NOTES AND REFERENCES

Module 7

LICENSING PRINCIPLES AND SAFETY ASSUMPTIONS

OBJECTIVES

After completing this module, you will be able to:

	7.1	State the basic requirement placed by the AECB on applicants wishing to construct and operate a NPP in Canada.	⇔ Page 3
	7.2	Risk is a function of abnormal event frequency and consequences. Briefly describe how regulatory licensing documents translate this concept into design limits on system reliability and radioactive environmental releases.	⇔ *Pages 3, 6*
CRO	7.3	Define the following: a) single failure b) dual failure	⇔ *Page 4*
	7.4	State <u>two</u> nuclear safety advantages achieved by compliance with applicable codes and standards.	⇔ *Page 4*
CRO	7.5	Briefly explain the rationale for requiring two independent and diverse shutdown systems on reactors built after Pickering-A.	⇔ *Page 5*
CRO	7.6	State the basic objective of the Safety Analysis, and what two pieces of information must be derived for each design basis accident in order to achieve this objective.	⇔ *Page 8*
	7.7	State <u>three</u> siting factors that influence the Safety Analysis, and briefly explain the impact of each.	⇔ *Page 9*
CRO	7.8	Define what is meant by the *safe operating envelope*, explain why a NPP must be operated consistent with the assumptions underlying the Safety Analysis, and give <u>three</u> examples of such assumptions.	⇔ *Page 11*

NOTES AND REFERENCES

Page 12 ⇔ **CRO** 7.9 Explain briefly how violating each of the following assumptions could invalidate the Safety Analysis:

a) PHT isotopic greater than specified lower limit;

b) PHT I-131 inventory less than specified upper limit;

c) Excess reactivity due to fueling ahead below specified limit;

d) Unanalyzed abnormal reactivity device configurations prohibited.

Page 12 ⇔ **CRO** 7.10 List and give the rationale for any nine general conditions of the Power Reactor Operating License (PROL).

Page 12 ⇔ **CRO** 7.11 Given any of the generic conditions of the PROL discussed in the text, give a brief rationale for its inclusion.

THE ASSESSMENT OF PUBLIC RISK

When a Regulator defines the limits of public risk, it considers the frequency of various events versus their pubic dose consequences. The higher the dose consequences, the lower the tolerable frequency. If frequency is plotted versus consequences, some sort of line or curve is obtained, as shown schematically in Figure 7.1.

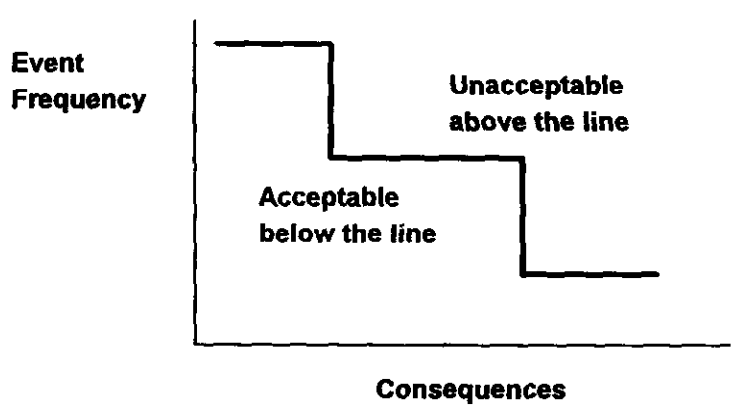

Figure 7.1: Schematic Representation of Limits on Public Risk

NOTES AND REFERENCES

The Siting Guide

In 1972, D.G. Hurst and F.C. Boyd of the AECB presented a paper to the Canadian Nuclear Society entitled, *Reactor Licensing and Safety Requirements*. This paper, which describes the AECB's expectations of an applicant wishing to construct and operate a NPP in Canada, came to be known as the *Siting Guide*. It requires the applicant to provide evidence that the chronic and acute radiological risks associated with the location, design, and operation of a proposed NPP are within licensing limits. All Canadian NPPs up to Darlington were licensed under the terms of the Siting Guide. Today's licensing requirements, although more sophisticated, still follow the same broad principles.

⇔ *Obj. 7.1*

The Siting Guide defines quantitatively what the AECB considered to be acceptable limits on public risk (dose) due to chronic and accidental releases. In the case of accidental releases, the basic principle is to limit both the frequency of occurrence and the consequences. This translates into limits on *serious process system failure* frequency, limits on safety system unavailability, and limits on public dose, as shown in Table 7.1.

