D. REACTOR, PERSONNEL AND PUBLIC PROTECTION

ENABLING OBJECTIVES:

2.20	State the three main isotopes produced in the moderator, when they are produced, and the hazards they pose.
2.21	Name the major hazards associated with the HTS at power and when shutdown.
2.22	Describe how the safety shutdown systems shut down the reactor.
2.23	Describe the Emergency Coolant Injection (ECI) system and state its purpose.
2.24	Describe the Negative Pressure Containment (NPC) system.
2.25	Describe the operation of and reasons for two-out-of-three trip logic.

HAZARDS

Significant numbers of neutrons are present in the core when reactor power is a few percentages of full power or higher. These neutrons interact with D_2O, in both the moderator and coolant, to produce a number of radioactive isotopes:

- **nitrogen-16** (N-16),
- **oxygen-19** (O-19)
- **tritium** (H-3).

NITROGEN-16 AND OXYGEN-19

N-16 and O-19 emit very high energy gamma rays along with energetic beta particles.[11] The beta particles do not penetrate pipe walls, but the

[11] Beta particles are another type of nuclear radiation. They are essentially negatively charged electrons.

penetrating gamma rays are a hazard around equipment containing these isotopes. N-16 and O-19 have short **half lives.**[12] These isotopes decay to harmless levels a few minutes after a reactor shutdown. They return to dangerous levels within seconds of restarting.

Systems that handle water circulating from the reactor core can be approached only with the reactor shutdown. Very heavy shielding around *this equipment may allow work on nearby equipment with the reactor* running. A few systems require attention when the reactor is at power. Some systems, such as the liquid zone control system, use a delay tank between the core and the equipment to delay the flow of water (H_2O or D_2O) thereby giving time for N-16 and O-19 to decay before reaching accessible areas.

TRITIUM

Tritium (H-3) with a half life of 12.3 years gradually builds in concentration over the operating life of the reactor in both moderator and heat transport D_2O. It represents a continuing hazard at all levels of operation. When decaying, tritium emits a low energy beta particle and no gamma ray. Normal radiation instruments cannot detect tritium. A person with Radiation Protection Training (RPT) qualifications can check most workplace radiation hazards but may depend on Health Physics experts to monitor areas where tritium could be a hazard.

The low energy beta particle from tritium will not penetrate the outer layer of dead skin. But as water vapour, tritium enters the body through the lungs and through the skin and disperses to all parts of the body. Body tissues and organs have no dead layer of skin to protect them. Tritium is our most significant radiation hazard, contributing typically 30% to 50% of staff radiation dose.

Moderator water has the highest tritium concentration of all plant fluids. Tritium escapes primarily when the system is open for maintenance. Little escapes otherwise because the moderator is not pressurized, and there are few leakage points. During normal operation the coolant D_2O contributes more tritium exposure to station personnel than moderator water because the coolant is hot and under pressure and the system has many possible leak points.

Station staff wear plastic suits with supplied breathing air to work in atmospheres containing tritium. These suits are required when a small

[12] A half life is the amount of time it takes for the radiation source to decay by 50%.

leak or spill of tritiated D_2O occurs or a system is opened for maintenance.

In the future the tritium hazard may be less dangerous. In 1990 a tritium removal facility started operating at the Darlington site. It is designed to remove 99.5% of the tritium in the heavy water it processes. This system will be discussed in more detail in module 5.

OTHER HAZARDS

Defective fuel releases a range of radioactive fission products into the coolant. Some, for example Iodine-131, are vapours that produce a radiation hazard around open equipment. Others plate out on piping and contribute to the plant radiation dose.

The heat transport system also presents two conventional hazards not seen in the moderator system. These are **high pressure** and **high temperature**.

SAFETY SYSTEMS

Each CANDU unit has four special safety systems. These are the **Shutdown Systems** (SDS1 and SDS2), the **Emergency Coolant Injection System** (ECI) and the **Containment System**. The plant design includes these four special safety systems to support the reactor safety requirement to control, cool and contain (refer to Module 1 - Reactor Safety).

SHUTDOWN SYSTEMS

Instruments monitor reactor conditions such as heat transport system pressure, reactor power and coolant flow. Any measurement that shows possible risk of damaging the fuel or other unsafe operating conditions will trigger a reactor shutdown. A shutdown by a protective system is called a **reactor trip**. A trip occurs automatically whenever a trip parameter (measurement) exceeds its trip set point (safe operating limit). The operator can trip the reactor manually if necessary.

