Canadian Approach to Defence in Depth

Presented at:

Defence-in-depth Inter-Agency Workshop

August 26 and 27, 2015

Dr. Doug Miller
Directorate of Regulatory Improvement and Major Projects Management

Outline

- The CNSC
- Defence in depth: Implementation
- Defence in depth: Enhancement
- Summary

BACKGROUND – THE CNSC

Canadian Nuclear Safety Commission

- Established May 2000, under the *Nuclear Safety and Control Act*
- Replaced the *AECB,* established in 1946, under the *Atomic Energy Control Act*
- The CNSC regulates all nuclear-related facilities and activities

Close to 70 years of experience

Our Mission

To protect the **health, safety** and **security** of persons and the **environment**; and to implement Canada's **international commitments** on the peaceful use of nuclear energy

The CNSC is Canada's nuclear watchdog

The CNSC regulates all nuclear-related facilities and activities…

- Uranium mines and mills
- Uranium fuel fabricators and processing
- Nuclear power plants
- Waste management facilities
- Nuclear substance processing
- Industrial and medical applications
- Nuclear research
- Export/import control

…from cradle to grave

Independent Commission

- Quasi-judicial administrative tribunal
- Independent Commission members
- Public hearings
- Supported by Secretariat and independent legal services
- Decisions can only be reviewed by Federal Court

Transparent, science-based decision-making

The licensee is the cornerstone of safety and is held accountable by their licence

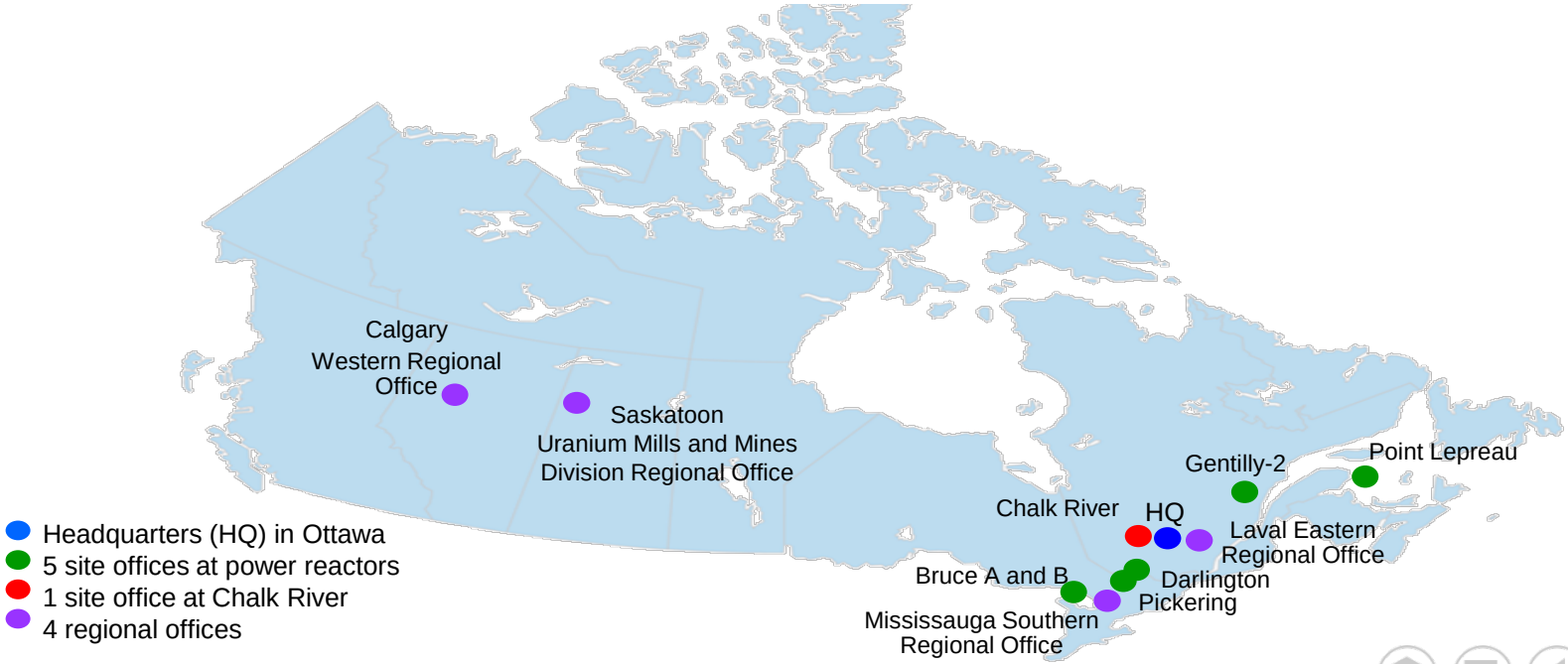
Section 24(4) of the *Nuclear Safety and Control Act*

