Overall Plant Control

Training Objectives

On completion of this lesson the participant will be able to describe;

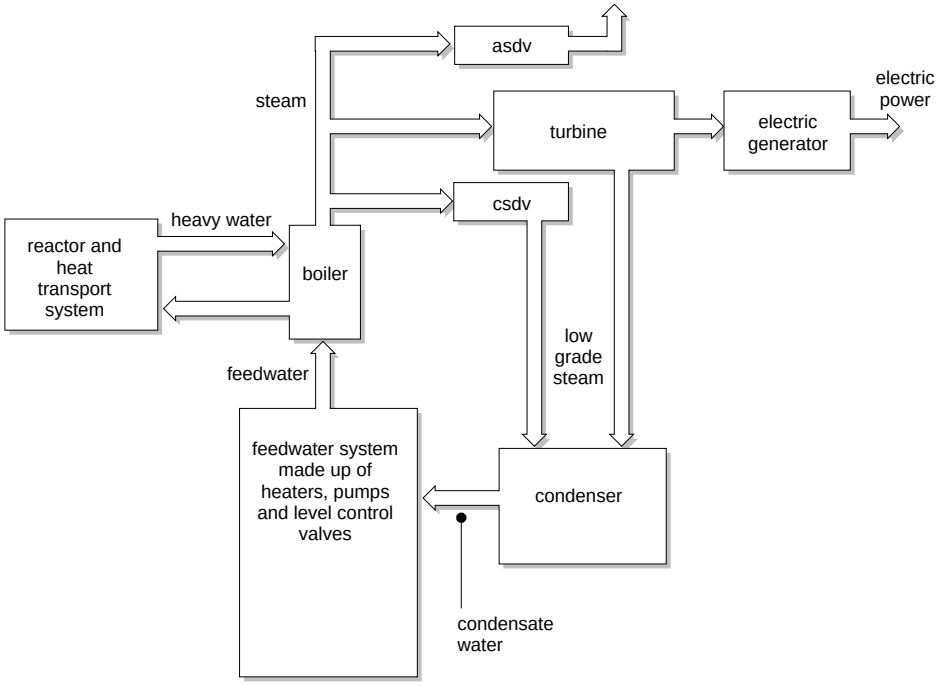
- The basic systems used in transferring the energy produced in the reactor to the electric grid.
- How these systems integrated and controlled
- How each of the component systems is controlled during normal operation and during upsets.
- The characteristics of the principal components in the energy path.

Table of Contents

1.0 Introduction

The systems and equipment that play a major role in handling the energy of the power plant are the reactor and the heat transport system; the feedwater and steam systems; and the turbine and its generator. The basic relationships are shown in Figure 1.

Figure 1
Major Plant Components



The energy is produced in the reactor, and is "consumed" by the plant loads. The plant loads are:

- The turbine generator - normally controlled by the unit power regulator program. The turbine load can also be controlled manually.
- The condenser steam discharge valves (CSDVs) - These are controlled by the boiler pressure control program, but can also be positioned by manual control. They permit continued operation of the reactor for an indefinite period in the event of a grid or a turbine generator fault. They are also used during startup and shutdown to control heating and cooling rates.
- The atmospheric steam discharge valves (ASDVs). These are normally kept closed, but are available as a controllable heat sink. They are controlled by the boiler pressure control program. They prevent opening of the boiler safety valves following a turbine trip by augmenting the capacity of the CSDVs.

The plant is operated in one of two modes;

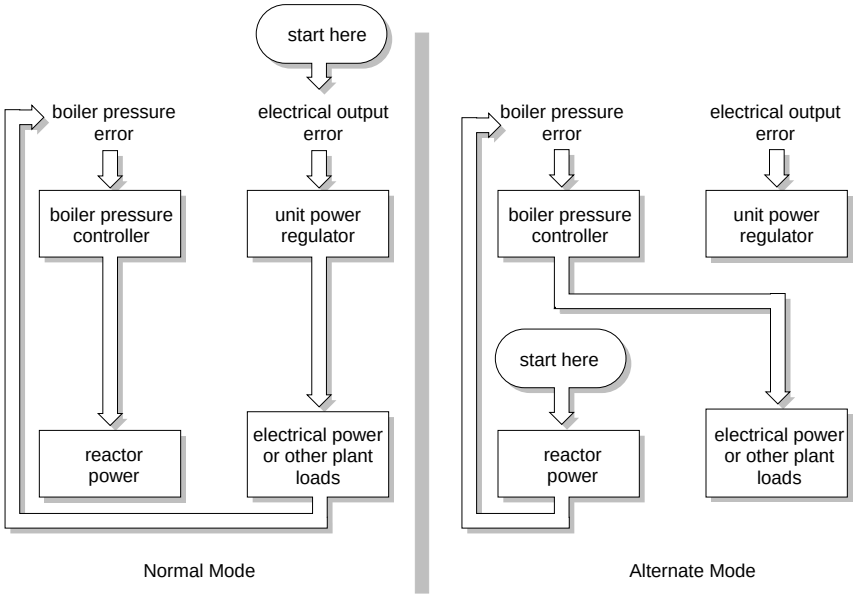
- Normal mode. In this case the steam flow to the turbine, ie the turbine loading, is adjusted to give the desired electrical output. These changes in turbine load produce changes in the steam pressure, and the boiler pressure control program initiates changes in the reactor power so that the steam pressure is maintained constant. This control mode is often termed "reactor follows turbine".
- Alternate mode. In this case the plant loads are made to follow the reactor output; the boiler pressure control program adjusts the plant loads to maintain a constant steam pressure. This mode is used at low reactor power levels, or during startup or shutdown when the steam pressure is insensitive to reactor power. It is also used in some upset conditions when it is not desirable to manoeuvre reactor power. It is known as the "turbine follows reactor" mode.

The systems that control the production and handling of the energy are;

- the reactor regulating system. This program monitors various power demands, determines the reactor neutron power setpoint, and adjusts the reactor's reactivity devices to maintain power at that setpoint.
- the boiler pressure controller (BPC). This program controls steam pressure to a constant setpoint by changing the reactor power setpoint. Under some conditions such as operation at low power or following a completed reactor regulating system set back, BPC adjusts the plant loads. By controlling changes to the boiler pressure, BPC also controls the heat transport system warm-up and cool-down.
- the unit power regulating system (UPR). This is the electrical output control program, which manoeuvres the unit power by adjusting the turbine load setpoint so that the generator output is maintained at the level demanded by the operator.
- the boiler level controller. This program controls the feedwater valves so that the water level in the boilers is maintained at a setpoint which is dependent on the reactor power level.
- the heat transport pressure controller. This program controls the pressurizer steam bleed valves and heaters to maintain the heat transport system pressure at a fixed setpoint.

Figure 2 illustrates how the control of the overall energy flow is done by each mode.

Figure 2
Normal and Alternate Modes



Figures 3 and 4 provide more detail of the overall control of the energy flow for both the normal and alternated modes.

Figure 3
Overall unit control in normal mode

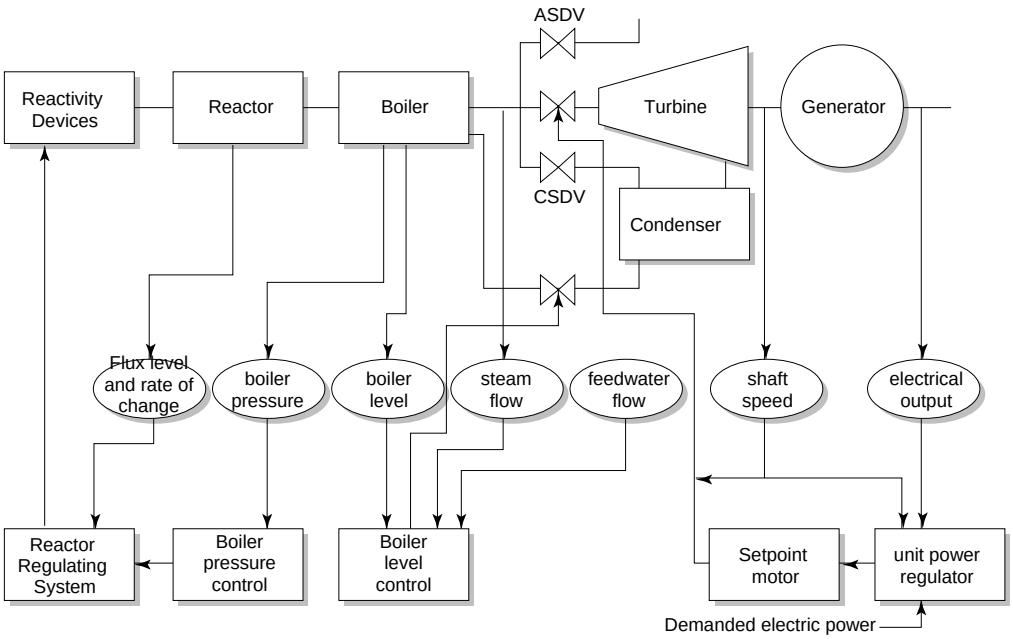
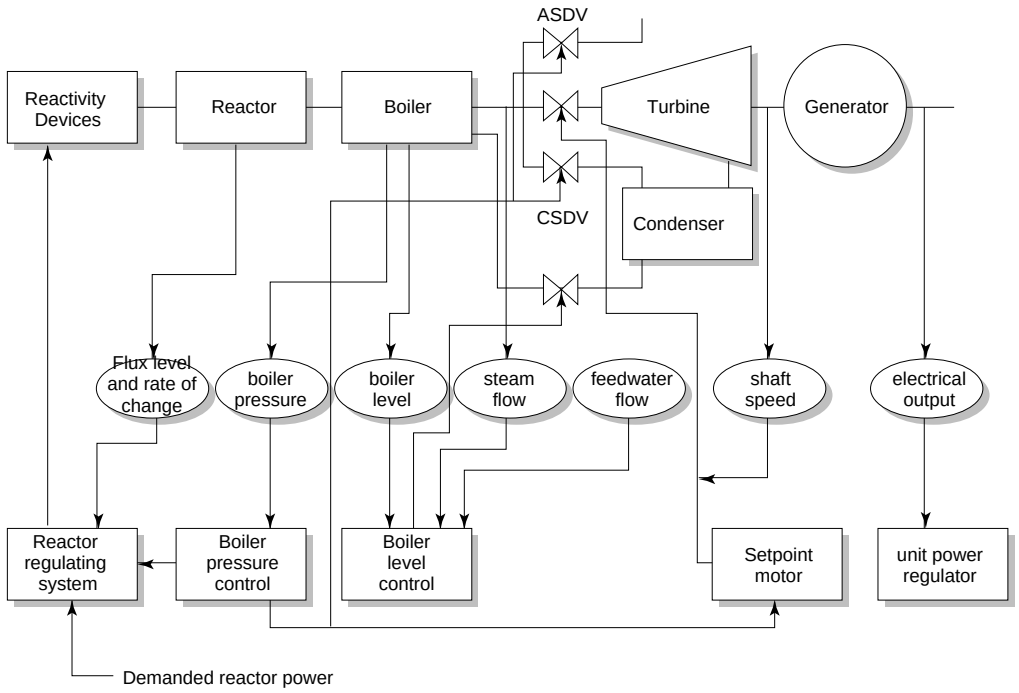


Figure 4
Overall unit control in alternate mode



The overall plant control system for a typical CANDU 6 uses digital computers to perform all major control and monitoring functions

2.0 Design Requirements

The overall plant control system:

- allows the turbine governor to respond to the load changes requested by the operator,
- changes the turbine output by governor action,
- controls the boiler pressure by varying reactor power, during normal operation,
- maintains the boiler pressure as closely as possible to its setpoint of 4.70 MPa(absolute) under all conditions other than warm-up or cool-down. Following a reactor trip, the steam pressure must not suffer a major decrease. This is necessary so that an adequate suction pressure margin for the primary heat transport system pumps is maintained,
- avoids the lifting of the boiler safety valves whenever possible,
- permits the unit to operate at reduced power indefinitely,
- permits the unit to continue supplying its auxiliaries when it is isolated from the grid,
- permits poison prevent operation of the reactor (i.e. operation of the reactor, without the turbine, at a power level sufficiently high to avert a poison out).

3.0 Plant Loads

The typical features of the plant loads for a CANDU 6 are described in this section. The plant loads are the turbine-generator, the condenser discharge valves and the atmospheric discharge valves.

3.1 Turbine Generator

The power output of the turbine is determined by the steam flowing through it. The flow is controlled by the position of the governor valves. The valve opening depends on the turbine load setpoint and turbine speed. The turbine load setpoint can be raised or lowered at several rates. The slower rates are used for normal load manoeuvres; the faster rates unload the set quickly during upset conditions such as a reactor trip.

The governor droop, i.e. frequency error, in per cent, needed to stroke governor valves fully, is typically 4%.

The turbine control can originate from the computer or from the turbine control panels.

Under automatic control, it is controlled by one of three control programs:

- **Unit Power Regulator** - controls the loading and unloading of the turbine when the plant is controlled in the normal mode.
- **Steam Pressure Controller** - controls the turbine when reactor power is not able to follow steam pressure control demands, i.e. when the plant is operating in the alternate mode.
- **Turbine Run-Up** - runs the turbine up to speed and, after synchronization, applies an initial load.

The turbine generator is capable of producing up to 680 MW(e) gross.

The load set point motor is capable of driving the turbine load setpoint at 2.2% FP /s in either direction, ie about 15 MW/s.

The recommended manoeuvring rate is calculated as a function of the turbine high pressure flange stress by a computer program. The maximum manoeuvring rate allowed, based on flange stress, is 80 MW/min.

The operation of turbine unloading and trip functions relevant to overall plant control is;

- The low steam pressure unloader operates linearly over a pressure range of 5%. The point at which it comes into operation is adjustable. Usually it begins unloading when the pressure falls to 90% of its nominal value and has unloaded the turbine fully when the pressure falls to 85%.
- The turbine is tripped on low condenser vacuum when the back pressure reaches 27 kPa(a). The operator can inhibit this trip to allow the turbine to

be run up to speed before vacuum is fully established.
- The turbine is tripped on high water level in the boilers. This is to prevent damage to the turbine from a carryover of water.
- The turbine should not be operated above about 1200 rpm when the condenser back pressure exceeds about 17 kPa(a).
- The steam flow to the turbine is decreased by the governor system if there is a major (40%) imbalance between the power delivered by the turbine and the load required. The governor valves will close and the load set point will be run back by the Electro-Hydraulic Governor (EHG) system.
- The droop (% change in frequency for a 100% change in load) is adjustable within 2-1/2 to 7%. The adjustment can be made by setting a potentiometer on a circuit board.
- The governor system has a motor driven load limiter that sets an upper limit to the turbine load. In normal operation the unit computer drives the motor to maintain the load limit at 10% above the turbine load setpoint in order to limit the size of load increases caused by governor action on under-frequency.

3.2 Condenser Steam Discharge Valves

The primary function of the condenser steam discharge valves (CSDVs) is to bypass steam to the condenser under turbine load rejection conditions. The CSDVs are normally controlled by the steam pressure control program on the basis of steam pressure error. They may be positioned manually.

CSDVs operation is constrained by low condenser vacuum, turbine exhaust spray flow, and high steam generator level to avoid damage to the condenser or turbine.

The valves have a stroking speed of about one second to avoid lifting the steam generator safety valves on a turbine trip from full power.

These valves have a capacity equivalent to about 86% of full power. They are operated, by three analog outputs, to improve their performance in spite of equipment failure. The valves are operated by a controller that receives an analog output from the computer and operates them to give a nominal opening time of 1 second with a dead time no greater than 300 milliseconds.

3.3 Atmospheric Steam Discharge Valves

The primary function of the atmospheric steam discharge valves (ASDV) is to provide a heat sink for the boiler when the condenser is not available. They are controlled by the steam pressure control program on the basis of steam pressure error with an offset. The operator can control the ASDV manually.

There are four of these valves, each of 2.5% capacity. They stroke fully within 2 seconds. Each valve is driven by a separate analog output from the computer.

4.0 Reactor Characteristics

4.1 Reactor

Reactor flux power is automatically controlled by the Reactor Regulating System over a range from 10^{-7}%FP to 1.05%FP (where FP stands for Full Power). Below 10^{-7}%FP special startup instrumentation is used for control and safety functions.

The maximum rates at which the reactor power setpoint can be manoeuvred are:

- 4% of the current power level per second when the flux power is below 25% FP.
- 1% of full power per second when the flux power is above this level.

A logarithmic manoeuvring rate is specified at low powers because the reactor is inherently a logarithmic device: a net reactivity increase of 1 mk causes power to increase at approximately 2% of its current value per second. Linear rates that would be very small at high power would be unmanageably large logarithmic rates at low power levels.

The reason for using a linear rate above 25% FP is that the plant loads are inherently linear.

The primary heat transport circuit of the CANDU 6 is designed to operate with 4% quality in the reactor outlet header at full power. Boiling commences in the channels at a power level of about 85%. If a high manoeuvring rate is used in this region for lengthy manoeuvres, the pressure, both in the channels and in the degasser condenser begins to rise rapidly. Simulation of the reactor suggests that with the reactor following the turbine, step increases in turbine load of up to 10% can be handled by the reactor manoeuvring at 1%/second at the high power levels. Step increases in turbine load greater than 10% are prevented by the computer maintaining the turbine load limit 10% above the load reference setpoint. In the alternate mode, with the turbine following the reactor, the operator selects the manoeuvring rate for the reactor. In this case it is doubtful that the reactor can manoeuvre at 1%/sec over a 10% range (at power levels above 80%) without leading to excessive pressure in the primary heat transport system. The operator will normally request much lower manoeuvring rates.

4.2 Fuel Limits

The CANDU 6 uses 37-element fuel bundles with a nominal rating of 42 W/cm, to which a 15% operating margin is allowed.

This absolute fuel rating limit is enforced during reactor operation by a flux mapping routine, which uses flux measurements from 102 in-core flux detectors to predict local peaks in regions of the core most likely to experience overpower conditions. Excessive local flux, implying high bundle powers, will cause a reactor power setback.

The fuel may also have incremental power increase limits, as well as limited rates of return to full power following lengthy operation at reduced power levels. These limits have not been fully defined and have not been taken into account in the predicted unit startup and power reduction capabilities in the following sections.

5.0 Overall Plant Computer Control

Digital computers are used for station control, annunciation and data display. This section describes the control function aspects.

Direct digital control is used for reactor power regulation, heat transport pressure and inventory control, steam pressure and boiler level control, moderator level control and fuelling machine operation.

The system consists of nearly identical independent computers known as DCCX and DCCY. Each is capable of complete station control. Experience has shown that availability of greater than 99% for each computer is readily achievable. As a result the dual computer system assures the high reliability required for station control

All functions essential to overall plant control are incorporated in both computers. They are;
- reactor power control,
- plant load control,
- boiler pressure control,
- boiler level control,
- heat transport pressure and inventory control,
- moderator temperature control,
- alarm annunciation,
- data display.

Some other functions such as fuelling machine control and turbine runup, which are not essential to overall plant control, are resident in only one computer.

6.0 Control Program Description

The main control programs are described in this section. In section 6 the behaviour of the programs during normal and alternate modes of operation is described.

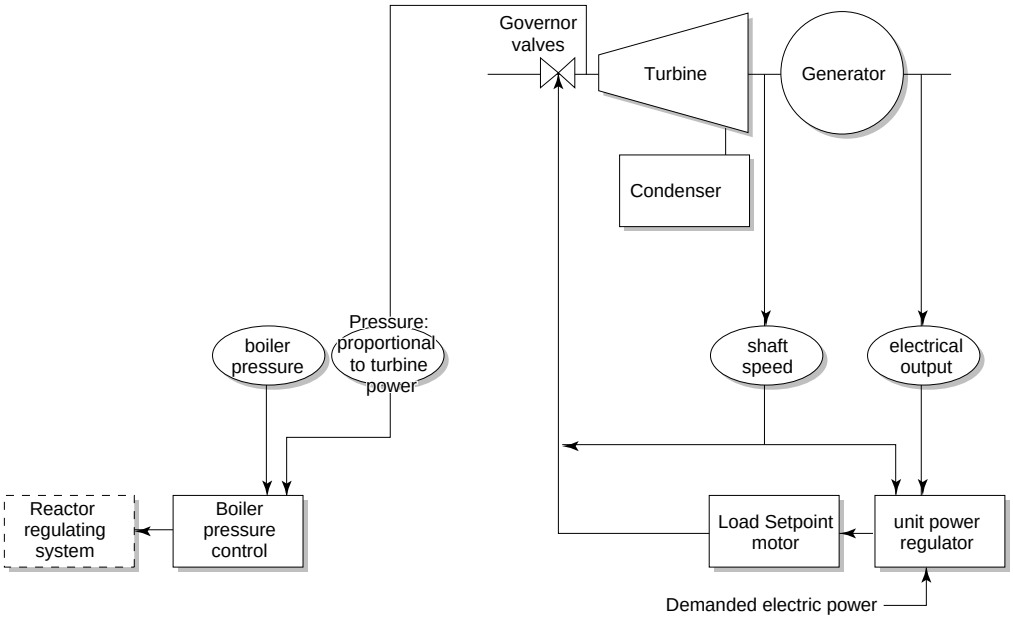
6.1 Unit Power Regulator

The principal components of the UPR control in normal mode are shown in Figure 5.

The UPR program resides in each of the two unit control computers. It has two main functions:

- to control turbine load changes. The turbine loading routine is active only while the generator is synchronized to the grid and varies turbine load at controlled rates by adjusting the load set point motor. The turbine load limiter is set at a value approximately 10% of full load above the turbine load setpoint to prevent too great a sudden load increase following a grid frequency upset.
- to monitor turbine and related plant variables.The turbine monitoring routines which are active before and after synchronization measure turbine, generator and other plant variables. In case of out-of-limit variables, the program sends a message to alert the operator and inhibits loading (or unloading) of the turbine.

Figure 5
Components of unit power regulator



6.1.1 Control of the turbine load

The operator, by means of the UPR, loads or unloads the turbine to a target power level and at a certain loading rate. When the target power level is reached the UPR maintains the generator load constant (for all disturbances except turbine speed errors). When synchronized the turbine will resist changes in grid frequency by the action of the turbine governor. That is, UPR positions the governor valves so that the generator load meets the setpoint which consists of the nominal load setpoint (MW) and a term which is proportional to turbine speed error.

Turbine load changes are made by the operator. All power manoeuvres are subject to a number of constraints which are:

- The turbine load setpoint must be under computer control.
- The plant must be in the normal mode of control, i.e. the reactor power level is changed to maintain the steam generator pressure constant.
- The turbine loading rate is limited as a function of turbine temperature.

When the plant is in the "normal" mode, the turbine load setpoint is manoeuvred towards the turbine target load at a rate that is either the maximum permissible on the basis of turbine metal temperatures or the one set by the operator. The steam pressure is controlled by manoeuvring reactor power keeping the pressure constant.

With the plant in the "alternate" mode, the turbine is used to control the steam pressure. Reactor power is kept at the specified setpoint and BPC controls the turbine load setpoint to maintain steam pressure constant. To avoid conflict between BPC and UPR, BPC is not permitted control of the turbine if the combined opening of the CSDVs and ASDV exceeds 5% equivalent full power steam flow. Alternate mode could be used to run up the turbine from low power, after a trip, when the reactor power is at a poison prevent level.

6.1.2 Monitoring of turbine parameters

The UPR monitoring routine:

- checks generator variables such as stator coolant and the hydrogen coolant system and inhibits further loading. It alarms unfavourable conditions,
- checks boiler pressure, condenser vacuum, access control violation, load limiter status and operation load hold requests,
- Turbine and generator variables which can affect loading of the turbine are monitored in the Turbine Run-Up Monitor Program . UPR monitors for unfavourable conditions, prevents further loading, and provides alarms.

In the absence of rational steam pressure signals the pressure is assumed to be 4.6 MPa(g). If the pressure is below 4.44 MPa(g) further loading is inhibited.

In the absence of rational condenser vacuum signals the vacuum is assumed to be 100 kPa(a). If pressure is greater than 13.5 kPa(a) further loading is inhibited. If vacuum deteriorates to 16.9 kPa(a) the turbine is run back at 10%/min. until vacuum improves or load reaches 30% of the rated power.

When there is a violation of access control, turbine loading is inhibited in order to force a hold on reactor power increase if plant is in the "normal" mode. The Access Control system limits the freedom of access of people into areas that have significant radiation fields while the plant is operating. By not allowing changes in the power level when people are in these areas, radiation levels should not be increased.

6.1.3 Turbine Run-up Program

The turbine run-up program (TRU) and turbine run-up monitors (TRM) are based on turbine manufacturer's specifications.

TRU runs the turbine up to synchronized speed. Subsequent loading is at a rate dependent on HP and LP turbine metal temperatures, when the plant is in “normal mode” of operation. When the plant is in "alternate" mode the turbine loading rates are limited to those provided by the BPC program.

TRM are the associated monitoring programmes of TRU and monitor the turbine-generator and subsystem conditions. These routines augment the unit annunciator system, providing additional information on abnormal conditions on the turbine and its auxiliaries. They are executed continually in DCCX only.

All routines in both TRU (including TRM) and UPR are required for run-up, UPR must be running in the same computer with TRU before run-up can proceed.

6.2 Boiler Pressure Controller (BPC)

The pressure control program has two functions:

- control steam pressure to a fixed setpoint.
- control the warm-up or cool-down rate of the heat transport system above shutdown cooling temperature by changing the steam pressure setpoint.

The boiler pressure control program is the heart of overall plant control. It controls steam pressure to its setpoint and also provides automatic warm-up or cool-down of the plant by changing the setpoint at an appropriate rate (the maximum of which corresponds to a rate of change of temperature of 2.8°C/minute) to limit thermal stresses of the heat transport system to acceptable values.

When the pressure is being controlled by changing the reactor power, when in “normal mode”, the required reactor setpoint is calculated using factors representing turbine power, warm-up rate, steam pressure and its error.

When the pressure is being controlled by changing the electrical output, when in “alternate mode”, the turbine governor valves are positioned (through the operation of the load setpoint motor) by the sum of terms representing steam pressure error, rate of change of reactor power, and rate of change of steam pressure.

In both modes the required CSDVs and ASDVs openings are calculated as the sum of factors representing the mismatch between reactor and turbine power, pressure error and a valve closing bias.

If the steam pressure exceeds the setpoint by some defined offset in this mode, the ASDVs open first and the CSDVs start to open only when the ASDVs are fully open. However, during a turbine trip or a sudden turbine load reduction exceeding 40% the CSDVs (and ASDVs if necessary) are opened on a process interrupt, and returned to their normal mode of control after four seconds.

In the other direction, very low steam pressure will cause the turbine to be unloaded until steam pressure is restored.

On BPC failure, the ASDVs and CSDVs fail closed, the contacts to the turbine fail open and control switches to ALTERNATE mode. The boiler relief valves limit the possible increase in steam pressure. Excessive drops in steam pressure are prevented by the hardware low pressure limiter within the turbine controller that runs back the turbine.

During alternate mode control, ie "turbine follows reactor", the steam pressure is controlled by adjusting the turbine governor valve setting, and if necessary the CSDVs and ASDV opening. Such a mode is necessary because at very low power, steam pressure does not react to neutron power changes and therefore, it cannot be a feedback signal. The conditions that switch the control to alternate mode are outlined in the next section, Section 6.3.

6.3 Reactor Regulating System

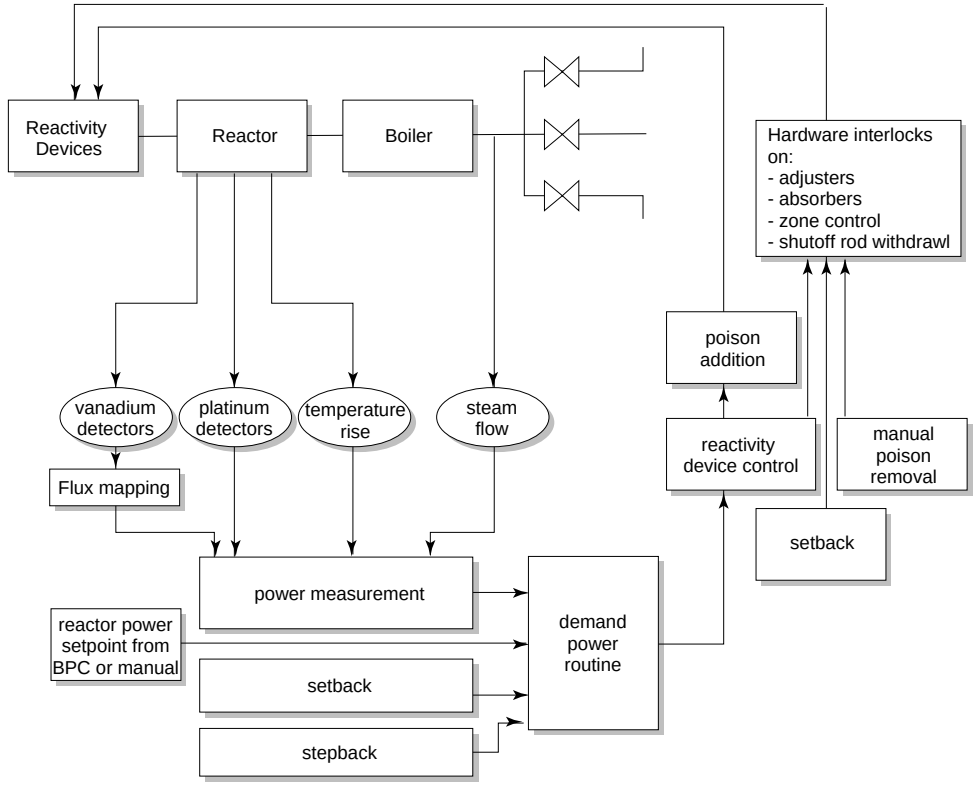
The reactor regulating system is an integrated system composed of reactor flux and thermal power measuring devices, reactivity control devices and a set of computer programs which perform three main functions:

- monitor and control total reactor power to meet the required station load,
- monitor and control reactor flux shape,
- Monitor important plant parameters and reduce reactor power at an appropriate rate when a parameter is outside of limits.

Figure 6 is a general block diagram of the regulating system.

Figure 6

Components of the reactor regulating system



The reactor regulating system controls reactor neutron power to a given setpoint by manipulating the reactivity control devices. These devices are; the light water liquid zone controllers, the adjusters and the control absorbers. The core of the reactor regulating system is the Demand Power Routine which computes the neutron power setpoint based mainly on the requirements of three sources.

- The boiler pressure control program.
- The setback routine which reduces reactor power during undesirable plant conditions.
- The reactor power setpoint commands set by the operator.

In addition, the access control program, and the safety system stepback feature limit changes in the neutron power set point.

All demanded power changes are rate limited to less than 1% of full power per second above 25% full power and 4% of present power per second at less than 25% full power. During normal operation these limits do not restrict power manoeuvring.

At all times, demanded power is limited by a deviation limiter which prevents the reactor setpoint from exceeding reactor power by more that 5% of present power. On a reactor trip, control of the reactor power setpoint is immediately

transferred to the `alternate' mode. Since actual reactor power is dropping sharply, the reactor power setpoint is reduced by the action of the deviation limiter. When the reactor trip is cleared, the setpoint is within 5% of actual reactor power, and control is in the `alternate' mode. Similar action by the deviation limiter drops the reactor power setpoint on a stepback.

7.0 Operation of the Control Systems.

The operation of the principal control systems during normal and upset conditions is outlined in this section.

7.1 Normal Situations

This section describes plant and control systems during normal operating conditions.

7.1.1 Full Power Operation

During power operation, the generator load is adjusted by positioning the turbine governor valves. Reactor power is raised or lowered to maintain steam pressure at its setpoint, and therefore follows generator load changes.

The unit power regulator changes the generator load in response to requests from the operator and maintains the load at the desired MWs except in the case of grid frequency upsets. In that case, the action of the turbine speed governor prevails. The nuclear steam supply system will follow such governor-initiated load changes through the action of the steam pressure controller.

Reactor power is controlled to a setpoint specified by the Demand Power Routine (DPR), which, in the normal mode, responds to the demands of the steam pressure controller. When a setback is necessary, DPR receives a negative rate and an end point from the set back routine.

7.1.2 Warm-up and Cool-Down

While the plant is shutdown the heat transport system temperature is controlled below 177° C by the shutdown cooling system. Above that temperature the heat transport system temperature is controlled by the steam pressure. Warm-up and cool-down rates of the heat transport system result from the change in the steam pressure setpoint by the boiler pressure control program. The operator selects the rate of change, normally 2.8°C/min.

Usually during warm-up, reactor power is adjusted up or down on the basis of steam pressure error. This is similar to what happens at power but with a lower gain because of the low reactor power level.

Alternatively the operator can select a steady reactor power (approximately 5% FP) which will give the rate of warm-up desired. This is the alternate mode of plant control.

Cool-down proceeds in much the same way, except that reactor power is not involved. The reactor is usually shut down when cool-down is initiated. Cool-down makes use of the CSDVs if the main condenser is available; otherwise cool-down is accomplished using the ASDVs.

On decreasing reactor power, the transfer from the normal to the alternate mode takes place automatically when power drops below 2%.

The power level at which the "low power" changes to "high power" depends on the mode selected. Unless warm-up is in progress, the plant is in the alternate mode at powers below 2%. If warm-up is in progress, the operator can change to the normal mode.

Typically it would proceed as follows: the heat transport system is hot, reactor power is approximately 5%; steam pressure control is via the CSDVs. As the turbine run-up program brings the turbine generator up to speed, the operator raises reactor power to a level capable of supplying the block load to be applied immediately upon synchronization. After block loading, the operator changes the reactor power setpoint mode to normal, and loads the turbine to the desired power level via unit power regulator.

7.1.3 Low power operation

At very low power levels when the flux is in the low log power range, the reactor power cannot be controlled by the steam pressure signals. At these low levels large changes in reactor power do not represent large thermal changes so have no effect on steam pressure. Under these conditions the reactor power is controlled to an operator specified flux setpoint. This set point can be manoeuvred up or down at different rates. Steam pressure at low powers is controlled by varying the plant loads ie by operating in "alternate" mode.

7.1.4 Alternate Operating Mode

"Alternate" mode is the low power and plant upset mode, in which the demand power routine is sensitive only to demand power changes from the keyboard. This mode is entered automatically when;

- a reactor trip or stepback has occurred,
- a setback has occurred,
- the reactor is at a very low power,
- the turbine has tripped or the generator has lost connection to the grid,
- the steam pressure controller is unavailable.

This mode may be entered at any time by an operator command through the keyboard. Entering the alternate mode is equivalent to a "hold power" command.

7.1.5 Manual Control of Reactor Power Setpoint

The operator always has the option of taking control of the neutron power setpoint. He may simply hold power, the automatic result of placing setpoint control in the alternate mode, or he may raise or lower the flux setpoint to a desired value at a desired rate using suitable keyboard commands.

Steam pressure control in this situation is by varying the plant loads, as it is during a setback, after a stepback, and at very low power levels.

If the operator raises reactor power beyond the capability of plant loads at that time, a reactor power setback on high steam pressure restores the power balance.

7.1.6 Manual Control of Turbine Load

When the turbine load is under manual control, the command outputs from the computer are disabled except for its ability to reduce turbine load. Steam pressure control in its "normal" mode is unaffected; reactor power is made to follow changes in turbine power up or down. The only difference is that the operator, instead of the unit power regulator, is controlling the turbine.

If the operator raises turbine power beyond the capability of the nuclear steam supply to follow, the turbine low steam pressure unloader will remove the power mismatch. If there is a reactor power setback or stepback, the steam pressure controller will override the manual commands and lower turbine power as necessary to maintain steam pressure.

Conversely, if the operator lowers turbine power too quickly or too far for the nuclear steam supply to follow, steam pressure controller will open the CSDVs to discharge the excess steam.

7.2 Operation During Upsets.

This section summarizes plant and control system behaviour during upset conditions.

7.2.1 Reactor Trip

The shutdown systems SDS1 and SDS2 trip the reactor: SDS1 dropping the shutoff rods into the reactor and SDS2 injecting liquid poison. In addition, the trip causes the control programs to make;

- the control absorbers fall into the core,
- the light water zone controllers fill,
- the control mode change to alternate,
- adjuster rod drive inhibited, both in and out.

A fast latched run back of the turbine occurs to zero load.

The generator remains connected to the grid system on a reactor trip.

The heat transport system pressure drops sharply as the voids collapse and the

water shrinks. The pressurizer maintains the adequate suction pressure for the heat transport pumps.

7.2.2 Reactor Power Stepback

A stepback is similar to a reactor trip. It is terminated at a power level which depends on the cause and in most cases this is 0% FP. Neither the SDS1 nor SDS2 operate; the power is reduced by dropping the control absorbers into the core.

On a stepback, the control mode is changed to the "alternate" mode. The turbine is unloaded through the action of the steam pressure control program.

7.2.3 Reactor Power Setback

Reactor power setbacks are applied directly to the neutron power setpoint and therefore override other demands for reactor power changes.

"Normal" mode of control is interrupted during a setback; the mode is changed to "alternate". If the setback condition clears before the endpoint of the setback is reached, the control returns to the "normal" mode. If the setback goes to its endpoint, the mode remains "alternate".

7.2.4 Turbine Trip or Loss of Line

On a turbine trip or loss of line, the CSDVs are immediately opened and the plant control mode is switched to “alternate”. The valve opening depends on the power level at the time. From power levels greater the 70% the valves will open fully for 4 seconds; from power levels between 30 and 70%, the valves will open to a proportional value; and below 30% the valves are not required to open. Subsequently, the CSDVs control steam pressure is based on the usual algorithm. If the station becomes disconnected from the grid system, the overall plant control system will maintain power to its own plant loads and prevent a reactor poison-out.

The condenser short-term steam dump capacity is great enough to avoid lifting the main steam safety valves. The long-term dump capacity may be somewhat lower, but is sufficient for continued reactor operation at a poison-prevent level (typically 60% full power) until the turbine operation can be restored, or the plant is shut down.

7.2.5 Poison-Prevent Operation

One of the by-products of fission is xenon. This fission product is a very strong absorber of neutrons and imposes a large reactivity load on the reactor. A reduction in power level is accompanied by a increase in the amount of xenon present since it is no longer being removed - "burned off" - by capturing neutrons. If the power remains at the new lower level too long, the xenon increases to a level where it is not possible to continue operating the reactor. So

many neutrons are absorbed in the xenon that there are not enough left to maintain the fissioning. This situation is known as "poisoning out". The xenon decays like most fission products and after about a day the level is low enough that the reactor can be restarted.

Following operation at full power the reactor can be reduced to about 60% without poisoning out.

If the turbine generator or connection to the power grid is unavailable, the reactor can be prevented from poisoning out by discharging steam directly to the main condenser.

During poison-prevent operation, the operator adjusts the reactor power setpoint to the desired poison-prevent level. In this manual reactor power setpoint mode, the CSDVs are used to control the steam pressure. When the turbine becomes available the operator returns to normal mode control and loads the turbine either manually or by use of the UPR. As the turbine power increases, the steam pressure controller will reduce the CSDVs load by an equal amount.

There is no feedwater heating from turbine extraction steam during poison-prevent operation. Sufficient live steam is fed to the deaerator to maintain the temperature of the feedwater entering the preheaters high enough to limit stresses in the steam generators.

7.2.6 Loss of Class IV Power

A total loss of Class IV power with the unit at full load has the following effects:

- The main heat transport pumps become unavailable. Circulation through the core and the steam generators is by thermosyphoning after the pumps run-down.

  When the pump breakers open, a stepback to low power is initiated. A reactor trip will also occur, possibly on high heat transport pressure, but certainly on low heat transport coolant flow. The low flow trip will occur approximately four seconds after the loss of Class IV power.

- The main feedwater pumps become unavailable. Feedwater flow to the steam generators stops until the Class III auxiliary feed pump becomes available.

  The interruption in feedwater is not expected to be a problem, because the integrated steam generator power for this period is only 0.5 full power minutes, whereas the steam generators normally contain in excess of 1.5 full power minutes of water. When the Class III auxiliary feed pump becomes available and feedwater flow is established, steam generator power has

dropped to below auxiliary feed pump capacity, and recovery of steam generator level to its controlled value begins immediately.

- The cooling water pumps for the main condenser become unavailable. The turbine is unloaded and the CSDVs are unloaded or inhibited from opening as condenser vacuum deteriorates. Steam pressure will rise because of the power mismatch, and the main steam safety valves lift. To prevent repeated brief lifting of the safety valves to dissipate reactor decay power, the ASDVs are brought into operation.

7.2.7 Low Condenser Vacuum

The condenser is the ultimate heat sink for both the normal (turbine generator) and back-up (CSDVs) plant loads. On low condenser vacuum, both the turbine and CSDVs are unloaded, forcing a reactor power reduction and perhaps a shutdown. Maintaining condenser vacuum by keeping steam to the turbine gland seals and operation of the air extraction pumps is very important. Re-establishing vacuum is time consuming, during which, reactor may poison out.

Condenser vacuum degradation is generally slow, and the reactor power will normally follow the turbine power down by the action of the steam pressure controller. If reactor power reductions are inhibited or because the reactor power is being controlled to a fixed setpoint, steam pressure will rise, initiating a reactor power setback on high steam pressure. No direct setback on low condenser vacuum is necessary.

In the event of a sudden loss of condenser vacuum, which unloads the turbine faster than reactor power can be reduced by a setback, a load mismatch builds up between the turbine and reactor power, causing steam pressure to rise until the safety valves lift. A setback on high steam pressure reduces reactor power until it is within the capacity of the ASDVs. The reactor power is reduced at 0.5% per second to about 8% full power. However, during this period the heat transport system pressure may increase to the point that its liquid relief valves open, discharging water to the pressurizer. The setback on high heat transport pressure would occur in this case.

7.2.8 Grid Frequency Upset

- **High Frequency**
  This brings about a partial loss-of-load and leads to system behaviour similar to, but less severe than, a loss of line. The turbine speed governor closes the turbine governor valves, and the steam pressure control program opens CSDVs to bypass excess steam to the condenser. The reduced steam flow to the turbine and high steam pressure will reduce the reactor power setpoint to match and reduce load.
- **Low Frequency**
  In this case the turbine speed governor opens the governor valves, admitting more steam to the turbine and causing steam pressure to drop. The steam pressure control program responds by increasing reactor power to match the

new turbine load. The plant is designed to accommodate sudden turbine load increases of 5% full power.

A number of limits and checks keep the transient within acceptable bounds:

- The turbine load limiter is set to limit the maximum sudden turbine load increase.
- Reactor power setpoint is limited to enforce fuel limits. If the reactor is unable to match the increased turbine load, steam pressure drops until the turbine is automatically unloaded to the reactor power level.
- The rate of reactor power increases are limited to those which the heat transport system can handle.
- Setbacks or stepbacks to prevent fuel overrating.
- The boiler pressure control program reduces the turbine load to match the reactor power if the turbine load demand continues to be greater than the reactor capability.

7.2.9 High Boiler Level

On high boiler level, the turbine is tripped to avoid turbine damage from water being carried over with the steam. The CSDVs also will be tripped on high steam generator level, but at a higher setpoint than for the turbine.

On a turbine trip from a power greater than 65%, a setback to 60% is initiated.

If the turbine and CSDVs are tripped, the main steam safety valves will lift, and the reactor is set back because of high steam pressure to about 8%, which is within the capacity of the ASDV's.

7.2.10 Low Boiler Level

Low boiler level indicates a loss of feed water supply. The reactor must be shutdown while there is sufficient inventory in the boilers to allow the operator time to provide an alternate heat sink. This is accomplished by having a setback on low boiler level and is backed up by a reactor trip on a very low boiler level.

7.2.11 Heat Transport Pump Trip

The loss of one heat transport coolant pump in a loop will cause a reactor power stepback to approximately half load. It could also result in a reactor trip on a transient high heat transport pressure or low flow, depending on the number and disposition of pumps tripped, the reactor power level and the state of the fuel core (fresh or equilibrium). The plant can be operated at powers up to the poison-prevent level with only one pump in each of the two loops operating, ie two of the four pumps.

If both pumps in either loop are not running, a full stepback is initiated, and a reactor trip on low gross flow will occur.

8.0 Effects Of Xenon

The buildup of xenon in the fuel following power reductions or trips affects reactor performance as discussed below.

8.1 Unit Startup Following a Reactor Trip

Figure 7 shows a typical power recovery after a reactor trip. The slow rate of rise from approximately 60% to 100% of full load is governed by fuel rating limits.

During startup most of the adjusters are removed from the core to overcome the negative reactivity load of the accumulated xenon poison. Consequently, flux shape distortions occur, and maximum reactor power is reduced to keep bundles within their power limits. As the excess xenon poison is burned out, adjusters are re-inserted, the flux shape reverts to normal, and reactor power is allowed to increase to 100%.

In the worst case, when a poison-out is barely averted and all adjusters are withdrawn for the restart, the return to full power may take up to 4 hours. If the trip is cleared quickly, fewer adjusters are withdrawn and the return to full power is somewhat faster.

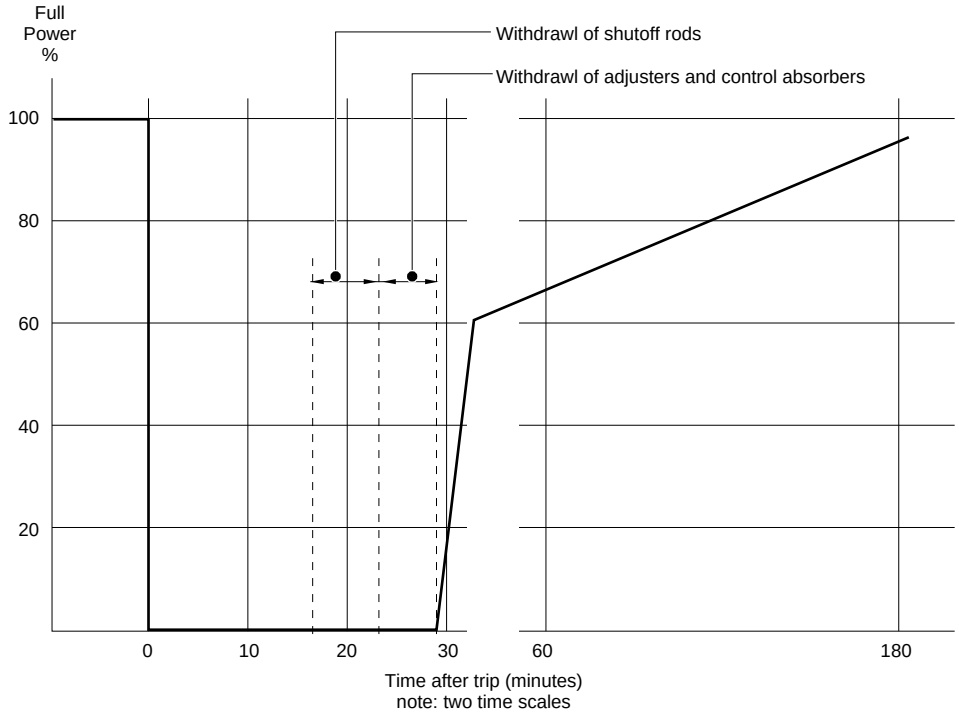
The time available to the operator between the trip and initiating shutoff rod withdrawal so that a poison out can be avoided is a function of several factors:

- the reactivity power coefficient which is a function of fuel irradiation amongst other factors,
- disposition of reactivity devices a time of trip,
- power history prior to trip.

About 17 minutes is available to understand the reason for the trip and to be assured that the cause has been dealt with, and to reset the systems and to restart. This assumes equilibrium fuel, little or no change in bulk moderator temperature, all adjusters initially in the core, and previous steady state operation at full power. The time is greater if reactor trips from steady state operation at less than full load. During early operation with fresh fuel, the large negative power coefficient for reactivity also adds several minutes to the time.

Figure 7

Startup after reactor trip



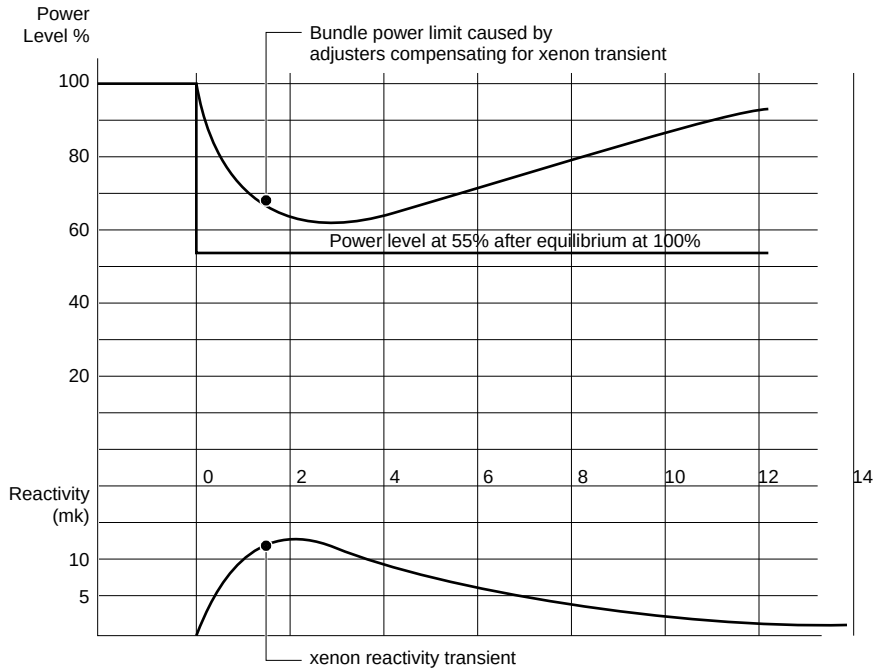
8.2 Load Reductions

The CANDU 6 is capable of suddenly reducing unit power from full load to any power down to a minimum of approximately 55% of full load and maintaining that reduced level indefinitely without poisoning-out. However, the subsequent rate of return to full power operation, as in the case of a startup following a reactor trip, is severely restricted by fuel rating limits, because of the use of adjusters to overcome the buildup of xenon poison. This is illustrated in Figure 8 where it is assumed that the power has been reduced after steady state operation at full power, to 55%. Three hours later the reactivity load is about 13.25 mk and several adjusters have had to be withdrawn. The resulting flux distortion limits the power level that the reactor can be returned to without overpowering a significant number of fuel bundles. This limit gradual reduces.

The situation is considerably better for smaller power reductions. For example, at any time after a reduction to 90% of full load, the unit can be returned to full power operation at the normal loading rates with no fuel overrating. However, there may be other constraints preventing a quick return to full load, such as channel power limits and insufficient trip margins on some overpower trip detectors.

Figure 8

Power recovery after step reduction in power



9.0 Summary

The plant control systems, taken together, provide safe and efficient operation of the plant, safeguarding worker, public health and the environment while producing a secure return on the investment of the owner.

The systems have these general features.

- automatic control is used extensively so that the operating staff are free for higher level monitoring of plant status,
- redundant information is provided so the operator can quickly assess the plant status and intervene manually when necessary,
- the design is tolerant of expected and unexpected transients,
- damage to plant equipment is prevented or minimized,
- high reliability and availability through redundancy and component selection,
- the intervention of safety systems should be avoided in all but cases where public safety might be threatened.

SDS2 (LISS)
Liquid Injection Shutdown System

Training Objectives

On completion of this lesson the participant will be able to:

- state the safety related function of the system,
- draw a simple flow diagram of the system,
- briefly explain how the system works,
- list the various modes of operation under normal and abnormal conditions,
- state the interdependence of the system with other systems,
- list the overpressure protection and environmental qualifications,
- identify the separation and independence from interfacing systems and other special safety systems, both within group 2 and group 1.

Table of Contents

1. Introduction

In all CANDU reactors, there are special safety systems which are specifically designed to mitigate the consequences of a serious process failure. These systems perform no function in the normal operation of the plant. They consist of the following:

a. Shutdown System Number 1 (SDS1)
b. Shutdown System Number 2 (SDS2)
c. Emergency Core Cooling System
d. Containment System.

This manual presents a description of the mechanical portion of SDS2 the Liquid Injection Shutdown System (LISS). A description of the trips, trip logic, etc., for SDS2 is given in the "CANDU Shutdown Systems" manual.

CANDU 6 is used as the reference design for the purpose of this manual. A comparison with Ontario Hydro stations is presented in subsection 3.3.

The LISS is part of the reactor SDS2. Upon receipt of signals on any two of the three SDS2 trip channels, the injection system must quickly shut down the reactor. This is accomplished by injecting a neutron absorbing liquid (gadolinium nitrate dissolved in heavy water) directly into the moderator in the reactor core.

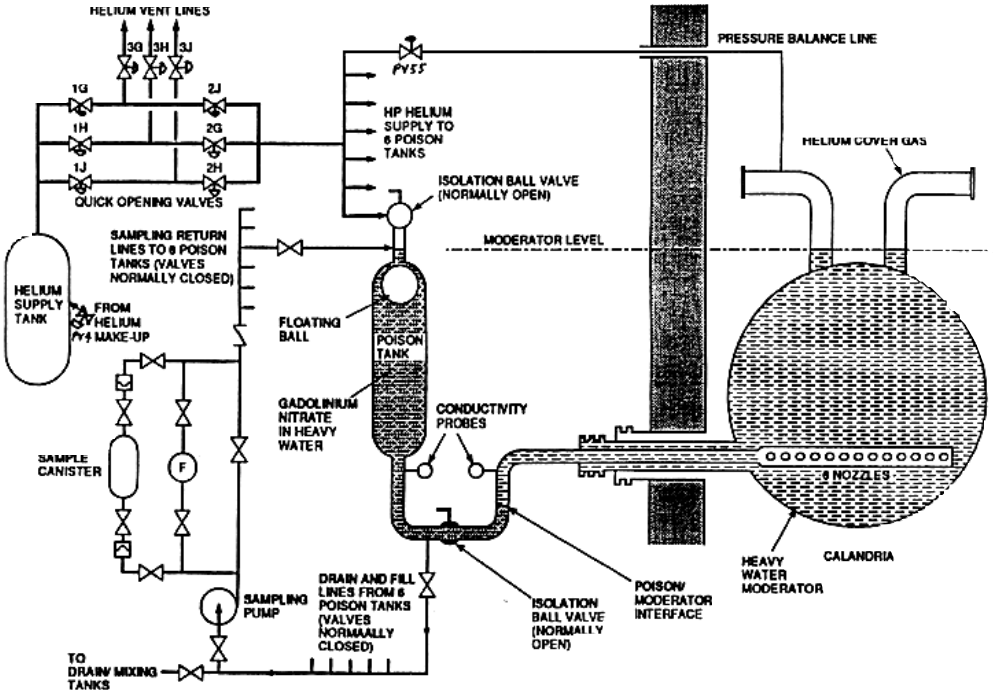
A schematic of the LISS is presented in Figure 1. The neutron absorbing gadolinium nitrate solution (called "poison") is stored in six identical pressure vessels (poison tanks) located in an accessible part of the reactor building. Each poison tank feeds one injection line which passes through the calandria vault to an injection nozzle passing horizontally through the reactor core. A single helium supply tank contains high pressure helium to force the liquid poison from the poison tanks into the core. An array of six quick opening valves in the line from the helium supply tank to the poison tanks isolate the poison tanks from the high pressure helium. Upon opening of these valves, the helium pressurizes the poison tanks and injects the liquid poison into the reactor. A floating polyethylene ball in each poison tank seals on a seat at the bottom of the tank when the tank is empty of liquid, preventing passage of the helium to the calandria.

2. Functional Requirements

2.1 Safety-related Functional Requirements

For the design basis initiating events (described in the "CANDU Shutdown Systems" manual) the LISS must have sufficient speed and negative reactivity depth to reduce the reactor power to levels consistent with available cooling. This has to be achieved with the most effective nozzle unavailable.

Figure 1
Liquid injection shutdown system for SDS2



2.2 Process-Related Functional Requirements

The LISS is designed to:

- Remain in a poised position at any time the reactor is in operation and, upon receipt of signals on any two out of three SDS2 trip channels, reliably and rapidly shut down the reactor. This is be achieved by injection of gadolinium nitrate in heavy water directly into the moderator.
- Ensure that normal operation of process systems cannot impair the effectiveness of the shutdown systems.
- With fuel in the reactor, under no circumstances be made unavailable (i.e., no more than one poison tank unavailable) except when the reactor is put in a "guaranteed shutdown state" and with SDS1 poised.
- Provide a means to drain the LISS, mix gadolinium nitrate uniformly with D_2O to the required concentrations and refill the system.
- Provide continuous measurement of gadolinium concentration in each poison tank by conductivity probes, with low concentration alarm.

- Provide continuous measurement of gadolinium concentration in injection lines near injection nozzles by conductivity probes, with high concentration alarm to indicate undesirable migration of poison toward the moderator D_2O.
- Provide gadolinium concentration measurements in mixing tank, by sampling.
- Provide measurement of gadolinium concentration in each poison tank, by sampling. The sampling system will:
  - confirm measurements made by conductivity probes,
  - recirculate the tank contents to ensure a representative sample is obtained,
  - be "on line", injection from tank being sampled will be possible,
  - include provisions for increasing poison concentration in poison tank.
- Provide indication and alarm of helium tank pressure, poison tank level, and ball isolation valve closure.

3. System Description

3.1 Design Evolution

Early CANDU reactors (Douglas Point, Pickering A) used moderator dump, rather than LISS, to rapidly shut down the reactor. The Bruce A reactors were the first to use LISS for the SDS2. The design has changed very little since then, the most significant change being the addition of a recirculating sampling circuit (for on-line sampling of poison tank gadolinium concentration) in subsequent reactors.

