9 Nuclear Safety

9.1 Introduction

There is no question that there is a real risk to the public from the radioactive fission products produced in nuclear power plant fuel. If plants are to be allowed to operate this risk must be extremely low. Managing the risk (keeping it low) is referred to as nuclear safety. Nuclear safety is the way the plant is designed, built, operated and maintained. It is the hardware, work processes, the administrative processes surrounding a nuclear plant. This section provides a very brief overview of the philosophy and practices in nuclear plant operation.

9.2 Units of Radiation Exposure

Large amounts of radiation present an extreme health hazard to exposed people. However, there is debate on the effects of low levels of radiation. In fact, we are exposed to low levels of radiation each and every day. Before we discuss these sources, we need to define the units of radiation exposure. The initial measurements of radiation were energy absorbed by a unit mass of living tissue. The unit was named Roentgen after one of the early experimenters with radioactive material. The units used for Roentgen is the rad.

The damage done to a humans is not only a function of the energy absorbed but also how localized the damage is. One joule of gamma energy is less damaging than one joule of energy delivered by an alpha source. The energy from the alpha source will be deposited in a local area of the body; the energy from the gamma will be distributed over a wider volume and will be less damaging. A second unit was developed to take into account not only the absorbed energy but also the type of radiation that caused the damage. This unit is the Roentgen-equivalent-man or rem. Rem is the standard for measuring radiation dose.

Another catch was the implementation of SI units. Nothing went unscathed and rads were replaced by grays, and rem by sieverts. The relationship is that grays are 100 times larger than rads and sieverts are 100 times larger than rem. It is all very confusing since rem were already too large to be practical so they were replaced with a larger even more useless unit. Practically, radiation doses in a plant are measured in millirem. If the official SI units are used the practical measurement are in microsieverts.

Dose is one of the major considerations in the basic design and construction of the plant. In order to get a license, a utility has to have a sound plant design and demonstrate that, during a year, the dose

received by someone living at the station fence will not receive a significant dose. In addition, it has to be shown that the probability of a failure that results in the maximum allowable dose to the person at the fence is very low. Everything that impacts on a release of radiation or the probability of a release of radiation is nuclear safety.

9.3 Radiation

The following introduces the concept of normal background radiation in our environment. Understanding background radiation is essential to a rational discussion of radiation hazards.

Background radiation is made up of a number of natural and man-made sources. Naturally, occurring radiation comes from radioactive elements, which have existed in the earth since its creation. All naturally occurring elements above 82 are radioactive as well as a few isotopes of elements with lower atomic numbers. In addition, the earth is subject to constant bombardment by cosmic radiation, which creates certain radionuclides in the atmosphere, such as tritium (hydrogen 3 -H^3) and carbon 14 (C^{14}). Man-made radiation results from nuclear weapons testing programs, the use of medical techniques which involve ionizing radiation, certain consumer items like luminous watches, television receivers, and video display terminals, and, of particular interest to us, nuclear power generation.

A by-product of the nuclear generation of electricity is large quantities of radioactive material contained within the reactors. Problems can occur if this radiation escapes into the environment. The largest source of the radioactivity and hence the greatest potential acute hazard is irradiated fuel; fuel in the reactor which contains radioactive elements from the fission process. How we prevent this acute hazard from becoming chronic is dealt with in the next section. Some chronic hazards are:

- the relatively large volume of low and medium level radioactive plant wastes such as process equipment, personal protective equipment, and clean-up materials, and

- low level radioactivity (mostly tritium) emitted from the plant on a more or less continuous basis as a normal consequence of operation.

Figure 9.1 gives the expected annual radiation dose to a member of the public from each of the sources listed above. Please be wary of these average numbers; they are averages over many varying circumstances. However, they do give some feel for the meaning of the numbers.

Sources of Radiation	Millirem/Year
Natural Radiation (Cosmic Rays, Potassium-40, Building Materials, radon, etc.)	202
Medical Exposures	110
Nuclear Weapons Test Fallout	2
Occupational	4
Consumer Products	2
Nuclear Power	0.3

Figure 9.1
Annual Individual Exposure to Background Radiation in Ontario
(Average for the Ontario Population)

As can be seen, the contribution of nuclear power to the radiation exposure of members of the public is extremely low. Exposure of Nuclear Energy Workers is more significant. The exposure limit set by the Canadian Nuclear Safety Commission (CNSC) for Nuclear Energy Workers is 5000 millirem/year. (For non-nuclear energy workers, the limit is 500 millirem/year.) This figure represents the amount of exposure a person can sustain year after year with no measurable effect. For comparison with actual exposures in and around our nuclear plants, see Figure 9.2.