No licence may be issued, renewed, amended or replaced unless, in the opinion of the Commission, the applicant:

a) is qualified to carry on the activity that the licence will authorize the licensee to carry on; and

b) will, in carrying on that activity, make adequate provision for the protection of the environment, the health and safety of persons and the maintenance of national security and measures required to implement international obligations to which Canada has agreed

CNSC offices across Canada
Regulating all nuclear-related facilities and activities



DEFENCE IN DEPTH: IMPLEMENTATION

Canadian Nuclear Power Plants

Evolution of Regulatory Requirements

NRX accident in Chalk River in 1952

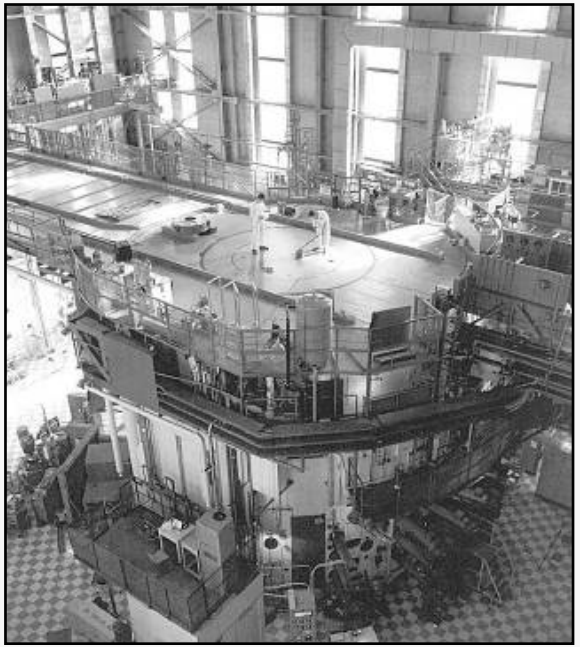
- Partial meltdown and hydrogen explosions due to operator error and mechanical problems in the shutdown systems
- Led to development of a concept of dual failure accident analysis

Single and dual system failure approach

- Separate, independent and redundant safety systems
- Two-group separation approach against common-cause failures
- Consideration of selected beyond-design-basis accidents

Adaptation of international standards and practices

- **Systematic application of risk-informed defence-in-depth strategy**
- Implementation of probabilistic safety goals



Implementation of Defence-in-Depth

- Safety objectives and safety goals are met through implementation of the defence-in-depth framework
  - **results in a strong safety case**

- Elements of the defence-in-depth framework are found in the CNSC's regulations and regulatory documents, and in national and international standards

Qualitative Safety Objectives for new Nuclear Power Plants (1)

- **General nuclear safety objective**

  Design and operate nuclear power plants (NPPs) in a manner that will protect individuals, society and the environment from harm. This objective relies on the establishment and maintenance of effective defences against radiological hazards in NPPs.

- **Technical safety objective**

  Provide all reasonably practicable measures to prevent accidents in the NPP, and mitigate the consequences of accidents if they do occur. This takes into account all possible accidents considered in the design, including those of very low probability. Any radiological consequences will be below prescribed limits, and the likelihood of accidents with serious radiological consequences will be extremely low.

Qualitative Safety Objectives for New Nuclear Power Plants (2)

- A limit is placed on the societal risks posed by NPP operation Individual members of the public shall be provided a level of protection from the consequences of NPP operation, such that there is no significant additional risk to the life and health of individuals. Societal risks to life and health from NPP operation shall be comparable to or less than the risks of generating electricity by viable competing technologies, and shall not significantly add to other societal risks.

- The design shall be such that plant states that could lead to significant radioactive releases are **practically eliminated**.

  - **For plant states that are not practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.**

Quantitative Safety Goals for new Nuclear Power Plants

- **Core damage frequency**
  The sum of frequencies of all event sequences that can lead to significant core degradation shall be less than 10^{-5} per reactor year.

- **Small release frequency**
  The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} becquerels of iodine-131 shall be less than 10^{-5} per reactor year. **A greater release may require temporary evacuation of the local population.**

- **Large release frequency**
  The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} becquerels of cesium-137 shall be less than 10^{-6} per reactor year. **A greater release may require long term relocation of the local population**.

