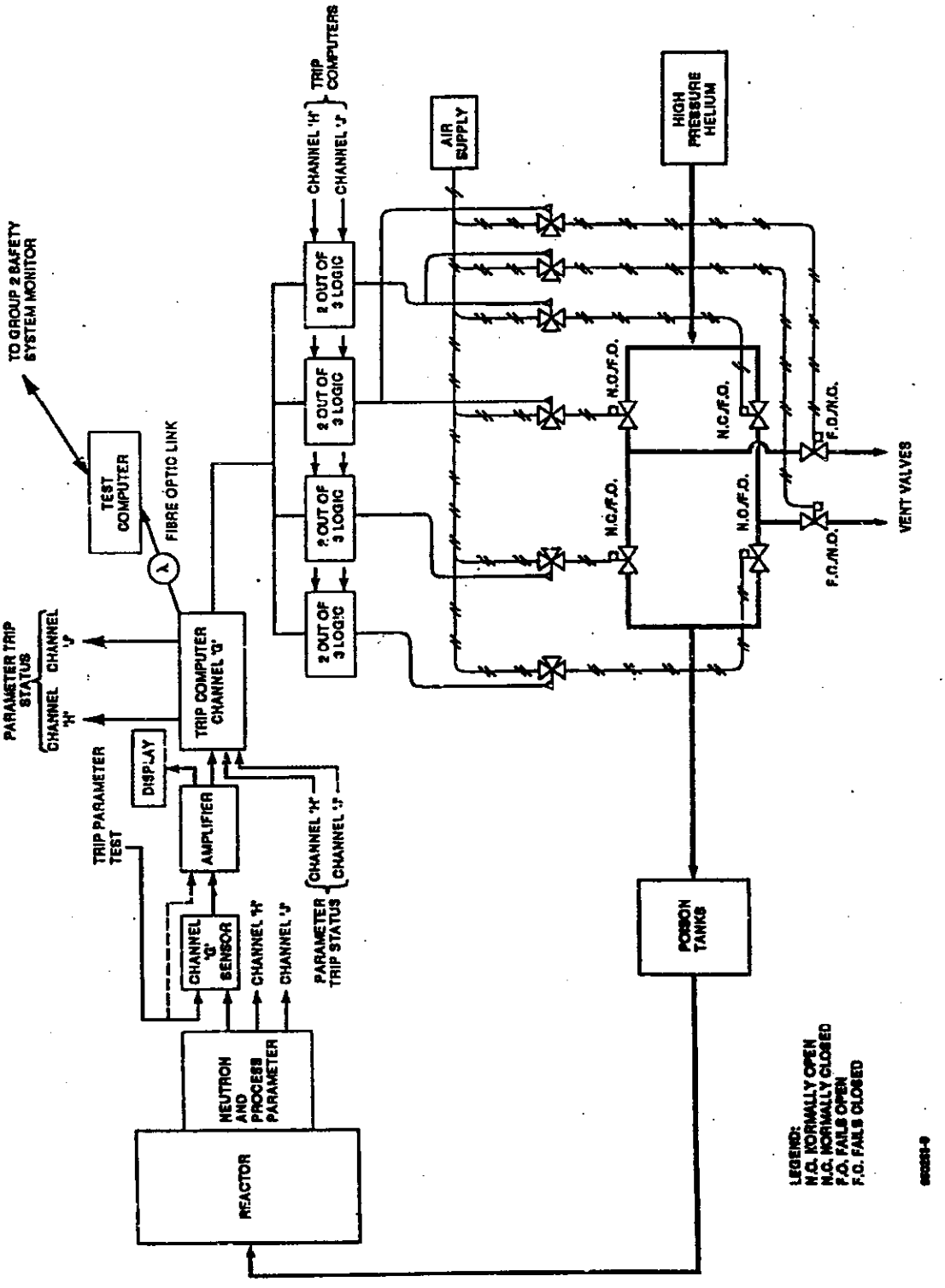

Figure 6.6. Shutdown System Number 2 - Block Diagram.

Liquid Poison Injection System

Figure 6.7 shows a simplified schematic diagram of the Liquid Poison Injection system. A vessel containing high pressure helium supplies the energy for rapid poison injection. The tank is connected, through four quick-opening valves arranged in two successive pairs, to a helium header which services the poison tanks. Thc quick-opening valves are air-to-close, spring-to-open, so that they fail safe on loss of air supply or electrical power. The cylindrical poison tanks are mounted on the outside wall of the reactor vault. Each of these poison tanks contains gadolinium nitrate solution. The nominal solution concentration is verified by an on-line recirculating sampling system.

Each poison tank is connected by a stainless steel pipe to a horizontal in-core injection tube nozzle which spans the calandria and is immersed in the moderator. The Zircaloy-2 nozzles penetrate the calandria horizontally and at right angles to the fuel channel tubes. Holes are drilled into the nozzle along its length to form four rows of jets which facilitate complete dispersion of the poison into the moderator.

