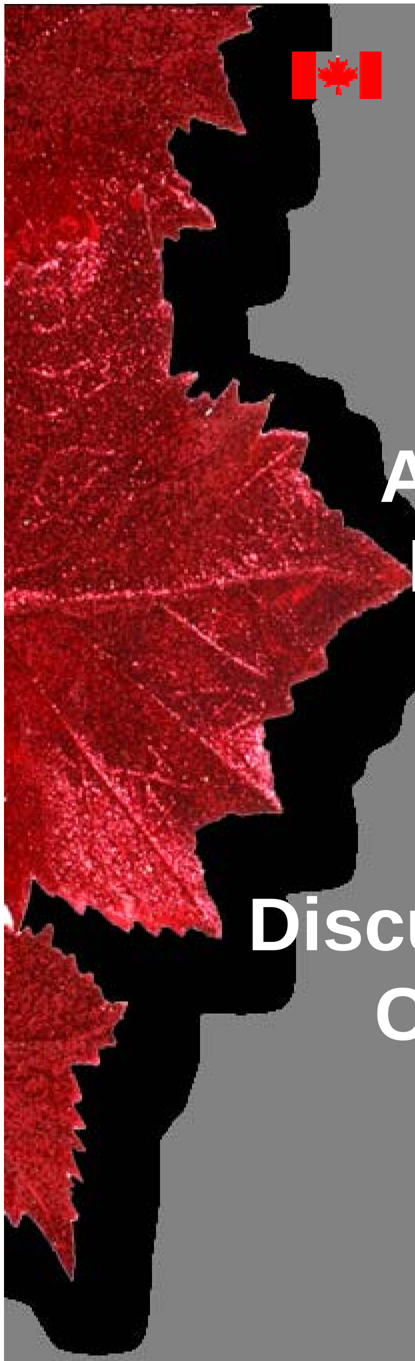
Canadian Nuclear
Safety Commission

Commission canadienne
de sûreté nucléaire



Pre-Consultation for RD-308 and RD-367

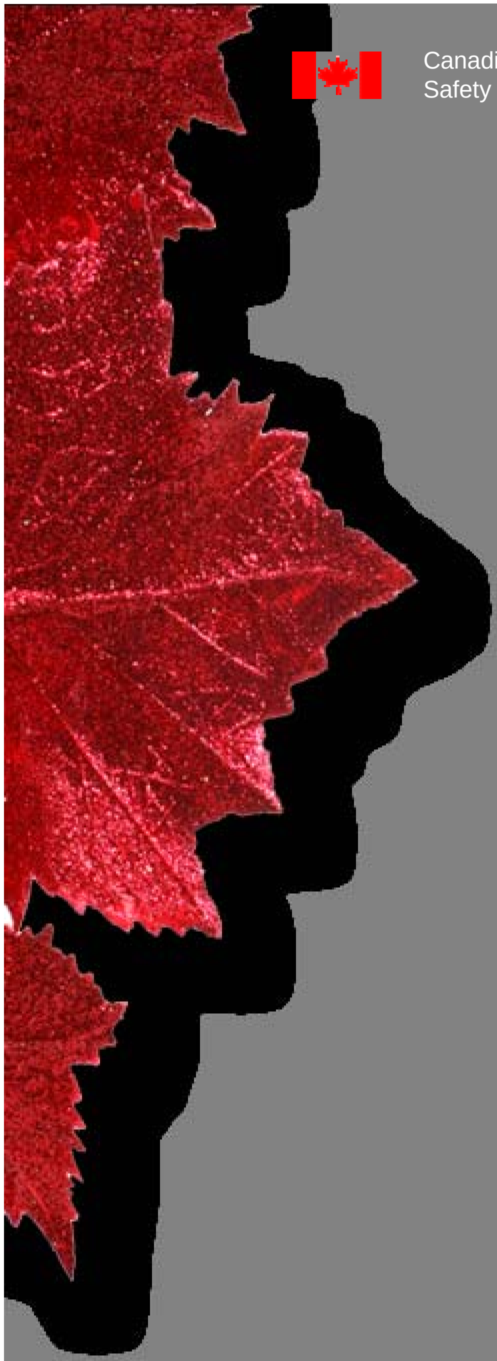
April 28, 2010 Public Webinar on Design and Safety Analysis for "Small Reactors":

SECTION 2

Discussion of Key Concepts that will be Contained in RD-308 and RD-367

Presenter: C. Harwood / M. de Vos

EDOCS 3517069



First Key Concept:

What is a “Graded Approach”?

Graded Approach (1)

- A risk-informed approach that, without compromising safety, allows safety requirements to be implemented in such a way that the level of design, analysis, and documentation are commensurate with the potential hazards posed by the facility.