Proximity to Station	Annual Radiation Dose above Background	Relative Value
Station Operating Staff	400 millirem/year	5000 millirem/year CNSC limit
Station Office Staff	20 millirem/year	The same as spending 4 months in Denver, Colorado.[1]
Person at Station Exclusion Fence	0.3 millirem/year	The same as a round-trip by air between Toronto and Vancouver.
Residential Area 1 kilometre from Station	0.1 millirem/year	The same as radon exposure from living 2 months in a brick building.

Figure 9.2
Typical Radiation Exposures in and Around Our Plants

Note that the typical dose for operating staff (including maintenance staff) in station stations is 400 millirem/year, considerably less than the legal limit. As the distance from the reactor increases, radiation normally falls off dramatically until at the Station Exclusion Fence, the typical potential exposure is 0.3 millirem/year.

In conclusion, the incremental increase from nuclear power over background radiation likely to be received by members of the public is very low. Medical risks at these low dosages cannot be accurately determined. In the worst case it is believed that the effect of radiation is directly proportional to the dose (e.g., half the dose, half the effect). However, there is evidence that this assumption overstates the actual risk. For example, people living in Denver, Colorado, where natural levels of radiation are higher, actually exhibit a lower incidence of cancer than those in other areas of the United States. This is not to suggest that low levels of radiation are beneficial, but merely to illustrate that the effects of low-level radiation are far from clear.

---

[1] **Background radiation increases at higher altitudes due to reduced shielding from the atmosphere against cosmic radiation.**

Even at the typical exposure of 400 millirem/year for operating staff, employees receive much less than the minimum dose considered dangerous to health. Even so, the Nuclear Business is always seeking ways of doing work to lower radiation exposure.

9.4 Conventional Safety

Nuclear generating stations have extensive conventional safety programs. It is not possible for people to work safely in one environment and not in another. In order to promote a safe work environment the utilities promotes safety in all aspects of the job and even off the job.

The first nuclear plants set safety targets that were twice as stringent as those in more conventional industrial plants. The safety targets have gotten better and better over the years so that now the targets are zero lost time accidents, not 1 lost time accident.

9.5 ALARA - A Philosophy towards Hazards

The radiation hazards associated with our facilities are very real. Control and containment methods are designed to prevent any harm to the public. The principle observed is to "play it safe" by reducing hazard levels As Low As Reasonably Achievable (ALARA). The practical application of ALARA has reduced the radiation dose received by those who work in the operating part of the plant by about a factor of 10 over the 40-50 years of plant operation in Canada.

9.6 Self-Checking

Most incidents have a number of causes but one of the causes is usually some type of human error. There is a major attempt by the industry to limit human errors. One way to keep incidents, from human error, low is through the technique of self-checking. This technique is designed to reduce the number of inappropriate actions that could lead to an incident by helping staff to focus consciously on the details of the task they are performing. A deliberate review of both an intended action and the expected response will often make it possible to identify a potential problem before it becomes real. Not all of our actions have the potential to cause serious problems.

9.7 Reactor Safety

There is an acute hazard posed by the radioactive materials contained within 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 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, AND
- 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.

9.8 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 a CANDU reactor. One way of presenting this concept is the five-part model illustrated in Figure 9.3.

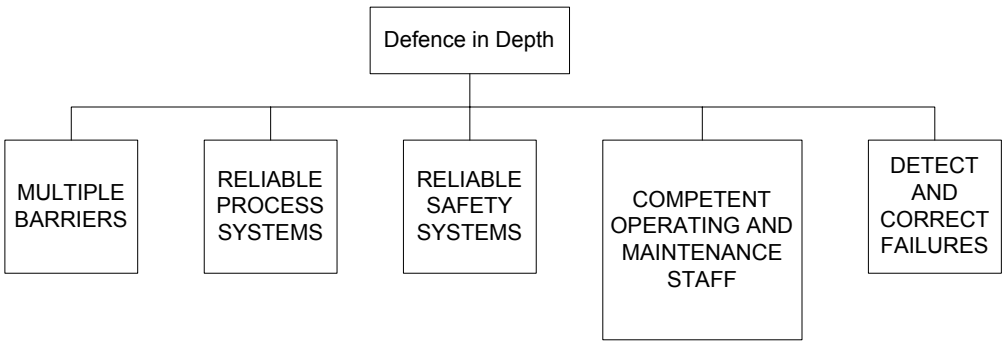

Figure 9.3
Defence in Depth Model

The Defence in Depth concept assumes the following:

1. Nuclear station design will have some flaws,

2. Equipment will occasionally fail, and

3. Operating personnel will occasionally make mistakes.

The key is to ensure sufficient depth of defense 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.