A comparison of LISS design in CANDU 6 and Ontario Hydro stations is provided in Section 3.3.

3.2 LISS System Description - CANDU 6

A vessel containing high-pressure helium at 8.3 MPa(g), supplies the source of energy for a rapid injection. The tank is connected, through six quick-opening valves arranged in a triplicated array, to a helium header which services six poison tanks. The quick-opening valves are air-to-close, spring-to-open, so that loss of air supply or electrical power initiates poison injection. The six cylindrical poison tanks are mounted vertically on the outside wall of the reactor vault. Each of these poison tanks contains gadolinium nitrate solution. The nominal solution concentration is 8000 mg of gadolinium per kg D_2O.

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, i.e., six 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 permit complete dispersion of the poison into the moderator.

Conductivity probes mounted in the lines immediately below the poison tanks provide on-line monitoring of gadolinium concentration in the poison tanks (new for Wolsong 2). In addition, a recirculating system is provided for taking samples from a selected poison tank while the reactor is operating and without requiring that the tank be removed from service.

There is a liquid-to-liquid interface between the poison solution and the moderator as shown in Figure 1. Motion of the interface is caused by the poison very slowly migrating 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 mixing of the poison solution with the moderator. The moderator system is designed to minimize these effects.

Conductivity probes are provided to detect when poison solution reaches the top of the U-section. Upon alarm from these probes, the injection line should be backflushed and the associated poison tank refilled with fresh gadolinium nitrate solution. Under normal conditions, this is expected to be an infrequent event. This procedure ensures that the poison concentration remains above an acceptable minimum. Analysis has shown that the system reactivity is insensitive to large variations in poison tank concentration.

The poison tanks are at a lower elevation than the moderator level. The tanks are thus overfilled and the interface between the poison solution and helium is in a smaller diameter vertical pipe leg above the tank. Variations in moderator level result only in the movement of small volumes of poison in the small diameter injection pipe.

Each poison tank contains a floating polyethylene ball. When an injection is initiated, the helium driving gas transfers the poison to the calandria and the ball is driven to the tank bottom. In the bottom position, the ball seats at the poison tank outlet and prevents the release of a large volume of helium to the calandria. The ball also back seats at the top of the poison tank prior to injection, restricting the movement of poison because of variations in moderator level. Usually back seating is for shut-off purposes but in this case it is important that shut-off does not occur. The flow of poison is required during recirculation while sampling and the level in the small pipe above must be the same as the Moderator level.

Each poison tank can be isolated by manual isolating valves located in both the gas and poison legs to permit maintenance and testing on one poison tank at a time without disabling the shutdown system. Using keyed interlocks, the operator is warned by alarm if valve closure occurs on more than one poison tank.

Measurements are made of helium make-up supply pressure, helium supply tank pressure (by two different methods), injection tank level, and injection check ball location. Any one will initiate an alarm in the main control room.

Limit switches are provided on each of the six quick-opening valves, three vent valves and helium make-up 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. A drain tank which is also provided may be used for sampling.

3.3 Comparison of Candu 6 with Ontario Hydro Stations

Pickering A uses moderator dump, rather than LISS, as its second shutdown system. All other Ontario Hydro stations use a LISS that is very similar to the one used on CANDU 6. The differences, most of which are minor, are described in Table 1 following.

Table 1
Comparison of CANDU 6 LISS with LISS in Ontario Hydro Stations

	CANDU 6	Pickering B	Bruce A	Bruce B	Darlington
Number of Poison Tanks/Injection Nozzles	6	6	7	8	8 (note 1)
Recirculating Sampling circuit?	Yes	Yes	No	Yes	Yes
Number of Quick-Opening Valves	6	6	6	6	4 (note 2)
Helium Make-up	He bottles	He bottles	(note 3)	(note 3)	(note 3)
Conductivity Probes on Lines Below Poison Tank?	(note 4)	No	No	No	Yes
Drain Tank?	Yes	Yes	Yes	Yes	No

Notes:
1. *poison tank volume = 0.079 m^3 each on all reactors, hence larger reactors require more poison tanks/injection nozzles*
2. *on Darlington, the number of quick opening valves was reduced from six to four by modifying the control logic*
3. *helium make-up is from bulk helium supply system, backed up by helium bottles*
4. *existing CANDU 6 do not have conductivity probes on lines below poison tanks. Wolsong 2 (under construction) will have them.*

4. Major Equipment Description

4.1 Helium Supply Tank

The helium supply tank is a Class 3 vessel with a capacity of 1.13 m^3. It is made of 304L stainless steel. Design pressure is 10.3 MPa(g). Normal operating pressure is 8.3 MPa(g).

4.2 Quick Opening Valve Array

The array consists of six 7.62 cm quick opening globe valves with two valves in each of three parallel lines. Venting the interspace between the two quick opening valves in each line is a powered .95cm globe valve in series with a check valve.

The quick opening valves and the .95 cm globe valves are operated by the three SDS2 trip channels; G, H, and J. The two quick opening valves of any one channel are in different lines. The vent valve for a channel is connected to the same line as the upstream quick opening valve of the channel.

Design pressure	=	10.3 MPa(g)
Operating pressure	=	8.3 MPa(g) upstream
	=	27 kPa(g) downstream

refer back to Figure 1

4.3 Gadolinium Pressure Vessels (Poison Tanks)

The poison tanks store the major part of the gadolinium nitrate poison solution in readiness for an injection. The remainder of the poison is contained in the pipes above and below the tanks.

Each poison tank is basically a length of 25 cm stainless steel thick-walled pipe with butt weld flanges on each end, capped with mating flanges. Each tank has a capacity of 0.079 m^3 and is made of 304L stainless steel. Design pressure is 10.3 MPa(g). Normal poised operating pressure is 0.1 MPa(g). The top mating flange holds the inlet nozzle, a baffle plate and the upper ball seat. The bottom mating flange carries the outlet nozzle, drain and instrument connections, and the lower ball seat.

Inside each poison tank is a solid polyethylene ball. The ball floats in the poison solution when the tank is full, resting on the upper ball seat. When the tank is empty of liquid the ball rests on the lower ball seat. Following an injection the residual helium pressure, approximately 5.5 MPa(g), forces the ball into tight contact with the seat and a good seal results.

4.4 Mixing and Drain Tanks

These tanks serve to mix the gadolinium nitrate poison solution, to drain the poison tanks and to fill them with fresh poison solution. They provide facilities for sampling the poison and for draining off excess solution.

The mixing tank, equipped with the attached agitator, is used to mix the gadolinium nitrate solution in preparation for transfer to the poison tanks. It is sized 0.85 m^3 to receive the contents of all the poison tanks following an injection so that the system can be repoised as quickly as possible. The material used is 304L stainless steel.

The drain tank receives the contents of one of the poison tanks during backflushing. It also receives a small volume of poison solution during sampling of the mixing tank contents. It has a capacity of 0.14 m^3 and is made of 304L stainless steel. Both tanks have a design pressure of 700 KPa(g) and a normal operating pressure of 140 KPa(g).

4.5 Injection Nozzles

The injection nozzles are constructed of Zircaloy-2. They are approximately 5 cm inside diameter and have a total of 336-3.175 mm diameter holes in four rows. They are supported by thimbles that penetrate the calandria vault, end shield tank, shielding walls, and by locators inside the calandria, on their inboard ends.

5. Layout

The entire LISS (with the exception of the helium supply bottles and manifolds) is located inside the containment building. The six poison tanks are located above the reactor centreline but below the normal moderator level, so that they are completely filled. The six injection nozzles are in two rows of three, 1.5 m above and below the reactor centreline. The helium storage tank and quick opening valves are located above the poison tanks. The mixing and drain tanks are at a low level.

6. Control and Instrumentation

The quick opening valves, interspace vent valves, and helium make-up isolating valve are controlled directly by the SDS2 logic. The remainder of the LISS controls are independent of SDS2.

The major LISS information that is available in the main control room is:

- status of the above-mentioned valves,
- poison solution level in each poison tank, with low level annunciation,
- poison tank ball position indication with off-normal annunciation,
- low gadolinium concentration annunciation for each poison tank, from conductivity probe below tank (new in CANDU 6 for Wolsong 2),
- high gadolinium concentration annunciation, for each injection line (from conductivity probe),
- annunciation if more than one poison tank is isolated (from key interlock system),
- helium supply tank pressure and low pressure annunciation,
- helium make-up manifold pressure and low pressure annunciation.

7. System Operation

7.1 Poised State

In this state, the system is in readiness for an injection. This is the normal state of the system during reactor operation. LISS conditions are as follows:

- all quick opening valves are closed and all interspace vent valves (3G, 3H and 3J on Figure 1) are open,
- helium supply tank pressure is approximately 8.3 MPa(g),
- pressure balance line isolating valve is open, hence the gas pressure downstream of the quick opening valves is the same as the moderator cover gas pressure, approximately 27 KPa(g). This ensures that the poison level above the poison tanks is the same as the moderator level,
- at least five of the six poison tanks are on-line, i.e.,
  - their upstream and downstream isolating valves are open
  - the tanks are overfilled, as shown in Figure 1
  - the gadolinium concentration in the poison solution in each tank is above the minimum of 8000 mg/kg gadolinium in D_2O
  - the poison/moderator interface is below the injection line conductivity probe, as shown in Figure 1.

7.2 Injection

Upon receipt of signals on two or three of the three trip channels (G, H and J), the quick opening valves of those channels open. The pressurized helium in the helium supply tank flows through the valve array into the helium header, pressurizing this to 8.3 MPa(g). The valve array vent valves close on the same signals that open the quick opening valves of their channel. This prevents unnecessary loss of helium. A valve on the cover gas balance line closes when header pressure exceeds 345 kPa(g), preventing helium transfer to the cover gas system. The automatic isolating valve on the helium make-up line to the helium supply tank closes, preventing repressurization of the helium supply tank.

The pressurized helium in the helium header forces the liquid in the poison tanks down the injection lines and into the calandria. The balls in the poison tanks are forced down and are sealed on the bottom seat when the tank is empty, preventing further flow. Time from the opening of the quick opening valves to the seating of the poison tank balls is approximately 1 second.

7.3 Post Injection

Immediately following an injection, with the quick opening valves still open, the helium supply tank, the helium header and the poison tanks are all pressurized to about 5.5 MPa(g). The SDS2 trip has to be cleared manually. When this is done the quick opening valves will close, isolating the helium supply tank from the helium header and the poison tanks.

7.4 Repoising After Injection

After a shutdown, when it has been decided to restart the reactor, the injection

system should be repoised as soon as practical. The station operating procedures require that the LISS be poised before moderator cleanup can commence. Repoising consists of:

- depressurizing the poison tanks and helium header by venting the helium. This allows the poison tanks to refill with D_2O from the calandria.
- closing all the poison tank downstream isolating valves
- draining all the poison tanks into the mixing tank
- bulk sampling of this solution
- adding concentrated gadolinium nitrate/D_2O solution to achieve the required gadolinium concentration of 8000 ppm minimum
- bulk sampling of the solution to confirm the required concentration was achieved
- refilling the poison tanks by pressurizing the mixing tank with He
- returning vent, drain, and isolating valves to their poised position
- pressurizing the helium storage tank.

7.5 Backflushing

This operation forces back the poison solution that may have migrated up the injection line past the ball isolation valve, preventing it from reaching the calandria. This need only be done following annunciation from the conductivity probe in the line under consideration. The frequency of such backflushing is determined by the actual experience gained during the initial operation period of the station.

7.6 Poison Tank Sampling

Each poison tank is sampled periodically as the station operational requirements demand.

Individual poison tanks are also sampled after low readings alarmed by the on-line poison concentration sensors or after any repoising or backflushing operation, and to verify the strength of the poison solution in the tanks.

Poison tank sampling is achieved as follows:

- The tank to be sampled remains connected to the LISS system and so remains available in the event of an injection during sampling.
- The poison solution is pumped from the selected poison tank, through the respective drain valve, into the common drain header and into the sampling pump. During recirculation, the poison flows through the pump, isolation valves, and check valve. It then returns to the respective poison tank via a separate return line connected upstream of the tank in the corresponding helium injection line above the liquid poison level. For the design flow of 4.5 *l*/min approximately a 35-minute recirculation time is required. This represents two complete recirculations of the poison tank contents.
- Shortly after recirculation has begun, the flow is checked locally by bypassing into a separate line containing a flowmeter. After the flow has been measured, the flow is diverted back into the recirculation line, until the recirculation time is completed. At this time the flow is diverted into an

evacuated sampling canister until the canister is filled. The pump is then shut off, the sampling circuit isolation valves closed, and the sample canister, with contents, is removed from the system lines and taken to the station laboratory for analysis.

- If the poison solution concentration is below the required 8000 mg/kg gadolinium minimum, a make-up solution must be prepared to increase the poison concentration to at least 8000 mg/kg. A make-up canister, filled with the required poison make-up solution, is connected in-line via quick-connect couplings. The recirculation and flow measurement lines are valved out, and the make-up solution is pumped through the sampling circuit to mix with the poison tank contents.
- The entire sampling circuit is designed for injection pressure. Should injection occur during sampling, backflow of poison solution and helium through the sampling circuit towards the calandria is prevented by the check valve in the sampling system. Immediately upon injection the operation will shut down and isolate the sampling circuit.

8. Nuclear Code Classification, Seismic Qualification, Etc.

8.1 Nuclear Code Classification

The parts of the system in which a component failure could impair system operation are classified as Class 1. This is because a failure of this part of the system could cause, indirectly, a significant radiation release. This includes the main injection flow paths, from the quick opening valves to, but not including, the injection nozzles.

The injection nozzles are classified as Class Special (Class 1C for Wolsong 2) and are designed to meet the intent of Class 1.

The helium supply portion of the system is classified as Class 3. The helium pressure in this part of the system is continuously monitored by two independent pressure sensors, each with an alarm in the control room. A failure in this part of the system would release only clean helium, and although it would lead to system unavailability, this would be known in the control room and the reactor could be shut down until the system is repaired and repoised.

For Wolsong 2, the portions of the two helium make-up lines penetrating containment are upgraded from Class 3 to Class 2, back to isolating valves.

The poison mixing, draining and filling part of the system is classified as Class 3 because a component failure in this section, although possibly causing a release of tritiated heavy water, would not impair system operation. Also this section is normally isolated from the rest of the system.

The helium make-up manifolds and the adjacent pressure regulating valves are classified as non-nuclear (CSA Standard B.51, Class 6). A failure of one of these

components would release only clean helium, and would not impair system operation.

All sampling circuit components are classified as Class 1, with the exception of the flowmeter and quick-disconnect couplings, which are classified as Class 3 and Class 6 respectively. These non-Class 1 components are allowed on-line for restricted time periods only. A failure of these non-Class 1 components would not impair LISS operation, and hence they are exempted from Class 1 requirements.

8.2 Seismic Qualification

The LISS must be capable of operating either during or after the Design Basis Earthquake (DBE) - the system seismic qualification is therefore DBE.

All the system components, with the exception of the six quick opening valves, are passive during system operation. These quick opening valves must be qualified to DBE Category B. Other components (such as manual valves, pressure vessels, and powered valves) whose operation is not required during operation of the system, but only the maintenance of pressure boundary integrity, may be qualified to DBE Category A.

Components whose failure during the DBE would not impair system operation, such as those tanks, valves and lines associated with the poison mixing, draining and filling part of the system, are not seismically qualified.

The Class 1 portions of the recirculating sampling system are seismically qualified to DBE Category A. Isolation valves that form seismic boundaries are qualified to DBE Category B.

8.3 Overpressure Protection

The helium supply tank, and piping upstream and downstream to the quick opening valves, is protected from overpressure by two redundant spring-loaded relief valves. Their setpoint is 8.96 MPa(g), compared to a design pressure of 10.3 MPa(g).

The mixing and drain tanks are each protected from overpressure by a spring-loaded relief valve set at 550 KPa(g), compared to a design pressure of 700 KPa(g). Also, the low pressure helium supply line to these tanks has a spring-loaded relief valve set at 550 KPa(g) to protect against overpressure in the event that the pressure regulating valve fails in the open position.

A rupture disc with a bursting pressure 414 KPa(g) protects the low pressure D_2O piping between the poison tanks and the drain/mixing tanks from overpressure in the event of an injection with some normally closed valves left open.

8.4 Environmental Qualification (EQ)

The LISS performs an essential safety function during events causing harsh environmental conditions (Loss of Coolant Accident or Main Steam Line Break) and therefore components of the system required for reactor shutdown, or whose failure would impact reactor shutdown, are environmentally qualified.

8.5 Grouping and Separation

The LISS is physically and functionally independent of SDS1, different in concept, and physically remote from it (outside the reactor core). The SDS1 is mechanical in nature and enters the reactor vertically from the reactivity mechanism deck whereas the LISS is hydraulic in nature, and enters the reactor horizontally from the side. The LISS is a Group III System

8.6 Waterhammer

When injection commences, the LISS pressurizes quickly and therefore pressure transients (waterhammer) must be considered in the design.

9. Interfacing System

9.1 SDS2

The SDS2 system provides the trip signals in three channels to the six quick opening valves, to initiate an injection. This system is described in the lecture on "CANDU Shutdown Systems".

9.2 Moderator Cover Gas System

The Moderator Cover Gas System provides the pressure balance to ensure D_2O levels in LISS and calandria are equal.

9.3 Moderator System

The Moderator System receives the injected gadolinium nitrate/D_2O mixture from the LISS. It and the system are in static equilibrium with the LISS poised.

9.4 Reactor Building Active Ventilation System

This system receives helium vented from the LISS and exhausts it while it is monitored for activity.

Emergency Core Cooling System (ECC)

Training Objectives:

On completion of this lesson the participant will have the required knowledge to:

- Outline the function and design requirements of the emergency core cooling system.
- Draw a simple sketch of the ECC System including identification of all major components.
- List and explain the parameters affecting the performance of the ECC System.
- Describe the operation of the ECC System under the following headings:
  - Loop Isolation
  - LOCA Detection and Initiation
  - Steam Generator and Crash Cool Down
  - High Pressure Injection Phase
  - Medium Pressure Injection Phase
  - Low Pressure Injection Phase
- Explain how the following parameters interact to initiate the ECC System:
  - Low Pressure
  - Conditioning Signals
- State the automatic actions which occur during the following phases:
  - High Pressure Injection Phase
  - Medium Injection Phase
  - Low Pressure Phase
- Describe the manual actions required upon the initiation of the low pressure phase.
- Explain when and how the ECC System is blocked.
- Describe the major components of the ECC System.
- Describe how overprotection is provided in the system.
- Describe how chemical control is achieved.
- Explain how water hammer could occur and the design features that prevent water hammer damage.
- Describe the interactions of the ECC System with support systems.

Table of Contents

1 Introduction

The basic function of the Emergency Core Cooling (ECC) system is to provide an alternate means of cooling the reactor fuel in the event of an accident, which depletes the normal coolant inventory in the heat transport (HT) system to an extent that fuel cooling is not assured. The ECC system is required to detect a loss of coolant accident (LOCA) and inject water into the HT system to refill the fuel channels and remove residual (stored) and decay heat from the fuel after a LOCA.

ECC system effectiveness is measured upon its ability to limit the extent of fuel and fuel channel overheating following a loss-of-coolant accident (LOCA).

ECC system effectiveness relies on the successful operation of HT loop isolation as well as the shutdown system and certain safety support systems. These safety support functions include the cooling water supply, power for pumps, valves and instruments, instrument air supply and steam generator cooldown. Sufficient monitoring systems are installed so that the operators can operate the ECC system properly in the long term, and confirm its operation.

The design of the ECC system complies with the requirements of the following Atomic Energy Control Board (AECB) Regulatory Documents:

- Atomic Energy Control Board (AECB) Regulatory Document R-9, Requirements for Emergency Core Cooling System for CANDU Nuclear Power Plants.
- Atomic Energy Control Board (AECB) Regulatory Document R-7, Requirements for Containment Systems for CANDU Nuclear Power Plants.
- Atomic Energy Control Board (AECB) Consultative Document C-6, Requirements for the Safety Analysis of CANDU Nuclear Power Plants.

2 Design Basis Events

Design basis events are those events which impose one or more requirements on ECC system performance. By definition, they are all LOCA events - where ECC is required to refill and maintain the primary circuit inventory. Simply, there are three main design requirements imposed by the LOCA events:

- Speed of ECC Response/Flow Requirements,
- Pressure of ECCS/Cooldown Requirements, and
- Detection of a very small LOCA.

The largest pipe breaks require the fastest ECC response and highest ECC system flows.

Small breaks, feeder size and smaller, do not require such high flows and quick response. However, the broken loop depressurizes so slowly due to the smaller breaks, that these breaks are critical to designing the secondary circuit cooldown

(steam generator crash cool). Good continuous ECC flow is maintained due in part to the opening of the Main Steam Safety Valves (MSSVs) on the secondary circuit.

For the very small break sizes, the ECC flow and pressure requirements are bound by those for the large breaks. However, the reactor building pressure may not increase significantly for the very small break sizes and the ECC conditioning signal of high reactor building pressure for large breaks may not be effective for LOCA detection. Although operator initiation of ECC is reasonable for such small breaks, automatic initiation is also provided by another ECC conditioning signal of sustained low heat transport pressure.

3 Design Requirements

3.1 Functional Requirements

3.1.1 Fuel Cooling Requirements

For all design basis events the ECC system meets the following fuel cooling requirements:

- The system is capable of maintaining or re-establishing sufficient cooling of the fuel and fuel channels for the design basis events, so as to limit the release of fission products from the fuel and maintain fuel channel integrity.
- After re-establishing sufficient cooling of the fuel, the system is capable of providing sufficient cooling flow for a period of three 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. After three months, no further damage to the fuel will occur even in the absence of emergency core cooling, due to low decay heat of the fuel.
- The system is capable of continuing to provide sufficient cooling flow and remove residual and decay heat from the fuel, following a Site Design Earthquake (SDE) occurring 24 hours after a LOCA.
- The release of radioactive material from the fuel in the reactor is limited such that the reference dose limits, defined in AECB consultative document C-6 (Reference 6.3-3), are not exceeded.
- The fuel in the reactor and the fuel channels is kept in a configuration such that continued removal of decay heat produced by the fuel can be maintained by the ECC system for as long as it is required to prevent further fuel damage.

For the small LOCA events, the ECC system will prevent 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.

3.1.2 Other Functional Requirements

a) The system is poised during normal reactor operation for the automatic detection of LOCA and injection of emergency cooling water into the heat

transport system following a LOCA. During reactor shutdown, with the HT system depressurized and below 100°C, the system can be normally blocked for maintenance.

b) The system is capable of detecting all LOCA's, both in-core and out-of-core LOCA's.
c) The system is capable of providing a signal to close the valves interconnecting the two HT loops to isolate the unfailed loop from the failed loop.
d) The system is capable of providing a signal to open the MSSVs in the event of a LOCA.

3.2 Seismic Qualification Requirements

All equipment required for continued fuel cooling is designed to remain functional following the site design earthquake for the plant site.

As the heat transport system is designed and qualified to withstand the effects of a design basis earthquake there is no requirement to design the ECC system for a loss-of-coolant accident coincident with or caused by a design basis earthquake. However, in the event of a postulated, random loss-of-coolant accident, the ECC system must operate for a period of up to three months. During this period, an earthquake could occur, but due to the limited time of interest (three months), the postulated earthquake is a site design earthquake (SDE).

Based on the low probability of the combined events, the earthquake is not assumed to occur within the first 24 hours after the LOCA. By this time only the low pressure injection portion of the ECC system is operating, hence, only it needs to be seismically qualified to SDE in order to ensure that the ECC system functions as required.

3.3 Environmental Qualification Requirements

Qualification is required for all ECCS equipment which is required to operate, or continue operating, after an accident has occurred. Qualification includes tests to demonstrate to the extent practicable that the type of equipment can be operated under conditions similar to those which would exist during or following an accident.

Possible adverse conditions which the ECC components, located inside the R/B, may experience include high temperature, humidity, radiation, water spray, effect of debris and increased pressure.

The ECC components outside the R/B that are required for the long term ECC operation, e.g. pumps, heat exchangers, motorized valves, may see high radiation.

All components which may contain radioactivity after a LOCA are qualified to withstand the maximum anticipated cumulative dose.

3.4 Reliability Requirements

There are two distinct reliability requirements for the ECC system i.e., demand unavailability and long term reliability. The former is defined as the probability that the system will not be available on demand to carry out its functions. Demand unavailability is estimated on the basis of the entire system being unavailable on demand and is not influenced by the mission time. The latter refers to the reliability of the components which must continue to function after a LOCA so that the system fulfills its functions over a mission period. A mission period of three months for the ECC system is assigned on the basis that no further fuel damage would result from the loss of ECC system after this time, due to low decay heat of the fuel.

The following reliability requirements are satisfied by the ECC system:

a) The system is designed such that the demand unavailability does not exceed 10^3. The system is considered available only if it can be demonstrated to meet all the minimum allowable performance standards. Calculations to demonstrate that this requirement can be met is based on availability data from direct experience or reasonable extrapolation therefrom.

b) The design of the ECC system and the relevant safety support systems must consider long term reliability of the components which must continue to function after a LOCA. The preliminary target for long term unavailability for the three month mission period is determined and the ECC system is designed to meet the target.

c) The ECC system is provided with sufficient redundancy of active components so that

(i) the system demand unavailability does not exceed the regulatory target and

(ii) failure of a single active component does not impair the ECC system (components which do not change state and do not depend on safety support system such as compressed air, electrical, power, etc, in order to perform their design functions are exempted from this requirement).

d) Redundant components/equipment are sufficiently separated from each other to minimize any possibility of disabling one from the failure of the other.

e) The ECC system design is such that a failed component can be put in a safe state, i.e., the failure mode of the components is in the fail-safe mode.

f) In the event of an accident, it is not readily possible for the operator to inhibit the automatic action of the ECC system. For example, placing a single switch in an inappropriate position should not disable both injection paths.

g) All necessary actions of the ECC system equipment initiated by automatic control logic, can also be initiated manually from the main control room or the secondary control area.

h) The control loops and essential monitoring instrumentation are independent from the process instrumentation. All initiating signals are triplicated.

i) All maintenance and availability testing, which may be performed while the ECC system is in a poised state, can be carried out without impairing the system.

3.5 Availability Testing Requirements

Dedicated test facilities are provided to allow regular on-power testing of components and confirm that the ECC system, including required safety support systems, will operate correctly when called upon to do so and to demonstrate the required availability of the system. A series of overlapping tests have been designed to check subsystem operation from instrumentation operation to valve operation, motor operation, etc., without causing the system to be unavailable during any testing.

3.6 Grouping and Separation Requirements

The ECC system is designated as a Group 1 system and is located with other Group 1 systems as far as practicable. Qualified portions of the system are located in qualified areas or protected by suitable barriers. The following general principles are applied.

- The ECC system is physically and operationally independent of the other special safety systems to ensure that simultaneous failures of the ECC system and other special safety system cannot be caused by a single common-mode event.
- The ECC system is independent from all other process systems, to ensure that the required safety function is not lost as a consequence of a process system failure.
- Radiation and Shielding Requirements

During normal reactor operation, there is no radioactivity in the ECC system components outside the reactor building. Sufficient shielding is provided in order to carry out maintenance on the ECC valves inside the R/B during a reactor shutdown.

Adequate shielding of any ECC system equipment in the service building, which could contain radioactive material following an accident, is provided to permit personnel access to plant equipment for which such access might be required.

3.7 Monitoring Requirements

The design of the ECC system is such that the status of important equipment required for operation of the ECC system can be monitored from the control room. All failures of ECC system components which may interfere with proper functioning of the ECC system is annunciated in the control room.

4 Parameters Affecting ECC Performance

4.1 Steam Generator Crash Cooldown

The Main Steam Safety Valves (MSSVs) are opened by the ECC initiation signal to depressurize the steam generators. This is not strictly required for good ECC performance, but it does affect the ECC design.

LOCA of any size will eventually depressurize the HT system down to about the secondary side pressure. The depressurization will be slow (if at all) before reactor trip, but rapid after trip. If the ECC system can provide sufficient flow at that high pressure, then crash cooldown is not needed. If the ECC system is designed to rely on crash cooldown, it is the small breaks which dictate how much crash cooldown is required (how many MSSVs must open). In order to meet ECC demand reliability requirements, usually the number credited in analysis is about half of the number which are instrumented to open.

Large-sized breaks would depressurize the HT system below the secondary side pressure without crash cooldown. Therefore, crash cooldown is not needed for ECC injection to occur. However, crash cooldown would relieve some heat to the atmosphere that the ECC system would otherwise have to cater for. Therefore, crash cooldown allows adequate performance from a less powerful ECC system.

Opening the MSSVs on a LOCA means that the steam generator tubes form part of the containment envelope. If the initiating LOCA is a steam generator tube(s) rupture, the failed steam generator must eventually be isolated. Crash cooldown must not be indefinite in this case, however, some amount of crash cooldown may be required to ensure effective ECC operation.

4.2 Pumped Injection

Pumps need electric power to run. In case of a loss of the normal electric supply, there is usually a time delay until the back-up supply is established. For ECC, this time delay must be in the order of seconds rather than minutes.

The shape of the pump curve is very important for ECC performance. If the curve is too flat, then the ECC flows, and hence ECC performance, is very sensitive to the HTS pressure.

Pumps can provide flow for an indefinite period (depending on water supply) up to pressures near the shut-off head. This has advantages for small LOCAs which only need a small ECC flow. If the shut-off head is high enough, ECC injection can occur without steam generator crash cooldown. The shut-off head required is usually about 1/2 MPa higher than the normal steam generator pressure.

4.3 Accumulator Injection

Accumulators usually consist of 1 or more gas tanks (air or pure nitrogen) plus 1 or more water tanks. The water is kept at low pressure while the gas is kept at high pressure. The initial gas pressure is obviously important in determining the ECC injection flow. However, more important is the amount of gas and the ratio of gas to water (by volume). An increase in initial gas volume allows the pressure to blowdown slower giving a faster injection. The ratio determines the final gas (and water) pressure. The final pressure must be designed to be similar to the ECC pump head.

Accumulators are relatively passive and can be very quick at initiation. They normally require steam generator crash cooldown to ensure continued injection for a small LOCA. Even if the accumulators start out at a high enough pressure, they will blow down to HTS pressure without crash cooldown, and injection will stop. The only way to maintain injection without crash cooldown is to provide a large amount of gas volume initially to slow down the accumulator depressurization. However, this would require ECC pumped injection to follow the accumulator injection at a very high head. In such a case, it would likely be better to simply use a very high head pump and no accumulators.

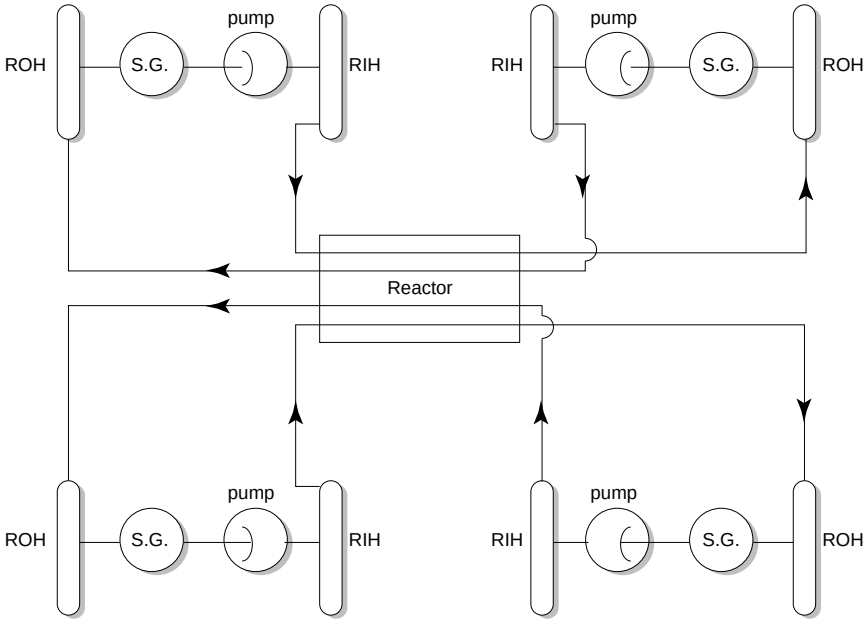
4.4 HT Pump Operation

The HT pumps promote flow in the nominal forward direction. Therefore they promote fuel cooling during a LOCA even before ECC is initiated. After ECC initiation, they would continue to promote forward flow (See Figure 1).

During a small LOCA, ECC acts like a make-up system to first refill the HTS, then match the break discharge to keep the HTS full. Meanwhile the HT pumps keep the flows strong in the forward direction. There may be some decrease in flow, after reactor trip and before refill, if the HT pumps see significant void. After refill, HTS flows can be higher than normal because the HTS is filled with cool liquid.

If the HT pumps are tripped due to a loss of electrical power (most likely just after reactor trip), computer codes and experiments show that the ECC system would refill the HTS just as effectively for small-sized breaks. This occurs because the HTS has not emptied very much before ECC injection. Post-refill flows in the HTS would be much less than if the HT pumps were running full-speed. ECC injection and thermosyphoning forces would dictate the magnitude and direction of the flows. It would not be unusual for some flows to reverse after refill. If the flow stagnates in some channels, a process of revoiding and refilling would occur termed Intermittent Buoyancy Induced Flow (IBIF).

Figure 1
H.T. Simplified Flow Sheet



During a large LOCA, HTS flow patterns don't necessarily follow the normal forward direction. However running HT pumps are still quite valuable. ECC injection usually occurs to the pump discharge near an Inlet Header, as well as near the Outlet Headers. Even if the pump suction lines are voided, running pumps can act like check valves to prevent the backwards flow of ECC through the pump. Therefore, the ECC must go forward to the header. If the break location is not in that Inlet Header, ECC would flow to the fuel channels. If the break is in an Inlet Header, the low pressure created by the large break size would promote ECC flow from the Outlet Header backwards through the fuel channels. Therefore, although HT flow patterns depend on the break location, running HT pumps are a benefit to ECC performance.

If the HT pumps are tripped due to a loss of electrical power, reverse flow through the pump can occur. This would significantly affect one core pass of a typical CANDU figure-of-eight HT loop. Consider a large Outlet Header break. The broken core pass would refill in the normal forward direction due to the very low pressure of the broken header. The other core pass does not have such an effect from the break. ECC injected to the Outlet Header could go forward over the adjacent steam generator or backwards through the core pass. In general the steam generator path is much less flow resistive (especially if crash cooled) and would receive the ECC flow and carry it to the Inlet Header of the broken core pass. ECC injected to the Inlet Header of the unbroken pass could go forward through the core pass or backwards through the HT pump. In general the pump path is much less flow resistive and would carry the ECC over the other steam generator to the broken Outlet Header. Therefore the unbroken core

pass remains unfilled. In practice the water from the headers could fall under gravity to fill the channels, but the process would be much slower than if the HT pumps were running full speed.

Whether the break size is large or small, HT pumps can not continue to run indefinitely. They must be tripped to avoid prolonged vibrations which could damage HT piping. Usually the pumps are tripped after the refill phase, either by manual or automatic action. Post-trip flows in the HTS could be; strong, if driven by a large break, small, if driven by steady thermosyphoning, or intermittent, if driven by IBIF.

5 System Description

5.1 General

The ECC system can be divided into six major subsystems as follows:

- Loop Isolation
- LOCA detection and system initiation
- Steam Generator crash cooldown
- High pressure injection stage
- Medium pressure injection stage
- Low pressure recirculation stage.

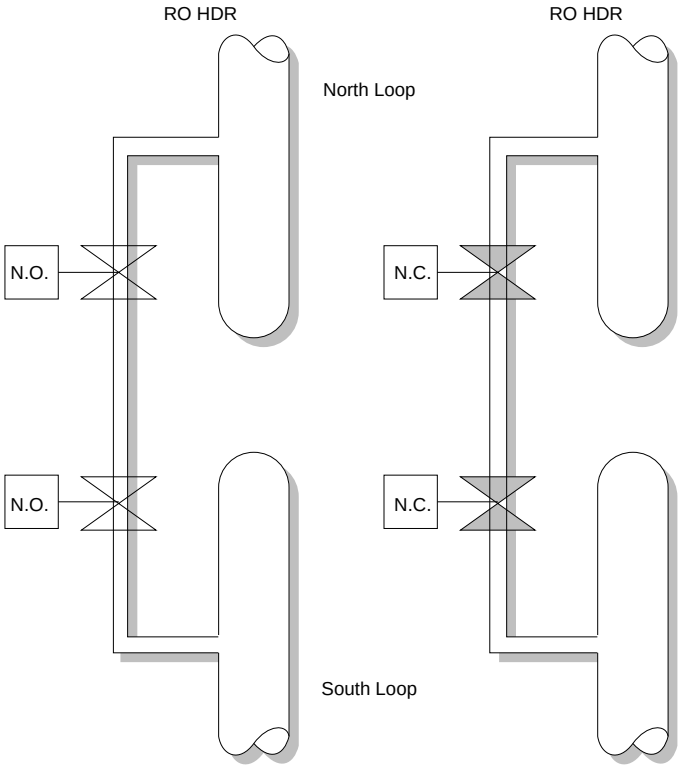
Figure 3.4 is a simplified diagram of the ECC system.

5.2 Loop Isolation

Following a LOCA, when the HT system pressure reaches 5.42 MPa(g), the loop isolation valves (D_2O feed valves, pressurizer isolation valves and HT purification system valves) close to prevent the transfer of coolant from one HT loop to the other. Each loop becomes isolated from the pressurizer, feed and bleed system and the purification system. The loop isolation function and hardware are completely independent of the other ECC functions and hardware. This independence allows the crediting of loop isolation in the event of a dual failure, namely LOCA plus the failure of ECC injection and/or steam generator crash cooldown.

Loop isolation ensures that sufficient inventory remains in the unfailed loop for its cooling to be effective (See Figure 2).

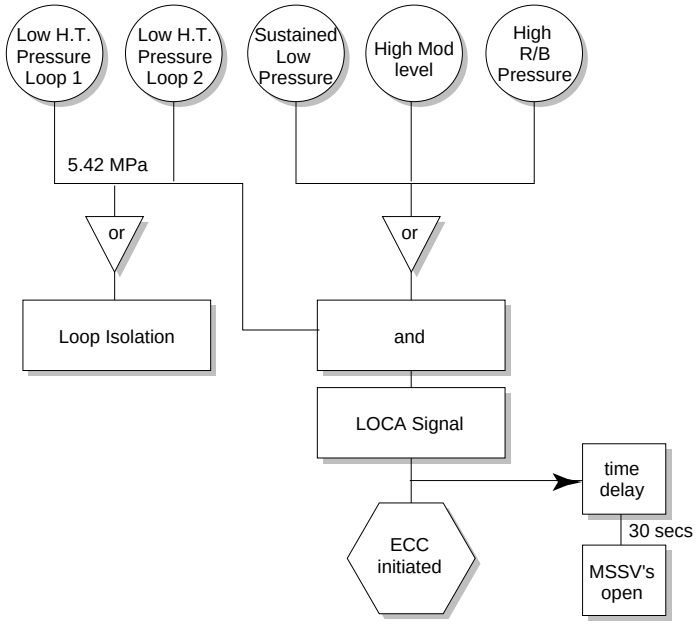
Figure 2
Simple Loop Isolation; (N.O.normally opened, N.C. normally closed).



5.3 LOCA Detection and System Initiation

The ECC system is poised during normal reactor operation and automatically initiated on a LOCA signal. The LOCA signal is generated when the HT system pressure falls to 5.42 MPa(g) and one of the conditioning signals, i.e., sustained low HT pressure, high moderator level or high reactor building (R/B) pressure, is present. Sustained low pressure signal provides coverage for small LOCAs, high moderator level for in-core LOCAs and high reactor building pressure for all other LOCAs.

Figure 3
Detection Logic



5.4 Steam Generator Crash Cooldown

The main steam safety valves (MSSVs) are opened on a LOCA signal with a 30 seconds delay to provide a rapid cooldown of the steam generators, commonly referred to as a steam generator crash cooldown. Each MSSV is fitted with a pneumatic actuator to overcome the spring force which normally keeps the valves closed, for this purpose.

5.5 High-pressure Emergency Core Cooling

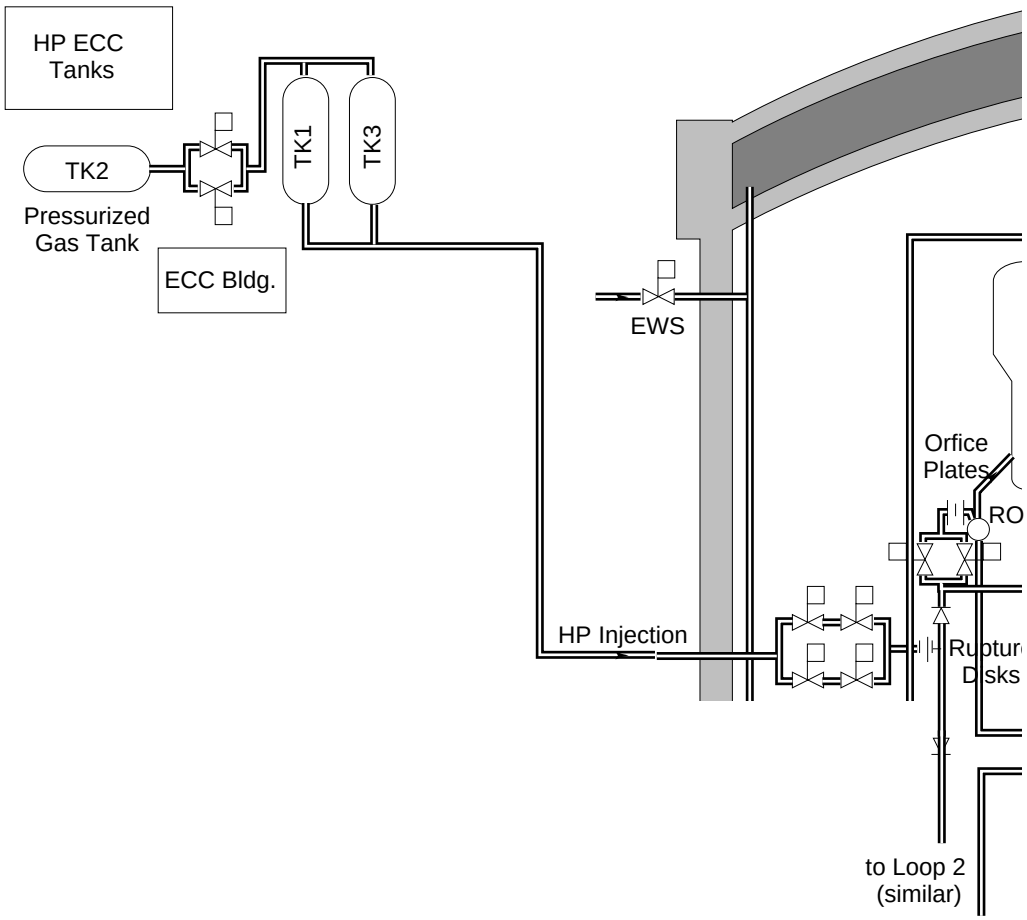
A high-pressure accumulator system containing one gas tank and two water tanks is provided to supply high-pressure emergency core cooling to the reactor. The tanks are located in the high-pressure ECC building. The volume of each tank is 108 cubic meters. The total quantity of water in the two water tanks is more than three times the inventory of one HT loop.

The ECC gas tank, normally pressurized to 4.14 MPa(g) is isolated from the ECC water tanks by two pneumatically operated valves. These gas isolation valves are in parallel for reliability reasons. Makeup for valve leakage is provided from an air compressor, backed up by a compressed gas supply from nitrogen cylinders. The ECC water tanks and the piping downstream are normally pressurized to 275 kPa and the water temperature is maintained at 21°C by an external heater and a recirculation pump. The water tanks are kept at relatively low pressure to minimize gas dissolution. To prevent corrosion, chemicals are added to the water tanks and are recirculated. Makeup water to the water tanks is by a connection to the demineralized water system.

Two parallel isolating valves known as the HP injection valves are provided to isolate the high pressure system from the injection piping downstream. These valves are operated by battery power and are normally closed. The two electrically operated valves in series with and downstream of the HP injection valves are normally open and are used only for testing. By having a test valve in series with each of the HP injection valves, testing can take place without blocking out both of the HP injection flow paths. Two check valves, in series with and downstream of the HP test valves provide passive protection to ensure that the HP accumulator system does not spuriously become over-pressurized by the HT system.

Since the ECC system is a light water system, two rupture discs, one in each of the common injection lines are used to provide a positive interface between H_2O and D_2O. Each of the injection lines to the reactor headers contains two motorized valves in parallel. These valves, called D_2O isolation valves, are supplied by battery power. They are normally closed and serve to isolate the heat transport system from the ECC system. Two parallel valves are provided for reliability reasons (See Figure 4.1).

Figure 4.1
Simplified HP Injection System



5.6 Medium Pressure Emergency Core Cooling Stage

In the medium pressure injection stage, two x 100% ECC pumps are provided to pump water from the dousing tank to the HT system headers.

The ECC Pumps are located outside the reactor building, at an elevation lower than the reactor building basement. A line from the dousing tank branches into two lines which connect to each of the pump suction lines. A normally closed air operated butterfly valve is provided in each branch line for isolation.

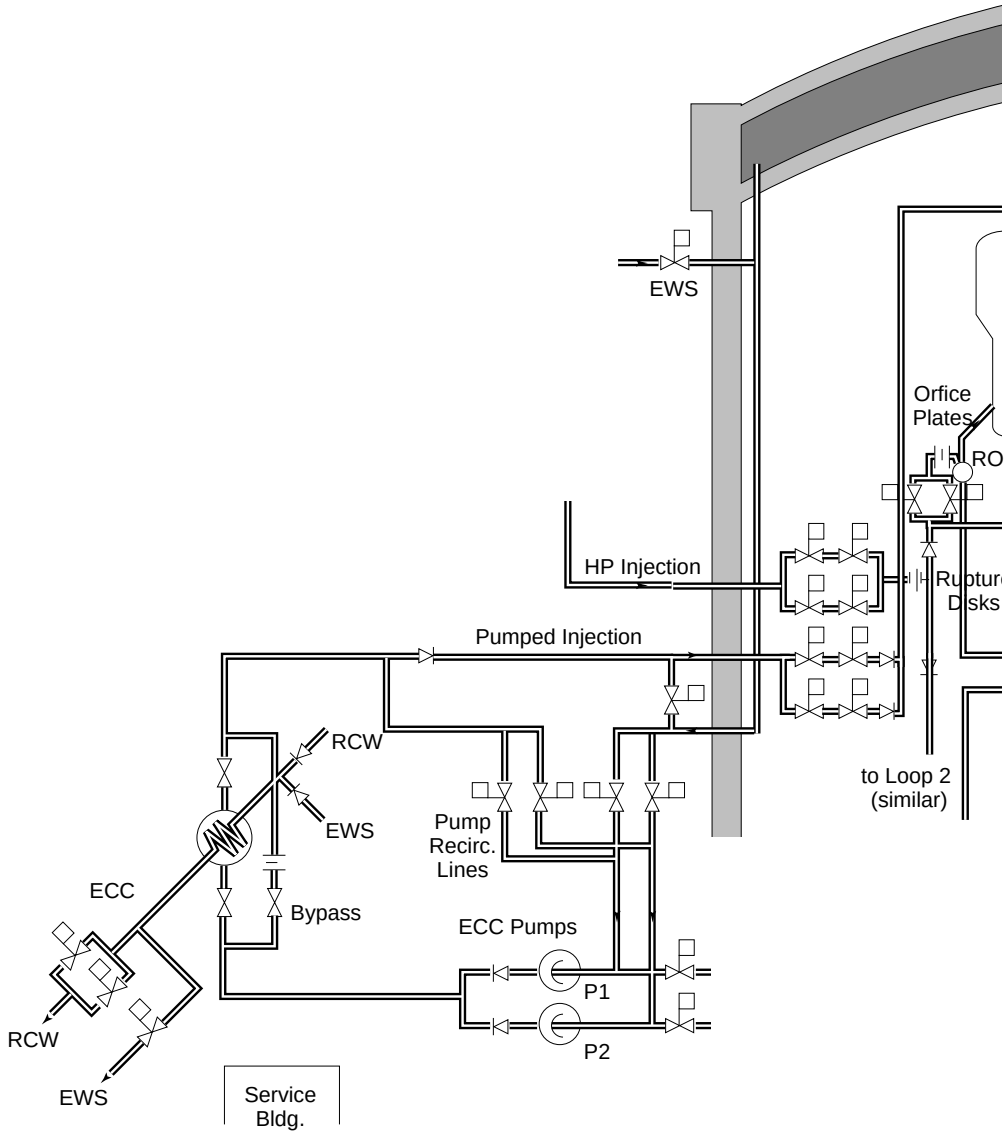
Each pump has a check valve and an isolating valve on the discharge. The isolating valve is used when pump maintenance is required. The check valve prevents high reverse flow through the non operating pump.

The discharge lines from each pump combine into one line that directs the coolant flow through the ECC heat exchangers.

Two parallel, normally closed, isolating valves called the MP injection valves provide the isolation of the MP injection system from the piping downstream. The two valves, in series with and upstream of the MP injection valves, are normally open and are used only during testing. By having a test isolating valve in series with each of the MP injection valves, testing can take place without blocking out the emergency injection system and hence testing has very little effect on system availability in terms of a system or valve being unavailable during the test.

Downstream of the MP injection valves are two check valves. These check valves separate the low pressure piping upstream of the MP injection valves from the high pressure piping when the MP injection valves are opened during the HP injection period (See Figure 4.2).

Figure 4.2
Simplified M.P. Injection System



5.7 Low Pressure Emergency Core Cooling

The long term low pressure injection stage utilizes the same ECC pumps as the MP stage but recovers the D_2O/H_2O mixture collected in the basement of the reactor building and pumps it back to the heat transport system via heat exchangers.

The two ECC pumps which take suction from the reactor building basement are provided with separate lines running through the basement slab. Strainers, located above the suction intakes, prevent foreign objects from entering the system. Trash screens around the strainers prevent them from being clogged by large objects.

Each suction line contains a pneumatic butterfly valve which is normally closed. This valve acts as a containment isolating valve and prevents the system H_2O

from draining into the reactor building. The dousing tank isolation valves of the MP stage are also normally closed to prevent rapid loss of H_2O from the dousing tank if the containment isolation valves are inadvertently opened.

The ECC pumps are supplied by Class IV and III power and are backed up by the emergency power supply system. The emergency power supply system ensures long-term reliability and it also ensures operation after a Site Design Earthquake. Sufficient instrumentation is supplied to detect possible failure of the operating pump and to automatically start the standby pump.

One of the two x 100% ECC heat exchangers is used to cool the recovered water during the low pressure stage operation. Each heat exchanger is designed to remove residual and decay heat from the reactor core and maintain the emergency core cooling flow at or below 49°C at the entry to the heat transport loop.

The cooling water side of the heat exchanger is provided with Class IV and III water from the Raw Service Water System. This is backed up by the Emergency Water Supply System to ensure long term reliability and to ensure operation of the ECC system after a Site Design Earthquake. Cooling water flow is not modulated since the requirement is that the emergency core cooling flow at the outlet of the heat exchanger be maintained a maximum value.

The heat exchanger are of plate type with titanium material to avoid pitting and general corrosion by stagnant service water during normal reactor operation. During normal reactor operation, both sides of the heat exchanger are filled with stagnant water. The water on the process side is circulated periodically during testing of the emergency core cooling pumps and during chemical addition. The service water flow is also tested during ECC pump testing.

Figure 4.3
LP ECC System

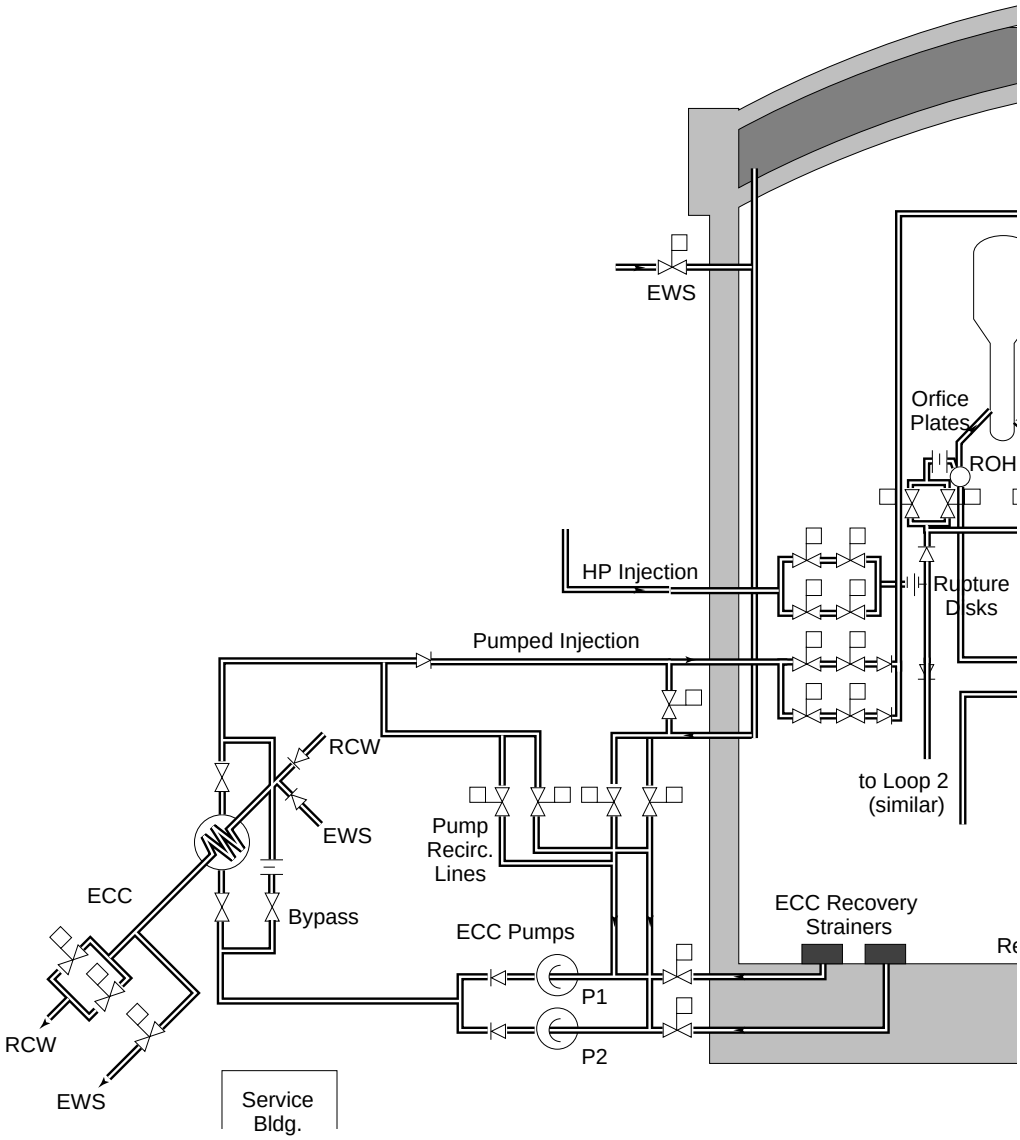
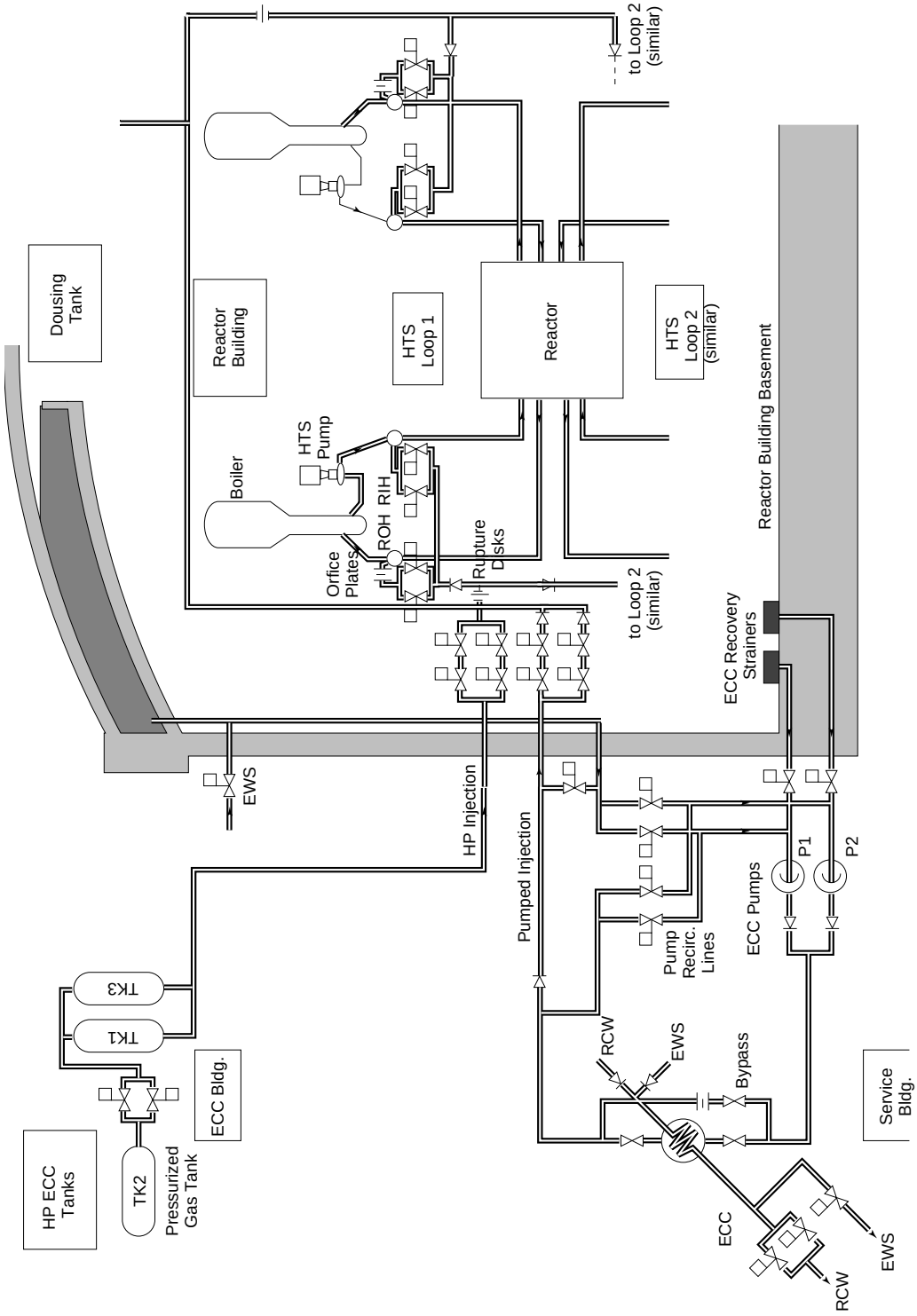


Figure 4.4
Emergency Core Cooling System



6 Operation

6.1 Initiation

Following a LOCA, a HT system depressurizes. This depressurization of the HT system from operating pressure to the pressure at which ECC water can enter the HT system is known as the blowdown phase. It varies in duration from a few seconds for large breaks to several minutes for small breaks. When two out of three header pressure measurements indicate that the pressure has dropped below 5.42 MPa(g), the loop isolation valves are closed, thereby isolating the failed loop from the unfailed loop.