- The applicant applies the graded approach in their safety case

Graded Approach (2)

This is not a new concept:

CNSC staff has always practised a graded approach, consistent with international practice, in the licensing of small reactor facilities

Graded Approach – Key Elements

- Reactor power
- The inventory of radioactive material in the core
- Inherent safety characteristics
- Passive safety features
- Other design features such as engineered safety systems
- The utilization of the reactor
- Proven design (knowledge and experience)

Graded Approach – Examples

Example 1: Core Cooling

- The design of any nuclear facility must provide for key safety functions such as core cooling during all possible events including design basis accidents – the requirement for such safety functions is not gradable
- However a graded approach permits core cooling to be achieved through a variety of means
- Depending on the type of reactor design different type of systems may be appropriate
  - A forced convection cooling system
  - Natural convection cooling
  - Emergency core cooling system

Graded Approach – Examples

Example 2: Confinement

- The extent of the confinement needed depends on the key elements discussed two slides earlier. The confinement design could vary from a simple reactor building to a Nuclear Power Plant like containment.

- To achieve the basic function of confinement, the means of confinement may require the following features:
    - Control the pressure and temperature;
    - Isolation of the confinement envelope;
    - Leak-tightness of the confinement envelope;
    - Control of combustible sources;
    - Reduction of the concentration of free radioactive material in the confinement envelope; and
    - Radiation shielding.

? ?

? ?

Question and Answers on the Graded Approach

(5 minutes)

? ?

Second Key Concept:

Safety Objectives, Dose Acceptance Criteria and Safety Goals

I. Safety objectives for Small Reactors

Regardless of the size of a reactor, there are three safety objectives:

1 **General Nuclear Safety Objective:**

- To protect **individuals, society and the environment** from harm by establishing and maintaining in nuclear installations effective defenses against radiological hazards*

** Article 1 of Convention of Nuclear Safety which Canada signed in 1994*

Safety objectives, Continued

This general objective is supported by :

2 Radiation Protection Objective:

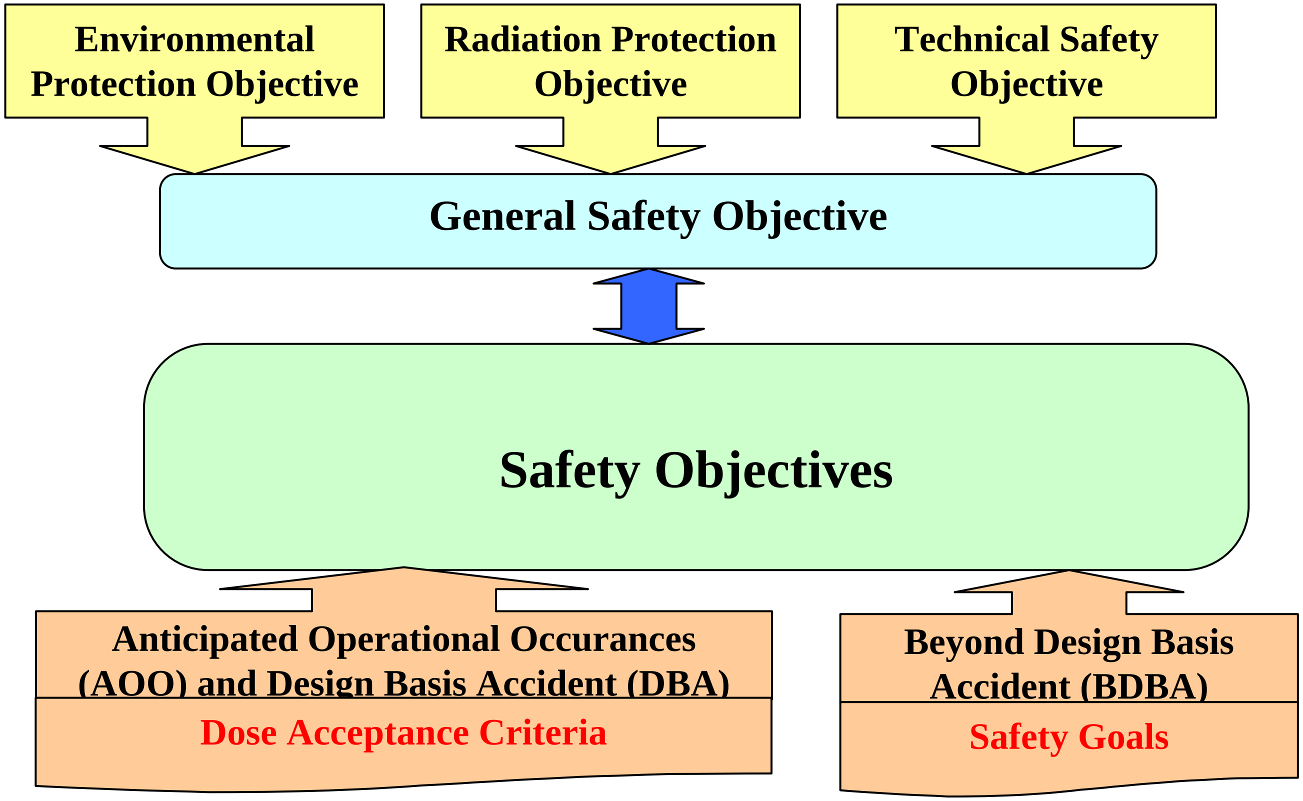
- Ensure that radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and As Low As Reasonably Achievable (ALARA), and
- Ensure mitigation of the radiological consequences of any accidents.

Safety objectives, Continued

3 Technical Safety Objective:

- Take all reasonably practicable measures to prevent accidents in nuclear installations and
- Mitigate their consequences should they occur;
- Ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and
- Ensure that the likelihood of accidents with serious radiological consequences is extremely low*.

