CHAPTER 6: SPECIAL SAFETY SYSTEMS

MODULE A: RELIABILITY CONCEPTS

MODULE OBJECTIVES:

At the end of this module, you will be able to describe the following for a CANDU reactor:

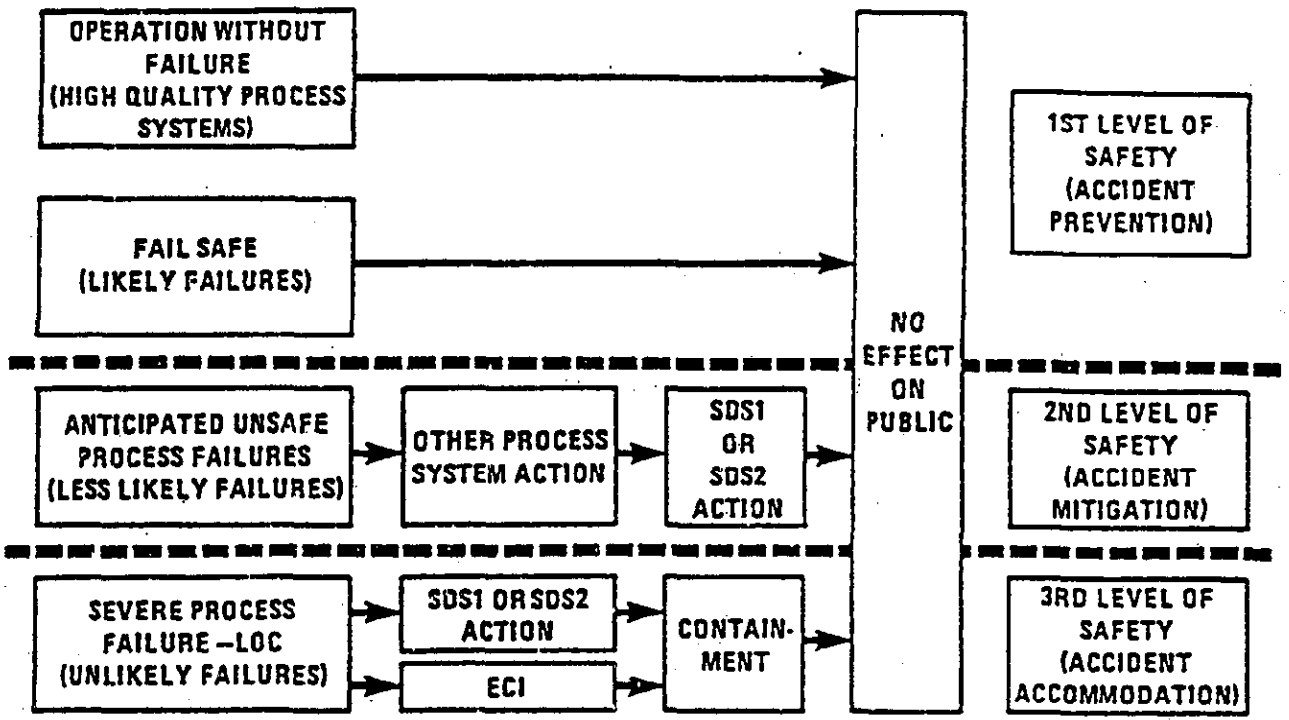
1. **define the four Special Safety Systems;**
2. **explain the increasing levels of safety provided by the Safety Systems in case of process system failures;**
3. **explain the significance of the eight main reliability principles and how a two out of three logic implements these principles.**

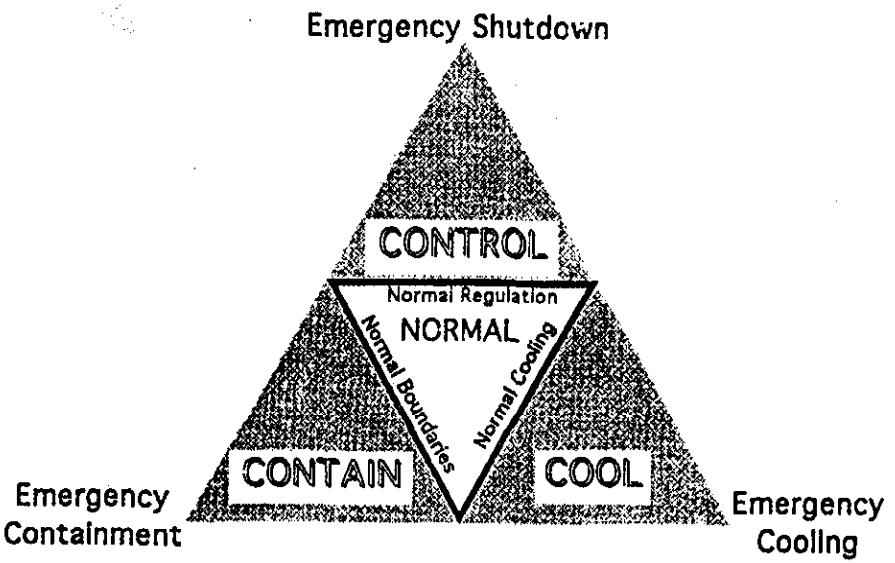
NTRODUCTION

pecial Safety Systems

- Mitigate the consequences of a serious process failure requiring reactor shutdown, decay heat removal and/or retention of released radioactivity.
- Do not perform any active functions in the normal operation of the plant: they are said to be 'poised' to prevent unsafe consequences of plant operation under abnormal or accident conditions.
- *The four special safety systems* are:
  - ⇒ shutdown system number 1
  - ⇒ shutdown system number 2
  - ⇒ emergency core cooling system
  - ⇒ containment system.
- The reactor may not be operated without all of the special safety systems being available.