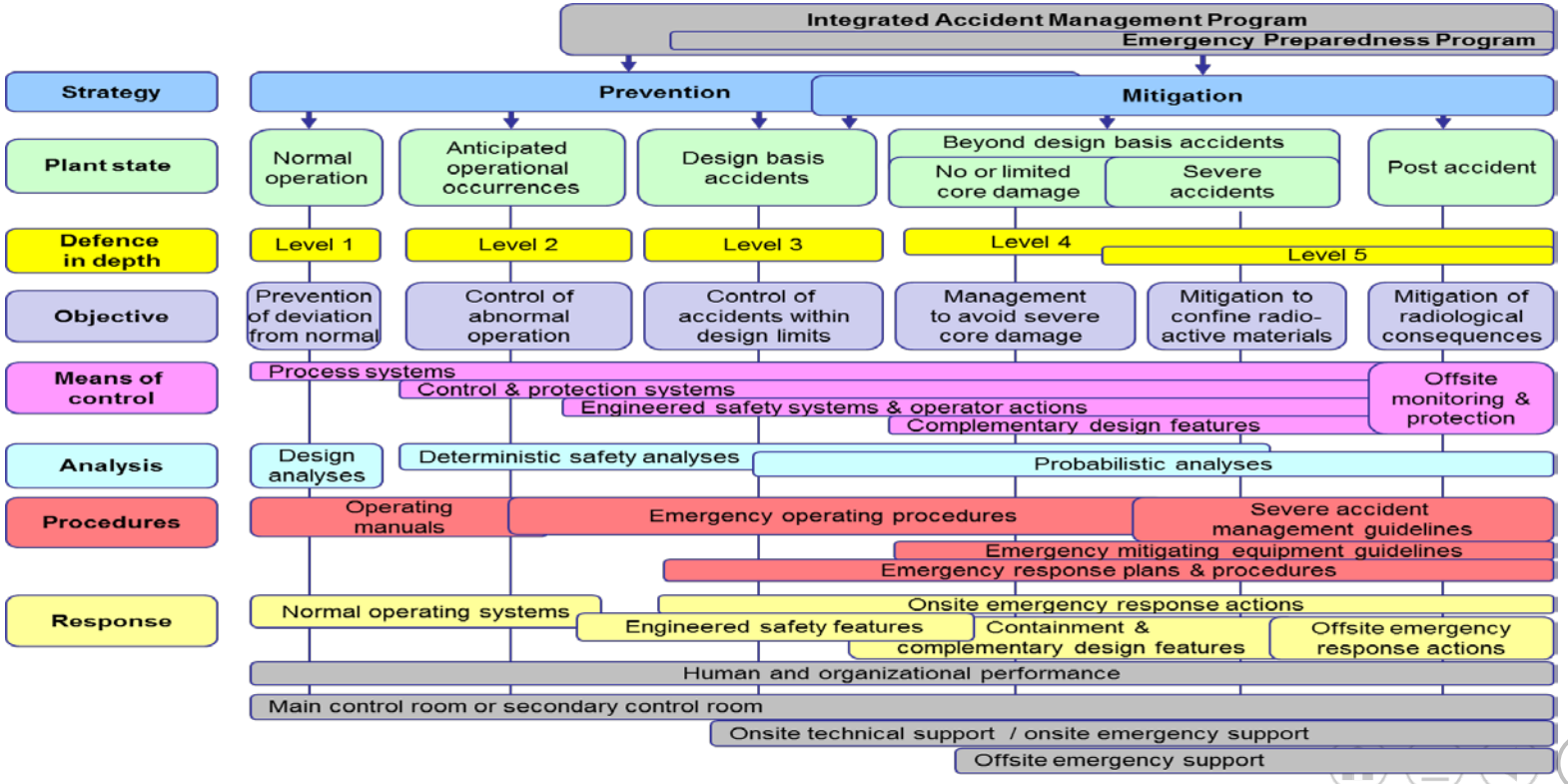
Defence-in-Depth: Concept

- Applied throughout the design process and operation of the plant to provide a series of levels of defence aimed at preventing accidents, and ensuring appropriate protection in the event that prevention fails.
  - allows the failure to be detected and compensated for or corrected
  - considers organizational and human performance
- The levels of defence in depth shall be independent to the extent practicable and subject to overlapping provision.