*: This is where Probabilistic Safety Assessment fits in



Environmental Protection Objective

Radiation Protection Objective

Technical Safety Objective

General Safety Objective

Safety Objectives

Anticipated Operational Occurances (AOO) and Design Basis Accident (DBA)

Dose Acceptance Criteria

Beyond Design Basis Accident (BDBA)

Safety Goals

What are AOOs and DBAs?

- An Anticipated Operational Occurrence (AOO) is defined as an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

- Design Basis Accidents (DBA) - Postulated events with frequencies at or higher than 1 accident per 100,000 reactor years (or 10^{-5} per year)

Dose Acceptance Criteria

- For Design Basis Accidents, dose must be kept to less than or equal to 20 millisievert.

- For Anticipated Operational Occurrences, dose must be kept to less than less than or equal to 0.5 millisievert.

- Dose limits are based on International Commission on Radiological Protection (ICRP) recommendations.

What are BDBAs?

- Beyond Design Basis Accidents (BDBA) are accident sequences that are possible but were not fully considered in the design process because they were judged to be too unlikely.

- They are generally defined as having frequencies less than 1 accident per 100,000 reactor years (or 10^{-5} per year).

For BDBAs, We Use Safety Goals

- Basis for setting Safety Goals: Section 3 of the *Nuclear Safety and Control Act* (NSCA): “the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment”

- The motivation for setting the Safety Goals is to avoid complex and costly computations; are not dependant on the reactor power and minimize uncertainties.

- This concept is already entrenched in RD-337 *Design For New Nuclear Power Plants*.

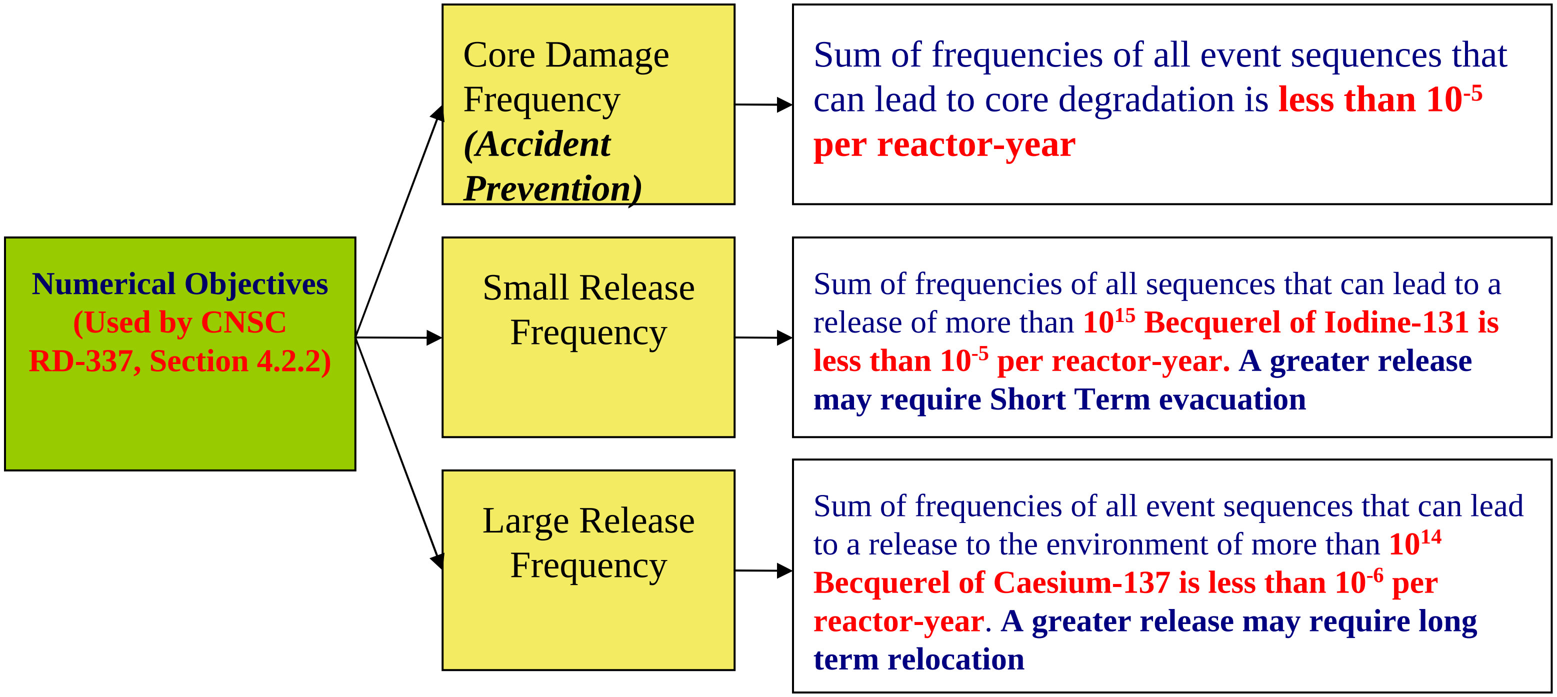
Safety Goals, Continued

- Quantitative safety goals establish frequency limits of events that may lead to:
  - Short Term Evacuation, or
  - Long Term Relocation

Predicted frequencies of Beyond Design Basis Events can depend on the individual site characteristics.