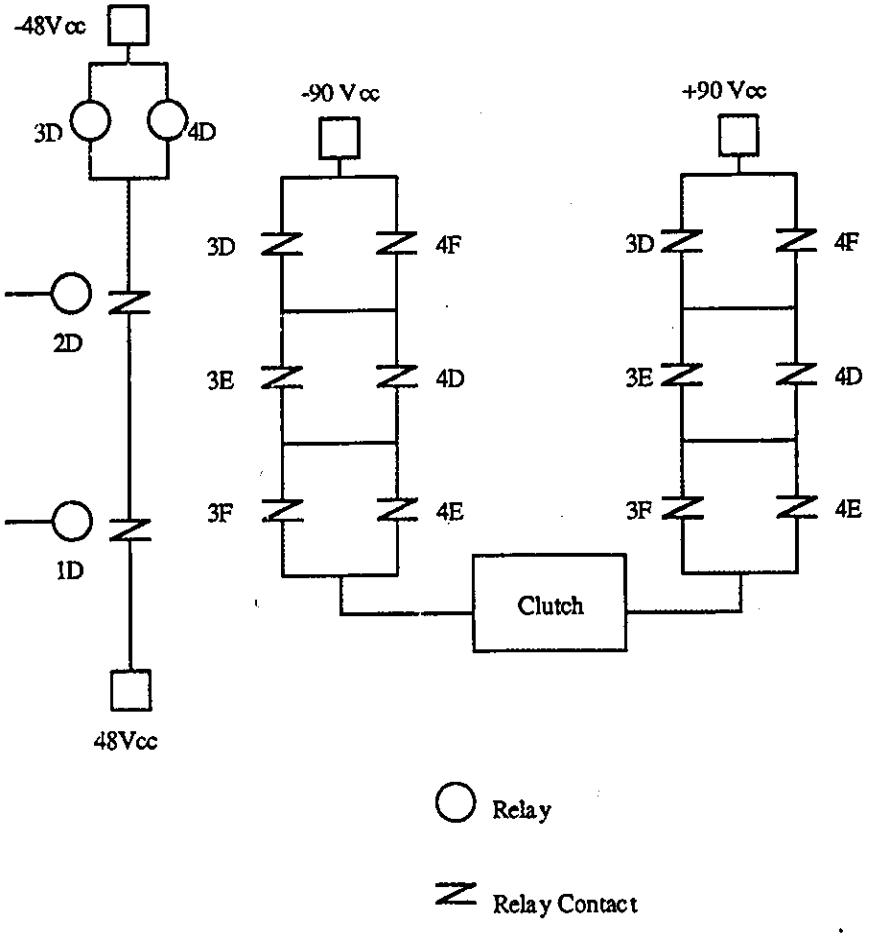
ystems which provide services, such as electrical ower, cooling water, and air to the special safety ystems are referred to as safety support systems.





RELIABILITY PRINCIPLES

- Redundancy
- Independence
- Diversity
- Periodic Testing
- Fail Safe
- Operational Surveillance
- Preventive Maintenance
- Predictive Maintenance



TWO OUT OF THREE LOGIC

- In order to reduce the number of unnecessary firings, a two out of three logic is used by each of the shutdown systems.
- Each shutdown parameter is related to three measuring devices, and each of these devices is associated with one of three electrical chains of the shutdown system.
- When a reading passes its setpoint, a relay logic acts to open the electric circuit. This chain of the SDS is then said to be "opened". Trip setpoints may be fixed or variable.
- Two such chains of an SDS must be opened for the firing of the SDS.

CHAPTER 6: SPECIAL SAFETY SYSTEMS

MODULE B: SHUTDOWN SYSTEM #1

MODULE OBJECTIVES:

At the end of this module, you will be able to describe the following features of a CANDU reactor:

