CONTROL AND INSTRUMENTATION SYSTEMS FOR THE 600 MWe CANDU PHW NUCLEAR POWER PLANTS

Systèmes de contrôle et d'instrumentation pour les centrales nucléaires CANDU-PHW de 600 MWe

R.M. LEPP and L.M. WATKINS

Chalk River Nuclear Laboratories

February 1982
ATOMIC ENERGY OF CANADA LIMITED

CONTROL AND INSTRUMENTATION SYSTEMS FOR THE 600 MWe CANDU PHWR NUCLEAR POWER PLANTS

by

R.M. Lepp and L.M. Watkins

Contribution to the IAEA Guidebook on Nuclear Power Plant Control and Instrumentation

Chalk River Nuclear Laboratories
Chalk River, Ontario K0J 1J0

February 1982

AECL-7519
Systèmes de contrôle et d'instrumentation pour
les centrales nucléaires CANDU-PHW de 600 MWe

par

R.M. Lepp et L.M. Watkins

Résumé

Les systèmes de contrôle et d'instrumentation des centrales nucléaires CANDU sont conçus pour avoir la grande fiabilité et la bonne disponibilité requises pour que les strictes exigences relatives au fonctionnement et à la sécurité des centrales soient respectées. Pour atteindre ces buts, on a recours à une philosophie conceptuelle de "défense en profondeur". Les divers systèmes conçus pour répondre à ces exigences sont décrits ainsi que l'utilisation en grand des ordinateurs pour les fonctions importantes du contrôle de la centrale et de l'interaction homme-machine.
CONTROL AND INSTRUMENTATION SYSTEMS FOR THE 600 MWe CANDU PHN NUCLEAR POWER PLANTS

Chalk River, Ontario, Canada

ABSTRACT

The control and instrumentation systems for CANDU nuclear power plants are designed for high reliability and availability to meet stringent safety and operational requirements. To achieve these goals a "defense-in-depth" design philosophy is employed. The diversely functioning systems, designed to satisfy these requirements, are described along with the extensive use of computers for important plant control and man-machine functions.

TABLE OF CONTENTS

1. INTRODUCTION 2

2. REACTOR FUNDAMENTALS 2
   2.1 Pressure Tube Concept 2
   2.2 Natural UO₂ and D₂O 2
   2.3 Reactivity Feedback 2
   2.4 Reactor Kinetics 2
   2.5 Xenon Feedback 3

3. OVERALL CONTROL AND INSTRUMENTATION DESIGN PHILOSOPHY 3
   3.1 Defence-In-Depth 3
   3.2 Special Safety Systems 4
   3.3 Reactor Regulation 4
   3.4 Electrical Power Supplies 4

4. AUTOMATIC CONTROL SYSTEMS 4
   4.1 General 4
   4.2 Overall Plant Control 5
   4.3 Digital Computer Systems 5
   4.4 Reactor Instrumentation 6
   4.5 Reactor Regulating System 6
   4.5.1 Zonal Control Absorbers 7
   4.5.2 Mechanical Control Absorbers 7
   4.5.3 Adjusters 7
   4.6 Flux Mapping 8
   4.7 Control Strategies 8
   4.7.1 Reactor Startup 8
   4.7.2 Normal Operation 8
   4.7.3 Power Setbacks 9
   4.7.4 Power Steepbacks 9
   4.8 System Response to Disturbances 9
   4.9 Xenon Override and Load Following Capabilities 10
   4.9.1 Xenon Override 10
   4.9.2 Load Following Capabilities 10
   4.10 Reliability and Maintainability 11

5. REACTOR SAFETY SYSTEMS 11
   5.1 Shutdown System Number One 11
   5.1.1 General Description 11
   5.1.2 Logic 12
   5.1.3 Individual Trips 13
   5.2 Shutdown System Number Two 13
   5.3 Emergency Coolant Injection 15
   5.4 Containment 15
   5.4.1 Dousing System 16
   5.4.2 Containment Isolation Control 16

6. CONTROL ROOM DESIGN AND INFORMATION DISPLAY 16
   6.1 Main Control Area 16
   6.2 Main Control Room Panels 17
   6.3 Safety Related Display Instrumentation 18

7. ON-Power Refuelling System 18

8. ELECTRICAL POWER SYSTEMS 19

9. MISCELLANEOUS INSTRUMENTATION AND CONTROL SYSTEMS 20
   9.1 Radiation Protection 20
   9.1.1 General 20
   9.1.2 Fixed and Portable Area Monitoring 20
   9.1.3 Access Control 20
   9.1.4 Liquid Effluent Monitoring 20
   9.1.5 Gaseous Monitoring 20
   9.1.6 Containment Monitoring 20
   9.1.7 Environmental Surveillance 20
   9.2 Fire Protection 20

10. HEAVY WATER MONITORING 21
    10.1 Heavy Water Leak Detection 21
    10.2 Process Monitoring 21

11. FAILED FUEL DETECTION SYSTEM 21

12. LICENSING PHILOSOPHY 22

13. ACKNOWLEDGEMENTS 23

14. REFERENCES 23
1. INTRODUCTION

The instrumentation and control systems provided in a CANDU nuclear power plant include all systems required for

- automatic control of the reactor, balance of plant and auxiliary systems
- safe shutdown of reactor and auxiliaries
- on-power refuelling
- control of access to high-radiation areas
- detecting heavy water leaks
- plantwide monitoring of radioactivity
- fire protection
- failed fuel detection and location

The major differences between CANDU control and instrumentation systems and other reactor concepts are in reactor control, safety philosophy, on-power refuelling and the need for heavy water instrumentation. These are treated in sufficient detail so that Control and Instrumentation (C & I) specialists from countries about to embark on a nuclear program can compare the CANDU systems to other systems. The other C & I topics listed above are more common to all nuclear power stations and are therefore only briefly discussed.

The systems described herein are being offered as part of the CANDU PHWR* 600 MWe power reactor design [1] which is being marketed internationally. Changes can be incorporated into the design to conform to the different regulatory standards that exist throughout the world.

2. REACTOR FUNDAMENTALS

2.1 Pressure Tube Concept

The CANDU PHWR Reactor is a heavy water moderated, heavy water cooled, natural uranium fuelled reactor which utilizes the pressure tube concept. The pressure tubes containing the fuel run horizontally through the reactor core as shown in Figure 2.1. Pressurized heavy water carries the heat from the fuel to the steam generators.

Each pressure tube is insulated and insulated from the heavy water moderator by a concentric calandria tube and a gas annulus. Consequently the moderator system is operated at low temperature and pressure. The reactivity control and shutdown mechanisms reside in the low pressure moderator, thus simplifying their design, construction and maintenance and eliminating the possibility of their ejection in an accident situation. As well, this cool moderator can act as a heat sink under certain accident conditions.

2.2 Natural UO₂ and D₂O

The use of natural uranium fuel in an optimized lattice, and heavy water as moderator and coolant, combined with the capability to refuel the reactor while at full power, gives the CANDU reactor its good neutron economy and low excess reactivity. This results in a power reactor with very low fuel costs.

2.3 Reactivity Feedback

The only reactivity feedback effects that are of any consequence are the coolant density (or void), fuel temperature and xenon effects. Since the moderator temperature is controlled independently of the primary coolant, it does not contribute any significant reactivity feedback.

The fuel temperature reactivity coefficient is negative and therefore stabilizing whereas the coolant void reactivity coefficient is positive and therefore destabilizing. The sum of these, and lesser reactivity feedback effects, is a power reactivity coefficient that is near zero under normal operating conditions.

2.4 Reactor Kinetics

The prompt neutron lifetime in a CANDU lattice is relatively long (~0.9 ms) and the delayed neutron fraction (~0.005) is enhanced by the presence of photoneutrons. These two factors, combined with the subdivision of the primary coolant circuit into two separate loops, slow down a potential power excursion considerably, as compared to typical light water reactors [2].
Figure 2.2 shows typical power pulses for the "hottest fuel bundle" due to a Loss-of-Coolant Accident (LOCA) resulting from 20%, 30% and 100% inlet header breaks followed by the action of one of the shutdown systems in the 600 MWe CANDU PHWR reactor. The additional energy stored in the fuel during these transients (>2.6 full power seconds) is more than a factor of 3 below that required to cause fuel damage (>9 full power seconds). Hence spontaneous fuel breakup is not a safety concern during a LOCA in CANDU PHWR.

