Assessment Document

APPLICATION OF INPRO (INNOVATIVE NUCLEAR REACTORS AND FUEL CYCLES) COMPARATIVE ASSESSMENT FOR ENHANCED CANDU 6 PERTAINING TO LESSONS LEARNED FROM THE FUKUSHIMA DAI-ICHI NUCLEAR EVENT

Enhanced CANDU 6 (EC6) Program

53A-03600-ASD-011

Revision 1

Prepared by
Boyle, Sabina - Senior Licensing Analyst

Reviewed by
Reid, Patrick - Senior Manager, Deterministic Safety Analysis

Approved by
Dinh, Ngoc-Boi - ENGINEERING MGR-EC6 Product Development

2013/12/02

UNRESTRICTED

Candu Energy Inc.

2285 Speakman Drive
Mississauga, ON
L5K 1B1 Canada
Assessment Document

APPLICATION OF INPRO COMPARATIVE ASSESSMENT FOR ENHANCED CANDU 6® PERTAINING TO LESSONS LEARNED FROM THE FUKUSHIMA DAI-ICHI NUCLEAR EVENT

Enhanced CANDU 6

53A-03600-ASD-011
Revision 1

2013 December  
décembre 2013

UNRESTRICTED  
ILLIMITÉ

Candu Energy Inc.  
Candu Energy Inc.
2285 Speakman Drive  
2285 Speakman Drive
Mississauga, ON  
Mississauga, ON
L5K 1B1 Canada  
L5K 1B1 Canada
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>INTRODUCTION .................................................................</td>
</tr>
<tr>
<td>1.1</td>
<td>Scope of INPRO Safety Assessment ........................................</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Fukushima Event – March 11, 2011 .......................................</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Fukushima Lessons Learned Applicability to INPRO Criteria for Innovations in Application of Defence-in-Depth (DID) Principle ...........</td>
</tr>
<tr>
<td>1.1.3</td>
<td>Selection of Basic Principle 1: Defence in Depth .....................</td>
</tr>
<tr>
<td>1.1.3.1</td>
<td>Selection of criterion CR 1.1.1 Robustness of Design ...............</td>
</tr>
<tr>
<td>1.1.3.2</td>
<td>Selection of criterion CR 1.1.2 Operation ..............................</td>
</tr>
<tr>
<td>1.1.3.3</td>
<td>Selection of criterion CR 1.3.3 Safety features .....................</td>
</tr>
<tr>
<td>1.1.3.4</td>
<td>Selection of criterion CR1.3.4 Barriers ................................</td>
</tr>
<tr>
<td>1.1.3.5</td>
<td>Selection of criterion CR1.3.5 Controlled state ......................</td>
</tr>
<tr>
<td>1.1.3.6</td>
<td>Selection of criteria CR 1.4.1 and CR1.5.1 Major release into containment and frequency of release to environment ..................</td>
</tr>
<tr>
<td>1.1.3.7</td>
<td>Selection of criterion CR 1.6.1 Independence of defence in depth .........................................................</td>
</tr>
<tr>
<td>2.</td>
<td>SELECTION OF REFERENCE PLANT .................................................</td>
</tr>
<tr>
<td>2.1</td>
<td>Evolution of EC6 Design to CANDU 6 .......................................</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Changes to the Original Design Basis .......................................</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Comparison of CANDU 6 and EC6 Design ....................................</td>
</tr>
<tr>
<td>3.</td>
<td>INPRO SAFETY ASSESSMENT .......................................................</td>
</tr>
<tr>
<td>3.1</td>
<td>Basic Principle 1: Defence-in-depth .......................................</td>
</tr>
<tr>
<td>3.1.1</td>
<td>User Requirement UR1.1 – Robustness .....................................</td>
</tr>
<tr>
<td>3.1.1.1</td>
<td>Assessment against criterion CR1.1.1 Robustness ......................</td>
</tr>
<tr>
<td>3.1.1.1.1</td>
<td>Margins of Design ............................................................</td>
</tr>
<tr>
<td>3.1.1.1.1.1</td>
<td>Improved Subcriticality Margins .........................................</td>
</tr>
<tr>
<td>3.1.1.1.1.2</td>
<td>Improved Safety Margins ..................................................</td>
</tr>
<tr>
<td>3.1.1.1.1.3</td>
<td>Improved Containment Design Margin ..................................</td>
</tr>
<tr>
<td>3.1.1.1.1.4</td>
<td>Improved Seismic Margin ..................................................</td>
</tr>
<tr>
<td>3.1.1.1.1.5</td>
<td>Increased Flood Margin ....................................................</td>
</tr>
<tr>
<td>3.1.1.1.1.6</td>
<td>Increased Heat Sink Margin ...............................................</td>
</tr>
<tr>
<td>3.1.1.1.2</td>
<td>Redundancy of Systems .....................................................</td>
</tr>
<tr>
<td>3.1.1.1.2.1</td>
<td>Reactivity Control ...........................................................</td>
</tr>
<tr>
<td>3.1.1.1.2.2</td>
<td>Heat Sink Capability ........................................................</td>
</tr>
<tr>
<td>3.1.1.2</td>
<td>Final assessment of criterion CR1.1.1 Robustness .....................</td>
</tr>
<tr>
<td>3.1.1.3</td>
<td>Assessment against criteria CR1.1.2 Operation ........................</td>
</tr>
<tr>
<td>3.1.1.4</td>
<td>Final assessment of criterion CR1.1.2 Operation ........................</td>
</tr>
<tr>
<td>3.1.1.5</td>
<td>Final assessment of user requirement UR1.1 - Robustness ................</td>
</tr>
<tr>
<td>3.1.2</td>
<td>User Requirement UR1.3 – Design Basis Accidents ...................</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2.1</td>
<td>Assessment against criterion CR1.3.3 Safety Features</td>
</tr>
<tr>
<td>3.1.2.2</td>
<td>Final assessment of criterion CR1.3.3 Safety Features</td>
</tr>
<tr>
<td>3.1.2.3</td>
<td>Assessment against criterion CR1.3.4 Barriers</td>
</tr>
<tr>
<td>3.1.2.4</td>
<td>Final assessment of criterion CR1.3.4 Barriers</td>
</tr>
<tr>
<td>3.1.2.5</td>
<td>Assessment against CR1.3.5 Controlled State</td>
</tr>
<tr>
<td>3.1.2.6</td>
<td>Final assessment of criterion CR1.3.5 Controlled State</td>
</tr>
<tr>
<td>3.1.2.7</td>
<td>Final assessment of user requirement UR1.3 - Design Basis Accidents</td>
</tr>
<tr>
<td>3.1.3</td>
<td>User Requirement UR1.4 – Release into Containment</td>
</tr>
<tr>
<td>3.1.3.1</td>
<td>Assessment against CR1.4.1 Frequency of release into containment</td>
</tr>
<tr>
<td>3.1.3.2</td>
<td>Final assessment of user requirement UR1.4 – Release into Containment</td>
</tr>
<tr>
<td>3.1.4</td>
<td>User Requirement UR 1.5 – Release into Environment</td>
</tr>
<tr>
<td>3.1.4.1</td>
<td>Assessment against CR1.5.1 Major release to environment</td>
</tr>
<tr>
<td>3.1.4.2</td>
<td>Final assessment of user requirement UR1.5 – Release into Environment</td>
</tr>
<tr>
<td>3.1.5</td>
<td>User Requirement UR1.6 - Independence of DID Levels</td>
</tr>
<tr>
<td>3.1.5.1</td>
<td>Assessment against CR1.6.1 Independence of DID levels</td>
</tr>
<tr>
<td>3.1.5.2</td>
<td>Final assessment of user requirement UR1.6 – Independence of DID levels</td>
</tr>
<tr>
<td>4.</td>
<td>SUMMARY</td>
</tr>
<tr>
<td>5.</td>
<td>REFERENCES</td>
</tr>
</tbody>
</table>

## TABLES

Table 1-1: INSAG Objectives and INPRO Criteria Pertaining to Fukushima Lessons Learned | 2
Table 2-1: General System Data of CANDU 6 in Comparison to EC6 Design | 15
Table 2-2: Important Safety Features | 17
Table 2-3: External Natural Events Design Basis | 19
Table 3-1: CR1.1.1 Evaluation for subcriticality design margins | 22
Table 3-2: CR1.1.1 Evaluation for improved safety margins | 23
Table 3-3: CR1.1.1 Evaluation for improved robustness of containment | 25
Table 3-4: CR1.1.1 Grouping Philosophy & Safety Function | 26
Table 3-5: CR1.1.1 Seismic Design | 27
Table 3-6: CR1.1.1 Seismic Safety Function Capability | 28
Table 3-7: CR1.1.1 Design Basis Flood | 32
TABLE OF CONTENTS

SECTION                                    PAGE

Table 3-8: CR1.1.1 Loss of All AC Power Event (Loss of Class IV + Class III Standby DGs + EPS DGs)..................................................................................................................33
Table 3-9: CR1.1.1 for Evaluation of improved redundancy of systems........................................37
Table 3-10: CR1.1.1 for Evaluation of Decay Heat Removal..............................................................39
Table 3-11: CR1.1.1 for Evaluation of heat sink capability .................................................................41
Table 3-12: CR1.1.1 Evaluation for improved heat sink capability ......................................................45
Table 3-13: CR1.1.2 Evaluation of improved plant availability and capability .....................................48
Table 3-14: CR1.1.2 Category and Component Identification for EHM ..............................................49
Table 3-15: CR1.3.5 Evaluation for Improvement of Controlled State .................................................57
Table 3-16: CR1.3.5 Trip Parameters ..................................................................................................58

FIGURES

Figure 2-1: CANDU 6 Reactor Design .................................................................................................14
Figure 3-1: Containment Design Margin .............................................................................................24
Figure 3-2: Water Inventory in CANDU 6 plants .................................................................................38
Figure 3-3: Schematic Diagram of the Severe Accident Recovery and Heat Removal System in EC6 Design .........................................................................................................................41
Figure 3-4: Schematic of Systems Important to Safety in the EC6 which Transfer Residual Heat to the Ultimate Heat Sinks ........................................................................................................43
Figure 3-5: Schematic of Safety Related Systems which Transfer Residual Heat to the Ultimate Heat Sinks for CANDU 6 ........................................................................................................44
Figure 3-6: CANDU 6 Defence in Depth Barriers ..................................................................................54
Figure 3-7: Severe Core Damage Margin ..............................................................................................62
Figure 3-8: LRF Margin (with seismic) ................................................................................................64

APPENDICES

APPENDIX A – CANDU 6 TECHNICAL SUMMARY ........................................................................70
1. INTRODUCTION

The INPRO [1] method of assessment is used in this report to compare the design of the generic Enhanced CANDU 6 (EC6®) reactor design, as an Innovative Nuclear Energy System (INS), to an operating generic CANDU® 6 reactor design pertaining to lessons learned from the Fukushima Dai-ichi nuclear event [2]. The EC6 is considered an ‘evolutionary design’ for the INPRO methodology; that is an advanced design that achieves improvements over the existing CANDU 6 design through small to moderate modification, with a strong emphasis on maintaining design proveness to minimize technological risk. This comparative assessment focuses on the design features in each of the five levels of defence-in-depth described in IAEA SSR-2/1 [3] and compares the capabilities of the INS against the operating generic CANDU 6 reactor design to cope with prolonged loss of AC power and loss of the ultimate heat sinks that occurred for Fukushima Units 1 through 3.

1.1 Scope of INPRO Safety Assessment

The INPRO methodology on reactor safety, in Volume 8 of IAEA-TECDOC-1575 Rev.1[1], is used to compare the capabilities of the evolutionary EC6 design to the capabilities of the operating generic CANDU 6 plants after implementation of the Fukushima lessons learned for prolonged loss of AC power and loss of the ultimate heat sinks. The INPRO basic principle on defence in depth is used in the evaluation.

1.1.1 Fukushima Event – March 11, 2011

On March 11, 2011, Japan suffered its highest recorded earthquake. A magnitude 9.0 earthquake struck off the eastern coast of Japan. The distance from the epicentre of the quake to the Fukushima Dai-ichi nuclear power station was approximately 180 km, with peak ground acceleration (PGA) of 0.56 g recorded in Unit 2. It caused an immediate loss of offsite power. Immediately after the earthquake, Units 1–3 shut down automatically, and emergency generators came online to control electronics and coolant systems. The earthquake also generated a series of large tsunami waves. The tsunami waves that hit the Fukushima Dai-ichi stations were 14–15 meters, much higher than had been considered in the plant design, and impacted both the normal and mitigating systems.

The Fukushima Dai-ichi plant comprised of six separate boiling water reactors (BWR) designed by General Electric (Units 1, 2 and 6), Toshiba (Units 3 and 5) and Hitachi (Unit 4), and operated by Tokyo Electric Power Company (TEPCO). At the time of the accident, Units 1, 2,

---

1 EC6 (Enhanced CANDU 6) is a registered trademark of Atomic Energy of Canada Limited (AECL), used under license by Candu Energy Inc.

2 (CANada Deuterium Uranium) is a registered trademark of Atomic Energy of Canada Limited (AECL), used under license by Candu Energy Inc.
and 3 were in operation, Unit 4 was defueled, and Units 5 and 6 were in cold shutdown for maintenance. In the hours and days that followed, Units 1, 2 and 3 experienced, according to assessments done by TEPCO, a core melt, with “damage and leakage suspected” in the Primary Containment Vessel (PCV). Hydrogen explosions destroyed the upper cladding of the buildings housing Units 1, 3 and 4, and damaged the Unit 2 primary containment, while multiple fires broke out in the Unit 4 building. The combination of the earthquake and tsunami at Fukushima exceeded the magnitude considered in the plant design for these external events.

The Fukushima Dai-ichi nuclear event demonstrated the importance of defence in depth features for beyond design basis events characterized by prolonged loss of AC power, loss of heat sinks and loss of emergency response capabilities. The INPRO criteria are selected for this evaluation to compare the capabilities of the EC6 design to those of the generic CANDU 6 plants to cope with prolonged loss of AC power, loss of heat sinks and loss of emergency response capabilities.

1.1.2 Fukushima Lessons Learned Applicability to INPRO Criteria for Innovations in Application of Defence-in-Depth (DID) Principle

Based on the ‘defence-in-depth’ principle, Table 1-1 below, identifies the INSAG objectives and the corresponding INPRO criteria pertaining to the key Fukushima Lessons Learned regarding the capabilities to cope with prolonged loss of AC power, loss of heat sinks and loss of emergency response capabilities. The Fukushima lessons learned have been summarized in the table, for simplification, based on Fukushima lessons learned reports that include the following: IAEA[2] [4], United Nations [5], Japanese Reports [6][7], ENSREG/EU[8], CNSC [9][10], USNRC [11], UK HSE [12], WANO and INPO [13][14].

Table 1-1: INSAG Objectives and INPRO Criteria Pertaining to Fukushima Lessons Learned

INPRO basic principle BP1(defence in depth): *Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations*

<table>
<thead>
<tr>
<th>DID Level</th>
<th>INSAG Objective</th>
<th>Innovation Direction</th>
<th>INPRO Criteria</th>
<th>Fukushima LL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prevention of abnormal occurrence and accidents</td>
<td>Enhance prevention by increased emphasis on inherently safe design characteristics and passive safety features, and by further reducing human actions in the routine operation of</td>
<td>More independence of levels from each other</td>
<td>UR1.1 Robustness: <em>Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Plant layout</td>
</tr>
<tr>
<td>DID Level</td>
<td>INSAG Objective</td>
<td>Innovation Direction</td>
<td>INPRO Criteria</td>
<td>Fukushima LL</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the plant.</td>
<td>CR1.1.1 robustness CR1.1.2 operation</td>
<td>should maintain ‘dry site’ concept, as well as physical separation and diversity (IAEA, Japanese Reports, UK HSE)</td>
</tr>
<tr>
<td>2</td>
<td>Control of abnormal operation and detection of failures.</td>
<td>Give priority to advanced control and monitoring systems with enhanced reliability, intelligence and the ability to anticipate and compensate abnormal transients.</td>
<td>UR1.2 Detection and interception: Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. CR1.2.1 I&amp;C and inherent characteristics CR1.2.2 grace period CR1.2.3 inertia</td>
<td>N/A to Fukushima lessons learned (AOO conditions)</td>
</tr>
<tr>
<td>3</td>
<td>Control of accidents within the design basis.</td>
<td>Achieve fundamental safety functions by optimized combination of active &amp; passive design</td>
<td>UR1.3 Design basis accidents: The frequency of occurrence of accidents should be reduced,</td>
<td>Review Design Basis and plant layout for infrequent and complex</td>
</tr>
<tr>
<td>DID Level</td>
<td>INSAG Objective</td>
<td>Innovation Direction</td>
<td>INPRO Criteria</td>
<td>Fukushima LL</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>4</td>
<td>Control of severe plant conditions, including prevention and</td>
<td>Increase reliability and capability of systems to control and monitor complex accident sequences; decrease expected frequency of severe</td>
<td>consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.</td>
<td>combinations of external events: confirm or amend Design Basis Accident List (IAEA, United Nations Report, Japanese Reports, EU Stress Test Reports, CNSC, USNRC, UK HSE) Assess and mitigate the risk of hydrogen explosion (IAEA, Japanese Reports, USNRC, UK HSE) Confirm long-term cooling of spent fuel pools, and adequate monitoring provisions, in case of loss of power (IAEA, Japanese Reports, EU Stress Test, UN, UK HSE, INPRO) Provide simple diverse alternative sources of power and water, in a safe location (IAEA, UN,</td>
</tr>
</tbody>
</table>

---

Copyright © 2013 Candu Energy Inc. All rights reserved. Unauthorized use or reproduction is prohibited.
<table>
<thead>
<tr>
<th>DID Level</th>
<th>INSAG Objective</th>
<th>Innovation Direction</th>
<th>INPRO Criteria</th>
<th>Fukushima LL</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Mitigation of the consequences of severe accidents.</td>
<td>plant conditions; e.g., for reactors, reduce severe core damage frequency by at least one order of magnitude relative to existing plants and designs, and even more for urban-sited facilities.</td>
<td>due to internal events should be reduced. Should a release occur, the consequences should be mitigated CR1.4.1 frequency of release into containment</td>
<td>Japanese Reports, CNSC, USNRC, UK HSE, INPRO) Effective use of probabilistic safety assessment (PSA) in risk management (UK)</td>
</tr>
<tr>
<td>5</td>
<td>Mitigation of radiological consequences of significant releases of radioactive materials.</td>
<td>Avoid the necessity for evacuation or relocation measures outside the plant site.</td>
<td>UR1.5 Release into environment: A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose. CR1.5.1 frequency of release to environment</td>
<td>Evaluate need for containment venting provisions (Japanese Reports, USNRC, UK HSE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UR1.6 Independence of DID levels: An assessment should be performed for an INS to demonstrate that the different levels of defence-in-depth are met and are more</td>
<td>Independence discussed under UR 1.3, CR 1.3.4 barriers, supported by CR 1.4.1 and CR 1.5.1.</td>
</tr>
</tbody>
</table>
1.1.3 Selection of Basic Principle 1: Defence in Depth

Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. The INPRO methodology applies the IAEA safety fundamentals and requirements in measuring the protection and prevention measures in the defence in depth levels. The defence in depth strategy is implemented, utilizing several levels of protection and successive physical barriers to prevent radioactive releases to the environment. It is emphasized that optimization of the balance among different levels of defence is important. The Fukushima event highlighted the importance of the defence in depth strategy in strengthening a design to be more flexible in responding to system challenges by providing adequate diversity and redundancy for the essential safety functions.

