# B. REACTOR SAFETY

**ENABLING OBJECTIVES:**

1.5 Explain how the principle of **Control, Cool and Contain** guides reactor operation.

1.6 Explain how the following concepts contribute to the reliability and/or availability of systems or equipment:

a) redundancy;
b) independence;
c) diversity;
d) fail safe operation;
e) periodic testing;
f) operational surveillance;
g) preventive maintenance;
h) predictive maintenance.

1.7 State what is meant by Defence in Depth, and describe the five parts of the Defence in Depth model.

1.8 List the five barriers that protect the public from fission products.

1.9 State the purpose of the following documents:

a) Safety Report;
b) Station Operating Licence;
c) Operating Policies and Principles (OP&Ps);
d) Operating Procedures.
e) Certificates of Approval;

1.10 State the possible consequences of an OP&P violation.

As mentioned in Section A, this section is concerned with the acute hazard posed by the radioactive materials contained within our nuclear stations. In order to minimize the potential threat from these materials, a number of principles have been developed and incorporated into the design and operation of Ontario Hydro's nuclear generating stations. Collectively, these principles are known as **Reactor Safety**. The golden rule of Reactor Safety can be stated as:

**THERE IS A MINIMUM RISK TO THE PUBLIC AND THE ENVIRONMENT FROM REACTOR FUEL, PROVIDED THAT AT ALL TIMES:**

- **THE REACTOR POWER IS CONTROLLED;**
- **THE FUEL IS COOLED;**
- **THE RADIOACTIVITY IS CONTAINED.**

This rule is often shortened to **CONTROL, COOL, AND CONTAIN.**

This section is intended as a brief introduction to some of the key concepts of Reactor Safety. It will examine basic reliability concepts, the Defence in Depth model and the role of station documentation.

## BASIC RELIABILITY CONCEPTS

The reliability piece in our operating philosophy puzzle is concerned with the overall reliability of our generating stations. CANDU generating stations have a world wide reputation for reliability. Their capacity factors (a measure of actual output against the theoretical maximum[8]) have been amongst the highest of all commercial reactors world wide. Typically CANDU reactors have filled five, or more, of the top ten ranking list. Recently, our reliability has not been as high as we were once able to boast. A programme called the **Quality Improvement Program** (QIP) has been put in place to help us to focus our efforts on bringing reliability back up to its previous level.

In addition to trained and motivated staff, overall station reliability is a function of the reliability of systems and equipment. As we will see in the section on Defence in Depth, this reliability is critical to the safe operation of our reactors. For this reason alone, it is vital that all staff work to ensure the success of the Quality Improvement Program.

The following material provides an introduction to basic reliability concepts as they relate to CANDU equipment and systems. It will provide you with the background to understand the role of reliable process and safety systems in our discussion of Defence in Depth.

---

[8] Refer to Section D, Economics of CANDU, for a definition.

## DEFINITIONS

**Reliability** is defined as:

> *the probability that a device will work adequately for the period of time intended under the operating conditions encountered.*

Reliability is a probability with a numerical value ranging from 0 (totally unreliable) to 1 (always operates for the time intended). If a pump is judged to have a reliability of 0.99 for its first year of operation (based on historical data for this type of pump), this means that for 1000 hours of operation the pump will be unavailable for no more than 10 hours.

Reliability is concerned with whether an operating component in a **process system**[9] is likely to fail. When dealing with **poised systems**[10] the concern is whether a system or component will be available when called upon to operate.

**Availability** is related to reliability but is defined as:

> *the fraction of time that a device is available to work if called upon to do so.*

Availability has a value of from 0 (never available) to 1 (always available) and is generally expressed as years per year or hours per year. The value which is more frequently encountered, however, is **unavailability**. For example, if a poised system has an unavailability target of $10^{-3}$ years/year, this means that it will be unavailable for no more than 8 hours during the year (1 year=8760 hours and 8/8760 is approximately $10^{-3}$).

## CONCEPTS

High reliability and availability can be achieved by attention to a number of reliability principles during design and operation of a station.

1. **Redundancy**

   If only one component exists to perform a certain function, when it fails, the system fails. This problem can be reduced by installing additional components, so that if one fails, there is another to do

---

[9] A process system is a system that operates continuously.
[10] A poised system is a system that is called upon to act only in special circumstances.

the job. In other words, higher reliability can be attained by providing a backup (or redundant) component. **It is important to understand that this redundancy is provided primarily to ensure reliable operation, not to allow more convenient maintenance.** Taking redundant equipment out of service for maintenance will lower the reliability of the system.

We can look at the space shuttle programme to provide us with an example. The computer control system in each shuttle contains more than one computer. Redundancy is provided by running the same software control programme on more than one computer. If one computer fails, another is immediately available to assume control.