Figure 2.2 HOT BUNDLE POWER TRANSIENT FOLLOWING A BREAK IN ONE REACTOR INLET HEADER

2.5 Xenon Feedback

A reactor that is unstable due to xenon feedback effects would undergo slow, divergent spatial power oscillations (e.g. side to side or end to end) which, at constant total power, would overheat some fuel. The CANDU PHWR reactor is equipped with a continuous, automatic spatial control system that prevents xenon oscillations and corrects flux distortions due to other causes.

The xenon load at full power is ~29 mk. When the reactor power is rapidly decreased, the xenon concentration increases over a period of a few hours and then decays. The resulting variation in core reactivity is made up by the movement of zonal control absorbers and, if necessary, the removal of some adjuster rods from the core.

In the event of a shutdown from full power, the adjuster rods have enough reactivity to restart the reactor within 1/2 hour, before poisoning out. A typical startup power history, using the 7 banks of adjusters, is shown in Figure 2.3.

Figure 2.3 REACTOR POWER TRANSIENT DURING A START-UP FOLLOWING A 30 MIN SHUTDOWN

3. OVERALL CONTROL AND INSTRUMENTATION DESIGN PHILOSOPHY

3.1 Defence-In-Depth

The CANDU C & I systems are designed for high reliability and availability to meet stringent safety and operational requirements. To achieve these goals a "defence-in-depth" design philosophy is employed. On the reactor design itself, this takes the form of multiple physical barriers to radioactive release, including the uranium oxide fuel, the fuel sheath, the primary heat transport system, the containment system and the exclusion zone of the site. "Defence-in-depth" manifests itself in the C & I design in such ways as providing diversely functioning systems that can do the same job, procuring components for different systems from different suppliers, using physical separation of systems and components that provide back-up functions to each other and annunciating and correcting minor system upsets before they become major.

The final elements in this "defence-in-depth" approach are the Special Safety Systems that shut down the reactor, provide long-term cooling of the fuel and contain potential releases of radioactivity. There are four Special Safety Systems:

- Shutdown System Number One (SDS-1)
- Shutdown System Number Two (SDS-2)
- Containment System (CS)
- Emergency Coolant Injection (ECI)
3.2 Special Safety Systems

Each system is completely independent from the others, with its own sensors, logic and actuators. Each system employs triplicated logic, meets the IAEA single failure criterion, and is designed with built-in features to facilitate on-line testing.

The provision of two shutdown systems, either of which is capable of shutting the reactor down for the entire spectrum of postulated initiating events, is a unique feature of the CANDU C & I design. The two shutdown systems are geometrically and functionally independent of each other, and each is designed such that at least two generally diverse trips (trips based on functionally different measured variables) are activated by any single process failure.

The Special Safety Systems, in turn, are to the greatest extent possible free from operational connection with any of the process systems, including the Reactor Regulating System.

To provide protection against postulated initiating events of low probability such as fires or local missiles, the plant systems, both process and safety, are divided into two groups.

All Special Safety Systems and associated support services are designated as Group 2 and located in a physically separate area from the normal plant process systems in Group 1. In the event that one group is disabled by a common mode incident, the following capability is preserved:

- Reactor shutdown
- Decay heat removal
- Preservation of radiation release barrier
- Supply of information required for the state of the nuclear steam supply.

Defence against earthquakes is facilitated by seismically qualifying all Group 2 equipment, and the main control room is sufficiently qualified against earthquakes that it is possible for the operator to remain in it after an earthquake. If the main control room were lost for any reason, the essential reactor systems could be regulated from a secondary control area, which is geographically isolated from the main control room.

3.3 Reactor Regulation

An essential principle of CANDU C & I philosophy is that major plant control, annunciation and display functions should be computerized. The resulting high degree of automation and improved man-machine interface leave the operator free to concentrate on unusual occurrences, and have the additional advantage during commissioning of facilitating design improvements. A dual computer system concept is employed to provide the required high reliability.

Each computer is capable of complete station control and transfers control automatically either completely, or by function, to the other on detection of a fault. Changeover from one to the other occurs when internal hardware and software self-checking, or an external "watchdog timer", detect a system fault. System faults result in an automatic reloading of memory followed by a computer restart, or a complete transfer of control to the other computer, depending on the severity of the condition detected.

The control functions are designed to be independent of each other, to be immune to single input faults and to ensure that all controlled devices produce their desired outputs. The system depends on redundant information, rationality checks and feedback from the controlled devices. In effect, each function determines for itself if it should continue or relinquish control. A function that relinquishes control produces an alarm for each abnormal condition and turns itself off, leaving its outputs in a safe state. Control of the function automatically transfers to the other computer.

The computer system plays an integral role in the defence-in-depth approach and attempts to intercept system upsets before they become reactor trips. This it does by control algorithms that reduce reactor power when certain variables are outside their acceptable control ranges, thus restoring normal operating conditions without invoking a trip.

3.4 Electrical Power Supplies

Finally, there is "defence-in-depth" in the electrical power supplies. Each channel of the triplicated safety systems is fed from independent uninterruptible power supplies. Similarly each computer of the dual computer system is fed from a separate independent uninterruptible power supply to avoid loss of control capability due to a common power supply fault.

4. AUTOMATIC CONTROL SYSTEMS

4.1 General

The maximum practical amount of automatic control is incorporated in the CANDU design, to reduce the routine workload of the operating staff. This frees them for high level monitoring of overall plant status, thereby enhancing operating efficiency.

Two identical, independent digital computers are used for direct digital control, and almost all major control functions are computer controlled. Each computer is capable of complete station control and will transfer control automatically to the other computer on detection of a fault. An availability in excess of 99.8 per cent has been achieved with this system [3].

The control systems are designed to make the plant tolerant to expected and unexpected transients to avoid unnecessary plant outages. A design objective has been to make the intervention of the shutdown systems unnecessary in all cases except
real accidents in which public safety is in question.

The loss-of-line to the bulk electrical system and a turbine trip are two transients that the control system must periodically cope with. This it does by rapidly reducing reactor power to about 80 percent combined with discharging steam to the turbine condenser or to the atmosphere. Following such a transient, the reactor system is capable of sustained operation at any load between 55 and 100 percent of rated capacity.

Some CANDU reactors are provided with control equipment for cogeneration — generation of electricity and the provision of process steam to a nearby industrial process.

4.2 Overall Plant Control

The control of the reactor and its steam loads is accomplished by keeping the boiler steam-drum pressure constant. Two distinct control modes exist for doing this:

- **NORMAL** is the usual control mode at high power. The turbine load is set to the desired value and the reactor power adjusts automatically to maintain constant steam generator pressure.

- **ALTERNATE** is the usual control mode at low power (below 20%) and during upset conditions. The operator specifies the reactor setpoint and the plant steam loads are adjusted to maintain steam generator pressure.

The main components of the overall plant control loops are shown in Figure 4.1, with the control computer programs in a separate box.

![Figure 4.1 BLOCK DIAGRAM OF OVERALL PLANT CONTROL](image)

The primary functions of the main programs shown are:

(i) **Unit Power Regulator** — Changes turbine load as demanded by the operator or by the Remote Control Centre, and maintains the desired generator load.

(ii) **Steam Generator Pressure Controller** — In the NORMAL mode it controls boiler pressure by changing the reactor power setpoint. In the ALTERNATE mode it adjusts the plant loads.

(iii) **Reactor Flux Control** — Adjusts the reactor's reactivity devices to maintain the neutron power specified by the Demand Power Routine.

Most of the other programs in the computer are described separately.