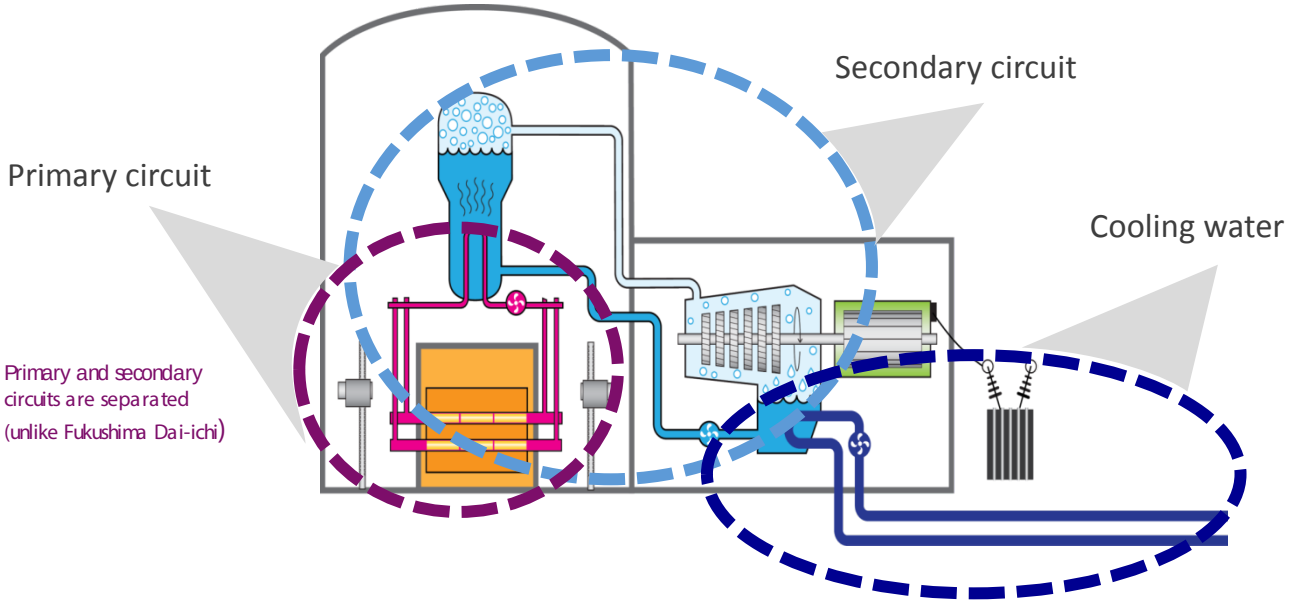
Defence-in-Depth Framework

Level	Implementation
1. To prevent deviations from normal operation, and to prevent failures of structures, systems and components important to safety.	• Conservative design • High-quality construction (e.g., appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, operational experience)
2. To detect and intercept deviations from normal operation, to prevent anticipated operational occurrences from escalating to accident conditions and to return the plant to a state of normal operation.	• Inherent and engineered design features to minimize or exclude uncontrolled transients to the extent possible
3. To minimize the consequences of accidents, and prevent escalation to beyond-design-basis accidents	• Inherent safety features • Fail-safe design • Engineered design features, and procedures that minimize consequences of DBAs
4. To ensure that radioactive releases caused by severe accidents or design-extension conditions are kept as low as practicable.	• Equipment and procedures to manage accidents and mitigate their consequences as far as practicable • Robust containment design • Complementary design features to prevent accident progression and to mitigate the consequences of design-extension conditions • Severe accident management procedures
5. To mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions.	• Emergency support facilities • Onsite and offsite emergency response plans

Defence in Depth: Integrated Accident Management



CANDU Nuclear Power Plant



Canadian Nuclear Power Plants

CANDU Reactor Design

Defence in depth

- Reliable safety system
- Independence of process, control and safety systems
- Multiple barriers

Large inventory of water

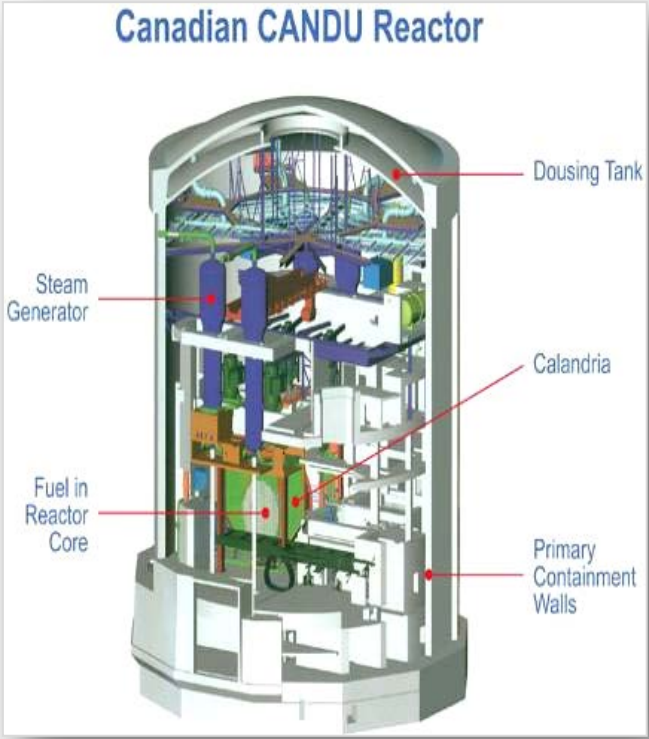
- Primary/secondary coolant
- Moderator coolant

Many hours of passive cooling

- Extended recovery time

In-ground spent fuel pools

- Seismically qualified
- Diverse means of adding water

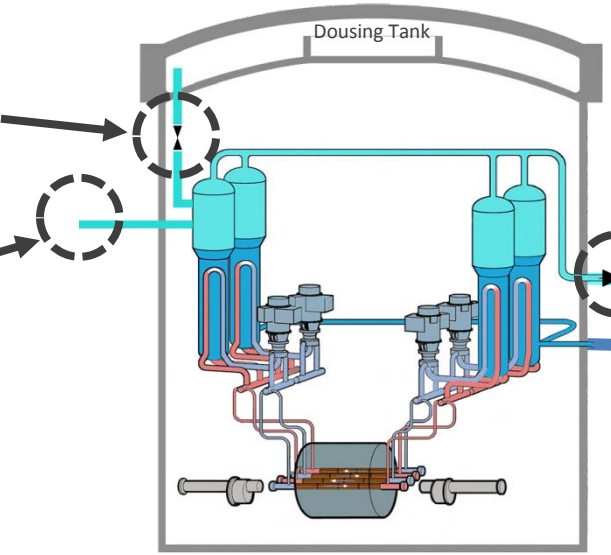


CANDU Design Overview

Based on the CANDU-6 Design

Emergency water supply (simplified)