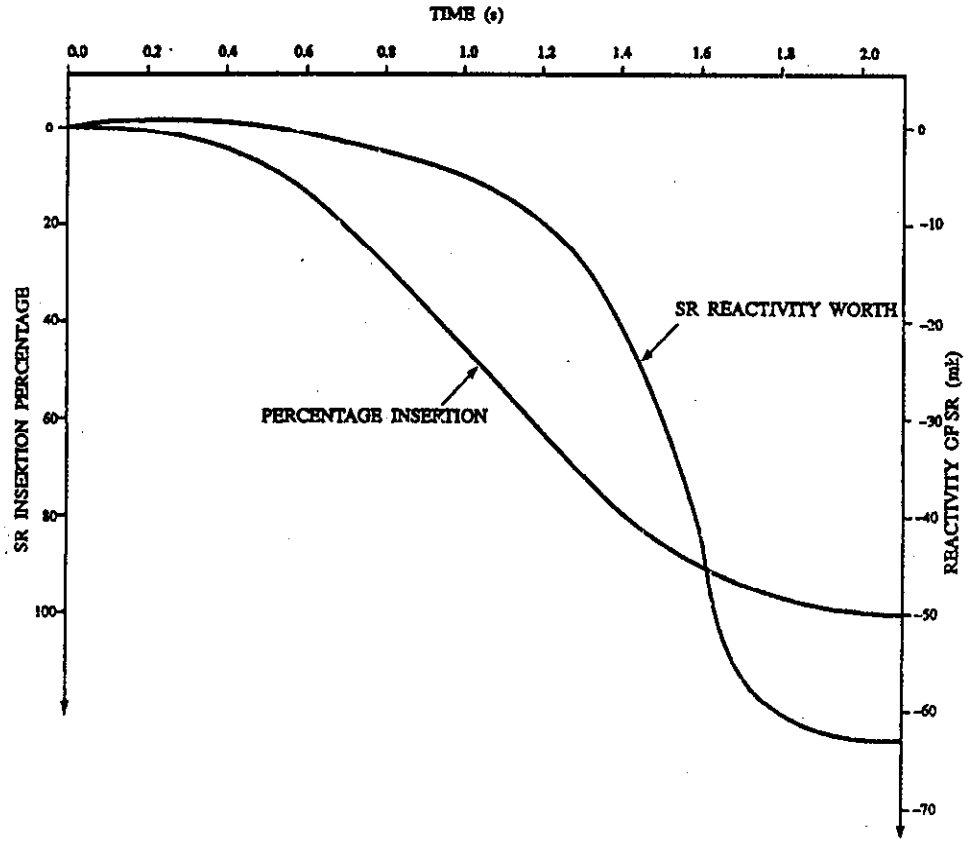
1. **The function, reactivity worth, insertion time, methods of insertion and testing of the shutdown rods;**
2. **The main types of trip parameters used for SDS1;**
3. **The role of the Reactor Regulating System in withdrawing the shutdown rods.**

NTRODUCTION

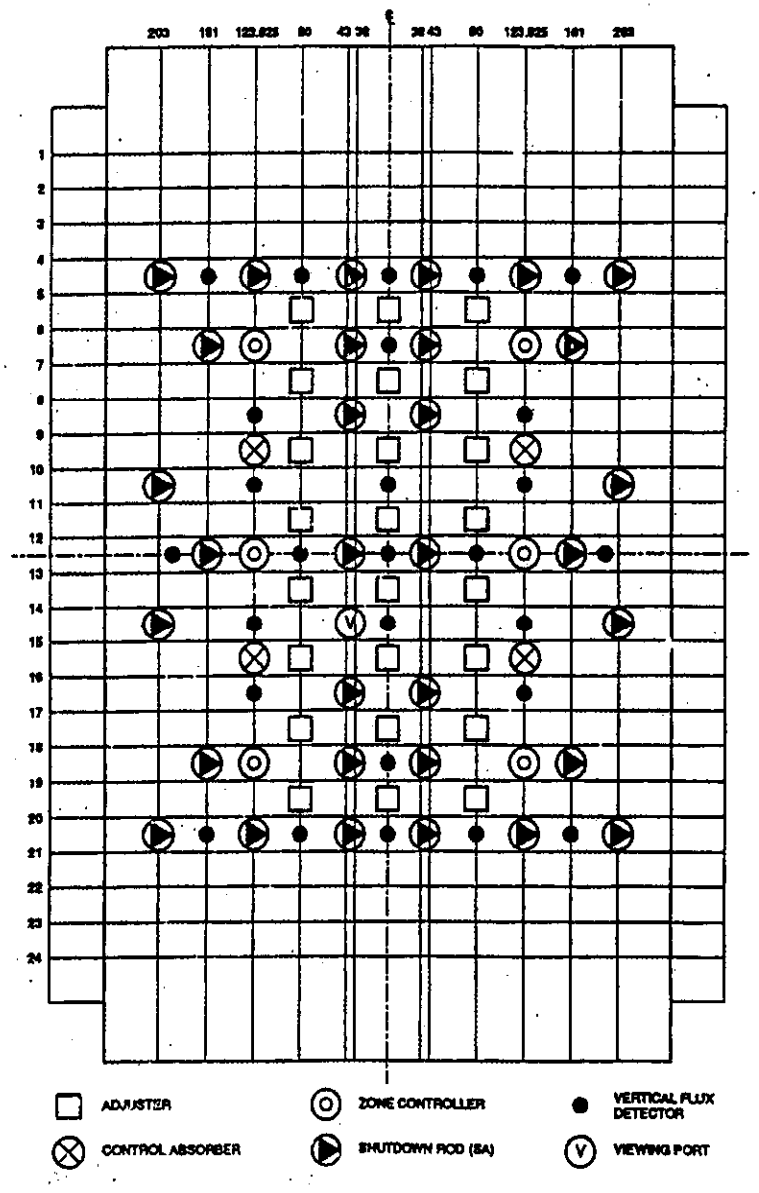
- Each CANDU reactor has two reactor shutdown systems, SDS1 and SDS2, completely independent of each other. They are also very different by design and by their intervention mode.
- Each of the shutdown systems must be able, by itself, to stop the neutron chain reaction during any accident condition.
- A further requirement is that the safety analyses used to show this capacity must be performed with part of the system impaired. For SDS1, the two most effective rods, on a total of 32, are assumed to stay out of core. For SDS2, the most effective injection line out of eight is assumed dead.
- Each shutdown system is environmentally qualified to the most severe conditions under which it is required to function.
- Each shutdown system meets an unavailability target of less than $1x10^{-3}$.
- The two shutdown systems incorporate the principles of redundancy, diversity, testability and separation throughout their design.
- The two shutdown systems are independent of the regulating and process systems.

SHUTDOWN SYSTEM NUMBER 1

- 32 Shutdown rods of cadmium and stainless steel
- reactivity worth is -60 to -70 mk;
- spring assisted gravity drop; fully inserted in 2 seconds.