9.8.1 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 containing.

9.8.2 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.

9.8.3 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 9.4) continuously available:

1. The uranium fuel is molded into ceramic fuel pellets which have a high melting point and lock in most of the fission products,

2. The fuel sheath which is made of high integrity welded metal (zircaloy) and contains the ceramic fuel,

3. The heat transport system which is constructed of high strength pressure tubes, piping and vessels and contains the fuel bundles,

4. 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, and

5. 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 public.

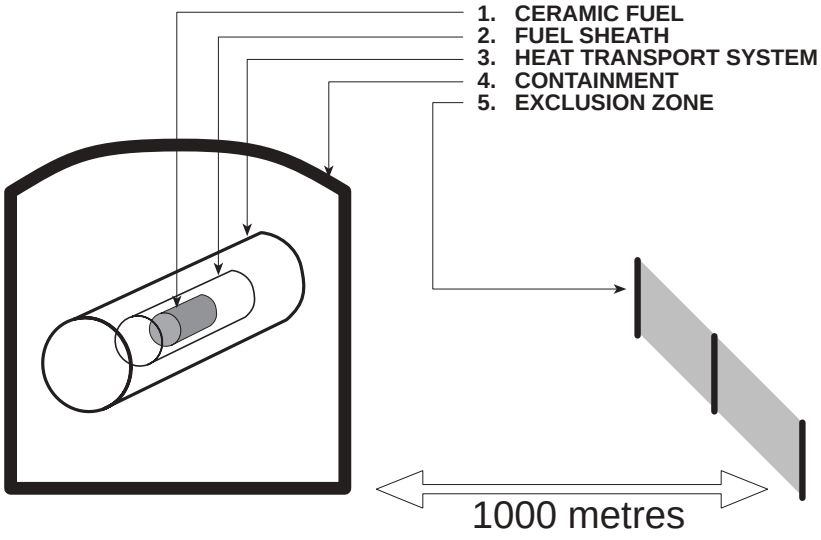

Figure 9.4
Physical barriers

9.8.4 Competent Operating and Maintenance Staff

The safety systems are designed to operate automatically and the five passive barriers are always in place, but the Defence in Depth concept does not allow reliance on equipment and systems to prevent accidents. It is important that 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.

9.8.5 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 program for safety systems helps meet the availability targets. An operational surveillance program in conjunction with a planned preventive maintenance program helps 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. Elaborate work control processes exist, allowing the quick reporting, prioritizing and repair of deficiencies.

9.9 Basic Reliability Concepts

Reliability is concerned with the overall operation of nuclear generating stations. In addition to trained and motivated staff, overall station reliability is a function of the reliability of systems and equipment. Reliability is critical piece of the Defence in Depth model and is therefore critical to the safe operation of our reactors. The following material introduces basic reliability concepts as they relate to CANDU equipment and systems.

9.9.1 Definitions

Reliability is defined as the probability that a device will work adequately for the period 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 is likely to fail. When dealing with poised systems, the concern is whether a system or component will be available when called upon to operate. A process system is a system that operates when the plant is producing power. A poised system is one that is sitting waiting to operate in the event of specific events. In your car the engine cooling system is a process system, the air bag is a poised system.

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).

9.9.2 Concepts

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

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 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 program 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 program on more than one computer. If one computer fails, another is immediately available to assume control.

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.

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 programs 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.

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:

- 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, and
- The danger of activating the system during the testing process.

Fail Safe Operation
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.

Operational Surveillance
Operational surveillance is a process of continual 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.

Preventive Maintenance
Reliability data on different types of equipment offers a means of estimating 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).

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.