The plant loads are shown in Figure 4.1, and include:

(i) **Turbine** — Normally controlled from the Unit Power Regulator. Hardware unloaders protect the turbine during abnormal conditions.

(ii) **Condenser Steam Discharge Valves** — Normally controlled from the Steam Generator Pressure Controller. Separate hardware logic closes these valves on low condenser vacuum to protect the condenser.

(iii) **Atmospheric Steam Discharge Valves** — Normally controlled from the Steam Generator Pressure Controller.

(iv) **Process Steam** — Controlled from the Steam Generator Pressure Controller in response to flow demands from the external process, or at low flows, in response to pressure control requirements.

4.3 Digital Computer Systems

Digital computers are used for station control, alarm annunciation and data display. The design of this system has been continually improved from the first direct digital control system in the Douglas Point generating station which went into operation in 1966.

The current station-control and data acquisition uses the dual configuration shown in Figure 4.2, consisting of two identical computers, one on hot-standby, connected by a data link and a shared display system[4]. No analog backup is needed because the availability of the dual computer system is more than 99.8 percent.

The high reliability of this dual computer control system results from a combination of highly reliable solid-state hardware and a self-checking system.

Software and hardware faults are detected by internal self-checking plus an external "watchdog timer". Detection of a fault results in individual control tasks being transferred to the other computer. A restart system, that automatically reloads the core memory from the disc memory and restarts the computer, is combined with the fault detection
to provide a system practically immune to transient faults.

Figure 4.2 CONFIGURATION OF PLANT COMPUTER SYSTEM

An extensive computer driven alphanumeric/graphics cathode ray tube (CRT) display system provides the operator with alarm annunciation and operating data. These colour CRTs are a modern replacement for most of the panel instrumentation found in conventional control rooms [5]. Direct-wired window annunciators are provided for group alarms as backup to the computerized alarm system. The operator communicates with the computers through keyboards in various locations in the control room.

4.4 Reactor Instrumentation

Separate nuclear instrumentation systems are provided for regulation and safety to measure reactor neutron flux over the full operating range of the reactor. As summarized in Table 4.1, proportional counters, uncompensated ion chambers and self-powered in-core flux detectors are used to give a continuous measurement of reactor power from source level to 150 percent of full power, i.e. approximately ten decades. A minimum overlap of 1 decade is provided between successive ranges of nuclear instrumentation.

![Diagram of the Reactor Regulating System](image)

Proportional startup counters are used only during the first criticality or for starting after a very long shutdown. Following high power operation, heavy water reactors retain a sufficient neutron source to keep the ion chambers on scale even after extensive shutdowns. The startup counters are therefore not normally required and are removed after startup.

4.5 Reactor Regulating System

The Reactor Regulating System consists of that part of the overall plant control system that directly controls reactor power - either to an operator specified setpoint (ALTERNATE mode), or to the power level required to maintain steam generator pressure (NORMAL mode). A block diagram of the Reactor Regulating System is shown in Figure 4.3.

![Block Diagram of Reactor Regulating System](image)
It is designed to satisfy the following requirements:

(i) Provide automatic control of reactor power between 10^-7 full power and full power.

(ii) Maintain the neutron flux distribution close to its nominal design shape[6] so that the reactor can operate at full power without violating bundle or channel power limits.

(iii) Monitor important plant parameters and reduce reactor power quickly when any of these parameters are out of limits.

(iv) Automatically withdraw shutoff rods from the reactor when the trip channels have been reset following a reactor trip on Shutdown System No. 1.

Reactor neutron power is controlled to a given setpoint by means of the reactivity control devices, which for fast control include:

- 14 light-water zonal control absorbers
- 4 mechanical control absorbers, and
- 21 solid adjuster rods.

Long-term negative reactivity is provided by the addition of soluble poison (boron or gadolinium) to the moderator. Boron is used to suppress the excess reactivity in a fresh core and gadolinium is used following a reactor poison out to compensate for xenon burnout.

4.5.1 Zonal Control Absorbers

The main method for controlling reactor power is by adjustment of average H2O level in the 14 independently controllable compartments of the zonal control absorbers. Differential adjustment of levels in individual compartments is used for spatial (zonal) control. Platinum in-core flux detectors provide the neutron flux feedback signals required by the digital control algorithms for regulation of both the bulk and spatial flux. The layout of the various reactivity mechanisms and detectors is shown in Figure 4.4.

4.5.2 Mechanical Control Absorbers

The reactivity range (±3 mk) provided by the zonal control absorbers is adequate for most power manoeuvres. However, certain situations require additional negative reactivity that is provided by the 4 mechanical control absorbers (±10 mk), normally out of the core (see Figure 4.4).

These situations include

- controlled shutdown of the reactor by the regulating system
- ramped power reduction (SETBACK) during upset conditions to allow continued operation at reduced power

4.5.3 Adjusters

The 21 adjuster rods, shown in Figure 4.4, have graded absorption and are normally fully inserted in the core for flux shaping. They are withdrawn in symmetrical banks, under the control of the digital control computer, to provide positive reactivity for shimming the zonal control absorbers as well as for xenon override following a shutdown. Their total reactivity worth of 15 mk makes it possible to start up the reactor within 30 minutes after shutdown from full power. As well the adjusters permit sustained power reductions to 55% of full power. During periods of refuelling incapability the adjusters can keep the plant operating for weeks

Normally the mechanical control absorbers are automatically driven by the control computer, however they can be manually controlled by the operator.

Figure 4.4 REACTIVITY MECHANISM LAYOUT
by compensating for the loss of reactivity of
\(0.31\) mk per day.

Manual control of the adjusters by the
operator is provided.

4.6 Flux Mapping

The platinum flux detectors used for spatial
control do not accurately represent average zone
power as they sense the flux over a small volume, 3
lattice pitches long. Therefore, a need exists for
the accurate measurement of average zone power to
calibrate these detectors. This is done with a
system of 102 vanadium flux detectors distributed
throughout the reactor core. Signals from these
detectors are processed by the flux mapping routine
in the control computer, to obtain average zone flux
estimates. Processing of flux detector signals
includes reading, checking for rationality, convert-
ing to proper units and correcting for detector
burnup. Detector readings that do not pass the
rationality check are rejected.

The flux mapping routine also estimates the
maximum flux levels in the core and uses this
information to initiate a reactor setback if the
power is too high in some fuel bundles.

The flux mapping routine also provides a
channel power map, as well as estimates of the flux
at Regional Overpower Trip (ROPT) detector sites.
This gives the operator accurate information on the
state of the core.

4.7 Control Strategies

4.7.1 Reactor Startup

The triplicated startup instrumentation
listed in Table 4.1 is used for the initial approach
to reactor criticality or for startup after a very
long shutdown. Each channel of instrumentation is
connected to the corresponding channel of SDS-1.
The trip and alarm parameters used are high log
power, low log power, high log rate and HV power
supply voltage.

On the approach to criticality the operator
removes boron from the moderator and records the
neutron count rate from each of the three instrumen-
tation channels at regular time intervals.
Between \(10^{-14}\) and \(10^{-13}\) full power the signals are
provided by in-core BF\(_3\) counters. Once the out-
of-core BF\(_3\) counters come on scale the instrument
channels are switched over to them. Finally, when the
ion-chamber system indicates a power level of
\(10^{-4}\) full power the digital control computer takes
control and raises power to the requested setpoint.

4.7.2 Normal Operation

During normal operation (above \(15\) F.P.) the
zonal control absorber program provides signals to
the absorber inflow control valves to hold both
reactor power and zonal power at their setpoint
values. The valve lift and hence flow varies with
power error as shown in Figure 4.5d.

Spatial flux control has lower priority than
reactor power control. If individual compartment
levels are too high or too low, spatial flux control
in those compartments is slowly phased out and the
remaining range is reserved for reactor power con-
trol. Flux tilt control is also removed below \(15\)%
full power where it is not needed.