Shutdown Rods Insertion and Reactivity Worth.



DS1 TRIP PARAMETERS

- ensure reactor power level is under CONTROL
- ensure that ability to COOL the fuel is maintained

Trip Parameter	Trip Condition	Typical Setpoint
Neutron Power	HIGH	120%FP
Rate Log Neutron Power	HIGH	10%/sec
Heat Transport System Flow	LOW (channel flow)	21 kg/sec
Heat Transport System Pressure	HIGH (ROH)	10.7 MPa
Heat Transport System Pressure	LOW	8.6 MPa
Pressurizer Level	LOW	2.5 m
Steam Generator Level	LOW	12 m
Steam Generator Feedline Pressure	LOW	5.1 MPa
Moderator Level	HIGH	9.5 m
Moderator Level	LOW	8.5 m

SHUTDOWN ROD WITHDRAWAL AND DROP TEST

- Normal withdrawal is controlled by the Reactor Regulating System.
- The shutdown rods are withdrawn as soon as the trip signal has been cleared and the trip has been reset by the operator.
- All shutdown rods are withdrawn simultaneously.
- Withdrawal of the shutdown rods is interrupted if:
  - ⇒ control is switched to manual, or
  - ⇒ the flux power error is excessive, or
  - ⇒ the reactor is tripped.
  - ⇒ if the log-rate exceeds 7 percent per second.
- The computer monitors the withdrawal time and, if it is greater than normal, the 'shutdown rod stuck' signal is generated.
- An individual rod may be selected for manual control at any time for drop testing or drive.
- A partial drop test facility is provided in the clutch circuit to allow the operation of each shutdown rod to be checked during reactor operation.
- Withdrawal of the rods by banks in the manual mode is possible when the automatic control is not available.

CHAPTER 6: SPECIAL SAFETY SYSTEMS

MODULE C: SHUTDOWN SYSTEM #2

MODULE OBJECTIVES:

At the end of this module, you will be able to describe the following features of a CANDU reactor:

1. **The function, reactivity worth and insertion time of SDS2 liquid poison;**
2. **The main operating features of the liquid poison injection system;**
3. **The main types of trip parameters used for SDS2.**

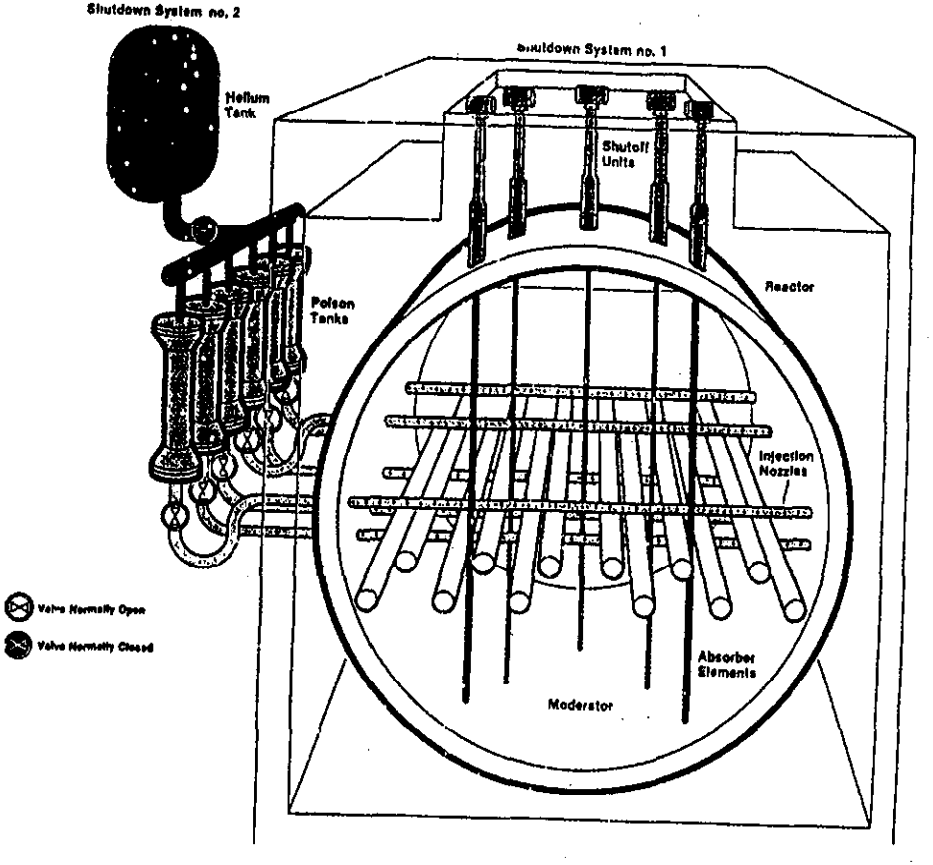
NTRODUCTION

Recall the following key requirements for the Reactor Shutdown Systems:

- Each CANDU reactor has two emergency shutdown systems, SDS1 and SDS2, completely independent of each other. They are also very different by design and by their intervention mode.
- Each of the shutdown systems must be able, by itself, to stop the neutron chain reaction during any accident condition.
- The two shutdown systems incorporate the principles of redundancy, diversity, testability and separation throughout their design.

o met these requirements and method of hutdown that was as different as possible from the hutdown rods used in SDS1 is required.