Opens automatically Boiler makeup water isolation valves fail open on loss of power or instrument air



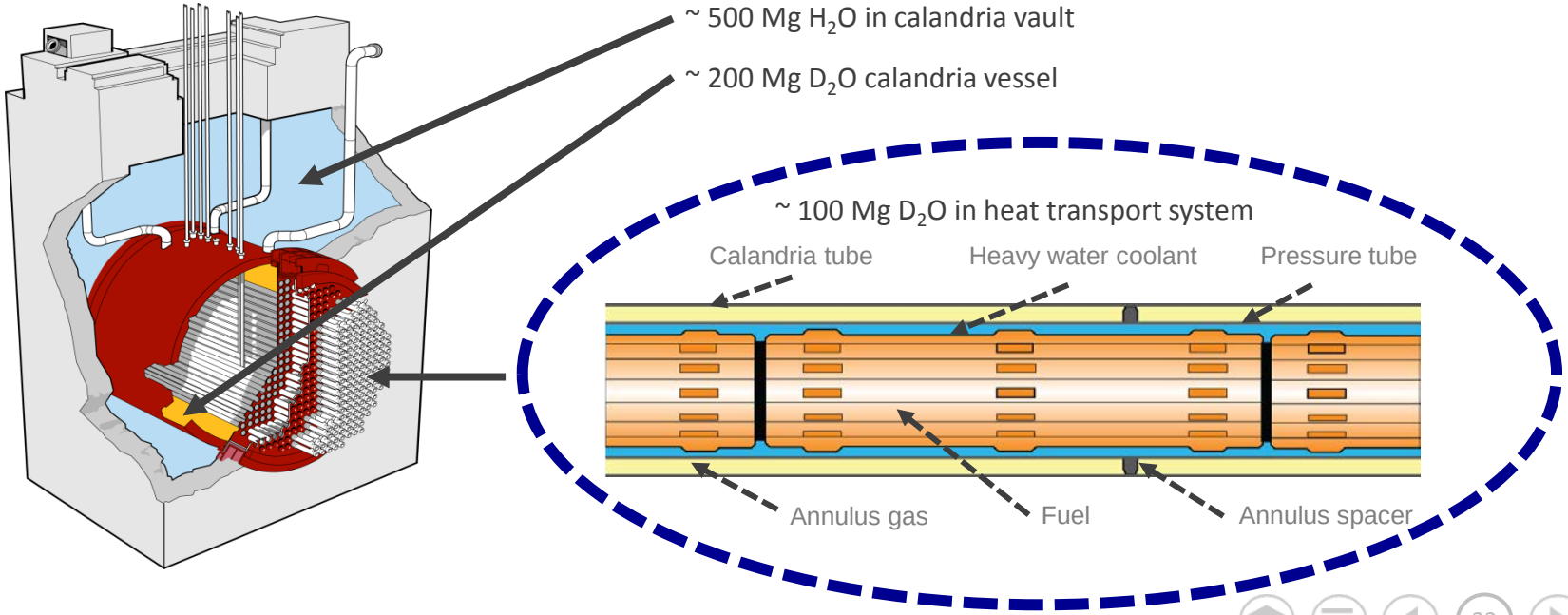
Main steam safety valves Opens automatically to depressurize primary and secondary sides

Feedwater supply

Source: CANDU Energy Inc.

CANDU Design Overview

Passive Heat Removal



DEFENCE IN DEPTH: ENHANCEMENT

Post-Fukushima Enhancements to Defence in Depth

General conclusion

- Canadian nuclear power plants are safe, and the risk posed to the health and safety of Canadians or to the environment is small. Recommended improvements will further reduce the risk to as low as reasonably practicable.

General recommendations

- Strengthening defence in depth
  - external events and beyond design basis accidents
  - design and safety analysis
  - severe accident management
- Enhancing emergency preparedness
  - onsite **and** offsite emergency response
- Improving regulatory framework and processes
  - Act, regulations and regulatory documents
  - compliance and licensing processes, including implementation of periodic safety reviews
- Enhancing international collaboration
  - CANDU owner countries
  - other international regulators

Defence in Depth: Post Fukushima Enhancements

Level 3: Protecting spent fuel pools

- Makeup water capability and instrumentation

Level 4: Preventing and mitigating severe accidents

- Protecting fuel
  - makeup water capability to steam generators / primary heat transport system / emergency core coolant / dousing spray
- Preventing severe core damage
  - makeup water capability to moderator system and calandria vessel/vault
- Protecting containment
  - passive recombiners and containment venting
  - severe accident management guidelines validation/exercise