For certain upset conditions (see Section
4.5.2) the required negative reactivity rates and
depths are beyond the capability of the zonal con-
trol absorbers. This capability is provided by the
insertion of 4 mechanical control absorbers (MCAs).
Inadequate negative reactivity is indicated by high
average water level in the zonal control absorbers
and/or by high positive power error. These condi-
tions are therefore used in the control computer to
initiate MCA in-drive, as shown in Figure 4.5b.
Under special conditions the use of the MCAs is
inhibited, e.g., both shutdown systems not avail-
able.

In addition to their normal uses for shaping
flux and providing xenon override following a shut-
down, the adjusters can be used to assist the zonal

Figure 4.5 REACTIVITY LIMIT CONTROL DIAGRAM
control absorbers when more positive reactivity is required. Hence adjuster out-drive is initiated on low average light water level and on excessive negative power error, as shown in Figure 4.5a. Conversely, high water level and positive power error cause adjuster in-drive. The speed of adjuster rods and of the mechanical control absorbers depends on power error as shown in Figure 4.5c.

Finally, the manual addition of gadolinium poison to the moderator is available to the operator as backup to the mechanical control absorbers. The automatic addition of gadolinium poison takes place on high power error (>10%) combined with positive flux-rate and prevents Loss-of-Regulation accidents due to the slow growth of reactivity in the core.

4.7.3. Power Setbacks

Reactor power setbacks are controlled reductions in power when certain plant parameters exceed specified limits. They are automatically initiated by the computer SETBACK routine which drives-in the mechanical control absorbers. Plant conditions that initiate setbacks include:

- high local neutron flux
- spatial control off normal
- low deaerator level
- high boiler pressure
- upsets in moderator temperature or pressure.

4.7.4 Power Stepbacks

As part of the "defense-in-depth" philosophy, a STEPBACk routine is provided in the regulating system to correct minor upsets before they become major. For certain upsets the routine initiates fast power reductions by dropping the four mechanical control absorbers into the core. If the stepback condition clears during the gravity fall of rods, the clutches are engaged and the rods caught in mid flight. Plant upset conditions that initiate reactor stepbacks include:

- reactor trip
- turbine trip
- loss of line
- heat transport pump trip
- high heat transport pump pressure
- high flux power or high flux rate
- low boiler level

To prevent the spurious initiation of stepbacks which could lead to a reactor poison out, the stepback routine is run in both control computers and a stepback is initiated only when both computers call for one.

4.8 System Response to Disturbances

As mentioned in section 4.2, the plant operates in one of two modes, NORMAL or ALTERNATE. In the NORMAL mode, boiler pressure is usually controlled by manoeuvring reactor power with help, on occasion, by varying the plant load. An example of this combined action is the rapid turbine rundown transient shown in Figure 4.6 where the steam discharge valves are lifted during the decrease in reactor power.

![Figure 4.6 NORMAL MODE TURBINE RUNDOWN AT 2.2%/s FROM 100% FULL POWER](image)

On a turbine trip, loss-of-line or loss of stator cooling, the reactor is stepped back to 60% power by partially dropping the mechanical control absorbers. As shown in Figure 4.7 both the atmospheric and condenser steam discharge valves are initially used to vary the plant load. This is followed by all the steam being bypassed directly to the condenser through the condenser steam discharge valve.
4.9 Xenon Override and Load Following Capabilities

4.9.1 Xenon Override

Figure 4.8 shows a typical power recovery after a reactor trip. The slow rate of rise from approximately 60% to 100% of full power results from the requirement to prevent any local fuel overrating caused by neutron flux distortions. These flux distortions result from the removal of adjuster rods during startup. 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 the adjusters are withdrawn for the restart, the return to full power may take up to 4 hours. If the reactor does poison out the buildup of Xenon-135 prevents reactor startup for a further 40 hours. Under normal conditions, a poison out is averted if the operator brings the reactor up to the poison-prevent level (%60%) within the poison override time (<30 minutes). If the turbine cannot pick up the load fast enough, the excess steam is temporarily discharged to the condenser.

4.9.2 Load Following Capabilities

Reactor power can be suddenly reduced from full power to as low as 55% power and kept there indefinitely without poisoning out. However, the subsequent rate of return to full power is somewhat restricted to avoid local fuel overpowering due to transient flux peaking. Figure 4.9 shows the estimated fastest possible rates of return to full power at various times following a power reduction to 55% power.
Although the present CANDU reactors are operated as base-load stations there are no technical reasons preventing daily load-cycling. Constraints on power increase rate would be built into the control algorithm.

4.10 Reliability and Maintainability

The demand for a highly reliable regulating system is driven by safety and economics. Experience with existing CANDU stations indicates that the loss-of-regulation (LOR) target failure rate of $10^{-2}$ (once per 100 years) is achievable. The more common regulating system outages requiring maintenance are resulting in a reactor unavailability of 20 hours per year. Less than 5 hours of this is attributed to unavailability of both control computers.

The high reliability of the regulating system and other nuclear systems results from quality control, careful commissioning, system redundancy and fail-safe philosophy.

Maintainability is achieved by:
- modular, plug-in construction of all the instrumentation,
- provision of a complete spare channel,
- use of standard commercially available detectors, instruments and cables,
- provision of test equipment to promote rapid diagnosis of faults,
- accessibility of all components for replacement.

5. REACTOR SAFETY SYSTEMS

5.1 Shutdown System Number One

5.1.1 General Description

Shutdown System Number One (SDS-1) uses 28 spring-assisted, gravity-drop absorber elements as its basic shutdown mechanism, and is the preferred method of quickly terminating reactor operation when specified parameters enter an unacceptable range. When any of the 9 trip parameters listed in Table 5.1 exceed their trip settings, a two-out-of-three 'general' logic system senses the requirement for a reactor trip. If a trip is required, the direct-current clutches on the shutoff rods, which are in two groups of 14 each, are de-energized, and the absorber elements drop into the moderator. The redundant logic system fails to a safe condition on loss of ac power.

A simplified block diagram of one channel of SDS-1 is shown in Figure 5.1, and a typical trip circuit, including shutoff rod absorber clutch connections, is shown in Figure 5.2.

*This preference is an economic factor since the use of Shutdown System No. 2, which injects poison into the moderator, results in a reactor "poison-out", with attendant unit unavailability to the electrical grid.

![Figure 5.1 SHUTDOWN SYSTEM NO. 1 - BLOCK DIAGRAM](image)
When any two of the three channels trip, the shutoff rods are dropped. With the general coincidence logic used, an entire channel trips when any measurement of any parameter reaches its trip setting. This approach makes testing easier and more complete as compared to local coincidence schemes, where testing requires a number of steps.

Use is made of light-emitting diodes (LEDs) in the shutoff rod trip network to indicate correct operation of the trip relays when a particular channel of a specific trip parameter is tested (see Figure 5.1). Correct operation of a particular relay contact is indicated by lighting of the associated LED, and failure of a relay to re-energize after test is detected by its LED remaining lit.

A facility for testing the drop time of the absorber elements during reactor operation is also provided.

In the main control room a separate instrumentation panel is allocated to SDS-1. On it are mounted

- all the annunciator alarms indicating the state of trip parameters and trip channels,
- the test LEDs and switches,
- the manual drive and test-drop handswitches for the shutoff units, and
- the manual trip button.

All trip parameters are connected through suitable buffers to the sequence-of-events monitor on the main computers for "post-event" analysis.

The unavailability requirement of $10^{-3}$ or less is met without taking credit for trip signals from more than one trip parameter at a time, even though diversity has been provided. The shutoff system is considered to be available if all except the two most effective absorbers drop when required to do so. The negative reactivity insertion rate for this situation is more than adequate to keep the result of any accident within regulating agency guidelines for any accident.

The principle of diversity in the design of the trip system is illustrated in Table 5.2. For each process failure there are at least two effective trip parameters, with the alternate trip parameter being based on a different measurement principle from the primary parameter.