Safety Goals, Continued

Numerical objectives



Numerical Objectives
(Used by CNSC RD-337, Section 4.2.2)

Core Damage Frequency ***(Accident Prevention)***

Sum of frequencies of all event sequences that can lead to core degradation is **less than 10^{-5} per reactor-year**

Small Release Frequency

Sum of frequencies of all sequences that can lead to a release of more than **10^{15} Becquerel of Iodine-131 is less than 10^{-5} per reactor-year. A greater release may require Short Term evacuation**

Large Release Frequency

Sum of frequencies of all event sequences that can lead to a release to the environment of more than **10^{14} Becquerel of Caesium-137 is less than 10^{-6} per reactor-year**. **A greater release may require long term relocation**

Identifying Initiating Events

The applicant is expected to identify, consider, classify initiating events to be analyzed.

The process is expected to consider:

- systematic review of the design
- results of deterministic and probabilistic assessments
- regulatory requirements and guidance
- past licensing precedents
- operational experience
- engineering judgment

What is Deterministic Safety Analysis?

An analysis of facility responses to an event, performed using predetermined rules and assumptions

- e.g., those concerning the initial facility operational state, availability and performance of the facility systems and operator actions

Deterministic analysis can use either conservative or best estimate methods.

What is a Probabilistic Safety Assessment (PSA)?

A systematic and comprehensive methodology to evaluate risks to safety associated with a complex engineered technological entity

How do Deterministic Safety Analysis and PSA Work together?

While deterministic analyses may be used to verify that acceptance criteria are met, probabilistic safety analyses may be used to determine the probability of damage for each barrier.

Probabilistic safety analysis is a suitable tool for evaluating the risk from low frequency sequences that may lead to barrier damage.

Deterministic analysis is used for events of higher frequency for which the acceptance criteria are set in terms of the damage allowed.

What is PSA Used For?

Probabilistic Safety Assessment usually answers three basic questions:

1. What can go wrong with the system being studied? (i.e. what are the initiating events that lead to adverse consequences?)
2. What and how severe are the adverse consequences that the system may be eventually subjected to as a result of the initiating event?
3. What is the likelihood of occurrence of the adverse consequences? (probabilities or frequencies)

PSA Applied to a Reactor Facility

The proponent reviews all the possible disturbances (so-called Initiating Events) in the facility such as:

- Equipment or component failures (Loss of coolant accidents, Loss of main or support systems) and,
- External events (Floods, Fire, Earthquakes, Tornadoes…)

The proponent confirms the plant responses to the disturbance have been analyzed to achieve the stable conditions:

- Controlled (usually shut down)
- Cooled (water flowing through the core and heat removed)
- Contained (containment isolated, pressure controlled)

How do the analyses link back to those Numerical Objectives?

The PSA results in a long list of credible event sequences, their probabilities and consequences

These are tested against requirements for:

- Core Damage Frequency
- Large Release Frequency
- Small Release Frequency

So How does this apply to Small Reactors?

- The CNSC has no plans to propose a quantified value of reactor power beyond which a PSA is required.
- Safety goals should always be met regardless of the power of the reactor
- The depth of a Probabilistic Safety Assessment (PSA) can be graded based on risk.

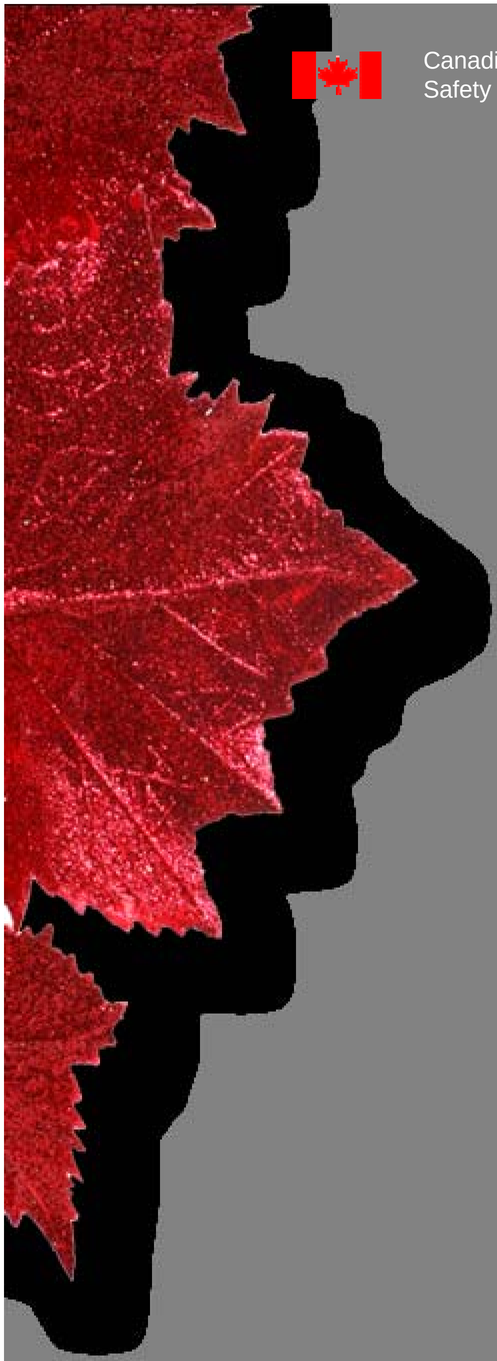
? ?