To provide greater assurance of availability, shutdown system instruments and mechanisms are completely separate from devices used for normal regulation. Each reactor has two physically separate shutdown systems to

ensure independence. All units use shut off rods for SDS1. Liquid poison injection is used for SDS2 in most of the CANDU reactor units.[13]

Shutoff Rods

The SDS1 shutoff rods are nearly identical to the control absorber rods in figure 2.14. Each rod is made of stainless steel sheathed cadmium material suspended vertically in guide tubes above the reactor as shown in figure 2.15. Each rod is restrained from dropping down its guide tube by a cable wound around a sheave and held by an electromagnetic clutch. A reactor trip signal cuts off the electricity to the clutches, dropping the rods completely into the core in about two seconds. Most stations use fast acting, spring-loaded shutoff rods.

Liquid Poison Injection System

SDS2 is a fully independent shutdown system intended to operate when unsafe conditions exist, whether or not SDS1 operates. Do not confuse this protective system with the liquid poison addition system. Both systems put neutron absorbing poison in the moderator. The operator adds small amounts manually with the addition system. SDS2 automatically injects a large quantity of poison in a couple of seconds.

SDS2 consists of several tanks containing a high concentration of gadolinium nitrate (a strong neutron absorber) in solution in heavy water. Each tank is connected by an open line to a perforated tube that runs horizontally through the reactor. The general arrangement is shown in figure 2.18.

The system is activated by opening the isolation valves at the top of the gadolinium tanks. High pressure helium injects the gadolinium solution from the poison tanks into the moderator. The poison enters through horizontal tubes, one tube per tank. As a tank discharges, a floating ball rides the liquid surface down the tank and seals the discharge line. This prevents the helium gas from entering and overpressurizing the calandria.

To increase the reliability of tripping the reactor when necessary, the detectors that activate SDS2 are completely independent of those activating SDS1. As mentioned above, both sets of instruments are also separate from the ones used by the regulating system.

---

[13] Pickering A relies on dump tanks for its SDS2.