2. **Independence**

Independence is the physical separation of systems or components so that a fault in one system will not affect the others. Using the space shuttle, an example of independence is separate power supplies for each of the computers. This way failure of the power supply to a computer does not at the same time disable the other computers.

3. **Diversity**

Diversity is an attempt to ensure that there is more than one way of doing a job. Again using the space shuttle, diversity is provided by running entirely different software control programmes on different computers to achieve the same purpose. The software is even created by a different design team. This ensures that a bug in one piece of software is not duplicated in the other so that one mistake cannot disable more than one computer.

4. **Periodic Testing**

When a component in a process system fails the effects are immediately apparent. Failure of a poised system, on the other hand, is not readily apparent and can only be determined by testing. Since it is not possible to determine at what point the failure occurred, the unavailability is considered to be half the time since the system was last tested (plus however long it takes to make the repairs). It follows that unavailability can be kept low by more frequent testing. The frequency of testing must, however, be balanced against:

6. CANDU stations have two different types of automatic shutdown system. What principle does this illustrate?

7. How does the frequency of testing affect unavailability of a poised system?

8. State at least two reasons why frequency of testing of safety systems must be limited.

9. A **heat exchanger requires cooling flow at all times**. A valve upstream of the heat exchanger regulates cooling flow. What would be the fail safe position of that valve? Open or closed?

## DEFENCE IN DEPTH

There are different ways of achieving the golden rule (**CONTROL, COOL AND CONTAIN**). Many of these have been incorporated into an important concept known as **Defence in Depth**. This underlies the whole process of design, construction, commissioning, and operation of an

Ontario Hydro CANDU reactor. One way of presenting this concept is the five part model illustrated in Figure 1.4.

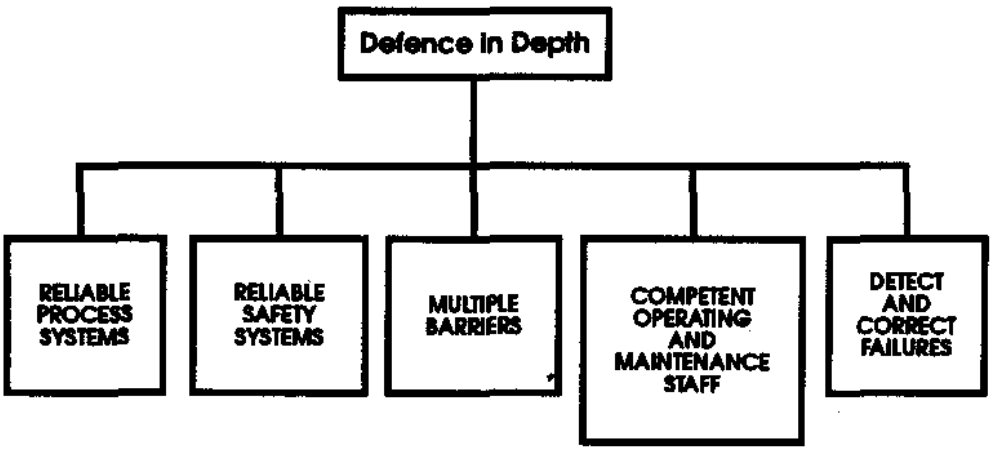


Figure 1.4
Defence in Depth Model

The Defence in Depth concept assumes the following:

- nuclear station design will have some flaws;
- equipment will occasionally fail;
- operating personnel will occasionally make mistakes.

The key is to ensure sufficient depth of defence that flaws, failures and mistakes can be accommodated without increasing the risk or consequences of an accident. If we look at each of the major blocks of the model in turn, we can see how this is accomplished.

1. **Reliable Process Systems**

   Process systems are those systems performing a continuous function in the normal operation of the plant. For example, the primary heat transport system is a process system that is continuously active in the removal of heat from the fuel. The reactor regulating system is a process system that is continuously active in the normal control of reactor power. Reliable process systems ensure that heat is produced and electricity generated while maintaining **control, cooling** and **containment.**

2. **Reliable Safety Systems**

   Safety systems are poised systems that operate only to compensate for the failure of process systems. They can do this by shutting

down the reactor to regain **control** (shutdown systems), by providing additional **cooling** to the fuel (emergency coolant injection system), and by **containing** radioactivity which has escaped from the fuel (containment system). Reliability in this context means that in the rare event these systems are called upon to act, they will be available to perform their intended function.