When a different (independent) set of pressure measurements on either loop indicates that the pressure has dropped below 5.42 MPa(g), and high reactor building pressure ≥ 3.4 KPa(g) or high moderator level ≥ 10.12 m or sustained HT low pressure ≤ 5.42 MPa(g) indicated, a LOCA signal is generated and the ECC system is initiated.

Also, with a time delay of 30 seconds from the generation of a LOCA signal, the MSSVs are opened to depressurize the steam generators. This reduces the transfer of heat from the steam generator secondary side to the heat transport coolant and allows the steam generators to function as heat sinks at low temperatures.

The initiation of the system is followed by three stages of operation.

6.2 High-pressure Emergency Core Cooling Operation

When the emergency core cooling signal is triggered, all emergency core cooling injection valves open from the high-pressure injection tanks to the heat transport headers. These 20 valves open simultaneously: two gas isolation valves (pneumatic) between emergency core cooling gas and water tanks, two high-pressure injection valves (electrical) and 16 D_2O isolation valves (electrical) to the heat transport headers. Check valves prevent any outflow of heavy water into the emergency core cooling piping. The flow of emergency coolant begins when the pressure in the heat transport system is lower than that in the high-pressure injection tanks (see Figure 4.1).

The water from the high-pressure injection tank refills the failed loop and provides make-up to the unfailed loop to assure thermosyphoning. The steam generator main steam safety valves are opened to provide a heat sink.

The high-pressure emergency core cooling flow is conveyed by the reactor headers to the fuel channels to refill the core in the primary heat transport system. When the coolant and injection flow escapes from the break, the water collects in the reactor building basement. Sufficient coolant is available in the high-pressure injection tanks to provide at least 2.5 minutes of high-pressure injection following a maximum size break. This is equivalent to an average flow of 1,400 l/s with both HP injection valves open. For smaller break sizes, the

duration of high-pressure injection is longer. The average flow for a 10% break size is reduced to 700 *l*/s. On low coolant level in the emergency core cooling water tanks, the high-pressure injection valves and their test valves are closed, and HP ECC terminates.

6.3 Medium-pressure Emergency Core Cooling Operation

The isolation valves in the line from the dousing tank to the emergency core cooling pumps suction open automatically on the loss-of-coolant accident signal and one of the emergency core cooling pumps is started when these valves are opened. If this pump fails to start as indicated by a low pump differential pressure, the second 100% pump starts automatically. The medium-pressure injection valves are opened automatically on the loss-of-coolant accident signal with a time delay of 90 seconds. The flow of emergency coolant from the dousing tank via the emergency core cooling pumps begins when the high pressure ECC stage is complete. The emergency core cooling pump will recirculate water through a bypass until the pressure in the primary heat transport system is less than the pump injection pressure. Check valves isolate the medium-pressure portion during high-pressure injection.

The Class III diesels are started on a loss-of-coolant accident signal. Class III power is backed up by the emergency power supply system to deal with seismic events.

The coolant and injection flow escapes from the break and collects on the reactor building basement floor. Sufficient coolant is reserved in the dousing tank for an emergency core cooling supply of at least 12.5 minutes for the maximum break size (100% header break). This is equivalent to an average flow of 645 *l*/s. For smaller breaks, this time is extended. The average flow for a 10% break size is reduced to 380 *l*/s.

6.4 Low-pressure Emergency Core Cooling Operation

On a low dousing tank level, LP injection starts and MP injection is terminated automatically by the following actions: the ECC pump suction valves on the lines to the basement of the reactor building open, the ECC pump suction valves from the dousing tank close and the recirculated cooling water (RCW) return valves open to provide flow to the ECC heat exchangers.

The long-term LP injection is provided by collecting the mixture of H_2O and D_2O from the reactor building floor basement and recirculating it into the HT system via the ECC heat exchangers.

The two ECC pumps which provide injection during medium-pressure injection also provide long-term recirculation. Only one pump is required for this operation, the other is on standby.

Both heat exchangers are connected in parallel initially causing a total service water flow requirements on both secondary sides of 760 *l*/s. During normal reactor operation, heat exchanger isolating valves on primary and secondary sides of both heat exchangers are open for maximum reliability and downstream RCW return valves are closed (no RCW flow). Hence at the start of LPECC, upon opening of RCW return valves, cooling is provided by both heat exchangers. When the operator has time for the manual operation, one heat exchanger is isolated to remain on standby. The secondary side of one heat exchanger requires 606 *l*/s service water flow initially or 115 *l*/s EWS flow 24 hours after LOCA.

For large breaks, decay heat is removed from the core and this heat is transferred to the recirculated cooling water system or the emergency water supply system via the heat exchangers.

For small breaks, the injection flow is small and hence the amount of heat removed by the heat exchangers is small. The pump flow may be increased if desired by returning part of the ECC pump flow cooled by the heat exchangers via the recirculation valve and the suction valve of the non-operating pump back into the basement of the reactor building using remote manual control of these valves. A dividing wall between the pump suctions ensures adequate circulation of coolant in the reactor building basement to cool the water accumulated in the basement.

In the event of a pump trip, during the LPECC operation mode, check valves in parallel, downstream of the connection with pump by-pass line, prevent the draining of the piping back to the recovery sump. This minimizes waterhammer concerns when the pump is restarted.

The steam generator feedwater supply during post-LOCA operation is provided by the main feedwater pumps on Class IV power or by the auxiliary steam generator feed pump on Class III power. These pumps draw water from the deaerator and the demineralized water storage tank. An alternative independent source of feedwater to the steam generator is provided by the emergency water supply system. The feedwater to the steam generator is required during the period of low-pressure emergency core cooling operation for cooling the failed loop following a small break, and cooling the unfailed loop for all break sizes.

During the above sequence of events, coolant circulation is maintained in the unfailed loop by thermosyphoning with heat removal by the steam generators. The inventory loss from this loop prior to its effective isolation from the failed loop is replenished in the early high-pressure stages of emergency core cooling operation and is maintained by the continued operation of the system.

6.5 Manual Actions

All ECC system actions required to be performed in the first 15 minutes from the time of the postulated loss-of-coolant accident (LOCA) are performed automatically.

All automatic actions have the capability of being initiated manually from the main control room. This does not include self-actuated actions such as the opening of check valves. Manual provisions are such that off-normal conditions are alarmed to alert the operator of an unsafe condition.

To enable the HT system to be depressurized for maintenance, manual control is required to block the ECC system. Annunciation is provided to indicate when ECC is in the "blocked" state.

Following several hours of low pressure ECC operation, the operator is required to manually isolate one of the two operating heat exchanger loops.

In the event of an earthquake during the long-term recirculation operation, 24 hours after a LOCA (an earthquake within 24 hours after a LOCA is considered incredible), the normal power to the ECC pumps and RCW supply to the ECC heat exchangers may be lost. The operator is required to re-establish the long-term operation by supplying cooling water to one of the ECC heat exchangers from the EWS system to continue removal of decay heat. The ECC pump automatically restarts when EPS power is established.

6.6 Blocking ECC

It is safe to block the ECC system when conditions are such that quick ECC initiation is not required. The reactor power must be very low so that, if a LOCA occurred, any fuel heatup would be slow. The heatup rate must be slow enough that the operator could be credited to manually initiate ECC, or any other effective cooling method, to prevent fuel heatup beyond acceptable limits. It is also beneficial to specify that the HT fluid must be less than the boiling temperature. In case of a LOCA, the HT fluid would not flash out of the fuel channels, it would have to be boiled (which takes longer). In practice, the reactor power criterion is much more important than the HT fluid criterion. Boiling away the fluid would be fairly quick, especially to expose the top fuel element to steam cooling conditions.

7 Component Description

7.1 ECC Water Tank

During initial ECC injection, water stored in two ECC water tanks is injected under pressure to the reactor headers.

The tanks are cylindrical vessels with hemispherical ends located vertically to ensure maximum usage of the water in the tank without gas entrainment during

ECC injection. The vessel material is unlined carbon steel. During normal reactor operation, the tanks are filled with water up to the vertical inlet piping at the top of the tanks. Water in the tanks is maintained at 21°C with an external electrical heater and is recirculated by a pump. To prevent corrosion, chemical addition is also provided.

The ECC water tanks are normally isolated from the upstream gas tank by the gas isolation valves and on the downstream side by the HP injection valves. However, the pressure inside the tank will tend to increase due to leakage past the gas isolation valves. A relief valve set at 206 kPa(g) is provided on the water tanks via two normally open vent valves in series to prevent excessive pressure buildup above the normal water tank pressure during reactor operation. These vent valves are closed on a LOCA signal to ensure gas does not escape via the relief valve which has a much lower setting than the gas tank pressure. The water tanks are not continually pressurized with gas at high pressure to minimize the concentration of non-condensables in the water to avoid the presence of non-condensables in the primary side of the steam generators which may affect heat removal for small breaks.

Makeup water to the tanks is provided by opening a manual valve when the level in the tanks falls due to valve leakage and testing of the HP injection valves.

The ECC water tanks and the associated auxiliary circuit components are located in a separate HP ECC accumulator building outside the reactor building.

7.2 ECC Gas Tank

Pressurized gas stored in the ECC gas tank is used to inject the water in the ECC water tanks into the HT circuit following a LOCA.

The vessel consists of a horizontal cylindrical tank with hemispherical ends. The material is unlined carbon steel. During the HP stage of ECC injection, the gas depressurizes to 848 kPa(g) when the ECC water tanks are emptied.

Makeup for valve leakage is provided from an air compressor and air dryer which are backed up by a compressed nitrogen supply via a pressure regulating valve to maintain the tank pressure at or above 4.14 MPa(g).

7.3 Heat Exchangers

During long term ECC operation, two 100% plate type heat exchangers are provided to cool the mixture of H_2O and D_2O which is recovered from the reactor building basement.

The plate material is stainless steel. During normal operation of the reactor, both sides of the heat exchanger are filled with stagnant water. The water on the process side is circulated periodically during testing of the emergency core cooling pumps and during chemical addition.

The cooling water side of the heat exchanger is provided with water from the Recirculated Cooling Water System at a flow rate of 606 litres/s. This is backed up for long term reliability by the Emergency Water Supply System which also caters to cooling after an SDE.

7.4 ECC Pumps

Two x 100% vertical turbine type pumps with enclosed inlets are provided. The pumps are rated at 606 litres/s, 70.1 m head. They are motor driven and supplied from the Class IV or Class III power supply and from the Emergency Power Supply System for long term reliability.

Temperature detectors are incorporated to provide thermal indication for the bearings, the seal and the motor windings. Thrust will be taken by the bearings in the motor. The pump and motor operate without an external cooling water supply.

7.5 ECC Pump Suction Strainers

Strainers located above each ECC pump suction intake in the reactor building basement prevent foreign objects from entering the system. These strainers are constructed of stainless steel sheet with 3.2 mm (0.125 in) diameter perforations. The ratio of flow area to total area is approximately 0.4.

7.6 Valves

7.7 General

All nuclear valves conform to the requirements of Section III of the ASME Boiler and Pressure Vessel Code. All non-nuclear valves conform to the requirements of B31.1 of the USAS Power Piping Code. They are rated at the ANSI value appropriate to their respective service conditions.

7.8 Power Operated Valves

Butterfly valves, with a ring type seal, are used for the low pressure part of the Emergency Core Cooling System which contains light water. Gate valves are used for those high pressure portions containing heavy water or light water.

All large low pressure valves in the light water system are flanged for ease of maintenance, while all high pressure valves and all heavy water valves are welded in order to minimize leakage.

Redundant valves in parallel are provided wherever power operated valves are required to open for emergency core cooling operation. The valves on cooling water lines to the heat exchangers are similarly duplicated. The opening of any one of the redundant valves provides sufficient flow.

7.9 Check Valves

The ECC check valves are located in normally stagnant lines, and hence require test mechanisms to ensure that they are free to open. The test mechanisms are designed such that they do not impair the check valves ability to open or close like a normal check valve.

Testing to demonstrate the availability of testable swing check valves consists of stroking each valve using the test mechanism, to ensure that it is free to open. During this test the check valve's ability to open on a positive forward differential is not impaired and hence the effectiveness of the ECC system is not diminished.

The ECC system utilizes three unique testable swing check valve design as follows:

- Check valves installed on the common ECC pump discharge line are wafer swing check valves, each fitted with a manual chain wheel for testing purposes. The check valves prevent the draining of piping downstream of the ECC pumps on the event of a pump trip during low pressure ECC operation.
- H_2O check valves are swing check valves, each provided with a manual lever for testing purposes.
- D_2O check valves installed in the ECC injection line to each loop at each end of the reactor, are swing check valves which are fitted with either a manual lever or a remote manually controlled air actuator, depending on supplier's valve design. These valves isolate the HT system from the rest of the ECC system during the testing of the D_2O isolating valves. They also prevent the intact loop from blowing down to the broken loop during ECC operation.

7.10 Relief Valves

Relief valves are provided for the protection of ECC equipment and piping. For further information see Section 8, overpressure protection.

7.11 Restriction Orifices

Restriction orifices are provided on the ECC injection lines to the reactor outlet headers. Their purpose is to improve fuel cooling following a large reactor outlet header break by reducing the ECC flow to the reactor outlet headers and increasing the flow to the reactor inlet headers.

7.12 Rupture Discs

Rupture discs are provided on the ECC system to separate the part of the system which is filled with D2O from the part of the system filled with water. They prevent downgrading during the testing of the D_2O check valves.

7.13 Compressed Gas Supply

An air compressor and a dryer capable of delivering dry compressed air at 6.9 MPa(g) at a rated flow of 43 Std m^3/h is provided for the initial fill up of the ECC gas tank and for maintaining the tank operating pressure of 4.14 MPa(g).

The air compressor is sized to pressurize the gas tank initially in a maximum of 5 days. The air compressor controls the ECC gas tank pressure using an automatically controlling circuit within the range of 4.14 MPa(g) to 4.36 MPa(g). This supplies makeup due to leakage via the gas isolation valves and the gas supply valves. This air supply is backed up by a compressed gas supply from nitrogen cylinders if the air compressor is unavailable due to repair. A supply manifold has been provided so that four cylinder bottles can be connected to the ECC gas tank to minimize maintenance by operators.

8 Overpressure Protection

Protection against overpressure of components in the ECC system is provided as described below:

a Emergency Core Cooling Pumps

Each of the Emergency Core Cooling pumps can be isolated for maintenance by closing its maintenance valve and the associated valve in the pump recirculation line. Accidental operation of any pump under these conditions is protected by spring actuated relief valves set at 1.65 MPa(g). The design pressure of the pumps and adjacent system is 1.72 MPa(g).

b Heat Exchangers

The primary sides of the heat exchangers can be isolated for maintenance by closing the upstream and downstream isolation valves. Protection from overpressure is provided by spring actuated relief valves, which are set at 1.65-MPa(g).

The design pressure of the heat exchangers and adjacent portions of the ECC system is 1.72 MPa(g). The design pressure of the RCW system is 1.03 MPa(g).

c ECC Water Tanks

Overpressure protection of TK1 or TK3, in the event of failure of the pressure regulating valve in the nitrogen purge gas line to the tanks with either one of the vent valves closed, is provided by a spring actuated relief valve which is set at 6.2 MPa(g). The design pressure of TK1 and TK3 and adjacent system and equipment is 6.2 MPa(g).

d ECC Water Tank Heater

The water tank heater is normally connected to the water tanks, however it can be isolated for maintenance by closing manual maintenance valves. Overpressure protection of the heater if it is accidentally turned on while isolated is provided by a spring actuated relief valve which is set at 6.2 MPa(g). The design pressure of the heater is 6.2MPa(g).

e ECC Gas Tank

The gas tank is normally isolated and contains gas at 4.14 MPa(g). Its

overpressure protection in the event of failure of the pressure regulating valve or the air compressor pressure control for gas makeup is provided by a spring actuated relief valve which is set at 6.2 MPa(g). The design pressure of gas tank and adjacent system is 6.2MPa(g).

9 Waterhammer Pressure Transients

Because of long length of the ECC piping and the requirement of the ECC system to develop large flows from rest or bring large flows to rest quickly, waterhammer pressure transients must be taken into design considerations. Based on CANDU design experience, there are five instances during the operation of the ECC system when considerable waterhammer pressure transients could occur:

- following ECC initiation,
- following closure of the accumulator discharge valves,
- following restart of the ECC pump after tripping during short term low pressure injection or long-term recirculation operation,
- following spurious injection or initiation without injection,
- during testing of gas isolation valves.

The nature and effects of the waterhammer pressure transients are analyzed and adequate provisions are made in the design to protect the system components against the waterhammer forces. The following general principles are employed in the design and layout of the ECC system to minimize waterhammer pressure transients.

9.1 Pressurization Rate of the Accumulator Water Tanks

The severity of pressure transient increases with an increase in the rate of the pressurization of the accumulator water tanks. The rate of pressurization in turn is proportional to the size and the opening time of the gas isolation valves. The opening time is made as slow as possible to minimize pressure transients, without impacting on the fuel cooling performance requirements.

9.2 Closing of the HP Injection Valves

Simultaneous closing of the HP injection valves at the end of short-term high-pressure injection may result in severe pressure transient behaviour in the piping upstream of the valves. The closing of these valves are staggered, if required, to reduce pressure transient behaviour to acceptable levels. Again closing of these valves are made as slow as possible to minimize pressure transients, without risking gas injection into the HT system.

9.3 Presence of Air or Voids in the System

The piping layout is designed to minimize the possibility of air being trapped in the system. Provisions are made to ensure that the system is full during initial

fill or any subsequent refill. Also the changes in elevation between isolated sections of piping is kept below 10 m to avoid draindown and hence void formation during system depressurization.

In the unlikely event that air is trapped in the piping, the relatively slow pressurization rate of the accumulator water tanks is generally expected to keep the pressure transient due to the compression of the air pocket within acceptable levels.

10 Interface with Other Systems

10.1 Support Systems

A number of support systems are required to function for the successful operation of the ECC system over the HP, MP and long-term LP stages. These include power systems, water systems and instrument air system. Capability to withstand an SDE after 24 hours, as well as the meeting of the unavailability target, requires special support from the emergency power supply (EPS) system and the emergency water supply (EWS) system.

10.1.1 Power Systems

The power systems serving the ECC system comprise Class IV, Class III, Class II, Class I electrical power and the EPS system.

Each ECC pump is supplied from an independent Class III power bus (as either ODD or EVEN) and backed up with a connection from the EPS system. Within each pair of valves, one valve is supplied from ODD power and the other from an independent EVEN power system. Sufficient number of valves are also backed up the EPS system in order to supply makeup water to the HT system following a DBE.

a. Class IV Electrical Power

For purposes of design, ECC operation does not rely solely on Class IV electrical power. However, the HT pumps are powered only with Class IV power. For purposes of analysis and reliability calculations, Class IV power is credited to the extent of its availability.

b. Class III Electrical Power

Class III electrical power is sufficient to power the ECC systems. The demand for Class III power will occur at 2.5 minutes or later after a LOCA (2.5 minutes is the minimum time to empty the accumulator water tanks). Should Class IV power fail when the ECC pumps are required (in their first hour of operation) Class III power will restart an ECC pump in a maximum of 40 seconds.

To meet the requirement of carrying the ECC pumps after 2.5 minutes, the moderator main motor is not a sequenced load (the moderator pony motors are powered by Class III power). To meet the requirement of restarting the ECC

pumps within 40 seconds of a Class IV power failure, the Class III diesels are started on a LOCA signal.

c. Class I and II Electrical Power

Class I and II electrical power are sufficient to respond to all ECC power demands that are required before the Class III generator can be started and loaded. The loads on Class I and Class II power are all electrical driven ECC injection valves, all electrically driven loop isolation valves, and all necessary instrumentation.

d. Emergency Power Supply (EPS) System

Because long-term ECC must be able to withstand a postulated SDE event 24 hours after a LOCA, the EPS system is capable of operating the ECC pumps. All necessary control systems for the use of EPS are in a DBE qualified area with remote manual control. Since ECC piping could have high radioactive fields, local manual control is not generally relied upon.

An exception to this is the manual operation of the ECC pump transfer switches. This could be necessitated if EPS is required 24 hours or later after a LOCA, when a SDE that results in the failure of normal power systems could occur. The operator is then required to transfer power to the ECC pumps from the field (S/B basement). Radiation dose to the operator under these conditions is within permissible values.

Because the D_2O make-up and recovery system is not totally DBE qualified, normal D_2O makeup following a DBE event may not be available. Hence, EPS power is provided for all valves necessary to bring the EWS water to each reactor loop via the ECC system.

10.1.2 Water Systems

The water systems comprise: Raw Service Water (RSW), Recirculating Cooling Water (RCW), Steam Generator Feed Water and Emergency Water Supply (EWS) systems.

a. Raw Service Water (RSW)

RSW is needed to cool the Recirculating Cooling Water.

b. Recirculating Cooling Water (RCW)

RCW is needed to supply cooling water to the ECC heat exchangers.

c. Steam Generator Feedwater (Main and Auxiliary System)

Feedwater to the steam generators is required for the continued cooling of the steam generators for long-term cooling. Following the detection of feedwater failure, EWS water can be made available after 30 minutes.

d. Emergency Water Supply (EWS) System

EWS is capable of providing adequate cooling water to the ECC heat exchanger should a SDE event occur 24 hours after a LOCA. All control systems required are remote manual from a separate seismically qualified secondary control area (SCA).

EWS is credited with the capability of providing makeup for the steam generators 30 minutes after the loss of other feedwater sources.

e. Demineralized Water System

A connection to the demineralized water system is provided for the initial fill of the ECC system and make-up when the level in the tanks falls due to valve leakage and due to testing of the HP injection valves. Another connection to this system permits initial filling of the dousing tank.

10.1.3 Instrument Air System

Compressed instrument air is used mainly as a driving force for the ECC pneumatic valve actuators in the ECC system. In the event of a loss of Class IV power the instrument air compressors operation is temporarily interrupted until Class III power is restored to them. To cater for such events, the dousing tank suction valves have back up air tanks to enable them to remain open in the MP injection phase. This provision is made in addition to the air reservoirs in the turbine building, which are capable of supplying instrument air to all of the valves in the service building. Therefore, the MP ECC continues to function despite the loss of Class IV power.

10.2 Process Systems

a. Dousing System

Dousing System provides a minimum of 500 m^3 of water for medium pressure ECC operation by reserving this volume in the bottom of the dousing tank (not available for dousing).

b. Fuelling Machine D2O Supply System and Pressure and Inventory Control System

Connection to these systems provide a means of adding makeup D_2O to the interspaces between the rupture discs and the D_2O check valves.

c. Active Drainage System

Active Drainage System is connected to the ECC system through all ECC vent pipings. It also provides leakage collection of the ECC equipment in the service building, and return such leakage back into containment.

d. Service Building Central Contaminated Exhaust System

Service Building Central Contaminated Exhaust System provides collection and controlled discharge of potentially radioactive gaseous leakage in the ECC enclosures in the services building.

e. D_2O Collection System

A connection is provided for D_2O collection from appropriate vents and drains of ECC system to the D_2O Collection System.

f. Shutdown Cooling System and Heat Transport System

The ECC system injects into the HT system via shutdown cooling system piping.

Candu Shutdown Systems

Training Objectives

On completion of this lesson the participant will be able to:

- state the three reactor safety principles.
- describe the terms single failure and dual failure.
- describe why there are two separate independent shutdown systems on a CANDU unit.
- describe the two shutdown systems.
- state what the design capability objective is for each shutdown system.
- describe the system design philosophy (independent, diverse and fully effective SDS).
- describe separation and grouping of the safety support and process systems.
- describe the relationship between Design Basis Initiating Events and Trip Parameters.
- state that the design basis for protective coverage is at least two independent trip parameters for each situation.
- briefly explain trip coverage maps.
- list trip set points and describe what conditioning of these means.
- state that the designed reactivity insertion rate is based on the incident that results in the fastest addition of reactivity which is a LOCA from a maximum reactor inlet header break.
- state that the design reactivity depth is required to maintain the reactor shutdown. This is dictated by an in-core LOCA, 40 mk needed.
- list the interlocks between systems SDS1, SDS2 moderator, regulating systems.
- state the effect of potential interaction between shutdown systems and the purpose of the power rundown discriminator.
- state the advantages and disadvantages of a fully computerized system over a non-computerized system (or partially computerized).

Table of Contents

1 Introduction

1.1 General

In the Canadian approach to reactor safety, the systems in the plant are categorized as either process or special safety systems. Process systems are those required for normal operation, and the special safety systems are those provided to limit any release of radioactivity that may follow failures in the process systems. Examples are:

Process Systems	Special Safety Systems
Heat Transport	Shutdown #1 (SDS-1)
Reactor Regulating	Shutdown #2 (SDS-2)
Electrical Power	Emergency Core Cooling (ECC)
Turbine	Containment

Shutdown systems number 1 and 2 (SDS-1 and SDS-2) are two of the special safety systems that limit radioactive release to the public by quickly making the reactor subcritical to shut it down. SDS-1, using mechanical neutron-absorbing shut off rods, is the preferred system for shutdown, over SDS-2 which uses liquid poison injection into the moderator. This preference is an economic factor resulting from plant unavailability following the use of SDS-2, due to the inability to quickly remove the poison from the moderator following an SDS-2 trip.

Both SDS-1 and SDS-2 use an independent triplicated logic system to sense plant measurements and evaluate the conditions for a shutdown system trip. Two-out-of-three logic is used to minimize spurious trips and allows on-line testing without tripping the shutdown systems.

1.2 The Canadian Approach to Safety

The Atomic Energy Control Board (AECB) in Canada sets the requirements that must be met by operating nuclear power plants. For normal operation, the AECB has used International Commission on Radiological Protection (ICRP)recommendations for maximum acceptable dose limits for the public. For accident conditions the AECB specifies does limits for single and dual failures. A single failure is a serious process system failure that can potentially lead to radioactive releases. A dual failure is a single process failure coincident with unavailability of a special safety system.

The dose limits chosen by the AECB for accident conditions result in decreasing risk to the public for low frequency, high consequence events. The risk is proportional to the frequency of event times the consequence (or dose limit). The release limits for a single failure are the same as the yearly limits for normal operation, but the frequency of single failures is lower than once per year and thus risk is lower. Similarly, dual failures have a lower risk than single failures.

In addition, general guidelines are published periodically by the AECB dealing with the release and monitoring of radioactivity during normal operation and following accidents. The guidelines also cover the design of the special safety systems with respect to their reliability, testability and independence. From these reference dose limits and guidelines, the designers establish derived criteria and design requirements for the special safety systems.

The limits of radiation dose to the public for the single and dual failures are shown in the table below:

AECB Guidelines for Accident Conditions

Situation	Maximum Frequency	Individual Dose Limit	Total Population Dose Limit
Single Failure	1 per 3 years	5 mSv whole body	10^3 man-Sv whole body
		0.3 Sv thyroid	10^4 man-Sv thyroid
Dual Failure	1 per 3000 years	0.25 Sv whole body	10^5 man-Sv whole body
		2.5 Sv thyroid	10^5 man-Sv thyroid

In addition to the dose limits, the AECB siting guidelines state two requirements of the special safety systems which are basic to the risk frequency approach:

- The special safety systems must be independent of the process systems and independent of each other. The single and dual failure approach is not valid, for instance, if a special safety system failure occurs as a consequence of the initial process failure.
- Each special safety system must have a demonstrated availability greater than 0.999. This means that each safety system must be available to function properly not less than 99.9% of the time.

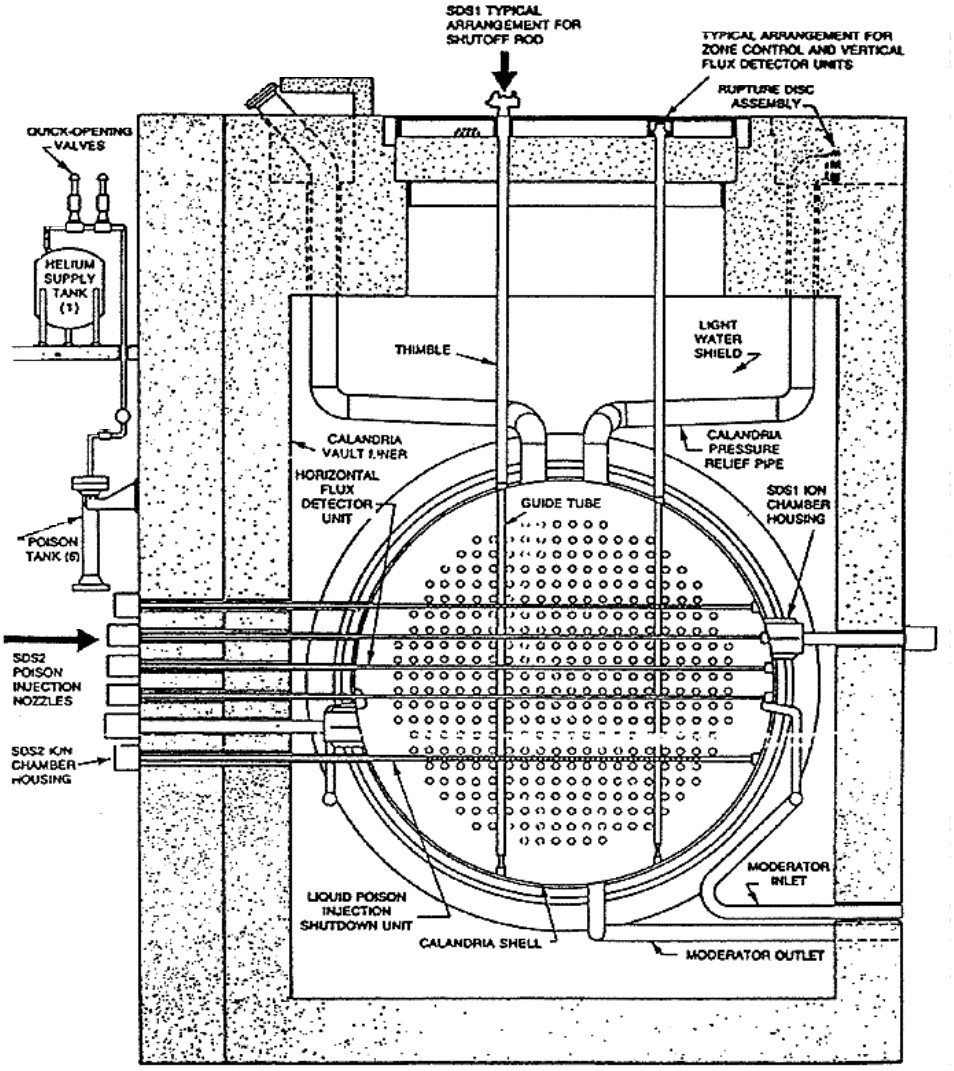
1.3 Use of Two Shutdown Systems In CANDU Reactors

CANDU reactors employ the use of two independent, diverse and equally effective shutdown systems. One benefit of this is that the design of special safety systems and safety analysis for dual failures can always assume shutdown system action occurs.

Shutdown system diversity is an important feature of CANDU design. Special effort is made to design SDS-1 and SDS-2 to perform equally well, but using different design factors such as principles of operation, location and orientation of equipment, suppliers of components and designers. The principle of diversity provides protection against undetected deficiencies in design, manufacturing and construction and against common mode failures.

The diversity between the design of SDS-1 and SDS-2 is most evident when looking at the shutdown principle (see Figure 1). SDS-1 uses solid rods, dropping from the top of the core under the force of gravity whereas SDS-2 injects liquid poison by use of high pressure helium into the side of the core.

Figure 1
General layout of SDS1 and SDS2



2 Design Philosophy

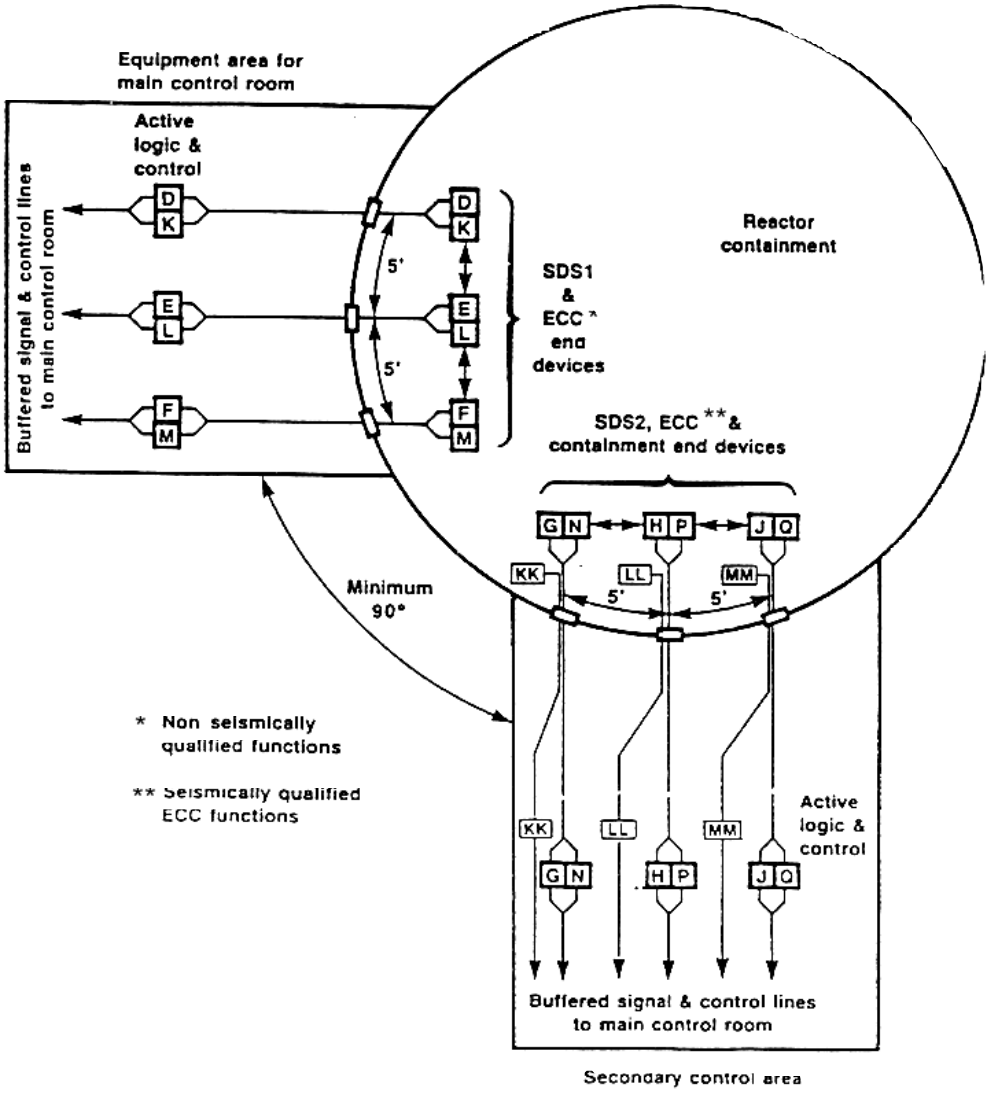
Various design concepts are employed to ensure that the shutdown systems operate when required, with high reliability. These concepts include redundancy, application of independence principles, qualification of equipment for accident conditions, continued monitoring and testing of equipment, and robustness in design.

2.1 Independence

Independence principles are designed into the special safety systems, both within each system and between the four special safety systems. A two-group philosophy is used to maintain physical separation between the special safety systems. SDS-1 and non-seismically qualified portions of ECC are part of group one. SDS-2, containment and seismically qualified portions of ECC are part of

group two. Separation is maintained between the redundant channels, within each special safety system. Figure 2 illustrates the separation between groups and channels for the special safety systems.

Figure 2
Location and Separation Requirements for safety related systems



The design philosophy being applied to the two shutdown systems is to keep them functionally and geometrically independent of each other and functionally independent of the Regulating Systems.

Functional independence is lack of commonality in physical principle of operation, design, construction or in sharing of devices. Where possible, all of these properties of functional independence are used.

The functional independence of the shutdown systems is basically achieved by the adoption of two different shutdown principles; metallic shutoff rod drop for the first shutdown system and direct liquid poison injection into the moderator for the second shutdown system. Where the function performed is identical (e.g. use of a pressure transmitter or flux detector, etc.), separate devices are used for each shutdown system and for the regulating system.

The geometric independence of the shutdown systems is basically achieved by having the shutoff rods inserted vertically in the top of the reactor and the poison injection tubes inserted horizontally in the side of the reactor. Ancillary mechanical and process equipment is similarly kept apart. The shutoff rod drives are above the reactor whereas the poison supply system is to the side of the reactor. The measurement elements of the two shutdown systems are geometrically separated. The active elements of the SDS1 are located in the control equipment room of the control centre, with the readout devices, manual trip buttons and the trip test facilities located in one main control panel reserved solely for the system. The active elements of the poison injection trip system together with the readout devices and manual trip buttons are located in the secondary control area (SCA) remote from the main control centre. Readout devices for trip parameters, a trip button and the trip test facilities for both shutdown systems are located on separate control panels in the main control room, reserved solely for that system.

Excluding the manual trip buttons and trip test facilities, there are no active elements of the SDS2 located in the main control centre. All signals to the main control room panel are isolated by buffering. Any possible common mode faults crosslinking poison injection channel elements to each other or to elements of any other system in the main control room, cannot affect the active automatic tripping elements of the system.

Emphasis has been placed on the independence between the two groups (consisting of both safety and process systems), and retaining separation between channels of systems. The same three channelized routes, however, are used for all systems in a group, by coupling similar channels of each system into one routing (see Figure 2). Except for this common routing, all other aspects of independence between safety and process systems are followed.
Each process and nuclear measurement loop essential for the operation of a special safety system is triplicated so that a single loop component or power supply failure will not incapacitate or spuriously invoke the operation of the special safety systems. The design approach emphasizes isolation between loops of different channels and between the different special safety systems. This is achieved by the use of separate transmitter mounting racks, electrical cubicles and power supplies for each channel.

The design aim is that the instrumentation, logic and mechanical components for each trip parameter path be testable right from the primary transducer to the final reactivity devices.

Both shutdown systems are environmentally qualified. Accident analysis is performed to determine the limiting environmental conditions in terms of maximum temperature, pressure, radiation dose and humidity. For shutdown systems, the time to operate under harsh environment conditions is relatively short. Once the shutdown system trips, there is no need for the instrumentation to continue operating and it is only necessary to be qualified for the period of time until the trip occurs. Environmental qualification involves type tests on the critical equipment exposed to harsh environments which simulate the limiting conditions. Some of the shutdown system equipment is qualified for longer periods to supplement post accident monitoring; however this enhancement is not necessary for the shutdown function.

2.2 Qualification

The principle of equipment qualification is used in the design of the shutdown systems to ensure that any accident requiring shutdown system action, does not adversely affect the SDS equipment needed to provide this protection. The two areas of special qualification necessary are for vibration due to seismic incidents and harsh environment due to a loss of coolant from the primary or secondary heat transport systems. The SDS equipment is also qualified for the worst conditions expected under normal operation, not necessarily related to a particular accident (e.g. electromagnetic interference).

Both shutdown systems are seismically qualified to operate during or after a design basis earthquake. Seismic qualification is achieved through equipment hardening and shake testing at the seismic response levels for the equipment location. Seismic qualification also involves locating equipment in protected areas or those not affected by failure of non-seismic systems (e.g. heavy equipment falling after a seismic incident).

2.3 Reliability

Each shutdown system has a requirement to be available 99.9% of the time that the station is operating. This number is specified to be consistent with the dual failure frequency limit. For example, the maximum probability of a shutdown system failure is 1-0.999 = 0.001. The maximum frequency of serious process system failure (single failure) is 1 per 3 years. The maximum frequency for dual failure is thus 1/3 x 0.001 or 1 per 3000 years, as specified in Section 1.2. Note that this is only valid because the process system and shutdown systems are independent as previously discussed.

The availability target is normally evaluated in terms of unavailability, which is defined as the ratio of the time the shutdown system is unavailable to the time that the reactor is in operation. This is more conducive to evaluation, using fault tree analysis and failure rate data. The unavailability limit is thus 10-3 years per year. For the shutdown systems, this limit applies to the sensing instrumentation of each trip parameter individually, combined with the trip logic and mechanical components.

The following describe the method of analysis of unavailability and the basic assumptions used:

- Generally component failures are assumed to occur randomly and independently of each other. The calculations also account for any foreseen cross-linked or common mode component failures. The shutdown systems have been designed with a view to eliminating all interdependence of components and failure modes, to minimize cross-linked failures.
- Based on the above assumption, component unavailability for passive equipment, tested routinely, is calculated using the relationship

  $$\text{unavailability} = \frac{\text{Unsafe Failure Rate} \times \text{Test Interval}}{2}$$

  This expresses the ratio of average time the component remains in the unsafe failed state (which is approximately half the test interval) to the average time between failures (which is the inverse of the failure rate), resulting in the average unavailability of the component. The relationship is an approximation, becoming valid when the test interval is much smaller than the mean time between failures. When an unsafe failure is detected during testing, the trip channel is placed in the safe (tripped) state.
- Component failure rates selected are based on past experience; test intervals are chosen so that the targets discussed above will be met. If demonstrated failure rates vary from those assumed, the test intervals are adjusted accordingly.
- Component unavailabilities are combined, using standard probability theory, to determine overall system unavailability.

One of the design features that significantly contributes to the high shutdown system availability, is the use of redundant, independent, triplicated channels to measure trip variables. With two-out-of-three channel logic to cause a trip, on-power testing is possible without having to trip the reactor. The capability to continually test after short periods of time, increases reliability by reducing the time that faults are undetected. The redundancy in trip variable measurement also increases availability since failure of any one channel does not disable the trip. Coincident unsafe failure of any two channels would disable the trip, but this has a very low probability since the channels are independent.

2.3.1 Monitoring and Testing

Each part of the shutdown systems has a test facility. These facilities are designed to test the parts of the trip logic in an overlapping manner, right from the sensing elements to the end mechanical components of the shutdown system. For example, when testing the primary heat transport high pressure trip, a test pressure signal would be valved into the sensing line of the pressure transmitter. The operator can then raise the test pressure until a channel trip occurs. In this way the entire system is proved to operate as designed. Testing frequencies are established on the basis of meeting the target unavailability (10^{-3}).

A shutdown system computerized monitoring facility is also employed on some CANDU reactors to detect early signs of failure as well as aid the operator in maintaining adequate operating margins to avoid spurious trips. The monitoring facility takes advantage of the redundant channels by detecting differences to identify faulty measurements. By use of isolation techniques the independence between channels is maintained, even though the computer obtains information from all channels.

2.4 Robustness of Design

For the shutdown systems, design robustness can be defined as a measure of capability to protect against the consequences of design basis events to a maximum extent with minimum complexity. One of the main elements of robust design, is the choice of trip parameters. This area of design is a significant factor in providing protection for all credible process failures. The concept of providing protection is termed trip coverage.

The number of shutdown system trip parameters has a large impact on station operation. The more parameters, the more testing required, which uses up operators time and also increases chances of a spurious trip since one channel is normally tripped during a test. The number of parameters by itself will increase the spurious trip frequency due to the cumulative effect of random failure. Efforts for robust design are made by minimizing the number of trip parameters within the constraint of providing adequate trip coverage.

The general principles employed to achieve a robust design, are to choose trip parameters which are relatively direct in relation to the safety factor being protected. Direct parameters are then evaluated for direct or indirect protection against other safety concerns (other process failures). By balancing the various parameters in their span of trip coverage, a minimum set is obtained and thus constitutes a robust design.

An example of trip parameter selection leading to robust design is as follows. A loss of grid power requires a reactor shutdown because this results in a loss of coolant flow due to the loss of heat transport pumps. If the stepback feature in the reactor control system fails to reduce power, a shutdown system trip is required. The two main safety concerns are fuel melting due to loss of flow and high heat transport pressure due to boiling of the coolant. When considering the second safety concern, an example of a non-robust trip parameter would be to trip on low grid voltage. Although this particular incident would be protected by this trip, a more robust parameter being directly related to the high pressure safety concern is high heat transport system pressure (HT-HP). This parameter also protects against the fuel melting in this case, as well as most incidents resulting in an imbalance between primary power produced and power removed such as loss of secondary heat sink or loss of regulation incidents. The HT-HP trip is thus a robust trip parameter.

3 Design Requirements

3.1 Functional Capability Requirements

The ultimate target for the shutdown systems is to meet the Regulatory guidelines specified in Section 1.2. To meet these targets, derived criteria are established by evaluation of the possible mechanisms leading to radioactive releases. Functional capability requirements are then specified to dictate what the shutdown systems must do to meet the derived criteria.

The derived criteria are that each shutdown system, acting alone to shutdown the reactor, shall be capable of:

- Maintaining the primary heat transport system intact by preventing failures due to overpressure, excessive fuel temperature, or fuel breakup.
- Maintaining containment intact by limiting both the rate of energy production and the total energy production.
- Maintaining the reactor in a suitable sub-critical state for a period sufficient to permit the shutdown system to be supplemented reliably.

Design objectives are obtained by considering which mechanisms may lead to violation of the derived criteria and by setting conservative objectives to meet the criteria. The considerations are expressed in terms of design basis initiating events. The major classes of design basis initiating events are:

a. loss of regulation (LOR)
b. loss of coolant accident (LOCA)
c. loss of coolant flow (loss of Class IV power)
d. loss of secondary heat sinks

3.1.1 Design Basis Protective Coverage

The design objective for each initiating event postulated is selected to ensure that the release limits are met, and is variously to avoid fuel dryout, sheath embrittlement, or centreline melting.

3.1.1.1 Loss of Regulation (LOR)

The derived criterion for loss-of-regulation events is prevention of pressure tube rupture. In order to ensure no pressure tube rupture, the design objective has been conservatively chosen as prevention of fuel element centreline melting.

Fuel element centreline melting can occur in two ways:

- A local power peak, producing outer element ratings of more than 70 W/cm may melt the fuel at the centre, even with normal heat transfer from fuel coolant.
- Increasing channel power beyond "fuel dryout" would cause the heat transfer to decrease and fuel temperature to rise. At some power level, above onset of dryout, the centre of the fuel element begins to melt. Though conservative, the design objective is to initiate shutdown before the onset of the fuel dryout, which is more limiting than objective (i), for CANDU reactors.

3.1.1.2 Loss of Coolant

The design objective for loss-of-coolant accidents is to maintain the integrity of the heat transport system (HTS) (except, of course, for the point of postulated failure).

To meet this objective it is sufficient to prevent fuel breakup for large breaks, to avoid sheath embrittlement (and dryout where practicable) for small breaks, and to maintain a coolable geometry in the long term.

3.1.1.3 Loss of Flow (Loss of Class IV Power)

The derived criterion for loss-of-flow accidents is prevention of pressure tube rupture. This may result from prolonged operation beyond the onset of fuel element centreline melting. The design objective is to prevent the onset of centreline melting. (Loss of Class IV power causes the HT pumps to trip and results in a loss of flow event).

A second derived criterion is prevention of primary heat transport system rupture due to overpressure following loss of flow. The design objective for safety system design chosen to satisfy that criterion is that SDS-1 prevent pressure excursions from exceeding 110% of design pressure and that SDS-2 prevent pressure excursions exceeding 120% of design pressure.

3.1.1.4 Loss of Secondary Steam Generator Inventory Heat Sinks

The secondary heat sink is provided by the steam generator light water system. Its loss is not a serious process failure in the traditional sense, however the consequences can lead to overpressurization of the heat transport system, and eventually a serious process failure if the Reactor Regulating System also fails. The requirement for the shutdown systems is to initiate a shutdown such that there is adequate time for the operator to provide an alternative heat sink and ensure primary system integrity.

Where an alternate heat sink of sufficient availability can be brought on line from the main control room, 15 minutes of post-shutdown inventory in the steam generators is required to allow the operator to act. Where operator action outside the control room is required, 30 minutes of inventory is the design target.

3.1.2 Trip Parameters

The selection of parameters is such that there are adequate measurements for all process failures identified. The regulatory requirements specify that all process failures must have one trip parameter and a back-up trip parameter on each shutdown system whenever practically possible.

Typical trip parameters and protective coverage are summarized in Tables 1 and 2. Setpoints are shown in tables 3 and 4. The credited protective coverage for each of these trips is outlined below. Document R8 referenced in Section 3.2.3 sets the requirement for two diverse trip parameters on each shutdown system for each event.

3.1.2.1 Regional Overpower Trip

The Regional Overpower (ROP) trip, which is sometimes also known as the Neutron Overpower (NOP) Trip, is designed to give protection against the following:

- loss of regulation accidents or localized power peaking which result in excessive overheating of the fuel

  In addition to considering loss of regulation accidents from the nominal full power flux shape, normal and perturbed flux shapes considered to be credible operating conditions are also covered. These perturbed shapes are typically as follows:
  - single zone control compartments drained,
  - flux tilts, whether due to an absence of spatial control or driven by zone controllers draining or filling,
  - control absorbers inserted in their normal sequence,
  - adjusters withdrawn in their normal sequence, whether for reactivity shim or xenon override during a stepback or setback,
  - adjusted startup

This trip is based on self-powered in-core flux detector measurements and is of special interest. It is discussed in greater detail in Appendix A.

- LOCA
  The overpower trip provides a quickly responding trip signal for large loss of coolant accidents where the induced void reactivity rate or depth exceeds the capability of the reactor regulating system to maintain power constant.

3.1.2.2 High Rate of Log Neutron Power Trip

The high rate log power trip is based on out-of-core ion chamber measurements, and designed to give protection against the following:

- loss of regulation from low power with the heat transport system pressurized or depressurized
- large LOCA

For a large LOCA, the induced void reactivity rate and depth exceed the capability of the reactor regulating system to maintain constant power, causing rapid increase in power. The high rate of log neutron power trip responds quickly to the increase.

3.1.2.3 Heat Transport System High Pressure Trip

This trip is designed to give protection against the following upsets:

- Loss of Class IV Power (loss of heat sink through loss of circulation)
- loss of regulation (power exceeds heat sink capacity)
- loss of secondary heat sink

3.1.2.4 Heat Transport System Low Pressure Trip

This trip is designed to provide protection against the following:

- very small loss of primary coolant accidents,
- small loss of primary coolant accidents where the reactor regulating system is capable of maintaining power constant.

It also provides limited backup coverage for very large main steam line breaks outside containment.

To allow for heat transport system maintenance, this trip is conditioned out at very low power.

This conditioning also makes the trip act as an overpower trip when the HTS is depressurized, whether or not the HTS pumps are running.

3.1.2.5 Heat Transport System Coolant Low Flow Trip

The coolant low flow trip is designed to give protection against the following:

- Loss of Class IV Power (through loss of circulation)
- loss of regulation from decay power levels when the HTS pumps are stopped, but the HTS is pressurized. The trip occurs because of the automatic low power conditioning described below.

To allow for shutdown and maintenance, this trip is conditioned on the log power signal from the SDS ion chambers.

This conditioning also makes the trip act as an overpower trip when the HTS pumps are stopped, and thus provides LOR trip coverage from decay power levels with the pumps stopped.

Table 1

Typical Trip Parameters for Shutdown Systems SDS1 and SDS2

	SDS-1	SDS-2	Detector Type
Neutron Over Power (NOP)	x	x	Self-powered in-core flux detectors
High Rate of Log Neutron Power (HRLOG)	x	x	Ion chambers
Primary Heat Transport High Pressure (PHT-HP)	x	x	Pressure Transmitters
*Primary Heat Transport Low Pressure (PHT-LP)	x	x	Pressure Transmitters
*Primary Heat Transport Low Gross Coolant Flow (PHT-LF)	x		Differential Pressure Transmitters
*Low Reactor Core Differential Pressure (LDP)		x	Differential Pressure Tranmitters
Reactor Building High Pressure (RB-HP)	x	x	Pressure Transmitters
*Pressurizer Low Level (P-LL)	x	x	Differential Pressure Transmitters
* Steam Genrator Low Level (SG-LL)	x	x	Differential Pressure Transmitters
*Boiler Feedline Low Pressure (BF-LP)	x	x	Pressure Transmitters
Manual (MAN)	x	x	-----

Note: * Trip parameter is disabled at low power for operating reasons.

Table 2

Shutdown Systems Trip Parameters of Process Failures

Process Failure		SDS-1 Trip Parameters		SDS-2 Trip Parameters	
Event	Magnitude	Primary	Back-up	Primary	Back-up
Loss of Regulation from High Power	Fast Slow	HRLOG NOP	NOP/PHT-HP PHT-HP/MAN	HRLOG NOP	NOP/PHT-HP PHT-HP/MAN
Loss of Regulation from Decay Power (Pressurized/Pumps-on)	Fast Slow	HRLOG PHT-HP	PHT-HP NOP/MAN	HRLOG PHT-HP	PHT-HP NOP/MAN
(Pressurized/Pumps-off)	Fast Slow	HRLOG *PHT-LF	*PHT-LF PHT-HP/MAN	HRLOG *LDP	*LDP PHT-HP/MAN
(Depressurized/Pumps-on)	Fast Slow	HRLOG *PHT-LP	*PHT-LP MAN	HRLOG *PHT-LP	PHT-LP MAN
(Depressurized/Pumps-off)	Fast Slow	HRLOG *PHT-LF	*PHT-LF *PHT-LP/MAN	HRLOG *LDP	*LDP *PHT-LP/MAN
Loss of Class IV Power		PHT-LF	PHT-HP	LDP	PHT-HP
Loss of Coolant into Containment	Large Medium	HRLOG NOP	NOP/RB-HP RB-HP	HRLOG NOP	NOP/RB-HP RB-HP
(with Power Regulation)	Small	RB-HP	PHT-LP/P-LL	RB-HP	PHT-LP/P-LL
(with Power Regulation/Pressurizer Isolated)	Small	PHT-LP	RB-HP	PHT-LP	RB-HP
(without Power Regulation)	Small	RB-HP	NOP	RB-HP	NOP
(with Power Regulation)	Very Small	PHT-LP	P-LL/MAN	PHT-LP	P-LL/MAN
(with Power Regulation/Pressurizer Isolated)	Very Small	PHT-LP	MAN	PHT-LP	MAN
(without Power Regulation)	Very Small	NOP	MAN	NOP	MAN
Calandria (with Power Regulation)	All	PHT-LP	P-LL/MAN	PHT-LP	P-LL/MAN
(with Power Regulation /Pressurizer Isolated)	All	PHT-LP	MAN	PHT-LP	MAN
(without Power Regulation)	All	NOP	MAN	NOP	MAN
Steam Main Break with feed pumps on (inside containment)	All	RP-HP	SG-LL/BF-LP/MAN	RB-HP	SG-LL/BF-LP/MAN
(outside containement)	All	SG-LL	PHT-LP/BP-LP/MAN	SG-LL	PHT-LP/BF-LP/MAN
Steam Main Break with feed pumps off (inside containment)	All	RB-HP	BF-LP/SG-LL/MAN	RB-HP	BF-LP/SG-LL/MAN
(outside containment)	All	BF-LP	SG-LL/PHT-HP/MAN	BF-LP	SG-LL/PHT-HP/MAN
Feedline Break (Upstream of Check Valves)	All	BF-LP	SG-LL/BF-LP/MAN	BF-LP	SG-LL/PHT-HP/MAN
(Downstream of Check Valves)	All	RB-HP	SG-LL/BF-LP/ PHT-HP/MAN	RB-HP	SG-LL/BF-LP/PHT-HP/MAN
Loss of Feedwater Control (closure of valves to one steam generator)	-	SG-LL	PHT-HP/MAN	SG-LL	PHT-HP/MAN
Feedwater Pumps Trip	-	SG-LL	PHT-HP/BF-LP/MAN	SG-LL	PHT-HP/BF-LP/MAN

Table 3

SDS1 Trip Parameters (4 Pump Mode)

Trip Parameter	Detector Type	Setpoint	Conditioning Parameter	Hand-Switches
Log N Rate High	Ion chambers	10% per second	---	---
Neutron Power High	Vertical in-core	121.4% full power as a reference bulk power trip Setpoint +		(1)
Heat Transport Pressure High	Pressure Transmitters	a. 10.24 MPa(g) or b. 10.45 MPa(g)	a. Trip is conditioned out for initial powers below 70% FP, or if power drops belwo 70% FP within 3 seconds of exceeding the trip setpoint.	(2)
Heat Transport Pressure Low	Pressure Transmitters	Function of reactor power 8.7 MPa(g) (at full power)	1. Setpoint determined by ion chamber linear power signal. 2. Conditioned out by log power less than 0.1 percent of full power.	(2)
Heat Transport Flow Low	Pressure differential transmitters	a. 80% NICF* or b. 50% NICF	a. Trip is conditioned out for initial powers below 80% FP, or if power drops below 80% FP within 5 seconds of exceeding the trip setpoint. b. power less than 0.1% full power.	(2)
Pressurizer Level Low	Pressure differential transmitters	Function of reactor power (7.26 m at full power)***	1. Setpoint determined by reactor power signal from in-core flux detectors. 2. Conditioned out when reactor power less than 1% full power.	(2)
Boiler Level Low*	Pressure differential transmitters	Function of reactor power (+0.38 m at full power)	1. Setpoint determined by flux detector signals. 2. Conditioned out when reactor power less than 5% full power.	(2)
Boiler Feedline Low Pressure (BFLP)	Pressure transmitters	3.9 MPa(g)	Conditioned out for power less than 10% full power.	---
Moderator Temperature Trip	RTDs	87°C	None.	
Reactor Building Pressure High	Pressure transmitters	3.45 kPa(g)	---	---
PDC 1/2 Watchdog Trip	---	---	---	---
Manual	---	---	---	---

* Boiler level setpoints are given relative to the narrow range taps which are 13.48 m above the AECL datum.