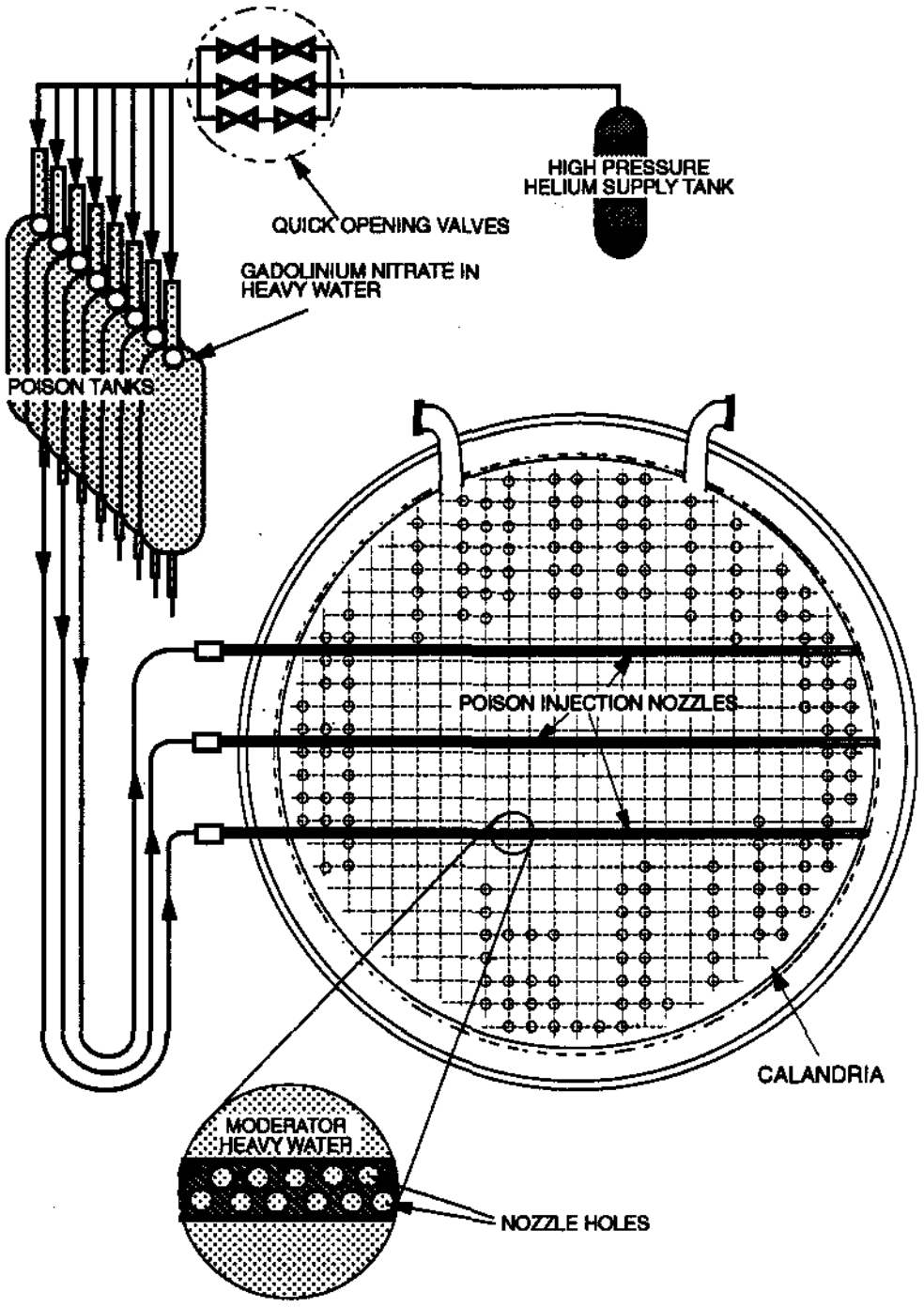

Figure 2.18
General Schematic of Shutdown System 2
(Liquid Poison Injection)

EMERGENCY COOLANT INJECTION (ECI)

Recall that in normal operation, five barriers stand between the main source of radiation and the public (ceramic fuel pellets, fuel sheath, heat transport system, containment system, and exclusion zone). Rapid shutdown protects the first three barriers. In most upsets, a rapid power reduction quickly matches the fuel heat output to available cooling. The fuel stays wet and does not release fission products. In accidents that release radiation, rapid shutdown limits fuel failures and radiation release. This allows the two final barriers, containment and dilution, to do their job.

The emergency coolant injection system protects the first three barriers when normal cooling fails. Its purpose is to refill the heat transport system and keep it full after a **Loss of Coolant Accident** (LOCA). This sets up an alternate heat flow path for removing decay heat. Both the ECIS and the containment system must operate under conditions caused by a LOCA. In a multi-unit station there is only one ECIS and containment system shared by all the units in the station. These two systems must be available in order to operate the station.

During a LOCA, low pressure (due to loss of D_2O) allows steam to form in the heat transport system (this is similar to opening a hot radiator on your car) blanketing the fuel bundle, hence impairing heat removal from the fuel. If this condition persists, fuel fails and releases fission products through the break. ECIS is intended to act quickly to limit these failures and reduce the demands on containment. For a small LOCA, rapid reactor shutdown and ECIS operation may prevent any fuel failures.

Figure 2.19 shows a typical ECIS during high pressure injection of cooling water to a unit. In the figure, gas pressure or a high pressure pump forces H_2O from the water tanks into the reactor.