There is a liquid-to-liquid interface between the poison solution and the moderator at the ball isolation valve in the piping downstream from each poison tank. Movement of the interface is caused by the poison very slowly migrating by diffusion from an area of high concentration to an area of low concentration. Also, physical motion of the liquid back and forth in the line causes a small amount of mixing of the poison solution with the moderator. This motion is caused by variations in the moderator level. The interface movement results in a periodic requirement for back flushing (moving of poison back to design position) approximately twice per year. This procedure is required infrequently because of the slow diffusion process and because the moderator level in the moderator head tank is maintained constant during warmup and upgrading by bleed and feed respectively from the D_2O supply system. Also moderator temperature is maintained constant during operation.

Two conductivity probes are installed in each poison injection line downstream of the poison tank. One is located close to the bottom of the poison tank to monitor- the poison concentration and alarm on low poison concentration. The second probe is located close to the bellows assembly of the shield tank to detect when the poison solution reaches the downstream top of the U-section. If an alarm is received from any of the latter probes, the associated poison injection line must be backflushed to pull the poison interface back to the ball valve or drain line inside the vault.

In the backflushing procedure, the affected poison tank is partially drained to the mixing tank with the ball valve in the poison injection line closed. This valve is then opened and the interface moves towards the poison tank, refilling it. Finally, the affected poison tank is drained and refilled with gadolinium nitrate solution from the mixing tank. The contents of the mixing tank must be sampled using the recirculating sampling system immediately before it is transferred to a poison tank, to verify that the poison solution has the correct concentration. A sample is also needed before adding concentrated poison solution to the mixing tank, to establish how much concentrate is needed to bring the concentration of the solution in the tank up to the required value. The sampling system can take samples from a selected poison tank while the reactor is operating without removal of the tank from service. This procedure ensures that the poison concentration in the poison tanks remains uniform and at an acceptable value.