Operating Condition	Maximum Frequency	Individual Dose Limits	Population Dose Limits
Normal operation	Continuous	0.5 rem/y whole body 3 rem/y to thyroid*	10^4 man-rem/y 10^4 thyroid-rem/y
Serious process system failure (single failure)	1 per 3 years		
Serious process system failure coincident with a failure of a special safety system (dual failure)	1 per1,000 years	25 rem whole body; 250 rem to thyroid**	10^6 man-rem 10^6 thyroid-rem

*For other organs, use one-tenth ICRP annual occupational dose limit
**For other organs, use five times ICRP annual occupational dose limit

Table 7.1: Siting Guide Limits on Public Risk

⇔ *Obj. 7.2*

NOTES AND REFERENCES

The Siting Guide defined a ***serious process system failure*** as a failure of a normally operating system that would cause fuel failures in the absence of special safety system action. Serious process system failures either *in*crease heat production above the capability of the in-service heat sinks (loss of regulation from high or low power), or *de*crease the heat removal capability of the in-service heat sinks (loss of class IV; loss of coolant; reduced HT coolant flow, steam flow or feed water flow; sustained loss of shutdown heat sink).

Obj. 7.3 ⇔

A serious process failure for which the special safety systems operate correctly to mitigate the consequences, is called a ***single failure***. A serious process failure coincident with the failure of one needed special safety system is called a ***dual failure***. The Siting Guide limits of Table 7.1 effectively define two regions of acceptable public risk on the frequency-consequence diagram of Figure 7.1—one for single failures, and one for dual failures. The consequences of a single failure are insignificant, in the sense that they are no greater than the consequences for normal operation. The consequences of a dual failure, even to the most exposed member of the public, are limited to non injurious doses of radiation.

The Siting Guide also requires, either explicitly or implicitly, the following:

- Each special safety system must be testable, and shall be tested at a frequency sufficient to demonstrate an unavailability $\leq 10^{-3}$ years/year.

- Each special safety system must be *independent* of the other special safety systems, so that coincident failure of two special safety systems is not a credible event—ie, a failure in one cannot induce related failures in another. Similarly, the special safety systems must be independent of process systems (except for the *safety support systems*), so that process system failures cannot induce related unsafe failures in special safety systems—ie, so that single failures cannot escalate to dual failures simply because of interdependence between process and special safety systems. (Note that failures of safety support systems, such as class 2 power, typically cause a special safety system to fail safe.)

- Failure rates claimed in the Safety Analysis must be based on operating experience, not mere hypothetical estimates. (Note that monitoring equipment failure rates is important to nuclear safety, even in a mature plant with a well established failure rate data base, because failure rates could rise due to unforeseen aging and material degradation effects.)

Obj. 7.4 ⇔

- Systems shall be designed, constructed, commissioned, operated and maintained in accordance with applicable ASME, ANSI and CSA codes and standards. This will help the plant meet the licensing requirements on serious process failure rate and special safety system unavailability.

NOTES AND REFERENCES

- A life-cycle quality assurance program must be implemented per CSA standards, in order to maintain the quality of physical plant and operations at acceptable levels throughout the life of the station.

Regulatory Document R-10

⇔ *Obj. 7.5*

In the case of a plant with only one shutdown system, one possible dual failure is a serious process failure, such as a LORA or LOCA, coincident with a failure to shut down. Since consequence analysis of this type of dual failure is difficult to the point of being speculative, all reactors subsequent to Pickering-A were required to have two *independent* and *diverse* shutdown systems. This requirement was formalized in Regulatory Document R-10, *The Use of Two Shutdown Systems in Reactors.* While the failure of one SDS is a credible event, the coincident failure of two independent, diverse shutdown systems during a serious process failure is considered to be incredible. (If the chances are less than 1 in 1,000 that one SDS is unavailable, then the chances are less than 1 in 1,000,000 that two independent SDSs are simultaneously unavailable.)

R-10, legally applicable to reactors licensed after January 1, 1977, stipulates the following with respect to SDS1 and SDS2:

- Independence from process systems, and from each other—ie, a process failure cannot cause related unsafe failures in either SDS, nor can a failure in one SDS cause related failures in the other.
- Diversity—ie, different physical processes used by SDS1 and SDS 2 to achieve reactor shutdown
- Equal effectiveness—ie, either SDS must be capable of keeping public dose consequences within licensing limits for single and dual failures.
- Two diverse trip parameters on each SDS--ie, four trip signals available to trigger automatic shutdown for each design basis accident. For example, on loss of class IV power, SDS1 might trip on high HT coolant pressure and low coolant flow, whereas SDS2 might trip on high HT coolant pressure and low core differential pressure.