? ?

Question and Answers on the Safety Objectives etc.

(5 minutes)

? ?



Third Key Concept:

Engineering For Safety - Defence-in-Depth and Safety Characteristics

What is Defence in Depth?

Defence in depth in the design of a facility provides a series of levels of defence (inherent features, passive features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection should prevention fail.

Levels of Defence in Depth (1)

Level	Objective	Examples of How Objective is Achieved
1	**Prevent failures** of plant components, systems and structures, and prevent deviations from normal operation	• Conservative and high quality design of systems • Design equipment to operate in the environments it may encounter under failure conditions • Conduct regular testing to show systems will do what they were designed to do • Effective Maintenance Programs
2	**Detect deviations from normal operation** to prevent Anticipated Operational Occurrences from escalating into accident conditions, and return the facility to a normal state.	• Detection and control systems that can react in a timely manner to manage transients to the extent possible without human intervention. • Design systems to maximize use of inherent behaviours (e.g. ability to self-control pressure) • Operator training "know the behaviour of the unit"
3	**Minimize the consequences** of accidents.	• Use inherent safety features (systems that are stable and self-controlling) • Passive safety features (safety features that self-actuate without human action) • Apply active engineered safety systems • Apply well tested procedures to the event.

Levels of Defence in Depth (2)

Level	Objective	Examples of How Objective is Achieved
4	Ensure that radioactive **releases** caused by severe accidents **are kept as low as practicable.**	• Design multiple barriers to ensure if a severe accident occurs releases are kept in the plant, cooled and contained. Examples include: – Use of a “hardy” fuel that does not break down easily in events. – a robust confinement function – cooling sprays – filtered exhausts from the plant – exclusion zone around the plant • Severe accident management procedures
5	**Mitigate the radiological consequences** of potential releases of radioactive materials that may result from accident conditions.	• Emergency support centre • Plans for on-site and off-site emergency response.

Design and physical barriers

- The design should provide multiple barriers against radioactive release.

- To the extent practicable, the design prevents:
  1. Challenges to the integrity of physical barriers;
  2. Failure of a barrier when challenged; and
  3. Failure of a barrier as a consequence of failure of another barrier.

Applying defence-in-depth

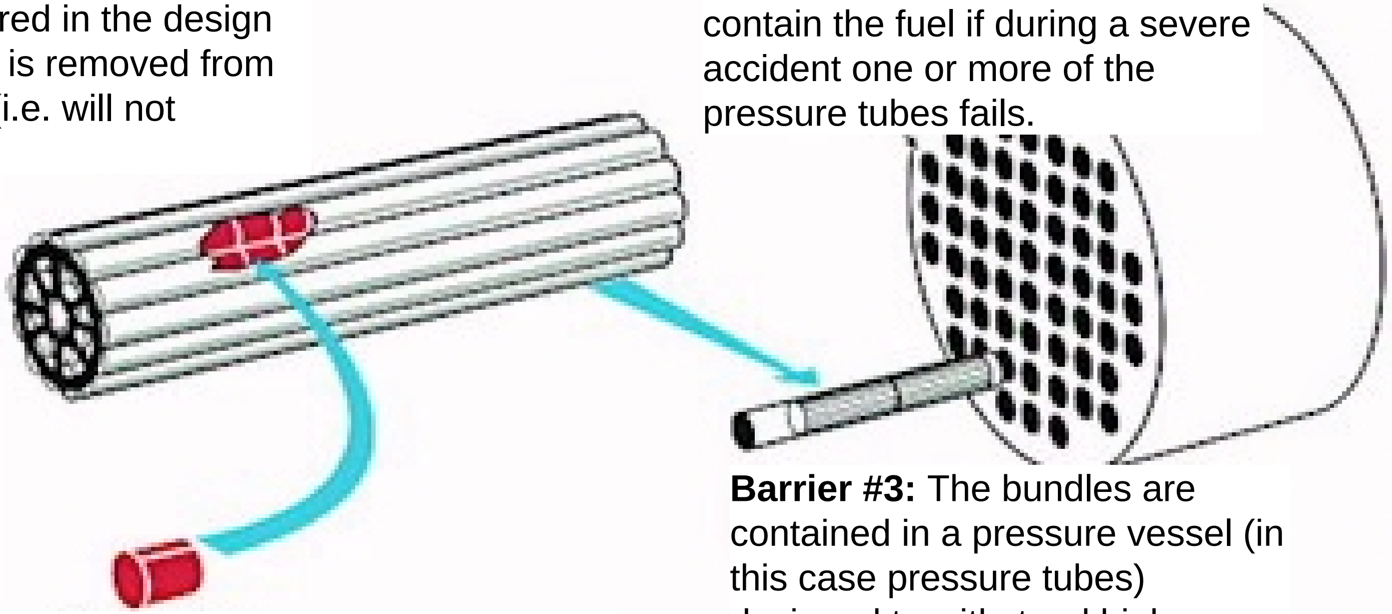
Defence in Depth is expected to be applied not only to design, but also to organizational, behavioural, and design-related safety and security activities to ensure barriers overlap.