3. **Multiple Barriers**

The multiple barrier approach that has been built into station design is intended to prevent or impede the release of radioactivity from the fuel to the public. There are five passive barriers (refer to figure 1.5) that are continuously available:

- the uranium fuel is molded into **ceramic fuel** pellets which have a high melting point and lock in most of the fission products;
- the **fuel sheath** which is made of high integrity welded metal (zircaloy) and contains the ceramic fuel;
- the **heat transport system** which is constructed of high strength pressure tubes, piping and vessels and contains the fuel bundles;
- the **containment system** which provides a relatively leak tight envelope maintained slightly below atmospheric pressure. This partial vacuum encourages air to leak in instead of out thereby helping to prevent release of radioactivity that escapes from the heat transport system;
- the **exclusion zone** of at least one kilometre radius around the reactor that ensures any radioactive releases from the station are well diluted by the time they reach the boundary.

For radioactivity to reach the public from the fuel, it would have to breach each of the five barriers in succession. This provides a significant degree of protection to the general public.

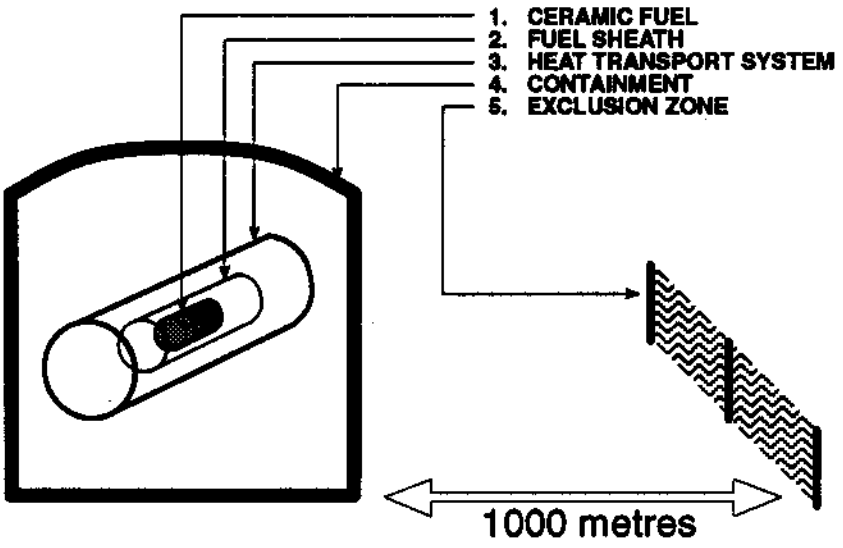


Figure 1.5
The Five Barriers

4. **Competent Operating and Maintenance Staff**

The safety systems are designed to operate automatically and the five passive barriers are always in place, but our Defence in Depth concept does not allow us to rely on equipment and systems to prevent accidents. It is important that our operating and maintenance staff are knowledgeable about system conditions, alert for any evidence that systems or equipment may be on the verge of failure, and act promptly to prevent or minimize the consequences of such failures. To achieve a high level of competence, the qualification criteria for each job family are clearly defined. Considerable effort goes into performance based training of staff to meet those criteria and maintain their qualification. This training starts on your first day and continues formally and on the job for the rest of your career.

5. **Detect and Correct Failures**

Adequate detection and correction of failures requires not just competent staff but also processes and procedures for the staff to carry out in a systematic fashion. For example, a routine testing programme for safety systems helps us meet the availability targets. An operational surveillance programme in conjunction with a planned preventive maintenance programme helps us to ensure that equipment and systems are monitored, inspected and repaired before they fail. Failures, when they do occur, are

thoroughly investigated and solutions applied through a rigorous change approval process.

A system has been put in place to allow any employee to report a deficiency quickly. This system will be discussed in the last section of this module.

## EFFECTIVENESS OF DEFENCE IN DEPTH

The effectiveness of the defence in depth concept is best illustrated by a survey of some of the highlights of Ontario Hydro's CANDU safety record:

- during more than 100 reactor years of operation, there has never been a fatality and there has not been an injury of any kind to a member of the public due to reactor operation;
- there has never been a release of radioactivity from a nuclear power plant that resulted in a measurable dose to a member of the public;
- the radioactivity risk criteria have been fully met at every station for every year of operation;
- emissions of radioactivity have been below the annual regulatory limits for all categories of radionuclide at every station for every year of operation;
- radioactivity emissions have been maintained at extremely low fractions of the annual regulatory limits, typically less than 1% of the limits.