Note that the second trip parameter is <u>not</u> credited when calculating SDS predicted unavailability--ie, each SDS must meet the 10^{-3} unavailability licensing limit for <u>each</u> parameter. The dual diverse parameter requirement is there to protect against unforeseen common cause effects, including design and analysis errors, which might invalidate the credited trip protection on a given parameter. The R-10 dual parameter, dual system requirements on shutdown capability may seem like overkill, until one considers the consequences of not shutting down. Whereas some reactor designs have ***negative*** void coefficients which make them

NOTES AND REFERENCES

go sub-critical in the event of a LOCA, CANDU has a *positive* void coefficient which makes it vulnerable to a power excursion in the event of a large LOCA. Therefore, effective automatic shutdown protection is absolutely essential to prevent compounding the effects of a LOCA with those of a power excursion.

Consultative Document C-6

Darlington was the first station to be licensed on the basis of Consultative Document C-6, *Requirements for the Safety Analysis of CANDU Nuclear Power Plants*, an evolution of the Siting Guide. C-6 was first issued in 1980, and was revised in 1994. Although C-6 was not then, nor is it yet today, a formal regulatory requirement*), it was treated essentially as such during the Darlington licensing process.

* The AECB issues consultative documents for comment, and in some cases (eg, C-6) for "trial use", prior to releasing them in final form as Regulatory (binding) documents.

The C-6 limits on public risk for 5 classes of failures are shown in Table 7.2. Note that the public dose consequences of the C-6 class 2 and class 5 events, respectively, correspond closely to those of the Siting Guide's single and dual failures. Also, note the absence of C-6 population dose limits, as the C-6 individual dose limits automatically restrict population dose, even in high population areas, to less than the Siting Guide population dose limits. Whereas the Siting Guide defines two regions of acceptable public risk on the frequency-consequence diagram of Figure 7.1, C-6 defines five.

Event Class	Event Frequency (Occurrences per reactor-year)	Individual Dose Limit	
		Whole Body rem	Thyroid rem
1	$> 10^{-2}$	0.05	0.5
2	10^{-3} to 10^{-2}	0.5	5
3	10^{-4} to 10^{-3}	3	30
4	10^{-4} to 10^{-5}	10	100
5	$< 10^{-5}$	25	250

Obj. 7.2 ⇔

Table 7.2: C-6 Limits on Public Risk

A few typical event combinations listed in the Darlington Safety Report for each of the five event classes of C-6 are shown in Table 7.3. The reader is referred to the Darlington Safety Report for a full list of class 1 to 5 analyzed event combinations, together with the tabulated public dose estimates from the Darlington safety analysis.

NOTES AND REFERENCES

Event Class	Example Abnormal Event Combinations
1	• Dual digital control computer stall • Loss of reactor power regulation • Loss of class 4 power
2	• HT feed valves fail open, bleed valves closed • End fitting failure • Loss of unit instrument air (pipe rupture)
3	• Severe flow blockage in one channel (< 53% nominal flow) • Large LOCA (> 1000 kg/s) • Loss of class 4 plus class 3 power
4	• Single SG tube failure plus failure of shutdown cooling • Loss of moderator inventory + failure of shutdown cooling • Feed water line failure downstream of last check valve
5	• End fitting failure plus seals in one air lock deflated • pressure tube/calandria tube failure plus failure of ECIS • Design basis earthquake

Table 7.3: Examples of Class 1 to 5 Abnormal Event Combinations

Other Regulatory Documents*)

* Authorization candidates are not accountable for this information.

The regulatory documents R-77, R-7, R-8 and R-9, are primarily of interest to special safety system Designers, but are mentioned here in passing. R-99 governs station documentation on regulatory reporting requirements. These documents expand on the basic requirements given in the Siting Guide and C-6.

R-77: ***Regulatory Policy Statement, Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems***

R-77 gives more detailed guidance on the effectiveness of both SDSs in providing overpressure protection for the PHTS.