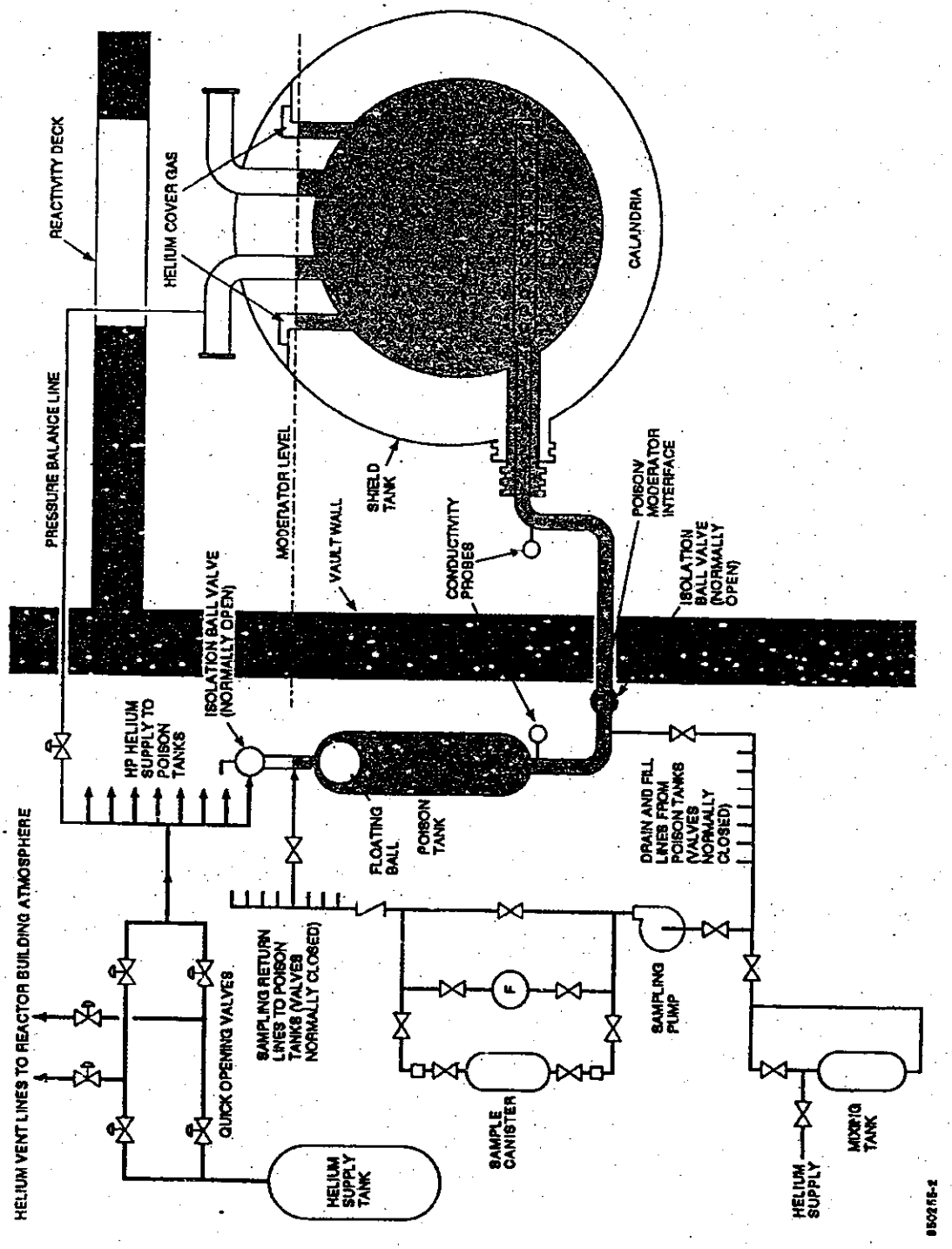

Figure 6.7. Shutdown System No. 2 Liquid Poison Injection System.

Each poison tank contains a floating polyethylene ball which seats at the top of the poison tank prior to injection to restrict the movement of poison upwards due to variations in moderator level. When an injection is initiated, the helium pressure transfers the poison to the calandria and the ball falls to the tank bottom. In the bottom position, the ball seats at the poison tank outlet and prevents the release of a high pressure helium to the calandria.

Each poison tank can be isolated by manual isolating valves located in the gas and poison legs to permit maintenance and testing on a poison tank without disabling the shutdown system. An interlock ensures that only one tank is out of service at any time. Alarms in the Main Control Room and Secondary Control Area warn the operator if valve closure occurs on more than one poison tank.

Measurements are made of helium makeup supply pressure, helium supply tank pressure, injection tank level, and injection tank ball position. Deviation from specified limits by any measurement initiates an alarm in the main control room. Limit switches are provided on each of the quick-opening valves, vent valves and helium makeup valve at the closed and opened positions. The poison solution is prepared in a mixing tank from which it is transported under moderate pressure to the poison tanks. After firing and flushing, the diluted poison solution is drained from the poison tank to the mixing tank where its concentration is restored. The mixing tank may also be used for sampling.

Equipment Layout

The quick-opening valves and poison tanks are located outside the reactor vault, where they are accessible during reactor operation. The poison tanks are situated at the vault wall to minimize injection time.

The ball valves in the poison injection line are located outside the reactor vault for ease of maintenance and operation. The drain valves adjacent to these ball valves are used during draining and refilling of the poison tanks. The poison interface is at the poison line ball valve.

The ion chambers and the in-core detectors for shutdown system number 2 are horizontally mounted and their cables are routed separately from those of shutdown system number 1. The cubicles containing the trip computers and relay logic for each channel are located in the secondary control area.

A section of the safety systems panels and console in the main control room is allocated solely to shutdown system number 2. The shutdown system number 2 annunciation is on a vertical panel, while the trip test and channel select switches, video display units and the manual trip buttons for shutdown system number 2 are mounted on the console. These are connected to the shutdown system number 2 trip and test computers in the secondary control area by channelized fiber-optic data links.

Instrumentation and Power Supplies

All the information required on the tripping parameters and the status and operation of the system can be displayed on video display units in the main control room and the secondary control area, at the operator's command.

Separately channeled Group 2, Class II power supplies are connected to each of the shutdown system number 2 channels. Fuse failure or loss of power to a channel results in a channel trip, and is annunciated. A loss of power to two or more channels results in a reactor trip.

Annunciation for shutdown system number 2 is provided in the secondary control area and in the main control room (using buffered outputs from the secondary control area).

The shutdown system number 2 control room panel contains window equivalent alarms which indicate the state of trip parameters. When a parameter reaches the trip level, these windows show an alarm state.

The parameter and channel trip status are fed to the plant display system through a fiber-optic link for annunciation and event sequencing. During upset conditions, the time and the sequence of shutdown system number 2 parameters exceeding their limits may be printed out on demand.

Helium tank pressure, valve position, poison tank level, helium makeup supply pressure and poison front position are indicated in the main control room and secondary control area. The quick-opening valve limit switches are also used to monitor the valve stroking time during channel test.

Trip and Test Computers

Shutdown system number 2 has computerization of the trip logic, system testing and monitoring and display functions, as was seen in Figure 6.6.

Design Evaluation

Shutdown system number 2 introduces negative reactivity with sufficient speed to meet all reactor shutdown design requirements. The gadolinium poison continues to disperse throughout the moderator until sufficient negative reactivity in excess of 200 mk is achieved. The initial variation of this worth is shown in Figure 6.8 Static reactivity calculations are valid on the assumption that delayed neutrons are in equilibrium with the flux.