*** Corresponds to a normal operating pressurizer level of 11.35m (0 is at lower tap).

\+ The operating trip setpoint is determined from the reference according to reactor conditions and licence limits.

*NICF: Nominal Instrumented Channel Flow

HANDSWITCHES

1. Neutron overpower trip setpoint selection:
   - nominal configuration
   - adjusted operation
   - two pump operation

2. Process trip setpoint selection:
   - four heat transport pumps
   - two heat transport pumps (P1 &P3)
   - two heat transport pumps (P2 & P4)

Table 4
SDS2 Trip Parameters (4 Pump Mode)

Trip Parameters	Detector Type	Trip Setpoint	Conditioning Parameters	Handswitches
Log N Rate High	Ion chambers	25% per second	---	---
Neutron Power High	Horizontal in-core detectors	121.4% full power as a bulk power reference trip Setpoint+		Three positions for setpoint adjustment - nominal configuration - adjusted operation - two pump operation
Heat Transport Pressure High	Pressure transmitter	a. 10.24 MPa(g) or b. 11.62 MPa(g)	a. Trip is conditioned out for initial powers below 70% FP, or if power drops below 70% FP within 5 seconds of exceeding trip setpoint.	---
Heat Transport Pressure Low	Pressure transmitter	Function of reactor power (8.7 MPa(g) at full power)	1. Setpoint determined from ion chamber signals 2. Ion chamber log power signal above 0.3% FP.	Three positions for setpoint adjustment: - four HTS pumps - two HTs pumps (P1 and P3) - two HTS pumps (P2 and P4)
HT Differential Pressure Low	Differential pressure transmitter	a. 950 kPa(d) or b. 450 kPa(d)	a. Trip is conditioned out for initial powers below 80% FP, or if power drops below 80% FP within 3 sec of exceeding trip setpoint. b. Log power from ion chambers and conditioning level selected by handswitch. Flux greater than 0.5% (normal operation) flux greater than 0.3% (handswitch when pumps stopped)	Three positions for setpoint adjustment: - four HTS pumps - two HTS pumps (P1 and P3) - two HTS pumps (P2 and P4) Handswitch to shift the conditioning level to five percent full power to allow for the slow rundown of the ion chamber signal, this helps prevent spurious injections following a loss of Class IV.
Pressurizer Level Low	Differential pressure transmitter	Function of power 7.26 m above 95% FP ramp to 4 m at 75% FP staying at 4 m to 55% FP ramp to 2 m at 40% FP (4 m above 41% FP, two pumps)	1. Setpoint conditioned on in-core flux detector signals 2. Conditioned out if reactor power less than 1% full power	Three positions for setpoint adjustments: - four HTS pumps - two HTS pumps (P1 and P3) - two HTS pumps (P2 and P4)
Boiler Level Low*	Differential pressure transmitter	Function of power 0 m above 90% FP ramp to -5 m at 0% FP	Ion chamber log power signal above 5% FP and flux detector signal above 10% FP.	
Boiler Feedline Pressure Low	Pressure transmitter	3.8 MPa(g)	Conditioned out if ion chamber log power signals below 10% FP.	
Reactor Building Pressure High	Differential pressure transmitter	4.0 kPa(g)	---	
PDC 1/2 Watchdog Trip	---	---	---	
Manual	---	---	---	

* Boiler level setpoints are given relative to the narrow range taps.
\+ The operating trip setpoint is determined from the reference according to reactor operating conditions and licence limits.

3.1.2.6 Heat Transport System Low Differential Pressure Trip

The low differential pressure trip is used on SDS-2 as an alternative to the low flow trip and is designed to give protection against the following:

- Loss of Class IV Power (through loss of circulation)
- loss of regulation from decay power levels when the HTS pumps are stopped, but the HTS is pressurized (see explanation below).

To allow for shutdown and maintenance, this trip is conditioned out at low power, on the log power signal from the SDS-2 ion chambers. The trip is typically conditioned out when the log power signal is less than 5% FP (manually switchable to 0.3% FP for extended periods of shutdown).

This conditioning also makes the trip act as an overpower trip when the HTS pumps are stopped, and this provides LOR trip coverage from decay power levels with the pumps stopped.

3.1.2.7 Reactor Building High Pressure Trip

The reactor building high pressure trip is designed to give protection against the following:

- loss of primary coolant
- loss of secondary coolant inside containment.

In both cases, the trip covers the large and intermediate size range of piping breaks. The cutoff point for small break protection is the capacity of building coolers and condensation heat sinks to prevent a pressure rise.

3.1.2.8 Pressurizer Low Level Trip

The pressurizer low level trip is designed to provide protective coverage in the event of a small LOCA. The loss of inventory due to a small LOCA appears as low level in the pressurizer.

3.1.2.9 Steam Generator Low Level Trip

The steam generator low level trip is designed to detect secondary side failures. Loss of steam generator inventory will always result in low steam generator level.

3.1.2.10 Steam Generator Feedline Low Pressure Trip

This trip , boiler feed line low pressure trip is designed to detect secondary side failures. Depressurization of the steam generator system occurs as a result of main steam and feed line breaks. A loss of feed pumps for the steam generators also causes a SGFLP trip.

3.1.2.11 Manual Trip

The manual trip provides protective coverage for all events, of small enough magnitude that a trip is not required until 15 minutes from the time that the operator is made aware of the event.

3.1.3 Reactivity Insertion Rate and Depth

The maximum negative reactivity insertion rate and delay for the shutdown systems are dictated by the incident that results in the fastest addition of positive reactivity. For CANDU reactors, a loss of coolant accident (LOCA), represented by a maximum reactor inlet header break, dictates the initial reactivity insertion rate requirements (including trip delay). This is due to the positive void coefficient of reactivity. Typically, the shutdown systems meet this requirement with an insertion time of two seconds.

The negative reactivity depth is dictated by the requirement to maintain the reactor in a shutdown state. The depth must thus overcome the worst addition of positive reactivity. This is dictated by an in-core LOCA which has a different scenario than described above. Typically a negative reactivity depth greater than 40 mk in magnitude meets this requirement.

3.2 Functional Assurance Requirements

Functional assurance requirements specify the programs and standards to be followed to achieve the functional capability requirements. In general, the adequacy of the shutdown systems is substantiated by analysis, experiment, and adherence to standards which validate analysis assumptions. Quality assurance programs ensure that the design, manufacture and installation of the shutdown systems meet the design requirements.

3.2.1 Analysis

The shutdown systems performance is assessed by two types of analysis, modelling of design basis accidents and reliability analysis. The first ensures that the shutdown system design is adequate, where as the second ensures that the system will operate reliably when required.

To allow for uncertainties the accident analysis uses conservative modelling assumptions for instrumentation dynamics, reactor and channel conditions. Process system functions that worsen the consequences are generally assumed to occur, to prevent dependence on process system action.

The reliability analysis shows that the shutdown systems meet an overall unavailability of 0.001 years/year. Failure rates are updated, based on operating experience. Testing frequencies are then adjusted as necessary to meet the unavailability target.

3.2.2 Monitoring, Testing and Maintainability

Test facilities are provided so that each component of the shutdown system can be verified to be functioning correctly, by simulating a trip condition. Each parameter's measurement and setpoint have a partial test facility to allow final element testing without shutting down the reactor. Similarly, all portions of SDS-2 can be tested at power, including the final injection valves. Injection valve testing is possible without causing an SDS-2 injection, because of the arrangement of the redundant valves (see Figure 5).

All components which may require maintenance during operation are located in accessible areas. Facility for on-power maintenance contributes to the high production reliability of CANDU reactors.

3.2.3 Codes, Standards and Design Guides

The following AECB documents are presently applicable to CANDU shutdown systems.

AECB Documents:

- C-6 Requirements for the safety analysis of CANDU Nuclear Power Plants.
- R-8 Requirements for shutdown systems for CANDU Nuclear Power Plants.
- C-70 The use of fault trees in licensing submissions.
- C-77 Overpressure protection requirements for class I systems.
- R-10 The use of two shutdown systems in reactors (Note: included in R-8).

4 Design Description

4.1 SDS-1 Shutoff Rods

The SDS-1 shutoff rods using cadmium absorber elements are provided to quickly shut down the reactor under normal and emergency conditions. The rods, being diverse in design principle and orientation from SDS-2, hang above the core, suspended from the reactivity mechanisms deck. Typical locations are shown in Figure 3 for CANDU 6 reactors which use 28 rods. The absorber elements fall into the reactor under gravity, inside a perforated zirconium alloy guide tube within the core, in response to a shutdown signal. A helical spring secured to the top of the thimble is compressed in the rod's "parked" position, to provide it with initial acceleration upon release. Typical shutoff rod construction is illustrated in Figure 4.

The stainless steel cable that suspends the cadmium absorber element, is wound on a cable sheave inside the shutoff rod drive mechanism. This mechanism is mounted on top of the reactivity mechanism deck directly above the absorber. The sheave and cable are open to the calandria atmosphere. Shaft seals isolate the sheave cavity from the gearing. The outer housings are also sealed to provide back-up enclosure of the calandria atmosphere. The vertical location of the absorber element is determined from a position indicator, fastened to the sheave shaft.

In addition to the shaft-driven indicator, a set of reed switches, actuated by a magnet in the top of the shutoff element, signals when the element is in the up or poised position. The switches are mounted in a readily replaceable assembly and thus are located in a chamber isolated from the moderator atmosphere.

The cable sheave is driven by an electric motor through a gear train, engaged by an electromagnetic friction clutch. When the clutch is de-energized the sheave is released and the element falls, unwinding the cable. It is arrested by a rotary oil snubber within the drive unit. When the clutch is energized, the element may be motor-driven in or out. Shutoff rod withdrawal is normally done under control of the reactor regulating system. When the clutch is released, the drive is disconnected from the sheave and the motor drive by the regulating system cannot influence the safe operation of the shutdown system.

SDS1 is repoised by operator command. After SDS1 and SDS2 trips are reset, the operator will demand a new reactor power setpoint. The Reactor Regulating System will attempt to raise reactor power by increasing the demanded power, creating a large negative power error and the shut off rods will be withdrawn from the reactor core. When the shut off rods are fully withdrawn, the operator initiates a request to hold reactor power. At this point, SDS1 is repoised.

Figure 3

Location of Vertical Reactivity Control Units (CANDU 6 Stations)

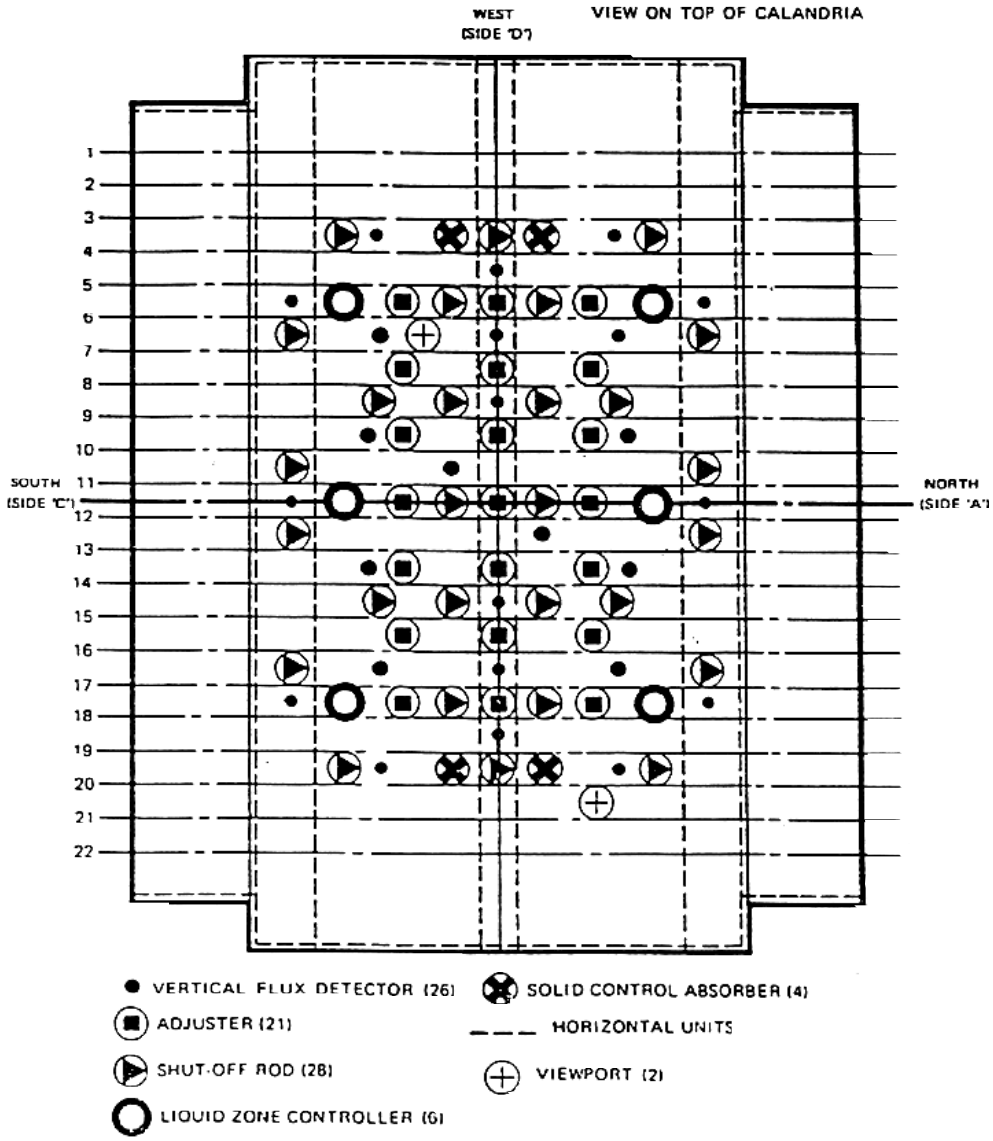
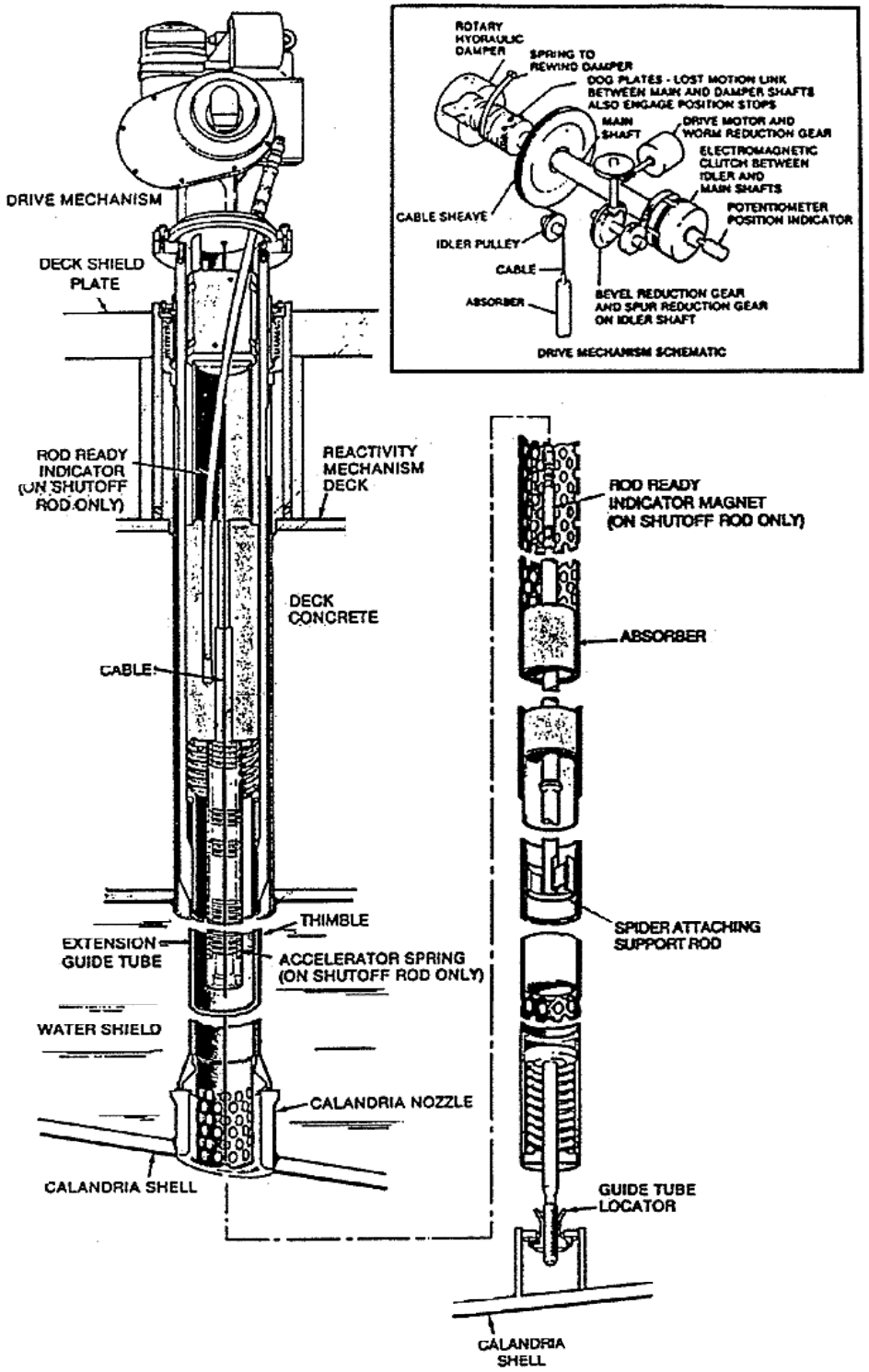


Figure 4
Shutoff and Solid Control Absorber Unit



4.2 SDS-2 Liquid Injection Shutdown System

The second shutdown system operates by injection of the neutron absorber, gadolinium, directly into the moderator. Figures 5 and 6 show a schematic of the liquid injection system and location of the injection nozzles respectively for CANDU 6 reactors. The Zircaloy-2 nozzles penetrate the calandria horizontally and at right angles to the fuel channels. A solution of gadolinium nitrate in heavy water forms the poison that is injected from each nozzle. Holes are drilled in the nozzle along its length to form four rows of jets which inject the poison upward, downward, and to the sides.

The poison solution is stored in the cylindrical tanks mounted vertically on the outside wall of the reactor vault. Each tank is connected to its own nozzle by piping which traverses the vault and shield tank.

A small diameter pipe is routed from the top of each poison tank to a helium header and thus to a pressurized helium tank. With a normal operating pressure of 8.27 MPa(g), this tank supplies the source of energy for a rapid injection. Typically the header is isolated from the helium tank by six quick-opening valves. These are in the usual triplicated array which allows for testing during operation. On recent CANDU reactors such as Darlington, four injection valves are used with different trip logic that allows these fewer valves to be used.

A small line with a valve connects the helium header to the moderator cover gas. Any small leak from the helium tank to the header cannot influence poison level which will stay equal to that of the moderator in the calandria relief ducts. Poison tank elevation is chosen so that poison finds a level in the small diameter pipe above the poison tank. As a consequence of the small diameter, changes in this level will not cause significant movement at the poison/moderator interface.

A polyethylene ball floats at the top of the poison tank. On firing it is forced to the bottom of the tank where it seats, preventing helium leaking into the calandria. This prevents the calandria relief duct bursting disks from rupturing. As an added precaution, a head tank is connected to the calandria and relief ducts to increase the helium volume.

Each poison tank can be isolated for maintenance or sampling using two valves, one on the helium side and one on the liquid side. The former valve protects the operator in case a firing occurs during maintenance. The latter valve prevents loss of heavy water. Both valves require a key for closure; a key that cannot be removed while the valve is closed. A key interlock arrangement provides a warning should more than one poison tank be unavailable at a time.

Repoising of SDS2 to be covered in the lesson on Liquid Injection Shutdown.System.

Figure 5
Liquid Injection Shutdown System

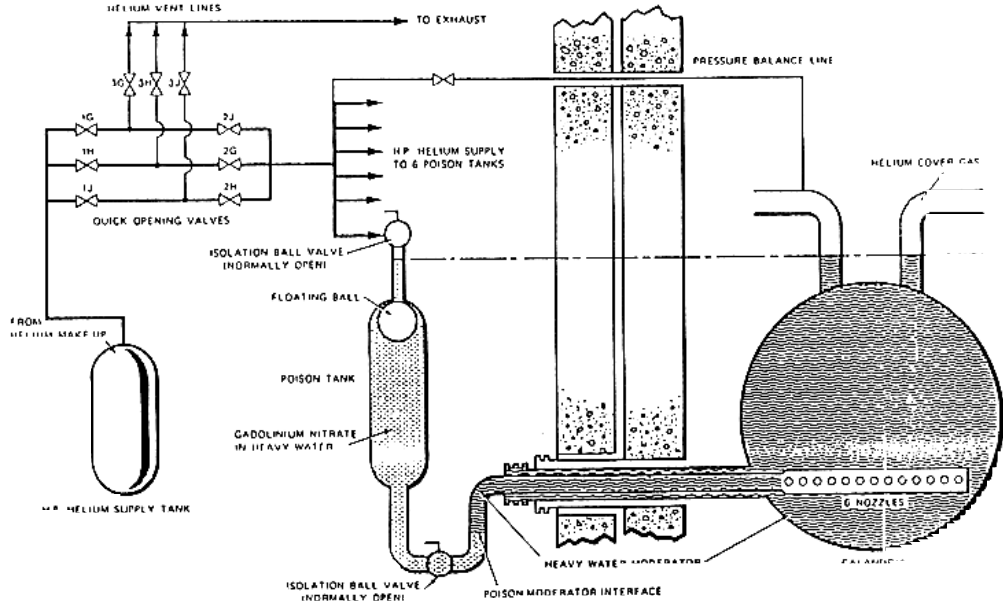
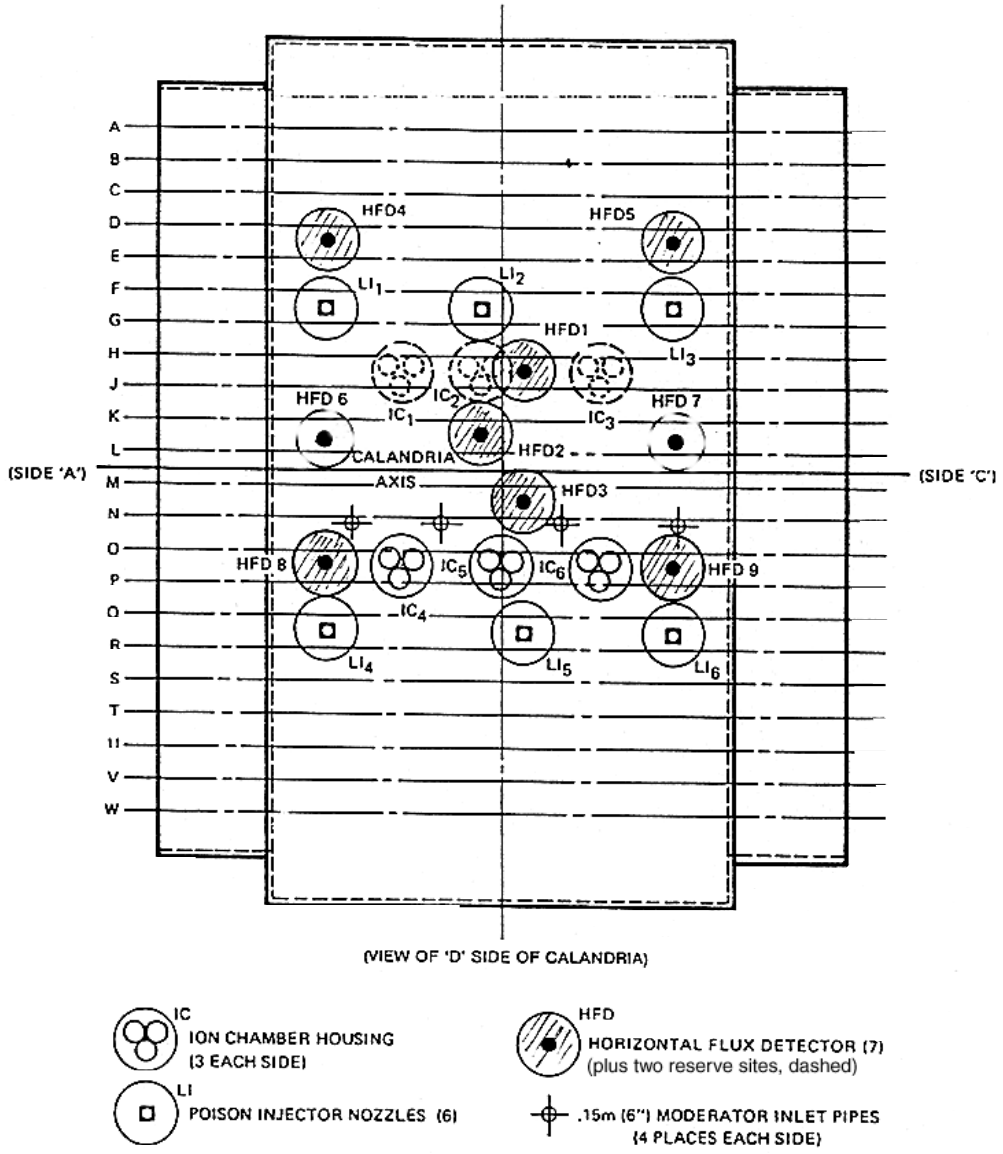


Figure 6
Location of Horizontal Reactivity Devices (CANDU 600)



4.3 Trip Logic and Instrumentation

4.3.1 Equipment Layout

The equipment layout for both shutdown systems is designed to maintain the two group separation philosophy as shown in Figure 2.

The SDS-1 shutoff rods drive mechanisms including clutch, motor, potentiometer, gear box and winch are located above the reactor core on the reactivity mechanisms deck plate. These are accessible during shutdown. Separate cables and junction boxes for the clutch and motor drive circuits are used to maintain separation from the regulating system.

The SDS-2 instrumentation used to actuate and monitor the liquid injection system is located at the side of the reactor core. This equipment is accessible on power.

The channelized cable routings for SDS-1 and SDS-2 are separated within the reactor building, and exit the building at greater than 90 degrees from each other. The SDS-1 cabling is routed to the control equipment room of the main control room, where its instrumentation for control logic is located. The SDS-2 cabling is routed to the secondary control area, where its control logic instrumentation is located. Buffered ties for SDS-2, link display and test equipment from the main control room to the secondary control area so that SDS-2 can be monitored and tested from the main control room.

The field measuring devices for the shutdown systems are mounted in a manner which minimizes the possibilities of common mode failure. The connecting cables are routed back via the channelized routes to the main control room and secondary control area for SDS-1 and SDS-2 respectively.

SDS-1 and SDS-2 both have a separate control panel in the main control room for monitoring trip variables, annunciations, testing and manual trip. Displays for monitoring and annunciation and a manual trip station are also included in the secondary control area for SDS-2.

4.3.2 Channelization and Trip Logic

A common feature in the shutdown systems of all CANDU reactors, is the use of triplicated instrument channels to measure the input variables. Various schemes of two-out-of-three voting logic are employed to initiate a shutdown system trip. Such schemes use general or local coincidence voting logic.

General coincidence logic votes using the trip status of each channel, without taking into account which parameters caused the trip in each channel. Local coincidence logic votes using the trip status of the three channels for each trip parameter. The voting logic is again triplicated into a final three channels which then use additional voting logic to initiate the shutdown system trip. This additional voting is done to prevent spurious trips on single relay failures. Figures 7, 8, and 9 illustrate the use of general and local coincidence logic.

The decision to use general or local coincidence trip logic depends on the economic considerations related to spurious trips. General coincidence logic is relatively simple, easy to test and has a good degree of separation between the channels, however it has less immunity to spurious trips which represent an economic burden. Local coincidence logic is more complex, has a lower degree of separation between channels and requires more complexity to test and reject failed channels. It is thus more expensive to implement than general coincidence

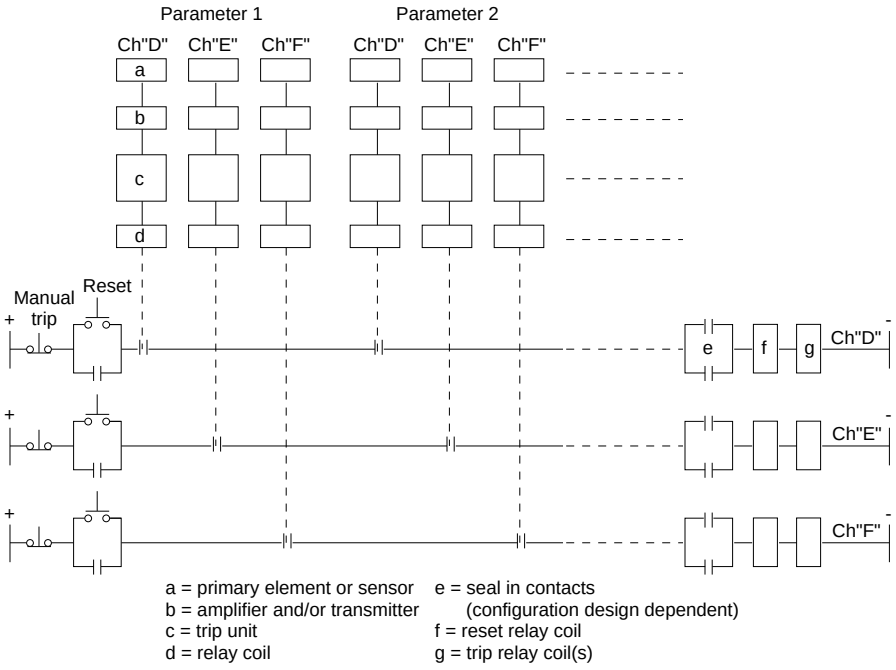
logic. The local coincidence logic is, however, more immune to spurious trips and thus the economic benefits must be balanced against the extra cost when choosing the type of trip logic. Both local and general coincidence logic are used in the various CANDU reactors.

The trip system makes extensive use of relay logic. Relay trip logic is standard in CANDU stations, and has proved on the basis of wide experience to be highly reliable. Use of relays, in trip systems having simple trip parameters, leads to a very simple fail-safe design, capable of being completely tested during operation.

Recent CANDU reactors also use computers to varying extents having some or all of the following features; trip logic, display of parameters, testing and monitoring. These are described in a later section.

Each channel has its own independent electric power supply. An instrument air supply is necessary for operating the ion chamber test shutters and the fast acting liquid injection valves on SDS2.

Figure 7
Schematic of General Coincidence Logic



4.3.3 Interfaces with Other Systems

Software interlocks are provided as follows for interface with other systems:

- The tripped conditions of SDS2 inhibits withdrawal of shutoff rods and moderator poison removal.
- SDS1 unavailable (less than 26 of 28 shutoff rods fully withdrawn) prevents moderator poison removal and adjuster or control absorber withdrawal.

Figure 8

Schematic of Local Coincidence Logic

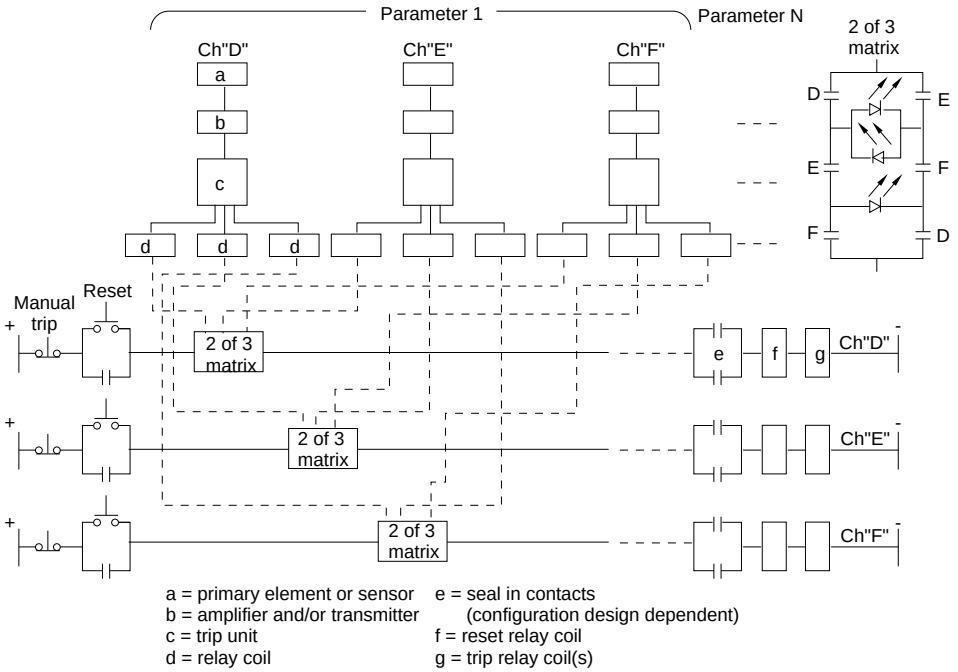
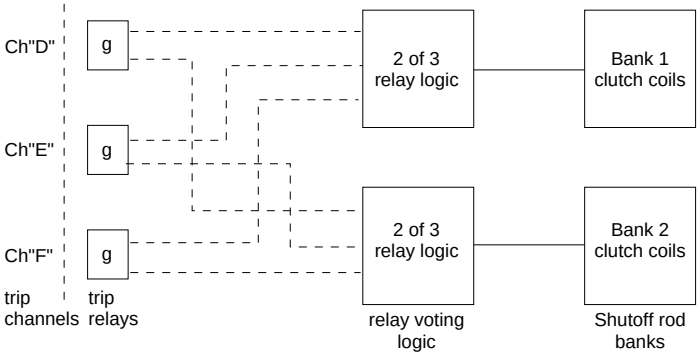
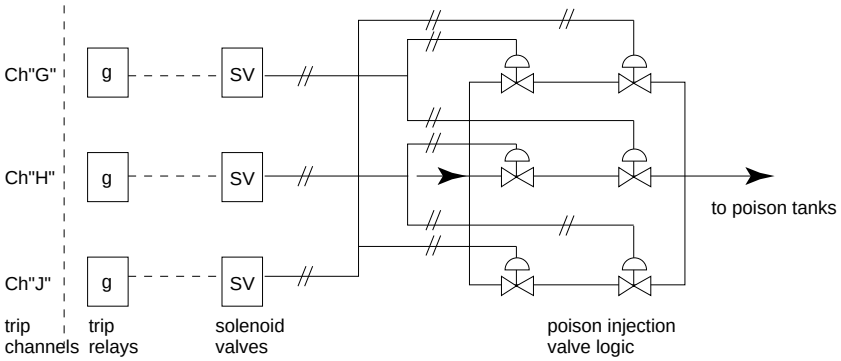


Figure 9

Schematic of Logic for Actuating Mechanical Elements of Shutdown Systems



a) Typical logic for actuating shutoff rods (SDS1)



a) Typical logic for actuating poison injection system (SDS2)

4.3.4 Power Rundown Discrimination

Power Rundown Discrimination (PRD) of low HT flow is used on Darlington and is implemented via software as part of the trip computer function. PRD is also used on Bruce B and Pickering B. The purpose of the PRD is to prevent an SDS2 trip following a loss of Class IV power accident in the event that SDS1 has successfully shut down the reactor. Inhibiting the SDS2 trip for a period of up to 20 seconds will prevent the unnecessarily long outage that would result from a poison injection. Essentially, the PRD functions by comparing a lagged log neutron power rundown as measured by the ion chambers to a reference rundown curve stored in the trip computer memory. It is really just a function of power time delay. The parameter trip is inhibited providing the measured log neutron power remains less than the reference rundown curve. The reference rundown curve is derived from computer simulations to determine the limiting power versus the time locus needed to provide the required accident coverage. A PRD is also installed on the high HT pressure trip logic. The high HT pressure PRD compares the average neutron power to a reference rundown curve stored in the trip computer memory.

The PRD is designed to maintain SDS2 effectiveness. One of the primary concerns involves the potential masking (or deception) of the PRD-conditioned SDS2 trips as a consequence of a partial rod drop initiated by an extremely impaired SDS1. The consequences associated with this postulated scenario have been analyzed for Bruce B and Pickering B and the safety implications have been found to be acceptable. The conclusions also apply to Darlington. PRDs are not used on CANDU 6. The operational objective of not firing SDS2 unnecessarily is met on the SDS2 high pressure trip by suitable time delays, power conditioning and setpoints. On the low core differential pressure trip using a similar approach this objective is also met at 100% FP but not at lower powers.

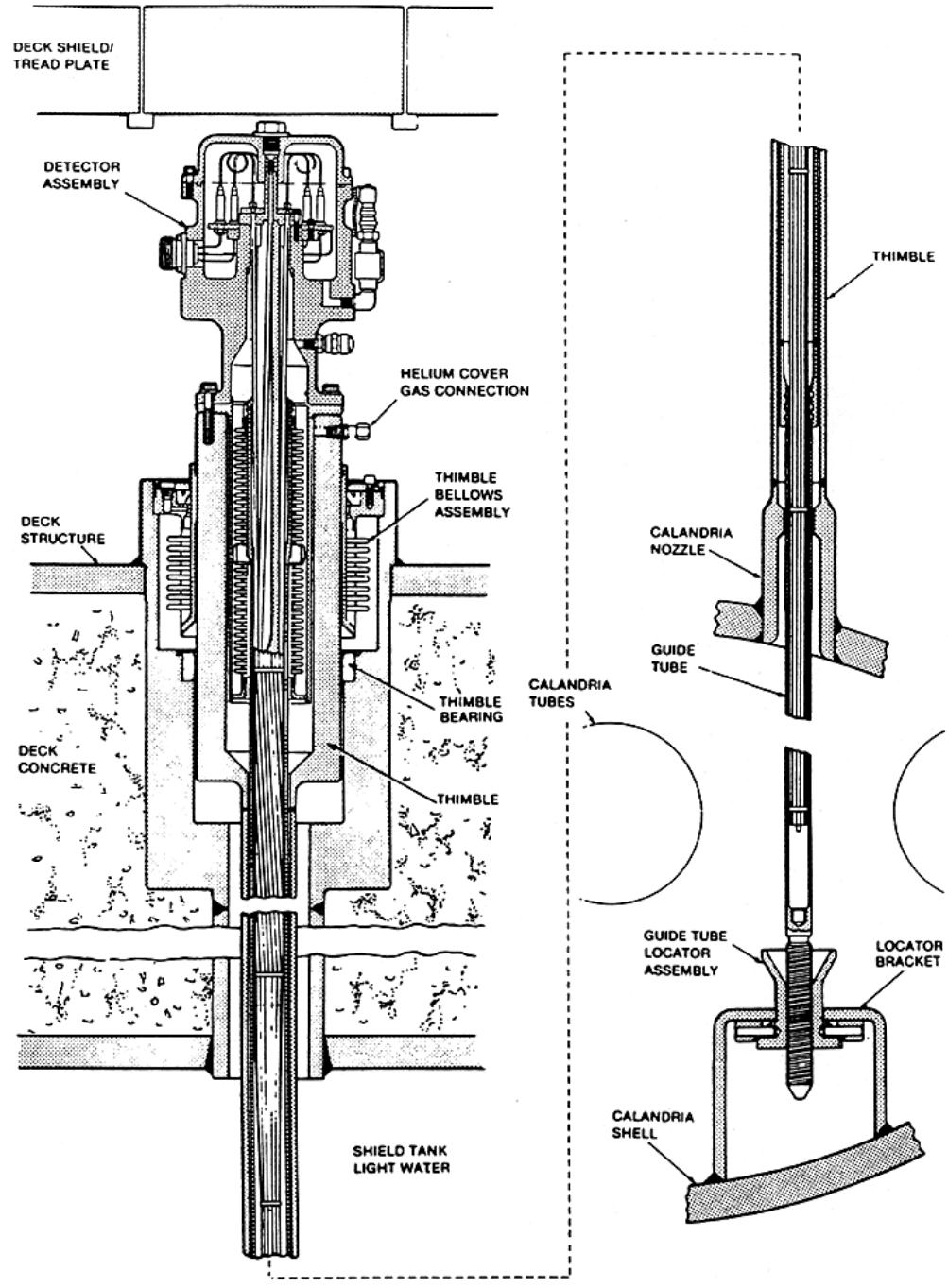
4.3.5 Neutronics Instrumentation

The neutronics trips for each shutdown system consist of neutron over power which is measured using in-core self-powered flux detectors and high rate of log neutron power, measured by out-of-core ion chambers. The flux detector and ion chamber power measurements are also used for some process trips to condition setpoints and inhibit trips at low power. The SDS-1 flux detector assemblies (see Figure 10) are located vertically in the reactor core from the reactivity mechanisms deck, whereas the SDS-2 assemblies are located horizontally from the poison injection side of the core. Figures 3 and 6 show typical locations for CANDU 6 reactors.

4.3.5.1 Flux Detectors

The in-core flux detectors used in CANDU reactors are of the self-powered type. This type of detector is essentially a coaxial cable consisting of an inner emitter electrode, and an outer collector electrode, separated from each other by an

Figure 10
Flux Detector Unit



annular insulator. It is "self-powered" because it does not require an applied bias voltage to separate and collect ionization charge to derive a signal. Exposure to radiation causes the emission of energetic electrons from the emitter, some of which penetrate the solid insulation, reach the collector and cannot return to the emitter to recombine. The deficiency of electrons in the emitter results in a

positive charge on the centre electrode. On connection to the amplifier, the electron deficiency in the emitter is made up by a flow of electrons from the collector to the emitter via the amplifier. The electron flow maintains the emitter at reactor ground (collector) potential. Therefore the detector acts as a current source (for small loads), dependent only on radiation intensity. There are two complicating factors, however, that must be allowed for in design. First, the signal response includes both gamma and neutron flux components. This makes the detector signal unusable at low power where the gamma component being less closely related to power, is more prominent. Secondly, there are time dynamics associated with the gamma component that require compensation so that the resulting signal is a suitably prompt indication of power.

The current output of the detector goes to a linear amplifier, producing an output covering the range 0% to 150% full power and adding dynamic compensation for delayed components of the detector signal. On recent CANDU designs using trip computers, the dynamic compensation is performed in the computer software.

Generally, two types of flux detector assemblies are used in CANDU designs. One design uses a set of detectors wound at various locations on the assembly. These include a number of spare detectors. When the spares are used up, the entire assembly must be replaced. Another design uses straight individually replaceable (SIR) type detectors. These detectors are not wound on an assembly, but are inserted straight into a well tube. The SIR detectors are straight and thus somewhat less sensitive than the wound detectors, being shorter in length when stretched out. The advantage of the SIR detectors is that they can be easily replaced individually.

The detectors are located so that they are not excessively close to adjusters, control absorbers, and zone control units, to reduce any interaction affects. They extend over about three lattice pitches and are separate from any regulating detectors.

Test facilities are provided in the control room to check the trip circuit by injection of a test current on the amplifier input. The detector outputs are displayed in the control room for the purpose of monitoring the signals for correctness, at power and during power maneuvering. There is also a facility for checking the insulation resistance of each detector. The resistance is a measure of detector integrity.

4.3.5.2 Ion Chambers

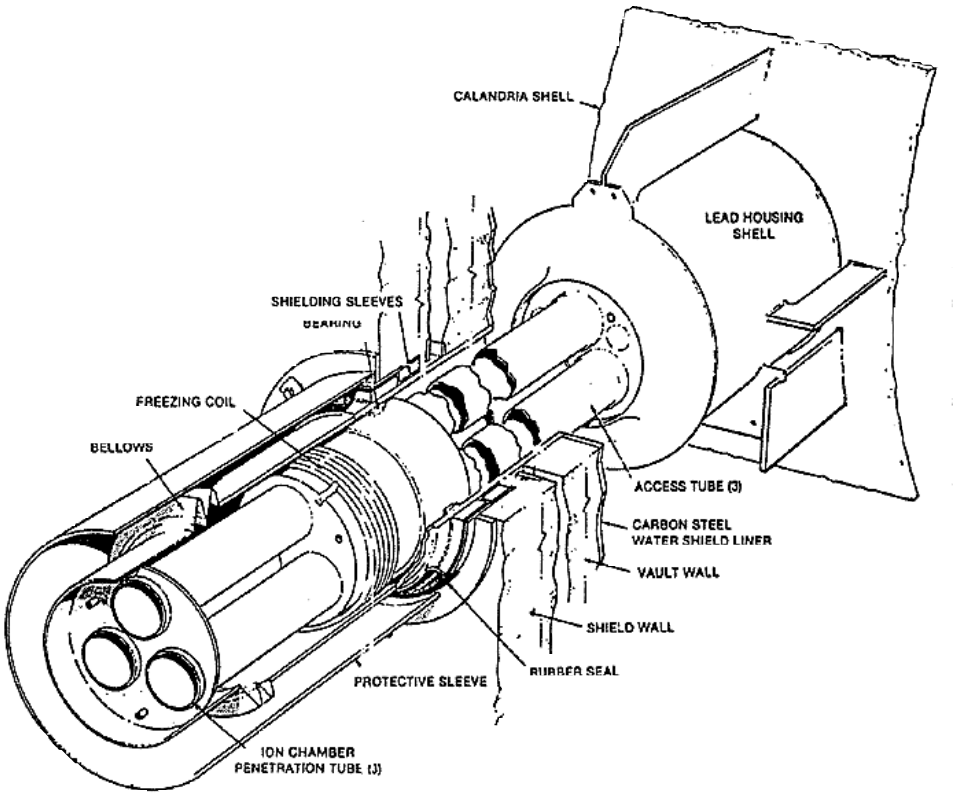
Three uncompensated ion chambers, located in separate housings are provided for each shutdown system. For SDS-1 each housing also contains one regulating system ion chamber, but in a separate cavity within the housing. The design minimizes the possibility of ingress of light water from the reactor vault, into the

ion chamber cavities. The SDS-2 ion chamber housings are located on the poison injection system side of the calandria. The SDS-1 housings are usually located on the opposite side of the calandria except for some CANDU designs (such as Bruce A), where they are located at the top. Figure 11 shows a typical housing with three cavities, two for ion chambers and one for a test shutter. Figure 1 shows the location of SDS-1 and SDS-2 ion chamber housings for CANDU 6 reactors.

A test shutter is provided for each ion chamber housing. The test shutter is a piston-operated boral sleeve driven by an air cylinder and has the capability of increasing the flux at the ion chamber by approximately 25 percent. The piston speed is adjustable to provide the necessary neutron rate signals for testing. A shutter test for both shutdown systems is initiated from the main control room. For SDS-1, the regulating system ion chamber is checked simultaneously.

The output current from each ion chamber goes to an amplifier, which produces log neutron power, linear neutron power, and rate log signals. The rate signal is a direct trip parameter. The log and linear power signals are used as conditioning signals for other trip parameters.

Figure 11
Ion Chamber Housing



4.3.6 Process Instrumentation

The process trips generally make use of pressure transmitters measuring variables such as flow, pressure and level of various components in the plant. In some CANDU reactors there are also trips based on high temperatures (such as the high core outlet temperature trip at Pickering).

The pressure transmitters are located in channelized racks in instrument rooms to allow easy access on power. Testing the process trips is generally achieved by isolating the impulse tubing from the system and valving in a test pressure signal. This ensures that each trip is functionally tested from the sensing element. Regular calibration is performed to maintain transmitter accuracy, typically one loop every three years.

The temperatures trips use resistance temperature detectors (RTD's) which are essentially a platinum wire that changes resistance with temperature. When using RTD's, it is impractical to heat the detector in situ and thus routine testing is achieved by switching in a known resistance in place of the RTD. To test the actual RTD itself, regular calibration is performed. In addition, comparison of actual to expected response during system transients also verifies correct operation of the RTD's.

5 Trip Coverage

The coverage for each event can be presented pictorially (for example see Figure 12) by the use of composite trip coverage maps for a particular CANDU 6. These show the number of effective trips for each shutdown system over the complete range of reactor power, for the particular event being discussed. For events for which trip coverage is dependent on the break size, such as primary circuit loss of coolant, two-dimensional maps are used. In these cases, circled numbers indicate the number of effective trips in each region (break size and power) for a particular shutdown system. The effective trip parameters in each region are also indicated on the map by abbreviations. The extent of individual parameter coverage is indicated by an arrow pointing away from the region of coverage to the line defining the extent of coverage.

Each shutdown system should have, where practicable, at least two effective trip parameters for all postulated events at all powers for the various process system conditions. Exceptions to this requirement are considered acceptable for limited configurations; namely, if providing two-parameter coverage is either:

- not practicable (that is either technically not feasible, or if the only means of detection would be a setpoint within normal operating conditions), or
- counterproductive to public safety, or
- a severe economic burden.

5.1 Example of Trip Coverage For Large Breaks in the Primary Circuit

Large breaks from five to 100 percent of a reactor inlet header break are considered in this section; this range is representative of large breaks in other pipes.

This assessment is based on the FIREBIRD-I analysis of large breaks at full power and FIREBIRD-III analysis of large breaks at reduced power.

Trip Effectiveness Criterion

For large breaks the effectiveness criterion is maintaining the integrity of the fuel channels. Channel integrity at high pressure is maintained providing that fuel elements do not contact a pressure tube. For the analysis of large breaks, a sufficient condition is chosen, the prevention of fuel breakup. This is demonstrated if the energy deposited in fuel during the overpower transient is less than 840 kJ/kg UO_2 above 0°C.

Process System Assumptions

The analysis does not consider any action of the reactor regulating system. Since reactor regulating system action has little effect on the overpower transient for a large break, the analysis is applicable to both operational and frozen reactor regulating systems. For the smallest of the large breaks considered (near five percent), the reactor regulating system could compensate to some extent for the power rise.

Individual Trip Parameter Coverage

Trip coverage maps for each parameter are shown in Figures 13 & 14. Differences between coverage for shutdown systems Nos. 1 and 2 are also indicated.

- **High Neutron Power (Regional Overpower) Trip (Both Shutdown Systems)**
  This is the primary trip signal at full power for large breaks. At lower power for the smaller breaks, this trip occurs after pressurizer low level, low heat transport system pressure and low flow trips, but is still effective. It is not effective for larger breaks at low powers, since the power would rise too quickly through the trip setpoint.
- **High Rate Log Neutron Power Trip (Both Shutdown Systems)**
  At full power, this trip is effective for breaks larger than about ten percent of a reactor inlet header . The effectiveness at low power is similar, possibly extending to smaller breaks. The dashed line shown in the figure for shutdown system No. 1 implies that the extent of trip coverage at low powers is not well defined. Coverage for shutdown system No. 2 is similar.
- **High Reactor Building Pressure Trip (Both Shutdown Systems)**
  At full power this trip occurs within two seconds and is effective for the complete large break range.

- **Pressurizer Low Level Trip (Both Shutdown Systems)**
  This trip is effective for the complete break range at low powers (above the 1 percent inhibit level), because the heat transport system would still have significant inventory when the setpoint is reached. It is not effective at high power.
- **Low Flow Trip (Shutdown System No. 1)**
  At low powers, this trip is effective for all break sizes. It is effective for the smaller breaks at high powers . Below 0.1 percent power, this parameter is inhibited.
- **Low Core Differential Pressure Trip (Shutdown System No. 2)**
  Coverage is similar to that for low flow. Since this trip occurs after the low flow trip, it has a marginally smaller region of coverage . This parameter is inhibited below five percent power.
- **Low Heat Transport System Pressure Trip (Both Shutdown Systems)**
  At low power, this trip is effective for all breaks. Below 0.1 and 0.3 percent full power on shutdown systems Nos. 1 and 2 respectively, this trip is inhibited. At high power, the trip is effective only for the smaller breaks .
- **Composite Trip Coverage for Large Breaks**
  Figures 13 and 14 show trip coverage over the complete range of break sizes and powers for shutdown systems Nos. 1 and 2, respectively. There are at least two effective parameter on each shutdown system over the complete break size range at all powers, and as many as six parameters for smaller breaks at low powers.