R-7, 8 and 9: ***Regulatory Policy Statements on Requirements for Containment, Shutdown and Emergency Coolant Injection Systems, respectively***

NOTES AND REFERENCES

These documents mandate internationally accepted industry practices regarding design and performance requirements—eg, environmental qualification, availability, separation and independence, status monitoring, codes and standards, and seismic qualification. They also provide guidance on operation and testing of special safety systems.

R-99: ***Reporting Requirements for Operating Nuclear Power Facilities***

R-99, which became effective January 1, 1995, requires Utilities operating NPPs to submit various types of oral and written reports to the AECB. R-99 prescribes the frequency of routine reports on station operation, and the time periods within which abnormal events must be reported. See Module 18 for a brief description of the R-99 requirements.

The Safety Analysis

The Utility alone, not the Regulator, is responsible to demonstrate the safety of a NPP. This obligation begins with the design phase, before the plant is constructed, and continues until the plant is decommissioned, and is in no way diluted by the separate activities of the various agents involved in the design, manufacture, construction, commissioning, operation and decommissioning phases. Both the Siting Guide and C-6 require a Utility wishing to construct and operate a NPP in Canada to submit a Safety Analysis in support of its application. When satisfied, the AECB approves the application and grants a construction license. The license to operate is issued separately, late in the commissioning process.

Obj. 7.6 ⇔

The basic objective of the Safety Analysis is to demonstrate that the public is adequately protected from the radiological hazards of both normal operation and abnormal operating events. Thus for all credible abnormal events, the applicant must demonstrate to the AECB that the following are within licensing limits*):

1. the frequency of occurrence, and
2. the public dose consequences.

* Hereafter, the generic term, "licensing limits", refers to either Siting Guide or C-6 requirements, whichever apply, as well as any other applicable regulatory limits.

The Safety Report tabulates the public dose consequences for both normal operation and credible abnormal events. The range of abnormal events chosen is not meant to include every conceivable accident—eg, a direct hit by a large meteoroid, but includes a complete range of credible events and event combinations. Those abnormal events and event combinations included in the Safety Analysis are called *design basis accidents.* The set of design basis accidents is derived by first identifying those systems which contain significant quantities of radioactive material, then determining the failure modes (initiating events) by which unplanned releases could occur. These initiating events are then considered

NOTES AND REFERENCES

in combination with failures of safety and safety support systems, to confirm that licensing limits on public dose are not violated.

⇔ *Obj. 7.7*

The Safety Report also describes the plant design, and discusses siting factors which impact the public dose resulting from both chronic and acute releases of radioactive material from the plant. Such siting factors include the local population distribution, local land use, and local meteorological data. The denser the local population, the higher the population dose resulting from chronic emissions, and from an acute release where the wind is blowing towards the population center.

Local land use impacts public dose because of the propensity of some radionuclides to concentrate in the food chain. For example, iodine and strontium radionuclides ingested by grazing dairy herds find their way into the milk. Humans consuming the milk then further concentrate these radionuclides in certain body organs, such as the thyroid or bones. Thus the public dose per curie of mixed fission products released into the atmosphere depends on the presence of dairy farms in the vicinity of the plant.

The dispersion of a radioactive atmospheric release is affected by wind speed and direction, and by precipitation (rain or snow fall). The higher the wind speed, the greater the dispersion, and the smaller the uptake by any individual down wind. The greater the tendency for local winds to blow in a certain sector of the wind rose, the greater the public dose in that sector, due to chronic emissions. The greater the local precipitation rate, the more atmospheric emissions tend to get scrubbed out of the atmosphere and deposited near the station. Therefore, wind speed and direction, and the pattern of precipitation impact the public dose received from both chronic and acute emissions.

Analysis of the site seismic stability determines the magnitude of the *design basis earthquake*, ie, the magnitude of earthquake that the plant must be designed to withstand. This in turn impacts the seismic design requirements on the reactor assembly and various safety related systems.

Safety Analysis tools include Safety Design Matrices and Probabilistic Risk Analyses, discussed below as background information only. Candidates are not accountable for reproducing these details.

Safety Design Matrices*)

* Authorization candidates are not accountable for this information.

Safety Design Matrices (SDMs) are an early version of Probabilitistic Risk Assessments (also known as Probabilitistic Safety Evaluations or Probabilitistic Safety Assessments). They were developed in the late 1970's in recognition of various deficiencies in the Siting Guide approach, including the following:

NOTES AND REFERENCES

- Failure to recognize the great variation in rates of occurrence and consequences of different process failures. For example, the Siting Guide treats large LOCAs (probability ~ 10^{-4}) the same as losses of regulation (probability ~ 10^{-2}).