1.1.3.1 Selection of criterion CR 1.1.1 Robustness of Design

- **Indicator IN1.1.1:** Robustness of design (simplicity, margins)
- **Acceptance Limit AL1.1.1:** New designs (EC6) should be superior to existing design in at least some aspects of robustness.

**Evaluation Parameter EP1.1.1.1:** Margins of Design
The objective of Level 1 defence in depth is for ‘prevention of abnormal operation and failures’ by providing ‘adequate margins in the design of systems and plant components, including robustness and resistance to accident conditions, in particular aimed at minimizing the need to take measures at Level 2 and Level 3’ [23].

The term ‘margin’ corresponds to the difference between a design limit and the actual design value of a safety related parameter, whereby an increase in design margins will increase the robustness of a design. The importance of conservatism in design margins to prevent cliff-edge effects from overtopping of the protection measures, emerged as a fundamental lessons learned. A ‘cliff edge’ is defined as ‘an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input’ [24]. The Fukushima plants were not able to withstand the consequences of tsunami heights greater than those estimated in the design basis, leading to a cliff edge effect, which subsequently resulted in core melt.

**Conclusion 3: There were insufficient defence-in-depth provisions for tsunami hazards.**

In particular, because failure of structures, systems and components (SSCs) when subjected to floods are generally not incremental, the plants were not able to withstand the consequences of tsunami heights greater than those estimated, leading to cliff edge effects’ [2]

**Lesson 1:** ‘..plant layout should be based on maintaining a ‘dry site concept’, where practicable, as a defence-in-depth measure against site flooding as well as physical separation and diversity of critical safety systems’ [2]

‘ensure the independence and diversity of safety systems so that common cause failures can be adequately addressed and the reliability of safety functions can be further improved’ [6]

Following the Fukushima event, the EC6 design was reassessed to ensure there are sufficient conservative margins to prevent ‘cliff edge’ effects. With respect to margins, the evaluation assesses subcriticality margins, safety margins for reactor shutdown, heat sink margins, containment leak tightness and integrity margins, seismic margins and flood margins.

**EP1.1.1.5: Redundancy of systems**

The principle of redundancy in design, improves safety system reliability to control abnormal operating conditions and detection of failures; Level 2 defence in depth, as well as controlling accidents within the design basis, Level 3 defence in depth. The design principles of redundancy, segregation and diversification provide a high degree of protection against potential functional failures. The combination of the massive earthquake and subsequent tsunami at
Fukushima challenged the ability to ensure subcriticality, to provide adequate heat sinks, to maintain containment integrity and to provide effective accident management. An important lesson learned was to ensure sufficient diversity and redundancy in the protection layers for prevention of accidents;

‘With the consideration to prevent and mitigate Beyond Design Basis Accident especially caused by extreme natural hazards, diversity of the ultimate heat sink are important means to ensure the robustness of a design, and additional attention should be paid to diversity in new NPP designs’[2]

Lesson 9: Particularly in relation to preventing loss of safety functions, the robustness of defence-in-depth against common cause failure should be based on providing adequate diversity (as well as redundancy and physical separation) for essential safety functions[2]

1.1.3.2 Selection of criterion CR 1.1.2 Operation

- Indicator IN1.1.2: High quality of operation
- Acceptance Limit AL1.1.2: new designs (EC6) should be superior to existing design in at least some of the operational aspect, such as availability/capability of plant

Evaluation Parameter EP1.1.1.1: availability/capability of plant

Plant availability/capability is adversely affected by equipment failures that cause forced outages and discovery of gaps in protection against external hazards for equipment needed to perform the fundamental safety functions.

Plant availability/capability is increased by

- Eliminating single points of vulnerability through increased reliability and redundancy for plant equipment whose failures cause forced outages, and
- Increasing protection against external hazards for plant equipment that are needed to ensure the safety functions.

‘At Fukushima Dai-ichi they were presented with a more or less complete prolonged loss of electrical power, compressed air and other services, with little hope of immediate outside assistance, and having to work in darkness with almost no instrumentation and control systems to secure the safety of six reactors, six nuclear fuel pools, a common fuel pool and dry cast storage facilities’[2]

At the Fukushima Dai-ichi plant, misunderstanding regarding the status and control of core cooling systems may have adversely affected decision-making and prioritisation during the first few days of the event. This item was highlighted in the IAEA missions report, and more explicitly by the recent INPO Fukushima Addendum report;

Lesson 5: Emergency Response Centres should have available as far as practicable essential safety related parameters based on hardened instrumentation and lines such as coolant levels,
containment status, pressure, etc., and have sufficient secure communication lines to control rooms and other places on-site and offsite[2]

Lesson Learned: Ensure that, as the highest priority, core cooling status is clearly understood and that changes are controlled to ensure continuity of core cooling is maintained. If core cooling is uncertain, direct and timely action should be taken to establish conditions such that core cooling can be ensured [25]

1.1.3.3 Selection of criterion CR 1.3.3 Safety features

- Indicator IN1.3.3: Reliability of engineered safety features (probability of failure of engineered safety system per demand and unit)
- Acceptance Limit AL1.3.3: new designs (EC6) in case of DBA should show equal or higher reliability than the reference CANDU 6 plants.

The strategy for defence in depth is two fold: first, to prevent accidents and second, if prevention fails, to limit the potential consequences of accident and to prevent their evolution to more serious conditions, as was experienced at the Fukushima Dai-ichi nuclear plant on March 11, 2011. The levels of defence include barriers to limit the progression to the next level, with the aim to fulfil the fundamental safety functions;

(1) Control of the reactivity;
(2) Removal of heat from the core;
(3) Confinement of radioactive materials, shielding against radiation;
(4) control of planned radioactive releases, as well as limitation of accidental radioactive releases and
(5) monitoring

Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled. Safety systems and their support systems must be designed to perform their safety functions with a high degree of reliability. This is achieved through the use of redundancy, diversity, separation, testability and application of high quality assurance standards and technical specifications. The Fukushima event highlighted the importance of ensuring that safety functions are available to perform when needed:

Lesson 9: Particularly in relation to preventing loss of safety functions, the robustness of defence-in-depth against common cause failure should be based on providing adequate diversity (as well as redundancy and physical separation) for essential safety functions [2]

‘ensure the independence and diversity of safety systems so that common cause failures can be adequately addressed and the reliability of safety functions can be further improved.’[6]
1.1.3.4 Selection of criterion CR1.3.4 Barriers

- **Indicator IN1.3.4: Number of confinement barriers maintained**

  The design of engineered safety features should deterministically provide for continued integrity at least of one barrier (containing the radioactive material) following any DBA

- **Acceptable Limit AL1.3.4: deterministically, at least one remaining barrier against a release of fission products to the environment; or, probabilistically, a very low probability of failure of all barriers in the NES**

The Basic Safety Principles for Nuclear Power Plants (INSAG-3) [26] discusses the implementation of defence in depth centred on several layers of protection, including successive barriers that prevent the release of radioactive material to the environment. The objective of which are to

- Compensate for potential human and component failures;
- Maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves; and
- Protect the public and environment from harm in the event that these barriers are not fully effective.

On March 11, 2011, the barriers at the Fukushima Dai-ich plant failed to maintain their effectiveness to protect the plant, public and the environment. The lessons learned identified lack of sufficient defence in depth against external events, protection against radiological releases, redundancy of heat sinks and ensuring continuous control and monitoring.

**Lesson 1: There is a need to ensure that in considering external natural hazards:**

- the siting and design of nuclear plants should include sufficient protection against infrequent and complex combinations of external events and these should be considered in the plant safety analysis – specifically those that can cause site flooding and which may have longer term impacts;
- plant layout should be based on maintaining a ‘dry site concept’, where practicable, as a defence-in-depth measure against site flooding as well as physical separation and diversity of critical safety systems; and
- common cause failure should be particularly considered for multiple unit sites and multiple sites, and for independent unit recovery options, utilizing all on-site resources should be provided.[2]

**Lesson 5: Emergency Response Centres should have available as far as practicable essential safety related parameters based on hardened instrumentation and lines such as coolant levels, containment status, pressure, etc., and have sufficient secure communication lines to control rooms and other places on-site and off-site.**[2]
Lesson 6: Severe Accident Management Guidelines and associated procedures should take account of the potential unavailability of instruments, lighting, power and abnormal conditions including plant state and high radiation fields.\[2\]

Lesson 8: The risk and implications of hydrogen explosions should be revisited and necessary mitigating systems should be implemented.\[2\]

1.1.3.5 Selection of criterion CR1.3.5 Controlled state

- **Indicator IN1.3.5:** Capability of engineered safety features to restore the INS to a controlled state (without operator actions)
- **Acceptable Limit AL 1.3.5:** the engineered safety features are sufficient to reach a controlled state after a DBA based on automatic actions within a grace period of at least 8 hours

The Fukushima event highlighted the importance of operator interventions to ensure a stable state has been achieved and being maintained following an event. Fukushima Dai-ichi Units 1 to 3 were successfully shutdown and decay heat removal was established immediately following detection of the earthquake. However, the tsunami caused prolonged loss of AC power, a consequential loss of the ultimate heat sinks and loss of monitoring capability to guide operator actions. Restoration of the heat sinks and monitoring capability relied on operator interventions. Due to the lack of operational personnel and difficult work conditions following the Fukushima Dai-ichi event, demand on operator interventions should be kept to a minimum;

‘…analysis of accident sequences for long-term severe accidents. This should identify appropriate repair and recover strategies to the point at which a stable state is achieved…’\[12\]

‘…comprehensive requirements for minimum times before significant operator interventions are required. Such requirements would be commensurate with the type of intervention, for example, the need for offsite portable equipment to be brought onsite.’\[9\]

1.1.3.6 Selection of criteria CR 1.4.1 and CR1.5.1 Major release into containment and frequency of release to environment

**Releases into containment**

- **Indicator IN1.4.1:** Calculated frequency of major release of radioactive materials into the containment/confine ment based on frequency calculated for a highly degraded core.
- **Acceptability Limit AL 1.4.1:** The frequency is an order of magnitude less than for existing sites.

**Frequency of release to environment**
- **Indicator IN1.5.1:** Calculated frequency of a major release of radioactive materials to the environment:

- **Acceptability Limit AL1.5.1:** the frequency is well below $10^{-6}$ per unit-year or practically excluded by design

One of the key lessons highlighted in the Fukushima reviews was to ensure adequate provisions are in place for maintaining containment integrity to prevent uncontrolled releases to the public and environment:

> 'The knowledge of the radioactive releases to the environment is necessary for the correct understanding of the event and for the decision making on countermeasures to protect the population.' [2]

> ‘… re-evaluate the need for hardened vents for other containment designs, considering the insights from the Fukushima accident.’[11]

> ‘Effective use of probabilistic safety assessment (PSA) in risk management:
- actively and swiftly utilize PSA while developing improvements to safety measures including effective accident management measures based on PSA.’[6]

### 1.1.3.7 Selection of criterion CR 1.6.1 Independence of defence in depth

- **Indicator IN1.6.1:** Independence of different levels of DiD

- **Acceptance limit AL1.6.1:** Adequate independence is demonstrated through deterministic and probabilistic means and other analyses.

A governing principle of defence in depth is to provide successive layers of protection, which are as far as possible independent of each other and each of which is sufficient to prevent harm from occurring. A detailed safety analysis is the basis for determining the adequacy of these barriers.

> ‘Conclusion 3: There were insufficient defence-in-depth provisions for tsunami hazards. In particular:
- although tsunami hazards were considered both in the site evaluation and the design of the Fukushima Dai-ichi NPP as described during the meetings and the expected tsunami height was increased to 5.7 m (without changing the licensing documents) after 2002, the tsunami hazard was underestimated;
- thus, considering that in reality a ‘dry site’ was not provided for these operating NPPs, the additional protective measures taken as result of the evaluation conducted after 2002 were not sufficient to cope with the high tsunami run up values and all associated hazardous phenomena (hydrodynamic forces and dynamic impact of large debris with high energy);
- because failures of structures, systems and components (SSCs) when subjected to floods are generally not incremental, the plants were not able to withstand the consequences of tsunami heights greater than those estimated, leading to cliff edge effects; and
- severe accident management provisions were not adequate to cope with multiple plant failures.’[2]
2. SELECTION OF REFERENCE PLANT

2.1 Evolution of EC6 Design to CANDU 6

The EC6 design is chosen for the INPRO methodology because it is updated from the proven CANDU 6 plant with safety and operational improvements to meet the latest requirements for new NPP designs [15]. The generic CANDU 6 plant has been chosen as the reference plant based on the following:

- Proven and mature technology: Over 150 reactor years of combined safe operation in five countries around the world; Canada, Romania, Argentina, Korea and China.
- High availability/capability: Operating in five different countries with a lifetime capacity factors of approximately 90%.

Both the EC6 and CANDU 6 are medium sized pressurized heavy water reactors (PHWR), with a power output in the 700 MWe range. The design is based on natural uranium as fuel with heavy water (D₂O) as a moderator. The reactor is equipped with horizontal fuel channels inside a cylindrical calandria vessel, which is further enclosed within a concrete, light water filled calandria vault. There are two functionally separate heat transport loops, each serving one half of the reactor, with heavy water as the coolant, as shown in Figure 2-1. The loops can be isolated from each other under certain accident conditions. Each loop contains two pumps, two steam generators, two inlet headers and two outlet headers, and half the fuel channels in a ‘figure of eight’ arrangement, with interconnecting piping. The flow through adjacent fuel channels in the reactor core is bi-directional (in opposite directions). The fission heat produced from the natural uranium fuel is transferred to the light water in the secondary side of the steam generators to produce steam, which drives the turbine generators to produce electricity. While retaining the basic features of the CANDU 6 plants, the EC6 reactor incorporates innovative features to enhance safety, operation and performance.
2.1.1 Changes to the Original Design Basis

The licensing design basis of the CANDU 6 reactors is in compliance with the standards applicable at the time of original licensing, which varies between 1980s to 2000 among the CANDU 6 fleet. As a Canadian prerequisite to refurbishment, corresponding to the midlife of the reactor, integrated safety reviews (ISRs) have been performed for the CANDU 6 reactors to assess the current state of the plant and plant performance to determine the extent to which the plant conforms to modern standards and practices, and to identify any factors that would limit safe long-term operation [9]. The Canadian CANDU 6 plants have completed this assessment, which resulted in making some design changes. This included a reassessment for external hazards, including seismic hazard. A seismic margin assessment (SMA) is performed to assess the safety margin based on current Canadian Standards Association (CSA) requirements. Other design changes were done to address the generic safety issues identified for pressurized heavy water reactors [16] and other CANDU safety issues.
Furthermore, following the March 11, 2011 Fukushima-Daiichi event, regulators worldwide, including the CNSC, issued letters to licenses requesting immediate actions [9]. The objective was to review initial lessons learned from the event and report on implementation plans for short-term and long-term measures to address any significant gaps, pertaining to the following:

- Robustness of design basis and beyond design basis earthquakes and floods
- Fire protection, including concurrent fires
- Response to prolonged station blackout
- Robustness of spent fuel management systems
- Ability to manage hydrogen generation and release
- Ability to restore and maintain cooling to a damaged core
- Operator action for emergency response.

This subsequently resulted in Fukushima driven design changes implemented at the CANDU 6 plants. This INPRO assessment recognizes the above discussed drivers and design changes implemented at the current operating CANDU 6 plants worldwide when making the comparison against the EC6 design.

### 2.1.2 Comparison of CANDU 6 and EC6 Design

The following tables provide a general description of the design features of the Enhanced CANDU 6 (EC6) design and the generic CANDU 6 plants. A technical summary of the CANDU 6 design is provided in Appendix A and the technical summary for EC6 design is found on the Candu Energy Inc. website⁴. Table 2-1 and Table 2-2 illustrate the main differences in the systems between the CANDU 6 and EC6 design.

#### Table 2-1: General System Data of CANDU 6 in Comparison to EC6 Design

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design Characteristics</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reactor type</td>
<td></td>
<td>Horizontal Pressure tube</td>
<td>Horizontal Pressure tube</td>
</tr>
<tr>
<td>Coolant</td>
<td></td>
<td>Pressurized D₂O</td>
<td>Pressurized D₂O</td>
</tr>
<tr>
<td>Moderator</td>
<td></td>
<td>D₂O</td>
<td>D₂O</td>
</tr>
<tr>
<td>Fuel</td>
<td></td>
<td>Natural Uranium</td>
<td>Natural Uranium</td>
</tr>
<tr>
<td>Gross Electrical Power Output</td>
<td>MW(e)</td>
<td>728</td>
<td>740</td>
</tr>
<tr>
<td>Number of Fuel Channels (Pressure tubes and calandria tubes)</td>
<td>380</td>
<td>380</td>
<td></td>
</tr>
<tr>
<td>Channel length</td>
<td>m</td>
<td>5.944</td>
<td>5.944</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel Bundle Design</td>
<td>37 element</td>
<td>37 element</td>
<td></td>
</tr>
<tr>
<td>Bundles per Fuel Channel</td>
<td>12</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Pressure Tube (PT) wall thickness</td>
<td>inches</td>
<td>0.165 (4.19 mm) (minimum)</td>
<td>0.193 (4.9 mm) (average)</td>
</tr>
<tr>
<td>PT Weight (average)</td>
<td>kg</td>
<td>61.5</td>
<td>69</td>
</tr>
<tr>
<td>Calandria Tube (CT) thickness</td>
<td>inches</td>
<td>0.054 (1.37 mm)</td>
<td>0.060 (1.52 mm)</td>
</tr>
<tr>
<td>Average Coolant Temperature</td>
<td>°C</td>
<td>288</td>
<td>288</td>
</tr>
<tr>
<td>Average Moderator Temperature</td>
<td>°C</td>
<td>69</td>
<td>69</td>
</tr>
</tbody>
</table>

### Reactivity Control

<table>
<thead>
<tr>
<th>Main Method</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>On power refuelling and light water zone control compartments</td>
<td>On power refuelling and light water zone control compartments</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moderator Poison Addition</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Boric acid addition to moderator</td>
<td>Boric acid addition to moderator</td>
<td></td>
</tr>
</tbody>
</table>

### Shutdown

<table>
<thead>
<tr>
<th>SDS 1</th>
<th>Spring-assisted, gravity accelerated, shutoff rods Moderator Poison System after Xe-135 decayed (not seismically qualified)</th>
<th>Spring-assisted, gravity accelerated, shutoff rods Moderator Poison System after Xe-135 decayed (not seismically qualified) Supplemental Absorber Rods after Xe-135 decayed (seismically qualified)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDS 2</td>
<td>Gadolinium poison injection</td>
<td>Gadolinium poison injection</td>
</tr>
</tbody>
</table>

### Reactor Regulating System

<p>| Liquid Zone Control Units, CARs, Adjusters, Moderator Poison System | Liquid Zone Control Units, CARs, Adjusters, Moderator Poison System |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>CANDU 6</th>
<th>EC6</th>
<th>Supplemental Absorber Rods</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Mechanical Control Absorbers Rods (CARs)</td>
<td></td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td># of Adjusters</td>
<td></td>
<td>21</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td># of Liquid Zone Control Units</td>
<td></td>
<td>6 units with 14 zones</td>
<td>6 units with 14 zones</td>
<td></td>
</tr>
<tr>
<td># of Supplemental Absorber Rods</td>
<td></td>
<td>0</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td># of Shut-off Rods (SOR)</td>
<td></td>
<td>28</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td># of Poison Injection Nozzles</td>
<td></td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reactor Thermal Power Output</td>
<td>MW(th)</td>
<td>2061</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>Design Life</td>
<td>years</td>
<td>40</td>
<td>60</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2-2: Important Safety Features**