Figure 12
Individual Trip Parameter Coverage for Large Breaks

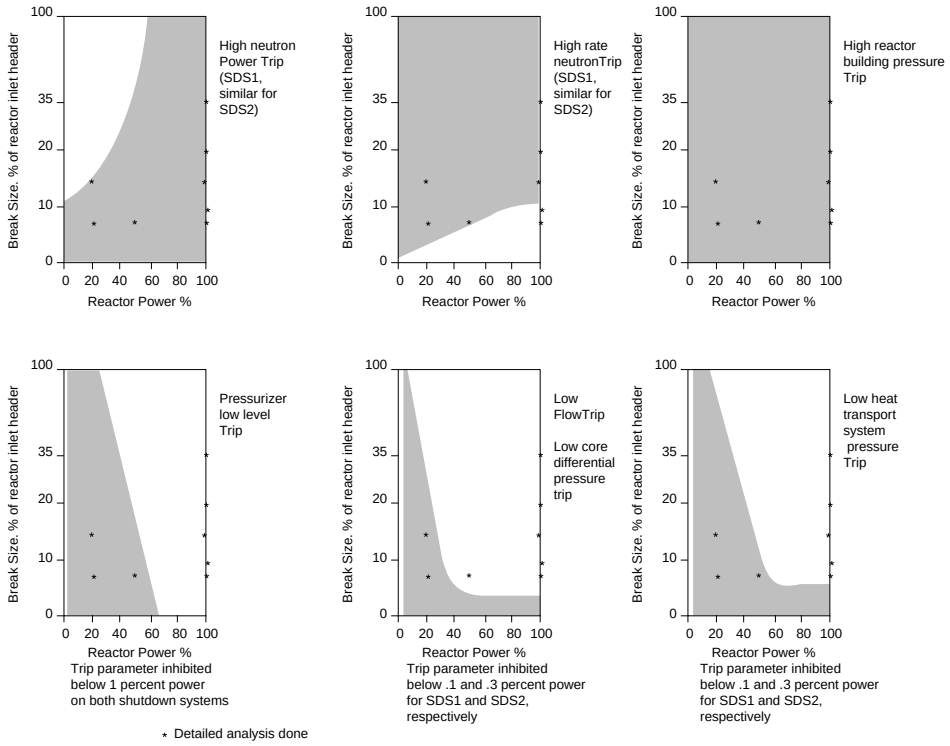


Figure 13
Trip Coverage Map for Large Breaks
Shutdown System Number 1

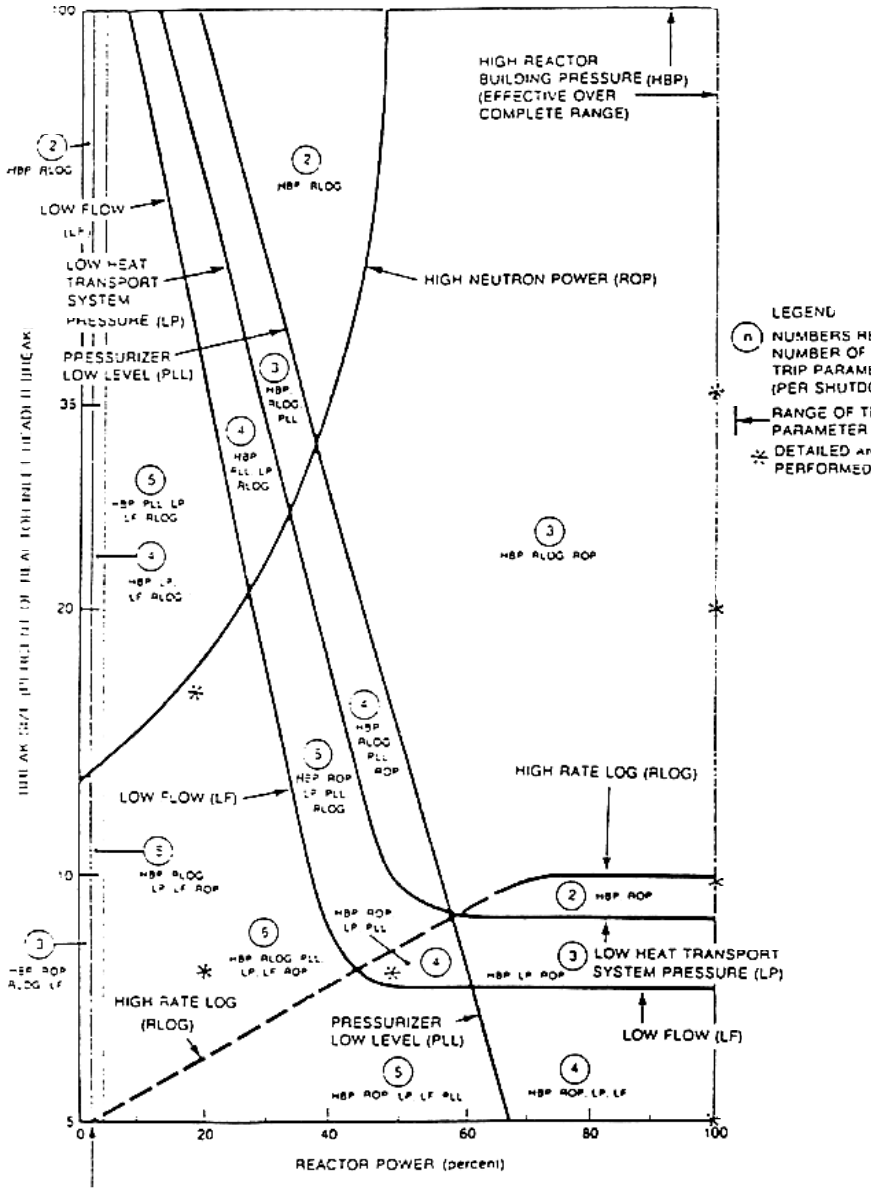
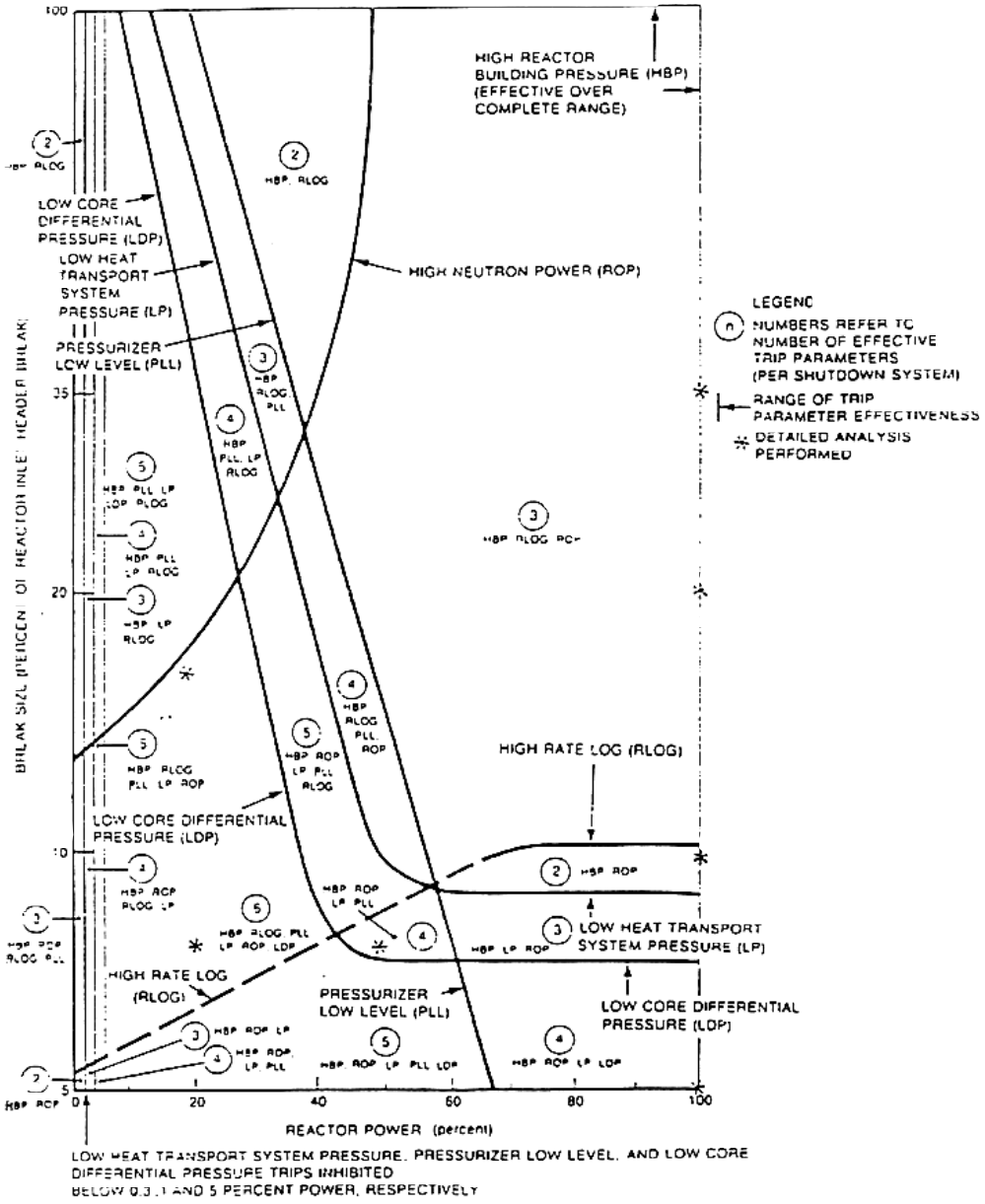


Figure 14
Trip Coverage Map for Large Breaks
Shutdown System Number 2



6 Use of Computers in Shutdown Systems

6.1 General

In recent shutdown systems designs for CANDU stations, computers have been increasingly used and to larger extents. The CANDU 6 plants in Canada and Korea use computers to perform the trip decision logic for most of the process trips. Bruce B uses computers to perform shutdown system monitoring functions and Darlington uses a fully realized computer system to perform trip logic, testing, display and monitoring functions. The decision to use computers in the shutdown systems was made for the following reasons:

- equipment cost savings
- better space utilization
- capability to use complex trips (setpoints that are a function of power)
- reduced operator load for testing and calibration, and
- increased safety reliability achieved by early fault detection through monitoring functions.

The improved ergonomics of the computerized shutdown system also leads to better production reliability through features such as margin to trip display and annunciation.

Although the computers replaced many relays that were used for trip logic, relays are still used in the final trip chain. These perform the higher powered switching functions to de-energize shutoff rod clutches or solenoid valves.

6.2 Evolution of Shutdown System Designs

6.2.1 Traditional Designs

A shutdown system consists of process sensors, reactivity devices (e.g., mechanical "gravity-drop" absorber rods) and intervening instrumentation and logic. If the plant is sensed to be operating in a potentially unsafe state (e.g. power too high, coolant flow too low) the reactivity devices are inserted to terminate the chain reaction very quickly. For reliability, the sensors and trip logic are triplicated, and majority voting determines system action.

The trip setpoint is generally a constant, but may be a simple function of some measured plant variable such as reactor power. The trip contacts from some comparators have parallel conditioning contacts which inhibit the trip under special circumstances, e.g., during very low power operation.

All trip signals, trip setpoints and trip status information are continuously displayed in the main control room. Manual controls allow the operators to test the shutdown systems. Tests are typically conducted between a weekly to monthly period and exercise the entire loop from sensor to reactivity devices.

In the traditional design, amplifiers, comparators, etc., are solid state devices, the trip logic is done via relays, operator displays and small panel meters and lights, and the operator controls are conventional push buttons and hand switches.

6.2.2 Monitor Computers (Bruce)

Early operating experience at Bruce A nuclear generating station, which started operation in 1976, suggested some improvements in the operator interface of the traditionally designed shutdown systems.

The addition of a second shutdown system, required by new licensing rules, and an increase in the number of in-core flux detector sensors, allowing closer operation to the trip setpoint, had the effect of increasing the number of trip signals three fold relative to the earlier Pickering reactors. Aside from the sheer number of measurements for the plant operators to monitor and test, the in-core flux detectors require periodic manual recalibration. Also, the reactor operates close to its licensed rating, leaving little margin to trip. The flux detectors respond to local flux variations resulting from refuelling, as well as to legitimate reactor power changes, increasing the risk of unnecessary and very expensive reactor shutdowns.

Additional manpower could handle the increased testing and calibration work load, but design improvements were required to enable the operator to assimilate all the trip signal data used to give him early warning of impending reactor trips.

A simple monitor computer system was designed and installed at Bruce to upgrade the operator interface. A remote multiplexer in each shutdown system channel scans important signals and sends them to the computer, which constructs convenient bar chart displays for a CRT display in the main control room. The computer also gives the operator warnings if it detects variables too close to their setpoints, failed signals or disagreement among similar signals measured in the three channels. A printer logs abnormal conditions and can provide hard copy for any display.

A single computer is used in each unit to monitor both shutdown systems and the emergency coolant injection system.

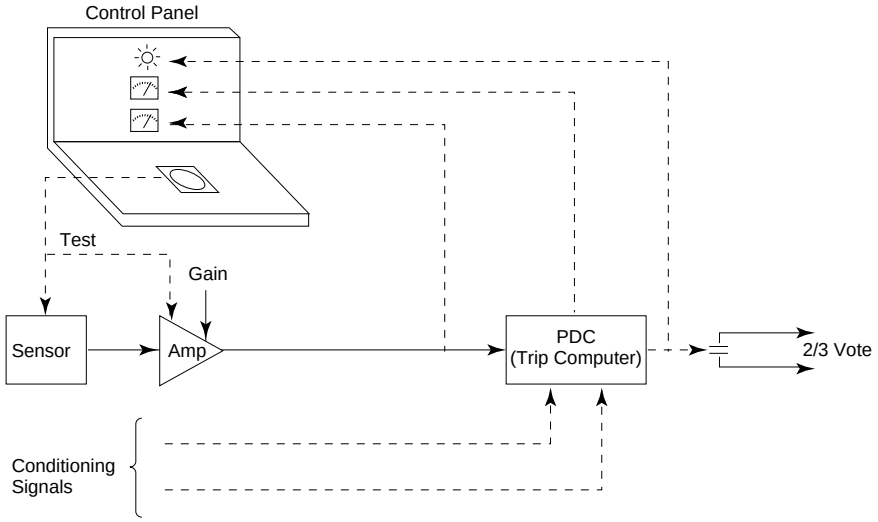
6.2.3 Trip Computers (CANDU 6)

The shutdown systems in the CANDU 6 reactors are quite similar to those at Bruce, but there is one significant difference. Detailed analysis showed that some of the trip functions would require complex conditioning logic in order to satisfy the conflicting requirements of plant safety and immunity to spurious trips for all expected operational transients.

The shutdown system designers proposed the use of microcomputers to implement this conditioning as the best way of meeting the reliability and schedule requirements. The computers were called programmable digital

comparators (PDCs) because they replace only the function of the analogue comparators and their associated conditioning. Figure 15 shows how the PDCs fit into the shutdown system. The proposed design approach was approved by the regulatory authorities and was put into operation at the Gentilly-2, Point Lepreau and Wolsong stations.

Figure 15
Trip Computer (CANDU 6 Design)



6.2.4 Fully Computerized Shutdown System (Darlington)

A laboratory prototype of a computerized shutdown system configuration was developed in a joint development program by AECL and Ontario Hydro. Subsequently, a complete system was developed and built by AECL and was installed in the Darlington Nuclear generating station.

The computerized shutdown system panel arrangement is shown in Figure 17. For comparison, the conventionally implemented CANDU 6 SDS1 panel is shown in Figure 18. Note that the conventional panel meters have been removed from the main control room panel in favour of CRT displays. The test controls have been replaced by a keyboard through which preprogrammed tests are initiated via the monitor and display/test computers. The manual amplifier gain adjustments have been replaced by software gain factors down-loaded from the monitor computer. All trip logic and conditioning are done in the trip computer. This system includes the Bruce and CANDU 6 computer features, and in addition overcomes some other inconveniences experienced at Bruce related to testing and calibration.

Figure 16
Fully Computerized Shutdown System

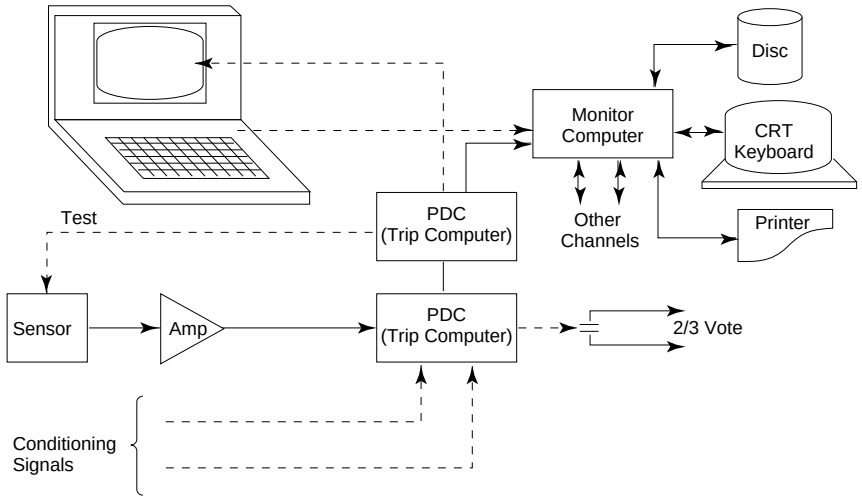


Figure 17
MCR Fully Computerized Shutdown Systems Panels

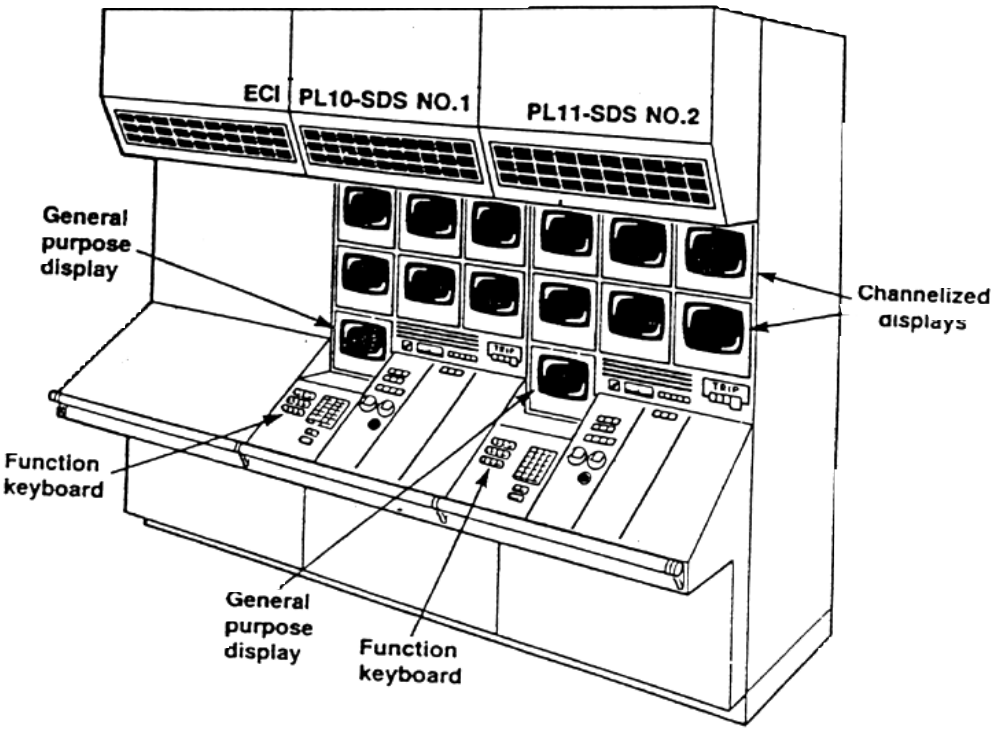


Figure 18
MCR Shutdown System Panel without Computer Display/Testing

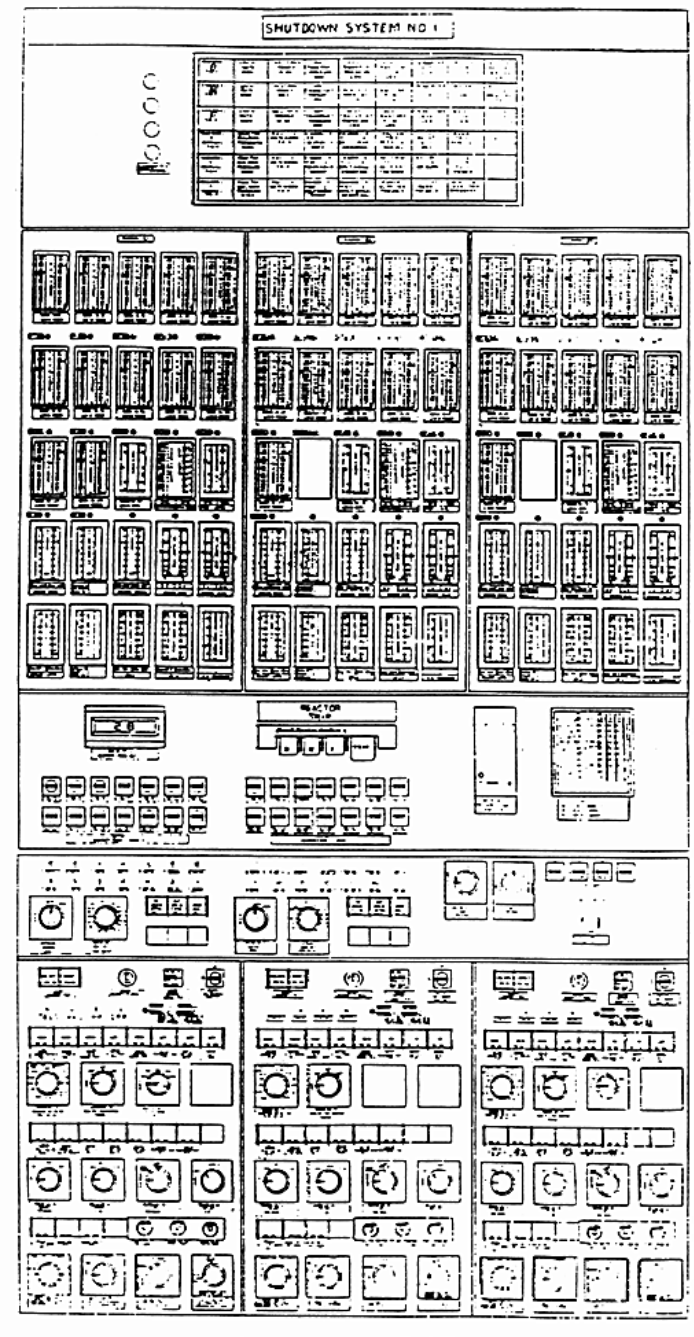


Figure 19 shows the computer configuration. Each shutdown system channel contains two computers: the trip computer and the display/test computer which displays trip variables and setpoints on CRTs in the main control room and initiates test actions in that channel. A shutdown system monitor computer gathers the information from all three channels, alarms on abnormal events or disagreements, stores historical data for later retrieval and provides a general

purpose display to communicate with the operator during testing, re-calibration, etc. Fibre optic data links between the various computers ensure channel separation. A common monitor computer has access to information from both shutdown systems, for convenient summary presentation to the operator on a display unit mounted on his desk console.

6.2.4.1 Major Design Concepts and Requirements

Shutdown system computers must meet essentially the same requirements as conventional shutdown system components. However, computers do have special characteristics and capabilities which result in new requirements. Some major computer system design concepts adopted to meet these various requirements, and reasons for choosing the system configuration shown in Figure 19 are briefly described below.

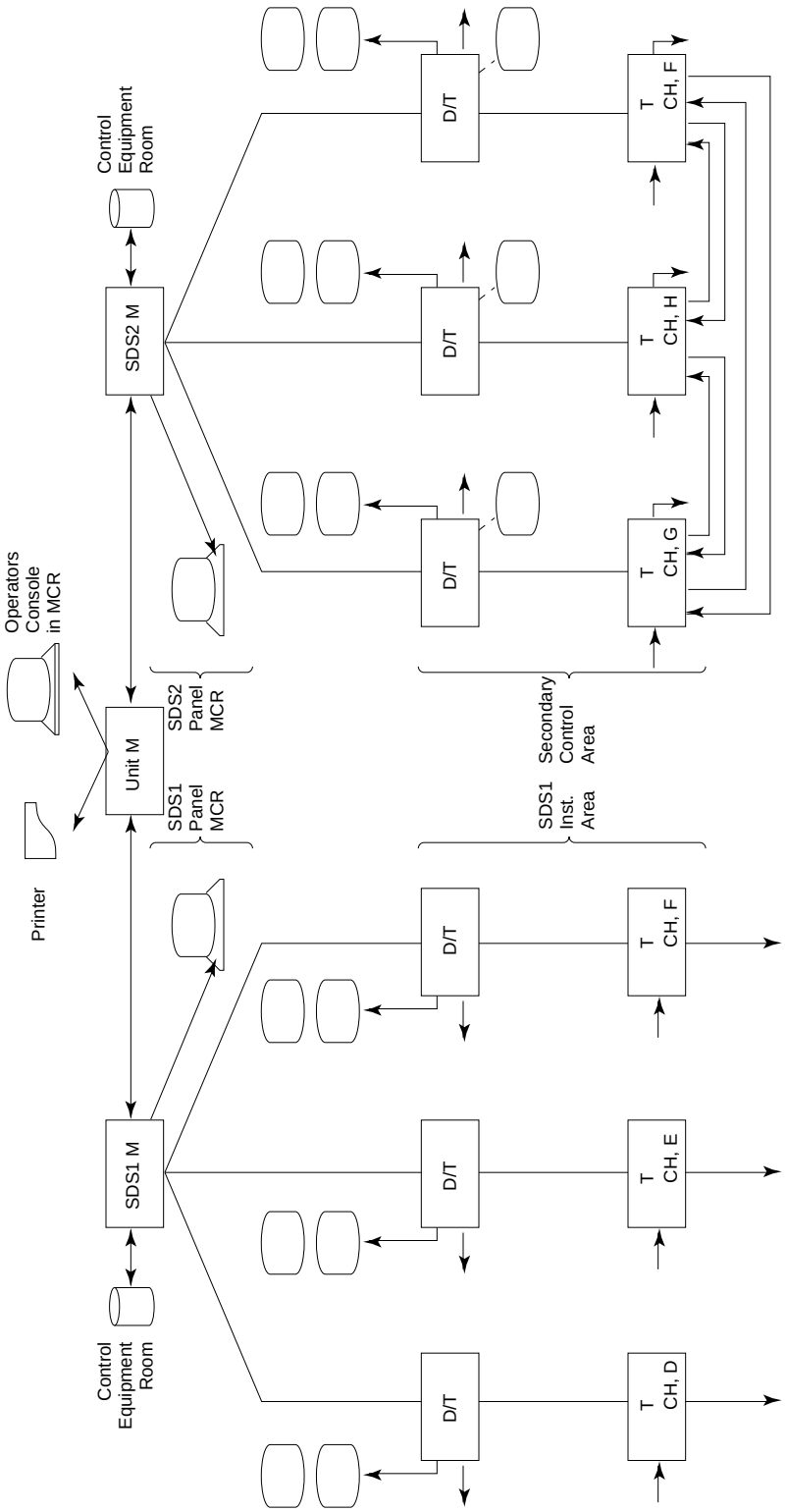
6.2.4.2 Operating Interface Requirements

The operator interface for the shutdown systems should be consistent with the remainder of the control centre, i.e., based on CRTs and keyboards. The system must sense off-normal conditions, both potentially unsafe and potentially leading to spurious trips, and must warn the operator to take appropriate action.

Testing of shutdown system components must be initiated from the main control room, and must be structured so that a test action can never result in a spurious trip. The tests should be automated to relieve the operator of repetitive tasks, but the operator must remain in ultimate control of starting and stopping the tests. The test results should be documented on a printer.

A convenient mechanism is required whereby the operator can, from the control room, change flux detector gain factors in the various trip channels. Gain changes must be documented on a printer.

Figure 19
Configuration of Fully Computerized Shutdown Systems



6.2.4.3 Separation Requirements

Adequate separation must be maintained among shutdown system channels and between the two shutdown systems. In addition, the two shutdown systems must be diverse. If feasible, different hardware and software should be used in the two systems to prevent any possibility of common mode failures.

Channel separation requires buffering for any signals linking two channels directly or indirectly through a common device. Therefore the links between the monitor and the channelized display/test computers must have electrical isolation, e.g., optic coupling. These links must also be functionally buffered, to prevent a failure in the monitor computer from affecting all three channels. Only one of the three links carrying information from the monitor to the display/test computers can be enabled at any one time.

Where the monitor computer is used in active roles such as testing, SDS1 and SDS2 require monitor computers. If only passive monitoring is involved, as in the Bruce system, a single monitoring computer shared by SDS1 and SDS2 is acceptable.

6.2.4.4 Performance Requirements

To handle the most severe accidents, the trip computers must act quickly, in less than about 100 milliseconds. A reactor trip, once initiated must be sealed in until reset by the operator.

The channelized displays of trip signals, setpoints, etc., must be updated at approximately one second intervals to give the operator up-to-date status information during transients.

The monitor computers must store approximately 12 hours of historical data, to allow operators to examine recent time trends of any variable. Suitable trend displays must be provided.

The trip computers must be capable of performing local coincidence trip logic voting. One of the shutdown systems uses local coincidence logic, the other uses general coincidence. (In local logic, a reactor trip is initiated only if the same variable trips in two or more channels, in general logic, a reactor trip is initiated if any variable in one channel and any variable in another channel trip.)

6.2.4.5 Reliability Requirements

The shutdown systems have stringent reliability requirements. For safety reasons, each system must be unavailable less than 10^{-3} of the time, and this performance must be confirmed by regular testing. For economic reasons, the system must be designed to minimize spurious reactor trips. The target is to have fewer than 0.1 spurious trips per year in each shutdown system.

These reliability requirements apply most directly to the trip computers, because they perform all the critical functions. The trip computer hardware and software must be kept as simple as possible to maximize reliability. The trip computer must fail safe, if possible, and should contain comprehensive self checks to ensure that all important components are operating correctly. If a serious failure is detected, the affected channel must be tripped.

6.2.4.6 Software Validation Requirements

Because of the high reliability requirements for the trip computers, the trip computer software must be checked more exhaustively than that of other computers, such as those used for plant control or shutdown system monitoring, which perform less critical functions. This testing is called "validation" and its purpose is to confirm that all detailed functional requirements are met. The validation process was developed as part of the joint AECL/Ontario Hydro development program and uses a separate computer system to perform the tests. The validation computer injects predefined combinations of inputs and senses whether the trip computer responds as intended.

The validation tests are planned and executed by staff independent of the trip computer programmers.

Appendix A
Calibration of Neutron Measurements

Introduction

Neutronic instruments are used in the shutdown systems because of their rapid speed of response, compared to standard thermal measurements, and, in the case of ion chambers, for their wide range of power measurement (10^{-6} of full power to full power).

Ion chambers are used primarily for measurement of log rate, which is insensitive to the absolute accuracy of ion chamber power measurement. However, self-powered in-core detectors are used for determining bulk power and flux tilts at high power, where accurate measurement is important to ensure that maximum power output is achieved without exceeding safety limits.

The self-powered in-core flux detectors have some desirable characteristics. They are simple, robust devices capable of functioning reliably for length periods under in-core conditions. They provide real-time three-dimensional information about the current neutron flux and power distributions within the core. Moreover, an appropriate choice of emitter materials (such as platinum or Inconel), gives suitably fast transient-response characteristics, an important consideration in shutdown applications.

In-core detectors do not measure fuel thermal power (usually the variable of primary interest) directly but respond to a mixture of local gamma and neutron fluxes. To overcome this limitation, a variety of calibration and compensation techniques, both on-line and off-line, are used.

Regional Overpower Protection

The CANDU overpower trips are known as the Regional Overpower Protection (ROP) trips because they are designed to "see" even localized or "regional" overpowers, and are one of several trip parameters which can actuate the two shutdown systems. If either ROP trip senses an overpower condition, it immediately activates its associated shutdown system, shutting down the reactor.

The calibration and compensation requirements for the ROP detectors arise out of the ROP design and operating procedures, as outlined below.

Each of the two shutdown systems uses some 25 to 50 self-powered in-core flux detectors of the same prompt-responding type (i.e., Inconel or platinum-clad emitters) as those used in the RRS. The SDS1 detectors share the vertical assemblies used by the RRS and vanadium flux-mapping detectors. The SDS2 detectors are located in horizontal assemblies to provide physical separation and immunity to common-mode events such as pipe-whip.

The signals from the ROP detectors are fed to amplifiers, dynamic

compensators, trip comparators, displays and test circuits and trip logic circuits as shown in figure 1. Redundancy of detectors and associated equipment ensures a very high degree of reliability . Within each of the shutdown systems, the detectors are "channelized", i.e., grouped into three separate subsets known as trip channels. Each detector has a pre-set trip setpoint. If any detector in a trip channel exceeds its setpoint, the channel itself is tripped. If two out of three channels are tripped, then voting logic produces a reactor trip, i.e., initiates automatic shutdown.

Trip setpoints are established during design of the ROP systems, using the principle that at least one detector must trip in each safety channel before the power in any fuel channel reaches the limiting or critical channel power (CCP). The design analysis is based on a large number of simulated flux shapes, for both normal and abnormal operating conditions, and on a critical heat flux correlation based on full-scale laboratory experiments. For each flux shape, a critical channel power is computed for every channel.

In determining the final level of ROP setpoints, an appropriate allowance is made for various uncertainties that could affect the certainty of a reactor trip occurring before any fuel channel reaches its limiting power.

ROP Calibration

Because of on-power fuelling, the core in an operating CANDU reactor will typically have channels and bundles with a mixture of widely varying irradiations (burnups) and varying powers. As fuel in a channel reaches its maximum burnup, it is discharged and replaced with fresh fuel. The resulting variation in individual channel powers about their time-average (or reference) values is known as refuelling ripple.

A basic simplification in the ROP design process is to separate out the effect of refuelling ripple from the other flux-shape variations, i.e., those due to reactivity devices or xenon changes. Therefore, the perturbation cases used to design the ROP systems are based on an idealized ripple-free nominal power distribution with time-average or equilibrium-burnup fuel properties.

The effect of refuelling power ripple is then accounted for while the reactor operates by an ongoing recalibration procedure, in which detectors are calibrated to the current flux-shape, with an offset equal to the maximum local power peaking in the current core.

That is, the ROP trip calibration consists of the following steps:

a. At periodic intervals (typically every three to four days), the maximum ratio (overall high-power channels) of the current (rippled) channel power to the reference channel power for that channel is calculated; this parameter is called the Channel Power Peaking Factor (CPPF).

b. At frequent intervals (e.g., daily or once per shift), the ROP trip detector readings are inspected and those outside of a preset tolerance band are recalibrated to the product of the CPPF and the current reactor power, i.e., so that their readings will equal the current CPPF when the reactor is at 100% power.

To illustrate, if the CPPF is 1.08, and the reactor is at 100%, then all the ROP detectors will be reset during recalibration to read about 108%. This reduces the margin between each detector and its setpoint by 8%, just as a few channel powers are 8% closer to their CCPs than they were in the original ROP analysis with an unrippled reference core.

The CPPF recalibration procedure is conservative since it applies to all parts of the core a maximum ripple factor that is appropriate and needed in only certain parts of the core. Implicitly, it assumes that for every flux-shape the peak ripple will coincide with the peak of the unrippled flux-shape.

The effect of this conservatism, along with provisions for other errors and uncertainties relating to the recalibration process, are considered in the ROP probabilistic assessment. The axial effects of fuelling variations are accounted for separately, in the critical channel power calculations.

On-line Calculation of CPPF

Different methods of determining the CPPF are used in different CANDU plants. In the Bruce station, the first CANDU to use an ROP system of the type described, the CPPFs are based on an off-line diffusion calculation of the prevailing power distribution. Reactivity device status information is supplied by the operator, and xenon equilibrium is ensured by performing the calibrations only under steady conditions. To ensure that the simulation results are reliable, periodic checks are made against thermal power measurements from 22 fully-instrumented fuel channels (flow, quality, and ΔT measurements).

In the CANDU 6 reactors, the CPPFs are calculated from channel power distributions obtained from the off-line power mapping program known as PMCR (Power Mapping and Calibration Routine) or from an off-line diffusion calculation. PMCR derives its spatial information from the vanadium in-core flux-mapping detector measurements and from operator-entered information on fuelling, with bulk power normalized to steam generator thermal power measurements (PTH). Periodic cross-checks against diffusion code calculations and against fuel channel flow and temperature measurements ensure the reliability of the PMCR calculations.

In both the CANDU 6 and Bruce G.S. approaches it should be noted that ROP calibration is based on measurements and calculations of thermal power. The gamma and neutron fluxes which drive the in-core detectors play the role of

intermediary variables, ensuring that a trip takes place before any fuel channel exceeds its critical power.

Detector Dynamic Compensation

Note that the above discussion assumed the reactor was in a quasi steady-state condition at trip, so that the detector dynamic response was not of relevance. In practice, however, dynamic compensation of the ROP detector response is used to ensure that the detector signal matches or leads the fuel power-to-coolant at any rate of power increase that could arise. For fast and medium-rate LORCs (Loss of Reactivity Control accidents) and LOCAs (Loss of Coolant Accidents), for which the ROP trip provides backup trip protection, the power to coolant lags the fission power by a sufficient margin that the detector response does not require compensation. However, for slow LORCs (for which ROP provides the primary means of protection), the thermal lag of the fuel is less significant, and the detector response may lag reactor power for some types of detectors due to delay components with larger time constants. Hence, in order to avoid unnecessarily conservative trip setpoints, dynamic compensation is provided for these types of detectors.

As in the case of on-line RRS detector calibration, the objective of compensation is to obtain a signal which matches the fuel power dynamics. A "conservative match", i.e., a compensated response which is greater than or equal to the fuel power transient, is desirable. Such a "conservative match" is obtained in the CANDU 6 using a simple second order analogue compensation module, which is installed between the amplifier and the trip comparator.

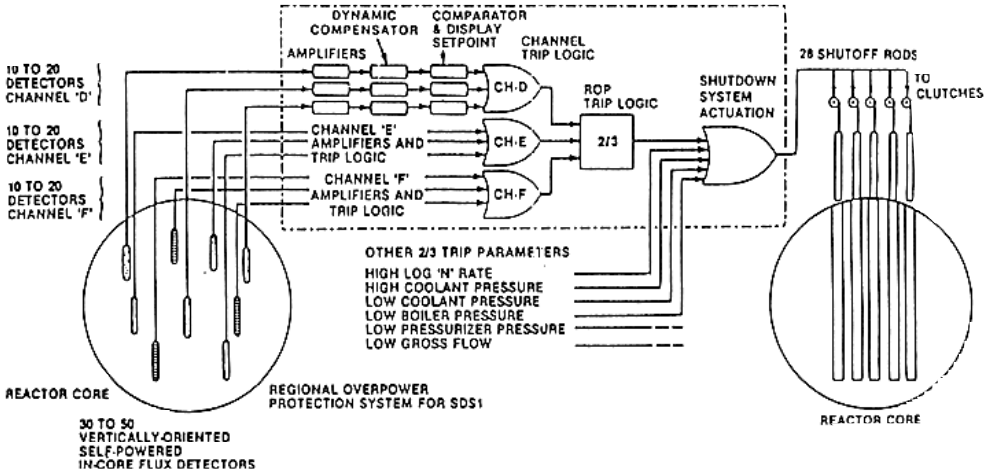
The compensator transfer function takes the form:

$$V_o(s) = V_i(s)\left[K_1 \frac{K_2}{1+\tau_1 s} \; \frac{K_3}{1+\tau_2 s}\right]$$

where Vi (s) and Vo (s) are the Laplace transforms of input and output signals, respectively.

The values of the gains K1, K2, K3 are selected to match the compensated detector signal to fuel fission power dynamics over the range of 10 to 5 x 104 seconds. The gains and time constants in the compensation module are adjustable over a small range to accommodate changes in detector dynamics that may occur over the life of the detector. Measurements taken during transients at CANDU research and power reactors confirm the validity of this dynamic compensation approach.

Figure 1:
ROP Trip For Shutdown System No. 1



Containment System

Training Objectives

On completion of this lesson the participant will be able to describe;

- The function of containment systems as one of the barriers between the radioactivity in the core and the public.
- How the design features accomplish that function.
- How the containment system responds to accidents such as LOCA.
- How testing assures the successful operation of the system.
- Some of the shortcomings of existing containment systems uncovered by testing.

Table of Contents

1. Introduction

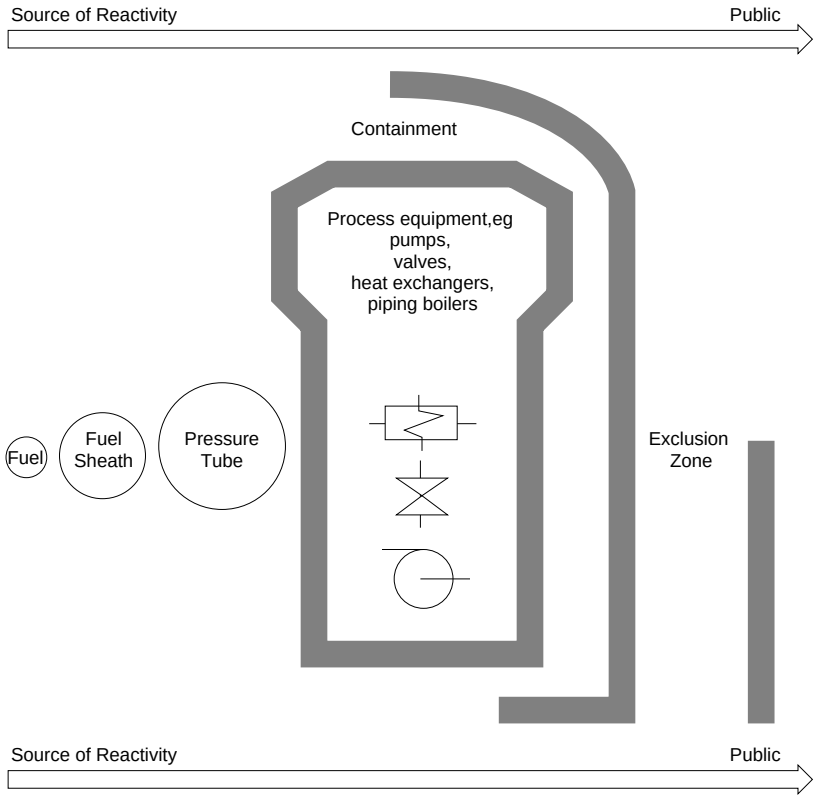
The continuing production of electric power from nuclear energy requires the prevention of harmful radiation doses to the public at large, the operating staff, and to the environment.

Containment is the structural envelope around the nuclear components of the plant and the systems that limit the pressure within the envelope after a loss of coolant accident.

Over 99.9% of the radioactivity produced by the operation of a nuclear power plant is held in the fuel. Small amounts of radioactive isotopes are present in the primary coolant, in the moderator and in the annulus gas and cover gas systems. Equipment failures and human errors can occur in spite of the best efforts of designers, manufacturers, constructors and power plant operators. One of the basic features of the Canadian approach to nuclear safety is the provision of a number of inherent and special barriers to the release of radioactive materials from the fuel to the environment. The probability of breaching one barrier to release radioactivity is higher than breaching two or more barriers. This is illustrated in Figure 1. The fuel itself is an inherent barrier, the fission products for the most part are trapped within the fuel material. The fuel sheath and the intact primary coolant system serve as the second and third barriers to the release of radioactive materials to the containment. The failure of these components could result in the release of significant amounts of radioactivity within the containment envelope, which is the third barrier. The final barrier is the exclusion zone of 1000 metres which surrounds the reactor. The public is not permitted to be within this area. This zone provides dilution of the dispersed activity.

Figure 1

Barriers to Fission Product Release



A large portion of the nuclear safety design and analysis effort is directed toward ensuring radioactive materials are retained within containment and to limit those that may be released to an acceptable level. The radioactivity of concern is from fission products, activation products and tritium. The containment system is designed to keep the doses to the public within limits specified by the Atomic Energy Control Board (AECB) as given in a paper by Hurst and Boyd (1972) and more recently in the AECB Consultative Document C-6. The dose limits for the most exposed individuals of the public at edge of the exclusion area is defined as a function of frequency in C-6 and is summarized in this table.

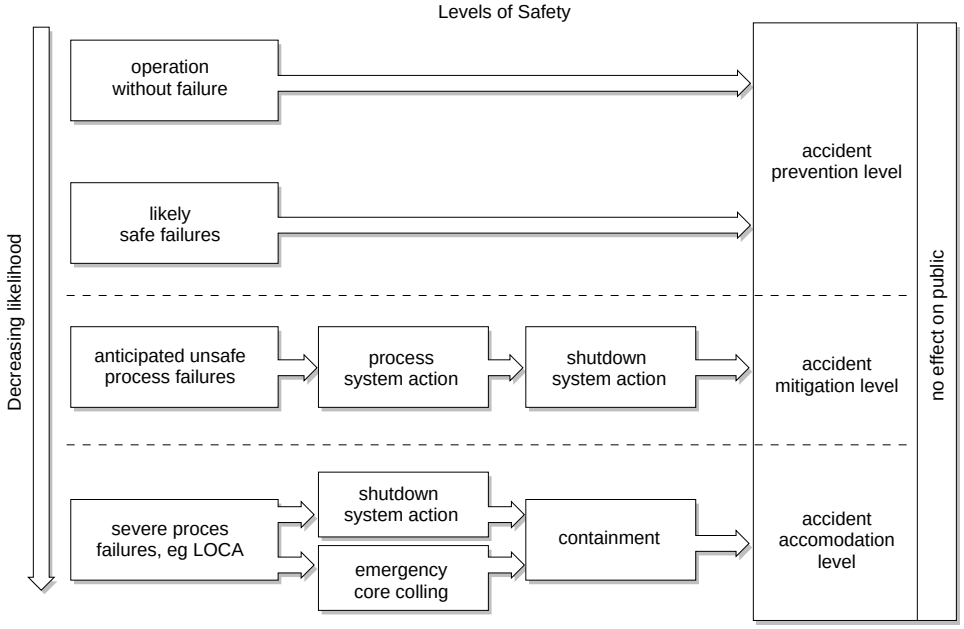
Class	Frequency (per reactor- year)	Whole body dose (Sv)	Thyroid dose (Sv)
1	between 10^{-2} and 1	0.0005	0.005
2	between 10^{-3} and 10^{-2}	0.005	0.05
3	between 10^{-4} and 10^{-3}	0.03	0.3
4	between 10^{-5} and 10^{-4}	0.1	1.0
5	less than 10^{-5}	0.25	2.5

The containment system is one of the special safety systems that prevents or limits activity releases to the environment. The other Special Safety Systems are the two shutdown systems, and the emergency core cooling system. Because of the large amounts of energy stored in the reactor coolant systems, the envelope must withstand a pressure rise and have a tolerable integrated leak rate during the pressure excursion.

The consequences of a wide range of single-, dual- and some multi-failure accidents with a probable frequency greater than one accident in a million years are analyzed for containment design. The AECB requires the evaluation of some extremely severe accidents, even with as low frequency as one accident in a hundred million years. To accommodate the variety of adverse incident or accident scenarios, the multilevel defense system is needed and has to be tolerant to a wide range of equipment failures and human error.

Accident scenarios can be grouped into levels based on their consequences as shown in Figure 2. By far most of the postulated events fall into the first two levels of safety. The third level generally receives the most attention, since the failures at this level challenge the special safety systems. Designing the special safety systems to deal with these extremely low probability events leads to large safety margins for the more likely events.

Figure 2
Levels of Safety



2.0 Functions and Components of the Containment System

For single unit CANDU nuclear power plants the reactor is enclosed in its containment while for multi-unit CANDU power plants several reactors (4 or 8) share the containment system (ie, 4 reactors at the Bruce and Darlington stations, and 8 at Pickering).

The containment system is a special safety system. It provides a means to limit the release of radioactive materials to the environment and so limit the radiation dose to the public after a severe accident. Any pressure excursion in the containment atmosphere must be limited so that there is no damage to the nuclear reactor and its coolant system, and to the containment envelope. The containment system has some additional functions, such as providing a weather-proof enclosure for the nuclear reactor and its associated systems, radiation shielding for workers in its environment, a protective barrier for the nuclear reactor and its cooling system against external explosions, impacting missiles or light aircraft.

In a single unit plant the entire nuclear reactor assembly, the cooling system (the heat transport system), and the regulating and safety devices of a CANDU plant are enclosed within the containment structure.

A containment system, during the course of a normal day-to-day operation, serves to control minor releases of radioactive materials from the reactor coolant and moderator systems.
The containment envelope is the principal component of the containment system. It surrounds the space were highly radioactive atmosphere may be present, and includes the penetrations of the walls. It is made of prestressed reinforced-concrete to meet the design aims outlined below. The containment walls and roof provide radiation shielding for the outside environment, and, obviously, normal housing and weather protection for the reactor.

Functions of the Containment System

1 Provide a pressure barrier and envelope that can retain, and limit the release of radioactivity to the environment from a LOCA and from fuel handling accidents
2 Provide a pressure barrier that can resist the ignition of hydrogen and air following a LOCA. (This applies to single unit stations.)
3 Maintain its structural integrity following a severe break within containment of the steam and feedwater coolant circuit such as a double ended discharge from a steam line break.
4 Maintain its structural integrity in the event of Design Basis Earthquake (DBE)
5 Protect the reactor an its process, control and safety systems from damage from floods, tornadoes, etc..
6 Protect the reactor and its process, control and safety systems from damage

from manmade causes such as an explosion of nearby trains or trucks, impact from missiles or small aircraft or turbine disintegration.

The components and subsystems of the containment system are outlined below. Active waste handling has small direct impact on the containment design and safety analysis, except that the water from a loss-of-coolant accident (LOCA) accumulates in the reactor building sump and is used during the longterm emergency core cooling. The mission time for post-accident cooling could be 2 to 3 months. The disposal of the radioactive water from the sump is a post-accident cleanup activity.

The reactor building and vault pressure sensors provide the conditioning signal for emergency core cooling (ECC) initiation after a loss of coolant accident (LOCA), the trip signals for both shutdown systems and the trip signal for containment isolation. The radioactivity measured before the filter of the reactor building ventilation system also serves as a trip signal for containment isolation.

Components of the Containment System

1 Containment Envelope.
2 Dousing system for pressure suppression, steam condensation, atmosphere cooling and absorbing, ie washing out, some airborne radioactive materials.
3 Filtered air discharge and emergency filtered air discharge systems.
4 Airlocks for operator access.
5 Fuel transfer ports for new and irradiated fuel.
6 Process line penetrations for steam, water, air, electrical, etc.
7 Process line isolation valves; one or two for each line, and automatically closing on lines that have the potential for opening the containment boundary.
8 Equipment port or hatch for moving large components in and out.
9 Local air coolers for containment atmosphere cooling.
10 Hydrogen mitigation equipment.
11 Gross contamination leakage monitoring.
12 Active waste handling.
13 Subatmospheric pressure containment and vacuum building - for the multi-unit stations.

3.0 Design Requirements

The perfect containment would be a concrete or steel structure surrounding all the nuclear components, with a zero leak rate at all pressures, no penetrations and a thickness to provide adequate shielding and missile protection. However, this simple concept is in conflict with the requirements arising from normal operation. Containment penetrations are required for process services such as

electrical cables, instrument air, and access for equipment maintenance and plant operations. In addition, systems required for accident mitigation pose a challenge. They can be located either inside the reactor building, where they would be subjected to the harsh environment resulting from the accident but do not require reactor building penetrations, or outside, where they have the benefit of access for maintenance but the disadvantage of the possible spread of activity due to leaks. A large number of factors including system characteristics, containment size, and regulatory requirements influence where the equipment is located.

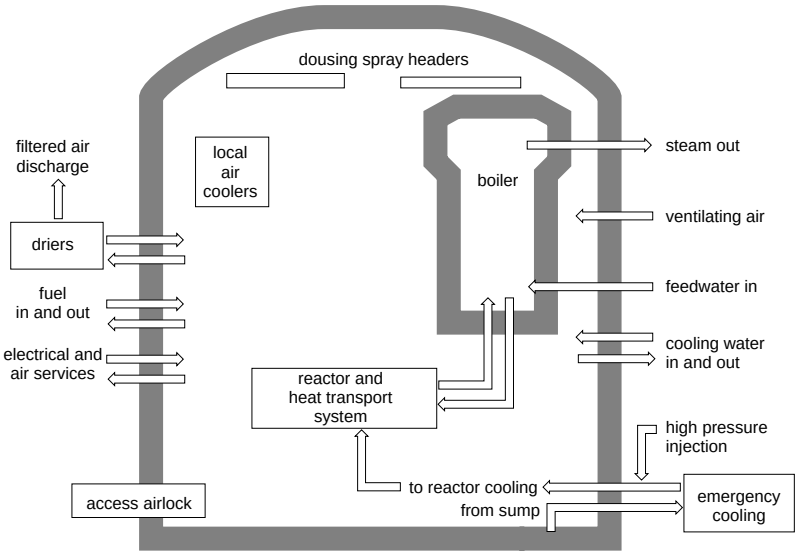
3.1 Requirements For Normal Operation

The normal operating requirements that affect the containment are:

- a need for routine daily access via personnel and equipment ports, airlocks or hatches to areas of the reactor building for new fuel loading, maintenance of equipment, and operator surveillance.
- a ventilation system that provides an adequate supply of cooled, filtered air for those working in the accessible areas and maintains the reactor building pressure slightly subatmospheric so that fresh air leaks in rather than the containment atmosphere leaking out.
- a vapour recovery system to recover heavy water escape, and to reduce tritium contamination,
- a system for the automatic transfer of irradiated fuel from the fuelling machine to the irradiated fuel bay located in the service building.

The penetrations through a CANDU 6 reactor building resulting from these requirements and from the requirements for energy suppression, services, etc. are shown in Figure 3.

Figure 3
Typical Penetration of Containment



3.2 Requirements for Accident Conditions

The accidents which could lead to an increase in pressure and in more severe cases to a release of activity within the reactor building include a failure of the reactor cooling system piping, a failure of the steam piping within the reactor building or a failure of fuel while it is being transferred from the reactor to the irradiated fuel bay.

The basic design requirement is a clearly defined continuous containment envelope which is capable of limiting the release of radioactive materials to an acceptable value for design basis accidents; this in turn requires;

- a reliable containment isolation system;
- a containment structure capable of sustaining the pressures following design basis accidents;
- energy absorbing systems to limit peak pressure and temperature within the containment envelope to protect the integrity of the containment
- means to wash out, plate out or filter out airborne radioactive materials within the containment.

3.3 General Requirements

Other requirements imposed on the containment system are:

- The components of the containment system must be separated physically, and functionally from other systems used to produce power and from other special safety systems.
- The containment system must meet a demand unavailability target of 10^{-3} during operation. This must be demonstrated by testing throughout the life of the plant.
- All operations must be automatic unless there is sufficient time for an operator to assess the situation and take appropriate action. This time is usually taken as a minimum of 15 minutes.
- A pressure proof test must be performed at the end of the construction stage and at suitable intervals during the life of the plant.
- A leak rate test must be performed at the end of construction (after the pressure proof test) and at intervals during the life of the plant; the initial target leakage rate is 0.1% of the containment atmosphere volume/day with the containment at design pressure.
- The containment system must be seismically qualified against loss of integrity due to a DBE; the seismic qualification may be analytical with accepted stress analysis codes.
- Safety analysis must demonstrate that the radiation dose to the public following a number of deterministic accident sequences is within acceptable limits. This requirement, in turn requires that;
- The containment system must be capable of responding effectively to the more probable small breaks (isolation requirement) as well as the less probable large breaks (peak pressure requirement).
- The design must deal with a postulated loss-of-coolant accident sequence

that assumes impairment of the emergency core cooling system. This gives the largest concentration of radioactive material within the reactor building.

- The design must handle accident sequences that assume failure of containment features coincidently with the initiating event. The failures to be considered include failure of isolation logic, partial failure of isolation devices, or partial failure of the pressure suppression system.

4.0 Design and Mode of Operation of Containment Systems

4.1 Containment Envelope

The CANDU 6 containment envelope is the reactor building and its penetrations. The building has an upright cylindrical perimeter wall, a flat base slab and a domed roof. It contains the reactor, the primary heat transport system, the steam generators, the moderator system and other auxiliary systems.

It is a post-tensioned reinforced concrete building. Beneath the dome there is a tank which stores water for containment dousing and emergency cooling.

The design pressure of the containment envelope is the upper bound of the peak pressures resulting from all of the design basis accidents considered. The CANDU design containment pressures based on primary coolant circuit LOCA are relatively low compared with the design pressures for the containment envelope for other reactor types. This is mainly because of the larger free air volume in the CANDU containment envelope. The local air coolers, condensation on the containment walls and the dousing spray system all help to reduce the severity of the pressurizing accident by absorbing energy. In the multi-unit CANDU reactor installations a separate vacuum building, which becomes connected to the accident reactor building, allows even lower design pressures than in the single-unit CANDU containments.

The containment envelope of each of the multi-unit Bruce-A, Bruce-B and Darlington nuclear generating stations includes four reactor vaults, a fuelling area, a fuelling machine service area, pressure relief ducts, a common pressure relief valve manifold, a common vacuum building, airlocks, transfer chambers, and extensions of containment at numerous piping penetrations. The moderator area, the instrument and miscellaneous equipment rooms, and the ECC recovery room are outside the containment envelope. They are in what is known as confinement areas.

The confinement rooms around the reactor vault contain reactor auxiliaries and secondary circuits of low temperature, pressure and generally of low radioactivity level. Systems in these rooms have little stored energy, and failures of these systems would result in small integrated energy release and could result

only in limited release of activity. These confinement rooms are enclosed and ventilated in such a way that activity release from these areas can be adequately controlled.

For Pickering, the envelope is more like a single unit one; the boilers are within the containment whereas for the other multi-unit stations the boilers are not.

4.2 Design Pressures for the Containment Envelope

The containment design pressure for primary coolant system failures is selected using the Canadian National Standards series CSA-N287 recommendation that

"A containment Design Pressure that is higher than the calculated peak value of overpressure in design basis accidents, which are selected from postulated single failure and dual failure accidents of the HTS, e.g., loss-of-coolant accident (LOCA) for single failure accidents, and LOCA with coincident unavailability of the Emergency Core Cooling System (LOCA+LOECC), for dual failure accidents."

In some cases this may result in release of radioactive isotopes from failed fuel into the containment.

The acceptance criteria for the stress analysis is that no through cracks develop in the concrete walls of the containment.

The envelope must withstand the higher pressures of a secondary side coolant system failures, such as a steam line break (SLB) within a containment. This accident has no significant release of radioactivity into the containment provided that there are not a significant number of failed fuel elements in the core and that most of the boiler tubes are sound.

In CANDU reactors, fuel failure during normal operation is rapidly identified, and the failed fuel is replaced by new fuel. Leakage of the heavy water primary coolant in a boiler into the light water secondary coolant through a crack in a boiler tube is carefully monitored also. When the leakage rate is great enough that the failed tube can be found, the reactor is shut down and the tube plugged. This operating requirement also evolved from an economic penalty associated with heavy water losses from the primary coolant circuit.

In addition, the fuelling machine is supplied with environmentally qualified backup cooling for the SLB case, so there will also be no releases from the fuel handling system.

Therefore the containment envelope has a second, much higher design pressure than the CSA recommended design pressure. With this design pressure the containment structure is stress analyzed to assure that the containment remains structurally sound after a SLB accident, to prevent damage to the contained reactor system.

The CANDU 6 containment design calculations assumed an initial containment atmosphere pressure of -0.3 kPa(g). In the present conditions of the Point Lepreau CANDU 6 at normal reactor operation the containment pressure is slightly reduced and is controlled at an average pressure of -0.5 kPa(g), with an alarm set point of -0.8 kPa(g).

The pressure in the reactor vaults of multi-unit CANDU containments during normal reactor operation is about -3 kPa(g) and a stronger vacuum in the vacuum building. This small negative pressure is easily maintained by a small purge fan on the vapour recovery units.

In Pickering the pressure relief duct is normally at atmospheric pressure, while in Bruce and Darlington it is at nearly the same pressure as the reactor vaults. After a pressurizing accident the vacuum in the vacuum building helps to reduce the positive peak pressure in the reactor buildings.

All systems and equipment in CANDU reactors whose failure can result in a loss-of-coolant accident (LOCA) are qualified to a design basis earthquake (DBE), and so the combination of LOCA and DBE are not considered in the design of CANDU containment structures. However, a slightly increased pressure load is considered based on possible rupture of non-seismically qualified systems and components.

The containment envelope structures are seismically qualified such that the pressure retaining integrity is not impaired during or following a design basis earthquake.

4.3 Liner for Leakage Reduction

Low leakage of a pressurized containment atmosphere through the perimeter walls of the reinforced concrete containment structure is required for minimizing the release of radioactive gases and vapours following and accident.