CNSC performs compliance activities to confirm that defence is depth is not being eroded.

Example #1: Barriers for a Power Reactor (1)

Barrier #2: zirconium tubes that will continue to contain the fuel and any by-products during events while transferring heat away from the fuel at all times. Long term storage is also considered in the design after the fuel is removed from the reactor. (i.e. will not corrode)

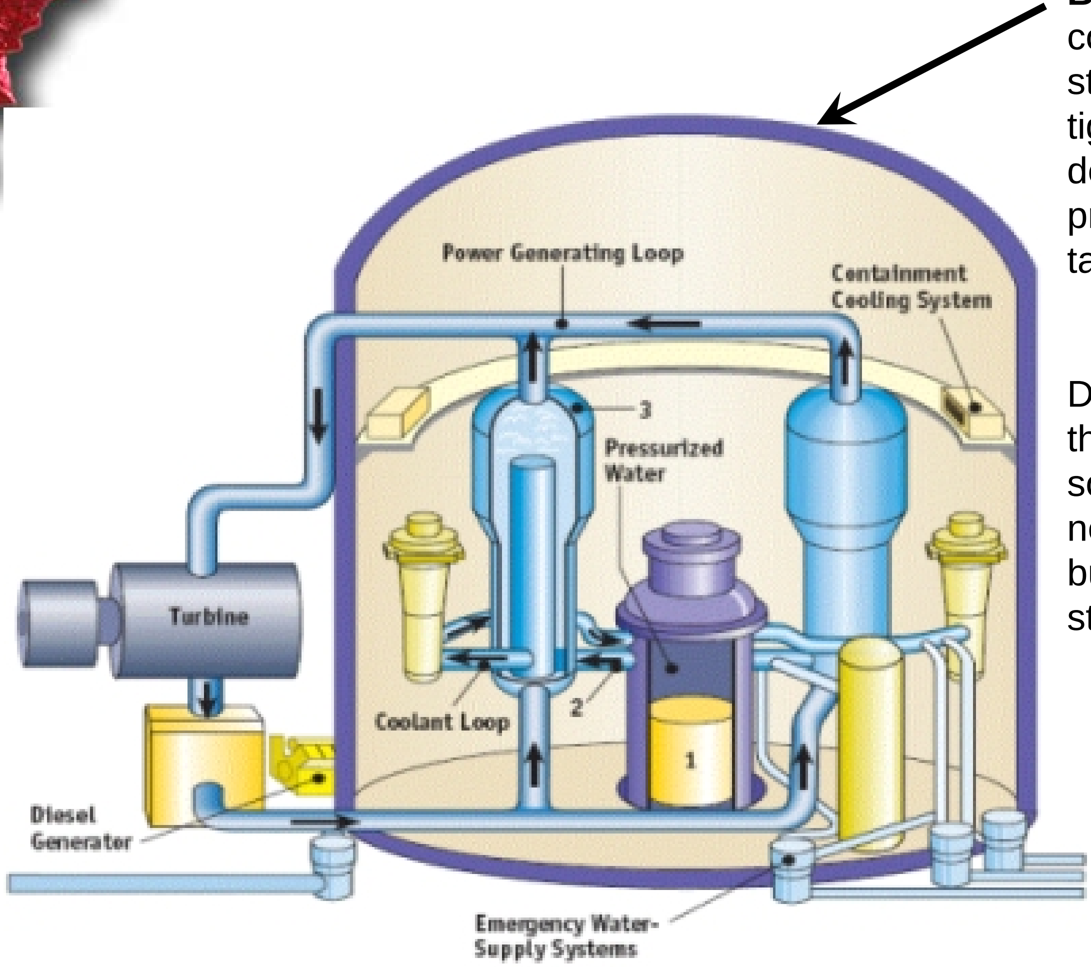
Barrier #4: In this case, a larger vessel called a calandria is designed to assist with cooling of the fuel during an event and to contain the fuel if during a severe accident one or more of the pressure tubes fails.



Barrier #1: A ceramic pellet that can tolerate high temperatures during an event

Barrier #3: The bundles are contained in a pressure vessel (in this case pressure tubes) designed to withstand high pressure and temperature events while cooling fuel.

Example #1: Barriers for a Power Reactor (2)



Barrier #5: The reactor vessel is then contained within several concrete structures that reside in a pressure tight “containment building” that is designed to: withstand 1.5 times the pressure from a worst case accident taking external events into account.

Dependent on safety characteristics of the reactor and the reactor layout some technologies may not necessarily need a containment building but rather a confinement structure instead.

Example #2: Barriers for a Research Reactor

Barrier #1: Fuel designed for temperatures it may encounter during events

Barrier #2: Reactor has very large negative reactivity coefficient so power excursion events cannot occur.

Barrier #3: Very large “heat sink” (water pool) in an engineered and shielded container.

Barrier #4: Confinement building with filtered ventilation

How do we know Defence in Depth is Adequate for a design?