The initial reactivities are based on calculations of the effect of short poison jets in the moderator. Power rundown measurements at operating CANDU plants confirm the calculation methods used to determine the neutronic characteristics of the system.

Concentration of the poison in the injection tanks can decrease to half its normal value and still retain over 90 percent of shutdown system number 2 effectiveness.

The effectiveness of shutdown system number 2 is evaluated on the basis of one of the poison injection tanks not functioning, (i.e. assuming the most effective unit is unavailable).

The unavailability of shutdown system number 2 is required to be 1x 10^{-3} years per year or less, assuming only one poison injection line is unavailable.

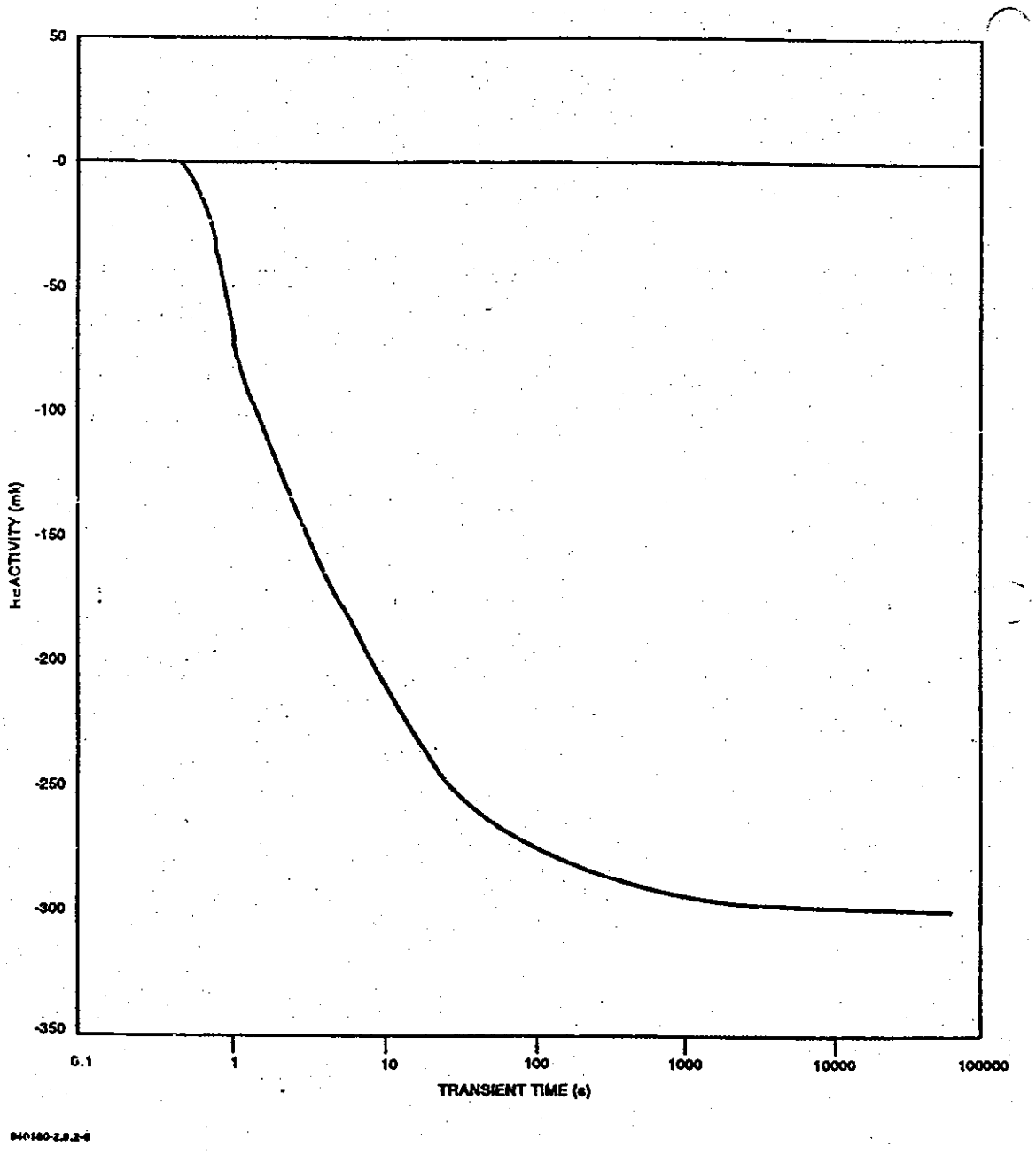

Figure 6.8. Shutdown System No. 2 Negative Reactivity Insertion Rate.