The initial leakage rates of intact, buttoned-up containments of CANDU 6 nuclear generating stations pressurized to the design pressure are typically:

Leakage rate (design target)	0.1 %volume/day
Leakage rate (safety analysis value)	0.5 %volume/day

For the Darlington multi-unit containment at design pressure

Leakage rate (design target)	0.5 %volume/hour
Leakage rate (safety analysis value)	2.0 %volume/hour.

With aging of the containment structure the leakage rates are likely to increase very slowly.

In the early CANDU power reactors, like Douglas Point and Pickering-A, the inside surface of the perimeter walls was bare concrete. In later reactors a liner was applied on the floors, inside surfaces of the walls and ceiling of a

containment envelope to reduce the leakage through hairline cracks in the concrete exterior walls, prevent downgrading of D_2O and aid the post-accident decontamination.

For the CANDU 6 reactors operating in Canada a polyurethane liner was developed in the late 1980s. It has been demonstrated that even partial recoatings could significantly reduce the leakage rates.

On surfaces which may be subject to wear, such as the spent fuel transfer canal and the spent fuel storage bay, a fibreglass reinforced epoxy liner is used.

In Bruce and Darlington the concrete containment envelope is steel-lined everywhere, except in the pressure relief valve manifold and above the bottom 6.5 m of the perimeter structure of the vacuum building. Wherever the liner is stainless-steel it needs no further attention. Where the liner is carbon-steel it is coated with a coal-tar-epoxy layer for corrosion protection.

A steel-liner is also useful as part of the formwork for pouring the concrete structures. In containment structural analysis the steel-liner is not credited as a load carrying component.

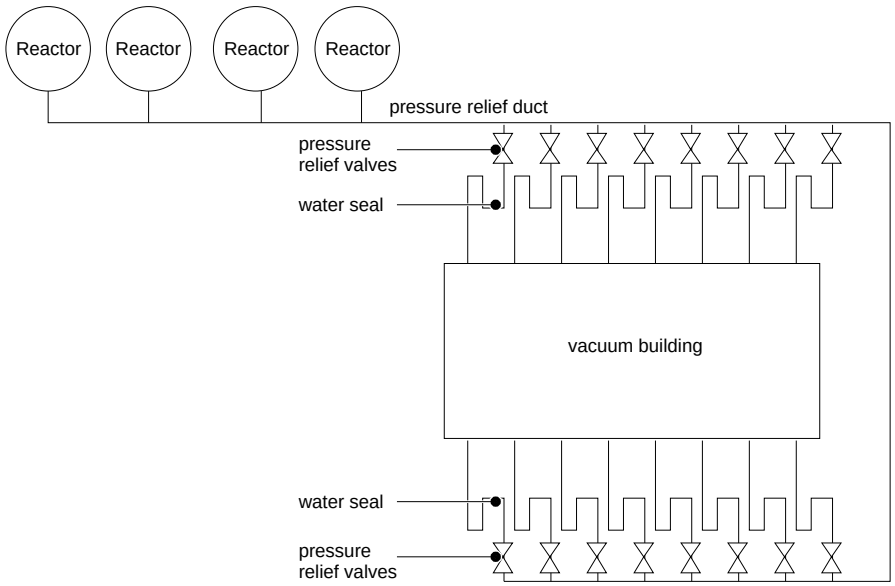
Special care is taken at embedded parts and joints between the various reactor building sections. At construction joints of the concrete walls and at embedded parts interrupting the containment surfaces a polysulphide rubber sealant is used.

4.4 Multi-unit CANDU Pressure Relief System

In a multi-unit nuclear generating station the pressure relief valves connect the accident vault volume with the vacuum building through the pressure relief duct. During normal operation there is vacuum in the vacuum building and a slightly subatmospheric pressure in the duct and reactor vaults. Isolation is provided between the vacuum building and the pressure relief duct by pressure relief valves. An accident in a reactor vault increases the pressure in the relief duct and the valves open automatically. They are self-powered by the pressure differential between the pressure relief duct and the vacuum building. The relief valves are connected to the vacuum building by u-shaped ducts which can be flooded with water for valve maintenance. Figure 4 gives a very simplified view of the system.

Figure 4

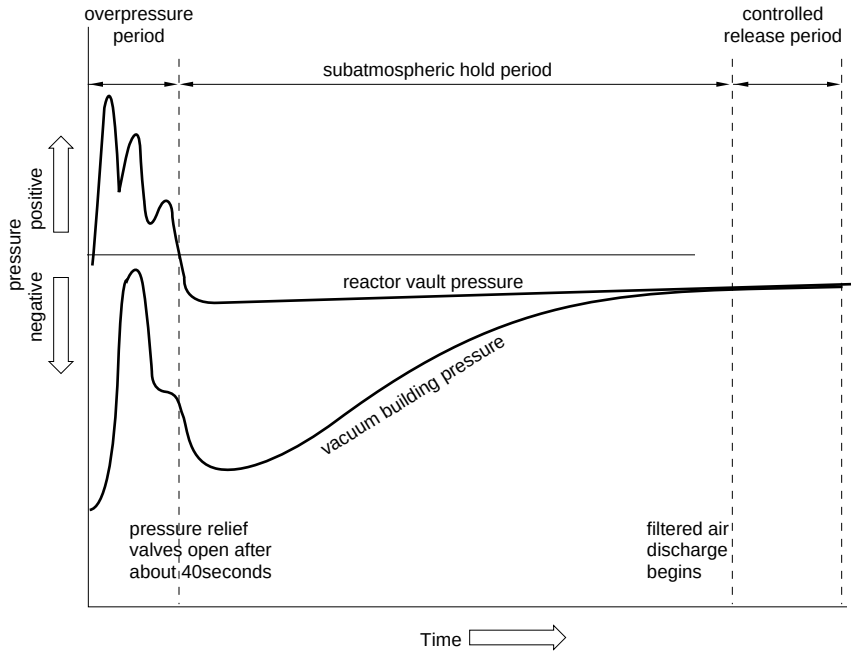
Simplified Containment Layout for Multi-Unit Stations



The opening of the pressure relief valves suddenly enlarges the available volume in the containment envelope by the vacuum building volume, and also the previous large negative pressure in the vacuum building reduces the accidental pressure rise. Thus, the reactor vault pressure drops, and the vacuum building pressure increases. This is illustrated in Figure 5.

Figure 5

Containment Pressure Following a LOCA



4.4.1 Pressure Relief Duct

In Pickering the reactor buildings are separated from the duct by blow-out panels so that they are isolated from reverse pressurization from the pressure relief duct.

In Bruce and Darlington all reactor vaults are always open to the pressure relief duct. Each reactor vault can be sealed off at the fuelling machine openings in the vault floor with a temporary bulkhead for the during a long maintenance outage. Installation of a leak tight bulkhead, once the reactor is shut down, cooled and placed in a guaranteed shutdown state, permits the vault to be separated from the remainder of the containment envelope without interfering with the operation of the rest of the containment system or the fuelling machines. Then the isolated reactor vault can be pressure and leak rate tested.

4.4.2 Pressure Relief Valves

Pressure relief valves keep the pressure in the reactor buildings within design limits following an accident. These valves provide isolation or connection between the vacuum building and the rest of the containment. The valves are closed during normal operation and open on increasing pressure differential. At Pickering, they are in the pressure relief duct. At the other multi-unit stations they are in a manifold.

In Bruce-B, there are 22 pressure relief valves arranged in two banks of 11. In each bank there 6 main pressure relief valves, 2 instrumented main pressure relief valves, 2 power-operated auxiliary pressure relief valves and a reverse flow valve. Some valves are instrumented and controlled to hold them open and thus quickly bring the reactor vault pressure below atmospheric and hold it there.

A metal grid separates the valve banks to two work areas. This is to assure that a common mode error could not disable an unacceptable number of valves.

The power-operated auxiliary pressure relief valves and instrumented main pressure relief valves are automatically controlled to maintain the containment at a slightly negative pressure following a pressurizing accident. (These valves have a manual override capability.)

The operation of the valves is summarized in this table. The pressures are in kPa(g) except where noted.

Auxiliary Valves			Instrumented Main Valves			Main Valves	
Open	Close	Modulate	Open	Close	Modulate	Open	Close
1.5			6.9			6.9	
	-6.5			-2			2.4
		*-3.5 and -6.5			-1 and -2		

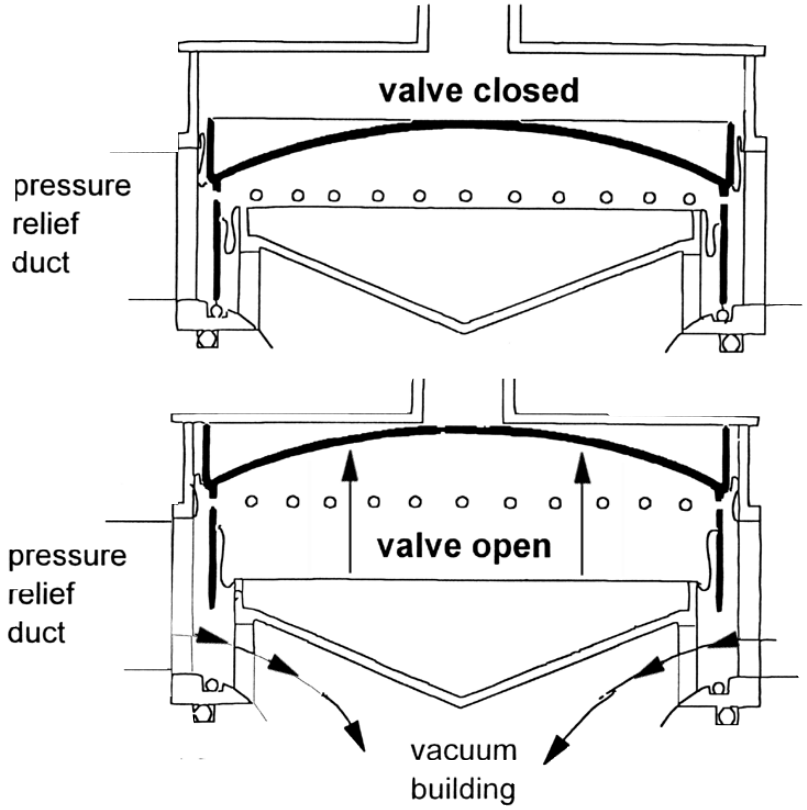
*Note: open and close for reverse flow;
open on 6.5 and close on 3.5 kPa(d)

The auxiliary valves, which are operated pneumatically, open when the pressure on the valve manifold rises to 1.5 kPa(g), reclose when the valve manifold pressure drops to -6.5 kPa(g), and then modulate to control the valve manifold pressure between -3.5 kPa(g) and -6.5 kPa(g). They also open for reverse flow on a reverse pressure differential of 6.5 kPa(d) between the vacuum building and the pressure relief manifold and reclose at 3.5 kPa(d).

If the containment pressure continues to rise, the main and instrumented pressure relief valves will open at a valve manifold pressure of 6.9 kPa(g). The main valves will reclose when the manifold pressure will drop below 2.4 kPa(g), and the instrumented valves close when the manifold pressure drops to -2 kPa(g). The instrumented valves will reopen at -1 kPa(g) and reclose at -2 kPa(g) manifold pressure if required to assist the auxiliary pressure relief valves.

Figure 6 shows a closed and an open Pickering pressure relief valve. The valves have a vertically moving piston which is sealed to the stationary upper casing and lower conical section by upper and lower rolling diaphragms. With the valve closed the volume inside the piston is vented to the pressure relief valve manifold. The conical section and the lower diaphragm isolate the piston from the vacuum duct/pipe. When the pressure under the top of the piston increases sufficiently to overcome its weight, the piston rises off its seat, venting the manifold into the vacuum building through the vacuum ducts. The air above the piston is vented to atmospheric pressure.

Figure 6
Pressure Relief Valve Basics



The diaphragms are flexible, reinforced, elastomeric elements, which are free to roll without sliding as the piston rises. All the elastomeric components of the valve can be inspected readily and are replaceable.

The pressure relief valves are seismically qualified so remain closed during a design basis earthquake, and remain functional after the earthquake.

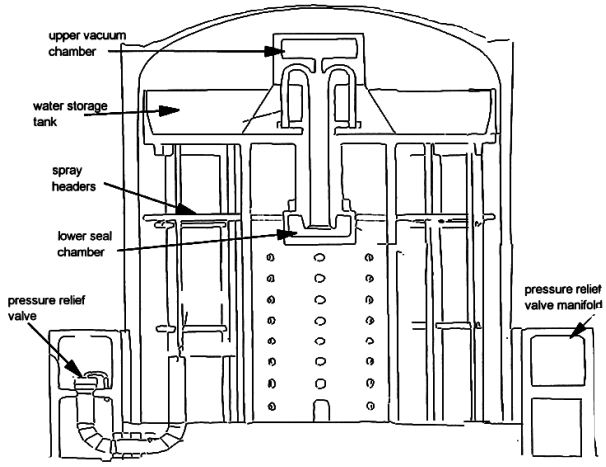
The vacuum ducts are large diameter pipes from the vacuum building-side of the pressure relief valves to the vacuum building. They are U-shaped so that isolation of any duct for testing, removal or servicing of a relief valve can be effected by flooding with water. This will provide a water seal between the manifold and the vacuum building.

The pressure relief valves can be tested without shutting down the reactor, because the valves are sized such that they are not all required to be operational at the same time.

Over the vacuum duct exit of each instrumented pressure relief valve and auxiliary pressure relief valve an elevated cover is provided, to prevent the dousing water from the spray headers to flood the vacuum duct.

4.4.3 Vacuum Building

Figure 7
Vacuum Building Design



In each multi-unit CANDU nuclear generating stations a vacuum building provides a means of rapid depressurization of pressurized containment buildings. In Bruce and in Darlington the pressure in a vacuum building is normally maintained between 6.9 and 13.8 kPa(a). (To assure a negative pressure containment everywhere, the rest of the containment envelope is normally kept at a slight subatmospheric pressure of -3 kPa(g).

In the Darlington vacuum building design the free volume of the vacuum structure main chamber is 95,000 m^3 and is sized to ensure the containment design pressure is not exceeded under postulated accident scenarios. The upper chamber volume is 275 m^3 and is sized to limit the dousing water cover gas compression effects in the central passage of the dousing system at the onset of dousing, and to reduce dousing flow pulsations subsequently.

The main chamber of the Darlington vacuum building is maintained at a pressure of 6.9 kPa absolute and the upper chamber at 3.45 kPa absolute. Three vacuum pumps operating in parallel can pump down the main chamber from atmospheric pressure to normal operating pressure in 24 hours. In the event of a loss of coolant accident the vacuum pumps are shut down and their isolation valves closed.

4.5 Dousing System

A dousing system is part of all Canadian nuclear plants. It is automatically initiated by high ambient pressures.

The dousing spray system is provided:

- to reduce the duration of the pressure excursion after a primary heat transport system LOCA and a main Steam Line Break (SLB) of the secondary-side cooling system within the containment.
- to reduce the peak pressure (this can be achieved only if the dousing occurs before the peak pressure is reached).
- to wash out as much as possible the water soluble radionuclides, eg iodine and cesium from the containment atmosphere.

In a CANDU 6 containment, a reinforced concrete emergency water storage tank is located in the dome of the reactor building. The tank holds enough water for dousing (1468 m^3) and emergency core cooling (500 m^3). The water volume available for dousing is sized by the requirement that at the end of a primary LOCA, the dousing spray will have reduced the containment pressure to 35 kPa(g). Separation is achieved by placing the inlet of the dousing downcomers above the bottom of the tank.

The top of the tank is open and the H_2O vapour-laden air space above the tank is separated from the reactor building atmosphere by a plastic membrane so as to prevent downgrading of heavy water.

The temperature of the water is held below 28°C by heat exchangers cooled by chilled water.

The spray headers are independently connected to the tank. To minimize the likelihood of spurious dousing, two series-connected, fail-closed valves are provided for each header.

These are independently controlled, normally closed, electrical-pneumatic or all pneumatic-powered butterfly valves. They open or close according to containment pressure signals.

Four of the six spray units are required to produce the design flow of 4540 kg/s used for containment accident analysis. The flow of the dousing water stops if there is no demand, or when the dousing tank is exhausted.

There is diversification not only in the method of valve actuation, but also in the control instrumentation. The spray units are divided into two groups of three. The valves on one of these dousing groups is controlled by pneumatic instruments which do not require electrical power and the valves on the other dousing group controlled by electro-pneumatic instruments. Thus the dousing system is divided into two dousing systems which are independent. The valves and instruments are of different designs, supplied by different manufacturers. Each dousing valve is controlled by an independent monitoring and logic system.

The single-unit dousing systems are active safety systems, in the sense that air and electrical power are used to activate two butterfly valves in each dousing downcomer automatically on containment high pressure trip signal. It is necessary that the dousing system continue to be operationally ready during loss of normal air supply. For that reason separate local air storage tanks are provided for the dousing valve actuators as well as the pneumatic control logic. The water flow from the dousing tank to the spray header is gravity-fed.

The dousing spray system is automatically initiated at a containment pressure of 14 kPa(g) and shut off automatically when the pressure is reduced to 7 kPa(g). This allows efficient utilization of the dousing water by cyclic usage when the pressures are too high. The dousing is initiated in 5 seconds. This time is made up as follows:

Sensing and logic operation	0.5 s
Opening stroke of dousing valves	2.25 s
Flow build up to 100%	2.25 s

The closing stroke of the dousing valves takes 7 seconds. The quantity of water for dousing is limited to that stored in the dousing tank.

The wetted surfaces of the tank and the outer dome are lined with fibreglass reinforced epoxy. The undersurface of the dousing tank is epoxy painted.

In multi-unit stations the dousing system is passive and is situated in the vacuum building. On reaching the dousing initiation pressure in the vacuum building, the dousing is initiated passively.

The flow of water from the storage tank is automatically started or stopped without external power supplies. Once a pressure differential between a vacuum chamber and the incoming accidental pressure exceeds the initiation limit, the water level (due to the differential pressure) rises and starts to flow over a weir into a downcomer and from there to spray headers. Thereafter the water is syphoned from the storage tank, unless the pressure in the vacuum building drops below a spray shut-off set point.

The water in the dousing tank is treated by chemicals and is recirculated to prevent freezing.

In Darlington the storage tank has a total capacity of 11,500 m^3, 10,000 m^3 of which is available for dousing.

To ensure optimum use of the dousing water, the dousing spray automatically cycles on and off depending on the pressures. For instance, after a small LOCA the demand is quite different than after a large LOCA. In Darlington once the containment goes subatmospheric (40 kPa vacuum) the pressure relief valves close and shortly after that the dousing will stop. The dousing can restart on demand, and continue until the dousing water is exhausted.

4.6 Reactor Building and Vault Local Air Coolers

A cooling system for the containment atmosphere is required:

- to supplement the dousing system's heat sink capacity after a LOCA;
- to limit the ambient air temperature to typically 41°C in the inaccessible areas so that heat will not damage the concrete walls of the building or the equipment.
- to limit the air temperature in the accessible areas to a level where work can be performed comfortably.

In a CANDU 6 reactor building there are 35 local air coolers (LAC): 19 smaller ones are provided for steady use (e.g., in the moderator enclosure, fuelling machine auxiliaries room, instrumentation transmitters room, etc.), and 16 larger ones for cooling the atmosphere after pressurizing accidents primarily (e.g., in the fuelling machine vaults and the steam generator/boiler room). High reactor building pressure from the containment isolation logic starts up all of the LAC.

The smaller LAC are supplied from Class 4 power, but the larger ones are backed up by Class 3. Their fans, the recirculated cooling water (RCW) pumps and the service water pumps outside the containment are also on Class 3. The heat exchangers between RCW and service water are outside containment. To minimize a common mode failure of LAC, separate circuits and physical separations are provided.

Standby LAC are switched on automatically by the containment isolation logic to give the greatest possible cooling capacity. The LAC control switches have "off-normal" monitoring to ensure that local air coolers are normally in an "auto" or "on" condition.

The reactor building safety related local air coolers are credited as a continuously operating heat sinks for postulated loss-of-coolant accidents.

4.7 Airlocks and Containment Penetrations and Containment Isolation

Those systems which have the potential for significant release of radioactivity need be located within the containment envelope. Where possible, services for these systems are located in accessible areas outside containment for ease of maintenance and lower radiation exposure of operating staff.

Penetrations through the reactor building wall are required for personnel airlocks, for equipment ports and hatches, steam and feedwater systems, services such as cooling water, air, ventilation, heavy water recovery and collection, sampling systems and electrical cables. In CANDU 6, the heat transport system coolant piping does not penetrate the walls of the containment building. In the CANDU 6 containment, the boilers are inside the containment and the secondary circuit piping penetrates the containment wall. The secondary components which penetrate the containment wall may carry some radioactivity if there is a tube break in the steam generators. Secondary-side

pipe breaks, such as a steam main break, or a secondary system valve malfunction outside the containment building still do not represent radiological hazards, if the primary-to-secondary coolant system barriers remain intact.

The containment penetrations are seismically qualified so that leakage from containment to the outside atmosphere is not increased in the event of a design basis earthquake.

In a CANDU 6 containment building there are two airlock penetrations, one for equipment and one for personnel and about 140 penetrations for pipes and instrument lines and electrical cables. The airlocks are manually operated, but need an air supply to do so. Without the air supply the seals around the airlock ports would be deflated and may present a leakage path. Normally one door of an airlock is closed, and it may be opened only after the other door is closed. Deviation from this procedure causes a partially or fully open airlock and is a containment impairment.

In the Pickering-A containment envelope there were only 250 penetrations. In the Darlington containment envelope there are 1000 penetrations.

In Pickering each reactor building is separated from the pressure relief duct with damper-like shutters which permit outflow from the reactor building but not inflow. These dampers do not provide airtight seals. In the Bruce and Darlington multi-unit reactors the reactor vaults are open to the pressure relief duct.

There are two types of piping penetrations; those for "open" and those for "closed" systems. Open systems are connected to the containment environment, an example is the reactor building ventilation system. Open penetrations are automatically isolated by the containment isolation system by means of two redundant valves in series. Closed systems are those that are closed to the containment environment either by means of a normally closed valve or inherently by means of a closed piping loop. An example of a closed system is the CANDU 6 recirculating cooling water system. Closed systems are generally provided with an isolation valve at each penetration. However, they do not require automatic isolation on demand as at least one physical barrier is continuously available.

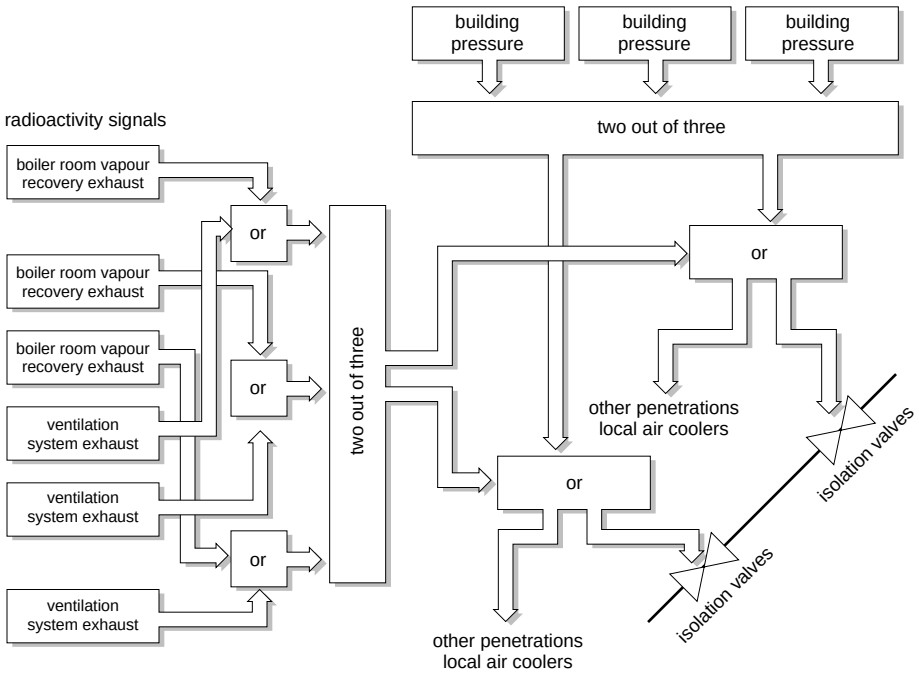
Isolation valves are also provided on the inlet and outlet of ventilation systems.

Most containment isolation valves are located outside of the reactor envelope. This provides the advantage of accessibility at power or during accident conditions for maintenance, testing or valve position verification. To be fail safe, the containment isolation valves all fail closed.

Automatic containment isolation is initiated when the reactor building pressure exceeds a selected pressure limit (for CANDU 6 this is 3.5 kPa(g)) or on high

radioactivity signals which are detected in either the ventilation exhaust from the reactor building or the steam generator room vapour recovery system exhaust. A block diagram for a typical automatic isolation control loop is shown in Figure 8.

Figure 8
Automatic isolation block diagram



The containment isolation system instrumentation and control loops follows the CANDU safety practice of triplication of measuring signals and control by two-out-of-three voting logic.

4.8 Filtered Air Discharge and Emergency Filtered Air Discharge

A number of systems and design measures are provided in order to limit the maximum value and duration of internal overpressure on the containment structure.

After a loss-of-coolant accident heat removal from the containment atmosphere is achieved by dousing, local air coolers and condensation on concrete and metal surfaces. One action to be taken to minimize the long-term overpressure transient is to isolate the inflow of instrument air. A review of the instrument air loads within the reactor building has shown that the instrument air can be isolated a few hours after a loss-of-coolant accident without affecting the ability to maintain the plant in a safe shutdown state.

During normal reactor operation the containment atmosphere in a CANDU 6 containment building is ventilated, and air is exhausted through a filtered air discharge (FAD) system. This system uses the D_2O vapour recovery driers and

the filters of the ventilation system. The exhaust flows are passed through both absolute and charcoal filters to remove particulates and iodine. A small exhaust flow from the vapour recovery driers is directed to the same exhaust fans. Any small releases are constantly monitored. The ventilation system is isolated in the event of an accident. The FAD system is not intended for emergency conditions, and may not be credited for analyzing accident conditions, because the filters may loose their efficiency with high pressure loads, with much fission product deposition, moisture, clogging and overheating. Neither the filters, nor the roughly 50 m tall ventilation stack are designed to handle the quantity of fission products in the containment atmosphere after some accident scenarios.

In all the multi-unit CANDU containments an Emergency Filtered Air Discharge (EFAD) system can be used to reduce the containment atmosphere pressure in the long term following a loss of coolant accident or a design basis earthquake.

During normal plant operation in Pickering, the reactor building ventilation system for each reactor building discharges through HEPA filters sized to remove relatively low activity iodine. They do not remove tritium or noble gases. The ventilated air exits through the stack.

On high activity or high containment pressure, the containment, including the ventilation system, is buttoned up.

The EFAD is credited in some safety analysis scenarios. The EFAD system provides a well defined, filtered and monitored pathway to the environment. EFAD operation is initiated by the reactor operators to maintain the containment pressure subatmospheric in the long term, and to allow a controlled and monitored release of fission products from the containment. It provides some flexibility for planning when discharges are made and thus can provide time to arrange any contingency planning that may be required or to take advantage of favourable weather conditions. Its components are automatically controlled during long-term post-LOCA operation. It can draw on either the pressure relief duct or the vacuum building.

The EFAD system consists of two x 100 percent filters, each containing a demister, heater, prefilter, upstream HEPA filter, charcoal filter and downstream HEPA filter. It can maintain the containment pressure between 0.25 to 1.0 kPa below atmospheric. The system connections to containment have normally closed isolating points. The system exhausts the through its own exhaust stack.

4.9 Post-accident Hydrogen Control

Under some postulated accidents such as LOCA coincident with LOECC (Loss Of ECC), or large LOCA with flow stagnation in the core, large amounts of hydrogen/deuterium can be generated by the reaction of zirconium with steam. In other accidents radiolytic hydrogen generation may be important. The hydrogen is removed in a controlled manner to prevent structural damage to the

containment envelope that might follow if the hydrogen deflagrated or detonated.

The mitigation is by recombiners and igniters. A hydrogen recombiner promotes hydrogen and oxygen reaction even at concentrations below the flammability limit. An autocatalytic hydrogen recombiner preforms the recombination without external (say, electrical) power source, using catalysts that heat up by the exothermic heat of the recombination. A hydrogen igniter ensures that on reaching the flammability limit for hydrogen in air the mixture is ignited without detonation.

Most igniters and recombiners can be "poisoned" by the presence of moderate concentrations of steam or by recombined condensed moisture. Newer recombiner devices are made with a water repellent catalyst surface.

Whether spark or glow igniters or recombiners are used the purpose is to prevent the hydrogen concentration to reach deflagration or detonation levels.

In the latest CANDU 6 reactor containments built at Wolsong, Korea, and at Cernavoda, Romania, the hydrogen control system consists of 44 glow igniters, which are distributed in the two fuelling machine vaults and in the reactor building dome area. This number of igniters ensures ignition with sufficient redundancy. During normal plant operation the igniters are not powered; on a LOCA signal the control system automatically energizes the igniters. Manual switching is also available. At power the igniters are at a surface temperature of 87°C.

In each Bruce reactor vault and fuelling machine duct 16 hydrogen igniters are provided (64 igniters per station). The electrically-powered igniters are automatically activated in the event of a pressure rise in the containment and will cause any hydrogen produced to be burned with a minimal pressure rise in the containment.

In the Darlington reactor vaults, the shutdown cooling rooms and the fuelling duct are equipped with electrical hydrogen igniters. These are activated automatically after most LOCA on high containment pressure signal, but may be activated by the operator as well.

The hydrogen control system does not require seismic qualification.

4.10 Containment Monitoring

Typically containment system monitoring includes:

Monitored Parameter	Main Control Room Indication	Alarm On
Containment atmosphere pressure	continuous	high pressure
Containment atmosphere activity	continuous	high activity
Airborne or liquid effluent activity	continuous	high activity
Dousing water level	continuous	low level
Dousing water temperature (in multi-unitstations also)	continuous	high temperature (low temperature)

Containment atmosphere high pressure or high activity signals initiate automatic isolation of the containment.

On-off status of containment local air coolers is monitored. Humidity sensors are provided for monitoring the flow streams of the vapour recovery dryers. Water level monitoring is provided for the reactor building sump.

The radiation monitoring system allows pre- and post-accident monitoring with radioisotopic analysis for noble gases, particulates and iodine. Tritium analysis and on-line gross gamma detection capability are also provided by the system. In CANDU 6 plants low range activity monitors for the airborne active effluents are downstream of the ventilation system dampers at the stack exit. In multi-unit plants I-131 concentration is measured in the inlet of the vault D_2O vapour recovery system. In-containment high range activity monitors are also provided for post-accident monitoring.

For the CANDU 6 dousing system the pressure in each air storage tank for the pneumatic dousing valve actuators is continuously monitored and an alarm is initiated whenever the pressure falls below a predetermined set point.

In multi-unit containments the pressures in and pressure differentials between the pressure relief valve manifold and vacuum building are monitored. The pressure relief valve piston is remotely indicated by a motion transmitter. The presence of unwanted water is monitored by beetles on the floor of the pressure relief duct or pressure relief valve manifold, near the pressure relief valves.

4.11 Heavy Water Vapour Recovery Air Dryers

This is a containment service system which, although not necessary for the operation of the containment system, is connected to the containment envelope.

Air drier systems are connected to the vaults, fuelling and service areas where heavy water may escape to the containment atmosphere. Each system consists of a loop from the containment proper to the dryer and back to the containment. The containment boundary is provided by redundant containment isolation dampers on both the take-off and return lines. These dampers close automatically on a containment button-up signal.

Each vapour recovery system includes a filter bank to reduce the radiation fields on the dryer beds.

In CANDU 6 stations a small amount of dried air can be exhausted from the vapour recovery dryer via the ventilation system to maintain a slight subatmospheric pressure in the containment.

In the multi-unit nuclear stations each reactor vault and fuelling duct vapour recovery system has a purge line to extract air to maintain a subatmospheric pressure during normal operation. The purge line discharges to the reactor building contaminated exhaust system.

5.0 Containment Safety Analysis Considerations

5.1 Containment Behaviour Under Postulated Accident Conditions

5.1.1 Loss-of-coolant Accidents

For small heat transport system leaks, the building coolers (LAC) condense the steam. There may be some additional outflow of air through the ventilation system. The building air temperatures rise somewhat.

If there is radioactivity accompanying the small break, the triplicated radioactivity monitors in the duct initiate a signal that causes a complete closure of the containment isolation valves.

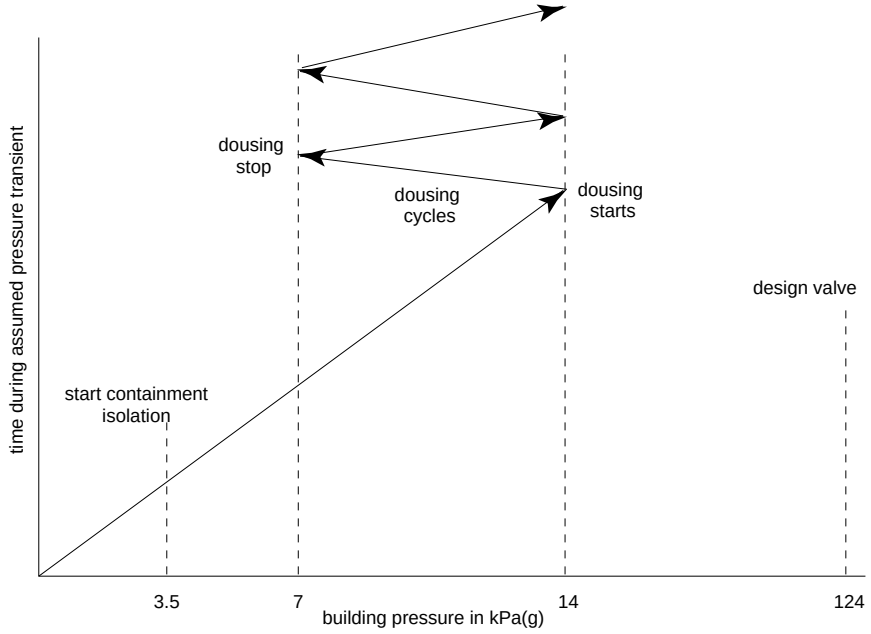
For larger breaks, building pressure rises and, unless an activity signal demands containment isolation beforehand, at an overpressure of 3.5 kPa(g), containment pressure sensors initiate containment isolation.

Figure 9 illustrates what happens.

If the containment pressure continues to rise, the dousing system will start to operate automatically at an overpressure of 14 kPa(g) and, following dousing operation, the dousing valves will re-close at an overpressure of 7 kPa(g). Depending on the size of the break, there may be a continuous or cyclic operation of the dousing valves. For any heat transport system break, overpressure is well within the design value of 124 kPa(g) for the CANDU 6 containment structure.

The next stage of depressurization of the building is effected by those building air coolers which have been designed to operate under steam/air conditions at 124 kPa(g). All air supplies to the reactor building are isolated (manual operation) within 3 hours after the loss-of-coolant accident to prevent pressurization by compressed air.

Figure 9
Dousing in ideal LOCA



The doused water collects in the reactor building basement. From there it may be recycled to the core by operation of the emergency core cooling recovery pumps. Instrumentation to indicate water level in the reactor building basement is provided.

5.1.2 Accident in a Fuelling Machine Room

If an accident involving fission product release occurs in a fuelling machine room, triplicated activity monitors in the vapour recovery system ducts isolate the containment when the high activity set point is reached. Such an accident might be caused by dropping all or part of a fuel string on the floor of the room, followed by rupture of the fuel sheaths due to high temperature or the impact on the floor. The fuelling machine room can be purged through the filtered air discharge system about 24 hours after the accident. This time is allowed for the decay of noble gases, that cannot be removed by the ventilation filters, and for a decrease in iodine activity to prevent overheating of carbon bed filters.

5.1.3 100 percent Steam Main Break Inside Containment

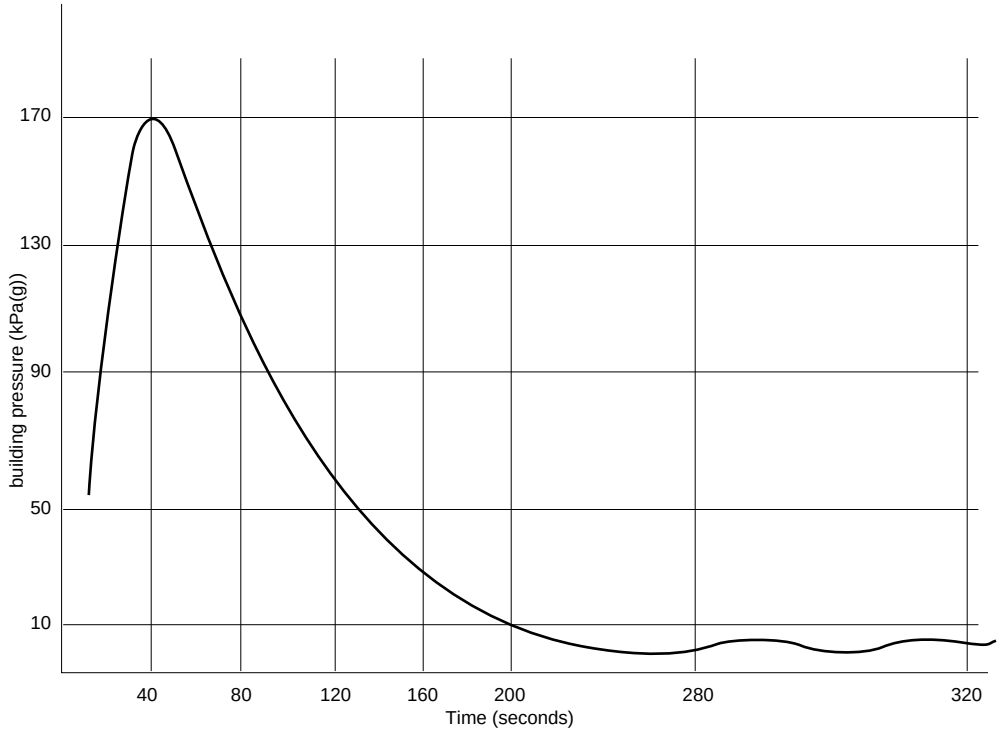
Most steam line breaks inside containment result in an early reactor trip on high reactor building pressure. For a 100 percent steam main break in a CANDU 6

containment the trip occurs at about 0.5 seconds. The analysis are limited to the pressure rise inside the containment, since the heat transport system remains intact and activity releases, if any, are not significant.

The reactor trip and increased heat transfer to the secondary circuit causes heat transport system to shrink. In a CANDU 6, at 42 seconds, HTS header pressures are all below 5.5 MPa(a) and the signal for ECC injection, HTS isolation and boiler crash cool down occur. Some ECC water would be injected into the HTS from the injection tanks, and the boiler safety valves would open 30 seconds later.

For a CANDU 6 dousing starts at 14 kPa(g). The pressure rises to about 270 kPa(a), near 38 seconds, and then decreases. Dousing reduces the building pressure to about 6.9 kPa(g) at 240 seconds, and then cycles to maintain building pressure below the on set point. Figure 10 illustrates the transient.

Figure10
Containment Pressure after steam line break



When the dousing water supply is exhausted, the pressure rises slowly until a heat balance is established with the LAC.

Steaming from the break at decay power levels continues for several hours unless the operator intervenes. The condensate extraction pumps and main feedwater pumps eventually trip on low condenser level, however the auxiliary

feedwater pump can supply up to three percent of nominal flow to the steam generators. This is sufficient to handle decay heat generation, and therefore primary circuit cooling is assured.

Alternatively the operator can initiate the shutdown cooling system in the mode which uses the shutdown cooling system pumps.

All actions can be completed from the main control room.

5.2 Initiating Events for Safety Analysis

The AECB consultative document C-6 and the earlier (1972) paper of Hurst and Boyd requires the evaluation of the effects on whole body and thyroid doses to the public of a variety of accidents.

The worst cases are selected for safety analysis of a containment. In past, safety analysis of
CANDU 6 containment, included these accidents.

- Large LOCA
- Large LOCA + Loss of emergency core cooling (LOECC)
- Small LOCA + LOECC
- End fitting failure
- Large LOCA + Loss of Class 4 power

These accidents are assumed to occur within intact containment and with combinations of specific losses of containment functions. The containment impairments may be due to a malfunction or loss of some of the containment subsystems, for instance:

- Breaches of the containment envelope;
- Loss of dousing;
- Loss of isolation;
- Loss of local air coolers (LAC),

Open airlocks are considered for large and small LOCA.

Some containment impairments are considered both as partial and total impairments. For instance, in a partial loss of isolation of the ventilation system, either the inlet or outlet lines of the ventilation system are not isolated, while in a total loss of isolation of the ventilation system, both lines remain open. Other containment impairment cases are analyzed assuming a total failure of a containment subsystem, for instance loss-of-LAC.

For evaluating significant hydrogen release the following two accident scenarios are considered:

- Dual failure accident (LOCA + LOECC);
- Single failure LOCA followed in 24 hours by site design earthquake (SDE) event.

The first leads to a considerable amount of hydrogen being generated in the first 20 minutes after a large LOCA (e.g., 100% header break). Here igniters and recombiners are needed, depending on the hydrogen distribution in the containment building. The second does not produce significant amounts of hydrogen from the zirconium-steam reaction but will cause a slow generation of hydrogen due to radiolysis. Within weeks a flammable hydrogen concentration may develop.

A design basis earthquake is not considered in the safety analysis in conjunction with primary or secondary side LOCA.

As mentioned earlier, a secondary coolant circuit large steam line break (SLB) inside the containment is also analyzed, not for radioactivity release, but for checking the integrity of the containment envelope under the larger internal pressure than there is after a primary LOCA. After an SLB the operator may open a main steam supply valve (MSSV) to relieve the pressure in the containment atmosphere via the broken steam line. This is done if there is no significant activity in the containment atmosphere.
The MSSV are also opened after a LOCA for crash cooling the heat transport system. Then, however, the secondary system is intact and therefore not communicating with the containment atmosphere.

5.3 Analysis Tools

The testing of complex accident scenarios is not feasible or practical, therefore most studies are based on analytical, evaluations. For design basis accidents the actual levels of expected damage are evaluated by deterministic calculations.

Probabilistic safety analysis, on the other hand, predict the occurrence frequency or frequency rating of different types of accidents. AECB sets the frequency limits for probable accidents within which deterministic analysis or experimental investigations are needed.

The probable frequency of the occurrence of failure of the containment system is determined approximately, based on component failure rate data if it is available or on estimates for comparable components.

The failure rate data also affects the unavailability of the containment system. Typically, the Bruce-B containment system is designed for an unavailability of less than 0.001 year/year of operation.

The CANDU containment deterministic safety analysis are performed with the following one-dimensional (unless otherwise noted) flow computer codes:

Used to analyze	Code name	Used at
Intact and breached containment flow dynamics response	- PRESCON - PATRIC - GOTHIC (3D)	AECL, HQ, PT.L. OH AECL, OH
Fission product dynamics in containment and release from containment	- SMART - FISSCON	AECL OH
Dispersal of radioactive releases outside the containment and health physics dose calculations	- PEAR	AECL, OH
Hydrogen distribution (without burning) in a containment	- GOTHIC (3D)	AECL, OH
Hydrogen-air mixture ignition, burning and detonation in a containment	- VENT - PHONICS (3D)	AECL AECL

The similar purpose codes were developed with somewhat different modelling assumptions. After careful allowances for the modelled or unmodelled phenomena, the corresponding codes may serve for some cross-checking of the analytical predictions.

The validation of the containment codes is an ongoing process. For instance, the VENT one-dimensional code has very limited validation for a three-dimensional containment configuration, but 3D modelling approaches are being developed. Ontario Hydro nuclear plants have hydrogen igniters, therefore they do not need to predict the consequences of uncontrolled hydrogen burning.

The validation of the containment analysis computer codes is performed only "by-parts" for selected phenomena, that is by checking the code predictions against some well-defined, usually single topic experiments.

For probabilistic safety assessment of the CANDU containment systems, general purpose reliability analysis codes are used (such as CAFTA at AECL and SETS at OH). The prediction of containment system unavailability is based on predicted or field data-based reliabilities of the subcomponents.

6.0 Testing of CANDU Containment

The containment system should function as a physical barrier to the release of radioactivity. The various sub-components of the containment system are tested to demonstrate the integrity of the whole system. The performance of the containment system, in whole and in its sub-systems, is tested during plant commissioning, and at intervals while it is in-service. In the commissioning

phase the testing challenges the system under conditions that can reasonably approach accident conditions. The in-service tests are more constrained, because safe plant operating or shut down conditions must be maintained during testing. The cost of the plant shutdowns gives rise to testing methods while at power. The in-service tests provide information about the current and extrapolated future state of the containment and about failure frequencies of the sub-systems for reliability analysis. From these analysis the unavailability of the overall containment system can be predicted.

The developed on-power tests and continuous monitoring ensure no sudden abnormal change of state of the containment boundary. On-line on-power testing is performed for leakage rates from a low containment pressure because this is a very important performance indicator of the containment envelope. Containment testing requiring plant outages are performed infrequently

6.1 Containment Structure Tests

Some of the test requirements are codified in Canadian standards N287.6 and N287.7.

6.1.1 Pressure Proof Test

The containment structure and all other parts of the containment boundary has to be overpressure proof tested and leakage tested before first criticality.

The positive pressure tests are performed with overpressure relief valves and the vacuum tests with vacuum breakers to protect the containment building from overloads beyond those caused by the test pressures.

Internal visual checking of concrete cracking is done during positive pressure testing, but not during vacuum testing. The containment is kept sealed up during the pressure testing, and only inspector access is allowed via an airlock; exiting inspectors are gradually depressurized to avoid effects harmful to health.

The proof pressure test is carried out at a pressure 1.15 times the design pressure. The leakage rate is measured immediately after the pressure proof test at the design pressure.

6.1.2 Leakage Rate Tests

The concrete containment of each CANDU nuclear power plant is tested during commissioning to determine the leakage rate during incremental pressurization to and at the positive design pressure. . A similar test procedure is performed for leakage rate during incremental evacuation to and at the negative design pressure.

To protect the containment structure during these tests the pressurization or depressurization rate usually does not exceed 14 kPa/hr. Also, special care is

taken to avoid over pressurization. No visual inspection is done in the containment building during leakage rate tests.

In a multi-unit plant, the units are brought into service sequentially with pre-operational isolation bulkheads installed to facilitate pressure testing.

The AECB Regulatory Requirements R-7 identifies the test acceptance leakage rates for a buttoned-up containment (for practical purposes it is the design leak rate) and the maximum allowable leak rates.

The acceptance value of leakage rate of a new containment should be below the commissioning target value, which must be less than that accepted for normal plant operation, which in turn must be less than that used in the safety analysis.

Qualitative measurements of leak rate include:

- trending the containment pressure versus time is the most basic method of measuring leakage. An abrupt change in containment integrity status may be diagnosed from the pressure trend or from a high containment pressure alarm. This method for containment leakage indication is fraught with uncertainties caused by factors such as ventilation system operation and open airlocks.
- observation of the bubbling of a soap emulsion applied to the external surfaces of a pressurized containment building. This will show where the leak paths are.
- ultrasonic detectors can be used to find defects in the internal liner or other places where leakage paths are likely to be found.

Quantitative leak rates can be calculated using the Canadian standards recommended classical method of "absolute" leakage rate calculation which is based on a mass balance. This simple mass plot method of leak rate analysis calculates the containment air pressure from measured pressures and temperatures:

$$P_{air} = P_{total} - P_{water\ vapour}$$
$$= P_{atmospheric} + P_{difference\ from\ atmospheric} - P_{water\ vapour}$$

and then the contained air mass from the ideal gas law for air:

$$M = (P_{air} \times V) / (R \times Temp)$$

where M is the air mass;
R is the gas constant for the air
V is the containment free volume, which during commissioning allows for any still unsealed tank or piping system air space as well.

The leakage rate (LR) is the slope of the mass vs time line fitted by linear regression to the mass versus time data:

$$LR = dM/dt\ [kg/hour]$$

A few other methods for determining the leakage rates are also accepted by AECB. Newer methods have to be validated and their accuracy calibrated either against the classical "absolute" mass balance based leakage rate determinations, or against an artificially created "known" leakage rate of magnitude comparable to the "unknown" leak rate measurement.

In most of the CANDU 6 containments and in the multi-unit CANDU containments low containment pressure leakage rate tests are performed with one of following two types of tests.

In a single-unit containment or in a unitized containment of a multi-unit plant (like Pickering) the leakage test is started from their slightly negative normal operating pressure. The instrument air in-leakage (for operation of control valves) gradually builds up the containment pressure with the airlocks and ventilation dampers closed. The rate of containment pressurization over several hours indicates the leakage rates.

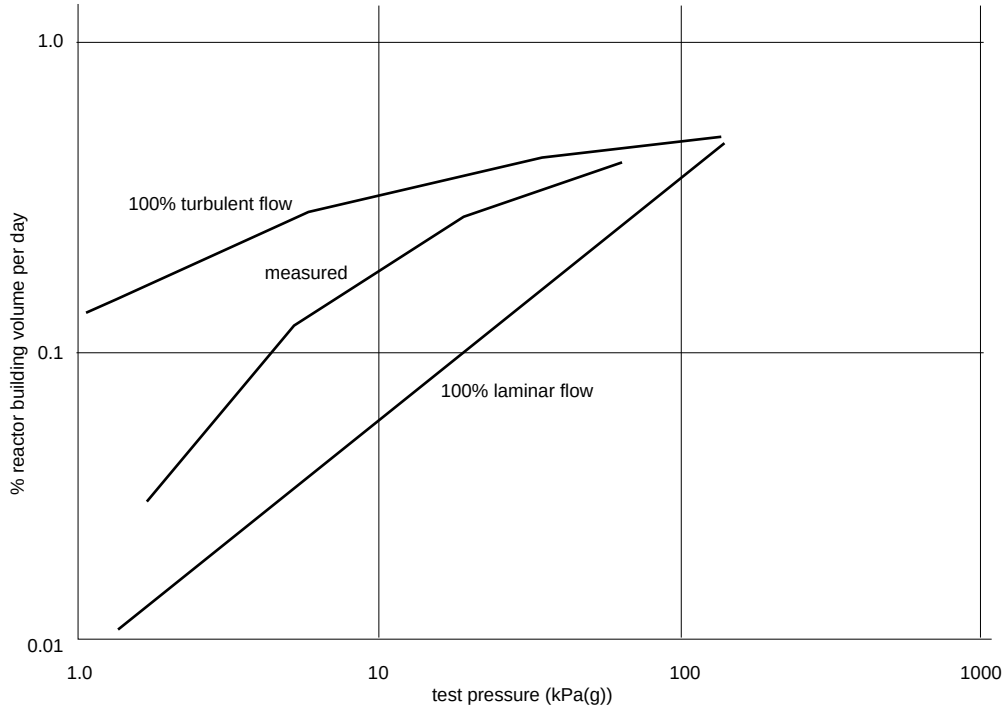
In CANDU 6 such an on-power low-pressure gross leakage rate test starts with a containment pressure of -1 kPa(g) and ends when the containment is pressurized to +1 kPa(g). The test takes about 1 to 1.5 days to perform and it takes about another day to analyze the leak rate measurements. The method is capable of identifying leaks of an equivalent hole size of 3 cm or larger.

In the multi-unit plants the vacuum building is used to draw all the reactor buildings and associated ducts significantly below atmospheric pressure in a controlled manner via an auxiliary pressure relief valve. Once at the test pressure of -15 kPa(g), the leakage rate analysis is performed with the measured instrument air in-leakage subtracted.

Since 1987 Hydro Quebec has used an on-line leak detection system with a Temperature Compensation Method (TCM) for the Gentilly-2 CANDU 6 containment building, that can be used at low or high containment pressures. It has a higher accuracy than the method used for the other CANDU 6 containments and the tests can be performed in a shorter time than with the other test methods.

On-line, on-power leak rate measurements at low containment pressures can already indicate changes in the condition of the containment building, and it is possible to extrapolate the low pressure measurements to the leak rate of the containment building at the design pressure. Unfortunately this extrapolation is nonlinear, as can be seen from Figure 11. At lower test pressures the leak rate through a given hole is near the laminar flow rates while at higher test pressures the leak rate is near the turbulent flow rates through the same hole.

Figure 11
Laminar, Turbulent and Measured Leak Rates



6.1.3 Test Frequencies

The current requirements for testing are set out in the AECB Regulatory Document R-7. They are:

- Clause 4.2.2(a): "A leakage rate test shall be carried out at full design pressure at least once every three years to demonstrate that the measured leakage rate is not greater than the maximum allowable leakage rate. If the measured leakage rate is in excess of the test acceptance leakage rate, the frequency of such tests shall be increased to once every two years"
- Clause 4.2.2(b): "A Leakage rate test shall be carried out at a frequency of not less than once per two years to demonstrate that the leakage rate is not greater than the maximum allowable leakage rate."

Clause 4.2.2 also states that the leakage rate tests can also be carried out at reduced or negative pressures. However, a leakage rate test at full design pressure must be done a minimum of once every six years in any case.

The test frequency is agreed upon between the owner and the AECB.

The testing of the in-service CANDU containment is done periodically at a positive pressure during reactor shutdowns. To provide assurance of leak tightness between outages supplemental on-power low positive or negative pressure tests are done. The relationship between these additional tests and the positive pressure tests has to be demonstrated.

In the vacuum building of each multi-unit plant the in-leakage rate is checked every week from the operating record of the vacuum pumps.

The in-service pressure proof testing of the structural integrity at 1.15 times the containment design pressure is done very infrequently, because each pressurization beyond the design pressure may induce additional crack formation and growth of previously present cracks in the aging concrete walls of the containment. CAN/CSA-N287.7 standard recommends that accessible components of a containment structure shall be visually inspected or pressure tested at least every 5 years. For non-accessible components such as the vacuum building the AECB sets the testing frequency.

For multi-unit containment, 20% per year of the containment may be tested for structural integrity, using an inspection programme approved by the AECB. The vacuum building pressure proof test is repeated every 10 years.

6.2 Containment Isolation Tests

All containment access closure seals and process pipe penetration isolations are tested or inspected periodically. Complete containment isolation test is done on a monthly basis. However, the isolation logic including the pressure and radiation monitors and isolation valve operability are tested more frequently, typically on a weekly or bi-weekly basis.

Caution must be exercised when containment closure is in effect for more than a few minutes. Building temperature changes may cause pressure changes which can cause damage to external portions of the ventilation system if the ventilation dampers are reopened suddenly.

The leak tightness of the ventilation dampers are checked periodically. This is done by pressurizing the interspace between closed dampers and measuring the pressure rundown.

The interspace between the automatic isolation dampers can be tested for leak tightness, separately for each pair of dampers.

Individual test points are provided at the special seals of some penetrations. These are checked on a regular basis. The electric cable penetrations are be tested individually by pressurizing the interspace between the primary and secondary seals. Most of the process piping penetrations are not testable individually, except by ultrasonic detectors during a reactor shutdown with a pressurized containment.

The multi-unit containment pressure relief valves are tested by flooding its corresponding water seal, closing the vent line, and connecting the valve to a vacuum source, which will lift the valve off its seat.

The airlocks are pressurized with both doors closed and the pressure rundown is measured. Airlock seals, penetrations, etc. are also periodically checked by visual inspection. These inspections search for incipient failures that may not yet be evident in the other tests. The main airlock equipment doors and the emergency airlock doors are operated about once a month so as to provide a functional test. The main airlock personnel doors are operated routinely.

6.3 Dousing System Tests

In CANDU 6 plants monthly in-service testing is performed on each of the 12 dousing valves. The valves are tested remotely, one at a time, by an automatic sequencer. Normally, there is no water between the two valves of a dousing downcomer, and if there is it will flow from that inter-valve space into a drain line. The presence of abnormal water in the drain line signals an alarm to the reactor operators in the control room.

For each downcomer, the bottom valve is opened first, its opening time measured, and when fully opened a limit switch initiates its automatic closing. If the valve does not open fully, then a delayed timer switch recloses the valve. Subsequently, a similar test is performed in the upper valve of the downcomer, but here the dousing water will enter the space between the two valves and will flow to a drain line. The arrival time of water is measured. Here again the upper valve is automatically reclosed. These dousing valve tests are performed by the operator in the control room with the reactor at full power.

Annually, during a shutdown, all components of the dousing system are tested or inspected. The spray nozzles have relatively large orifices such that occasional visual inspection is all that is required. The dousing tank vapour barrier is also inspected at these yearly shutdowns. The barrier is replaced if deterioration is observed.

The dousing system of a multi-unit plant is not a poised system, but is a continuously operating system. The water to the dousing tanks is circulated for chemistry and temperature controls and these are continuously monitored. The vacuum in the main chamber of vacuum building and in the upper chamber of the dousing system are continuously monitored to check that the vacuum pumps are operating or if not that the back-up vacuum pumps started to operate. The water level in the dousing tank is monitored continuously, and also water on the floor of the vacuum building provides alarm for the reactor operators.

In multi-unit plants the entire dousing system's operation is tested once every 10 years. The vacuum building's pressure is increased by letting in atmospheric pressure air through the instrumented pressure relief valves. A douse occurs when the pressure difference between the main chamber of the vacuum building and the upper chamber of the dousing system reaches the dousing initiation

level. For this event additional instrumentation is provided to test the dousing patterns, droplet size distributions, dousing times, etc. This testing is done during a station outage for containment inspection.