Level 5: Protecting the public

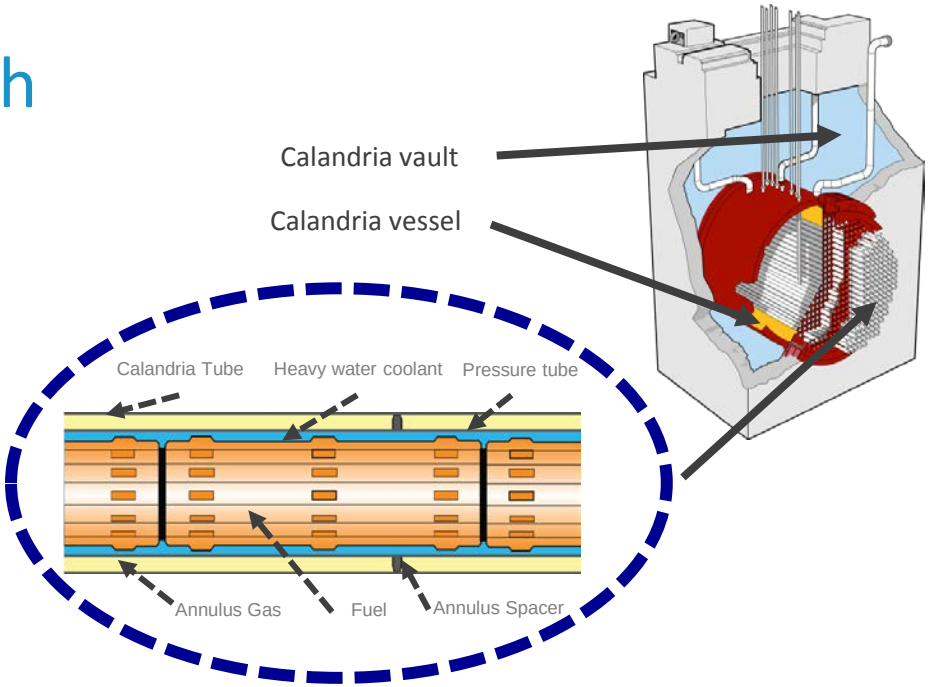
- Containment filtered venting
- Integrated emergency plans and full-scale emergency exercises

Reactor Defence in Depth

Protect Fuel (1/2)

Analyses and reassessments

- Re-evaluation of site-specific magnitudes of external events
  - high winds, seismic, tsunami / storm surges, flooding
  - significance of station blackout event on spent fuel bundles inside fueling machine
- Re-evaluation of multi-unit events

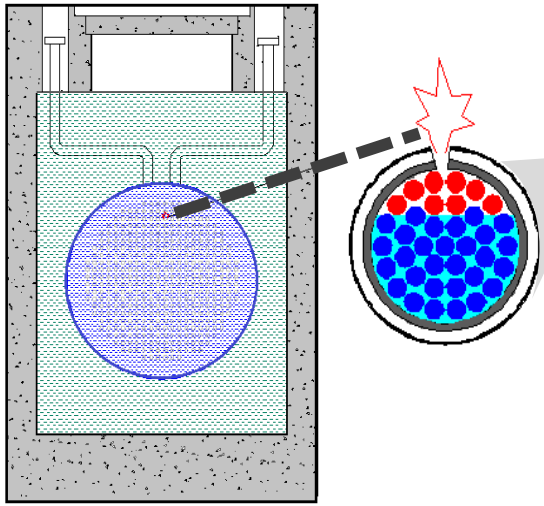


Reactor Defence in Depth

Protect Fuel (2/2)

Design improvements

- Emergency mitigating equipment
  - mobile water pumps and diesel-generators
- Water makeup connections to:
  - steam generators
  - primary heat transport system
- Provision to open main steam safety valves after station blackout
- Upgrades of power systems to improve reliability, longevity of battery supply
  - improved load shedding to extend battery availability
  - upgrades to power supply for key instrumentation (e.g., local air cooler)
- Protection against flooding (barriers, water-tight doors, sealing penetrations)



Four hours of cooling for unmitigated total loss of heat sinks due to natural circulation.

Fuel channel failure not expected for several hours due to gravity water feed from dousing tank.

A design change to permit water make-up to steam generators or primary heat transport system maintain fuel and feed channel integrity.

Reactor Defence-in-Depth

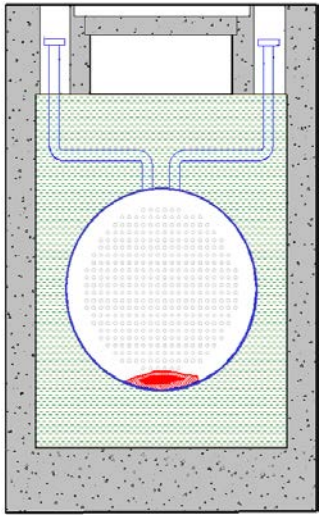
Prevent Severe Core Damage

Analyses and reassessments

- Severe accident studies including modelling for multi-unit plant events
- Reassessment of main control room and secondary control Room habitability during emergencies
- Instrumentation qualification for severe accident (SA) conditions

Design improvements

- Water makeup connections to
  - calandria vessel (moderator)
  - calandria vault (shield tank)
- Improve pressure relief capability of calandria/vault
- Instrumentation upgrades for SA conditions



40 hours to calandria vessel failure for unmitigated total loss of heat sinks.