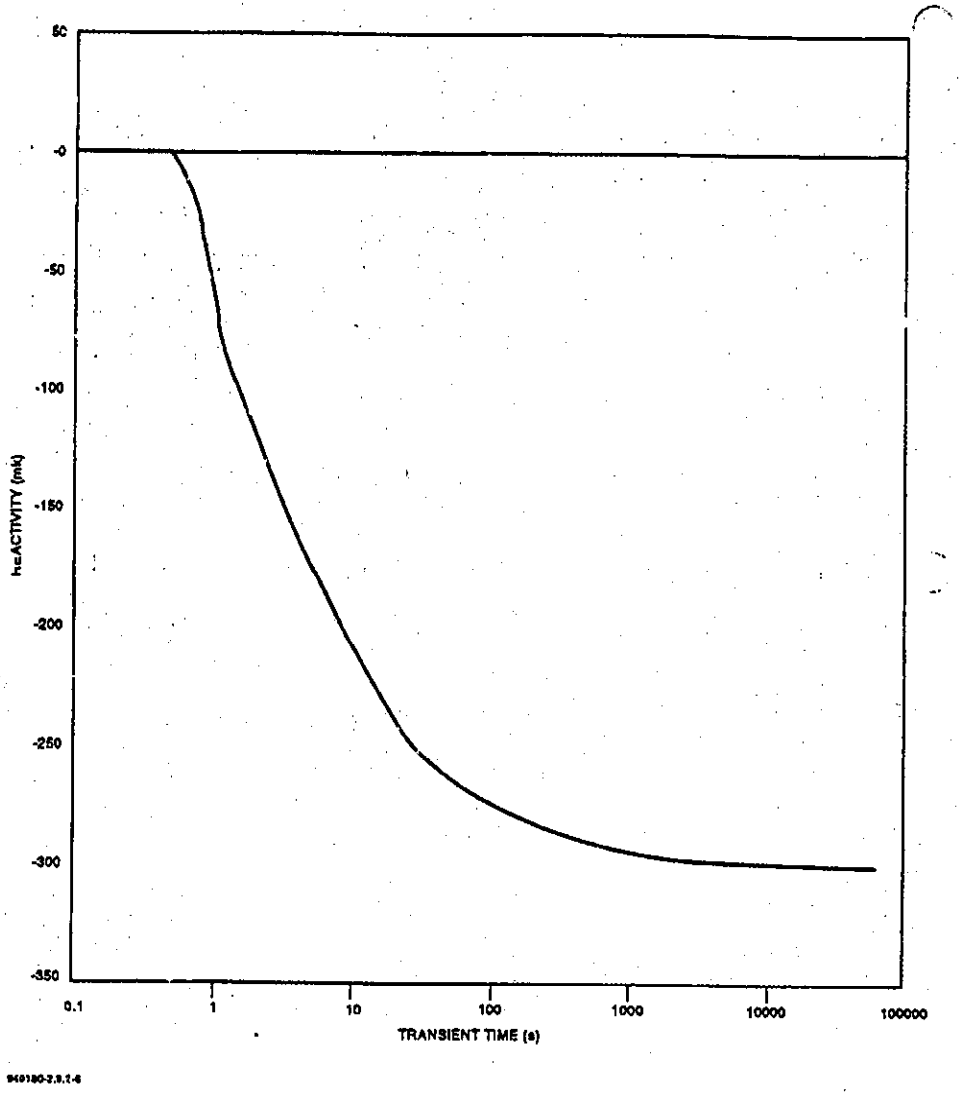
DS2 uses a liquid poison injection system.



IQUID POISON INJECTION SYSTEM

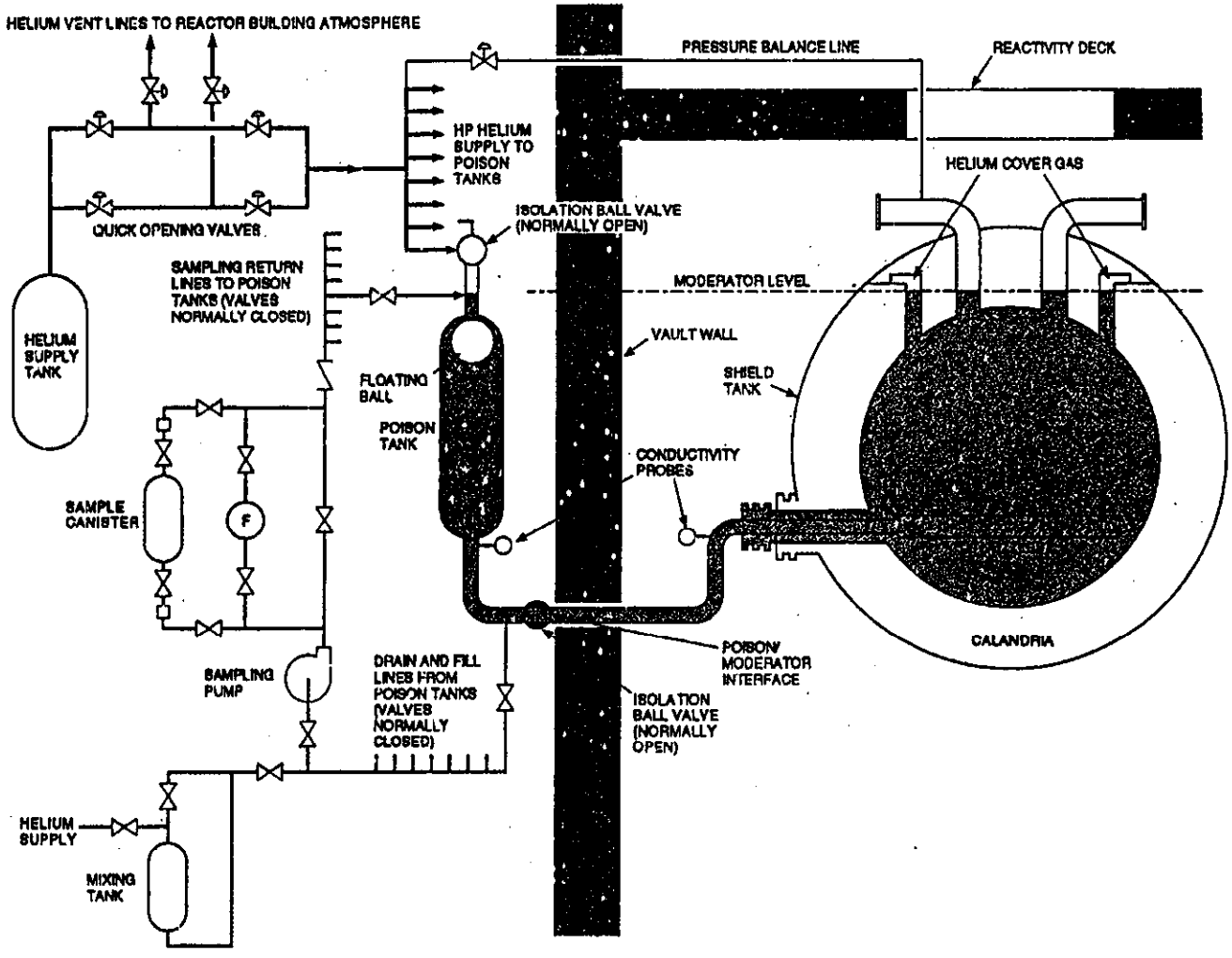
he method chosen incorporates the following features:

- liquid poison;
- horizontal orientation of both trip measuring devices and of poison injection assemblies;
- three independent channels signal the opening of fast-acting valves which release high pressure helium to inject gadolinium poison into the moderator.



SHUTDOWN SYSTEM NUMBER 2

- high pressure helium supplies energy for rapid poison injection;
- four quick opening valves in two successive pairs
- valves are air-to-close, spring-to-open
- eight poison tanks,
- polyethylene floating ball to prevent backflow of poison and injection of helium into the calandria
- liquid-to-liquid interface at the ball isolation valve that is normally open
- four rows of eight injection jets on each nozzle



SDS2 TRIP PARAMETERS

- ensure reactor power level is under CONTROL
- ensure that ability to COOL the fuel is maintained
- ensure CONTAINMENT is maintained

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

CHAPTER 6: SPECIAL SAFETY SYSTEMS

MODULE D: EMERGENCY CORE COOLING SYSTEM

MODULE OBJECTIVES:

At the end of this module, you will be able to describe the following features of a CANDU reactor:

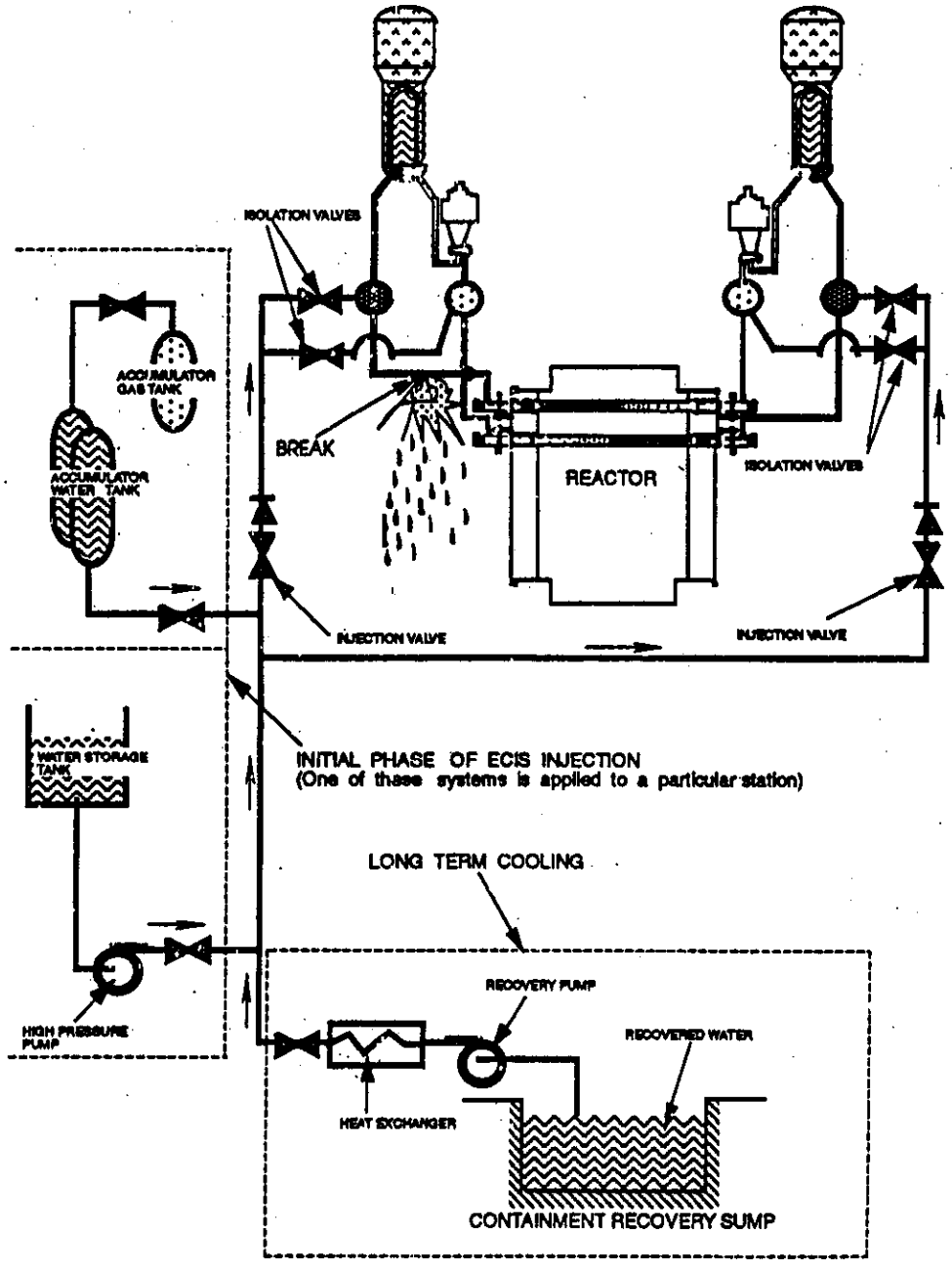
1. **The functional requirements for Emergency Core Cooling;**
2. **The equipment and operation of the ECC systems during the injection phase;**
3. **The equipment and operation of the ECC systems during the recovery phase;**
4. **The operation of the process systems during a loss of coolant accident.**