<table>
<thead>
<tr>
<th>Process Failure</th>
<th>Trip parameter</th>
<th>Alternate Trip Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of regulation from high power, etc.</td>
<td>High neutron power</td>
<td>High neutron power</td>
</tr>
<tr>
<td>Loss of Regulation from Decay, Power Levels</td>
<td>High neutron power</td>
<td>Low neutron power</td>
</tr>
<tr>
<td>Pressure/Pump-On</td>
<td>High neutron power</td>
<td>Low neutron power</td>
</tr>
<tr>
<td>Pressure/Pump-Off</td>
<td>High neutron power</td>
<td>Low neutron power</td>
</tr>
<tr>
<td>Depressurized/Pump-Off</td>
<td>Low neutron power</td>
<td>Low neutron power</td>
</tr>
<tr>
<td>Depressurized/Pump-On</td>
<td>Low neutron power</td>
<td>Low neutron power</td>
</tr>
<tr>
<td>Loss of Class IV</td>
<td>Low neutron power</td>
<td>Low neutron power</td>
</tr>
</tbody>
</table>

5.1.2 Logic

The trip system makes extensive use of relay logic. Relay trip logic is standard in CANDU stations built during the 1960s and 1970s and has proven to be highly reliable. In trip systems having simple trip parameters, relay logic leads to a simple, testable, fail-safe design.

The trip systems for later generation CANDU stations combine relay logic with micro-processors called Programmable Digital Comparators (PDCs) for implementation of trip parameters that require extensive conditioning, or those that have setpoints that are functions of reactor power and/or heat transport system pump configuration. The microprocessors are standard field-proven units with read-only memory.
A typical illustration of PDC use is the design shown in Figure 5.3 where two are used per instrumentation channel; one for the primary trips requiring a significant degree of conditioning and one for the associated alternate or backup trips.

![Diagram of TRIP CHAIN LOGIC OF CHANNEL](image)

Figure 5.3 TRIP CHAIN LOGIC OF CHANNEL

As operational experience is gained, one PDC per trip channel will be employed. The PDCs replace analog trip comparators used previously for complex trips. Digital outputs controlled by the PDCs drive relays in the channel trip logic, as do other trip parameters.

5.1.3 Individual Trips

The various trip parameters are listed in Table 5.1. There are nine automatic trips, a manual trip which allows operator intervention, and a startup-count rate trip, which is in service only for the initial startup from low source current.

The High Neutron Power trip is based on prompt responding, self-powered platinum flux detectors mounted vertically in the core such that all regions of the core are protected from over-power. These flux detectors are independent of any regulating system or SDS-2 detectors, and are tested by injection of a current at the amplifier inputs, and by checking the insulation resistance of each detector. The detector outputs are displayed in the control room for the purpose of monitoring the signals.

The other neutronic trip, High Rate Log of Neutron Power, is based on three uncompensated ion chambers located in separate housings on different sides of the reactor vessel. Testing is initiated from the control room by driving an adjustable, piston actuated bore-sleeve shutter which is set to provide the necessary lograte signals.

The other trip parameters are based on standard process instrumentation transmitters. In all cases, testing can be automatically initiated from the control room, and consists of operating the relevant transmitter instrumentation valves and applying appropriate test pressures.

5.2 Shutdown System Number Two

Shutdown System Number Two (SDS-2) provides a second method of quickly terminating reactor operation for the same spectrum of postulated initiating events as SDS-1. Provision of two functionally and physically independent shutdown systems, both designed for a very low unavailability, 10^-7, virtually guarantees shutdown capability under all reactor or accident circumstances.

SDS-2, employing an independent 2 of 3 general logic system (a channel of which is shown in Figure 5.4), opens fast acting helium pressure valves to inject gadolinium nitrate 'poison' directly into the D_2O moderator when any of the eight measured parameters listed in Table 5.3 exceeds its limits.

![Diagram of SHUTDOWN SYSTEM NO. 2 - BLOCK DIAGRAM](image)

Figure 5.4 SHUTDOWN SYSTEM NO. 2 - BLOCK DIAGRAM

Six horizontal poison injection nozzles are provided. The basic principles of operation are illustrated in Figures 5.4 and 5.5. The actuation of any two trip channels opens valves to establish a path from the high pressure helium supply tank to the poison tanks, and gadolinium nitrate is forcibly injected into the moderator.
The selection of trip parameters is such that there are again, as with SDS-1, at least two trips for each process failure, and, in general, the alternate trip parameter is based on a different measurement parameter from the primary trip as illustrated by Table 5.4.

The High Neutron Power Trip is based on a number of prompt-responding self-powered platinum flux detectors mounted horizontally in the core. These detectors are separated from any regulating system and SDS-1 detectors by the spatial separation of the assemblies. The detector outputs and trip setpoints are displayed in the control room for monitoring purposes.

The High Rate Log of Neutron Power trip, as for SDS-1, uses uncompensated ion chambers, but the ion chambers, and their associated amplifiers are of different manufacture than those of SDS-1 and the ion chambers are located at a different reactor face. Testing is similar to that done in SDS-1, with the use of a piston actuated boral-sleeve shutter to simulate a rate of change of neutron power.

The other trip parameters are based on standard process instrumentation transmitters. In all cases, testing can be automatically initiated from the control room, and consists of applying appropriate test pressures to the relevant transmitter.

Testing also includes automatically operating the quick operating valves in one trip channel periodically, as well as taking a poison tank out of service to check that its gadolinium nitrate concentration meets requirements.

Indication of a successful channel test is obtained by observing correct operation of the quick acting valves in the control room. The logic processing for SDS-2 is similar to that of SLC-1, and employs a combination of relay and micro-processor technology. However, different designs and suppliers are utilized.
A separate panel in the main control room is allocated solely for SDS-2. As for SDS-1 the panel consolidates all annunciator alarms, test switches, etc., associated with SDS-2.

Connections are also made through suitable isolating buffers to the main computer systems sequence-of-events monitor.

The target unavailability of the system of $10^{-3}$ is met without taking credit for alternate trips, and having at least 5 of 6 poison tanks available.

5.3 Emergency Coolant Injection

The emergency coolant injection (ECI) system, shown in Figure 5.6, is composed of three stages: high pressure, medium pressure and low pressure.

The high pressure stage uses pressurized nitrogen to inject water into the reactor core from water tanks located outside the reactor building. The medium pressure stage supplies water from the dousing tank. When this water supply is depleted, the low pressure stage recovers water that has collected in the reactor building sump and pumps it back into the reactor core via the emergency cooling heat exchanger and the emergency cooling recovery pumps.

The high pressure injection stage consists of one nitrogen gas tank and two water tanks. The gas tank normally operates at a pressure between 4.1 MPa and 5.5 MPa, whereas the water tanks operate slightly above atmospheric pressure. Two recovery pumps, each capable of supplying 100% of ECI flow, are provided. Each pump is supplied by Class III power and by the emergency power supply system (see Section 8). The heat exchanger in the recovery pump discharge line is designed to maintain the emergency cooling flow at about 50°C at entry to the heat transport system.

Since inadvertent injection of emergency coolant would be economically penalizing, precautions are taken in the logic design to prevent inadvertent initiation of ECI, while still providing the redundancy required to meet the unavailability target of less than $10^{-3}$. Typical design features are:

(i) All instrumentation and associated control loops used to initiate ECI are triplicated (e.g., low heat transport pressure and high reactor building pressure). The sensors used are dedicated to ECI and are not shared either by other safety systems or other process systems.

(ii) Local coincidence is used in the logic to help eliminate spurious trips of the system.

(iii) All logic for isolating each of the two separate heat transport loops, during a LOCA, is separate from the logic for other functions.

(iv) Redundant valves in parallel are used wherever power operated valves are required for ECI. Either one opening would be sufficient. Each valve of a pair is fed from an independent power supply and annunciation is made of valve power supply failure.

(v) On-power testing facilities are provided to assure that the target unavailability is met.

5.4 Containment

The containment system shown in Figure 5.7 comprises a prestressed, post-tensioned concrete containment structure, an automatically initiated dousing system and building air coolers, a filtered air discharge system, access airlocks, and an automatically initiated containment isolation system.