<table>
<thead>
<tr>
<th>Features</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containment Design Pressure</td>
<td>124 kPa (g) design pressure with dousing from Dousing Tank</td>
<td>400 kPa (g) design pressure with reserve water tank (RWT)</td>
</tr>
<tr>
<td>Containment Design</td>
<td>Epoxy liner with 0.5vol%/d leakage rate 124 kPa(g)</td>
<td>Includes a steel liner with 0.2vol%/d leakage rate at 400 kPa(g)</td>
</tr>
<tr>
<td></td>
<td>• Controlled leakage up to 235 kPa(g)</td>
<td>• Controlled leakage up to 600 kPa(g)</td>
</tr>
<tr>
<td>Containment Wall Thickness</td>
<td>1.07 m</td>
<td>1.5 m</td>
</tr>
<tr>
<td>Safety Systems</td>
<td>1. Shutdown System 1</td>
<td>1. Shutdown System 1</td>
</tr>
<tr>
<td></td>
<td>2. Shutdown System 2</td>
<td>2. Shutdown System 2</td>
</tr>
<tr>
<td></td>
<td>3. Emergency Core Cooling System (ECC)</td>
<td>3. Emergency Core Cooling System (ECC)</td>
</tr>
</tbody>
</table>

Severe accident management engineering features

- Water inventory in reactor
  - 3 000 Mg of water available for passive heat removal:
    - 2056 Mg in Dousing Tank
    - 215 Mg HPECC
  - 3 000 Mg of water available for passive heat removal:
    - 2056 Mg in RWT
    - 215 Mg HPECC
    - 240 Mg D₂O in calandria

---

4 For CANDU 6 plant, this is the EWS designated as a safety support system
<table>
<thead>
<tr>
<th>Features</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- 240 Mg D₂O in calandria vessel</td>
<td>- 520 Mg H₂O in calandria vault</td>
</tr>
<tr>
<td></td>
<td>- 520 Mg H₂O in calandria vault</td>
<td>- 190 D₂O in HTS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control of reactivity</td>
<td>Light water make-up to Calandria vault</td>
<td>Light water make-up to Calandria vessel</td>
</tr>
<tr>
<td>Extended Cooling Capability</td>
<td>*Make-up to the calandria vault via portable water source for some CANDU 6 plants</td>
<td>-Severe Accident Recovery and Heat Removal System (SARHRS) to extend cooling makeup capability. Cooling for the SARHRS heat exchanger is by a dedicated SARHRS cooling water pump, using inventory from the on-site water supply (once-through cooling).</td>
</tr>
<tr>
<td>Shielding against radiation</td>
<td>Containment wall (1.07 m)</td>
<td>Containment wall (1.5 m)</td>
</tr>
<tr>
<td>Control of planned radioactive releases, as</td>
<td>*Emergency Filtered Containment Venting Systems added to some CANDU 6</td>
<td>-Emergency Filtered Containment Venting System, initiated above containment design pressure</td>
</tr>
<tr>
<td>well as limitation of accidental radioactive releases</td>
<td>plants, initiated above containment design pressure</td>
<td>-33 PARs</td>
</tr>
<tr>
<td></td>
<td>*33 Passive Autocatalytic Recombiners (PARs) added to some CANDU 6 plants</td>
<td>-RWT low flow spray for containment heat removal and pressure suppression</td>
</tr>
<tr>
<td>Means of monitoring the status of the plant</td>
<td>Safety Monitoring System in MCR and SCA</td>
<td>Safety Monitoring System in MCR, SCR and Emergency Support Centre</td>
</tr>
<tr>
<td>Seismic Design</td>
<td>Up to 0.2 g peak ground acceleration</td>
<td>Up to 0.3 g peak ground acceleration</td>
</tr>
<tr>
<td>Control Room Availability during Seismic</td>
<td>Secondary Control Room</td>
<td>Main Control Room (MCR)</td>
</tr>
<tr>
<td>Design Basis Event (DBE)</td>
<td></td>
<td>Secondary Control Room (SCR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardened Emergency Support Centre</td>
</tr>
<tr>
<td>Diesel Generators</td>
<td>2 Standby DGs per unit; 2 EPS, common for 2 units</td>
<td>2 Standby DG per unit; 2 Emergency Power System (EPS) per unit plus 1 common for maintenance back-up</td>
</tr>
</tbody>
</table>
Table 2-3 identifies the variation among the two designs for external natural events considered in the design basis, in line with regulatory requirements. The proceeding sections will demonstrate the increased safety features incorporated into the EC6 design.

### Table 2-3: External Natural Events Design Basis

<table>
<thead>
<tr>
<th>Event</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>-Original design basis earthquake applied a return frequency of $10^{-3}$ years; reassessments used $10^{-4}$ years where the HCLPF exceeds 0.3 g PGA.</td>
<td>-Return frequency of $10^{-4}$ years, as per CSA standard N289.1-08; Seismic Margin Assessment measured in terms of High Confidence of Low Probability of Failure (HCLPF) which exceeds 0.5g PGA (1.67 x DBE).</td>
</tr>
<tr>
<td></td>
<td>-Design Basis Earthquake (DBE): seismic level up to 0.2 g Peak Ground Acceleration (generic design)</td>
<td>-DBE seismic level up to 0.3 Peak Ground Acceleration (Horizontal peak ground acceleration (PGA) at DBE level is 0.21 g for CSA based spectra and 0.3g for Uniform Hazard Spectra (UHS))</td>
</tr>
<tr>
<td>External Flood</td>
<td>-Return frequency of $10^{-4}$ years if sufficient data; otherwise use maximum observed flood plus margin</td>
<td>-Return frequency of $10^{-4}$ years if sufficient data; otherwise use maximum observed flood plus margin</td>
</tr>
<tr>
<td></td>
<td>-Design Basis Flood: Dry site concept</td>
<td>-Design Basis Flood: Dry site concept – 0.60 m above max. ground water level</td>
</tr>
<tr>
<td>Tornado</td>
<td>-Return frequency up to $10^{-6}$ per year.</td>
<td>-Return frequency of $10^{-7}$ per year.</td>
</tr>
</tbody>
</table>
Event | CANDU 6 | EC6
--- | --- | ---
-Design Basis Tornado (F4 on Fujita Scale Classification of Tornado Wind Intensity):  
  • Maximum wind speed: 420 km/h;  
  • Translational wind speed: 92 km/h | -Design Basis Tornado (F5 on Fujita Scale Classification of Tornado Wind Intensity):  
  • Maximum wind speed: 483 km/h;  
  • Translational wind speed: 97 km/h |
3. INPRO SAFETY ASSESSMENT

3.1 Basic Principle 1: Defence-in-depth

*Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.*

The INPRO methodology applies the IAEA safety fundamentals and requirements in measuring the protection and prevention measures in the defence in depth levels. For each INPRO basic principle, requirements are identified with corresponding indicators and acceptance criteria.

3.1.1 User Requirement UR1.1 – Robustness

*Installations of an innovative NEW should be more robust relative to existing designs regarding system and component failure as well as operation.*

INPRO has defined four criteria, CR 1.1.1.1 to CR 1.1.1.4 for each indicator, IN 1.1.1 to IN 1.1.4. CR.1.1.1 on robustness, using the Evaluation Parameter of margins of design (EP 1.1.1.1) and redundancy of systems (EP 1.1.1.5); CR.1.1.2 on operation, using the Evaluation Parameter of availability and capability of plant, are deemed to be most applicable to Fukushima lessons learned.

3.1.1.1 Assessment against criterion CR1.1.1 Robustness

- **Indicator IN1.1.1:** *Robustness of design (simplicity, margins)*
- **Acceptance Limit AL1.1.1:** New designs (EC6) should be superior to existing design in at least some aspects of robustness.

3.1.1.1.1 Margins of Design

a) **Evaluation Parameter EP1.1.1.1:** *margins of design*

The EC6 design has incorporated design changes to improve safety margins for subcriticality, shutdown, containment leak tightness and integrity, seismic and flood margins, thereby strengthening the defence in depth layers.

3.1.1.1.1 Improved Subcriticality Margins

The CANDU 6 and EC6 design have maintained CANDU separation philosophy by strict separation of control and safety systems. In addition to the Reactor Regulating System (RRS), the CANDU designs employ two engineered independent shutdown systems, each individually capable of shutting down the reactor for all design basis accidents. The RRS includes liquid zone control compartments, mechanical absorbers rods, adjuster rods, moderator poison system and Supplemental Absorber Rods (SORs) for reactivity control. Shutdown System 1 (SDS1) consists of spring assisted gravity operated shutoff rods which fall into the moderator between the rows of channels. The non-seismically qualified moderator poison system is used to add
Boric acid to the D₂O moderator to compensate for the decay of transient fission product poisons to supplement SDS1. The set of 10 seismically qualified SARs are also available for to compensate for the decay of transient fission product poisons to supplement SDS1. Shutdown System 2 (SDS2) consists of liquid absorber injection into the moderator through horizontal perforated tubes. Both achieve fast (< 2 seconds) and automatic shutdown. The EC6 design has improved the shutdown margin over the CANDU 6 that is attributed to an optimization in the location and performance of the shutoff rods; the number of shutdown rods (SORs) have increased from 28 to 32 to achieve an improved subcriticality margin (reactivity depth of -30 mk for NO and AOO conditions), as well with the addition of an acceleration spring. The EC6 design contains 32 SORs with an additional 10 Supplemental Absorber Rods (SOR-type units) located in the reactivity mechanism deck vacancies previously occupied by adjuster rods in the reference CANDU 6 plants (21 in CANDU 6 and 11 in EC6), as presented in Table 3-1.

Each of the two shutdown systems provides, independently, sufficient negative reactivity margin to shut down the reactor under all reactor conditions, including that of maximum excess reactivity.

**Table 3-1: CR1.1.1 Evaluation for subcriticality design margins**

<table>
<thead>
<tr>
<th>Shutdown Design</th>
<th>Unit</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDS 1</td>
<td>Spring-assisted, gravity accelerated, shutoff rods (SORs) Moderator Poison System after Xe-135 decayed (not seismically qualified)</td>
<td>Spring-assisted, gravity accelerated, shutoff rods (SORs) Moderator Poison System after Xe-135 decayed (not seismically qualified)</td>
<td>Supplemental Absorber Rods after Xe-135 decayed (seismically qualified)</td>
</tr>
<tr>
<td>SDS 2</td>
<td>Gadolinium poison injection</td>
<td>Gadolinium poison injection</td>
<td></td>
</tr>
<tr>
<td>Reactor Regulating System</td>
<td>Liquid Zone Control Units, Control Absorber Rods, Adjusters, Moderator Poison System</td>
<td>Liquid Zone Control Units, Control Absorber Rods, Adjusters, Moderator Poison System</td>
<td>Liquid Zone Control Units, Control Absorber Rods, Adjusters, Moderator Poison System, Supplemental Absorber Rods</td>
</tr>
<tr>
<td>Liquid Zone Control Units</td>
<td>6 units with 14 zones</td>
<td>6 units with 14 zones</td>
<td></td>
</tr>
<tr>
<td># of Mechanical Control Absorbers Rods (CAR)</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
### 3.1.1.1.2 Improved Safety Margins

The pressure tube creep for the EC6 design has been reduced, by increasing the pressure tube (PT) thickness by 12%, to achieve a safety margin improvement associated with the loss of coolant accident (LOCA) safety margin for the EC6 design over the CANDU 6 plants. Reducing the pressure tube creep for EC6 results in a smaller positive coolant void reactivity (CVR) and, therefore, reduces the positive reactivity inserted during a LOCA, as presented in Table 3-2. The calandria tube (CT) thickness has also been increased in the EC6 design for added robustness and longer life.

### Table 3-2: CR1.1.1 Evaluation for improved safety margins

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design Characteristics</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Fuel Channels</td>
<td></td>
<td>380</td>
<td>380</td>
</tr>
<tr>
<td>Channel length</td>
<td>m</td>
<td>5.944</td>
<td>5.944</td>
</tr>
<tr>
<td>Fuel Bundle Design</td>
<td></td>
<td>37 element</td>
<td>37 element</td>
</tr>
<tr>
<td>Number of Pressure Tubes (PT)</td>
<td></td>
<td>380</td>
<td>380</td>
</tr>
<tr>
<td>PT Length trimmed for installation (approximate)</td>
<td>m</td>
<td>6.30</td>
<td>6.30 (20 ft 8 in)</td>
</tr>
<tr>
<td>PT Weight (average)</td>
<td>kg</td>
<td>61.5</td>
<td>69</td>
</tr>
<tr>
<td>PT wall thickness</td>
<td>inches</td>
<td>0.165 (4.19 mm)</td>
<td>0.193 (4.9 mm) (average)</td>
</tr>
<tr>
<td>Calandria Tube (CT) thickness</td>
<td>inches</td>
<td>0.054 (1.37 mm)</td>
<td>0.060 (1.52 mm)</td>
</tr>
<tr>
<td><strong>Reactivity Characteristics</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coolant Void Reactivity</td>
<td>$</td>
<td>~ 3.3</td>
<td>~ 3</td>
</tr>
<tr>
<td>(Limit of Operating Envelope)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peak positive reactivity inserted during LOCA</td>
<td>$</td>
<td>~ 0.9</td>
<td>~ 0.61</td>
</tr>
</tbody>
</table>
3.1.1.1.1.3 Improved Containment Design Margin

One of the key lessons learned from the Fukushima accident is maintaining containment integrity and limiting radiation releases following a severe accident, such as a prolonged station blackout or loss of ultimate heat sinks. The EC6 design has made a number of improvements to the safety margin for containment performance to enhance protection against external events, both natural hazards and malevolent acts over the CANDU 6 plants.

The reactor building consists of the containment structure and the internal structure. The design pressure for the EC6 containment structure has been increased to 400 kPa (g) versus 124 kPa (g) for the CANDU 6 plants. The 400 kPa (g) design includes a design margin relative to the maximum pressure resulting from a main steam line break event, in line with international approach [17]. A comparison between containment design margins and pressures in the two designs is presented in Figure 3-1.

![Figure 3-1: Containment Design Margin](image-url)
The EC6 containment structure consists of a prestressed concrete cylindrical perimeter wall, with a torispherical dome, ring beam, and conventionally reinforced concrete base slab. A steel liner plate is provided on the entire inside surface of the containment structure, to ensure that leak-tightness is within acceptable limits and prevent spalled concrete to be generated as a result of an external impact. The CANDU 6 containment structure is designed for a test acceptable leakage rate of 0.5% of the containment free air volume per 24 hours at 124 kPa(g). The EC6 design has a more leak tight containment, providing a leakage rate of 0.2% volume per day at 400 kPa(g), due to a steel liner and testable penetrations. The EC6 containment design contributes to reduced radioactive releases from severe accidents and allows sufficient time for the implementation of off-site emergency procedures.

The thickness of the containment structure is 1.5 m, to meet the requirements for radiation shielding, missile protection, aircraft crash, and fire protection, as compared to 1.07 m for the CANDU 6 plants.

The EC6 airlocks employ dual solid face type seals, rather than the inflatable seals in the CANDU 6 plants, to enable the EC6 containment to withstand higher containment pressure before failure of the airlock seals could occur.

Reinforcing steel is provided in the EC6 containment structure, in both directions, to resist bending moments, shear, and/or a portion of membrane forces in addition to prestressed cables. Reinforcing steel is also provided to control crack propagation due to heat of hydration, shrinkage, design loads, and seasonal temperature variations. Additional reinforcing steel bars are provided around penetrations and at discontinuities, to resist local moments and shear, and to meet the requirements for local stress concentrations.

A protective layer of refractory concrete is provided on top of the EC6 calandria vault floor to delay molten corium interaction with structural concrete, slow down the rate of production of non-condensable gasses, and hence reduce the rate of containment pressurization in the event that a severe accident progresses beyond the in-vessel stage to the ex-vessel stage.

Differences between the CANDU 6 and EC containment design are depicted in Table 3-3.

<table>
<thead>
<tr>
<th>Design Feature</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containment Design</td>
<td>-124 kPa (g) design pressure with dousing tank</td>
<td>-400 kPa (g) design pressure with Reserve Water Tank (RWT)</td>
</tr>
<tr>
<td></td>
<td>-1.07 m containment wall thickness</td>
<td>- 1.5 m containment wall thickness</td>
</tr>
<tr>
<td></td>
<td>-Inflatable airlock seals, good to 235 kPa(g)</td>
<td>-Solid face type airlock seals up to 600 kPa (g)</td>
</tr>
<tr>
<td>Leak Rate</td>
<td>Epoxy liner with 0.5%/d leakage rate</td>
<td>Steel liner with 0.2%/d leakage rate</td>
</tr>
</tbody>
</table>
3.1.1.1.4 Improved Seismic Margin

The EC6 design applies the seismic design methodology in CSA standard N289.1-08 [18], and uses the design basis earthquake with a probability of exceedance of one in ten thousand years. The EC6 design also improves robustness against seismic events to avoid cliff-edge effects for beyond design basis events by applying the seismic margin methodology in EPRI NP-6041-SL [19].

The CANDU 6 plants used the seismic design methodology in the CSA standard N289.1-80 [18][20][21] whereby the structures, systems and components are designed to sustain the most severe effects of earthquakes that have a probability of being exceeded at a given site of one in one thousand years. The seismic safety functions, which must be maintained during and after a seismic event, to limit the release of radioactivity are:

- Control of the reactivity: ability to shut the reactor down and maintain it in a safe shutdown condition. Note that nuclear criticality in the spent fuel bay is not a safety concern, because the fissile content in the spent fuel is less than that of natural uranium.
- Removal of heat from the core and spent fuel.
- Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.
- Monitor capability to perform safety control and monitoring functions.

Grouping Philosophy

The seismic design philosophy of the CANDU 6 plants is consistent with the plant overall safety design philosophy where all plant systems are assigned to one of two separated, independent and redundant groups. The Group 1 and Group 2 systems and components are functionally and physically separated from each other, to the extent that no component failures in one group would impair the capability of the other group to perform its safety functions, as illustrated in Table 3-4. This grouping approach maximizes protection against common cause events such as earthquakes and minimizes physical and functional cross connections between the two groups.

Table 3-4: CR1.1.1 Grouping Philosophy & Safety Function

<table>
<thead>
<tr>
<th>Safety Function</th>
<th>Group 1 System</th>
<th>Group 2 System</th>
</tr>
</thead>
</table>
| Control – Reactor Shutdown | • Reactor Control System  
|                         | • Shutdown System 1                                      | • Shutdown System 2                                       |
| Cool - Remove Heat         | • Heat Transport System  
|                          | • Steam & Feedwater System  
|                          | • Shutdown Cooling  
|                          | • Emergency Core                                           | • Emergency Water System – CANDU 6  
|                          |                                                            | • EHRS – EC6                                               |
Cooling

| Contain Radioactivity | • Moderator piping | • Containment |
| Containment Monitor  | • Main Control Center | • Secondary Control Center |

Each group can independently shut down the plant, remove decay heat, and monitor/control essential safety functions. The systems in each group are designed to be independent from each other and physically separate from each other to the extent practicable.

**Design Earthquake Levels**

Based on the CSA N289.1-80 [18], for the design and qualification of SQ structures, systems and components, two design earthquake levels are used to provide assurance of meeting the safety functions during an earthquake; design basis earthquake (DBE) and site design earthquake (SDE). For CANDU 6, the DBE corresponds to an engineering representation of an earthquake with a frequency of occurrence of once in 1000 years, while the SDE corresponds to an engineering representation of an earthquake with a frequency of occurrence not greater than once in 100 years. The CANDU 6 plants are designed to withstand an earthquake, based on the ‘design basis earthquake’ (DBE) of 0.2 g peak ground acceleration. The EC6 is designed to meet 0.3 g peak ground acceleration (PGA), based on an earthquake with a frequency of occurrence of one in 10 000 years, as per CSA N289.1-08. A Probabilistic Safety Assessment (PSA) is adopted for evaluating seismic induced risk based on an event/fault tree approach to delineate the accident sequence. The objective of the seismic margin assessment is to demonstrate conservative margin beyond the DBE level to withstand a seismic event larger than DBE, measured in terms of High Confidence of Probability of Failure (HCLPF), which represents with a 95% confidence, that the probability of failure of a component or structure will not exceed 5%. Table 3-5 shows the comparison of the HCLPF values for the CANDU 6 plants and EC6 design.