INTRODUCTION

The system is required to maintain or re-establish COOLING of the fuel and fuel channels for specified loss-of-coolant accidents so as to limit the release of fission products from the fuel and maintain fuel channel integrity.

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

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

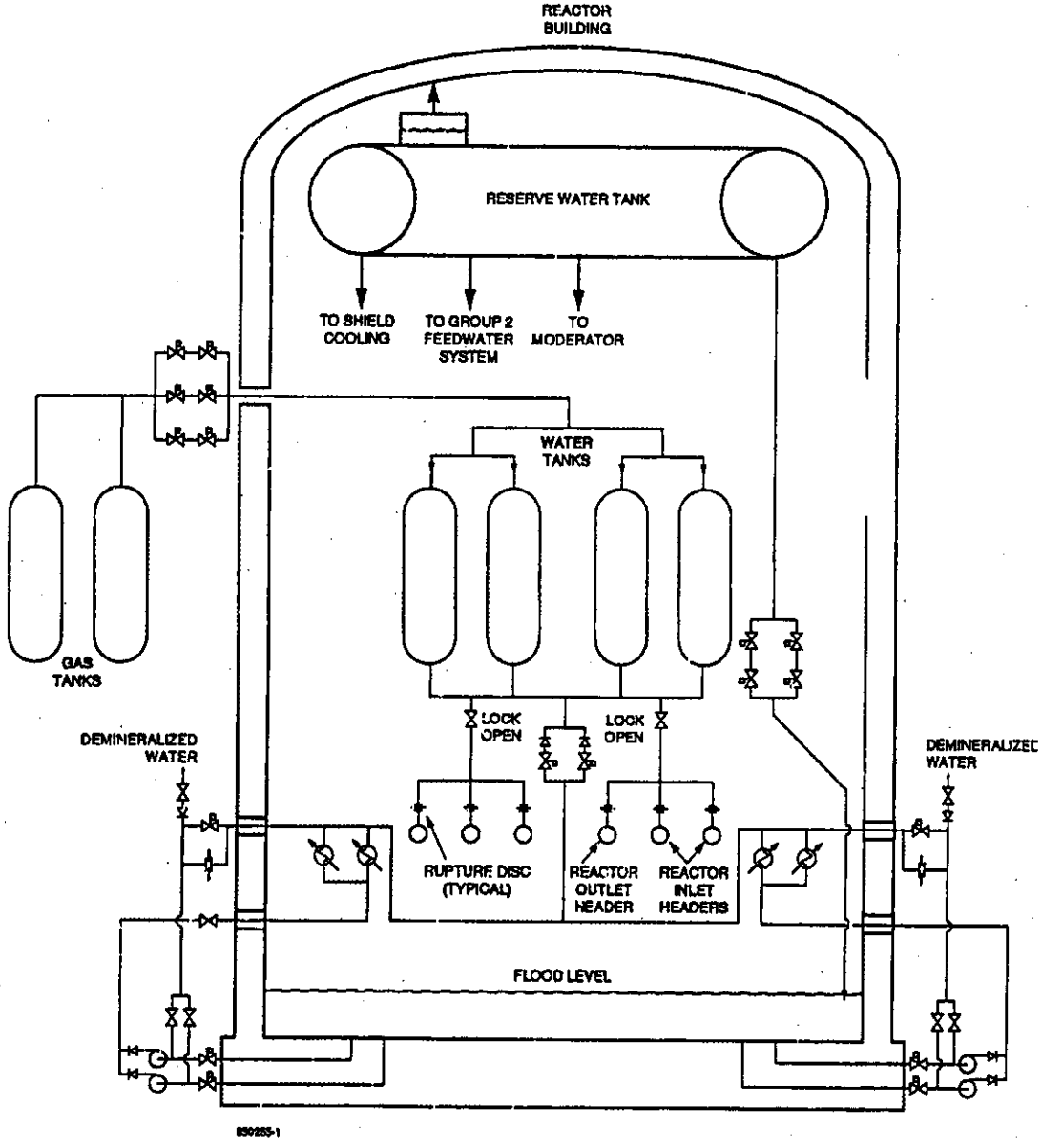


SYSTEM DESCRIPTION

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

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

In the recovery stage, the recovery pumps draw water from the fuelling machine vault floor, and discharge it into the reactor headers via the emergency core cooling heat exchangers. The recovery stage begins when the emergency core cooling system water tanks are depleted. The water subsequently escapes from the break in the heat transport system, falls to the floor and is recirculated by the recovery pumps. The recovery stage provides a long term heat sink.