- The design provides safety functions to ensure integrity of physical barriers.
- The intended safety functions must be fulfilled for all possible accidents considered in the design, including those of very low probability.
- The adequacy of the design of the facility is demonstrated through safety analysis.

Design should balance Safety Characteristics

Specific designs provides a balance of:

- Inherent safety features (e.g. negative reactivity coefficient)
- Passive safety features (e.g. natural circulation cooling, neutron absorber rods drop by gravity)
- Engineered safety features (automatic safety systems)

Safety case

- The design provides a balance of the safety features – inherent, passive, engineered.
- It must demonstrate how well it can fulfill the necessary safety functions for all possible accidents.
- It demonstrates meeting the dose acceptance criteria and safety goals.
- It demonstrates preventing uncontrolled release during severe accidents.

Fourth Key Concept:

Security Considerations

Security is regulated via:

The same rules apply regardless of reactor size

Nuclear Safety and Control Act

- Risks to national security, the health and safety of persons and the environment that are associated with development, production, and use

General Nuclear Safety & Control Regulations

- Lays the foundation for other, more specific regulations (e.g. Class I, II Nuclear Facilities)
- Outlines specific obligations, namely security for any nuclear facility

Nuclear Security Regulations

- Nuclear Facilities that possess, use, or store Category I, II or III nuclear material (e.g. enriched uranium, plutonium)

Identifying Threats

Threat and Risk Assessment

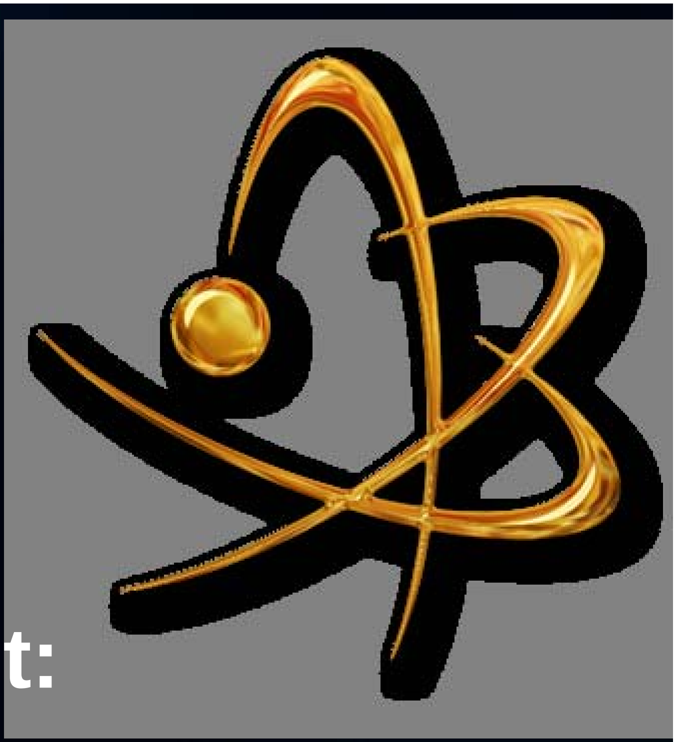
- identify threats, risks and/or vulnerabilities

Design Basis Threat (baseline)

- characteristics/attributes of potential insider/external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated

Beyond Design Basis Threat

- topography, compact versus spread, bunker design, containment structure including heat sinks, shielding



Fifth Key Concept:

Robustness Considerations and Engineering Safety Provisions

Robustness Considerations

- **Robustness** of nuclear facility refers to its general invulnerability to threats and human – induced hazards provided by many different aspects of the facility and its operation.
- **Engineering safety provisions** are focused on increasing structural strength using protective design.

What Does This Mean for Small Reactors? (1)

- Robustness against non-malevolent internal and external events should receive the same rigour as that applied to large nuclear reactors.

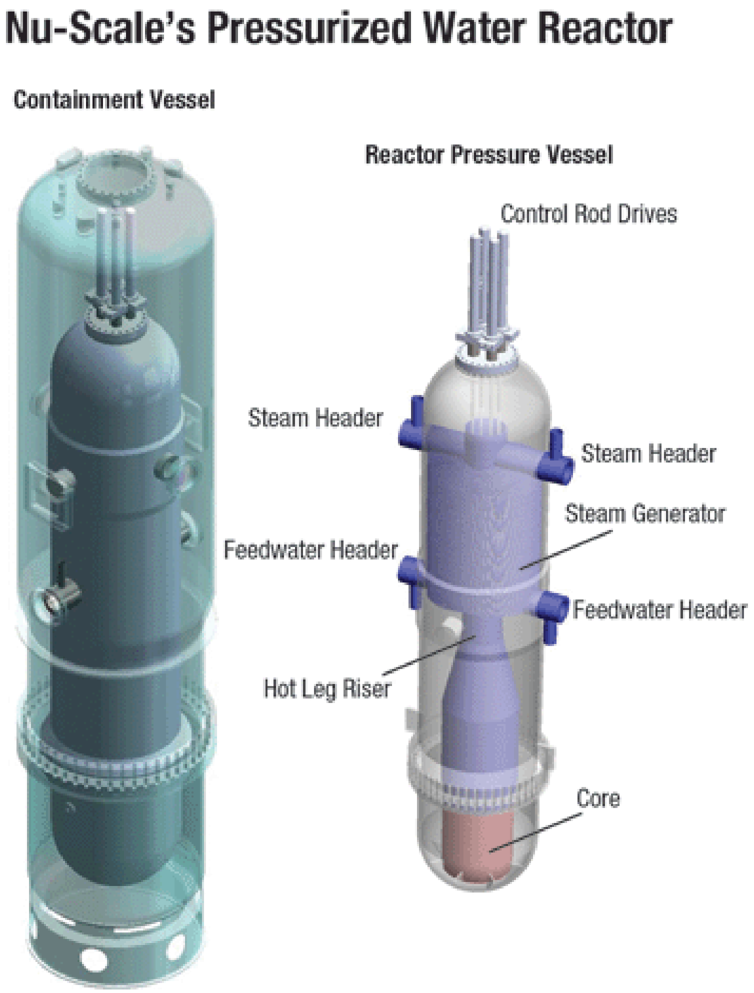
- This involves good defence in depth demonstrated through research and development efforts as well as analysis.