Operation

Interlocks are provided as follows for interface with other systems:

The tripped condition or unavailability of shutdown system number 2 (more than one tank out of service or helium tank pressure low) prevents moderator poison removal and also adjuster, shutdown rod and mechanical control absorber withdrawal. The D_2O supply to the moderator is also isolated.

As a normal condition, all channels (three) of each trip parameter are available and clear. Each channel is periodically tested. Unavailable channels (i.e., unsafely failed) are placed in a safe (tripped) condition immediately and kept in that state until the repair is completed.

The shutdown system number 2 test logic prevents the testing of two channels in succession within a specified time period to prevent spurious trips. The reactor may not be operated at power if shutdown system number 2 is not available.

6.4 EMERGENCY CORE COOLING SYSTEM

The emergency core cooling system is designed in compliance with the Canadian Regulatory Requirements as described in the following sections.

Cooling Requirements

The system maintains or re-establishes cooling of the fuel and fuel channels for specified loss-of-coolant accidents so as to limit the release of fission products from the fuel and maintain fuel channel integrity.

The fuel in the reactor and the fuel channels are kept in a configuration such that continued removal of decay heat produced by the fuel can be maintained by the emergency core cooling system for as long as it is required to prevent further fuel damage.

For small loss-of-coolant accident events, the emergency core cooling system prevents any failure of the fuel in the reactor due to lack of cooling. Where the initiating failure is in a fuel channel, this requirement does not apply to that channel.

After reestablishing sufficient cooling of the fuel, the system is capable of providing sufficient cooling flow for a period of four months to prevent further damage to the fuel. This is accomplished by recirculating the coolant mixture discharging from the accident location, back to the heat transport system.

Environmental Requirements

Emergency core cooling system equipment, required to operate or continue operating following exposure to severe environmental conditions following a loss-of-coolant, is environmentally qualified to withstand these conditions.

Unavailability Requirements

The system is designed to meet the unavailability on demand target of $1x10^{-3}$ for ECC initiation. Each component of the system and subsystems is monitored and/or periodically tested to demonstrate that this target is met. Valves located inside containment are accessible to permit testing and maintenance during normal reactor operation.

Long-term reliability targets are defined, and the design of the system takes into account the long term reliability of those components which must continue to function.

Redundancy is provided such that failure of any single active component in the system will not impair the system to the extent that it will not meet its minimum allowable performance requirements.

Seismic Requirements

All equipment and components in the system and subsystems needed to maintain cooling of the fuel 24 hours after a loss-of-coolant accident are designed to withstand at least an earthquake of site design earthquake intensity.

Tornado Requirements

A tornado is not postulated to cause a loss-of-coolant accident since the reactor building serves as a barrier to missiles. Also, based on probability, the coincident event of loss-of-coolant accident and tornado is considered incredible. Therefore, there is no requirement to qualify the emergency core cooling system for tornados. However, most of the emergency core cooling system is located within the reactor building, and therefore protected, while the high energy components located outside the reactor building (the gas tanks, recovery pumps, valves and piping) are tornado protected, consistent with site requirements.

Separation and Independence Requirements

The emergency core cooling system is physically and operationally independent from other special safety systems and from other Group 1 and Group 2 systems, except for those which are required to assist in the system operation.

The emergency core cooling system is designed so that pipe whip in adjacent systems will not impair operation.

System Description

The emergency core cooling system supplies coolant to the reactor headers in the event of a loss-of-coolant accident. Irrespective of the break size or location, the emergency coolant is directed to all reactor headers. Figure 6.9 shows a schematic diagram of the emergency core cooling system.

The system operation is divided into two stages; the injection stage and the recovery stage. The injection stage is provided by two high pressure gas tanks located outside the reactor building and connected via a valve station to the top of four water tanks located inside the reactor building. The water tank outlets are jointed by a distribution header from which two separate lines symmetrically feed the reactor headers (two inlets and one outlet) at each end of the reactor.

During the injection stage, flow from the reserve water tank to the emergency core cooling system sumps is initiated and the emergency core cooling pumps, located outside the reactor building are started and the recovery stage begins. When flow from the reserve water tank stops, there is about 1.5 m of water on the reactor building floor.