PROCESS SYSTEM OPERATIONS

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

The main steam safety valves are opened on the loss-of-coolant signal, to provide a rapid cooldown of the steam generators, commonly referred to as steam generator crash cooldown. This reduces the transfer of heat from the secondary side to the primary side during the initial period of emergency core cooling injection and allows the steam generators to provide a long-term heat sink for 'small' breaks during steady state emergency core cooling operation.

For scenarios involving a small loss-of-coolant accident and the loss of the emergency core cooling, a steam generator crash cooldown depressurizes the heat transport system and reduces the stress on pressure tubes.

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

CHAPTER 6: SPECIAL SAFETY SYSTEMS

MODULE E: CONTAINMENT SYSTEM

MODULE OBJECTIVES:

At the end of this module, you will be able to describe the following features of a CANDU reactor:

1. **The functional requirements for the Containment System;**
2. **The equipment and operation of the Containment System.**

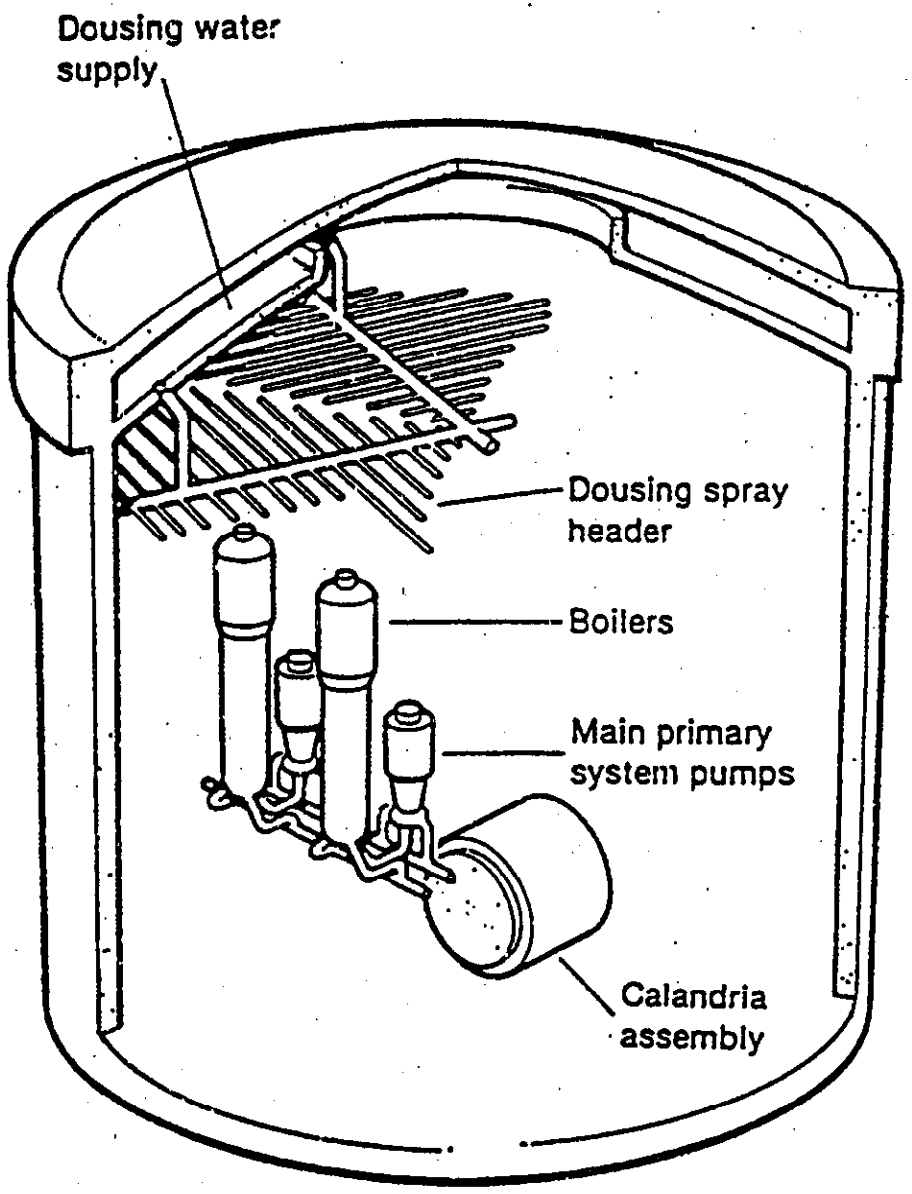
INTRODUCTION

The basic function of the containment system is to form a continuous pressure-confining envelope about the reactor core and the heat transport system in order to limit the release to the external environment of radioactive material resulting from an accident.

An accident which causes a release of radioactive material to containment may or may not be accompanied by a rise in containment pressure.

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

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



he containment structure also serves the following functions:

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