- Inadequate treatment of safety support systems, whose failure could result in common cause (cross-link) failures of process and special safety systems.

- Failure to address the need for continuing operation of safety systems after an accident.

- Failure to address credible common cause events, such as steam and feed line failures, earthquakes, floods, and aircraft crashes.

The SDMs addressed these concerns by looking at an expanded range of initiating events, including failures of safety support systems, and by analyzing multiple failure accident sequences using event trees. SDMs were prepared for each serious process failure (design basis accident) considered in the original design—eg, large LOCA, small LOCA, loss of class IV, loss of moderator, and so on. Both equipment failures and human errors were considered. System interactions were treated by inspection--reviewers with detailed knowledge of the plant reviewed the event sequences to identify any potential interactions.

SDMs were prepared as part of the design process for the Bruce B, Pickering B, and CANDU 600 plants. Each SDM starts from an initiating event of known or assumed frequency, and branches to various chronological sequences of events, depending on which of the mitigating systems operate or fail to operate. At each branch point of the event tree, the probability that a mitigating action fails is multiplied by the event combination frequency to that point in time. The process is continued until either the reactor has reached a safe, stable state, or until the event combination frequency reaches the incredible range ($< 10^{-7}$ per year).

For example, one actual SDM for a pressure tube rupture as the initiating event, included branches for each of the following mitigating systems: containment, shutdown, HTS, ECIS, electrical power, the secondary side, service water and instrument air. Under the ECIS branch, the probability that, within 30 minutes of the rupture, ECIS initiating logic fails, the injection valves fail to open, or the HPECI equipment fails to deliver flow, is multiplied by the initiating event frequency to get an event combination frequency for loss of HPECI following a pressure tube rupture. This frequency is then multiplied by the probability that the moderator fails to act as a heat sink. Since this latter result is $< 10^{-7}$, a loss of moderator heat sink in combination with the earlier failures is considered incredible, and the branch is terminated.

NOTES AND REFERENCES

Probabilistic Risk Assessments*)

* Authorization candidates are not accountable for this information

While the SDMs represented a considerable advance over earlier risk assessment techniques, by the mid 1980's, still more sophisticated techniques called probabilistic risk assessments (PRAs) were developed. State-of-the-art techniques used in PRAs to address some of the residual shortcomings of the SDMs, included the following:

- a more comprehensive search for credible accident initiating events
- an improved human reliability model
- improved communication between the analysts, designers and operators to ensure the validity of assumptions in the analysis.

Probability risk assessments (PRAs) completed to date are the Darlington Probabilistic Safety Evaluation (DPSE, pronounced *dip-see*), and the Pickering A Risk Assessment (PARA). When PRAs are eventually completed for Pickering B and Bruce B stations, they will supersede the SDMs for these stations.

PRAs are used to quantify both public and economic risk due to station operation. Accidents are categorized according to postulated severity of fuel damage, then the sum total frequency of occurrence for each category is calculated. The public risk due to each of a number of ex-plant release categories is calculated by multiplying the total frequency of accidents contributing to that release category times the public dose consequences for that release category. The total risk for one reactor unit is the sum of the risks for all ex-plant release categories. The total risk for a 4-unit station is simply 4 times that of one unit. For example, the estimated total public risk for Darlington was calculated as 0.9 mrem/y for an individual and 7 person rem/y for the population within 100 km. For comparison, the risks due to normal operation are typically < 5 mrem/y for an individual and < 1 person rem/y for the population, ie, < 1% of AECB limits.

The economic risk is determined by summing over all fuel damage categories, the product of the category's frequency of occurrence times its costs of repairs and replacement power. For example, the total economic risk for Darlington was estimated at 10 million dollars per reactor year, a small fraction of annual operating costs.

Safe Operating Envelope

⇔ *Obj. 7.8*

Assumptions made in the safety analysis about how the plant will be operated are typically captured in the Operating Policies and Procedures. These assumptions collectively define what is called the *safe operating envelope*. Authorized staff must understand that the **Safety Analysis is valid only within a specified range**

NOTES AND REFERENCES

of analyzed plant operating states, ie, within the *safe operating envelope*. To operate in an unanalyzed state, outside of the safe operating envelope, is assumed to be unsafe. The Shift Supervisor and CRO must ensure that plant operation remains within the safe operating envelope, by adhering rigorously to OP&Ps, and by following operating instructions.