**Table 3-5: CR1.1.1 Seismic Design**

<table>
<thead>
<tr>
<th>Event</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>-Original design basis earthquake applied a return frequency of $10^{-3}$ years; reassessments used $10^{-4}$ where the HCLPF exceeds 0.3 g PGA.</td>
<td>-Return frequency of $10^{-4}$ years, as per CSA standard N289.1-08; Seismic Margin Assessment measured in terms of High Confidence of Low Probability of Failure (HCLPF) which exceeds 0.5 g PGA ($1.67 \times$ DBE).</td>
</tr>
</tbody>
</table>
Design Basis Earthquake (DBE): seismic level up to 0.2 g Peak Ground Acceleration (generic design)

-DBE seismic level up to 0.3 g Peak Ground Acceleration (Horizontal peak ground acceleration (PGA) at DBE level is 0.21 g for CSA based spectra and 0.3 g for Uniform Hazard Spectra (UHS))

Table 3-6 shows the seismic improvements for the EC6 design, as compared to the generic CANDU 6 plants, pertaining to the fundamental safety functions.

Table 3-6: CR1.1.1 Seismic Safety Function Capability

<table>
<thead>
<tr>
<th>CANDU 6</th>
<th>EC6 Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control - Reactor Shutdown</td>
<td></td>
</tr>
<tr>
<td>• 28 seismically qualified SORs for SDS1</td>
<td>• 32 seismically qualified SORs for SDS1</td>
</tr>
<tr>
<td>• 6 seismically qualified liquid poison injection tanks for SDS2</td>
<td>• 6 seismically qualified liquid poison injection tanks for SDS2</td>
</tr>
<tr>
<td>• 10 seismically qualified Supplemental Absorber Rods for RRS to prevent recriticality after transient fission product poisons have decayed when using SDS1</td>
<td></td>
</tr>
</tbody>
</table>

Cool - Remove Decay Heat

<table>
<thead>
<tr>
<th>CANDU 6</th>
<th>EC6 Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Seismically qualified Heat Transport System pressure boundary</td>
<td></td>
</tr>
<tr>
<td>• Seismically qualified Emergency Water Supply system to the steam generators and ECC heat exchanger.</td>
<td></td>
</tr>
<tr>
<td>• Seismically qualified source of feedwater from the dousing tank to the steam generators</td>
<td></td>
</tr>
<tr>
<td>• ECC system is qualified to a Design Basis Earthquake</td>
<td></td>
</tr>
<tr>
<td>• 2 seismically qualified EPS, common for the two units.</td>
<td></td>
</tr>
<tr>
<td>• Added emergency mitigating equipment, e.g., mobile diesel generators and water</td>
<td></td>
</tr>
<tr>
<td>• Seismically qualified Heat Transport System pressure boundary</td>
<td></td>
</tr>
<tr>
<td>• Seismically qualified Group 2 Emergency Heat Removal System (EHRS) is provided, supported by seismically qualified Group 2 electrical power, which initially uses gravity-driven water from the Reserve Water tank (RWT) to provide make up to the steam generators. In the long term, this system draws water from a reservoir or nearby body of water. The control logic to automatically depressurize the steam generators has been seismically qualified so that depressurization of the steam</td>
<td></td>
</tr>
</tbody>
</table>
Provisions for recharging batteries through mobile diesel generator stored on site added

- Seismically qualified emergency coolant injection system that caters for any small post-seismic leaks in the Heat Transport System.
- Seismically qualified shield cooling system (SCS) piping inside the reactor building to protect against possible draining of the end shield and the reactor vault and to retain the vault/end shield coolant inventory following a DBE.
- Increased capacity for seismically qualified firewater to address possibility for simultaneous fires at a station, across both units.
- Electrical power is provided from two independent emergency diesel generators that are seismically qualified.
- Redundant line of defence includes the SARHRS system with its own separated and SQed dedicated power supply that can remove heat. This is accomplished by refilling the reserve water tank with water from on-site cooling water source (lake or river).
- Seismically qualified 24 H UPS to power loads required for heat sinks
- Provisions for recharging batteries through seismically qualified mobile diesel generator stored on site.
- Emergency mitigating equipment, e.g., mobile diesel generators and water sources, stored on and off-site.

<table>
<thead>
<tr>
<th>Contain – limit the release of radioactive material</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Seismically qualified barriers: fuel sheath, pressure tubes, calandria tubes, and Heat Transport System pressure boundary.</td>
</tr>
</tbody>
</table>
- Seismically qualified containment system, including isolation
- Containment structures is seismically qualified to withstand the DBE loads combined with a reduced accident pressure, attributed to failure of piping or components that are not qualified and that may contain high energy.
- Seismically qualified spent fuel storage bay.
- *Fire water pipe connections to spent fuel bay and the reception bay have been upgraded to be seismically qualified in some CANDU 6 plants.*
- Seismically qualified Emergency Filtered Containment Venting Systems have been added to some CANDU 6 plants
- Seismically qualified igniters for hydrogen control for DBA conditions
- Seismically qualified PARs for hydrogen control after severe accident *(implemented or to be implemented in CANDU 6 plants)*

**Monitor** – perform essential safety related control and monitoring functions

<table>
<thead>
<tr>
<th>Monitor – perform essential safety related control and monitoring functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Seismically qualified Secondary Control Area (SCA) and associated control and monitoring systems.</td>
</tr>
<tr>
<td>- Main Control Room (MCR) and associated equipment are seismically qualified to the extent that operators are protected.</td>
</tr>
<tr>
<td>- Electrical power is provided from the two SQed EPS, common for the two units.</td>
</tr>
<tr>
<td>- SSCs which may pose a hazard to seismically qualified systems are seismically qualified. Structures that house and support these systems have a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitor – perform essential safety related control and monitoring functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Seismically qualified Secondary Control Area (SCA) and associated control and monitoring systems.</td>
</tr>
<tr>
<td>- MCR and associated equipment are seismically qualified such that operators have sufficient time to place the reactor in a safe shutdown condition.</td>
</tr>
<tr>
<td>- Electrical power is provided from 2 seismically qualified EPS per unit</td>
</tr>
<tr>
<td>- SSCs which may pose a hazard to seismically qualified systems are seismically qualified. Structures that house and support these systems have a</td>
</tr>
</tbody>
</table>
safety function to maintain their structural integrity during and following the DBE. (including reactor building, service building, secondary area, high pressure ECC structure).

- Seismically qualified route for the safe exit of the operator from the MCR to the SCA, and to any other seismically qualified equipment to which access is required during a DBE (i.e. Emergency power system diesel generators)
- Safety related control and monitoring capability provided in SCA
- Emergency mitigating equipment, e.g., mobile emergency support centre, added on-site for some CANDU 6 plants.

The EC6 design incorporates more seismic margin than the CANDU 6 plants by using 0.3 g PGA for the design basis earthquake, and providing additional features to perform the safety functions after a DBE.

### 3.1.1.1.5 Increased Flood Margin

The CANDU 6 plants are assessed for their capability to withstand both internally caused (i.e. pipe rupture) and externally caused flood hazards. The approach for CANDU 6 plants is to maintain a ‘dry site’ condition whereby an externally caused flood would not affect the systems and structures inside containment, which is designed to be sealed off from the outside. The elevation of the site for safety related equipment and structures is higher than the highest design basis flood level, refer to Table 3-7. Each site is evaluated to the probable maximum flood, waves, seiche, tsunami and/or surge and potential dam failure, based on site characteristics. In addition, protection against internal flooding due to component failure is provided by locating all equipment in the basement on platforms above the highest flood level.
Table 3-7: CR1.1.1 Design Basis Flood

<table>
<thead>
<tr>
<th>Event</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Flood</td>
<td>-Return frequency of $10^{-4}$ years if sufficient data; otherwise use maximum observed flood plus margin</td>
<td>-Return frequency of $10^{-4}$ years if sufficient data; otherwise use maximum observed flood plus margin</td>
</tr>
<tr>
<td></td>
<td>-Design Basis Flood: Dry site concept (ie. 0.50 m margin for heavy rain coincident with design basis flood [22])</td>
<td>-Design Basis Flood: Dry site concept using 0.60 m above max. ground water level</td>
</tr>
</tbody>
</table>

The EC6 is designed to ensure that all SSC’s important to safety that perform any safety function are protected against both internal and external flooding, as per new build requirements [15]. The EC6 design is protected from external flooding by maintaining a ‘dry site’ condition whereby the plant is built at a site grade level of +0.6 m above the design basis flooding level. The seismically qualified EPS battery and essential power distribution components and connections to facilitate utilization of emergency mitigating equipment are protected from external flooding.

With respect to severe meteorological events, all structures/buildings are required to have a roof drainage system. The EC6 design ensures that component failures resulting from internal flooding will not prevent safe shutdown of the plant or prevent mitigation of the flooding event. The EC6 design applies the CANDU 6 design philosophy for flood protection.

3.1.1.1.1.6 Increased Heat Sink Margin

The CANDU 6 plant has a number of systems to remove decay heat, such as the feedwater system, shutdown cooling system, moderator system and emergency water supply. Feedwater, shutdown cooling, and moderator systems operate under Class IV and Class III power. In the event that Class IV and Class III power are unavailable, seismically qualified EPS will be started, to ensure provisions available for long term fuel cooling. The EC6 design incorporates the EHRS as a fifth safety system, to remove heat from the steam generators following DBA that fail the process systems that remove heat to the ultimate heat sink.

Following total loss of off-site and on-site power, the steam generator heat sink is maintained by make-up to the steam generators from the dousing tank for CANDU 6 plants and from the reserve water tank for the EC6 design, after steam generator rapid cooldown. The steam generator automatic depressurization is initiated on an abnormally low steam generator level in two or more steam generators conditioned by low feedwater header pressure, which indicates an
unavailability of normal feedwater. The steam generator make-up valves are opened automatically on steam generator secondary side pressure falling to <345 kPa(g) and reactor building pressure <3.25 kPa(g). These valves are pneumatic powered and in order to address prolonged station blackout, provision can be made to keep the valves opened to a minimum flow while the batteries are still effective, thus matching make-up flow to long term decay heat removal requirement.

**Restore and maintain cooling to a damaged core**

The CANDU 6 core is designed with defence in depth provisions that provide a relatively “forgiving” response to severe accidents such as prolonged loss of cooling to the fuel. In addition, the CANDU 6 core is subdivided into fuel channels, each surrounded by low-pressure, low-temperature moderator heavy water. This means that, overall there is a relatively large amount of water available for emergency fuel cooling. The CANDU safety case has traditionally covered accidents where coolant is lost to the fuel channels for a long time, in the event that the Emergency Core Cooling System is unavailable. Even for this case, the backup moderator heat sink is effective in removing the decay heat from the fuel.

Furthermore, the moderator tank is itself surrounded by a large volume of water, which functions as a “core-catcher” and further backup heat removal system. The core is situated inside the containment, while the heat removal elements (pumps and heat-exchangers) are located outside containment where they can continue to function. Thus, if cooling to the core is interrupted, even to the extent of fuel damage, the capability remains to continue core cooling. The large quantities of water in the moderator mean that, even in the prolonged absence of electric power, and assuming the failure of natural circulation cooling, many hours of time would elapse before the water needs to be replenished. Provisions to respond to a total loss of AC power event are presented in Table 3-8.

**Table 3-8: CR1.1.1 Loss of All AC Power Event (Loss of Class IV + Class III Standby DGs + EPS DGs)**

<table>
<thead>
<tr>
<th>System Availability &amp; Consequence</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Availability:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDS1/SDS2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SARHRS</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HPECC</td>
<td>X</td>
<td>No</td>
</tr>
<tr>
<td>Batteries</td>
<td>X</td>
<td>No</td>
</tr>
<tr>
<td>RWT to SG</td>
<td>X</td>
<td>No</td>
</tr>
</tbody>
</table>
Consequence

| Containment Integrity | Containment failure after ~6 days | Containment failure after ~5 days* | Containment Integrity maintained – prevention of SCD |

*If calandria vault makeup available, as in some CANDU 6 stations, containment integrity is maintained.

The EC6 design further improved the heat sink margin by incorporating the following features:

- **Addition of a Severe Accident Recovery and Heat Removal System (SARHRS) to extend cooling makeup capability.** The SARHRS can recover and cool water from the containment floor and cool it using heat exchangers before pumping it back into the calandria vessel or calandria vault (for core heat removal) and/or the Reserve Water Tank (to ensure long-term containment pressure suppression and fission product washout by low-flow sprays). SARHRS has its own dedicated diesel generator and is capable of independently drawing water for cooling of heat exchangers and/or for make-up to the Reserve Water Tank from the local water supply (lake or river).

- **Improved heat sink capability by seismically qualifying Shield Cooling System (SCS) piping inside the reactor building.**

- **Provision for external valve access for the SARHRS to supply water.**

For a severe core damage accident, SARHRS, or the Shield Cooling System may be used to remove heat from corium to maintain in-vessel retention strategy. The SARHRS system is considered a complementary design feature, and is a completely independent means of transferring decay heat to the ultimate heat sink for prevention and mitigation of severe accidents, due to its own dedicated diesel generator and provisions for make-up, which provides additional heat sink margin.

**Final assessment of evaluation parameter EP 1.1.1.1** The EC6 design provides added safety margin for reactor shutdown, subcriticality, containment design, seismic margin, flood margin and heat sink margin.

Therefore, evaluation parameter EP1.1.1.1 has been demonstrated by the EC6 design.

**3.1.1.1.2 Redundancy of Systems**

b) **Evaluation parameter EP1.1.1.5:** Redundancy of systems

*Describe the increased redundancy for EC6 versus CANDU 6 reactors for reactivity control (including Guaranteed Shutdown State (GSS)), decay heat removal, and containment heat sinks.*

**Acceptability of EP 1.1.1.5:** Demonstration of increased redundancy of (operational) systems of the EC6 design in comparison to the CANDU 6 plants for reactivity control and heat sink capability.
A lessons learned from the Fukushima event was to provide adequate diversity, as well as redundancy for essential safety functions [2]. The CANDU 6 design incorporates strict grouping and separation requirements to ensure that common mode events and functional interconnections between systems do not impair the ability of the systems to perform required safety functions. Plant systems are separated into two groups which, to the extent possible, are located in separate areas of the plant:
- Group 1 consists of process systems used for power production and
- Group 2 includes standby systems used only for plant shutdown and accident mitigations.

The systems and equipment in each group are capable of shutting the reactor down and maintain shutdown, cooling the reactor, and monitoring plant conditions independent of the other group. The EC6 design has incorporated improvements that allow flexibility in responding to events and provide redundancy for heat sinks capability and for additional capability to shut down the reactor and maintain it in a safe shutdown condition.

3.1.1.1.2.1 Reactivity Control

The CANDU 6 plant has four systems for reactivity control:
1. Level 1 and 2 DiD: Reactor Regulating System (RRS), which is used to control reactivity in normal plant conditions, and to reduce power or shut down the reactor for most abnormal events, and consists of:
   - 14 liquid control zones using light water,
   - 4 mechanical Control Absorber Rods that are normally parked out of the reactor core and are inserted to control the neutron flux level at times when a greater rate or amount of reactivity control is required than can be provided by the liquid zone control assemblies,
   - 21 Adjuster Rods made of stainless steel for flux flattening and overcoming the build up of Xenon-135, and
   - Gadolinium addition via the Moderator Poison System.

2. Level 1, 2 and 3 DiD: Moderator Poison System, which is used to manually add either boron or gadolinium to the moderator to achieve a shutdown condition.

3. Level 3 DiD: Shutdown system #1 (SDS1) which consists of 28 SS-clad cadmium rods, vertically oriented that are dropped by gravity into the calandria vessel, when a reactor trip is initiated by its dedicated instrumentation.

4. Level 3 DiD: Shutdown system #2 (SDS2) which consists of 6 injection nozzles for gadolinium nitrate solution, horizontally oriented that are liquid injection driven by high pressure helium, when a reactor trip is initiated by its dedicated instrumentation.

These reactivity control capabilities provide sufficient multiple, diverse and independent barriers to failure.

The EC6 design has five systems for reactivity control:
1. Level 1 and 2 DiD: Reactor Regulating System (RRS), which is used to control reactivity in normal plant conditions, and to reduce power or shut down the reactor for most abnormal events, and consists of:
   - 14 liquid control zones using light water,
   - 4 mechanical Control Absorber Rods that are normally parked out of the reactor core and are inserted to control the neutron flux level at times when a greater rate or amount of reactivity control is required than can be provided by the liquid zone control assemblies,
   - 11 Adjuster Rods made of stainless steel for flux flattening and overcoming the build up of Xenon-135,
   - Gadolinium addition via the Moderator Poison System.

2. Level 1, 2 and 3 DiD: Moderator Poison System, which is used to manually add either boron or gadolinium to the moderator to achieve a shutdown condition.

3. Level 3 DiD: Shutdown system #1 (SDS1) which consists of 28 SS-clad cadmium rods, vertically oriented that are dropped by gravity into the calandria vessel, when a reactor trip is initiated by its dedicated instrumentation.

4. Level 1, 2 and 3 DiD: 10 Supplemental Absorber Rods, made of SS-clad cadmium, which are manually inserted to maintain a stable shutdown condition after decay of Xenon-135.

5. Level 3 DiD: Shutdown system #2 (SDS2) which consists of 6 injection nozzles for gadolinium nitrate solution, horizontally oriented that are liquid injection driven by high pressure helium, when a reactor trip is initiated by its dedicated instrumentation.

Guaranteed Shutdown State (GSS) is used in the CANDU 6 plants to ensure that the reactor will remain in a stable sub-critical state independent of reactivity perturbations caused by any possible change in core configuration, core properties or process system failures. Two types of GSS can be used for the CANDU 6 plants:

- Overpoison GSS: The stable sub-critical state is achieved by adding gadolinium poison to the moderator. The Moderator Poison System is usually used to manually add gadolinium nitrate solution to the moderator, for entry into GSS.

- Rod-Based GSS: The stable sub-critical state is achieved by manually inserting the 28 SORs from SDS1, locking the 21 Adjuster Rods in the core, manually inserting the 4 Control Absorber Rods and adding small amounts of either boron or gadolinium to the moderator using the Moderator Poison System. This form of GSS is not fully diverse and independent of the overpoison GSS. It is being implemented at some CANDU 6 plants.

GSS is also used in the EC6 design to ensure that the reactor will remain in a stable sub-critical state independent of reactivity perturbations caused by any possible change in core configuration, core properties or process system failures, as per new build requirements. Two types of GSS are included in the EC6 design:
Overpoison GSS: The stable sub-critical state is achieved by adding gadolinium poison to the moderator. The Moderator Poison System is usually used to manually add gadolinium to the moderator. This is the same system as is used in the CANDU 6 plants.

Rod-Based GSS: The stable sub-critical state is achieved by manually inserting the 32 SORs from SDS1, locking the 11 Adjuster Rods in the core, manually inserting the 4 Control Absorber Rods and manually inserting the 10 Supplemental Absorber Rods. This form of GSS is fully diverse and independent from the overpoison GSS.