9.10 Documentation

Operation of a nuclear station is governed by a licence issued by the federal nuclear regulator, the Canadian Nuclear Safety Commission (CNSC). 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 CNSC. The safety report is updated every three years. When granted, the Station Operating Licence is the contract between the utility and the CNSC 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 program, 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 analyzed and approved. On a day-to-day basis, the Work Authorization Process serves a similar purpose by enabling the control room staff 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 a utility has with regulatory agencies. A provincial government agency grants Certificates of Approval that govern operation of non-nuclear facilities at 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 utility and the regulator (in Ontario this is the Ministry of the Environment) concerning conventional processes within the plant.

9.11 Nuclear Station Radioactive Emissions

With respect to the Nuclear Business' obligation to control radioactive emissions from the nuclear stations, performance has consistently met the standards imposed by the CNSC. Typically, utilities control discharges to less than 1% of the regulatory limits set by the CNSC. Utilities monitor airborne emissions for tritium, iodine, noble gases, and particulates, and waterborne emissions for tritium and gross radioactivity.

The small amount of radioactivity released from plants is either to atmosphere or to the lake. Within the plant, a release to atmosphere is reduced significantly by dilution in the surrounding air. For the public, further dilution is provided by the exclusion zone (the last of the five barriers) around the stations. In any event, the amount and type of radioactivity that is released is carefully controlled and monitored. Typically, a utility’s internal emission target is 1% of the allowable emission for the radioactive substance.

In order to ensure that operating targets are achieved and maintained, an extensive program of environmental monitoring has been established. Samples are taken from fixed positions around nuclear sites at regular intervals. Measurements are taken of both the air and water at sampling sites. Samples are also taken of lake sediments, fish, fruit and vegetables. In addition to the monitoring carried out by a utility, both federal and provincial regulatory agencies carry out independent sampling as well.

9.12 The Role of Licenced Positions within the Nuclear Station

Nuclear stations are operated within the framework of the station operating licence granted by the CNSC. The CNSC is responsible for verifying that operation is carried out within the terms of the licence. Those terms require the following positions within the station organization to be approved or licensed by the CNSC:

- Shift Manager,
- Authorized Nuclear Operator.

To obtain authorization from the CNSC for these positions, individuals undergo a rigorous training and examination process. The process is monitored and audited by the CNSC. In fact, the CNSC monitors the training of all employees; the program for control room staff is the most extensive. Approval of some department managers usually requires previous experience as a Shift Manager and requires a formal interview with the CNSC. These requirements are outlined in the operating license.

The Shift Manager is the senior position on shift. This position has the ultimate responsibility for managing the station (both operation and maintenance) to ensure that the Station License, OP&Ps and other high level procedures are not violated. In the large multi-unit stations, there is a third licensed position, the Control Room Shift Supervisor. The Control Room Shift Supervisor reports to the Shift Manager and has the responsibility for supervising control room operations of all units. This includes monitoring operations and maintenance carried out in the station to ensure that they comply with the OP&Ps.

The Authorized Nuclear Operator (ANO) carries out operations according to approved procedures. The ANO exercises direct control over one unit in the station. A unit is a reactor, associated turbines, generator and all of the associated support systems. The ANO is responsible for carrying out panel operations, directing field operations and maintenance on the unit. The ANO authorizes most work in the

unit, but sometimes the approval of the shift manager is required as well. Work on special safety systems or reactivity devices (devices for controlling reactor power) would typically require this type of approval. This is a procedural barrier to prevent OP&P violations. The OP&Ps and operating procedures indicate where higher level of approval is needed.

The important feature of each of the above positions is that, in addition to normal supervisory responsibilities, they are directly licensed by the CNSC to provide assurance that station operation is carried out within the limits of the Operating Licence. As such, they are legally required to be intimately involved in the work carried out by most work groups within the station through the work approval process.

9.13 Assignment

1. Explain the reactor safety philosophy that is encompassed by the words control, cool and contain.

2. Explain the purpose of self-checking.

3. Define self-checking.

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

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

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

7. Explain the difference between reliable and available.

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

9. Provide an example of system independence.

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

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

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

13. 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?

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

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

16. What roles do the Operating Licence and Certificates of Approval play?

17. What are the four airborne and two waterborne emissions monitored at nuclear stations?

18. Why does the CNSC directly license several supervisory positions within the station.

19. How does the Control Room Shift Supervisor monitor work going on in the station to ensure that the operating license is being observed?