Figure 5.7 CONTAINMENT SYSTEM
5.4.1 Dousing System

The dousing spray header system is illustrated in Figure 5.8. Two valves in each of the six independent headers open on high building pressure to start dousing. The valves in three headers are of one type and manufacturer and the valves in the other three headers are of a second type and manufacturer. This results in two independent dousing systems with three spray headers in each.

Figure 5.8 DOUSING SPRAY HEADER SYSTEM

Twelve independent valve control loops are provided, one for each valve, each with its own sensor of building pressure. The unavailability targets can easily be met because the valves can be tested via the "2-valves-in-series" arrangement, plus the fact that only four of the six spray headers are needed for adequate dousing. Any failure of air or power needed to open the valves is immediately annunciated, and a log of position of the valves is available in one of the dual computers.

5.4.2 Containment Isolation Control

The control system for containment isolation continuously monitors the building pressure and radioactivity and automatically closes isolation dampers and valves when limits on either are exceeded. Figure 5.9 illustrates that a two-out-of-three 'high' indication is required to initiate closure.

Two series-connected valves are provided for isolating each penetration, and closing either one effectively "bottles up" the penetration. The conversion of the two-out-of-three measurement to the required one-of-two logic for the valves is also illustrated in Figure 5.9.

Figure 5.9 SIMPLIFIED BLOCK DIAGRAM OF CONTAINMENT AUTOMATIC ISOLATION CONTROL LOOP

6. CONTROL ROOM DESIGN AND INFORMATION DISPLAY

Two major control areas are provided, - the main control room and secondary control area. The main control room centralizes all the information and man-machine controls required for safe operation of the plant, including those items required for the Group 2 Safety Systems previously described in Section 3.

The secondary control area, which is geographically remote from the main control room, would be used for performing the shutdown and decay heat removal functions associated with Group 2 safety systems, if the main control room became inaccessible.

6.1 Main Control Area

A typical main control room layout for a two unit station is shown in Figure 6.1.
The basic philosophy of design is to display sufficient information to allow the unit to be controlled from the control room. To achieve this goal, all indications and controls essential for operation (startup, shutdown and normal) are located on the control room panels. Also located there are the controls for any systems requiring attention within 15 minutes of an alarm. For systems not requiring attention within 15 minutes, local control may be provided.

Most information is presented to the operator via the station computer system. However, sufficient conventional display, annunciation and recording of plant variables is included to allow the plant to be properly run in the shutdown condition with both computers out of service.

In case the control room becomes uninhabitable, enough display and control instrumentation is provided in the secondary control area to allow the plant to be shut down and maintained in a safe shutdown condition.

6.2 Main Control Room Panels

As shown in Figures 6.1 and 6.2 the control panels form part of the boundary walls of the control room. With the degree of automation provided, the need for operator action at the control panels is infrequent. Therefore, the main control panels have been designed as standup panels with no sitdown console. An exception to this is the fuelling machine console where, despite a high degree of automation, manual intervention is sometimes required. To reduce interference with the rest of the control room, this console is located to one side, out of the main traffic flow.

The panels are laid out on a system basis with the controls for a specific system being located in one bay. Spacing between instruments is kept to a minimum in an attempt to achieve a compact display of information.

In laying out each system, consideration is given to the relative location of the controls based on process function and/or plant location. Ml nics of the more complex process and electrical systems are displayed using colour graphic lines to represent the flow paths. There are seven cathode ray tubes (CRTs) with their associated keyboards located on various process panels for system parameter or trend displays (see Figure 6.2). Two CRTs are mounted in the fuel handling control console to display fuelling system information.

There are two CRTs located centrally on the unit panel for display of annunciation messages. For the convenience of the control room operators, a CRT is located in their desk, which allows them to view computer-driven graphics or alpha-numeric displays of any important plant parameters. Printed copy of CRT display information can be generated on demand.

The CRTs replace many of the meters and recorders normally found on conventional panels. Sufficient redundancy is built into the display system to ensure a high availability comparable to the dual computer controller system itself. The use of computer driven displays results in less congested panels and allows easier correlation of information. The greater flexibility possible is of considerable use during commissioning and at other times, such as during extended shutdowns, when special display requirements must be met. Furthermore, infrequently used information can be suppressed during normal operation.

The panels are laid out on a system basis with the controls for a specific system being located in one bay. Spacing between instruments is kept to a minimum in an attempt to achieve a compact display of information.

In laying out each system, consideration is given to the relative location of the controls based on process function and/or plant location. Ml mics of the more complex process and electrical systems are displayed using colour graphic lines to represent the flow paths. There are seven cathode ray tubes (CRTs) with their associated keyboards located on various process panels for system parameter or trend displays (see Figure 6.2). Two CRTs are mounted in the fuel handling control console to display fuelling system information.

There are two CRTs located centrally on the unit panel for display of annunciation messages. For the convenience of the control room operators, a CRT is located in their desk, which allows them to view computer-driven graphics or alpha-numeric displays of any important plant parameters. Printed copy of CRT display information can be generated on demand.

The CRTs replace many of the meters and recorders normally found on conventional panels. Sufficient redundancy is built into the display system to ensure a high availability comparable to the dual computer controller system itself. The use of computer driven displays results in less congested panels and allows easier correlation of information. The greater flexibility possible is of considerable use during commissioning and at other times, such as during extended shutdowns, when special display requirements must be met. Furthermore, infrequently used information can be suppressed during normal operation.

The panels are laid out on a system basis with the controls for a specific system being located in one bay. Spacing between instruments is kept to a minimum in an attempt to achieve a compact display of information.

In laying out each system, consideration is given to the relative location of the controls based on process function and/or plant location. Ml mics of the more complex process and electrical systems are displayed using colour graphic lines to represent the flow paths. There are seven cathode ray tubes (CRTs) with their associated keyboards located on various process panels for system parameter or trend displays (see Figure 6.2). Two CRTs are mounted in the fuel handling control console to display fuelling system information.

There are two CRTs located centrally on the unit panel for display of annunciation messages. For the convenience of the control room operators, a CRT is located in their desk, which allows them to view computer-driven graphics or alpha-numeric displays of any important plant parameters. Printed copy of CRT display information can be generated on demand.

The CRTs replace many of the meters and recorders normally found on conventional panels. Sufficient redundancy is built into the display system to ensure a high availability comparable to the dual computer controller system itself. The use of computer driven displays results in less congested panels and allows easier correlation of information. The greater flexibility possible is of considerable use during commissioning and at other times, such as during extended shutdowns, when special display requirements must be met. Furthermore, infrequently used information can be suppressed during normal operation.

The CRTs replace many of the meters and recorders normally found on conventional panels. Sufficient redundancy is built into the display system to ensure a high availability comparable to the dual computer controller system itself. The use of computer driven displays results in less congested panels and allows easier correlation of information. The greater flexibility possible is of considerable use during commissioning and at other times, such as during extended shutdowns, when special display requirements must be met. Furthermore, infrequently used information can be suppressed during normal operation.
A reactor alarm annunciation system consists of small direct-wired window annunciators, two computer driven CRTs for alarm message presentation, and a facility to provide a printed record of all alarm conditions in chronological order of their occurrence. Alarm windows are illuminated independently of the computers for all alarm conditions that can cause reactor trips, power runbacks, turbine generator trips, high voltage breaker trips and other important system upsets.

6.3 Safety Related Display Instrumentation

Most of the information on the state of the plant is presented to the operator via the two station control computers. This includes the data logging, sequence-of-events functions, displays of plant variables and initiation of most alarms. The computer system is designed to fail safe on dual computer failures by dropping the four mechanical control absorbers and flooding the 14 light water zone control absorbers. However, when dual computer failures occur, the operator will be deprived of the normal source of most of this information.