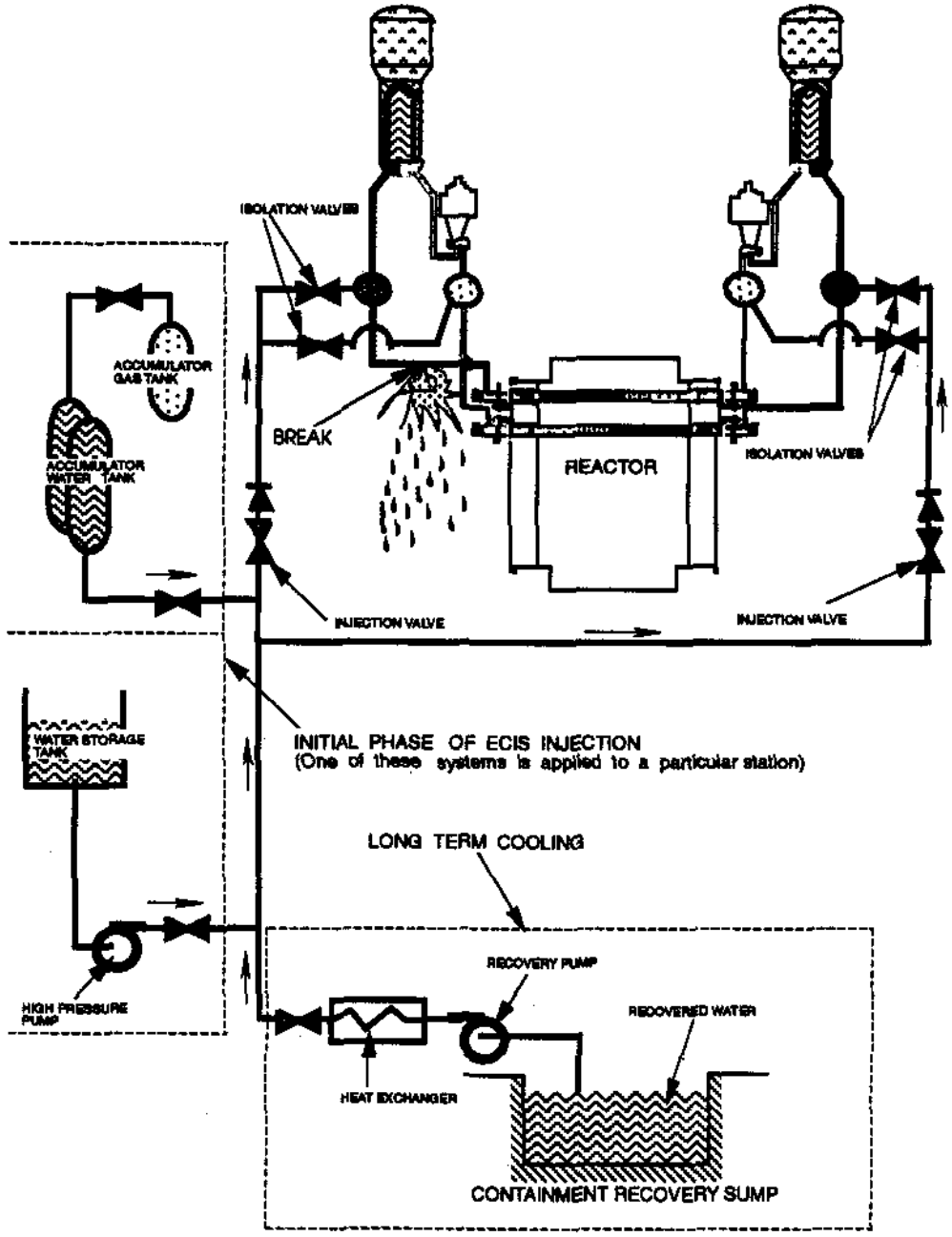

Figure 2.19
General Schematic of the Emergency Coolant Injection System (ECIS)

A sudden drop in HTS pressure automatically triggers the ECIS, otherwise the operator can trip ECIS manually if pressure drops too slowly and no other means of cooling is available. The ECIS signal opens the injection valves of the affected unit. These valves separate the ECIS H_2O from the coolant D_2O. The signal also connects the high pressure source that forces the light water into the reactor inlet and outlet headers.

Injection begins when the HTS pressure is lower than the ECIS injection pressure.

Coolant moves from the inlet and outlet headers towards the break. Water injected at the headers passes over the hot fuel and rewets it. A mixture of light and heavy water and steam escapes from the break. The hot water mixture spills to the reactor floor and is collected in the recovery sump. For long term cooling, the recovery pump returns the recovered water to the reactor headers through a recovery heat exchanger for cooling. This cooling loop can operate indefinitely.

CONTAINMENT

The containment system is the fourth barrier to release of radiation. Its purpose is to establish and maintain a protective barrier to hold released radioactive material. This limits staff and public exposure to radioactivity when the first three barriers fail.

The containment system is actually a set of subsystems and equipment that maintains and protects the barrier to release of radiation. The entire system is considered unavailable if any of these subsystems is not available. Like ECIS, containment must be available before any unit can operate. The subsystems include:

- envelope and isolation equipment,
- dousing,
- coolers,
- filtered air discharge.