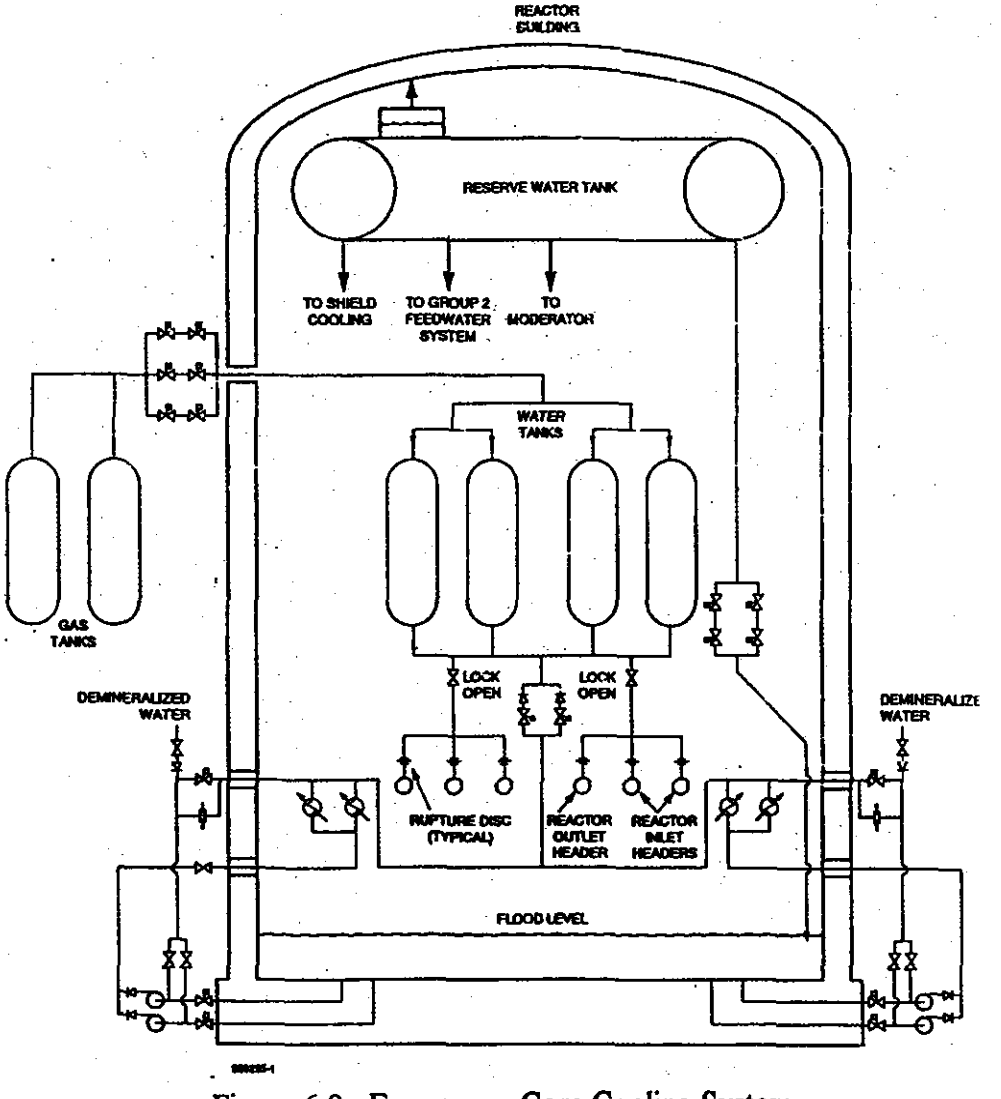

Figure 6.9. Emergency Core Cooling System.

In the recovery stage, the recovery pumps draw water from the fuelling machine vault floor, and discharge it into the reactor headers via the emergency core cooling heat exchangers. The recovery stage begins when the emergency core cooling system water tanks are depleted. The water subsequently escapes from the break in the heat transport system, falls to the floor and is recirculated by the recovery pumps. The recovery stage provides a long term heat sink. The emergency core cooling pump motors are powered by Class IV and provided with backup power from the Group 2 Class III electrical systems.

Emergency core cooling is initiated when the heat transport system pressure drops to a predetermined value and either the high reactor building pressure, or a sustained low reactor outlet header pressure conditioning signal is activated.

Instrumentation and Control

The emergency core cooling system employs dedicated computers which perform data acquisition and automatic activation functions.

Each signal loop essential for the system operation is triplicated so that a single loop component or power supply failure does not incapacitate or spuriously invoke the operation of the system. This triplication approach involves isolation between loops of the three channels and the use of unique transmitter mounting racks, electrical cubicles, initiation computers and power supplies for each channel.

The logic used with the three channels is such that any two channels alarming in the heat transport pressure monitoring loops in conjunction with any two-out-of-three of the conditioning signal loop will generate the loss-of-coolant accident signal.

The controls and power supplies to each valve of a pair of valves are separated and independent. They are referred to as the 'odd' and 'even' circuits. All electrical valves required to operate to allow light water injection are supplied from Group 2, Class III power.

System Operation

The emergency core cooling system does not operate during normal reactor operation but remains fully poised to be activated on a loss-of-coolant accident signal.

Blowdown

Following a loss-of-coolant accident, the heat transport pressure drops at a rate dependent on the size of the break. The time from the loss-of-coolant accident until the heat transport pressure reaches the injection pressure is known as the blowdown period.