7.0 Operational Experience with CANDU Containment Systems

During the pre-operational proof pressure tests, hairline cracks were observed on the inside walls of the reactor buildings. An intensive study was carried out with the conclusion that the cause of cracking was the presence of additional tensile stresses induced in the concrete surface layers by a higher rate of shrinkage in these layers than in the concrete core. The crack pattern or density was influenced by non-uniformities present in the reactor building wall, such as embedded parts, buttresses, permanent openings, etc. The presence of these cracks was found to have minimal effects on the ability of the reactor building wall to fulfill its structural and leak tightness requirements.

Up to 1993 no containment system has been called into use ie there have been no feeder or header break or pump inlet or outlet breaks in the primary heat transport system, nor large pipe breaks in the containment on the secondary side coolant circuit. There have been some pressure tube and associated calandria tube failures, and significant leaks at the fuelling machine to end fitting joint due to fuelling machine faults. There have been a few occasions of fuel bundles overheating and the release of activity into the containment. Also moderator and cover gas with tritium found its way into the containment on a few occasions. The containment systems responded as expected in all these incidents.

There were, however, a number of occasions when some components of the containment system did not function properly. Any "failures" experienced to-date imply a loss of redundancy or diminished effectiveness of the affected components rather than a failure of the containment.

7.1 Containment Structural Shortcomings

During commissioning a CANDU 6 containment leakage rate was high. Methods of sealing while a containment is under pressure were developed such that the final tests demonstrated leakage rates of between 0.15 to 0.25 percent per day. Although these values are above the design target, they are well within the initial 0.5% air mass leakage/day at the design pressure used for safety analysis. In Pickering-A in its first years of operation the concrete perimeter walls overheated at the hot secondary side coolant system pipe penetrations and the concrete powdered and crumbled. One could see into the containment through the gaps around these pipes. This was later corrected by annular gas gap insulation and a second outer cooler tube wall penetrations on the hot pipes.

With the aging of concrete structures increased cracking and some spalling were also encountered. Some of these may be fixed by caulking and epoxy injections into some cracks, or by repairs to the concrete structure. In some instances when the measured leakage rate from the containment was high or was showing an excessively increasing trend, then the containment was repainted with a new non-metallic liner. In parts of the Bruce-B pressure relief duct under the water table some cracks developed.

7.2 Breach of Containment at Airlocks and Penetrations

The most common problems are small breaches of containment from the operation of components such as airlocks and fuel transfer chambers. These have been caused by;

- failed equipment such as deflated airlock seals, door latches and hinges, limit switches, interlocking monitors and controls,
- operating errors such as leaving both doors open in an airlock and shortcomings of communication devices with people in the airlocks.

Only a few of the perimeter wall penetrations by process piping and by electrical cables in the existing CANDU reactors were designed for testing individually.

7.3 Non-Functioning Containment Isolation

Examples of failures to maintain the containment boundary when it becomes part of the process equipment include;

- process pipes or their extensions disconnected for repairs or cut without plugging, or were opened for valve replacements
- valves opened or left open in error, or manhole left open

Some of the ventilation system dampers did not close for a variety of reasons.

In the Darlington multi-unit stations the diaphragm of a pressure relief valve folded the wrong way during a test.

In Pickering the electric heater failed for the common drain header of six vacuum ducts in a bank and the drain line froze, so that after a flooding of a U-tube for testing a pressure relief valve, the water could not drain, but entered the other vacuum ducts in the bank.

7.4 Dousing System Problems

In 1980 a dousing test was done at Pickering by pumping down the upper chamber with vacuum pumps with the main volume at atmospheric pressure. The dousing water entrained air, which accelerated the dousing flow rate beyond the design value.

The choice of some steel alloys has been a problem with dousing systems. These alloys when in long-term contact with water are subject to corrosion promoted by the presence of anaerobic sulphate reducing bacteria and iron oxidizing bacteria. Remedial actions include water treatment, coatings or choice of different materials for newer installations.

In 1987 at Gentilly-2, during pressurization of the containment for leakage rate testing, the pressure inadvertently reached the dousing initiation set point and an inadvertent dousing occurred.

8 Summary

The containment system provides the final barrier to limit the release of radioactive materials to the environment such that the permissible doses will not be exceeded.

A CANDU containment envelope is designed to the requirements of the Canadian National Standards and AECB regulatory guides. The Canadian seismic design assumptions ensure that the combination of loss-of-coolant and earthquake events is incredible and therefore not considered as a design basis.

The multi-component nature of typical CANDU containment systems and the multi-disciplinary nature of their design, computational methods and their validations, and the deterministic and probabilistic safety analysis have been emphasized. The derivation of the design bases was outlined from considerations of normal operation, accident conditions and from the requirements of the Canadian licensing and regulatory authority, the AECB. The testing methods for containments and some difficulties encountered in containment operations were also described.

The containment system is the last, but not the least, major defence system to protect the public and the environment against harmful doses of irradiation from radioisotopes released in a nuclear accident. The CANDU containment systems are designed to survive the accidental depressurization of a primary or a secondary coolant system without structural damage and without unacceptable release of radioactivity to the
environment.

Appendix 1

Evolution of the CANDU Containment Design

The containment systems for CANDU reactors has been improved over the years;

- The early research reactors (e.g., NRX, NRU) used confinement rooms or areas. These reactors had low pressure coolant systems.
- NPD, the Canadian demonstration power reactor, used underground containment;
- Douglas Point, the prototype CANDU power reactor, and subsequent commercial reactors, used above ground containment;
- The containments were equipped with means of pressure suppression and reduction;
- For multi-unit stations such as used by Ontario Hydro, a single pressure suppression and reduction facility was provided to several nuclear reactors at the same site.

The earliest designs served a single-unit reactor, with improvements incorporated in each subsequent design. The multi-unit reactors with a joined containment system in a nuclear station could eliminate the duplication of some of the containment components at great cost savings. The containment design improvements cannot be strictly separated on single-unit and multi-unit bases, because of cross-fertilization of ideas.

The CANDU pressurized heavy water reactor (PHWR) development began with the Nuclear Power Demonstration (NPD) reactor, rated at 20 MWe, which began operation in 1962. The NPD single-unit reactor and its boiler were in underground vaults. The containment building was a rectangular block-shaped concrete structure, going several stories deep below grade level. The vaults were designed to withstand internal pressures of 70 kPa(g) and 35 kPa(g), respectively. Both vaults had energy-absorbing dousing systems, gravity-fed from a water storage tank. A pressure relief duct was used to cope with the initial pressure rise in the case of the fracture of a pipe in the steam generator vault. The direct pressure relief to atmosphere feature has not been used since.

The next unit in the Canadian nuclear power program was a commercial prototype reactor, Douglas Point (1965), rated at 200 MWe. It featured an above-ground cylindrical concrete building with a steel roof. Its internal design pressure is 42 kPa(g) and its water dousing spray system was designed to cool the containment atmosphere by absorbing thermal energy. A containment isolation system was provided to close automatically the open penetrations on a LOCA signal. Duplicates of Douglas Point were built by AECL in India: RAPP-1 (1969), RAPP-2 (1972) and some newer copies by India.

The CANDU containment buildings built or committed to be built before 1994 all use prestressed, reinforced concrete structures. The prestressing was applied by post-tensioning the solidifying concrete. Except for NPD the reactor buildings were above ground level apart from some basement rooms..

The next single-unit design was Gentilly-1 (1971), was rated at 250 MWe, but due to problems not related to the containment system never operated at full power and was decommissioned subsequently. It was a prototype of a CANDU reactor using boiling light water for direct-cycle cooling (the primary and secondary coolant circuits were unified into a light water cooled circuit). Its containment featured a reinforced, post-tensioned concrete reactor building with a concrete dome, designed for 118 kPa(g) pressure. The containment design incorporated a dousing system, local air coolers, a containment isolation system and a filtered air discharge system. Automatic isolation included high-speed main steam isolation valves necessitated by the direct-cycle coolant circuit design.

A 125 MWe single-unit CANDU known as KANUPP (1972) was built and designed by General Electric Canada and it operates in Pakistan. This has a containment building of cylindrical shell with domed top, made of reinforced concrete. The perimeter wall thickness of the shell is 1.35 m.

Containment design in Canada took two paths after Douglas Point. The first path led to the continued development of the single-unit pressure containment system. The other path led to the vacuum building concept for multi-unit plants.

After gaining experience with the NPD and Douglas Point single-unit CANDU, Ontario Hydro, with its large demand for electricity, needed larger nuclear power stations. To economize on the containment, turbine hall and a number of common services, starting with Pickering-A (1971), four CANDU reactors were grouped into a multi-unit power station with a joint containment envelope. In 1982 the four reactors of Pickering-B were connected to an extension of the Pickering-A containment system, forming a common containment for eight reactors. Multi-unit nuclear stations Pickering-A (1971) and Pickering-B (1982), used cylindrical reactor buildings which could accommodate some pressure build up before being connected to the joint containment system. Bruce-A (1976), Bruce-B (1984) and Darlington (1990) used rectangular block-shaped reactor buildings, in which only the reactor vault in each reactor building is part of the containment envelope. In the Bruce and Darlington reactors all reactor vaults are always open to the rest of the containment envelope.

A multi-unit containment with its larger free volume allows lower design pressures for the containment structures than a single unit containment. The multi-unit CANDU plants further reduced the containment design pressure by introducing a vacuum building which with its preexisting vacuum can reduce the post- accident pressure peaks. A second, lesser negative containment pressure feature was also utilized by a slightly subatmospheric pressure in the reactor building or vault. This allows leakage rate monitoring of the containment envelope and preventing outleakage of the containment atmosphere during normal operation.

In a multi-unit plant, each reactor is in a separate reactor building, which are or can be connected to a common pressure relief duct and that in turn, on sufficient

pressure build up, becomes connected via pressure relief valves, to a vacuum building. The reinforced concrete vertical cylindrical vacuum building allows maintaining a pre-accident vacuum. After an accident in a reactor building the containment atmosphere pressure is raised and that opens the large pressure relief valves. The preexisting vacuum in the vacuum building and the increased overall containment volume reduces the accident-induced pressure in the rest of the containment atmosphere. Dousing is provided only in the vacuum building subsequent to a significant pressurizing accident in either of the reactor buildings.

The next single-unit reactors were the very successful CANDU 6 type, operating at Gentilly-2 (1982), Point Lepreau (1982), Wolsong-1 (1982) in Korea and Embalse (1983) in Argentina and those being built, such as Wolsong-2, -3 and -4, and Cernavoda-1 in Romania. The CANDU 6 containment has evolved from the experience gained with each earlier design. The CANDU 6 containment features a reinforced, post-tensioned concrete cylindrical reactor building with concrete dome, designed for 124 kPa(g). Again, the containment system incorporates a dousing system, local air coolers for various rooms within the reactor building, blow-out panels allowing pressure equalization of pressure differences amongst different rooms in the containment and a containment isolation system.

After the 1979 Three Mile Island Unit No.2 accident at Harrisburg, PA, USA, hydrogen mitigation was recognized to have high importance. The Bruce-B and the Darlington containments were the first CANDU power plants designed with comprehensive hydrogen mitigation features (such as sensing instruments, intentional mixing and hydrogen ignition).

The containment design evolution since building the Darlington plants was in several directions. One direction is making the containment system more "passive". The containment function is comprised primarily of passive sub-systems, such as the containment envelope and the airlocks which are not required to change state following an accident. The filters for activity removal are all passive components. The dousing systems in CANDU containments have different levels of passivity: in multi-unit CANDU the main pressure relief valves and the dousing systems do not rely on instrumentation to be activated. The CANDU 6 dousing system is controlled and activated by compressed air in local tanks, while the multi-unit dousing is initiated by vacuum in a chamber of the dousing system. Since both this pressurized air or vacuum are prepared well before an accident, the dousing system is classified as a passive sub-system.

The newer passive systems include hydrogen recombiners which do not require electrical power for operation. Other evolutionary trends in passive containment involve using steel liners or new polymeric liners for concrete containment buildings for leakage reduction. Some new on-line quasi-steady and oscillating flow testing methods for containment gross leakage rate detection are also under development.

Research Reactors

Training Objectives

On completion of this lesson the participant will be able to:

- outline the development of research reactors in Canada.
- three uses of Canadian research reactors.
- the difference between, and different uses of, zero power, medium power and high power reactors.
- the reason for the current importance of NRU and the reason for the development and construction of the MAPLE-X10 reactor.
- understand the design of various research reactors and what is meant by a 'loop'.
- state the safe operating features of the SLOWPOKE reactor.

Table of Contents

1 Introduction

Since the Second World War nuclear research reactors have played a central role in the development of nuclear programs. After the 1942 success of the Chicago Pile, demonstrating the first sustained chain-reaction in a critical reactor, the U.S.A. embarked on the development of nuclear weapons. In 1942-43 an Anglo-Canadian nuclear research laboratory was set up at the University of Montreal, and the first Canadian research reactor ZEEP, a Zero Energy Experimental Pile went into operation on September 5th, 1945 in Chalk River, Ontario. This reactor was first for another reason as well: it was the first reactor to operate outside the United States. Too late to be used for war efforts, it started, however, the Canadian nuclear development program for the peaceful uses of nuclear energy.

Over a period of the next half century a number of Canadian research reactors were designed, developed and built to serve as:

- Test facilities for the development of more and more sophisticated, multi-purpose research reactors;
- Test facilities for nuclear physics, irradiation behaviour of materials, thermal-hydraulic processes, control and safety systems and components of a whole generation of neutron efficient, natural uranium-fuelled CANDU power reactors;
- Experimental facilities to collect scientific databases to broaden the fields of basic and applied research in nuclear science and technology;
- Assaying, activation analysis facilities for use in biosciences, geosciences, forensic studies, etc.;
- Production facilities for industrial and medical radioisotopes (for instance, Canadian research/irradiation reactors provide nearly all of the world's supply of the Tc-99m (Technetium) used as an injected contrast material in CAT-scan imaging in hospitals everywhere); and, last but not least
- Undergraduate teaching and graduate training and research facilities for universities.

This lesson outlines the evolution of the Canadian research reactors, showing the major design and safety improvements and increased operational capabilities and flexibility of successive research reactors, which in many instances have led to international acclaims and business in this field of Canadian high-technology.

The manual is organized along the power level of the Canadian test facilities, starting with non-critical test piles. The chronological order of the Canadian research reactors may differ somewhat from the ordering according to power level, but experience gained from earlier designs are usually reflected in later ones.

2 Sub-critical Test Facilities in Canada

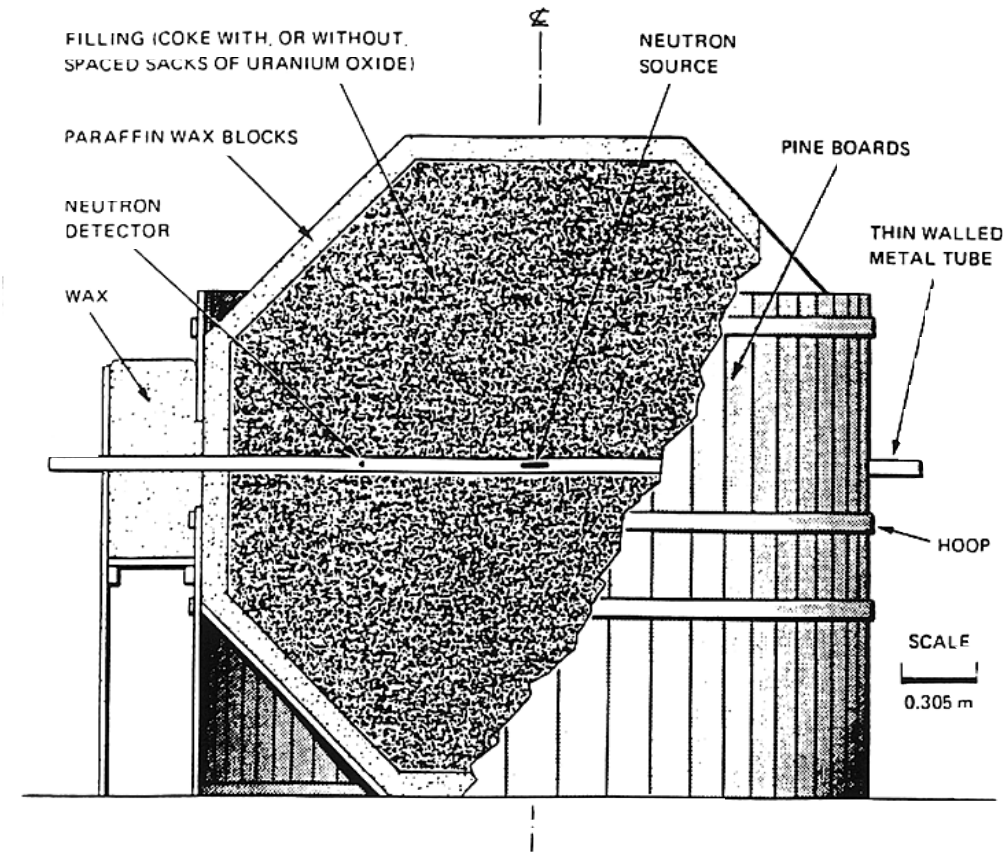
2.1 Early Sub-critical Experiments

In 1940 March, Canadian nuclear pioneer, G.C. Laurence performed the first Canadian sub-critical experiments using half a ton of natural uranium-oxide powder and a similar mass of relatively pure calcined coke. Placing the uranium in paper coffee bags (each with about 3 kg U_3O_8), he formed a primitive heterogeneous lattice by surrounding each bag uniformly with coke. He then placed the fuel and moderator in a bin lined with paraffin which acted as a reflector. He used a mixture of metallic beryllium and radium as a neutron source and built a set of Geiger counters to measure the neutron flux at selected locations within the lattice, (Figure 1). Although the pile was highly subcritical and the results inconclusive, the experience spurred on Canadian efforts to establish the feasibility of a chain reaction with natural uranium moderated by graphite.

Collaborating with B.W. Sargent on subsequent experiments in 1941-1942, Dr. Laurence eventually built a much larger spherical pile, 2.8 m in diameter. In a series of experiments conducted with approximately 9 Mg of graphite (density of about 1.2 $Mg.m^{-3}$) and 0.9 Mg of uranium oxide (density of 3.4 $Mg.m^{-3}$), they achieved a neutron multiplication factor of about 0.90 with the oxide packaged in lumps of 3 kg. Although they were working with the best available materials, it became clear that higher-density uranium and a more efficient moderator (either purer graphite or heavy water) would be required for a successful chain reaction. Accordingly, the main benefit of this pioneering work was the creation of a small cadre of experienced Canadian physicists who would play key roles in building research reactors at the Chalk River Laboratories. However, the data obtained by Laurence and Sargent was directly useful to the international team established in 1943 at a new laboratory in Montreal.

Figure 1a:
Dr G.C. Laurence

Figure 1b:
Early Canadian Experimental Pile



CUTAWAY DRAWING OF OTTAWA SUB-CRITICAL ASSEMBLY, 1941-42

Scientific interest at the Montreal laboratory centred on natural-uranium heavy water lattices because Canada did not expect to develop enrichment facilities and therefore preferred a moderator with a very low neutron-absorption cross-section combined with good thermalization properties. Between 1943 and 1945, many exponential experiments were performed to characterize the nuclear properties of heavy water, e.g., the transport mean free path and the diffusion length, and to measure the buckling for lattices containing proposed ZEEP uranium-metal fuel rods with different cladding specifications, and at various lattice spacings.

The exponential facility consisted of a cylindrical steel tank, 1.6 m in diameter and 1.65 m in height, filled with about 3.1 m^3 of heavy water and mounted on a large block of graphite. Neutrons were generated by impinging X-rays from a 1.4 mA, 2 MeV generator upwards towards a beryllium target located on the vertical axis of the tank, 0.86 m below the tank bottom. Cadmium sheets on the exposed surfaces of the graphite and the heavy water tank avoided distortions of the neutron distribution within the tank due to reflected neutrons. The main result of the experimental program was the optimization of core dimensions for ZEEP and for the first Canadian high-power reactor, NRX (**N**ational **R**eactor E**X**perimental).

2.2 Sub-critical Facility for Nuclear Education

In the mid-1950s, a sub-critical facility was designed and built for nuclear engineering education and research at the University of Toronto. The facility consisted of a stainless steel tank in which 2 m long fuel rods of aluminum-clad U-metal or uranium dioxide, could be arranged in a variety of lattice patterns. The fuel was submerged in D_2O moderator, but the assembly was grossly sub-critical. A beryllium reflected radium-beryllium neutron source, parked at the bottom of the tank, can be lifted by external controls and this permits the performance of exponential experiments, or approach to criticality. This facility was in use until 1990.

3 Canadian Low-power Facilities

3.1 ZEEP

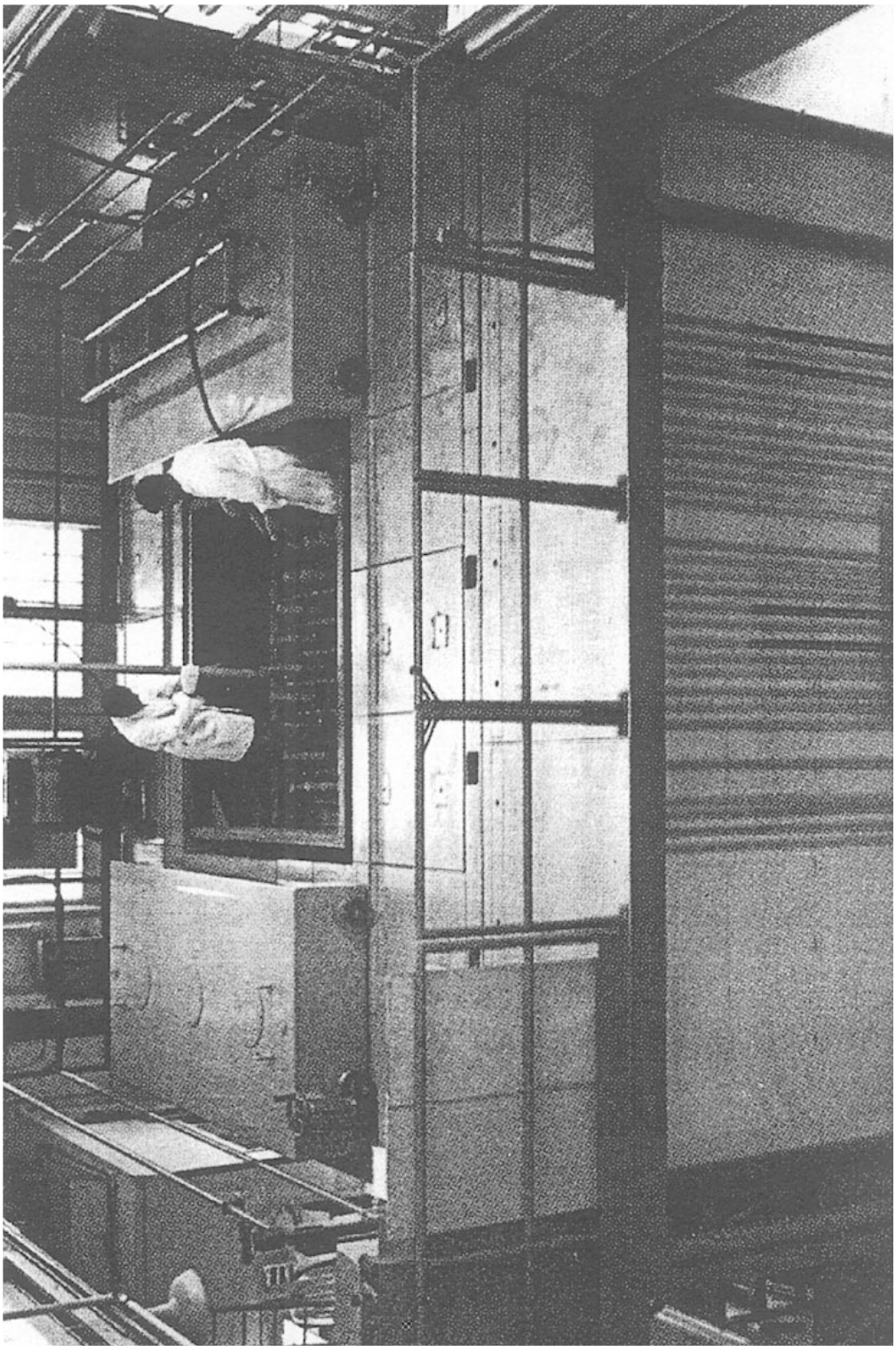
Design of the ZEEP (Figure 2) critical facility began in 1944. The principal purpose of ZEEP was to perform measurements of lattice design, fuel-rod dimensions, and sheathing alternatives to resolve the design of NRX. ZEEP's technical specifications are summarized in Table 1; its main features were a large (9 m^3) cylindrical aluminum vessel with graphite radial and lower reflectors, into which heavy water moderator could be pumped from a storage tank below. Experimental lattices were formed by hanging fuel rods from steel beams that bridged the top of the tank. The lattice arrangement of the rods and the depth of heavy water were adjustable. The fuel rods consisted of 3 cm diameter and 15 cm long natural uranium metal or uranium-dioxide pellets stacked inside 2.5 to 3 m long aluminum tubes.

Reactivity control was provided by four cable-driven cadmium-plated steel control plates located between the tank and the radial reflector. The reactor was shut down via two sets of four cadmium-plated stainless steel shutoff rods suspended on stainless steel cables. The reactor was so low-powered that it did not require a cooling system.

Following a period of comprehensive studies of the reactor itself, ZEEP was operated over the next twenty years to provide valuable information on the characteristics of heavy-water-moderated fuel lattices for the NRX and NRU research reactors, the NPD (**N**uclear **P**ower **D**emonstration) and other early CANDU power reactors. For example, immediately after the initial commissioning program, instruments developed for NRX were tested in ZEEP. Procedures for irradiating and processing radioactive isotopes in NRX were also developed and neutron yields for ^{233}U fission were measured. To support the design of the first British graphite pile at Harwell, measurements of neutron cross-sections for graphite blocks were performed in ZEEP. Other early ZEEP utilization included the production of trace radioisotopes, for example, sodium for biochemical research at the University of Toronto, and "pulsing" of the reactor from 1 W to 50 W to facilitate cloud-chamber experiments. Later ZEEP

measurements on heavy water lattices included studies of the benefits derived from clustering fuel rods and the relative merits of uranium-metal and uranium-oxide for NPD fuel meat.

Figure 2:
ZEEP Reactor at Chalk River Laboratories



3.2 Pool Test Reactor (PTR) and Zero Energy Deterium-2 (ZED-2)

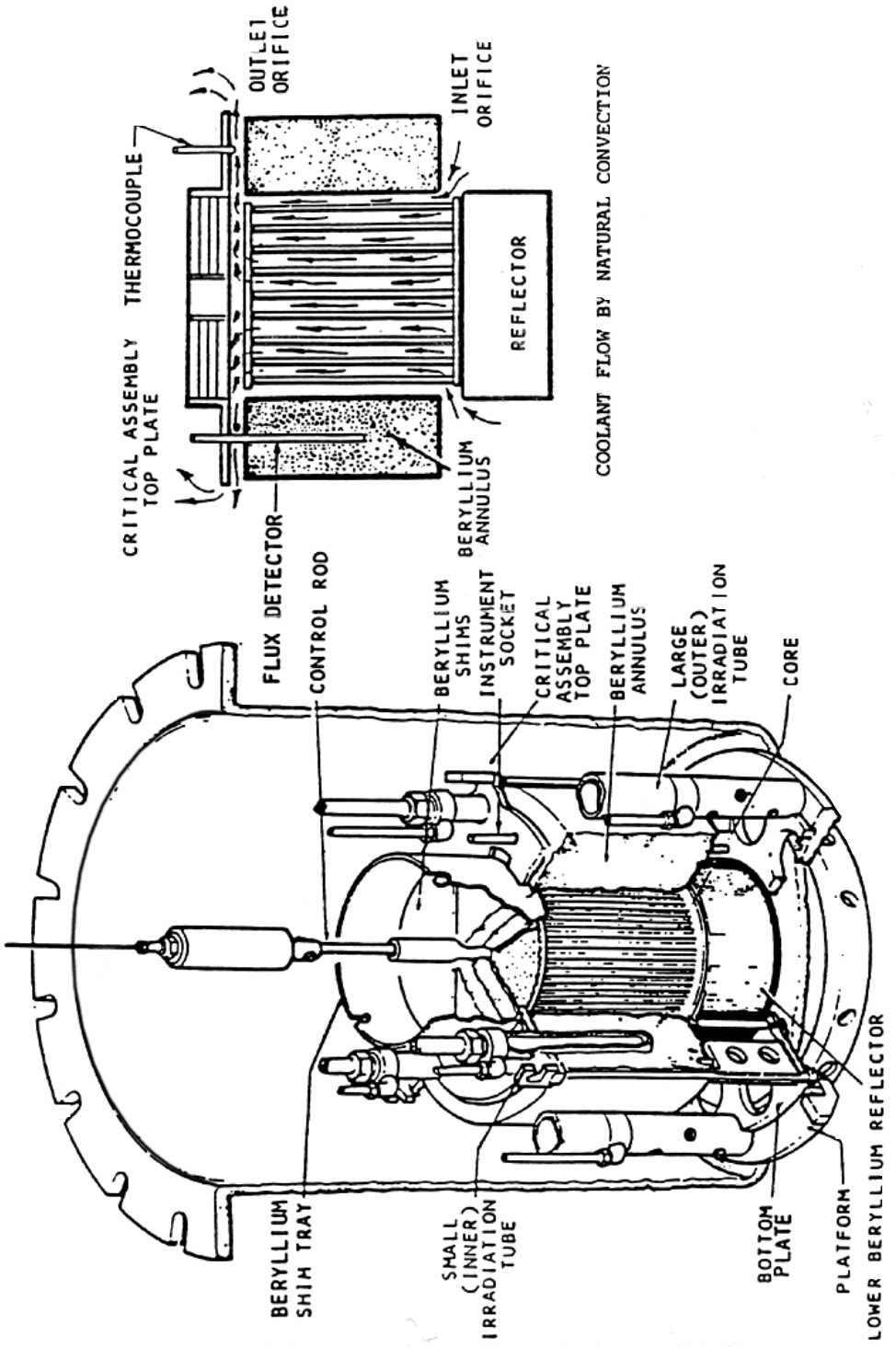
The successful operation of ZEEP eventually led to the building of two other zero-power facilities at the Chalk River Laboratories (CRL). The Pool Test Reactor (PTR) is a 10 kW swimming-pool reactor based on 93% enriched uranium-aluminum plate-type fuel. It incorporates an oscillating shuttle that can swing fuel assemblies or specimens of irradiated fuel rods through the core. Ion chamber measurements of the neutron flux enable the corresponding dynamic reactivity changes to be deduced. Other specifications are summarized in Table 1.

Because of ZEEP's relatively modest dimensions, a larger version, ZED-2 (**Z**ero **E**nergy **D**euterium - **2**) was built to facilitate measurements on larger, more representative CANDU core lattices. As indicated in Table 1 at the end of this manual, the ZED-2 heavy water tank accommodates cores up to 3.3 m in diameter and roughly 3 m in height. Reactivity control involves controlling the heavy water level by pumping heavy water moderator (inventory 30 Mg) from a dump tank below the reactor. Fast moderator dump and an independent system of 12 cadmium-aluminum shutoff rods provide reactor shutdown. The remote adjustment of lattice spacing is possible using a lattice-change mechanism that hangs fuel assemblies into the reactor vessel. ZED-2 serves all current Canadian needs for heavy water lattice measurements. The facility has been utilized for definitive studies of the effects of heavy water and alternative light water and organic coolants, coolant void measurements and studies of fuel lattices of advanced CANDU bundles containing plutonium-uranium-oxide and ^{233}U oxide fuel meat.

3.3 Safe Low Power Critical Experimental (SLOWPOKE)

From 1968 to 1970, the PTR pool provided a convenient home for testing the prototype (SLOWPOKE-1) of a new type of reactor for neutron-activation analysis, trace radioisotope production, and teaching in nuclear science and engineering. SLOWPOKE (**S**afe **LOW** **PO**wer **K**ritical **E**xperiment) is a 20 kW thermal power tank-in-pool reactor with an unusually high degree of inherent safety. The reactor assembly (Figure 3), which comprises a small (~ 9 L) light-water-moderated core with a close-fitting beryllium reflector, is housed within a containment tank that can be installed in a 2.5 m diameter by 6 m deep pool. A central cadmium control rod (worth 5.5 mk, i.e., 0.55% $\Delta k/k$) that responds to a self-powered neutron flux detector in the radial beryllium annulus provides both regulation and normal shutdown. Table 1 provides a summary of SLOWPOKE specifications. The thermal neutron flux per unit power, 5×10^{17} $n.m^{-2}.s^{-1}.MW^{-1}$, is very high.

Figure 3:
Slowpoke-2 Critical Assembly



The core is undermoderated to provide appropriately negative reactivity coefficients for increasing temperature and void. Furthermore, the number of fuel rods loaded into each core unit is adjusted to limit the maximum excess reactivity to 3.4 mk with a minimal number of beryllium shim-plates loaded in

the top reflector. Tests involving the rapid insertion of up to 6.8 mk of excess reactivity have demonstrated that this strategy limits the potential for power excursions such that credible reactivity-addition accidents will not damage the reactor or pose a radiation hazard to persons in or near the reactor room. Figure 3 also shows the natural convection cooling flows through a SLOWPOKE reactor. SLOWPOKE-2 reactors (commercial versions of SLOWPOKE-1) have been licensed for unattended operation by the Atomic Energy Control Board of Canada. Reactivity compensation for fuel burnup is provided periodically by a small increment to the thickness of the top reflector.

Between 1971 and 1983, a total of six SLOWPOKE-2 units were built with 93% enriched U-Al-alloy fuel; five units are at various universities and laboratories in Canada and one is in Jamaica. A seventh SLOWPOKE-2 unit with a 19.9% enriched UO_2 core began operation at the Royal Military College of Canada, in Kingston, Ontario, in 1985.

The SLOWPOKE reactor is internationally recognized for its inherently safe features and for its thermal-neutron efficiency. The SLOWPOKE design provided the basis for the Miniature Neutron Source reactor built by the People's Republic of China.

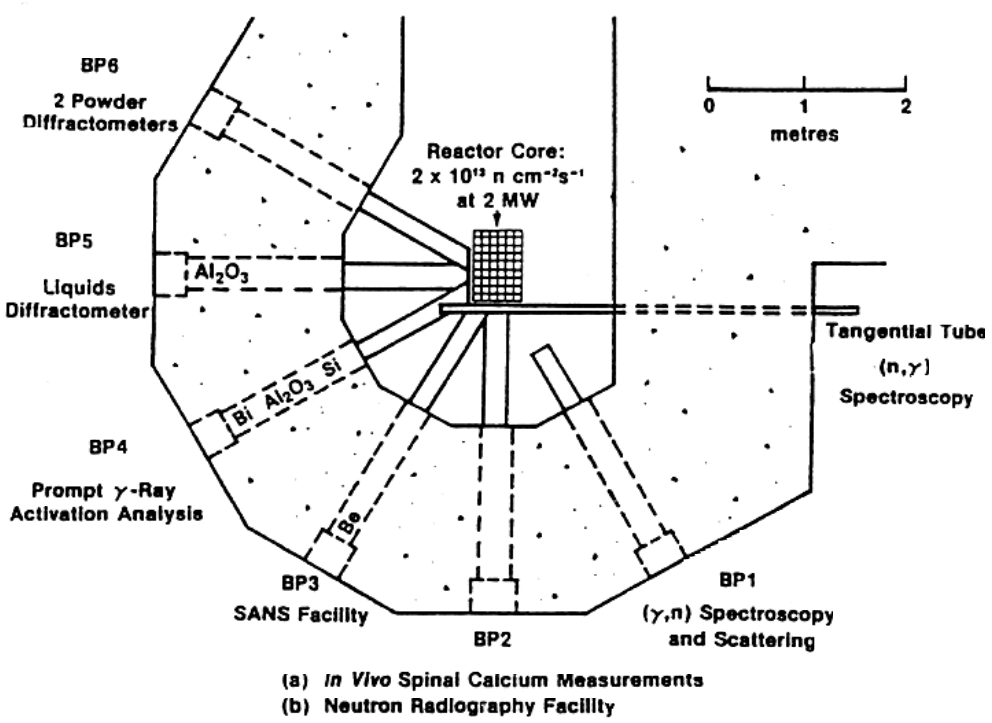
4 Canada's Medium-Power Facilities

4.1 McMaster Nuclear Reactor (MNR)

The **M**cMaster **N**uclear **R**eactor (MNR) is a swimming-pool reactor built at McMaster University in Hamilton, Ontario, in the late 1950's. It is one of seventeen similar reactors built by AMF Atomics. Licensed to operate at up to 5 MW thermal power, the MNR is a multipurpose facility (see Figure 4) used for research with extracted neutron beams, neutron-activation analysis, teaching, and short-lived radioisotope production. The moveable reactor assembly provides a core grid of 54 sites, 34 of which typically contain 93% enriched U-Al plate-type fuel elements (28 standard, 6 control). Reactivity control is provided by five AG-In-Cd shim-safety rods and one stainless-steel regulating rod; full insertion of the three lowest-worth safety rods is sufficient to ensure reactor shutdown. The reactor is housed within a reinforced-concrete containment building. Table 1 provides a summary of MNR technical specifications.

The MNR provides six radial beam ports and one tangential tube. These facilities terminate in the light water adjacent to one of two core positions. At 5 MW, the perturbed thermal flux at the beam-tube noses is approximately 5×10^{16} $n.m^{-2}.s^{-1}$. Irradiation facilities include two in-core positions with thermal fluxes of 2-4 10^{17} $n.m^{-2}.s^{-1}$, six reflector positions with thermal fluxes of 1-2 $\times$ 10^{17} $n.m^{-2}.s^{-1}$, and low-flux (3-9 10^{16} $n.m^{-2}.s^{-1}$) positions for seven pneumatic-transfer systems and three large-sample sites.

Figure 4:
McMaster Nuclear Reactor Plan View - Neutron Beam Facilities



4.2 Slowpoke Demonstration Reactor (SDR)

In the 1980s, AECL developed a district-heating reactor concept derived on the SLOWPOKE-2 reactor. A 2 MW prototype called the SLOWPOKE Demonstration Reactor (SDR) was built and put through low-power commissioning tests at the Whiteshell Laboratories.

The SDR is located in a new building attached to Building 100 which houses the shutdown WR-1 reactor. Figure 5 shows the general arrangement of the facility. The reactor core, hot riser duct and heat exchangers are installed in a water-filled pool, inside a steel-lined concrete vault. The pool water serves as both coolant and shielding.

The core consists of 196 uranium-oxide fuel elements of the type used in CANDU reactors, but using 4.9% enriched uranium instead of natural uranium. Each fuel element is 0.5 m long and contains 0.5 kg of uranium. Assuming an annual load factor of 50%, the four fuel bundles comprising the core will be replaced every four years. A 10 cm thick beryllium reflector surrounds the core on four sides. Figure 6 shows the reactor core and reflector.

Primary cooling is by natural circulation through two plate-type heat exchangers. Secondary coolant is pumped to a third heat exchanger, where heat is rejected to cold water from the Winnipeg River. The river water circuit and

secondary circuits each have a single manual valve for flow control. The primary circuit has no valves.

The SDR was initially equipped with two shutdown systems. The first system uses gadolinium nitrate solution, which flows into the pool by gravity alone, through two temperature-actuated valves. These valves require no external power supply and open automatically at the desired reactor coolant outlet temperature.

A second, fast shutdown system incorporating four gravity-drop absorbers was also provided.

The four absorber plates used for shutdown are also used for periodic step-wise reactivity adjustment by an operator. In addition, a central absorber rod was used for automatic control of coolant temperature. The control rod rate of removal was restricted by three timers and multiple interlocks. The absorber plate rate of removal was restricted by two timers, a revolution counter interlock and several other interlocks.

The temperature sensors and valves for the liquid absorber shutdown system were fluidic throughout. One fluidic valve was constructed of glass and the second of stainless steel. Visual observation of fluid in the glass valve, fluid level detection in the stainless steel valve, and low-level alarms in the liquid absorber storage tanks, provide adequate assurance of availability during routine operation.

The reactor pool is covered by an insulated cover, enclosing a gas space over the pool. The air and water vapour are continuously circulated through a hydrogen recombiner and condenser. After filtering and monitoring, a fraction of the circulating cover gas is released to the atmosphere through the Building 100 stack. Building ventilation is provided by an extension of the Building 100 ventilation system.

Figure 5:
SLOWPOKE Demonstration Facility

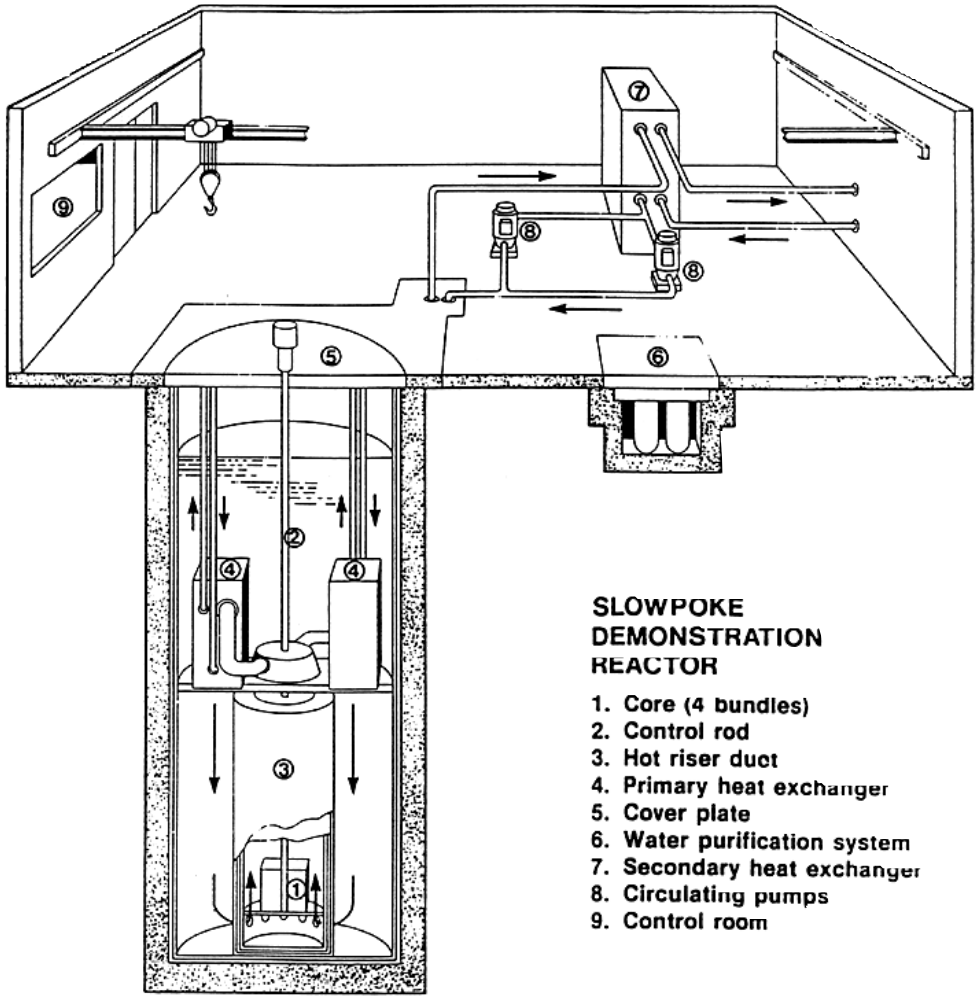
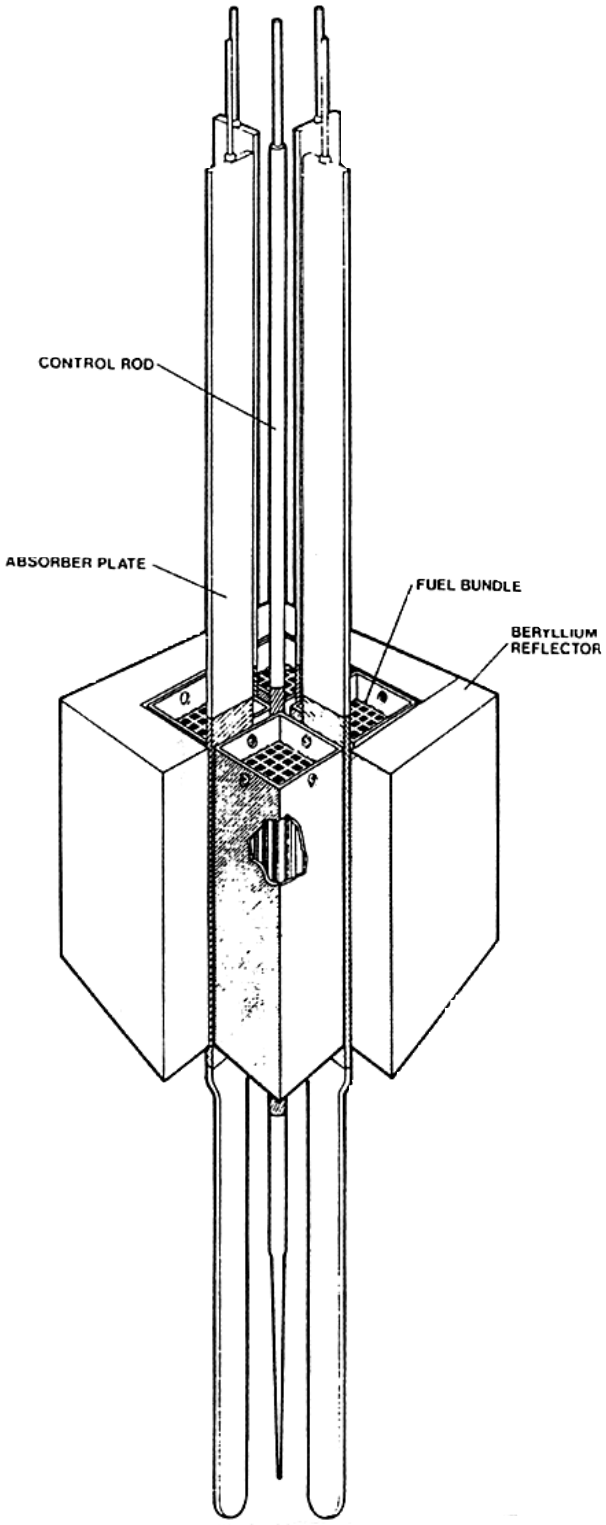


Figure 6:
SDR Core and Reflector Assembly



5 Canadian High-power Facilities

5.1 National Reactor Experimental (NRX)

NRX (Figure 7) is a heavy-water-moderated high-flux multipurpose reactor with once-through light water cooling. The large (17 m^3) reactor core provides a central irradiation thimble (140 mm diameter) plus 198 smaller (57 mm diameter) vertical sites for fuel assemblies, test loops, irradiation targets, and shutoff rods. The core lattice (Figure 8) is hexagonal with a centre-to-centre spacing of 173 mm. Reactor regulation is achieved by controlling the level of heavy water flowing over a weir. A 0.9 m thick graphite reflector plus a 0.3 m thick iron thermal shield and a 2.4 m thick ordinary concrete biological shield surround the core radially; the axial thermal shields are composed of steel and water. Other technical specifications are given in Table 2.

When NRX first started up in 1947 July, it was fuelled with aluminum-clad uranium-metal rods of diameter 35 mm, one per core site. With a fresh fuel loading of 10.5 Mg uranium (~75 kg fissile), a k_{eff} of 1.042 was obtained. The approach to the original design-maximum power of 20 MW was gradual; 1 MW was achieved by the end of 1947, 8 MW in 1948 May, and 20 MW in 1949 January. At this time, NRX produced the highest peak neutron flux of any existing reactor, about 3×10^{17} $n.m^{-2}.s^{-1}$ in the moderator. Shielding improvements permitted uprating to 30 MW in 1950. The accident in 1952 December demonstrated the need for redundancy in shutdown and control systems. The restoration program (which included core and vessel replacement, instrumentation improvements, and modifications to the thermal shields) enabled further power uprating to 42 MW, at which power it produced a peak thermal neutron flux of 7×10^{17} $n.m^{-2}.s^{-1}$. In the late 1950s, the peak flux was improved by 50% via a change in fuel to natural UO_2 fuel rods in the outer core regions and 93% enriched uranium-aluminum-alloy fuel in the central regions. The new enriched-uranium fuel rods, which consisted of 6.35 mm uranium-aluminum fuel meat coextrusion clad with finned aluminum fuel sheaths, were employed in a seven-rod cluster that fit into a 35 mm NRX flow channel. The UO_2 rods were of similar dimensions to the original uranium-metal rods; some of these rods were fitted with a central irradiation hole for radioisotope-production targets. The available thermal neutron flux was further increased to 1.2×10^{18} $n.m^{-2}.s^{-1}$ in 1962 via the complete conversion to the 93% enriched aluminum-alloy fuel. The corresponding maximum fast neutron flux was 2×10^{16} $n.m^{-2}.s^{-1}$.

The experimental facilities in NRX initially included a so-called J-rod annulus for producing ^{60}Co in the graphite reflector, fifteen user-operated "self-serve" irradiation facilities in the reflector, fifteen radial horizontal beam holes, two graphite thermal columns and a central vertical thimble. In response to American interest in testing proposed fuel for nuclear submarines and to Canadian and international interest in developing fuels for nuclear generation of

electricity, fuel test loops were introduced to NRX. By the mid-1960s, NRX contained six H_2O-cooled fuel test loops and one organic-cooled test loop which permitted power-reactor fuel pins to be irradiated realistically under a wide range of physical and chemical conditions.

More recently, as part of a rationalization of the operation of Canadian research reactors, the loop facilities have been removed and NRX now serves to back up NRU radioisotope production. It is expected that NRX will be decommissioned in the mid-1990s.

Figure 7;
NRX Reactor at Chalk River Laboratories

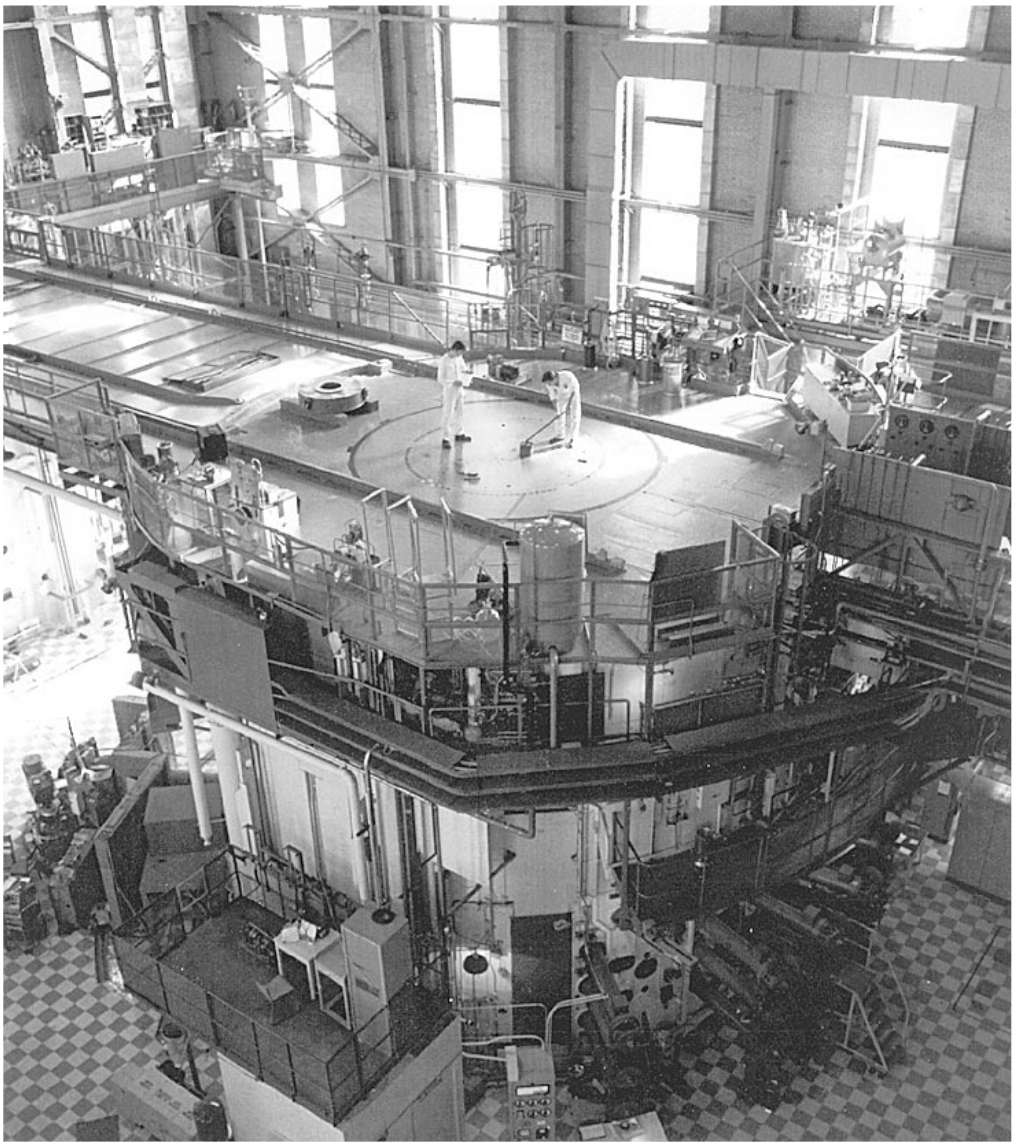
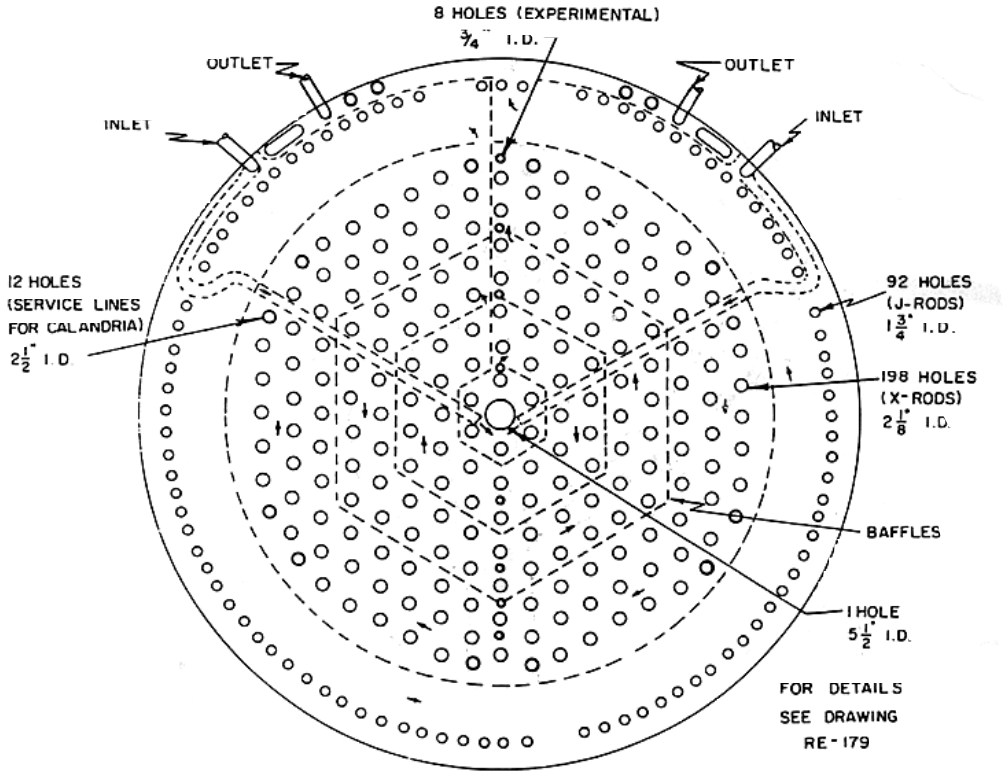


Figure 8:
NRX Core Cross-section



5.2 National Reactor Universal (NRU)

NRU (**N**ational **R**eactor **U**niversal), which began operation in 1957 November, is a heavy-water-cooled and -moderated multipurpose reactor (see Figure 9) that was designed to provide a relatively high thermal neutron flux over a large volume (23 m^3 reactor vessel). Its intended utilization included fuel and materials testing in support of power reactors, large-scale production of plutonium, ^{233}U, ^{60}Co and other medical and industrial radioisotopes, and the provision of intense neutron beams for basic and applied research.

The main design features of NRU include: a 227-position triangular lattice (Figure 10) with a pitch distance of 197 mm, reactivity control and shutdown by a system of 16 (later 22) cadmium and cobalt absorbers, a light water radial reflector of thickness 0.3 m with a 0.15 m thick irradiation space (J-rod annulus) between the core and the reflector, a 0.3 m thick steel axial thermal shield, and a 3.0 m thick biological shield of heavy concrete. Table 2 gives additional technical specifications. Heavy water is pumped into the reactor through a lower header block (~1.8 $Mg.s^{-1}$ total flow) where about 7% directly enters the moderator and the remainder flows upwards past the fuel assemblies and then into the moderator through slots in the flow channels.