What Does This Mean for Small Reactors? (2)

Robustness against malevolent internal and external events should also receive the same rigour as that applied to large nuclear reactors.

But small reactors are, by their nature, designed differently, and may employ different protective measures that would not be considered for large reactors.

Example:



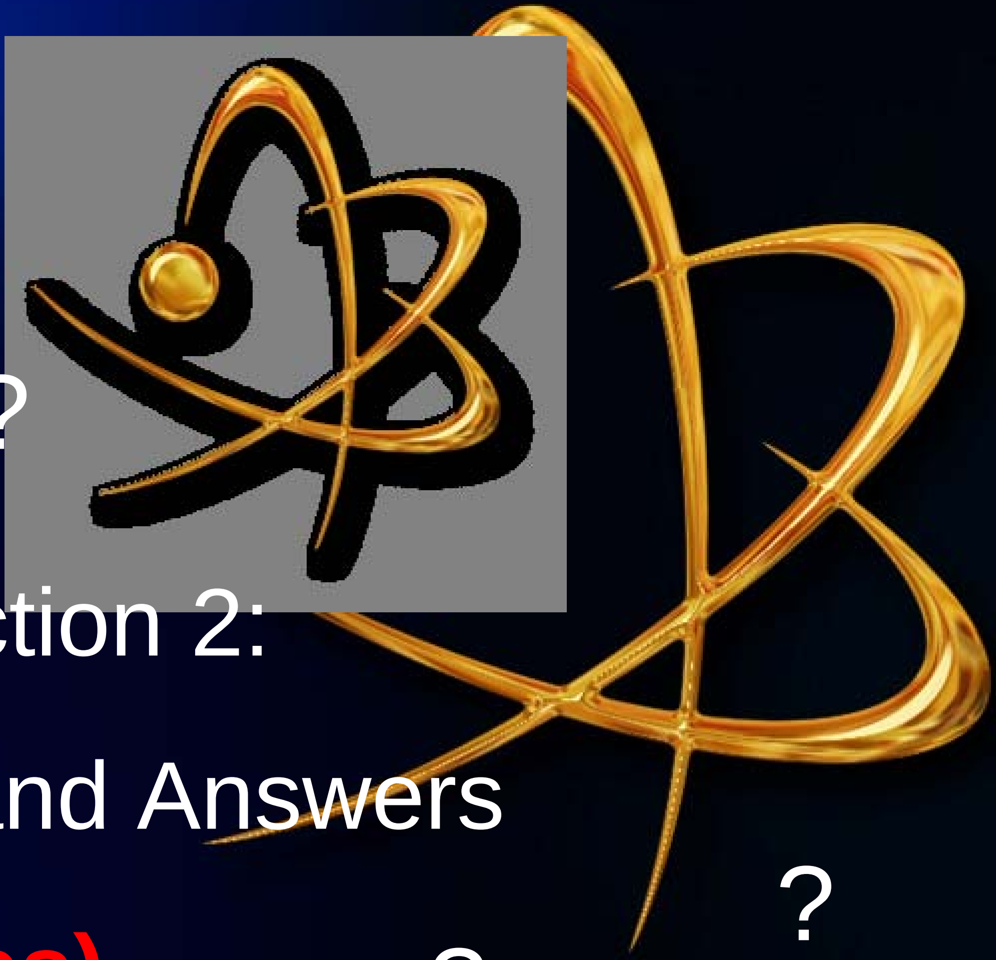
This 150 MWth (45 MW electric) reactor, in its containment vessel would could be located in a concrete "bunker" below ground with the associated steam plant above ground. This means that the plant has a very small profile and may be easier to protect against malevolent acts.

Engineering Safety Provisions

- **The protective design** is focused on areas containing equipment, systems, devices or nuclear substances the sabotage of which would or would likely pose an unreasonable risk to health and safety.
- The goal of the protective design is:
  1. Reactor shutdown;
  2. Fuel cooling; and
  3. Limitation of radioactive and toxic releases.

? ?

? ?



End of Section 2:

Question and Answers

(15 minutes)

? ?