Certain plant information must be available to the operator at all times and, therefore, he cannot rely on the computer system for this data. This includes the status of all the safety systems and sufficient information about the status of the plant to enable him to establish the existence, nature and extent of an accident and to allow him to intervene intelligently, where necessary, with manual actions. This objective is achieved by displaying the following information directly on the control room panels:

- Red alarm windows to indicate the trip state of any parameter in any of SDS-1, SDS-2, ECI or CS Special Safety Systems.
- Other alarm windows to indicate abnormalities in the shutdown and safety related systems, e.g., loss of power, loss of helium pressure.
- The values of each trip parameter in each channel of SDS-1, SDS-2, ECI and CS Special Safety Systems.
- Alarm windows to indicate the existence of single and dual computer failures.
- Process indicators to display information on the status of subsystems required for the operation of the safety systems, and other safety related systems, e.g., dosing tank and reactor building basement water levels and temperatures.

7. ON-POWER REFUELLING SYSTEM

CANDU reactors rely on semi-continuous, on-power refuelling for close control of core reactivity and efficient utilization of the natural uranium fuel.

The fuel handling system comprises equipment for storage of new fuel, for fuel changing and for temporary storage of spent fuel. Reactor fuel is changed on a routine basis with the reactor operating at full power.

The flow of fuel through the plant is shown schematically in Figure 7.1.

![Figure 7.1 FUEL HANDLING SEQUENCE](image)

Figure 7.1 FUEL HANDLING SEQUENCE

The major steps in the movement of fuel are normally under remote and automatic control from the control room, i.e.,

- loading the fuelling machine
- loading and unloading a reactor channel, and
- discharging spent fuel

One of the two station control computers is used to control the fuel handling system. In addition, there are separate consoles and control panels in the control room specific to the fuel handling system. Interconnections between the control system components and the fuel handling equipment are shown in the block diagram of Figure 7.2.

Refuelling can be carried out under automatic or manual control. In both modes, certain output commands are routed through a protective logic system that protects against inadvertent operations that could damage the equipment or cause personnel hazards.

Abnormal control functions are carried out from the automatic section of the refuelling control console and selected data is displayed on a CRT. A printer provides a hard copy of this data when requested. Minimum operator intervention is required during automatic control.
3. ELECTRICAL POWER SYSTEMS

Figure 8.1 shows the classes of electrical power and their separation into two completely independent groups (one for group 1 process systems and one for group 2 safety systems). Each power supply group comprises two or three independent trains, depending on class of power.

Four classes of power are provided for service power and instrumentation loads. Their uses in order of their reliability are:

CLASS I - Uninterruptible direct current (dc) supplies for essential instrumentation, protection and control equipment.

CLASS II - Uninterruptible alternating current (ac) supplies for essential instrumentation, protection and control equipment.

CLASS III - Alternating current (ac) supplies to essential auxiliaries which can tolerate short interruptions required during startup of the standby generators. These essential auxiliaries are necessary for an orderly shutdown of the reactor.

CLASS IV - Normal alternating current (ac) supplies to auxiliaries and equipment which can tolerate long duration interruptions without affecting personnel and equipment safety. Complete loss of Class IV power will initiate a reactor shutdown.

All standby generators of the group 2 power supplies including D/G-3 and D/G-4 are seismically qualified.

Within each separate train, an "even, odd" bus concept is followed to provide "dual-bus or better" reliability at all voltage loads for Class III and IV power. Loads and redundant auxiliaries are connected such that half of any actual process is supplied from an odd bus and the other half from an even bus. The odd and even concept is applied throughout, including the cable tray system, junction boxes, etc., in order to maintain physical separation and so achieve maximum reliability under normal and abnormal conditions.

Class I and II power is triplicated at all needed voltage loads. Each of the three Class I buses is fed from its own rectifier which is in turn connectible to either the odd or even Class III bus (see Figure 8.1).

Loads of triplicated systems, such as SDS-1 and SDS-2, are connected so as to ensure independent power supplies for each channel of the triplicated system. Independence of the triplicated power supplies is carried right through to separate cable trays, junction boxes, conduits and routing to decrease vulnerability to common mode faults.
9. MISCELLANEOUS INSTRUMENTATION AND CONTROL SYSTEMS

9.1 Radiation Protection

9.1.1 General

Limitation of external and internal radiation exposure to persons at the site boundary and to plant personnel is accomplished by a combination of facilities incorporated into the station, and by adherence to a set of administrative and operating procedures.

Exposure of members of the population is limited by exclusion of all unauthorized persons from the station area, and by preventing any habitation nearer than 1000 metres from the station. The release of all effluents, liquid and gaseous, that might conceivably carry significant radioactivity is monitored and controlled. Active solids are stored in a manner that prevents the release of radioactivity.

The exposure of station personnel to radiation is limited by key interlock control of access to areas of high activity or possible contamination.

9.1.2 Fixed and Portable Area Monitoring

Fixed alarming area gamma monitors are permanently installed in areas of potentially dangerous radiation exposure to detect the occurrence of radiation hazards and to warn personnel of the presence of high fields. Two setpoints are normally provided on these monitors, both of which activate a flashing light and audible alarm in the area being monitored. The lower setpoint indicates equipment failure. The higher setpoint indicates high radiation levels.

Alarms from the area gamma monitors would, in accident cases, be preceded by other indications of impending trouble. The control room, associated air conditioning system and instrument areas are arranged so they can be atmospherically isolated, and could remain in service following any design basis reactor accident, or failure of a main or auxiliary steam or water header.

Portable alarming systems are used in the plant for various maintenance and operations tasks in high fields. These devices are used in-plant to minimize exposure and prevent overexposure.

9.1.3 Access Control

Personnel entry to the exclusion zone is restricted to qualified personnel and to those under their escort. There are "Access Controlled Areas" where the radiation hazard is such that entrance must be made only with the knowledge and consent of the control room staff and by using a special key. Visible signals are provided in the control room to indicate which keys are in use.

There are some areas where radiation is directly related to power level. If the access key is not in the keyboard, reactor power cannot be raised. All personnel access doors are equipped with devices to permit escape, irrespective of the status of access locks.

9.1.4 Liquid Effluent Monitoring

Facilities are provided to collect a sample from each effluent tank for laboratory analysis. The results of the analysis determine whether the effluent needs treatment or can be safely discharged.

Effluent from the liquid waste management system is monitored continuously, the sample being taken at a point upstream of the confluence with the condenser cooling water flow, in order to achieve maximum measurement accuracy.

Continuous samples are taken, using a pump, of the discharge canal water. These samples are checked for tritium content and the nature and concentrations of any radionuclides present. Sampling and measurement frequency are determined by the Health Physics group.

9.1.5 Gaseous Monitoring

Continuous samples of the effluent are taken and monitored to determine releases of iodine particulates and noble gases. The signal from each of these monitors is recorded in the main control equipment room. A high level signal is annunciated in the control room. Tritium monitoring is carried out by laboratory analysis of gaseous effluent monitor samples. There is no continuous recording or annunciation of this function.

9.1.6 Containment Monitoring

A separate triplicated gross-gamma monitoring system monitors the containment duct activity. A high activity measurement at any two of the three instruments will close the dampers and permit manual operation of the dousing system.

9.1.7 Environmental Surveillance

Beyond the site boundary, the Canadian practice has been for government agencies to monitor and sample the environment. In addition, the operators of Canadian plants do some environmental monitoring, both to check the data compiled by the government agencies or others, and to assist in the development of more accurate correlations between station releases and environmental radioactivity levels.

To date, this monitoring has shown that, in general, CANDU plants can meet their operational target of keeping below one percent of the allowable releases.

9.2 Fire Protection

In general fire detectors are provided for protection of all key areas of the station. The
detectors alarm on the fire protection panel and in the main control room. The signals from the fire detectors also cause the ventilation system for the fire zone to go into a "fire mode" of operation.

Various system types, ranging through sprinkling, automatic water deluge, carbon dioxide, Halon 1301 and foam are used, dependent on the nature of the hazard and the equipment in the area. Automatic Halon 1301 systems are used in such key centres as the Battery and Telecommunication Room, Plant Control Computer Room and Counting Room. Automatic foam protects the fuel tanks for the Class III diesel generators and the auxiliary steam generator.