Obj. 7.9 ⇔ Some examples of safety analysis assumptions which define the *safe operating envelope* are listed below:

1. That the PHT coolant isotopic will be kept above a specified lower limit, in order to limit the core void coefficient for loss of coolant accidents.

2. That the PHT I-131 inventory will be kept below a specified upper limit with the reactor at power, so that the public thyroid dose limits will not be exceeded in the event of a LOCA outside of the containment boundary, or coincident with failure of the containment boundary.

3. That excess core reactivity achieved by fueling ahead will be kept below a specified limit. Otherwise, SDS1 protection against an in-core LOCA could become ineffective. The greater the excess reactivity in the fuel, the greater the required poison concentration in the moderator to counteract this excess reactivity, the greater the sudden insertion of positive reactivity by HT coolant displacing moderator during an in-core LOCA, and the greater the required rate of insertion of negative reactivity by SDS1 to prevent fuel damage caused by a power excursion.

4. That reactivity device configurations will be limited to those analyzed and specified as being permissible, since unanalyzed configurations could result in inadequate shutdown protection.

Obj. 7.10 ⇔

The Power Reactor Operating License

The *Power Reactor Operating License (PROL)*, more commonly called the *Reactor Operating License*, the *Operating License*, or simply the *License*, is a contract between the Utility and the AECB describing how the station will be

Obj. 7.11 ⇔ operated. The following are typically written into the PROL as mandatory generic conditions under which the operating license is issued:

1. ***Compliance with OP&Ps***—This ensures

   - continual operation within the assumptions of the safety analysis, ie, within the operating envelope analyzed to be safe,

   - key operating staff observe the limits of their authority, so as to preserve adequate defense in depth, and

NOTES AND REFERENCES

- use of certain good operating practices based on industry operating experience and nuclear safety principles.

OP&Ps are drawn up by the Utility and approved by the AECB prior to use.

2 ***Physically secure access to fissionable substances, and mandatory International Atomic Energy Agency (IAEA) inspections***—International security depends on strict control of fissionable substances which could be used to manufacture nuclear weapons. IAEA inspection of inventory and handling of fissionable substances is carried out pursuant to the **Nuclear Non Proliferation Treaty**.

3 ***Designated key positions to be AECB approved***—The AECB can thus assure itself that position holders are sufficiently knowledgeable, experienced and committed to ensure safe plant operations.

4 ***Maintain minimum complement on site at all times***—This ensures sufficient manpower to operate and maintain units safely under normal operating conditions, and to respond effectively to an emergency per Abnormal Incidents Manual (AIM) and radiation emergency procedures.

5. ***Significant amendments to radiation emergency procedures require AECB approval***—The Regulator reserves the right to review and approve proposed changes to these procedures, which are critical to public safety under accident conditions, For example these procedures cover the initial notifications of civil authorities, projection of public dose, protective action recommendations, and off-site surveys.

6. ***Bundle/channel/reactor thermal power limits***—Compliance ensures an adequate margin of safety to fuel failures due to overrating fuel.

7. ***SDS trip set points (TSPs) to remain at approved values***—Adequate trip coverage is a major feature of the safe operating envelope, and TSP changes must be justified by safety analysis.

8. ***Radioactive emissions to be monitored and controlled***—These emissions directly impact public and environmental nuclear safety. The Utility must demonstrate that public dose remains within licensing limits.

9. ***Compliance with all Provincial legislation***—This covers off areas of public safety under Provincial jurisdiction—eg, pressure boundary codes and standards (MCCR), emergency response (MOSG), and chemical spills (MOEE).

10. ***AECB to approve any use of Exclusion Zone land***—The AECB can thus assure itself that the nuclear safety risks associated with Exclusion Zone land

NOTES AND REFERENCES

use proposals are acceptable, and that provisions are made to notify occupants promptly of any required protective actions in the event of an accident.

11. ***Maintenance standard to assure continued integrity of analyzed state***— Integrity of the safe operating envelope is a basic condition under which the PROL is granted. Any deterioration of system reliability below that assumed in the safety report results in unacceptable public risk.

12. ***Actions requested by AECB to be completed expeditiously***—The AECB must have the authority to demand timely response to its concerns in order to regulate effectively, to protect the public.