Table 3-9: CR1.1.1 for Evaluation of improved redundancy of systems

<table>
<thead>
<tr>
<th>Parameter</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reactivity Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRS</td>
<td>On power refuelling light water in liquid zone control assemblies Adjuster Rods Control Absorber Rods Boron or gadolinium poison addition to moderator</td>
<td>On power refuelling light water in liquid zone control assemblies Adjuster Rods Control Absorber Rods Boron or gadolinium poison addition to moderator</td>
</tr>
<tr>
<td>Moderator Poison System</td>
<td>Boron or gadolinium poison addition to moderator</td>
<td>Boron or gadolinium poison addition to moderator</td>
</tr>
<tr>
<td>SDS 1</td>
<td>Spring-assisted, gravity accelerated, shutoff rods (SORs)</td>
<td>Spring-assisted, gravity accelerated, shutoff rods (SORs)</td>
</tr>
<tr>
<td>SDS 2</td>
<td>Gadolinium poison injection</td>
<td>Gadolinium poison injection</td>
</tr>
<tr>
<td># of Mechanical Control Absorbers Rods (CAR)</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td># of Adjusters (ADJ)</td>
<td>21</td>
<td>11</td>
</tr>
<tr>
<td># of Shut-off Rods (SOR)</td>
<td>28</td>
<td>32</td>
</tr>
<tr>
<td># of Poison Injection Nozzles</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td># of Supplemental Absorber Rods</td>
<td>0</td>
<td>10</td>
</tr>
</tbody>
</table>

3.1.1.1.2.2 Heat Sink Capability

The CANDU 6 plants have the following water inventory as passive heat sinks to prevent or significantly delay progression to a severe accident in case safety systems are not available, refer to Figure 3-2:

- Heat Transport System: 190 Mg D₂O capacity
- Emergency Core Cooling System: 215 Mg H₂O in high pressure ECC and 500 Mg H₂O in medium pressure ECC.
- Moderator: approximately 240 Mg of D$_2$O within the calandria vessel surrounding the fuel channels.
- Calandria vault: 520 Mg of light water surrounding the calandria vessel.
- Dousing tank: 2056 Mg capacity; 1550 Mg H$_2$O for dousing to remove heat from containment, also provides water for MPECC, HTS and EWS.

Figure 3-2: Water Inventory in CANDU 6 plants

The CANDU 6 plants use the moderator and/or the reactor vault as emergency heat sinks for severe accident prevention and mitigation. The moderator system, serves as a backup heat sink for absorbing the heat from reactor core in the event of severe accidents. The moderator heat
removal arrests sequences at the limited core damage (LCD) state without progressing to severe core damage (SCD), by providing external cooling of the fuel channels to prevent fuel melting and maintain channel integrity.

The EC6 design has the following water inventory as passive heat sinks to prevent or significantly delay severe accident progression:

- **Heat Transport System:** 190 Mg D$_2$O capacity
- **Emergency Core Cooling System:** 215 Mg H$_2$O in high pressure ECC and 2056 Mg H$_2$O in medium pressure ECC.
- **Moderator:** approximately 240 Mg of D$_2$O within the calandria vessel surrounding the fuel channels.
- **Calandria vault:** 520 Mg of water surrounding the calandria vessel.
- **Reserve Water tank:** 2056 Mg capacity (provides water for MPECC, EHRS, HTS, SARHRS - moderator makeup, calandria vault make-up, low flow spray)
  - 1556 Mg H$_2$O for low flow spray to remove heat from containment for BDBA
  - From 500 to 2056 Mg for ECC (2056 Mg of RWS water is reserved for MPECC)

The CANDU 6 plants and EC6 design have multiple heat transfer paths to remove decay heat from the fuel to the ultimate heat sink via the primary and/or secondary sides during normal operation, anticipated operational occurrences, design basis accidents and beyond design basis accidents, including severe accidents:

**Table 3-10: CR1.1.1 for Evaluation of Decay Heat Removal**

<table>
<thead>
<tr>
<th>Plant State</th>
<th>CANDU 6 Plant</th>
<th>EC6 Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Operation And AOO</td>
<td>Main Feedwater System including Auxiliary Feedwater Shutdown Cooling System Recirculated Water System/Raw Service Water System LACs</td>
<td>Main Feedwater System including Auxiliary Feedwater Shutdown Cooling System Recirculated Water System/Raw Service Water System LACs</td>
</tr>
</tbody>
</table>
The Emergency Water Supply System for the CANDU 6 plants is a safety support system. For the EC6 design, the Emergency Water Supply System has been upgraded to be the fifth safety system – EHRS. The EHRS removes heat from the steam generators following a DBE, and from the ECC heat exchangers in the event that an earthquake occurs 24 hours after a LOCA.

The EC6 design has added a complementary design feature to prevent and mitigate severe accidents – Severe Accident Recovery Heat Removal System (SAHRS). SAHRS would be used to replenish the moderator or the calandria vault water inventory by providing makeup water via the Reserve Water Tank, from fresh water source or by collecting, cooling and recirculating water from the ECC sumps using dedicated pump and heat exchangers, as depicted in Figure 3-3. This feature improves the Level 4 defence in depth provisions for preventing the onset of severe accidents and mitigating their consequences. The EC6 design includes additional flow paths to the ultimate heat sink (local body of water and/or atmosphere) for beyond design basis accidents, as shown in Figure 3-4, which are not included in the CANDU 6 plants, as shown in Figure 3-5.
The heat sinks available to the CANDU 6 plants and EC6 design during severe accidents are presented in Table 3-11.

Table 3-11: CR1.1.1 for Evaluation of heat sink capability

<table>
<thead>
<tr>
<th>CANDU 6 Plant</th>
<th>EC6 Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make-up to the calandria vault via portable water source for some CANDU 6 plants</td>
<td>Make-up to the calandria vessel from SARHRS allows heat removal from the calandria vessel. Cooling for the SARHRS heat exchanger is by a dedicated SARHRS cooling water pump, using inventory from</td>
</tr>
</tbody>
</table>
If make-up is relied upon (i.e. no active cooling), sufficient steam relief capacity is provided on the calandria vault for severe accident conditions. This allows the calandria vault inventory to boil off gradually, thereby prolonging the calandria vault heat sink and the integrity of the calandria vault structure.

The EC6 design has a 24” rupture disc for the calandria vault to ensure that there is sufficient pressure relief capacity following a severe accident. Some CANDU 6 plants have also incorporated this 24” rupture disc.
Figure 3-4: Schematic of Systems Important to Safety in the EC6 which Transfer Residual Heat to the Ultimate Heat Sinks
Portable Equipment – Design Flexibility

The EC6 has provisions for flexible portable supplies of power and water which can be deployed if the permanently installed systems fail, and ensure that these can be connected quickly and in adverse environments.

It is recognized that following the Fukushima event, CANDU 6 plants worldwide have made provisions for portable power and equipment to address the lessons learned.

Critical Loads – Back-up

The EC6 design incorporates provisions to provide an external connection that provide power for recharging batteries through a mobile diesel generator securely stored on site. The 250 KWe, 600 VAC, 3 phase, 60 Hz seismically qualified portable diesel generator (DG) will be stored in a safe, protected, elevated area on site and will be able to start supplying the power to the 75 KVA UPS with an 8 hour backup battery. This manual switchover to start recharging and supplying the extended SBO loads can be made anytime up to 24 hours. This feature will ensure that operation of crucial instrumentation monitoring parameter and lighting will be available continuously during an extended station blackout event.

Spent Fuel Bay – Heat Sink Back-up

Figure 3-5: Schematic of Safety Related Systems which Transfer Residual Heat to the Ultimate Heat Sinks for CANDU 6
The probability of fuel uncovering in CANDU 6 spent fuel bays (SFB) is extremely low due to the redundant power supply options, the modest fuel heat load, and the large inventory of water which ensures a long period of time available to restore cooling. The spent fuel bay cooling and purification system provides cooling of the water in the spent fuel, reception and discharge bays, to dissipate the decay heat from the irradiated fuel. This is done by circulating the elevated temperature water from the spent fuel bays through a heat exchanger and then returning the water to the bays. During normal operation, the system is designed to remove decay heat that is released from irradiated fuel in the spent fuel bays and maintain the bay water temperature within acceptable limits. Normal circulation is ensured with pumps powered by off-site non-seismically qualified Class IV and backup Class III power.

During a loss of Class III and Class IV power, the primary heat sink for removal of heat from the fuel is the heat capacity of the large volume of water in the spent fuel bay. In order to maintain the water level in the spent fuel bay, water is available from the fire water system extended into the storage and reception bays. Instrumentation is provided to monitor the spent fuel bay water level, water temperature and radiation fields.

To ensure that cooling in the long term is available to the SFB after an accident, the following EC6 provisions have been added;

- The make-up connection for the spent fuel storage bay and the reception bay to maintain the level has been designed to be seismically qualified.
- The make-up connection is connected to the seismically qualified fire water system, and each seismically qualified firewater line is provided with a check valve in series with a parallel arrangement of manual and motorized butterfly valves for flow isolation and the downstream piping will be routed to the SFBs.
- The remotely-operated motorized valve will be controlled from the MCR for ease of operation, in additional to a manual valve provided. The operator in the MCR will need to open the motorized valves to control the flow and to maintain a safe water level in the bays.
- To guide operator actions, seismically qualified spent fuel bay level, temperature, and activity parameters are provided to monitor conditions of SFB. The instrumentation is also environmentally qualified for postulated harsh conditions in the SFB.

A summary of design features for CANDU 6 and EC6 for heat sink provisions is provided in Table 3-12.

**Table 3-12: CR1.1.1 Evaluation for improved heat sink capability**

<table>
<thead>
<tr>
<th>Design Feature</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Systems</td>
<td>1. Shutdown System 1</td>
<td>1. Shutdown System 1</td>
</tr>
<tr>
<td></td>
<td>2. Shutdown System 2</td>
<td>2. Shutdown System 2</td>
</tr>
<tr>
<td></td>
<td>3. Emergency Core Cooling System (ECC)</td>
<td>3. Emergency Core Cooling System (ECC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Containment System</td>
</tr>
<tr>
<td>Design Feature</td>
<td>CANDU 6</td>
<td>EC6</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Water inventory in reactor</td>
<td>3 000 Mg of water available for passive heat removal:</td>
<td>3 000 Mg of water available for passive heat removal:</td>
</tr>
<tr>
<td></td>
<td>- 2056 Mg in Dousing Tank</td>
<td>- 2056 Mg in RWT</td>
</tr>
<tr>
<td></td>
<td>- 215 Mg HPECC</td>
<td>- 215 Mg HPECC</td>
</tr>
<tr>
<td></td>
<td>- 240 Mg D(_2)O in calandria vessel</td>
<td>- 240 Mg D(_2)O in calandria vessel</td>
</tr>
<tr>
<td></td>
<td>- 520 Mg H(_2)O in calandria vault</td>
<td>- 520 Mg H(_2)O in calandria vault</td>
</tr>
<tr>
<td></td>
<td>- 190 Mg of D(_2)O in HTS</td>
<td>- 190 Mg of D(_2)O in HTS</td>
</tr>
<tr>
<td>Extended Cooling Capability</td>
<td>-Make-up to the calandria vault via portable water source for some CANDU 6 plants</td>
<td>-Severe Accident Recovery and Heat Removal System (SARHRS) to extend cooling makeup capability. Cooling for the SARHRS heat exchanger is by a dedicated SARHRS cooling water pump, using inventory from the on-site water supply (once-through cooling). -Make-up to the calandria vessel from the reserve water tank (RWT)</td>
</tr>
<tr>
<td>Battery Back-up</td>
<td>1H Group 1 batteries *battery life for CANDU 6 plants has been extended based on distribution of loads</td>
<td>24 H UPS batteries 1 Hour Group 1 batteries 8 Hour batteries for Safety Monitoring</td>
</tr>
<tr>
<td>On-site Portable Power Supplies</td>
<td>*provisions for portable power in CANDU 6 plants to address Fukushima LL</td>
<td>1 portable power supply/unit</td>
</tr>
<tr>
<td>Spent Fuel Bay – Long term cooling</td>
<td>* seismically qualified make-up provisions incorporated in some CANDU 6 plants to address Fukushima LL(^\text{[22]})</td>
<td>-Provide make-up to SFB from seismically qualified firewater - Design requirements for SFB to specify 100°C for</td>
</tr>
</tbody>
</table>

\(^5\) In CANDU 6 plant, this is the EWS designated as a safety support system.
Final assessment of evaluation parameter EP 1.1.1.5
The EC6 design provides increased redundancy for reactivity control during normal operation, and increased shutdown margin for SDS1 during DBAs. The EC6 design provides increased heat sink capability during severe accidents, as compared to the CANDU 6 plants. Therefore, evaluation parameter EP1.1.1.5 has been demonstrated by the EC6 design.

3.1.1.2  Final assessment of criterion CR1.1.1 Robustness
The assessment of the evaluation parameters of the first criterion CR1.1.1 has confirmed an increased robustness of the EC6 design as compared to the CANDU 6 plants in terms of improved safety margins and improved redundancy of systems.

3.1.1.3  Assessment against criteria CR1.1.2 Operation

- **Indicator IN1.1.2**: High quality of operation
- **Acceptance Limit AL1.1.2**: new designs (EC6) should be superior to existing design in at least some aspects of operation

  a) **Evaluation Parameter EP1.1.2.7**

  Describe the increased availability/capability of the EC6 design, over the CANDU 6 plant.

  **Acceptability of EP 1.1.2.7**: The EC6 incorporates design improvements and use of operating experience to increase the plant capacity factor and achieve an outage interval of once per 3 years and outage durations of 30 days, as compared to the CANDU 6 plants.

The CANDU 6 plants are often ranked by World Association of Nuclear Operators (WANO) as top performers among all nuclear reactors, measured through the capability factor. A unit capability factor, is defined as the ratio of the available energy generation over a given time period to the reference energy generation over the same time period, expressed as a percentage. Available energy generation is the energy that could be produced if the unit were operated continuously at full power under reference ambient conditions. The CANDU 6 plants are proven performers, with a lifetime capacity record, hovering around 90%. The EC6 design applies operating experience to further improve the already high capacity factor of the CANDU 6 plants to 92% over the lifetime and 94% year to year, as shown in Table 3-13.
Table 3-13: CR1.1.2 Evaluation of improved plant availability and capability

<table>
<thead>
<tr>
<th>Availability/Capability</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability Factor</td>
<td>Lifetime capacity factor greater than 85%</td>
<td>Lifetime capability factor greater than 92%, with a year to year plant capability factor greater than 94%.</td>
</tr>
<tr>
<td>Design Life</td>
<td>40 years</td>
<td>Operate for 60 years</td>
</tr>
<tr>
<td>Outage Interval/Duration</td>
<td>Between 24 and 30 months/~30 days</td>
<td>3 years/30 days</td>
</tr>
</tbody>
</table>

Operating CANDU reactors have recently implemented measures aimed to optimize maintenance schedules, with consideration of OPEX information, resulting with 24 to 30 month operating cycles for outages. The approach for extending the maintenance outages was to systematically review the impact of the extension on reliability targets for the safety systems and support systems. All components were systematically assessed with a potential impact on outage interval extension. It was determined, that majority of components would be able to maintain component functionality from a safety or equipment reliability perspective, while others could be maintained on line. For the remaining limited components, a detailed analysis was performed to address and improve reliability to perform predictive and preventative maintenance. Improvements were made through either i) adjustments to maintenance strategy (improving accessibility) or ii) design modifications to reduce system failures. For the group of components which were susceptible to repeated failures, the existing performance monitoring plan was improved to achieve system/component performance improvement.

The EC6 design builds on the CANDU 6 lessons learned to achieve higher availability and capability of the plant, through the implementation an extensive Equipment Health Monitoring (EHM) system, which purpose is to monitor equipment for any degradation in order to optimize maintenance schedule. The objective of the EHM system is to achieve safe, reliable, predictable and economical plant performance through the following improvements;

- Improved plant reliability and operating margins
- Improved configuration management capability
- Reduction in maintenance induced equipment failures
- Reduced outage frequency and duration
- Reduce operations, maintenance and administrations costs

The selection of components for monitoring is guided by the best practices in the industry and feedback from operating CANDU plants using current technologies. An estimate of the number
of critical components in the EC6 design is in the range of 4000 – 5000, in the following categories – as depicted in Table 3-14.

<table>
<thead>
<tr>
<th>Category</th>
<th>Component/Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical components</td>
<td>Batteries, Inverters and battery charging systems, motor control centres, circuit breakers and switchgears, large motors, high voltage transformers</td>
</tr>
<tr>
<td>Instrumentations and Control components</td>
<td>Computers, Transmitters</td>
</tr>
<tr>
<td>Rotating Equipment</td>
<td>Pumps, motors, fans, compressors, chillers</td>
</tr>
<tr>
<td>Valves</td>
<td>Air operated valves (AOV), motor operated valves (MOV), check valves (NV).</td>
</tr>
</tbody>
</table>

Table 3-14: CR1.1.2 Category and Component Identification for EHM

The EHM system will collect equipment maintenance data that will be available for trending, diagnostics and analysis through the SMART CANDU suite of analysis applications. This approach enables proactive maintenance that will reduce equipment failure by providing information to plant staff on equipment status and identify any signs of degradation. The indices that are used to measure the status are based on industry and OPEX data. The EC6 design will, wherever possible, implement ‘smart’ (or digital) hardware that is based on the latest technology that used actuators and positioners for condition monitoring. The gathered information is then analyzed for trending patterns using statistical distribution models. Statistical methods for estimating distribution parameters and confidence intervals are used to provide indication of component reliability (component reliability is degrading over time when the slope is found to be greater than 1; improving over time when slope is less than 1; not changing when slope is equal to 1). The results of which can be used to forecast trending patterns and indicate to maintenance staff when equipment degradation has or is expected to occur. This enables the health monitoring of equipment by improving EC6 operability and performance through provisions for monitoring and trending to assess aging mechanisms, verify predictions and identify unanticipated behaviours or degradation that may occur during operation. The EHM fosters a management of knowledge in real time, that enables the EC6 to achieve improved availability and capacity factors over the CANDU 6 plants.

It has been demonstrated that evaluation parameter EP 1.1.2.7 has been met.

3.1.1.4 Final assessment of criterion CR1.1.2 Operation

The EC6 is designed to achieve a higher availability and capacity factor, resulting with a longer design life, as compared to the CANDU 6 plants. Therefore, criterion CR 1.1.2 on operation has been demonstrated by the EC6 design.
3.1.1.5 Final assessment of user requirement UR1.1 - Robustness

It has been demonstrated that the EC6 design has improved robustness over the CANDU 6 plants, for which criteria CR 1.1.1 and CR 1.1.2 have been met. Therefore, user requirement UR1.1 is deemed to have been met by the EC6 design.

3.1.2 User Requirement UR1.3 – Design Basis Accidents

The frequency of occurrence of design basis accidents (DBA) should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an innovative NES to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.

INPRO has developed four criteria for this requirement CR.1.3.1 to CR 1.3.6. In the context of applicability to Fukushima lessons learned, CR 1.3.3 on safety features, CR 1.3.4 on barriers and CR 1.3.5 on controlled state will be evaluated for the EC6 design.

3.1.2.1 Assessment against criterion CR1.3.3 Safety Features

- **Indicator IN1.3.3:** Reliability of engineered safety features (probability of failure of engineered safety system per demand and unit)
- **Acceptance Limit AL1.3.3:** New designs (EC6) in case of DBA should show equal or higher reliability than the reference CANDU 6 plants.

**Evaluation Parameter EP1.1.1.1:** The EC6 is designed with a higher reliability, than the CANDU 6 plants, to meet latest regulatory requirements.