## ASSIGNMENT

1. What are the three basic assumptions upon which the Defence in Depth concept is based?

   i)

   ii)

   iii)

2. Identify the five parts to the Defence in Depth model and briefly describe the intent of each:

   i)

ii)

iii)

iv)

v)

3. List in order the five major barriers designed to prevent the release of fission products from the fuel to the environment:

i)

ii)

iii)

iv)

v)

## DOCUMENTATION

Operation of a nuclear station (or heavy water plant) is governed by a licence issued by the federal nuclear regulator, the Atomic Energy Control Board (**AECB**). To support the application for a licence, the station designers prepare a **Safety Report** that describes the physical plant and

how it supports protection of the public, the environment and the employees. The safety report also analyzes how well the plant will cope with a number of accident scenarios specified by the AECB. The safety report is updated every three years. When granted, the **Station Operating Licence** is the contract between the station director and the AECB and defines the general boundaries within which the station will be operated.

Within the licence, one of the clauses dictates that operation of the station will be governed by a set of **Operating Policies and Principles (OP&P)**. The OP&Ps ensure safe station operation by defining limits on station operation. These limits are either stated qualitatively or spelled out with quantitative values. The OP&Ps embody good operating practices based on established reactor safety principles. For example, the OP&Ps define the requirement for a maintenance programme, periodic testing, and reactor power limits. Violation of an OP&P would place the plant in a state which has not been analyzed in the Safety Report, and which might therefore be unsafe. To operate in such a state could impair the capability of the plant to respond properly to accident conditions.

Subordinate to the OP&Ps, station **Operating Procedures**, which include **operating manuals** and **maintenance manuals**, define the precise details of station operation and maintenance. These procedures are rigorously prepared, verified and approved.

To provide some assurance that station operation remains within the bounds specified by the OP&Ps while enabling improvements to be made, each station has a **Change Control Process** in place to ensure that all planned deviations in plant operation or design are properly analysed and approved. On a day-to-day basis, the **Work Authorisation Process**[11] serves a similar purpose by enabling the Shift Superintendent to monitor work to ensure that it will not step outside the bounds of the OP&Ps. It also serves to protect workers doing the job.

The operating licence is not the only contract the station director has with regulatory agencies. The Ministry of the Environment grants **Certificates of Approval** that govern operation of non-nuclear facilities at our plants such as the Water Treatment Plants, or limit the temperature differential between the cooling water inlet and outlet at a generating station. These are contracts between the station director and the regulator (in this case

---

[11] The work authorisation process is a paperwork system administered through the work control desk in the control room. It helps to ensure that all work carried out in the station is monitored and controlled, and that the work is carried out within the rules of the **work protection code**. This will be dealt with more fully in your safety training.

the Government of Ontario) concerning conventional processes within the plant.

## ASSIGNMENT

1. What role do the Operating Licence and Certificates of Approval play?

2. Apart from the legal consequence, what is the danger of violating a limit defined in the OP&Ps?

3. How does the Safety Report support the Operating Licence?

- wear and tear on the system and components caused by testing;
- unavailability due to removing components from service for the duration of the test;
- the risk (by human error) of leaving the system in a degraded state after a test;
- the danger of activating the system during the testing process.

5. **Fail Safe**

A system or component is called fail safe if after failing it leaves the remainder of the system in a safer state. For example, train locomotives are equipped with a "deadman" brake. It must be depressed by the engineer to allow the locomotive to move. If the engineer falls over dead, his foot will come off the brake and the locomotive will come to a halt.

6. **Operational Surveillance**

Operational surveillance is a process of continuous monitoring and trending of process parameters and equipment with the intent of spotting potential problems before they become real problems. Thus corrective action can be taken before a major problem occurs. An example is vibration monitoring of rotating equipment. If unusual vibrations are detected, the equipment can be stopped and repaired before the vibration causes serious damage.

7. **Preventive Maintenance**

Reliability data on different types of equipment offers a means of predicting when failures are likely to occur. By planning replacement or maintenance before any appreciable deterioration occurs that can contribute to the predicted failure, it is possible to reduce the number of unscheduled outages and consequent loss of production. This sometimes has the appearance of throwing away good equipment, but the reliability statistics indicate that the equipment is likely to fail shortly and probably inconveniently (remember Murphy's Law).

8. **Predictive Maintenance**

The best form of preventive maintenance is predictive maintenance which is based on equipment condition. Maintenance or

replacement is only done when diagnostic test results (such as vibration monitoring) indicate equipment degradation.

## ASSIGNMENT

1. Fill in the blanks to complete the Golden Rule of Reactor Safety:

   There is a _____ risk to the _____ and the environment from reactor fuel, provided that at all times:

   - the reactor power is _____,
   - the fuel is _____,
   - the radioactivity is _____.

2. Fill in the blanks to provide the definition of reliability:

   The _____ that the device will _____ adequately for the period of _____ intended under the operating _____ encountered.

3. Fill in the blanks to provide the definition of availability:

   The _____ of _____ that a device is _____ to _____ if called upon to do so.

4. How does redundancy contribute to higher reliability for a system?

5. Provide an example of system independence.