13. ***Mandatory testing to substantiate system reliability claimed in Safety Report***—Otherwise the safety analysis is invalidated, and licensing limits might be violated.

14. ***AECB approval required to change SSSs from documented, analyzed state***—The SSSs are critically important to public safety. The impact of any changes must be assessed, possibly by repeating parts of the safety analysis.

15. ***AECB approval required for changes potentially resulting in hazards differing in nature, probability or magnitude from those described in the Safety Report***—The licensee cannot unilaterally change the case on which the operating license was granted.

16. ***Only AECB-approved fuel design permitted in reactor***—Irradiated fuel integrity is crucial to public safety under both normal and accident operating conditions. The AECB must be assured that the fuel design is sufficiently proven to meet stringent safety standards.

17. ***Mandatory reporting per Regulatory Document R-99, "Reporting Requirements for Operating Nuclear Power Facilities"*** — Reports on both normal operation and abnormal events mandated by R-99 permit the AECB to monitor the quality of nuclear safety management, including the implementation of appropriate corrective action as required.

18. ***Mandatory records of operation, maintenance, test/inspection results, and significant events***—Such reports permit the AECB to audit and identify deteriorating trends in the quality of station operations, including equipment reliability, and management and work practices.

19. ***Mandatory register of all licensing documentation to be kept by Utility***— The AECB can thus assure itself that the Utility is paying adequate attention to maintaining important reactor safety documentation, as this register is reviewed prior to each license renewal.

NOTES AND REFERENCES

SUMMARY OF KEY CONCEPTS

- Public risk is a function of event frequency and consequences. The more frequent an event, the lower the tolerable consequences, and conversely.

- Licensing documents (Siting Guide and C-6) require a Utility to submit a safety analysis showing evidence that the radiological risks associated with the location, design, and operation of a proposed nuclear power plant are acceptable, as a prerequisite to obtaining a construction license.

- Licensing limits on public risk translate into limits on serious process system failure frequency, safety system unavailability, and public dose.

- Two nuclear safety advantages of compliance with applicable codes and standards are:

    1. to obtain sufficient equipment reliability to meet licensing reliability requirements on process and special safety systems

    2. to ensure that the quality designed into the plant remains at an acceptable level throughout the plant's life cycle.

- R-10 requires that CANDU plants be fitted with two independent and diverse shutdown systems, so that failure to shut down on a serious process failure is incredible.

- The basic objective of the Safety Analysis is to demonstrate that the public is adequately protected from the effects of both normal operation and abnormal operating events. Thus for all design basis accidents, the applicant must demonstrate to the AECB that both event frequency and public dose consequences are within licensing limits:

- The Safety Report describes siting factors, including population distribution, land use, meteorological data, and seismic stability. These factors affect the public dose resulting from chronic and accidental releases.

- Four examples of Safety Analysis assumptions which define the safe operating envelope were discussed.

- Authorized staff are responsible to ensure that the plant is operated within the safe operating envelope defined by the assumptions in the Safety Analysis, as specified in OP&Ps and operating instructions, since operation outside this envelope has not been shown to be safe.

NOTES AND REFERENCES

- 19 typical generic conditions of a CANDU reactor operating license were given together with rationale

- The AECB authorizes some key positions to provide confidence that the incumbents are sufficiently knowledgeable, experienced, and committed to ensure safe operation.

- A minimum shift complement must always be on site to provide adequate capability to maintain safe plant operation, and to perform emergency actions credited in the Safety Analysis.

ASSIGNMENT

1. Carefully prepare detailed answers to Module 7 learning objectives.

2. Identify six positions which must be authorized by the AECB, and state why such authorization is required.

3. Briefly describe the purpose and content of the following documents, and identify any interrelationships between them:

   a) Siting guide or C-6, whichever applies to your station

   b) R-10

   c) safety analysis

   d) safety report

   e) power reactor operating license

4. Briefly explain why a station must be operated within the assumptions of the safety analysis, identify the individual by position who must ensure that this is done, and state a specific responsibility of this individual with respect to safety system testing.

5. State three parameters or device configurations which are constrained by the safety analysis, and briefly explain how they could invalidate that analysis.

6. Sketch the frequency versus consequences diagrams, using log-log axes, for the following cases:

   a) the single and dual failures of the Siting Guide

   b) the five classes of abnormal events per C-6

7. Explain why it is just as important, or more so, to monitor equipment failure rates in the last decade, as in the first decade of a NPP's operation.