The CANDU 6 plants have four independent safety systems: Shutdown System (SDS 1 and SDS 2); Emergency Core Cooling System and Containment System. The CANDU 6 licensing design basis evaluates the consequences of accidents arising from serious failures in process systems, both when they are considered alone and in combination with various unavailability or failures of the special safety systems. These events are classified as single and dual failure accidents. The dual failure concept assumes a simultaneous failure combination between a process system and a special safety system (i.e., Emergency core cooling (ECC), Shutdown system). These analysed events enable a risk evaluation to be made that ensures safety system effectiveness. The requirement for single failure accidents is to meet unavailability of each safety system, not to exceed $10^{-3}$ per year. Dual failures must be at least a factor of $10^{-3}$ less frequent than single failures [27][28][29]. The overall system unavailability target is $10^{-3}$ per year for CANDU 6.

In the EC6 design, the Emergency Heat Removal System (EHRS) removes decay heat from the steam generators, when required as a result of a Design Basis Accident. The EHRS uses the seismically qualified Group 2 Emergency Water System and the seismically qualified Group 2 Emergency Power Supply, both of which are upgraded from the CANDU 6 reference design to meet safety system standards for reliability, code class, automation and seismic qualification. In
addition, the EC6 design separates the shared two-unit Emergency Power Supply (EPS) of the CANDU 6 plants into individual EPSs for each EC6 unit, that provides increased redundancy of the EPS diesel generator to ensure the appropriate reliability for a safety support system and to also meet the single failure criterion. The reliability targets are established during system design and verified by reliability analysis. The safety systems meet high reliability requirements, based on the latest regulatory requirements for reliability and meeting the single failure criterion:

7.6 Design for Reliability

‘The safety systems and their support systems are designed to ensure that the probability of a safety system failure on demand from all causes is lower than 10^{-3}’ [15]

7.6.2 Single Failure Criterion

‘All safety groups function in the presence of a single failure’ [15]

The CANDU 6 plants satisfy the requirements for single failure in Canadian regulatory documents R-7 [28], R-8 [27] and R-9 [29], which requires that no failure of a single component of a special safety system can result in an impairment of the system to the extent that the system will not meet its minimum allowable performance standard.

System unreliability values are derived by considering both the acquired knowledge from past CANDU 6 plants and by taking into account the results of recent reliability and summed severe core damage estimates produced for EC6. The EC6 design satisfies the requirements for single failure in Canadian regulatory document RD-337 [15], which requires each safety group to perform the required safety functions under the worst permissible systems configuration, taking into account such considerations as maintenance, testing, inspection and repair, and equipment outage. Under this definition of single failure criterion, a broader set of safety and safety support systems, and interfacing process systems are taken into account.

Both, the CANDU 6 and EC6 meet the regulatory reliability targets. The EC6 design has increased the redundancy in safety support and interfacing process systems to protect against single failures.

3.1.2.2 Final assessment of criterion CR1.3.3 Safety Features

The EC6 is designed with similar reliability targets as the CANDU 6 plants, and satisfies the latest regulatory expectations.

The EC6 design has increased the protection against single failures for the safety groups relative to the CANDU 6 plants.

Therefore, criterion CR 1.3.3 on safety features has been demonstrated by the EC6 design.
3.1.2.3 Assessment against criterion CR1.3.4 Barriers

- **Indicator IN1.3.4:** Number of confinement barriers maintained
  
  The design of engineered safety features should deterministically provide for continued integrity at least of one barrier (containing the radioactive material) following any DBA.

- **Acceptance Limit AL1.3.4:** Deterministically, at least one remaining barrier against a release of fission products to the environment; or, probabilistically, a very low probability of failure of all barriers in the NES.

  The strategy for defence in depth is two-fold; first, to prevent accidents and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions. Preventative measures are balanced with mitigative measures to limit consequences. Mitigative measures, in particular a well designed confinement function can provide the necessary additional protection of the public and the environment. The independence of different levels of defence in depth is a key element in meeting this objective.

  The objectives and CANDU 6/EC6 approach for the five level of defence-in-depth are as follows:

  **Level 1**  
  *Prevention of abnormal operation and failures.*

  The CANDU 6 plant employs conservatism and consists of safety features for prevention of abnormal operation and failures. The EC6 design provides additional capability and greater shutdown margin for shutdown conditions, including during GSS, as presented in CR 1.3.5.

  **Level 2**  
  *Control of abnormal operation and detection of failures.*

  The CANDU 6 plant has a reliable reactor regulating systems (RRS) to control core reactivity in normal plant operation, and reduce power or shut down the reactor for abnormal events. The EC6 design provides additional parameters to respond to anticipated operational occurrences as presented in CR 1.3.5.

  **Level 3**  
  *Control of accidents within the design basis.*

  The CANDU 6 plants have safety features to control accidents within the design basis, including two reliable, diverse and independent shutdown systems. The EC6 design provides faster shutdown and greater shutdown margin for SDS1 as presented in CR 1.1.1, an additional safety system to respond to non-LOCA events to ensure transfer of heat from the core to the ultimate heat sink and a more robust, lower leakage containment.

  **Level 4**  
  *Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.*

  The CANDU 6 plant employs a severe accident strategy for prevention and
mitigation of accident progression that provides sufficient time for emergency response. The EC6 design has installed complementary design features to provide additional capability to cope with beyond design basis accidents, including severe accidents, as presented in CR 1.1.1.

The CANDU 6 plants and EC6 design include means for providing portable sources of power and water to prevent and mitigate severe accidents.

The EC6 design improves safety monitoring capability for operator with additional severe accident monitoring parameters.

Some CANDU 6 plants have incorporated an Emergency Filtered Containment Venting System (EFCVS) to protect the containment by relieving pressure and controlling and filtering releases during a severe accident. The EC6 design has incorporated an EFCVS for relief of pressure and removal of aerosols and iodine, as a final barrier in a severe accident to protect containment leak tightness. The setpoint for the EFCVS is above the containment design pressure respectively, to prevent over pressurization of the containment beyond its elastic range.

Level 5 Mitigation of radiological consequences of significant releases of radioactive materials through off-site emergency response.

Following the Fukushima event, CANDU 6 plants have implemented off-site emergency centers that contain additional portable supplies of power and water, which can be deployed to mitigate severe accidents.

The defence in depth approach in the CANDU 6 plants incorporates four major physical barriers to the release of radioactive materials to the environment, as follows (also refer to Figure 3-6 for a detailed depiction):

Fuel matrix – The bulk of the fission products generated in the fuel are contained within the fuel grains or on the grain boundaries, and are not readily available to be released even if the fuel sheath fails.

Fuel sheath – There are large margins to fuel sheath failure under normal operating conditions.

Heat Transport System – Even in the event that the fission products are released from the fuel during an accident, they are contained within the HTS. The HTS is designed to withstand the pressure and temperature loading resulting from the accident conditions.

Containment – In the event of a design basis accident (DBA), automatic containment isolation will occur, ensuring that any subsequent release to the environment does not occur.
For both CANDU 6 plants and EC6 design, the fuel matrix is contained within the boundary where no fuel melting occurs for DBA conditions. Therefore, at least two confinement barriers remain secured in a DBA – the fuel matrix and the reactor containment. For example, the consequence of a large loss of coolant accident (LOCA) maintains a contained fuel matrix with no fuel melting, and intact containment boundary; fuel sheath and pressure boundary is maintained in the unbroken loop. However, as discussed previously the safety margin for large LOCA has been improved for the EC6 design (Refer to CR 1.1.1).

![Figure 3-6: CANDU 6 Defence in Depth Barriers](image)

The containment boundary is the last barrier in preventing radiological releases following a severe accident. The Fukushima lessons learned highlighted the importance of measures that protect containment integrity as a result of i) high pressure core-melt, ii) hydrogen explosions and iii) containment over pressurization[2]. The following presents the additional enhancements provided in the EC6 design, over the CANDU 6 plants with regards to containment design, resulting with additional margin.
Containment Design

The CANDU 6 containment is a cylindrical pre-stressed concrete leak tight containment structure with 1.07 m thick walls with a design pressure of 124 kPa (g). The CANDU 6 reactor building, its penetrations and the isolation valves form the containment envelope. The containment envelope includes containment isolation and hydrogen control. The containment will automatically isolate during accident conditions. Cooling in the reactor building is provided by electrical driven forced air coolers in the reactor vaults and upper boiler room. Heat is removed by the recirculating cooling water system. The CANDU 6 contains a dousing tank, located at the top of the reactor building which is connected to a spray header system by a set of valves. In the event that the reactor building pressure exceeds a certain point, these valves automatically open initiating the dousing spray which will condense any steam that may be present and quickly drop the pressure in the building. For hydrogen control, some CANDU 6 plants contain igniters and have recently added passive autocatalytic hydrogen recombines (PARs). PARs do not require external power and can remove hydrogen from the containment atmosphere that might be generated in events with prolonged loss of ac power.

The EC6 design has made a number of improvements to strengthen the containment building, with a design pressure of 400 kPa (g) and an improvement in leak rate to 0.2%/day. This provides additional margin in maintaining containment integrity following severe accident events and provides additional time for emergency response. The containment structure consists of a prestressed concrete cylindrical perimeter wall, with a torispherical dome, ring beam, and conventionally reinforced concrete base slab. For the EC6 design, the dousing tank has been replaced with the Reserve Water Tank (RWT). The capacity of the RWT is the same as the reference CANDU 6 dousing tank. In the event of a design basis accident (DBA), automatic containment isolation will occur, which is ‘fail-safe’. Containment isolation valves are designed to fail closed on loss of instrument air or loss of control power supply, which results with a fail-safe condition. Containment atmospheric hydrogen control is achieved by mixing of the containment atmosphere using the local air coolers, active igniters and PARs. The mitigation strategy is the same as for the CANDU 6 plants, with 33 PAR units and 44 igniters.

A steel liner plate is provided on the entire inside surface of the containment structure, to ensure that leak-tightness is within acceptable limits and prevent spalled concrete to be generated as a result of an external impact. The major opening in the EC6 containment structure is for the equipment airlock, enhanced with dual solid face type seals. An opening in the perimeter wall for an auxiliary personnel airlock is also provided in the RB basement. The thickness of the containment structure has been increased to 1.5 m, to meet the requirements for radiation shielding, missile protection, aircraft crash, and fire protection.

---

6 PARS have been added to CANDU 6 stations as a result of refurbishment work and/or due to Fukushima lessons learned.
The containment design described above includes design enhancements that have been made for the EC6:

- The design pressure of the reactor building has been increased to 400 kPa(g).
- Increased thickness of concrete.
- Increased level of seismic qualification.
- Addition of the steel liner along the entire inside surface of the containment structure.
- A protective layer of refractory concrete is provided on top of the calandria vault floor. It delays molten core interaction with structural concrete, slows down the rate of production of non-condensable gasses, and hence reduces the rate of containment pressurization.
- Capability to prevent containment failure due to over pressurization during severe accidents through core heat removal and containment spray cooling provided by SARHRS.

Controlling and Filtering Releases

As a result of the Fukushima lessons learned and to meet regulatory requirements to control, monitor and filter releases, the EC6 will include an emergency filtered containment venting system (EFCVS) for relief of pressure and removal of aerosols and iodine, to be used as a last resort in a severe accident event. The emergency filtered containment venting system will be protected from external events, such as seismic. Some CANDU 6 plants, have incorporated an EFCVS, either due to refurbishment or as a result of Fukushima lessons learned. For the EC6, the emergency filtered containment venting system (EFCVS) is not credited to meet safety goals, rather it is part of SAMG function in the unlikely event of overpressurization of the containment to prevent unfiltered releases of radioactive products.

3.1.2.4 Final assessment of criterion CR1.3.4 Barriers

Depending on the accident severity, a minimum of two confinement barriers can be maintained by CANDU 6 and EC6 designs. As well, the fuel channels may remain intact, as long as they are surrounded by water. The EC6 improves safety margins for containment design by increasing containment design pressure from 124 kPa(g) to 400 kPa(g) with a conservative design margin. The EC6 is designed with ‘enhanced’ defence in depth provisions than the CANDU 6 plants, resulting with improved barriers to protect the plant, public and environment.

Therefore, criterion CR 1.3.4 on barriers has been demonstrated by the EC6 design.

3.1.2.5 Assessment against CR1.3.5 Controlled State

- **Indicator IN1.3.5:** Capability of engineered safety features to restore the INS to a controlled state (without operator actions)
- **Acceptance Limit AL1.3.5:** the engineered safety features are sufficient to reach a controlled state after a DBA based on automatic actions within a grace period of at least 8 hours.
The CANDU 6 reactor design is based on a number of important safety concepts that include defence in depth, independence, diversity, redundancy, separation and fail safe design. These levels of defence include inherent and engineered features, with strict adherence to ensuring independence of each system dedicated to each level of defence. The EC6 design has enhanced the ability to restore plant to a normal status following upset conditions.

Reactor Shutdown Systems

AOOs – Anticipated Operational Occurrences conditions

The Reactor Regulating System (RRS) is used to control the core reactivity in normal plant operation and to reduce power or shut down the reactor for most abnormal events. The RRS in a CANDU 6 plants employs the following mechanisms: liquid zone controllers, adjuster rods, and control absorbers (and shutoff rod in withdrawal only). The control absorbers are typically held outside the reactor core and, in the case of abnormal events, are driven or dropped into the core. The RRS in the CANDU 6 plants is independent of both the shutdown systems in terms of design, mechanism, physical location, instrumentation and logic.

The EC6 design had enhanced the RRS functionality, from the CANDU 6 reference design, consistent with the expectations of requirements for new build designs [15]. RRS used redundant digital control, with a design unreliability of $10^{-2}$/year. In order to reduce the likelihood of unsafe failures of the control system, setback and stepback routines are incorporated into the digital control software. The EC6 design has added additional trip parameters for setback and stepback, as compared to the CANDU 6, refer to Table 3-15. These intercept deviations from normal operation by reducing power. They are not fully independent of the control system but use separate routines. In particular the stepback function (rapid power reduction by dropping the four control absorbers after an abnormal event) has been strengthened to be more independent (in software) of normal control, so that many faults can be terminated by stepback. The stepback routine is implemented in the Class 2 Essential control Subsystem, independent of the logic used for the reminder of the RRS. This independence results with a reduction of the frequency of Loss of Regulation (LOR) events caused by failures within the RRS partition, since stepback is still available. The stepback function can therefore handle certain AOOs without reliance on the shutdown system, as long as the fault is not caused by a common error in the control programme itself or one of its inputs.

Table 3-15: CR1.3.5 Evaluation for Improvement of Controlled State

<table>
<thead>
<tr>
<th>Design Feature</th>
<th>CANDU 6</th>
<th>EC6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 2 (AOO function)</td>
<td>• Setback: 9 parameters</td>
<td>• Setback: 14 parameters</td>
</tr>
<tr>
<td></td>
<td>• Stepback: 8 parameters</td>
<td>• Stepback: 10 parameters</td>
</tr>
<tr>
<td>DiD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3 (DBA)</td>
<td>• 28 shut-off rods and manual</td>
<td>• 32 shut-off rods and manual</td>
</tr>
</tbody>
</table>

Copyright © 2013 Candu Energy Inc. All rights reserved. Unauthorized use or reproduction is prohibited.
reactivity devices) DiD

- addition of liquid poison
  - Poison moderator
- addition of liquid poison or 10
  SQed Supplemental Rods
  - Improved safety
    margin for SDS1
  - Poison moderator

Level 3 DiD

- SDS1: 10 trip parameters
- SDS2: 9 trip parameters

SDS1: 15 trip parameters
SDS2: 14 parameters

Level 3, 4 and 5 DiD

- 1 Hour Group 1 batteries
  - battery life for CANDU 6
    plants has been extended
    based on distribution of
    loads
- 38 post accident monitoring
  (PAM) parameters for
  Operator Action

- 1 Hour Group 1 batteries
- 24 Hour UPS batteries
- 8 Hour batteries for Safety
  Monitoring
- Increased PAM for Operator
  Action
  - 22 existing parameters
    SQed
  - 7 parameters added for
    DBA (L3)
  - 36 parameters added for
    BDBA (L4&L5)

Trip Parameters

Each SDS is required to provide effective trips for both AOOs and DBA conditions. In addition, the EC6 design has improved trip coverage by adding five new trip parameters for SDS1 and SD2 for a total of four neutronic and eleven process trip parameters, refer to Table 3-16. The trip logic circuit consists of three independent channels where each channel has physically separated power supplies, trip parameter sensors, instrumentation, trip logic, conditioning and annunciations. This ensures maximum protection against single failures and common cause failures, in line with modern requirements. The trip signals for each parameter is triplicated and designed so that each of the three channels functions independently from the other two. Therefore, if any of the two channels is tripped, regardless of the parameter that caused the trip, a reactor trip is initiated. It is recognized, that some CANDU 6 plants, have incorporated additional process trip parameters, as part of improvement activities.

**Table 3-16: CR1.3.5 Trip Parameters**

<table>
<thead>
<tr>
<th>Shutdown Systems Trip Parameters</th>
<th>CANDU 6 (uses ion chambers to measure flux levels)</th>
<th>EC6 (uses fission chambers to measure neutron flux levels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- High Neutron power</td>
<td>a) Neutronic Trip Parameters:</td>
<td></td>
</tr>
<tr>
<td>- High rate log neutron power</td>
<td>- Regional overpower</td>
<td></td>
</tr>
</tbody>
</table>
### Shutdown Systems Trip Parameters

<table>
<thead>
<tr>
<th>CANDU 6 (uses ion chambers to measure flux levels)</th>
<th>EC6 (uses fission chambers to measure neutron flux levels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Heat transport system pressure</td>
<td>- protection (ROP) (based on in-core flux detectors).</td>
</tr>
<tr>
<td>- Low gross coolant flow</td>
<td>- Linear rate of in-core flux detector averaged signal (ICFDLR).</td>
</tr>
<tr>
<td>- High reactor building pressure</td>
<td>- High log rate (HLOGR) (based on out-of-core fission chambers).</td>
</tr>
<tr>
<td>- Low Pressurizer level</td>
<td>- Linear rate (HLINR) of fission chamber signal (based on out-of-core fission chambers).</td>
</tr>
<tr>
<td>- Steam Generator low level</td>
<td></td>
</tr>
<tr>
<td>- High Moderator temperature</td>
<td>b) Process Trip Parameters:</td>
</tr>
<tr>
<td>- Low Heat transport system pressure</td>
<td>- Heat transport system pump low speed (PLS).</td>
</tr>
<tr>
<td>- Steam Generator low pressure</td>
<td>- Heat transport system high pressure (HP).</td>
</tr>
<tr>
<td>* It is recognized that some CANDU 6 plants have added trip parameters, due to refurbishment (ie. moderator low and high level)</td>
<td>- Heat transport system low flow (LF).</td>
</tr>
<tr>
<td></td>
<td>- Pressurizer low level (PLL).</td>
</tr>
<tr>
<td></td>
<td>- Steam generator low level (SGLL).</td>
</tr>
<tr>
<td></td>
<td>- Steam generator feedline low pressure (SGFLP).</td>
</tr>
<tr>
<td></td>
<td>- Reactor Building high pressure (RBHP).</td>
</tr>
<tr>
<td></td>
<td>- Moderator high temperature (MHT).</td>
</tr>
<tr>
<td></td>
<td>- Moderator high level (MHL).</td>
</tr>
<tr>
<td></td>
<td>- Moderator low level (MLL).</td>
</tr>
<tr>
<td></td>
<td>- Manual Trip.</td>
</tr>
</tbody>
</table>

* It is recognized that some CANDU 6 plants have added trip parameters, due to refurbishment (ie. moderator low and high level)
The approach for CANDU 6 reactors has been strict separation of control and safety systems, to the point that they share no detectors, instrumentation, logic or end devices. Therefore, in addition to the reactivity control system, there are two independent shutdown systems, each individually capable of shutting down the reactor for all design basis accidents. The importance of reliable reactor shutdown after an accident has been recognized in the early days of CANDU and culminated in the provision of two shutdown systems on all modern CANDU reactors. Shutdown System 1 (SDS1) consists of spring-assisted gravity operated rods (not those used by the control system) which fall into the moderator between the rows of channels; and Shutdown System 2 (SDS2) consists of liquid absorber injection into the moderator through horizontal perforated tubes. Both use independent and diverse three-channel computerized trip logic, in a two-out-of-three voting arrangement. The trip computers for each shutdown system use different platforms, and the software is developed by independent engineering teams using fundamentally different methods. Both systems are fast (< 2 seconds) and automatic. Both can achieve short-term shutdown. SDS2 can also achieve long-term hold-down, while SDS1 needs to be supplemented by manual poison addition to the moderator in the longer term (tens of minutes to hours, depending on the accident) as xenon decays for a CANDU 6. The EC6 design has added additional rods to SDS1, to provide another option for achieving guaranteed shutdown (GSS mode). In addition, the slower shutdown system, SDS1 has been modified for the EC6 design to improve the safety margin for a large loss of coolant accident (LLOCA), which reduces the power pulse in a LLOCA by almost a factor of 2.