A design change to permit water makeup to calandria vessel or calandria vault maintains calandria vessel integrity.

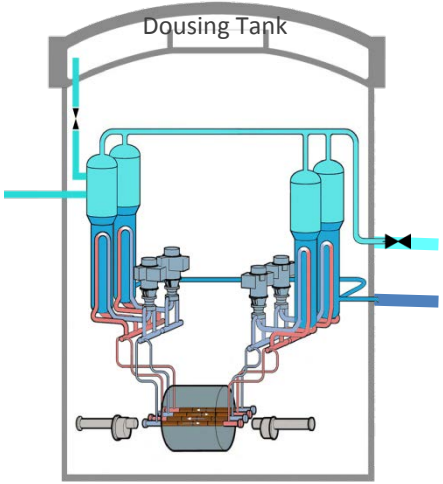
Reactor Defence in Depth
Protect Containment

Analyses and reassessments

- Enhancement of **filtered** containment venting system
- Severe accident management guidelines (SAMGs)
- Instrumentation for SA conditions monitoring (qualify existing or new)
- Control facilities' habitability during SA
- Improved modelling of SAs for multi-unit plants

Design improvements

- Installation / enhancement of containment venting
- Installation of passive autocatalytic recombiners



Source: CANDU Energy Inc.

After 56 hours, molten fuel debris fall into the basement of the reactor building for unmitigated total loss of heat sink.

Controlled venting protects containment from high internal pressure and cracking.

Reactor Defence in Depth
Protect Spent Fuel Pools

Analyses and reassessments

- Structural integrity check for temperatures above design values

Design improvements

- Instrumentation to measure water level and temperature
- Piping and connections for external addition of water
- Operating procedure for loss of cooling

Enhancing Emergency Preparedness (Onsite)

Implemented Safety Enhancements

Onsite emergency preparedness

- Incorporating SA management into emergency plans

Backup power and telecommunications

- Implementation of backup power to emergency facilities and telecommunications equipment
- Formalized **mutual aid agreement** for external support
  - *Regional Emergency Response Support Centre*

Station boundary monitoring and dose modelling

- Installation of automated real-time boundary radiation monitoring
- Development of source term estimation capability

…minimize consequences of extreme events

Enhancing Emergency Preparedness (Offsite)

Integration of Federal and Provincial Nuclear Emergency Plans

- Establishing formal, transparent, national-level oversight process for offsite nuclear emergency programs
- Reviewing planning basis of offsite arrangements
  - developing capability for predicting offsite effects – needs for sheltering and evacuation
  - simple instructions to public in case of nuclear emergency
- Monitor performance of full scale emergency drills involving multi-levels Federal/provincial/municipal
  - New Brunswick Power “Intrepid” (March 2012)
  - Bruce Power “Huron Challenge” (Oct. 2012)
  - OPG “Unified Response” at Darlington (May 2014)

Improvements to Regulatory Framework and Processes

Amendments to regulations

- *Class I Nuclear Facilities Regulations* – offsite emergency
- *Radiation Protection Regulations* – dose to workers during emergencies

Developing new regulatory documents

- design of reactor facilities
- periodic safety review process
- accident management and nuclear emergency preparedness

Implementing new licence conditions

- accident management
- public information program

…all updates consider lessons learned from Fukushima

Challenges: General

- Ensure alignment of the qualitative safety objectives with the quantitative safety goals
  - practical elimination of significant releases
- Define performance objectives for design-extension conditions
  - uniform approach across disciplines based on reasonable confidence
- Develop safety analysis guidelines
  - external hazards
  - complementary design features
  - accident management procedures and SAMGs
- Applied to multi-unit sites:
  - safety objectives and goals
  - initiating events and common-cause failures
  - dependencies and interactions

Challenges: Alignment of Safety Objectives and Goals

Practical elimination of significant releases

- The design shall be such that plant states that could lead to significant radioactive releases are practically eliminated
  - only protective measures that are **of limited scope in terms of area and time** shall be necessary for protection of the public
- Application of the safety principles in the defence-in-depth concept
  - independence, diversity, and separation
  - passive safety features and use of multiple independent controls

➢ **assists in achieving the appropriate level of confidence that significant radioactive releases are practically eliminated**

Challenges: Design Extension Conditions

Design objectives

- Design extension equipment
  - complementary design features, such as core catchers and containment filtered venting systems
  - fixed or portable equipment located onsite or offsite, such as mobile pumps or electric power generators
  - Equipment credited in emergency procedures and SAMGs
- Safety classification
  - safety functions should be assigned a safety category commensurate with safety significance (e.g., likelihood of use, consequences of failure)
- Survivability of equipment and instrumentation