The design used for multi-unit CANDU reactors is negative pressure containment. Units in a multi-unit station share a vacuum building. Negative pressure in the vacuum building is maintained by a set of vacuum pumps located in the basement of the vacuum building. Figure 2.20 shows that the vacuum building and reactor building are each part of the **containment envelope.**

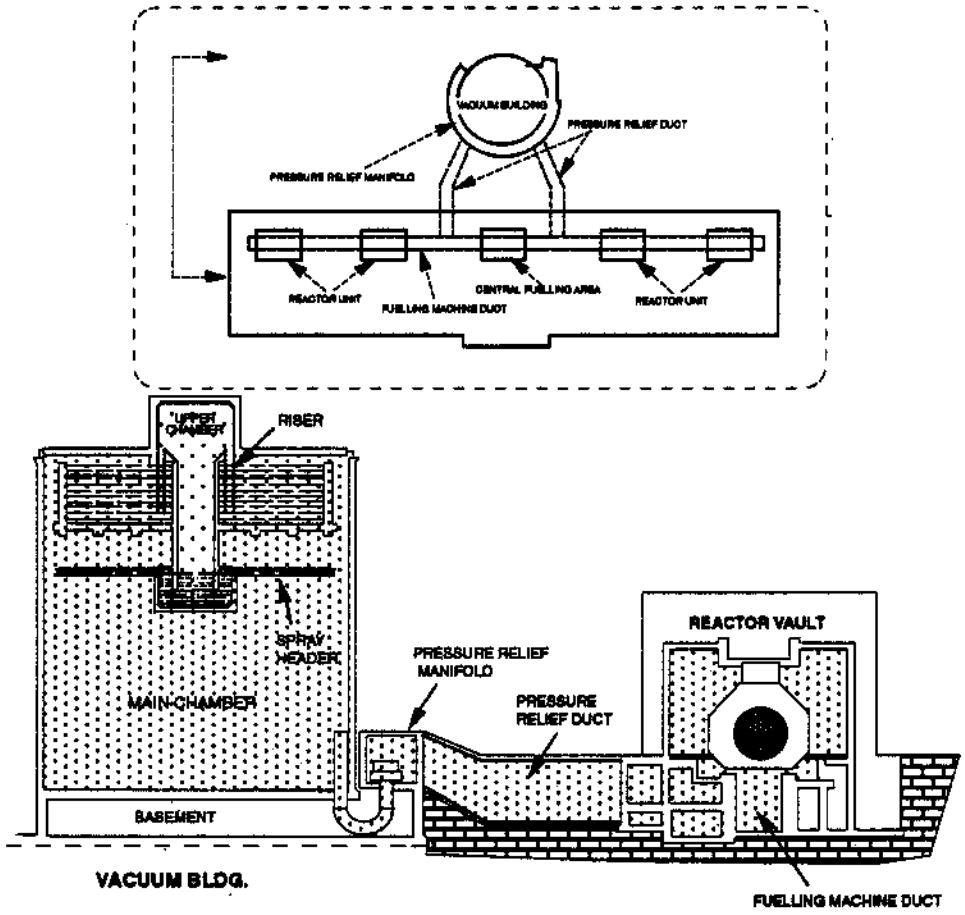

Figure 2.20
Negative Pressure Containment Envelope

During a LOCA, steam released from the heat transport system flows through the pressure relief duct to the pressure relief manifold, automatically opening the pressure relief valves. The high pressure steam expands into the low pressure vacuum building. The pressure buildup inside the building forces the water in the tank, located at the upper portion of the building, to the riser section then to the spray header. The water spray **dousing system** condenses the steam in the vacuum building, reducing the pressure buildup inside the building and containing radioactive release from the reactor.

The **coolers**, located inside the reactor vault and normally used to maintain the containment atmosphere below 40°C during operation, are needed to perform a long term containment function following a LOCA. They provide sufficient heat removal capacity to assist in maintaining the integrity of the containment envelope.

A **filtered air discharge system** is operated over the long term to relieve high pressure buildup after a LOCA. This maintains containment pressure sub atmospheric and allows a controlled and monitored release of fission products from containment.

TWO-OUT-OF-THREE TRIP SYSTEM

Safety systems must operate reliably when called on, but should not trip unnecessarily. For example, the shutdown systems must stop the fission process quickly when required. An unnecessary trip, however, could prevent reactor restart for 35 to 40 hours (due to rapid buildup of xenon). Apart from the cost of replacement power, the sudden power reduction is hard on equipment.