Administrative Control: Automatic Actions

The EC6 design has made improvements to reduce operator demand during accident conditions. In case of an extended station blackout (SBO), a seismically qualified UPS is provided to power loads required for heat sink. At the onset of a Class III failure, the UPS batteries are in a fully-charged state capable of supporting the EPS loads for up to 24 hours for monitoring and manual control functions during a SBO event. Furthermore, with the objective to lessen demand on operator intervention required for manual actions, the safety related computers, that allow safety critical actions to be performed automatically are now available for a minimum of 8 hours following a loss of power event for the EC6. After that the demand for required operator actions is significantly reduced. The EC6 design has improved operator monitoring capability during accident conditions by adding additional parameters, as presented in Table 3-15.

3.1.2.6 Final assessment of criterion CR1.3.5 Controlled State

The EC6 is designed with improved margins for shutdown in reaching a controlled state, than the CANDU 6 plants, consistent with the latest regulatory expectations. Therefore, criterion CR 1.3.5 on controlled state has been demonstrated by the EC6 design.
3.1.2.7 Final assessment of user requirement UR1.3 - Design Basis Accidents

It has been demonstrated that the EC 6 design has improved safety features, additional barriers for defence in depth and improved margins for shutdown, than the CANDU 6 plants, demonstrated by CR 1.3.3, 1.3.4 and 1.3.5 that pertain the Fukushima lessons learned. Therefore, user requirement UR1.3 is deemed to have been met by the EC6 design.

3.1.3 User Requirement UR1.4 – Release into Containment

The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated.

3.1.3.1 Assessment against CR1.4.1 Frequency of release into containment

- **Indicator IN1.4.1**: Calculated frequency of major release of radioactive materials into the containment/confinement based on frequency calculated for a highly degraded core.
- **Acceptance Limit AL1.4.1**: The frequency is an order of magnitude less than for existing sites.

The Level 1 PSA identifies initiating events by conducting a systematic review of plant design for initiating events and evaluates the plant response following these initiating events. It consists of the identification and quantification of accident sequences that could lead to core damage and gives insights into the performance of the safety systems aimed to prevent core damage. The Level 1 PSA evaluates the summed severe core damage frequency as a measure of risk, and demonstrates the compliance with regulatory safety goal for core damage frequency. The Level 1 PSA insights are used to provide: feedback into the design change process for modifications and refinements, input to technical specifications, outage planning, emergency operating procedures and to the risk-importance decision making process. A Level 2 PSA extends analysis of reactor core damage provided by Level 1 PSA in order to quantify releases of radioactivity into environment.

The EC6 is designed to meet the safety goals established for new designs for the core damage frequency (CDF):

*Core damage frequency (CDF): The sum of frequencies of all events sequences that can lead to significant core degradation is less than 10^{-5} per reactor year. The design should be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account.* [15]

For the comparison, a refurbished CANDU 6 CDF results will be applied, as discussed in Section 2.1, which include a number of design changes and safety upgrades during the refurbishment. From the Figure 3-7 and 3-8 below, it can be seen that the EC6 safety goals for CDF (1E-5/year) is met with margin, thereby an improvement over the CANDU 6 reference design.
Figure 3-7: Severe Core Damage Margin

CANDU 6 vs. EC6 - Severe Core Damage Margin

Target: CDF < 1E-4/year

Safety Goal: CDF < 1E-5/year
3.1.3.2 Final assessment of user requirement UR1.4 – Release into Containment
The EC6 is designed to meet more rigorous safety goals than CANDU 6 plants, which it achieves with margin. Therefore, criterion CR1.4.1 and UR1.4 on release into containment has been demonstrated by the EC6 design.

3.1.4 User Requirement UR 1.5 – Release into Environment
A major release of radioactivity from an installation of a NEW should be prevented fall all practical purposes, so that NES installation would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose.

INPRO has developed three criteria for this user requirement. CR 1.5.1 relating to the frequency of major release of radioactivity into the environment is deemed to be pertaining to Fukushima lessons learned.

3.1.4.1 Assessment against CR1.5.1 Major release to environment

- **Indicator IN1.5.1:** Calculated frequency of a major release of radioactive materials to the environment:
- **Acceptance Limit AL1.5.1:** The frequency is well below $10^{-6}$ per unit-year or practically excluded by design.

A nuclear power plant is designed to limit any radioactive exposure to the public to acceptable levels for a wide variety of postulated accidents. A probabilistic safety assessment (PSA) is used as a valuable tool for assessing the adequacy of plant design by identifying the plant features that contribute most to the dominant accident sequences. PSA is used to assess different design options at an early stage of the design process, providing feedback from past similar designs and identifying areas for improvements.

One of the main objectives of a PSA is to give confidence that the design will comply with the fundamental safety objectives and to demonstrate that a balanced design has been achieved. The EC6 is designed to meet the safety goals and acceptance criteria for new build designs:

*Small release frequency (SRF): The sum of frequencies of all event sequences that can lead to release to the environment of more than $10^{15}$ Bq of iodine-131 is less than $10^{-5}$ per reactor year. A greater release may require temporary evacuation of the local population [15],*

*Large release frequency (LRF): The sum of frequencies of all events sequences that can lead to release to the environment of more than $10^{14}$ Bq of cesium-137 is less than $10^{-6}$ per reactor year. A greater release may require long term evacuation of the local population [15]*
In addition, the EC6 is designed to meet containment performance criteria for severe accidents:

*Containment maintains its role as a leak-tight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage.*

*Containment also prevents uncontrolled releases of radioactivity after this period [15]*

Based on the preliminary PSA results, the LRF safety goal (1E-6/year) is expected to be met with margin, as presented in Figure 3-8.

**Figure 3-8: LRF Margin (with seismic)**
The EC6 design has incorporated an emergency filtered containment venting system (EFCVS) as a complementary design feature to prevent uncontrolled, unmonitored and unfiltered releases. Some CANDU 6 plants have or are in the process of installing an EFCVS.

3.1.4.2 Final assessment of user requirement UR1.5 – Release into Environment

The EC6 design meets more stringent safety goal requirements than the CANDU 6 plants, and therefore more margin exist in the EC6 design. The Emergency Filtered Containment Venting System is not required to meet the safety goals for the EC6 design, as it is a last resort to prevent uncontrolled and unfiltered releases. The EC6 design meets UR 1.5 and no major releases of radioactivity should occur thereby avoiding relocation or evacuation measures.

Therefore, criterion CR1.5.1 and UR1.5 on release to the environment has been demonstrated by the EC6 design.

3.1.5 User Requirement UR1.6 - Independence of DID Levels

An assessment should be performed for an INS to demonstrate that different levels of defence-in-depth are met and are more independent from each other than for existing systems.

3.1.5.1 Assessment against CR1.6.1 Independence of DID levels

- Indicator IN1.6.1: Independence of different levels of DiD
- Acceptance limit AL1.6.1: Adequate independence is demonstrated through deterministic and probabilistic means and other analyses.

The CANDU 6 plants were originally designed with independence between levels 1, 2 and 3 DiD for control of reactivity, removal of heat from the core, confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases. Some CANDU plants have installed systems, structures and components to improve the level 4 DiD, in part to address the external hazards that lead to prolonged loss of AC power, loss of the ultimate heat sink and loss of emergency response capability.

The EC6 design has added improvements relative to the reference CANDU 6 plant to provide independence between levels 1 through 5 DiD for control of reactivity, removal of heat from the core, confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases. Hence, there are more systems, structures and components in each level of DiD for the EC6 design than for the CANDU 6 plants. Safety margins in each level of DiD for the EC6 design have been increased when compared to the corresponding safety margins for the CANDU 6 plants, as shown in the above discussions.

The results of the probabilistic safety analyses show lower values for CDF and LRF for the EC6 design, as shown in CR 1.4.1 and CR 1.5.1. These lower values of CDF and LRF are mainly...
arising from having greater safety margins in the systems, structures and components in level 3 DiD and more systems, structures and components in level 4 DiD.

3.1.5.2  Final assessment of user requirement UR1.6 – Independence of DID levels

The EC6 is designed to meet more stringent safety goals and provides complementary design features to cope with system challenges, that strengthen independence between the DiD levels. Therefore, criterion CR1.6.1 and UR1.6 on release to the environment has been demonstrated by the EC6 design.

4.  SUMMARY

The INPRO methodology for evaluation of reactor safety was used in a comparative assessment of the EC6 design to the CANDU 6 reference plants pertaining to Fukushima lessons learned. The EC6 comparative INPRO assessment evaluated the extent of the improvements in the EC6 design to respond to a Fukushima type of event, as compared to the reference plant based on the ‘defence in depth’ principle. The EC6 is considered an ‘evolutionary design’ for the INPRO methodology; that is an advanced design that achieves improvements over the existing CANDU 6 designs through small to moderate modification, with a strong emphasis on maintaining design proveness to minimize technological risk. The uncertainty of the INPRO assessment of the EC6 comparison to the CANDU 6 design, is judged to be low, based on the maturity level factors (Volume 1 of 9 in [1]), which includes a completion of all three phases of a vendor pre-licensing design review with the Canadian regulator [30].

The results of the INPRO comparative assessment of the EC6 design against the CANDU 6 plants, deemed to be most relevant to design features arising from the Fukushima lessons learned, show that defence-in-depth has been enhanced for the EC6 design. In particular, the barriers for defence in depth for external events, redundancy of heat sinks, control and monitoring, and protection against radiological releases have been strengthened, as compared to the reference CANDU 6 plants.

The EC6 design incorporates features for accident prevention, accident mitigation and accident control and monitoring. This includes improved operation performance, improved ability of the control system to handle AOOs, improved safety system performance, more robust leak-tight containment and more capability to prevent and mitigate severe accidents, which provide additional safety margins. The EC6 design has greater resistance to cliff-edge effects arising from prolonged loss of AC power, loss of the ultimate heat sinks and loss of accident monitoring capability.

The EC6 design and the CANDU 6 plants include similar provisions for flexible portable supplies of power and water which can be deployed if the permanently installed systems fail.
5. **REFERENCES**


[22] ENSREG, ‘Romania Peer Review Country Report – Stress tests performed on European nuclear power plants’.


APPENDIX A – CANDU 6 TECHNICAL SUMMARY
CANDU 6
Technical Summary
The systems described in this brochure are those of a typical CANDU 6 generating station; however, they are essentially the same as those of other CANDU stations in most respects.
CANDU nuclear power stations have consistently proven to be competitive with other types of nuclear power plants, while offering unique advantages to their operators. Some of the design features and unique characteristics of the CANDU reactor are:

- a reactor core comprising several hundred small diameter fuel channels rather than one huge pressure vessel
- heavy water (D₂O) for moderator and coolant
- separate low pressure moderator and high pressure fuel cooling systems
- on-power refuelling
- reactivity devices that are located in the cool low pressure moderator, and not subjected to high temperatures or pressures
- natural uranium fuel or other low fissile content fuel
- reduced consequences from accidental reactivity fluctuations — excess reactivity available from the fuel is small and the relatively long lifetime of prompt neutrons in the reactor precludes rapid changes in power levels
- two fully capable safety shutdown systems, independent from each other and the reactor regulating system.

This Technical Summary provides an overview of the CANDU 6 nuclear power system. All CANDU 6 power plants are fundamentally the same, although there are differences in detail: these largely result from different site conditions, and from improvements made in the newer designs.

The evolution of CANDU 6 is illustrated in the inside back cover.
Major Systems

Pictorial symbols representing major systems are used throughout this publication to indicate relationships between major systems and their sub-systems.

Systems that are not featured on this page are described later in the document.
A CANDU 6 nuclear steam supply system’s power production process starts like that of any other nuclear steam supply system, with controlled fission in the reactor core. However, unlike other reactors, the CANDU 6 is fuelled with natural uranium fuel that is distributed among 380 fuel channels. Each six-meter-long fuel channel contains 12 fuel bundles. The fuel channels are housed in a horizontal cylindrical tank (called a calandria) that contains cool heavy water (D₂O) moderator at low pressure. Fuelling machines connect to each fuel channel as necessary to provide on-power refuelling; this eliminates the need for refuelling outages.

The on-power refuelling system can also be used to remove a defective fuel bundle in the unlikely event that a fuel defect develops. CANDU 6 reactors have systems to identify and locate defective fuel.

Pressurized heavy water (D₂O) coolant is circulated through the fuel channels and steam generators in a closed circuit. The fission heat produced in the fuel is transferred to heavy water coolant flowing through the fuel channels. The coolant carries the heat to steam generators, where it is transferred to light water to produce steam. The steam is used to drive the turbine generator to produce electricity.
Turbine Generator System

The turbine generator system comprises steam turbines directly coupled to an alternating current electrical generator operating at synchronous speed.

- The steam turbine is a tandem compound unit, generally consisting of a double flow, high pressure turbine and three double flow, low pressure turbines, which exhaust to a high vacuum condenser for maximum thermal efficiency. The condenser may be cooled by sea, lake or river water, or by atmospheric cooling towers.

- The generator is a high efficiency hydrogen-cooled machine arranged to supply alternating current at medium voltage to the electric power system.

Electric Power System

The electric power system comprises a main power output transformer, unit and service transformers, and a switchyard. This system steps up (increases) the generator output voltage to match the electric utility’s grid requirements for transmission to the load centres and also supplies the power needed to operate all of the station services.

The main switchyard portion of the electric power system permits switching of outputs between transmission lines and comprises automatic switching mechanisms, and lightning and grounding protection to shield the equipment against electrical surges and faults.
Reactor
The reactor comprises a stainless steel horizontal cylinder (called the calandria), closed at each end by end shields, which support the horizontal fuel channels that span the calandria, and provide personnel shielding. The calandria is housed in and supported by a light water-filled, steel lined concrete structure (the reactor vault) which provides thermal shielding. The calandria contains heavy water (D₂O) moderator at low temperature and pressure, reactivity control mechanisms and several hundred fuel channels.

Fuel Handling System
The fuel handling system refuels the reactor with new fuel bundles without interruption of normal reactor operation; it is designed to operate at all reactor power levels. The system also provides for the secure handling and temporary storage of new and irradiated fuel.

Heat Transport System
The heat transport system circulates pressurized heavy water coolant (D₂O) through the reactor fuel channels to remove heat produced by fission in the uranium fuel. The heat is carried by the reactor coolant to the steam generators, where it is transferred to light water to produce steam. The coolant leaving the steam generators is returned to the inlet of the fuel channels.

Moderator System
Neutrons produced by nuclear fission are moderated (slowed) by the D₂O in the calandria. The moderator D₂O is circulated through systems that cool and purify it, and control the concentrations of soluble neutron absorbers used for adjusting the reactivity.

Feedwater and Steam Generator System
The steam generators transfer heat from the heavy water reactor coolant to light water (H₂O) to form steam, which drives the turbine generator. The low pressure steam exhausted by the low pressure turbine is condensed in the condensers by a flow of condenser cooling water. The feedwater system processes condensed steam from the condensers and returns it to the steam generators via pumps and a series of heaters.

Reactor Regulating System
This system controls reactor power within specific limits and ensures that station load demands are met. It also monitors and controls power distribution within the reactor core, to optimize fuel bundle and fuel channel power within their design specifications.

Safety Systems
Four special safety systems (shutdown system number 1, shutdown system number 2, the emergency core cooling system and containment system) are provided to minimize and mitigate the impact of any postulated failure in the principal nuclear steam plant systems. Safety support systems provide services as required (electric power, cooling water and compressed air) to the special safety systems. (See Safety Systems on page 46.)
Reactor Assembly

The CANDU 6 reactor assembly, shown in the figure opposite, includes the fuel channels contained in and supported by a horizontal cylindrical tank known as the calandria. The calandria is closed and supported by end shields at each end. Each end shield comprises an inner and an outer tubesheet joined by lattice tubes at each fuel channel location and a peripheral shell. The inner space of the end shields are filled with steel balls and water, and are water cooled. The fuel channels, supported by the end shields, are located on a square lattice pitch. The calandria is filled with heavy water moderator at low temperature and pressure. The calandria is located in a steel lined, water filled concrete vault.

Horizontal and vertical reactivity measurement and control devices are located between rows and columns of fuel channels, and are perpendicular to the fuel channels.

The fuel channels are also shown in the figure opposite, with additional detail provided in the accompanying figure. Each fuel channel locates and supports 12 fuel bundles in the reactor core. The fuel channel assembly includes a zirconium-niobium alloy pressure tube, a zirconium calandria tube, stainless steel endfittings at each end, and four spacers which maintain separation of the pressure tube and the calandria tube. Each pressure tube is thermally insulated from the cool, low pressure moderator, by the CO₂ filled gas annulus formed between the pressure tube and the concentric calandria tube.

Each end fitting incorporates a feeder connection through which heavy water coolant enters/leaves the fuel channel. Pressurized heavy water coolant flows around and through the fuel bundles in the fuel channel and removes the heat generated in the fuel by nuclear fission. Coolant flow through adjacent channels in the reactor is in opposite directions.

During on-power refuelling, the fuelling machines gain access to the fuel channel by removing the closure plug and shield plug from both end fittings of the channel to be refuelled.

Fuel

The CANDU 6 fuel bundle consists of 37 elements, arranged in circular rings as shown in the photo opposite. Each element consists of natural uranium in the form of cylindrical pellets of sintered uranium dioxide contained in a zircaloy 4 sheath closed at each end by an end cap. The 37 elements are held together by end plates at each end to form the fuel bundle. The required separation of the fuel elements is maintained by spacers brazed to the fuel elements at the transverse mid-plane. The outer fuel elements have bearing pads brazed to the outer surface to support the fuel bundle in the pressure tube.
Fuel Channel
End Shield
Tubesheet
Fuel Bundles
End Fitting
Feeder Pipe
Channel Closure
Liner Tube
Positioning Assembly
Heavy Water Moderator
Calandria
Lattice Tube
Fuel Channel
Calandria Tube
Gas Annulus
Spacers
Shield Plug
Pressure Tube
Fuel Bundles
Annulus Gas
Fuel Bundle
Heavy Water Coolant
Annulus Spacer
Calandria assembly schematic
Fuel channel arrangement
37 Element Fuel Bundle
The fuel handling system:

- provides facilities for the storage and handling of new fuel
- refuels the reactor remotely while it is operating at any level of power
- transfers the irradiated fuel remotely from the reactor to the storage bay.