Hose cabinets and dry type chemical extinguishers are located throughout the turbine and service buildings. Hose stations have adjustable nozzles, and are located so that two water streams can reach all areas.

10. HEAVY WATER MONITORING

Heavy water is a major component of the capital cost of CANDU reactors. Consequently, suitable instrumentation is required for quantitative determination of the deuterium concentrations for heavy water inventory, management and process control. The two analytical approaches used to measure the isotopic concentrations of water over the entire range of D2O concentrations are chemical laboratory analysis of grab samples, and on-line monitoring of process streams.

Manual sampling is used on those process streams that are of secondary importance in the overall operation of the reactor. At present, on-line D2O monitoring offers the greatest benefit for those systems capable of leaking heavy water to the environment and those whose D2O concentration is used for process control. For these applications, precise isotopic measurements at the two extremes of the concentration range are needed, i.e., around natural and reactor grade isotopic values.

10.1 Heavy Water Leak Detection

Although leaks have been minimized so that heavy water upkeep accounts for less than 5% of the total unit energy cost, the potential for large losses still exists. Rapid response leak detection is provided by two fully automatic heavy water liquid analysers. These units use infrared spectrometry to measure low concentrations of excess D2O in the various process light water streams, viz.,

- boiler light water,
- fuelling machine heat exchangers,
- moderator heat exchangers, and
- other process system heat exchangers.

When a high concentration of D2O is detected in any of these streams, it is alarmed in the control room. The station staff then uses the instrument to verify the location and size of the leak. With this analytical data, the decision can be made to either shut down immediately to repair the leak, or wait for a scheduled shutdown.

10.2 Process Monitoring

A CANDU reactor normally has two heavy water upgrading towers, one for moderator D2O and the other for primary coolant D2O. Each tower has two heavy water liquid analysers. One monitors the low level effluent from the tower and provides a signal for the automatic control of the tower. The other monitors the upgraded D2O product and isolates the tower if the product is unsatisfactory.

The measured D2O concentrations from these units are recorded and displayed in the control room. Alarms in the control room are also provided to indicate out-of-limit conditions or equipment faults.

11. FAILED FUEL DETECTION SYSTEM

If the zirconium cladding around the UO2 fuel is breached, the failed fuel must be located and removed while the reactor continues to operate at power. The presence of failed fuel in the reactor is determined by the Gaseous Fission Product Monitoring System, shown in Figure 11.1, which continuously monitors flowing samples of the heat transport system coolant.

The gaseous fission product activity in the sample is detected by a gamma sensitive spectrometer that is fitted with a high-resolution germanium detector. A multi-channel analyser is used to determine the difference in the gamma count rates between the sample and the natural background. The gamma energy, above background, for each of four radioisotopes, is sent to the control computers for display and comparison to allowable limits. When these limits are exceeded, indicating a fuel failure, the Failed Fuel Location System can be used to find the channel with the defective fuel.

Figure 11.1 GASEOUS FISSION PRODUCTS MONITORING SYSTEM
The Failed Fuel Location System, shown in Figure 11.2, extracts, on demand, a continuous sample from each fuel channel feeder. Coils in these sample lines are arranged in a matrix that is automatically scanned by moving BF$_3$ neutron counters and the results are output on a local printer. A sample that shows a higher delayed neutron count, with respect to other samples, indicates a fuel failure in the corresponding channel. The operator then switches to the manual mode to double check the readings before deciding on channel refuelling. If refuelling is initiated, the Location System is used to identify the faulty fuel bundle pair.

The licensing process is the means by which the AECB gains assurance that a nuclear facility will be sited, designed, constructed, commissioned and operated in compliance with safety criteria and requirements established by the AECB.

The central safety criterion is that the risks due to nuclear power production should be much smaller than those due to other methods of energy production. Since the danger to the public would be the accidental releases of radioactivity to the environment, the AECB has set maximum permissible releases that the utilities must meet for operating conditions as well as accident conditions.

The operational target dose at the plant boundary from routine releases is 5 mrem/a. The resulting average exposure to the surrounding public would then be less than 1 mrem/a, which is less than 1 percent of natural background.

For accident conditions, the AECB guidelines are based on the "single and dual failure" concept. A "single failure" is a serious failure of a single process system. A "dual failure" is a coincident failure of a process system and unavailability of any one of the special safety systems. The AECB guidelines specifying the maximum allowable frequencies and doses for these accidents are summarized in Table 12.1.

**TABLE 12.1**

<table>
<thead>
<tr>
<th>Event</th>
<th>Maximum Frequency</th>
<th>Individual Dose Limit</th>
<th>Total Population Dose Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Serious</td>
<td>1 in 3 a</td>
<td>0.5 mrem (whole body)</td>
<td>10$^4$ mrem-a</td>
</tr>
<tr>
<td>Failure*</td>
<td>1 cm</td>
<td>10$^3$ mrem (thyroid)</td>
<td></td>
</tr>
<tr>
<td>Dual Failure</td>
<td>1 in 3000 a</td>
<td>25 mrem (whole body)</td>
<td>10$^6$ mrem-a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>250 mrem (thyroid)</td>
<td></td>
</tr>
</tbody>
</table>

* Serious process failure is defined as any failure of process equipment or procedure which, in the absence of action by the Special Safety Systems, could lead to significant fuel failures or significant releases of radioactive material from the station.

Serious process failures include such incidents as loss-of-regulation and loss-of-coolant accidents. Safety analyses of such events are carried out, as part of the licensing process, to show that the limits of Table 12.1 are not exceeded. Table 12.2 shows a typical matrix of process failures that are analysed. The 'X's on this table are failures that need not be considered as they do not change the outcome of the analysis.

The duty cycle of the Failed Fuel Location System is very low because CANDU fuel bundles currently have a proven reliability of $99.97$ percent [7].

12. **LICENSING PHILOSOPHY**

The design of CANDU reactors reflects the requirements laid down by the Atomic Energy Control Board of Canada (AECB). The AECB is a Federal Agency that is responsible for the licensing of commercial nuclear reactors in Canada.
TABLE 3.1

<table>
<thead>
<tr>
<th>PROCESS FAILURES</th>
<th>EMERGENCY COOLANT</th>
<th>CONTAINMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUEL AND FUEL HANDLING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- fuel failures in the core</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>- fuel failures during fuel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ELECTRICAL SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- complete and partial loss of</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Class 4 power supply</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>REACTOR CONTROL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- reactivity disturbances from</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>improper use of reactivity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>decay at both full and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>low power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of primary pressure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of secondary pressure</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>REACTOR CONTAINMENT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- flow blockage in a fuel channel</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>- failure of heat transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- failure of heat transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>system pump circulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of shield cooling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of shutdown cooling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of service water</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COOLANT SYSTEM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- failure in the major pipe of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the heat transport system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- feeder failure</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- end fitting failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- pressure tube failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- prime pump failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- loss of feedwater supply</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

13. ACKNOWLEDGEMENTS

We are indebted to W.R. Cooper, E.M. Hinchley, J.J. Lipsett, G.F. Lynch and E.M. Yaremko for their assistance and advice in the preparation of this document. We would also like to acknowledge the continued encouragement and support of E.O. Moeck and A.J. Stirling during the preparation of this document.

13. REFERENCES


ISSN 0067 - 0367

To identify individual documents in the series we have assigned an AECL- number to each.

Please refer to the AECL- number when requesting additional copies of this document from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada
KOJ 1J0

Price $3.00 per copy

ISSN 0067 - 0367

Pour identifier les rapports individuels faisant partie de cette série nous avons assigné un numéro AECL- à chacun.

Veuillez faire mention du numéro AECL- si vous demandez d'autres exemplaires de ce rapport au

Service de Distribution des Documents Officiels
L'Energie Atomique du Canada Limitée
Chalk River, Ontario, Canada
KOJ 1J0

Prix $3.00 par exemplaire