Safety systems are made with very reliable equipment. Maintenance programs and frequent testing make certain that they operate correctly. An important part of the reliability of these systems is the tripping mechanism. Figure 2.21 shows the two-out-of-three trip logic and figure 2.18 shows its location in the liquid poison injection system. The electronic contacts that open to trip SDS1, containment and ECI have a similar arrangement.

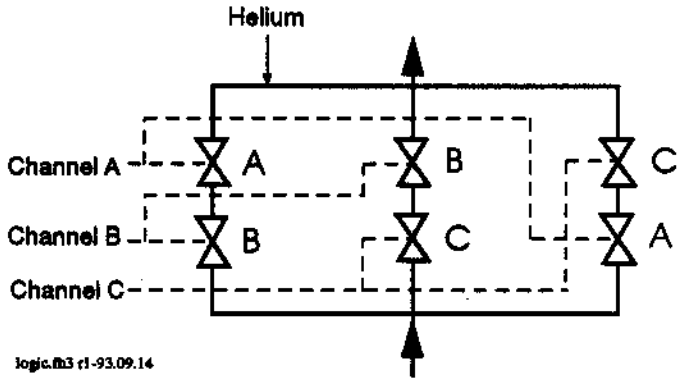

Figure 2.21
Typical Trip Logic

Consider the trip system for SDS2 in figure 2.21. It has three helium lines. Each line has two valves in series. Three independent signal channels labeled A, B and C send the trip signal to the valves. Signal A opens the two A valves, signal B opens the two B valves and signal C opens the two C valves. (Do not confuse the helium line [a pipe containing helium gas] with a trip channel which sends the signal to open the valves.) On a normal trip, all three channels simultaneously send trip signals. All valves open. Helium flows through all three lines, causing a shutdown by poison injection. The system also operates if only one or

two helium lines open on a trip. Why then have three lines? There are three reasons for the arrangement of figure 2.21:

a) **There is no reactor trip on a spurious signal in any one channel.**

Suppose one channel fails, producing a spurious trip signal. For example, a fault in a signal transmitter in channel A could open the channel A valves. With just one set of open valves, helium cannot pass through any of the three lines. There is no trip.

An unnecessary trip caused by this type of equipment failure requires simultaneous failures in two channels. Very reliable equipment is used, and the equipment is tested and maintained regularly. This makes a single fault unlikely. The chance of two channels failing simultaneously is extremely small.

b) **A trip occurs even if one channel fails to respond to a real trip situation.**

On a valid trip, if any one channel fails to provide a trip signal the system still operates. For example, a faulty transmitter in channel A could fail to send a signal to the channel A valves. The other four valves, operated by signals B and C, do open. Flow of helium through the line with no A valve will cause a reactor trip.

Again, reliable equipment that is carefully tested and maintained makes a single fault unlikely. Simultaneous failures in two channels, which could make the system fail, are highly unlikely. However, if one shutdown system does fail, the other shutdown system will shutdown the reactor. Reactor shutdown in a real emergency is almost certain.

c) **Two-out-of-three trip logic allows for maintenance and testing at power without any loss of protection.**

A single channel can be tested by tripping it to see if it works. This does not trip the reactor, provided testing is done on one channel at a time. There is no loss of trip coverage should a real emergency arise during testing. A trip signal on any other channel will trip the reactor. There is an increased risk of an unnecessary shutdown, caused by a spurious trip on another channel during testing. This does not reduce reactor safety, but it is expensive.

Some on power maintenance can be done one channel at a time with the channel tripped. In this state a trip signal on either of the

other channels will cause a shutdown. There is no loss of trip coverage should a real emergency arise during maintenance. Again, there is an increased risk of an unnecessary shutdown.

ASSIGNMENT

1. What are the three main radioactive isotopes produced in the moderator and what kind of hazard do they pose?

2. How do the hazards present in the HTS differ when at full power and when shutdown?

3. What are the two types of safety shutdown system and how does their design support the reliability concept of **independence**?

4. From a reactor safety point of view, what role does the ECIS play?

5. What event is the containment system designed to protect against and how does it carry out that function?

6. How does two-out-of-three logic accommodate a failure in one channel to allow a valid trip to occur?