Originally designed for plate-type natural uranium-metal fuel, NRU generated a peak thermal neutron flux of 3 x 10^{18} $n.m^{-2}.s^{-1}$ at 200 MW. With a fresh fuel loading of 199 assemblies (10.75 Mg U, 76.4 kg fissile), the maximum k_{eff} obtained was 1.09. The use of on-power refuelling, first demonstrated in NRU and later applied to CANDU power reactors, permitted the facility to operate for relatively long periods of time without the need to allocate a major portion of the available excess reactivity to burnup compensation during the operating cycle. Although fuel failures were frequent in the early history of NRU, the problem was eliminated by using extrusion-clad fuel with an intermediate nickel bond. Like NRX, NRU was converted to 93% enriched uranium-aluminum alloy fuel rods. In 1960, some enriched uranium metal fuel rods were introduced to facilitate the efficient production of neutron-absorbing radioisotopes such as ^{60}Co. With the expiration of the plutonium production contract in late 1963, NRU was fully converted to 93% enriched uranium-aluminum fuel rods similar to those of NRX (twelve rods per assembly in a 50 mm diameter flow channel). Although a thermal neutron flux increase to 2 x 10^{19} $n.m^{-2}.s^{-1}$ was feasible, the peak flux was maintained at the earlier level and the operating power was reduced to 115-135 MW. Experience with this fuel has been favourable, with high exit burnups (above 80% average U-235 depletion) routinely achieved without swelling or defects. During the 1980s, a low-enrichment (19.7%) version of the NRU fuel rod has been developed using U_3Si-A1 as the fuel meat.

Experimental facilities include three (later five) vertical through tubes for fuel and materials test loops, a thermal column and an array of 27 horizontal neutron-beam holes, of which two are elliptical through tubes. Figure 10 shows the arrangement of the NRU test facilities.

NRU was shut down from 1972 to 1974 to provide heavy water for the Canadian nuclear power program and to replace the corroded reactor vessel. The new vessel provided more (five instead of three) in-core sections for loops and longer re-entrant cans to increase the neutron fluxes available to various horizontal beam tubes. The central loop position was eliminated and the configuration of control and adjuster rods was modified.

Figure 9:
NRU Reactor

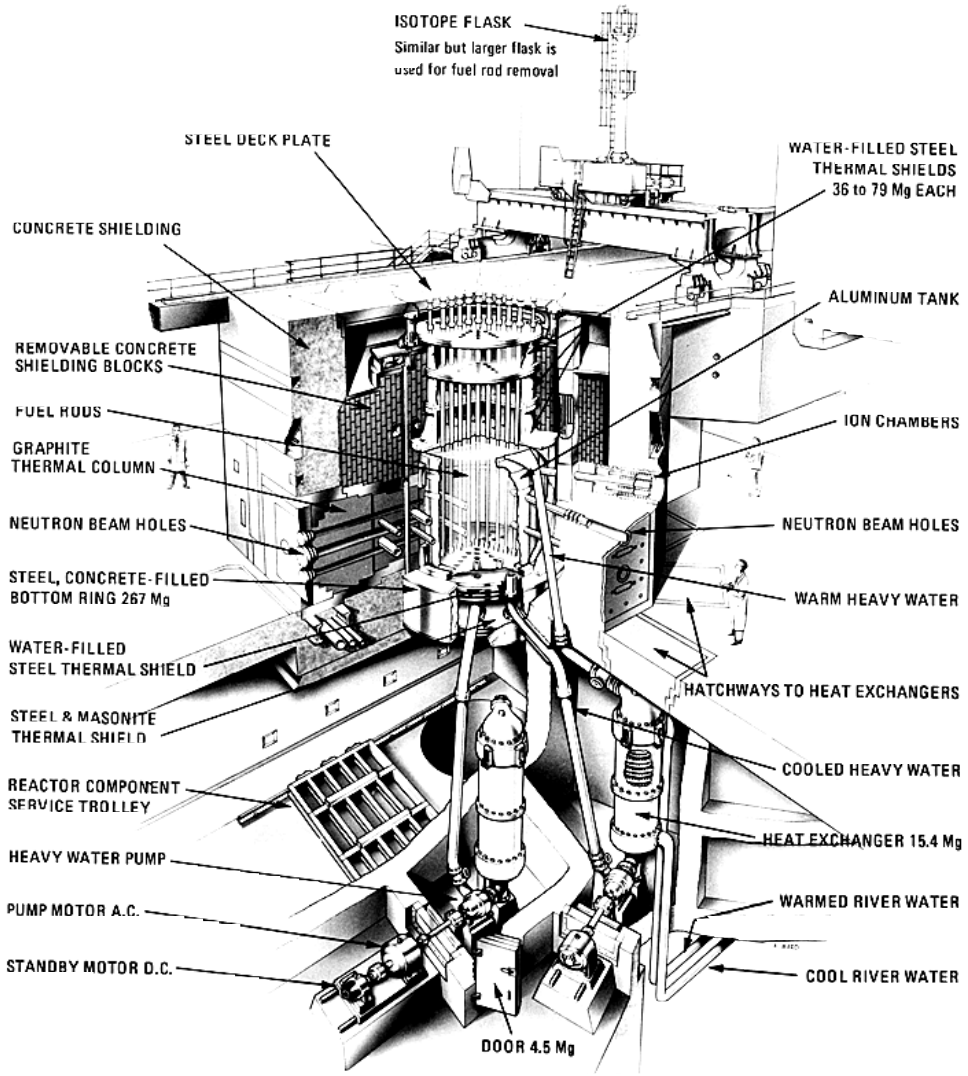
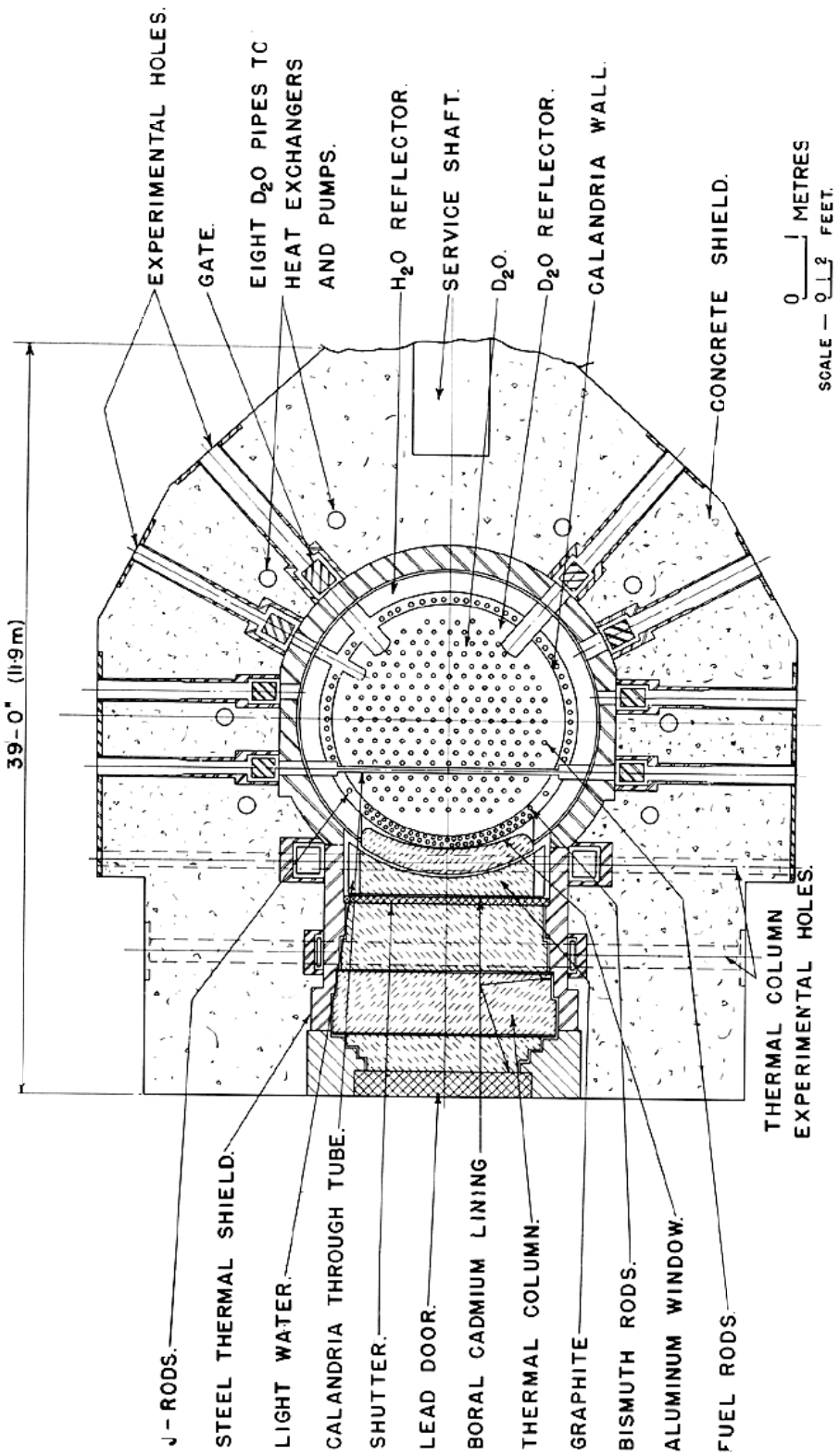


Figure 10:
NRU Reactor Plan View



There are now eleven cadmium and seven cobalt absorber rods and three cobalt adjusters and one aluminum nitride adjuster in NRU. The cobalt absorbers and the adjuster rods are used for reactor regulation. The eleven cadmium rods (which have no shrouds) are used for reactor shutdown. For safety analysis only the first eight cadmium absorbers (in two banks of four) are considered. These shutoff rods are activated when their holding magnets are released and the rods drop in the core due to gravity. The shutoff rod activation system is designed so that it can override any unsuccessful rod insertion by jumping over to the next rod in the insertion sequence.

Since 1990, the high-enriched (93%) ^{235}U fuel has gradually changed to low-enriched (20%) ^{235}U fuel. This change is being made to reduce the inventory of high-enriched uranium as part of the international program on reduced enrichment for research and test reactors. The current reference fuel is uranium silicide dispersion in aluminum, coextruded with aluminum sheath.

NRU's large irradiation space has been an important factor in the testing of fuel bundles and fuel channel components for CANDU reactors. A high temperature H_2O loop began operation in 1959 and an organic loop and a boiling water loop followed in 1963-64. With an extrapolated flux length of 3 m and a peak unperturbed thermal neutron flux of 3×10^{18} $n.m^{-2}.s^{-1}$ at the loop positions, NRU has been able to irradiate sections of CANDU pressure tubes with up to six full size fuel bundles operating under representative axial irradiation conditions. For the 19- and 28-rod bundle designs used by early CANDU power stations such as Douglas Point and Pickering, NRU could achieve fuel ratings of interest (up to 45 kW/m) with natural enrichment fuel. For later 37- and 43-rod fuel bundles, some enrichment (typically 1.2% to 2.0% ^{235}U in total uranium) has been employed to produce ratings up to 65 kW/m). NRU operates with up to ten fast neutron rods that provide 74 mm diameter central irradiation holes with enhanced fast (> 1 MeV) fluxes up to 6×10^{17} $n.m^{-2}.s^{-1}$ for studying irradiation damage in small zirconium-alloy specimens. Although this flux level implies annual fast fluences in NRU comparable to current reference CANDU pressure tube conditions, fast fluxes of 1.5 to 2×10^{18} $n.m^{-2}.s^{-1}$ are desirable for timely irradiations to end-of-life fast fluences; accordingly, such accelerated aging studies must presently be performed in foreign research reactor facilities.

NRU is also utilized for research in support of the safety of power reactor fuels. In particular after the Chernobyl accident, to resolve concerns about fuel behaviour under high temperature and severe accident conditions, a new fuel loop, the Blowdown Test Facility (BTF) was installed in one of the existing loop positions. Thus, NRU continues to be adapted to meet the main irradiation requirements of the CANDU program.

Since NRU's inception, extracted neutron beams have been utilized for basic and applied research that exploits the neutron's unique ability to determine the bulk

properties of matter without causing significant material damage. Eight beams are currently used, one for neutron radiography and seven for neutron scattering. One of the spectrometers is dedicated to the determination of residual strain deep inside engineering components.

Additionally, NRU has been used to produce commercial radioisotopes on a large scale. During the early years of NRU operation, the production of ^{60}Co for cancer therapy was of major importance; however, as CANDU power reactors began to produce large quantities using (byproduct) neutrons that had to be absorbed in cobalt flux adjuster rods, ^{60}Co production in NRU shifted to small quantities of very high specific-activity materials. J-rod irradiations shifted to the production of ^{14}C and other isotopes, e.g. ^{131}I from tellurium and ^{192}Ir, became important. The radioisotope that has come to dominate NRU production, however, has been ^{99}Mo produced as a fission product. As the development and wide distribution of technetium generators and radiopharmaceuticals combined to make Tc-99m the most widely used radioisotope for nuclear medicine, the conversion of NRU to 93% enriched-uranium-aluminum-rodded fuel provided a unique opportunity for efficient ^{99}Mo production in targets based on the CRL metal-fuel technology. In the early 1990s, NRU, with backup from NRX, has now established AECL as the dominant world producer of fission product ^{99}Mo.

The NRU reactor has successfully operated for more than 35 years, and for more than 20 years with the current vessel. A program of upgrading and repairs to the reactor process and safety systems is expected to permit the NRU reactor to continue operating until the end of this decade.

5.3 Whiteshell Reactor-1 (WR-1)

In the late 1950s when CRL had grown to the maximum size considered optimal for nuclear research and development, the Whiteshell Laboratories (WL) were established in eastern Manitoba. The central experimental facility at the new establishment was a unique reactor called WR-1 (**W**hiteshell **R**eactor-**1**) (Figure 11) which used a mixture of terphenyls as a high temperature (300-400°C) but low pressure (1.1-2.2 MPa) liquid coolant. Beginning in 1965 November, WR-1 operated for nearly twenty years, to demonstrate the feasibility of an organic-cooled version of the CANDU power reactor. In the early 1990s decommissioning of WR-1 was initiated as part of AECL's rationalization of research reactor operation. The technical specifications of WR-1 are summarized in Table 2.

Although WR-1 is no longer operational it represents an important stage in the evolution of Canadian research reactor design beyond NRX and NRU. To avoid the need for vessel replacement, the WR-1 calandria was fabricated from stainless steel instead of aluminum. The hexagonal core lattice (Figure 12), with a pitch distance of 235 mm, provided for 53 fuelable sites of which 24 were fitted

with 99 mm diameter (Douglas Point size) calandria tubes and 29 with 121 mm diameter (Pickering or Bruce size) calandria tubes. Each site accommodated a 2.5 m long pressure tube of stainless steel or zirconium alloy and five CANDU-length fuel bundles. Any fuel channel could be connected to one of the four test loops whose cooling circuits were located in close proximity to the reactor assembly. Reactivity control was entirely provided by adjustment of the heavy water level in the core region. The moderator was sprayed into the top of the calandria and flowed downward over a doughnut-shaped weir (Figure 13) into a dump space below the core; regulating the differential helium pressure between the dump space and the top of the core provided moderator height control in the core region; fast shutdown was achieved by safety system actuation (using 2-out-of-3 voting logic) of helium dump lines which rapidly equalized the helium pressure.

Figure 11:
WR-1 Reactor

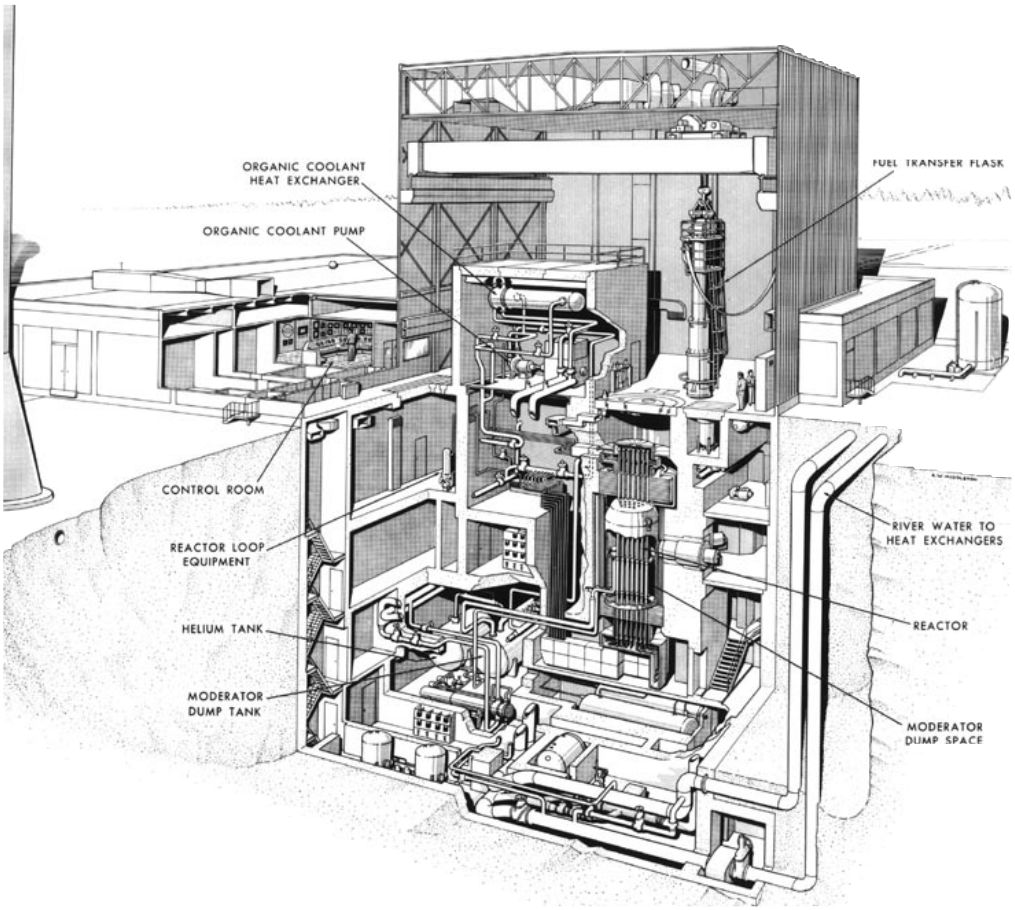
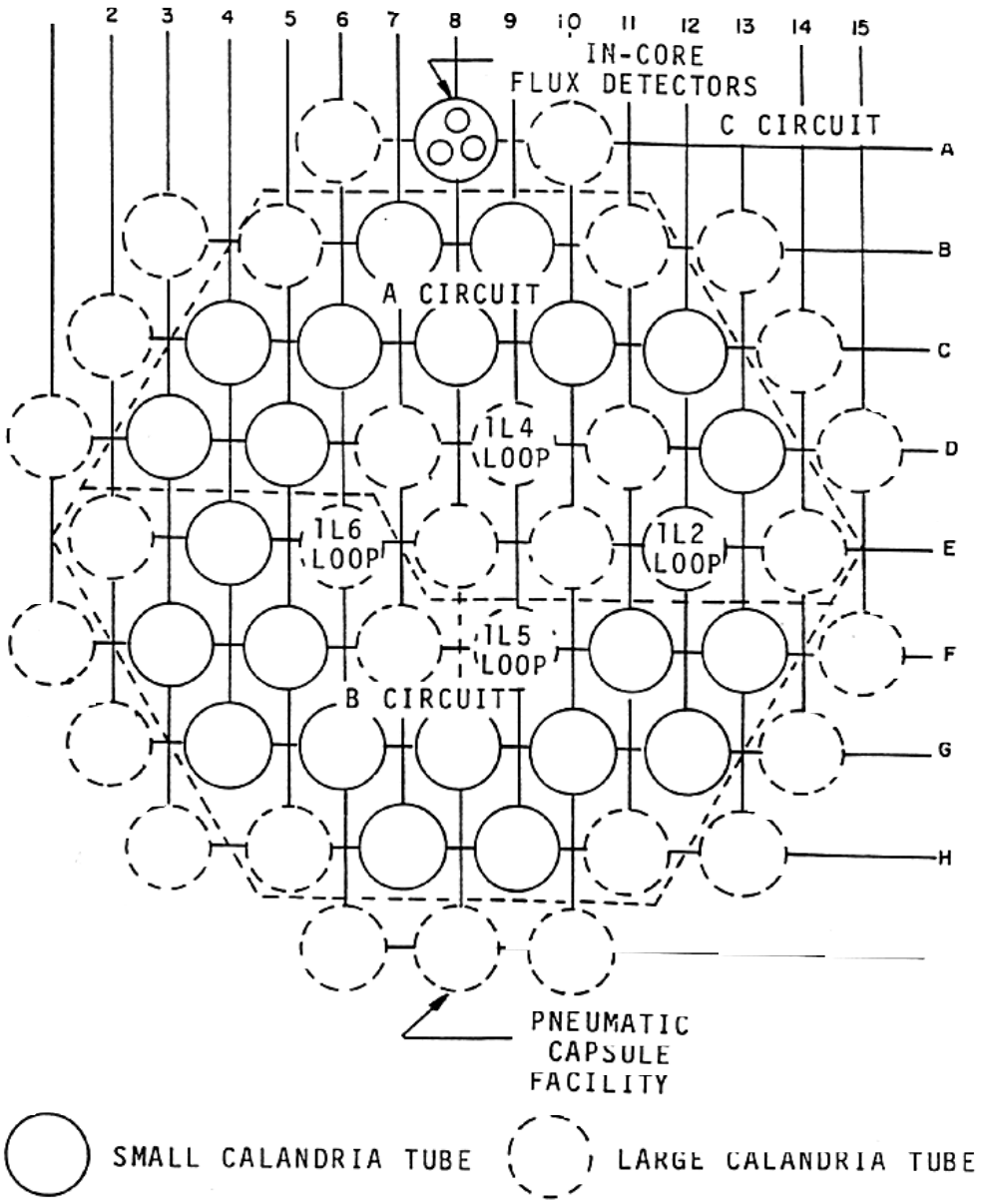


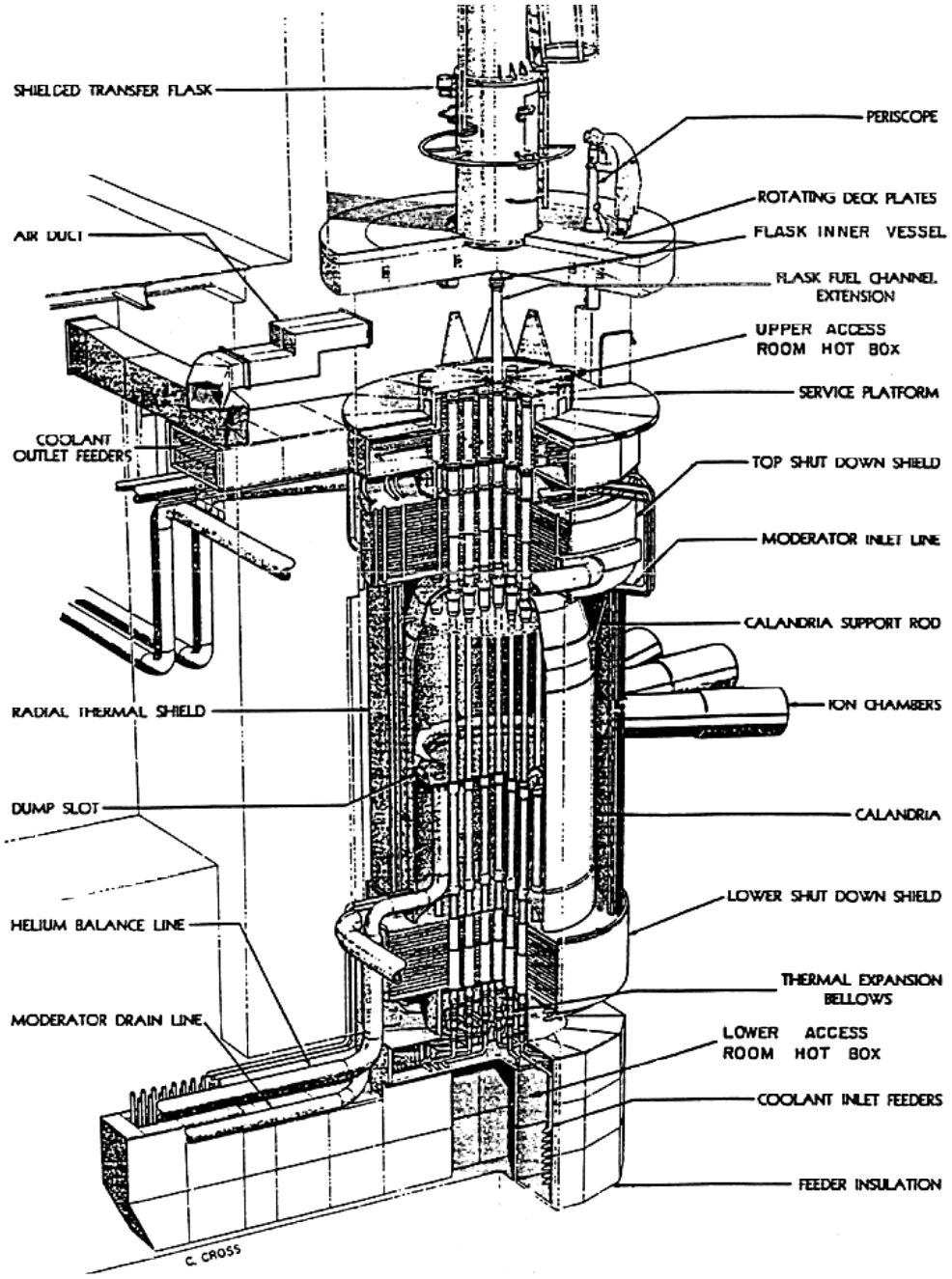
Figure 12:
WR-1 Core Lattice



The reactor was cooled by three independent organic cooling circuits, each with about 20 MW capacity. Initially, 18-rod, zirconium-alloy-clad, 2.4% enriched UO_2 fuel bundles were employed in the central 37 sites. Subsequently, when the core was expanded to 53 sites, all of which were converted to use zirconium-alloy pressure tubes, lower-fissile-content fuel was used and uranium monocarbide eventually displaced uranium dioxide as the fuel meat. Three of the loops were cooled with organic and fuelled with 5.0% enriched UC fast-neutron fuel assemblies that contained 76 mm diameter irradiation holes. Materials test studies involving the irradiation of creep and growth specimens were conducted in the fast-neutron sites at (> 1 MeV) fluxes of up to

1 x 10^{18} $n.m^{-2}.s^{-1}$. A 400 kW light-water-cooled loop enabled the testing of bundles of up to six CANDU-size fuel elements. WR-1 also contained a three-position pneumatic capsule facility with thermal neutron fluxes up to 6 x 10^{17} $n.m^{-2}.s^{-1}$.

Figure 13:
WR-1 Reactor Cutaway



5.4 MAPLE-X10

The MAPLE (**Multipurpose Applied Physics Lattice Experiment**) family of research reactors is being developed by AECL to meet Canadian and international requirements for advanced neutron sources. The contemporary requirements include high neutron fluxes for radioisotopes production, for small scale materials testing and analysis, and for scientific, medical and commercial applications of neutron beams.

The MAPLE design is an open-tank type light water-cooled and heavy water-reflected reactor within a light water pool. The reactor assembly consists of an inlet plenum, a grid plate supporting the core, the core structure and a chimney (see Figure 14).

In normal operation a MAPLE reactor primary coolant circuit forces about 90% of the pumped light water flow through the reactor core and bypasses about 10% of the pumped flow through the water pool surrounding the reactor assembly. The bypass flow leaves the lower plenum of the reactor via parallel flow diode orifices, which have flow resistances depending on the flow direction. The bypassed flow returns from the pool by flowing down in the chimney (open at its top and completely submerged in the pool), to join the main flow in the primary coolant circuit just above the core. The flow resistances and flow rates are selected such that the flow in the chimney is downwards toward the core.

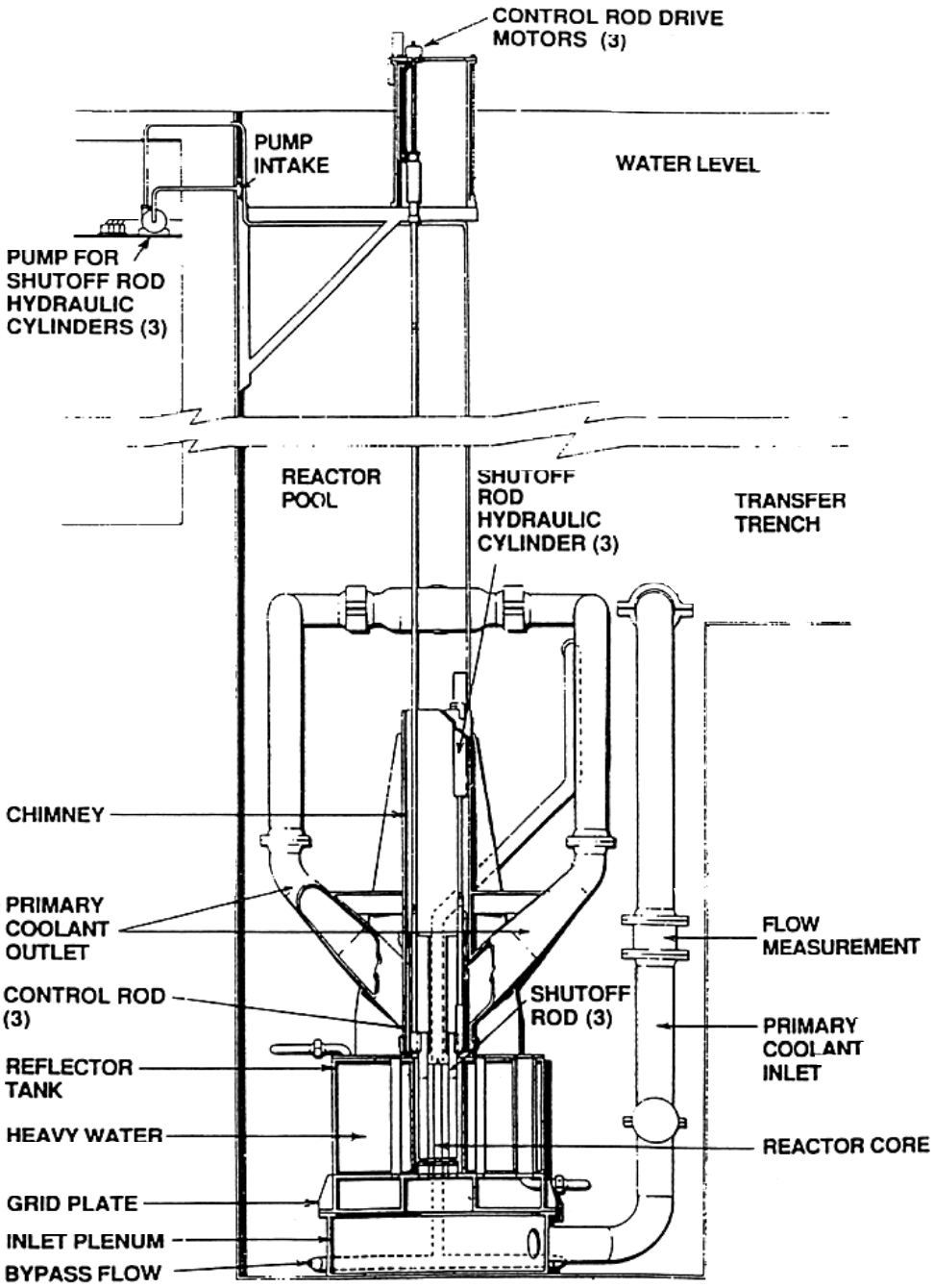
After a loss of pumping or after a pipe break in the primary coolant circuit the normally forced bypass flow comes to a halt and a reversed direction natural circulation flow becomes established through the diode orifices (with low flow resistance in the reverse flow direction), through the lower plenum, the core and the chimney back to the pool. Thus the MAPLE reactor has lots of inherently passive core cooling capability.

Two MAPLE-type research reactors have been designed by AECL: the 10 MW(th) MAPLE-X10 which will provide AECL with dedicated radioisotope production capability and the 30 MW(th) KMRR (Korean Multipurpose Research Reactor) which will provide South Korea with fuel-irradiation, materials testing and basic research capability.

The MAPLE-X10 prototype employs a compact (63 L), low enrichment uranium-fuelled, light water-cooled and -moderated core within a radial reflector of heavy water to supply neutrons efficiently to a variety of irradiation facilities in the core and reflector. The core grid accommodates a hexagonal arrangement of 19 fuelable sites. Assemblies of 36 fuel rods latch into hexagonal zirconium-alloy flow tubes. Reactivity control assemblies of 18 fuel rods latch into circular flow tubes in the six middle-outer lattice positions. Reactivity compensation and reactor shutdown are provided by hafnium cylinders that insert into the water annuli outside the circular flow tubes. The fuel is 19.7% enriched U_3Si-A1

extruded as 6.35 mm diameter rod within a coextruded finned aluminum cladding; this fuel has been developed as a proliferation-resistant replacement for NRU and the reference fuel for MAPLE reactors. Radially surrounding the core region is an annular cylindrical zirconium-alloy vessel containing the heavy water reflector. Table 2 presents other technical specifications.

Figure 14:
MAPLE-X10 Schematic



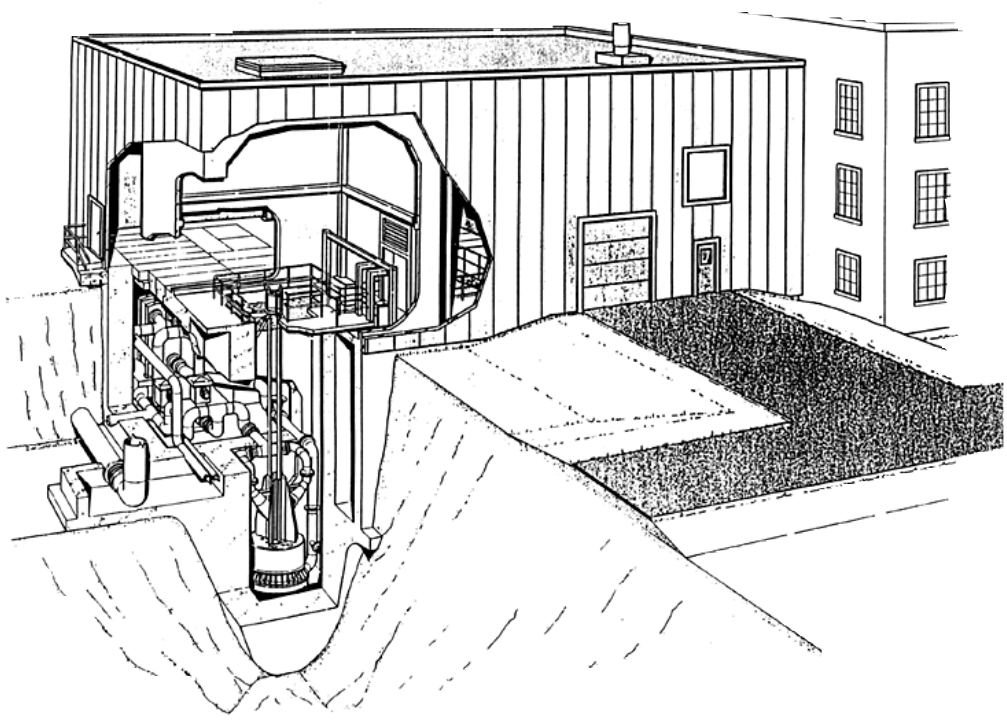
Dynamically pressurized light water enters the vertical reactor assembly via a stainless steel inlet plenum and flows upward past the fuel assemblies into an open chimney. A pump draws the heated water via two nozzles at the sides of the chimney through outlet piping to a plate-type heat exchanger and returns cooled water to the inlet plenum. Flow diodes on the inlet plenum direct about 10% of the inlet water to the bottom of the pool in which the reactor assembly sits, thereby creating downflow in the upper part of the chimney; the diodes also provide a low-resistance flow path for establishing natural convection cooling to the pool during shutdown and loss-of-pumped-flow conditions. An elevated accumulator tank connected to the inlet plenum provides surge flow through the core to ease the transition from forced-to natural-convection cooling. The chimney also houses the parked reactivity control devices and provides access to the core for fuel and irradiation target handling.

A digital computer system performs power regulation, process control, and data collection. It controls the reactor by vertically positioning a set of three hafnium absorbers and by manipulating other process control devices. The operator employs a dual keyboard/display console to interact with the control system which is designed to prevent operator action that might drive the reactor to an unsafe state.

For reactor shutdown, Shutdown System No. 1 (SDS1) inserts a set of three hafnium shutoff absorbers that are normally held poised above the core by hydraulic cylinders. A second independent shutdown system initiates a partial dump of the heavy water reflector and de-energizes electromagnetic latches to insert the three hafnium control system absorbers.

The MAPLE-X10 prototype facility (Figure 15) is under construction at CRL where it will commercially produce key short-lived radioisotopes (such as ^{99}Mo, ^{125}I and ^{192}Ir) and provide neutron-transmutation doping of silicon. In support of its construction and licensing, an AECL development program is underway to verify the performance of reactor components and characteristics unique to the MAPLE concept during both normal operating and upset conditions. At its design power of 10 MW, MAPLE-X10 will produce a peak thermal neutron flux of 2×10^{18} n.m^{-2}.s^{-1} in the reflector and 4×10^{18} n.m^{-2}.s^{-1} in a central flux trap.

Figure 15:
MAPLE-X10 Reactor Artist's Drawing



6 Revolutionary Trends in Canadian Research Reactor Design

Over the first fifty years of the nuclear era, the evolution of Canadian research reactors has been guided by the pragmatic development and exploitation of appropriate technology for Canada. Each new facility has been engineered with the best available resources to extrapolate slightly from a current technology base to meet specific program requirements. In view of uncertainties in the technology base, each design has incorporated considerable flexibility to accommodate evolving priorities as well as to meet the initial objectives. This approach has resulted in several generations of multipurpose reactors with a common heritage of neutronic efficiency.

The focus on neutronic efficiency stemmed from the incentive for direct use of Canada's abundant uranium resources and the improbability of Canadian investment in uranium enrichment facilities. Dr. Laurence's lack of early success with natural uranium and the available impure graphite promoted interest in more efficient moderators, especially heavy water. The first nuclear engineering group in Montreal, which included French and British experts on heavy water systems, conducted exponential experiments primarily oriented to optimizing

the core configuration for ZEEP, the first Canadian critical facility. The experiments on alternative fuel-cladding materials established a preference for aluminum because of its low parasitic absorption of neutrons, relative to stainless steel.

Choosing natural uranium fuel and heavy water moderator as the basis of Canadian reactor technology resulted in large cores for the first three Canadian research reactors: 9 m^3 for ZEEP, 17 m^3 for NRX, and 23 m^3 for NRU. As a consequence, the neutron flux per unit power was low, 2 x 10^{16} $n.m^{-2}.s^{-1}.MW^{-1}$. Light water cooling was chosen for NRX because of the unavailability of large quantities of heavy water and the need to ensure efficient fuel cooling at surface heat fluxes of 1-2 $MW.m^{-2}$ with the large (36 mm diameter) uranium-metal rods. With heavy water becoming available when NRU was built, a single heavy water system was chosen to provide both cooling and moderation which maximized the neutronic efficiency without the cost and complexity of two separate systems. To provide more heat transfer area to limit NRU's surface heat flux to 2 $MW.m^{-2}$ without greatly enlarging the core relative to NRX, plate-type fuel was specified. Largely because of concerns about the potential for downgrading the heavy water via leakage, both NRX and NRU were tank-type reactors with relatively complex thermal and biological shields. It is noteworthy that NRX provides some diversity of shutdown methods by the partial heavy water dump and/or by the shutdown rods.

Both NRX and NRU evolved as their patterns of use changed. The most significant evolution occurred in the early 1960s with the shift away from natural uranium fuel after plutonium production ceased. With the introduction of highly-enriched fuel, the flux-to-power ratio became 3 x 10^{16} $n.m^{-2}.s^{-1}.MW^{-1}$ for both reactors. With fewer sites fuelled, NRUs available in-core irradiation space also greatly increased. The main benefits of the knowledge gained from building and operating NRX and NRU and their experimental facilities were the building of prototype CANDU reactors during the 1960s, the building of commercial CANDU nuclear power generating stations during the next two decades, and significant development of the technology for advanced fuel cycles.

The building of the PTR and MNR reactors in the late 1950s represented the broadening of Canadian interest from strict reliance on heavy water reactors. In both cases, the simplicity of the swimming-pool concept enabled to achieve the purpose of the facility at modest costs. The ratio of thermal flux to power for the MNR core is 8 x 10^{16} $n.m^{-2}.s^{-1}.MW^{-1}$.

WR-1 represented the evolution of Canadian research reactors beyond NRX and NRU with the provision of a full lattice of standard-sized CANDU fuel channels (24 Douglas Point size and 29 Pickering or Bruce size) and the use of a durable reactor vessel of stainless steel instead of aluminum. Any fuel channel could be connected to one of the test loops whose cooling circuits were located in close

proximity to the reactor. WR-1 demonstrated the feasibility of reactor control entirely by regulation of the heavy water level in the core region combined with a fast dump capability. The facility also successfully demonstrated the utilization of organic coolants for nuclear generation of electricity and combined high-grade-heat-production plus multipurpose research reactor applications.

The development of the SLOWPOKE-2 reactor is particularly significant for its exceptional neutronic efficiency, its high level of inherent, passive safety, and the minimal requirement for nuclear infrastructure to support the safe operation of a low neutron flux (2×10^{16} $n.m^{-2}.s^{-1}$ thermal peak) research reactor. The thermal neutron flux-to-power ratio (5×10^{17} $n.m^{-2}.s^{-1}$.MW-1) is the highest practical level for any reactor based on the fission of ^{235}U. Although the strong measures to limit the excess reactivity to half of prompt critical are not feasible in higher-flux reactors, the SLOWPOKE reactor avoids the need for engineered safety systems and full time operator attendance because the worst case transients do not pose a hazard to people or the integrity of the facility. Local and district heating reactors based on the SLOWPOKE research reactors are being developed by AECL.

The MAPLE concept combines the low enrichment uranium fuel technology developed for NRU with Canadian expertise in heavy water systems to provide an efficient neutron source (a thermal neutron flux in the heavy water reflector per unit power of 2×10^{17} $n.m^{-2}.s^{-}1.MW^{-1}$) for pool-type reactor facilities based on the MAPLE-X10 facility. The high efficiency of neutron generation will enable the 10 MW MAPLE-X10 reactor to take over the short-lived isotope production role of the much higher powered NRX and NRU reactors.

As of the fiftieth anniversary of the first reactor, NRX and NRU have been in operation for 45 and 35 years, respectively. NRU continues to act as the major national irradiation facility, performing fuel and materials testing in support of CANDU development, producing radioisotopes, and acting as a source of neutrons for research using extracted neutron beams. In view of its mature age, NRX now serves in a limited role as a backup isotope producer. Its mandate complete, WR-1 is being decommissioned. NRX will be decommissioned when the MAPLE-X10 facility begins radioisotope production in the mid-1990s. As NRU will require costly refurbishing if it is to continue to operate into the next century, AECL is presently considering its options for maintaining Canada's irradiation research capability.

7 Safety Assessment and Licensing of Canadian Research Reactors

While the safety assessment of the earliest low-power research reactors extended only to some fundamental issues such as critical mass prediction, control of reactivity, cooling needs, shutdown system evaluation, etc., the safety assessment of each ensuing research reactor has evolved to meet the latest requirements of the regulatory authority.

In developing a new research reactor design, AECL has focused on one overall safety objective, which is to protect individuals, society and the environment by establishing and maintaining the facility with effective defences against radiological hazards. This overall objective is supported by the following three objectives:

a. Radiation exposure within the facility and that due to any release of radioactive material from the facility shall be kept as low as reasonably achievable (ALARA) and below prescribed limits in all operational states; radiation exposures from accidents shall be mitigated.
b. The frequencies of and radiological consequences from accidents shall be within acceptable bounds.
c. There shall be no significant detrimental effects on the environment for all reactor operational states and those accidents taken into account in the reactor design; the impact resulting from accidents beyond the design bases shall be mitigated to the extent practicable.

The design of Canadian research reactors makes use of a "defence-in-depth" strategy to compensate for potential human errors, mechanical failures and unexpected occurrences. Abnormal events will be prevented, then mitigated, then accommodated - in order of importance; and, a series of barriers will prevent, reduce or slow down releases of radioactivity to the environment.

Prevention is provided by inherent reactor characteristics and by the reliability of the equipment employed in normal operation.

Mitigation is provided by redundant, diverse and testable shutdown systems, designed to arrest the event and to limit the consequence.

Accommodation means that features are provided to contain radioactive releases such that design targets for dose are met. For example, the MAPLE-X10 pool water, pool structure and the reactor hall confinement system will contain radioactive releases from the reactor core in the event of an event resulting in fuel damage.

8 Reading List for Further Information

1 B.W. Sargent, "Research in Neutron Physics at Chalk River: The Low Energy Pile at Chalk River", The Science and Engineering of Nuclear Power II, Chapter 5, pp. 58-69, Addison Wesley Press (1947).

2 R.E. Manson and H.E. Smyth, "The NRX Reactor, A General Description", AECL-2692, Atomic Energy of Canada Limited (1967 February).

3 W. Boyd, F.W. Gilbert, G.C. Laurence and I.N. Mackay, "The NRU Reactor", Proceedings of the Second International Conference on the Peaceful Uses of Atomic Energy, P/211, Vol. 10, p. 128, United Nations (1958).

4 A.E. Foster, "ZED-2 . . . Canada's Newest Research Reactor" AECL-1301, Atomic Energy of Canada Limited (1960 November).

5 B.M. Townes and J.W. Hilborn, "The SLOWPOKE-2 Reactor with Low Enrichment Uranium Oxide Fuel", AECL-8840, Atomic Energy of Canada Limited (1985 June).

6 D.G. Turner, "The WR-1 Reactor, A General Description", AECL-4763, Atomic Energy of Canada Limited (1974 November).

7 A.G. Lee, W.E. Bishop and W. Heeds, "Safety Features of the MAPLE-X10 Reactor Design", AECL-10262, Atomic Energy of Canada Limited (1990 September).

8 A.G. Lee, R.F. Lidstone and J.V. Donnelly, "Developing the MAPLE Materials Test Reactor Concept", AECL-10638, Atomic Energy of Canada Limited (1992 May).

Table 1

Technical Specification for Low and Medium Power Canadian Research Reactors

	ZEEP	ZED-2	PTR	SLOWPOKE-2	MNR
GENERAL					
Reactor Type	D_2O Tank	D_2O Tank	Pool	Pool	Pool
Thermal Power Output	10 W (max. 250 W)	200 W	10 kW	20 kW	5 MW
Utilization	lattice experiments physics measurements trace RI production	lattice experiments physics measurements	physics measurements	activation analysis training physics measurements	activation analysis research training
Date of Initial Criticality	1945 September	1960 September	1957 November	first unit in 1971	1958 September
FUEL					
Fuel Material	U-metal or UO_2	U-metal or UO_2	U-A1 alloy	U-A1 alloy UO_2	U-A1 alloy
Fuel Enrichment in U-235	natural	natural	93%	93% 19.9%	93%
Subassembly Form	~2.5 m long rods	various	plates	rods	plates
Subassembly Dimensions	32.5 mm diameter	<0.14 m dia. x 3.65 m	0.5 mm x 73 mm x 610 mm	4.2 mm dia. x 220-227 mm	0.5 mm x 63 mm x 600 mm
Cladding	aluminum	various	aluminum	A1 Zircaloy 4	aluminum
Cladding Thickness	1-2 mm	various	0.5 mm	0.5 mm	0.4 mm
Subassembly Rating (kW/m)	~0	~0	~0	0.4 0.7	-
Assemblies	single rods	<340 kg	10 plates	298-317 rods 198 rods	18 plates (contr. 9)
Assemblies Fissile Content (kg)	variable	variable	0.165	0.8 1.12	0.2 (0.1)
Assembly Heat Transfer Area (m^2)	-	-	0.89	1.1 0.74	1.36 (0.68)
Maximum Surface Heat Flux (MW/m^2)	-	-	-	0.02 0.03	0.4
CORE					
Reactor Vessel	A1 cylinder	A1 cylinder	core grid/reflector	aluminum	core grid/reflector
Vessel Dimensions	2.1 m ID x 2.6 m high	3.36 m ID x 3.34 m high	1.65 m x 1.65 m x 0.76 m	0.6 m dia. x 4.3 m	1.65 m x 1.65 m x 0.76 m
Core Dimensions	2.1 m dia. x 2.6 m high	3.36 m ID x 3.34 m high	0.24 m x 0.4 m x 0.6 m	230 mm dia. x 220-227 mm	0.24 m x 0.4 m x 0.6 m
Core Volume (L)	9000	<29600	66	9.1-9.4	124
Number of Fuel Sites	variable	variable	17	1	28 and 6 control
Fuel Channel Material	variable	variable	-	-	-
Fuel Channel Dimensions	variable	variable	-	-	-
Number of Test Loops	-	-	-	-	-
Total Number of Lattice Sites	variable	variable	9 x 9 grid	1	6 x 9 grid
Lattice Pitch (mm)	120-305	120-305	80	-	80
Coolant	D_2O	variable	H_2O	H_2O	H_2O
Coolant Flow Velocity (m/s)	natural circulation	natural circulation	natural circulation	natural circulation	0.9
Peak Thermal Flux ($10^{**}18$ $n/m^2/s$)	0.000001	0.00002	0.0015	0.01	0.4
Peak Fast Flux ($10^{**}18$ $n/m^2/s$)	-	-	0.0045	0.01	0.2

Table 1 (continued)

Technical Specification for Low and Medium Power Canadian Research Reactors

	ZEEP	ZED-2	PTR	SLOWPOKE-2	MNR
REACTIVITY CONTROL					
Reactor Regulation	4 Cd-clad st.steel rods	D_2O-level control	2 B4C & 1 st.steel rod	1 Cd-A1 rod	5 Ag-In-Cd shim rods & 1 st.steel regulating rod
Maximum Excess Reactivity	variable	variable	-	3.4 mk	62 mk
Prompt Neutron Lifetime (ms)		0.75	0.07	0.07	0.051
Shutdown System No. 1	8 Cd-clad st. steel rods	12 Cd-st. steel rods	2 B4C rods	none	override control rods
Shutdown System No. 2	D_2O Dump	D_2O Dump	-	-	-
Shutdown System Reactivity Worth	-	-	60 mk	-	120 mk
MODERATOR MATERIAL	D_2O			H_2O	
REFLECTOR					
Material (Axial)	Graphite	Graphite	H_2O	Be	H_2O
Thickness (Axial)	0.76 m (bottom)	0.9 m (bottom)	thick	0-100 mm (T), 100 mm (B)	thick
Material (Radial)	Graphite	Graphite	Graphite	Be	H_2O/Graphite
Thickness (Radial)	0.93 m	0.6 m	0.46 m	100 mm	thick/76 mm
Number of Vertical Sites	-	-	-	5 (Be) & 5 (H_2O)	19
Number of Beam Tubes	none	none	none	none	6
Peak Thermal Flux (10**18 $n.m^2/s$)	-	-	-	0.01	0.05
THERMAL SHIELDING					
Material (Axial)	-	-	-	-	H_2O
Thickness (Axial)	-	-	-	-	~7.3 m
Material (Radial)	-	-	-	-	H_2O
Thickness (Radial)	-	-	-	-	~0.85 m
BIOLOGICAL SHIELDING					
Material	H_2O	H_2O	H_2O	H_2O	barytes concrete
Thickness	1 m	1 m	~4 m	4.2 m	1.85 m
CONTAINMENT					
Type	Conventional Building	Conventional Building	Room in Conventional Building	Conventional Building	Reinforced concrete building
Inside dimensions	20 x 17 m x 10 m high	22 x 13 m x 14 m high	Pool: 2.6 m dia. x 6.1 m deep	25 x 22 m x 17 m high	25 m dia. x 22 m high x 6.1 m deep

Abbreviations: RI radioisotopes
SDS1 Shutdown System no. 1

Table 2

Technical Specification for High Power Canadian Research Reactors

	NRX	NRU	WR-1	MAPLE-X10
GENERAL				
Reactor Type	H_2O-cooled D_2O Tank	D_2O Tank	Organic-cooled D_2O Tank	Open-Tank-in-Pool
Thermal Power Output	42 MW	200 MW 135 MW	60 MW	10 MW
Utilization	materials testing RI production	materials testing RI production beam research	OCR demonstration materials testing	RI production MAPLE demonstration
Date of Initial Criticality	1947 July	1957 November	1965 November	end of 1994
FUEL				
Fuel Material	U-metal/UO_2 U-A1 alloy	U-metal U-A1 alloy	UO_2, UC	U-Si-A1
Fuel Enrichment in U-235	natural 93%	natural, 93%, 20%	1.2-2.4% 1.3-2.0%	19.7%
Subassembly Form	rods	plates rods	18-rod (bundle) 14-rod	rods
Subassembly Dimensions	35.8 mm dia. 6.35 mm dia.	4 mm x 43 mm 5.5 mm dia.	14 mm (495 mm) 13 mm	6.35 mm dia. x 600 mm
Cladding	aluminum	aluminum	Zr-2.5%Nb	aluminum
Cladding Thickness	1.3 mm 0.76 mm	1 mm 0.76 mm	0.35 mm	0.76 mm
Subassembly Rating (kW/m)	205/100 54	110	45 76	85
Assemblies	single rod 7 rods	5 plates 12 rods	5 bundles	18 or 36 rods
Assemblies Fissile Content (kg)	0.384 kg 0.384 kg	0.384 kg 0.493 kg	0.7-1.4 0.7-1.0	0.21 or 0.42
Assembly Heat Transfer Area (m^2)	0.37 0.77	1.32 1.22	1.9 1.4	0.43 or 0.86
Maximum Surface Heat Flux (MW/m^2)	1.75/1.35 2.2	2.0 5.0	1.0 1.8	3.5
CORE				
Reactor Vessel	aluminum	aluminum	stainless steel	Zircaloy
Vessel Dimensions	2.7 m ID x 3.2 m high	3.51 m ID x 3.66 m high	2.7 m dia. x 2.4 m high	1.6 m dia. x 0.9 m high
Core Dimensions	2.67 m dia. x 3.05 m high	3.1 m dia. x 3.0 m high	1.8 m dia. x 2.3 m high	366 mm dia. x 600 mm
Core Volume (L)	17000	23000	5900	63.2
Number of Fuel Sites	192	202 80-105	53	19
Fuel Channel Material	aluminum	aluminum	st.steel or Zr-2.5%Nb	Zircaloy
Fuel Channel Dimensions	42 mm ID 35 mm Id	60 mm ID 50 mm ID	83 mm ID (std)	60 mm dia. or 74 mm hex
Number of Test Loops	up to 8	up to 5	4	none
Total Number of Lattice Sites	199	227	54	19
Lattice Pitch (mm)	193	197	235	80
Coolant	H_2O	D_2O	Monsanto OS-84	H_2O
Coolant Flow Velocity (m/s)	2.7 to 4.0	9-11	11-13	5.5-7
Peak Thermal Flux ($10^{**}18$ $n/m^2/s$)	0.7 1.2	3.0 4.0	1.6	2
Peak Fast Flux ($10^{**}18$ $n/m^2/s$)	1.0 2.0	0.35 0.65	8	0.9

Table 2 (continued)
Technical Specification for High Power Canadian Research Reactors

	NRX	NRU	WR-1	MAPLE-X10
REACTIVITY CONTROL				
Reactor Regulation	D_2O-level control	11 Cd & 7 Co absorbers 4 Co adjuster rods	D_2O-level control	3 Hf absorbers around 18-rod fuel
Maximum Excess Reactivity	42 mk ~65 mk	83 mk ~150 mk	89 mk	70 mk
Prompt Neutron Lifetime (ms)	~1	1.6	0.47	~0.08
Shutdown System No. 1	18 boron-carbide rods 6	override control rods	D_2O Dump	3 Hf shutoff tubes
Shutdown System No. 2	D_2O Dump	-	-	override regulation & D_2O
Shutdown System Reactivity Worth	~75 mk (SDS1)	213 mk	del k = -1.0	dump 140-160 mk (SDS1) 140 mk (Hf) 130 mk (D_2O)
MODERATOR				
REFLECTOR				
Material (Axial)	-	D_2O, H_2O	-	H_2O
Thickness (Axial)	-	0.3 m D_2O, 0.3 m H_2O	-	thick
Material (Radial)	Graphite	D_2O, H_2O	D_2O	D_2O
Thickness (Radial)	851 mm	0.2 m D_2O, 0.3 m H_2O	0.45 m	0.6 m
Number of Vertical Sites	92 (J rods)	107	none	22
Number of Beam Tubes	15	24	none	none
Peak Thermal Flux (10**18 $n.m^2/s$)	0.2	3	-	2.0
THERMAL SHIELDING				
Material (Axial)	steel/H_2O & A1/H_2O	steel & (T) 3 m H_2O	steel/H_2O	H_2O
Thickness (Axial)	0.9 m (T), 1.3 m (B)	0.6 m (T), 1.1 m (B)	1.1 m	8.5 m (T), 0.9 m (B)
Material (Radial)	iron	steel	steel/H_2O	H_2O
Thickness (Radial)	0.15 m	0.3 m	0.3 m	0.7-1 m
BIOLOGICAL SHIELDING				
Material	concrete	ilmenite concrete	ilmenite	H_2O/ilmenite concrete
Thickness	2.44 m	3 m	2.1 m	~8 m/~0.3 m
CONTAINMENT				
Type	conventional building vented confinement	conventional building vented confinement	conventional building vented confinement	reinforced-concrete hall vented confinement
Inside dimensions	34 m x 44 m x 27 m height	~40 m x ~80 m x 50 m height	63 m x 54 m x 36 m height	8 m x 8.5 m x 19 m height

Abbreviations: OCR Organic-cooled reactor
B bottom
T top2