Challenges: Safety Analysis Guidelines

- External hazards
  - systematic assessment of external hazards on a periodic basis
  - assessment of conditions where a small change in conditions may results in a large increase in the severity of an event (cliff-edge effects)
- Complementary design features
  - consideration of design objectives such as design targets and reasonably high confidence
- Accident management procedures and SAMGs
  - demonstration that equipment and instrumentation is capable of performing their intended safety function(s) under accident conditions
- Human and organizational performance
  - assessment of adequacy of staffing and staff performance
  - evaluation of training and drills

Challenges: Multi-Unit Sites

- Safety objectives and goals
  - objectives and goals should be established to eliminate significant radioactive releases and the need for long-term evacuation
  - methodology for analyses demonstrating the safety objectives can be met needs to be developed
- Initiating events and common-cause failures
  - initiating events demonstrating that safety objectives are met need to address all credible common cause internally and externally initiated events
- Dependencies and interactions between units need to be systematically evaluated in consideration of all layers of defence in depth
  - design-extension conditions should specifically be considered
  - accident management procedures and SAMGs should be extended to include multi-unit events

SUMMARY

Concluding Remarks

Safety Benefits

Enhanced accident prevention

- Accident risk reduced by a factor of 2 to 10, depending on accident scenarios

Improved mitigation of accident consequence

- Potential radiological consequences reduced to as low as reasonably practicable

Public protection

- Effective strategies for sheltering and evacuation

…Continuous safety improvements

Concluding Remarks

Safety Upgrades

Portable generators

Portable pumps

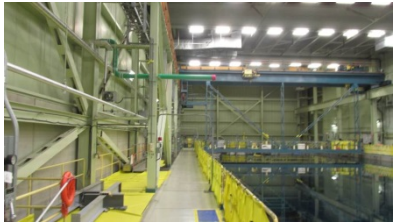
Flood barriers

Calandria vault makeup

Passive autocatalytic recombiners

Emergency containment filtered ventilation system

Storage buildings



Improvements to irradiated fuel bays

...making Canadian nuclear power plants safer

APPENDIX

Industry Regulatory Developments: Safety Enhancements to Defence in Depth (1/2)

Level/Description	Objectives	Design upgrades	Guides/procedures	Safety assessments
Level 1: Prevention of abnormal operation and failures	Prevent deviations from normal operation, and to prevent failures of systems, structures, and components			
Level 2: Control of abnormal operation and detection of failures	Detect and intercept deviations from normal operation in order to prevent anticipated operational occurrences (AOOs) from escalating to accident conditions, and to return the plant to a state of normal operation			Reassessment of AOOs to confirm adequacy of plant operational safety.
Level 3: Control of accidents within the design basis	Minimize the consequences of accidents by providing inherent safety features, failsafe design, additional equipment, and mitigating procedures	Irradiated fuel bays: makeup water capabilities and instrumentation		Reassessment of design-basis accidents to confirm adequacy of plant design safety.
Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents	Ensure that radioactive releases caused by severe accidents are kept as low as practicable	Emergency mitigating equipment and connections: o provision of an alternate and independent supply of make-up water to steam generator/primary heat transport/calandria(moderator)/shield tank o provision to open main steam safety valves after station blackout Installation/enhancement of filtered containment venting	Emergency mitigating equipment guidelines Severe accident management guidelines	External hazards assessment: re-evaluation of site-specific magnitudes of external events, including multi-unit and irradiated fuel bay events for: o high winds, o seismic margin assessment / seismic probabilistic safety assessment, o tsunami, and flooding

Industry Regulatory Developments: Safety Enhancements to Defence in Depth (2/2)

Level/description	Objectives	Design upgrades	Guides/procedures	Safety assessments
(Cont'd) Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents (cont'd)	Ensure that radioactive releases caused by severe accidents are kept as low as practicable (cont'd)	Installation of passive hydrogen recombiners Installation of shield tank (or calandria vault) overpressure relief Upgrades of power systems to improve reliability, longevity of battery supply, improved backup for critical loads o improved load shedding to extend battery availability o battery charging capability and uninterruptible power supply (ups) system backup o upgrades to power supply for key instrumentation (e.g., emergency filtered air discharge system) Protection against flooding (barriers, water-tight doors) Instrumentation upgrades for severe accident conditions		Demonstration of adequacy or provision of additional relief capacity to the reactor during severe accident Structural integrity assessment of irradiated fuel bays for temperatures above design values Reassessment of main control room and secondary control room habitability Instrumentation qualification for severe accident conditions Assessment of airplane crash
Level 5: Mitigation of radiological consequences of significant releases of radioactive materials	Mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions	Onsite and offsite emergency response centres Regional Emergency Response Support Centre available to all Canadian NPP operators Emergency operations centre	Integrated emergency plans Provincial Nuclear Emergency Response Plan Regional and Municipal Emergency Response Plans	Study of Consequences of a Hypothetical Severe Nuclear Accident Plume dispersion and dose modelling

Find out more about us


Visit us online


Like us on Facebook

View us on YouTube


Follow us on Twitter


Subscribe to updates


Contact us