For larger size breaks, the blowdown period is short and fuel cooling may or may not be adequate during this period depending on the break size and location. For small breaks, the initial emergency core cooling injection pressure is such that fuel cooling is adequate during blowdown. Therefore, the purpose of injection is to restore cooling for large breaks, and maintain cooling for small breaks.

Emergency Core Cooling Initiation

The emergency core cooling system is initiated on a loss-of-coolant accident signal. To generate this signal, the heat transport system pressure has to fall to a predetermined value and one of the conditioning variables (high reactor building pressure or sustained low reactor outlet header pressure) has to be activated. The sustained low reactor outlet header pressure signal is used as a conditioning variable for detection of a small loss-of-coolant.

The high reactor building pressure signal provides coverage for all other loss-of-coolant accidents. The conditioning signals are provided to prevent spurious operation of the system.

The system logic performs the following functions:

- opens the gas isolation valves,
- opens the main steam safety valves,
- opens the isolation valves in the line connecting the reserve water tank to the F/M vault floor,
- starts the emergency core cooling recovery pumps, with a time delay,
- opens the emergency core cooling pump suction valves and starts the Group I and Group 2 Class III diesels,
- opens the recirculation line isolation valves (when high pressure injection is complete).

The rupture discs in the emergency core cooling system burst when the gas isolation valves open after the heat transport system pressure falls sufficiently below the high pressure emergency core coolant injection pressure.

The opening of the main steam safety valves on the loss-of-coolant signal provides a rapid cooldown of the steam generators, commonly referred to as steam generator crash cooldown. This reduces the transfer of heat from the secondary side to the primary side during the initial period of emergency core cooling injection and allows the steam generators to provide a long-term heat sink for "small" breaks during steady state emergency core cooling operation. Water to the steam generators is supplied by the feedwater system and is backed up by the Group 2 feedwater system. For scenarios involving a small loss-of-coolant accident and the loss of the emergency core cooling, a steam generator crash cooldown depressurizes the heat transport system and reduces the stress on pressure tubes.

During the full sequence of emergency core cooling operation, decay heat removal is by transfer of heat to the steam generators or by discharge of fluid through the break. The latter mode predominates for the large breaks; the former mode predominates for small breaks.

Injection Stage

Upon a loss-of-coolant accident signal, water from the emergency core cooling water tanks under pressure is directed via the reactor headers to the fuel channels to refill the core. Simultaneously, demineralized water is transferred by gravity from the reserve water tank to the emergency core cooling system sump.

While injection is underway, two of the emergency core cooling recovery pumps are started. If one pump fails to start (indicated by a low pump differential pressure), a standby pump starts automatically.

Recovery Stage

Recovery stage operation follows the injection stage. The mixture of the heat transport coolant and water from the reserve water tank collected on the floor of the reactor building is then returned to the heat transport system by the emergency core cooling recovery pumps. For large breaks, decay heat is removed from the core via the coolant discharged from the break and this heat is transfer-red to the Group 1 recirculated cooling water, or the Group 2 raw service water as a backup, via the emergency core cooling heat exchanger. The containment air coolers, serviced by raw service water, also remove heat.

For small breaks, decay heat is transferred to the steam generators and rejected via the main steam safety valves. These valves have a total capacity of over 100 percent steam flow at normal steam generator pressure.

The steam generator feedwater supply after a loss of coolant is provided by the main feedwater pumps on Class IV power or by the diesel powered auxiliary feedwater pump, which draws water from the deaerator and the demineralized water storage tank. An alternative source of feedwater to the steam generators is the Group 2 feedwater system. The feedwater to the steam generators is required during the long-term emergency core cooling operation following a small break.

6.5 CONTAINMENT SYSTEM

The basic function of the containment system is to form a continuous pressure-confining envelope about the reactor core and the heat transport system in order to limit the release to the external environment of radioactive material resulting from an accident. An accident which causes a release of radioactive material to containment may or may not be accompanied by a rise in containment pressure.

To achieve this overall function, the containment system includes the following related safety functions:

- Isolation: to ensure closure of all openings in the containment when an accident occurs.
- Pressure/activity reduction: to control and assist in reducing the internal pressure and the inventory of free radioactive material released into containment by an accident.
- Hydrogen control: to limit concentrations of hydrogen/deuterium within containment after an accident to prevent potential detonation.
- Monitoring: to monitor conditions within containment and the status of containment equipment, before, during and after an accident.

In addition, the containment structure also serves the following functions:

- limits the release of radioactive materials from the reactor to the environment during normal operations,
- provides external shielding against radiation sources within containment during normal operations and after an accident,
- protects reactor systems against external events such as tornados, floods, etc.

Design Basis

The containment system is designed in compliance with Canadian Regulatory Requirements for Containment Systems. The design pressure for the containment is above the maximum building pressure resulting from any failure of the heat transport system (with or without credit for the emergency core cooling system), coupled with unavailability of the most effective active pressure reduction system. The containment is designed for an unavailability of not more than 1×10^{-3} years per year. The containment structure will not be damaged following any steam or feedwater line break.

The containment design leakage rate is 0.2 percent of the containment free volume per day at the design pressure.

Test facilities and procedures are provided to confirm that the containment system (including required safety support systems) operates satisfactorily when required and to demonstrate the reliability of the system.

The containment envelope, including the containment isolation devices, e.g., in the reactor building ventilation system, is seismically qualified for a design basis earthquake.

Control measures are included to limit hydrogen/deuterium content within any significant enclosed subvolume of containment following an accident.

System Description

The containment system includes a reinforced concrete containment structure (the reactor building) with a reinforced concrete dome and an internal steel liner, access airlocks, equipment hatch, building air coolers for pressure reduction, and a containment isolation system consisting of valves or dampers in the ventilation ducts and certain process lines penetrating the containment envelope.

Definition of Containment Envelope

a. Building Structure

All internal surfaces of the reactor building perimeter wall, dome and base slab are part of the containment boundary.

b. Piping and Ducts

All pipes or ducts which penetrate containment (except closed Class 1 or 2 systems which can be monitored for leaks) are provided with containment isolation valves or dampers. Lines which are open to the containment atmosphere during normal operation have two isolation valves in series which are automatically closed on a high containment pressure or high radioactivity signal. The containment boundary includes the pipe or duct from the containment structure inner surface up to and including the outer containment isolation valve. The main steam fines connect to the high pressure turbine via turbine stop valves, which can be used to isolate pairs of steam generators, if required, following a steam generator tube rupture. A check valve prevents blowback from a steam generator in the event of a failed feedwater line.

The irradiated fuel discharge duct and new fuel duct are part of containment during fuel transfer. When the fuelling machine is not attached, both ducts are sealed with a pair of containment isolation valves, in series.

The valves and lengths of pipe forming part of the containment boundary are designed in accordance with the design requirements for the containment boundary.

c. Airlocks and Hatch

The airlocks incorporate two sealed doors in series. The doors are interlocked so that only one can be open at any time. The containment boundary extends to the outer door of the airlocks and includes the equipment hatch.

Containment Components and Subsystems

The containment system comprises the following structures, components and subsystems:

a. A reinforced concrete containment structure, with a leaktight steel liner covering the inside of the concrete perimeter wall, dome and base slab.

b. Steel pipe and ducting form part of the containment boundary where they penetrate containment.

c. Piping and cable penetrations, which provide an engineered seal at the point where piping, ducting and electric cables penetrate containment.

d. Containment isolation - dual valves or dampers normally open on process penetrations are automatically closed on a two out of three signal indicating high containment pressure or high activity within containment.

   Measurements of reactor building pressure and radioactivity are triplicated and channelized. A two-out-of-three indication of a containment isolation requirement on either variable initiates automatic closure of normally open containment isolation valves and dampers, together with other active containment measures, e.g., energizing the hydrogen igniters. The N, Q channels of N, P, Q channelization are used on portions of

   the system which are duplicated. In these areas, either of two operating valves provides containment isolation. The isolation setpoint for radioactivity is set at a value consistent with operational limitations and background activity levels. The radioactivity monitors are located upstream of the building air exhaust isolation valves.

e. Airlock, auxiliary airlock and equipment hatch.

f. Reactor building and vault air coolers: the air coolers are used to cool the reactor building atmosphere, condense released steam, and thereby reduce containment internal pressure following a failure of the primary or secondary cooling systems.

   The air coolers also operate while the plant is operating to cool the building and maintain a suitable environment for personnel working within the reactor building.

   By promoting steam condensation, the air coolers also act to remove soluble radioactive material (except noble gases) from the containment atmosphere and to sweep hydrogen out of the reactor and fuelling machine vaults following loss-of-coolant accident.

   During normal operations, the fuelling machine vault cooling circuit is separate from the air coolers and dryers for the accessible part of the reactor building. During loss-of-coolant accident, blowout panels and dampers open to ensure that both sets of air coolers act to condense the released steam.

   The design basis for the building air coolers is established by normal operational heat loads and post-accident heat removal requirements.

In addition to handling air flow under normal operational conditions, the fan motors for building air cooler operating on Class III power are also rated to handle continuously the steam/water/air mixture and the temperature existing at the design value of pressure under accident conditions.

g. Hydrogen igniters: the hydrogen igniters, located in the feeder cabinets at the bottom of the steam generator enclosure, and in the upper part of the reactor building, ensure that hydrogen/deuterium releases are ignited at low concentrations, thus ensuring that concentrations sufficient for a detonation do not occur.