**Fuel Changing**

The fuel changing operation is based on the combined use of two remotely controlled fuelling machines, one operating on each end of a fuel channel. New fuel bundles, from one fuelling machine, are inserted into a fuel channel in the same direction as the coolant flow and the displaced irradiated fuel bundles are received into the second fuelling machine at the other end of the fuel channel. Typically, either four or eight of the 12 fuel bundles in a fuel channel are replaced during a refuelling operation. For a CANDU 6 reactor, about 10 fuel channels per week are refuelled.

Either machine can load or receive fuel. The direction of loading depends upon the direction of coolant flow in the fuel channel being fuelled, which alternates from channel to channel.

The fuelling machines receive new fuel while connected to the new fuel port and discharge irradiated fuel while connected to the discharge port.

The entire operation is directed from the control room through a pre-programmed computerized system. The control system provides a printed log of all operations and permits manual intervention by the operator, if required.

**Fuel Transfer**

New fuel is received in the new fuel storage room in the service building. This room accommodates six months’ fuel inventory and can store temporarily all the fuel required for the initial fuel loading.

When required, the fuel bundles are transferred to the new fuel transfer room in the reactor building. The fuel bundles are identified and loaded manually into the magazines of the two new fuel ports. Transfer of the new fuel bundles into the fuelling machines is remotely controlled.

Irradiated fuel received in the discharge port from the fuelling machine is transferred into an elevator which lowers it into a water filled discharge bay. The irradiated fuel is then conveyed under water through a transfer canal into a reception bay, where it is loaded onto storage trays or baskets and passed into the storage bay.
The discharge and transfer operations are remotely controlled by station staff. Operations in the storage bays are carried out under water, using special tools aided by cranes and hoists. Defective fuel is inserted into cans under water to limit the spread of contamination before transfer to the defective fuel bay.

The storage volume of the bays has sufficient capacity for a minimum of 7 years’ accumulation of irradiated fuel.

Neither new or nor irradiated CANDU fuel can achieve criticality in air or light water, regardless of the storage configuration.
Moderator System

About four per cent of reactor thermal power appears in the moderator. The largest portion of this heat is from gamma radiation; additional heat is generated by moderation (slowing down) of the fast neutrons produced by fission in the fuel, and a small amount of heat is transferred to the moderator from the hot pressure tubes.

The system includes two 100 per cent capacity pumps, two 50 per cent flow capacity heat exchangers cooled by recirculated cooling water and a number of control and check valves. Connections are provided for the purification, liquid poison addition, heavy water (D$_2$O) collection, supply and sampling systems.

The moderator pump motors are connected to the medium voltage Class III power supply. In addition, each pump has a pony motor, capable of driving the pump at 25 per cent speed, connected to the Class II power supply. In the event of a loss of Class IV power (see page 34), the power to the main motors is lost until the diesel generators can supply Class III power. The cooling water supply to the heat exchangers is also re-established after three minutes at a reduced flow rate following a total failure of Class IV power. The rate of heat removal is sufficient to limit the increase of moderator temperature in the calandria to an acceptable value during a failure of Class IV power and subsequent reactor shutdown.

The heavy water in the calandria functions as a heat sink in the unlikely event of a loss of coolant accident in the heat transport system coincident with a failure of emergency core cooling.

Cover Gas System

Helium is used as the cover gas for the moderator system because it is chemically inert and is not activated by neutron irradiation. Radiolysis of the heavy water moderator in the calandria results in production of deuterium and oxygen gases. The cover gas system prevents accumulation of these gases by catalytically recombining them to form heavy water. The deuterium and oxygen concentrations are maintained well below levels at which an explosion hazard would exist.

The system includes two compressors and two recombination units which form a circuit for the circulation of cover gas through the calandria relief ducts. Normally one compressor and both recombination units operate, with the other compressor on standby.

Purification System

The moderator purification system:

- maintains the purity of D$_2$O, thereby minimizing radiolysis which can cause excessive production of deuterium in the cover gas.
- minimizes corrosion of components, by removing impurities present in the D$_2$O and by controlling the pD.
- under operator command reduces the concentration of the soluble poisons, boron and gadolinium, in response to reactivity demands.
- removes the soluble poison, gadolinium, after shutdown system number 2 has operated.

D$_2$O Sampling System

This system allows samples to be taken from the:

- main moderator system
- moderator D$_2$O collection system
- moderator purification system
- D$_2$O cleanup system.

Laboratory tests may be performed on the samples to determine:

- pD (pH)
- conductivity
- chlorides concentration
- isotopic purity
- boron and gadolinium concentration
- tritium content
- fluorides content
- organics content.
Operation of the Moderator System

The series/parallel arrangement of the system lines and valves permits the output from either pump to be cooled by both of the heat exchangers and assures an acceptable level of moderator cooling when either of the two pumps is isolated for maintenance. Reactor power must be reduced to about 60 per cent if one moderator heat exchanger is isolated.

The primary functions of the system are to:

• provide moderator cooling
• control the level of heavy water in the calandria
• maintain the calandria inlet temperature at approximately 70°C.
System Operation

The heat transport system (HTS) circulates pressurized D$_2$O coolant through the fuel channels to remove the heat produced by fission in the nuclear fuel. The coolant transports the heat to steam generators, where it is transferred to light water to produce steam to drive the turbine. Two parallel HTS coolant loops are provided in CANDU 6. The heat from half of the 380 fuel channels in the reactor core is removed by each loop. Each loop has one inlet and one outlet header at each end of the reactor core. D$_2$O is fed to each of the fuel channels through individual feeder pipes from the inlet headers and is returned from each channel through individual feeder pipes to the outlet headers. Each heat transport system loop is arranged in a ‘Figure of 8’, with the coolant making two passes, in opposite directions, through the core during each complete circuit, and the pumps in each loop operating in series. The coolant flow in adjacent fuel channels is in opposite directions. The HTS piping is fabricated from corrosion resistant carbon steel.

The pressure in the heat transport system is controlled by a pressurizer connected to the outlet headers at one end of the reactor. Valves provide isolation between the two loops and the pressurizer in the event of a loss-of-coolant accident.

Key Features

- The steam generators consist of an inverted U-tube bundle within a cylindrical shell. Heavy water coolant passes through the U-tubes. The steam generators include an integral preheater on the secondary side of the U-tube outlet section, and integral steam separating equipment in the steam drum above the U-tube bundle.
- The heat transport pumps are vertical, centrifugal motor driven pumps with a single suction and double discharge.
- Cooling of the reactor fuel, in the event of electrical power supply interruption, is maintained by the rotational momentum of the heat transport pumps during reactor power rundown, and by natural convection flow after the pumps have stopped.
- No chemicals are added to the heat transport system for the purpose of reactivity control.
- Carbon steel piping, which is ductile and relatively easy to fabricate and to inspect is used in the heat transport system.
- Radiation exposure to personnel is low because of the low fuel defect rate, and is minimized by designing for maintenance, application of stringent material specifications, controlling the reactor coolant chemistry and by providing radiation shielding.
### Heat Transport System Conditions

<table>
<thead>
<tr>
<th></th>
<th>Electrical Output (MW)</th>
<th>Number of Fuel Channels</th>
<th>Elements in Fuel Bundle</th>
<th>Number of Loops</th>
<th>Outlet header Pressure (MPa)</th>
<th>Maximum Channel Flow (kg/s)</th>
<th>Outlet Header Quality (%)</th>
<th>Total Operating Motor Rating (kW)</th>
<th>Operating Motor Rating (kW)</th>
<th>Motor Rating (kW)</th>
<th>Area (m²) per Steam Generator</th>
<th>Integral Preheater</th>
<th>Steam Pressure (MPa)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point Lepreau,</td>
<td>680/633</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>3200</td>
<td>Yes</td>
<td>4.7</td>
</tr>
<tr>
<td>Gentilly 2</td>
<td>675/638</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>3200</td>
<td>Yes</td>
<td>4.7</td>
</tr>
<tr>
<td>Wolsong 1</td>
<td>678/638</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>3200</td>
<td>Yes</td>
<td>4.7</td>
</tr>
<tr>
<td>Embalse</td>
<td>648/600</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>2800</td>
<td>Yes</td>
<td>4.7</td>
</tr>
<tr>
<td>Cernavoda 1, 2</td>
<td>710/665</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>3200</td>
<td>Yes</td>
<td>4.7</td>
</tr>
<tr>
<td>Wolsong 2, 3, 4</td>
<td>715/668</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>3200</td>
<td>Yes</td>
<td>4.7</td>
</tr>
<tr>
<td>Qinshen 1, 2</td>
<td>728/668</td>
<td>380</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>24</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>6700</td>
<td>3200</td>
<td>Yes</td>
<td>4.7</td>
</tr>
</tbody>
</table>

### Other CANDU operating stations

<table>
<thead>
<tr>
<th></th>
<th>Electrical Output (MW)</th>
<th>Number of Fuel Channels</th>
<th>Elements in Fuel Bundle</th>
<th>Number of Loops</th>
<th>Outlet header Pressure (MPa)</th>
<th>Maximum Channel Flow (kg/s)</th>
<th>Outlet Header Quality (%)</th>
<th>Total Operating Motor Rating (kW)</th>
<th>Operating Motor Rating (kW)</th>
<th>Motor Rating (kW)</th>
<th>Area (m²) per Steam Generator</th>
<th>Integral Preheater</th>
<th>Steam Pressure (MPa)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pickering A 4 Units</td>
<td>542/515</td>
<td>390</td>
<td>28</td>
<td>2</td>
<td>8.7</td>
<td>23</td>
<td>-</td>
<td>16</td>
<td>12</td>
<td>1420</td>
<td>1850</td>
<td>Yes</td>
<td>4.1</td>
</tr>
<tr>
<td>Bruce A 4 Units</td>
<td>904/840</td>
<td>480</td>
<td>37</td>
<td>1</td>
<td>9.1</td>
<td>24</td>
<td>&lt;1</td>
<td>4</td>
<td>4</td>
<td>8200</td>
<td>2400</td>
<td>No</td>
<td>4.4</td>
</tr>
<tr>
<td>Pickering B 4 Units</td>
<td>540/516</td>
<td>380</td>
<td>28</td>
<td>2</td>
<td>8.7</td>
<td>23</td>
<td>-</td>
<td>16</td>
<td>12</td>
<td>1420</td>
<td>1850</td>
<td>Yes</td>
<td>4.1</td>
</tr>
<tr>
<td>Bruce B 4 Units</td>
<td>915/860</td>
<td>480</td>
<td>37</td>
<td>1</td>
<td>9.1</td>
<td>24</td>
<td>&lt;1</td>
<td>4</td>
<td>4</td>
<td>8200</td>
<td>2400</td>
<td>No</td>
<td>4.7</td>
</tr>
<tr>
<td>Darlington 4 Units</td>
<td>936/881</td>
<td>480</td>
<td>37</td>
<td>2</td>
<td>10.0</td>
<td>25</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>9600</td>
<td>4900</td>
<td>Yes</td>
<td>5.1</td>
</tr>
</tbody>
</table>
Heat Transport Auxiliary Systems

Pressure and Inventory Control System

The heat transport pressure and inventory control system consists of a pressurizer, D\textsubscript{2}O feed-pumps, feed and bleed valves and a D\textsubscript{2}O storage tank. This system provides:

- pressure and inventory control for each heat transport system loop
- overpressure protection
- a controlled degassing flow.

Heavy water in the pressurizer is heated electrically to pressurize the vapour space above the liquid. The volume of the vapour space is designed to cushion pressure transients, without allowing excessively high or low pressures in the heat transport system.

The pressurizer also accommodates the change in volume of the reactor coolant in the heat transport system from zero power to full power. This permits the reactor power to be increased or decreased rapidly, without imposing a severe demand on the D\textsubscript{2}O feed and bleed components of the system.

When the reactor is at power, pressure is controlled by the pressurizer; heat is added to the pressurizer via the electric heaters to increase pressure, and heat is removed from the pressurizer via D\textsubscript{2}O steam bleed to reduce pressure. The coolant inventory is adjusted by the feed and bleed circuit. Pressure can also be controlled by the feed and bleed circuit with the pressurizer isolated at low reactor power and when the reactor is shut down. This feed and bleed circuit is designed to accommodate the changes in coolant volume that take place during heat-up and cool-down.

D\textsubscript{2}O Collection System

- collects leakage from mechanical components
- receives D\textsubscript{2}O sampling flow
- receives D\textsubscript{2}O drained from equipment prior to maintenance.

The collected D\textsubscript{2}O is pumped from the collection tank to the storage tanks of the pressure and inventory control system for re-use in the heat transport system. However, if the isotopic purity of the collection tank contents is low, the D\textsubscript{2}O can be pumped to drums for upgrading.

Shutdown Cooling System

The shutdown cooling system is capable of:

- cooling the heat transport system from 177°C down to 54°C, and holding the system at that temperature indefinitely
- providing core cooling during maintenance work on the steam generators and heat transport pumps when the heat transport system is drained down to the level of the headers
- of being put into operation with the heat transport system at full temperature and pressure.

The shutdown cooling system consists of two independent circuits, one located at each end of the reactor. Each circuit consists of a pump and a heat exchanger, connected between the inlet and outlet headers of both heat transport system loops. The system is normally full of D\textsubscript{2}O and isolated from the heat transport system by power operated valves.

The shutdown cooling pumps are sized so that no boiling can occur in any of the fuel channels. For normal cool-down, steam from the steam generators bypasses the turbine and flows into the turbine condenser to reduce the heat transport system temperature to 177°C in approximately 30 minutes.

For cool-down from 177°C to 77°C, the isolating valves at the reactor headers are opened and all heat transport pumps are kept running. The heat transport pumps force a portion of the total core flow through the shutdown cooling heat exchangers, where it is cooled by recirculated cooling water flowing around the heat exchanger coils.

At 77°C, the heat transport pumps are shut down and the shutdown cooling system pumps are started. The system is then cooled to 54°C. D\textsubscript{2}O can be drained down to the level just above the reactor headers, if required for maintenance of the steam generators or pumps.
**Purification System**

The heat transport purification system:

- limits the accumulation of corrosion products in the coolant by removing soluble and insoluble impurities
- removes accumulations of fine solids following their sudden release due to chemical, hydraulic or temperature transients
- maintains the pH of D$_2$O at the required value.

Flow is taken from one reactor inlet header of each heat transport loop, passed through an interchanger, cooler, filter and ion exchange column before being returned through the interchanger to a pump inlet in each circuit. The heat transport pump provides the flow through the purification system. The interchanger-cooler combination minimizes the heat loss in the D$_2$O purification cycle.

Isolating valves in the purification system inlet and outlet lines are provided for maintenance. The valves also allow draining of the heat transport system coolant to just above the elevation of the headers without the need to drain the purification system. These valves close automatically in the event of loss-of-coolant accident.
The fundamental design requirement of the reactor regulating system (RRS) is to control the reactor power at a specified level and, when required, to manoeuvre the reactor power level between set limits at specific rates.

The reactor regulating system combines the reactor’s neutron flux and thermal power measurements, reactivity control devices, and a set of computer programs to perform three main functions:

- monitor and control total reactor power to satisfy station load demands
- monitor and control reactor flux shape
- monitor important plant parameters and reduce reactor power at an appropriate rate if any parameter is outside specific limits.

**Control**

Reactor Regulating System action is controlled by digital computer programs which process the inputs from various sensing devices and activate the appropriate reactivity control devices.

All measurement and control devices are located perpendicular to and between rows or columns of fuel channels, in the low pressure moderator.

**Computer Programs**

The principal computer programs employed provide the following:

- reactor power measurement and calibration
- the demand power routine
- reactivity control and flux shaping
- setback routine
- stepback routine
- flux mapping routine.

**Instrumentation**

The principal instrumentation utilized for reactor regulation includes:

- ion chamber system
- self-powered, in-core, flux detector system
- thermal power instrumentation.

The nuclear instrumentation systems are designed to measure reactor neutron flux, over the full operating range of the reactor. These measurements are required as inputs to the reactor regulating system and the safety systems. The instrumentation for the safety systems is independent of that utilized by the reactor regulating system.

**Reactivity Control Devices**

Short-term global and spatial reactivity control is provided by:

- light water zone control absorbers
- mechanical control absorbers
- adjusters
- soluble poison* addition and removal to the moderator.

The zone control system operates to maintain a specified amount of reactivity in the reactor, this amount being determined by the specified reactor power setpoint. If the zone control system is unable to do this, the program in the reactor regulating system calls on other reactivity control devices. Adjusters are removed from the core for positive reactivity shim. Negative reactivity is provided by the mechanical control absorbers or by the automatic addition of poison to the moderator.

**Stepback/Setback Routines**

In addition to controlling reactor power to a specified setpoint, the reactor regulating system monitors a number of important plant parameters. If any of these parameters is outside specific limits, reactor power is reduced. This power reduction may be fast (stepback), or slow (setback), depending on the possible consequences of the particular parameter excursion. The power reduction/shutdown functions provided by the reactor regulating systems are completely separate and independent of the two special safety shutdown systems (see safety systems section on page 46).

* A neutron absorbing substance
Reliability

The reliability of the reactor regulating system is of paramount importance and is achieved by:

- direct digital control from dual redundant control computers
- self-checking and automatic transfer to the standby computer on fault detection
- control programs that are independent of each other
- duplicated control programs
- duplicated and triplicated inputs
- hardware interlocks that limit the amount and rate of change of positive reactivity devices.
Reactor Power Measurements

For the reactor regulating system to control total reactor power and to maintain the proper power distribution in the reactor, power measurements in the reactor core are required.

In the high power range, zonal reactor power estimates based on platinum flux detectors are adjusted by comparison with thermal and vanadium flux detector measurements. In the low power range, total reactor power is determined based on measurements from uncompensated ion chambers with logarithmic amplifiers.

The Demand Power Routine

The demand power routine serves three functions:
- selects the mode of operation of the plant
- calculates the reactor power setpoint
- calculates an effective power error that is used as the driving signal for the reactivity control devices.

Reactivity Control and Flux Shaping

Long-term reactivity control in CANDU 6 is provided by the on-power refuelling system. Depleted fuel bundles are removed and new fuel bundles added to the core in a manner that maintains a constant long-term reactivity distribution throughout the core. The functions of short-term reactivity control and flux shaping are performed by the light water zone control absorbers, adjusters, mechanical control absorbers, and moderator poison control.

The primary method of short-term reactivity control is by varying the levels of light water in the liquid zone control system water compartments.

Setback Routine

The setback routine monitors a number of plant parameters and reduces reactor power gradually, in a ramp fashion, if any parameter exceeds specified operating limits. The rate at which reactor power is reduced and the level at which the setback is terminated are determined by the particular parameter.

Stepback Routine

A situation which could possibly result in damage is indicated when certain plant variables are outside their specified ranges. The stepback routine checks the values of these variables and if necessary, disengages the clutches of the mechanical control absorbers. This allows the absorbers to drop into the core, to produce a rapid decrease in power.

Flux Mapping Routine

The flux mapping routine uses measurements from vanadium detectors to calculate the spatial distribution of reactor power. Flux mapping serves the following functions:
- guards against locally over-rating the fuel
- helps to calibrate the zone power detectors to properly reflect the spatial flux distribution
- provides information for optimizing power output and fuel management.
The instrumentation systems provide the operating personnel with measurements of the reactor-neutron flux and with other core information. These systems also provide the necessary inputs for reactor regulation during start-up, shutdown, steady power and power manoeuvring conditions. Proportional counters, uncompensated ion chambers, and self-powered in-core flux detectors are used to provide continuous measurement of the reactor power from spontaneous fission level to 150 per cent full power (approximately 14 decades). A minimum overlap of one decade is provided between successive ranges of instrumentation.

**Start-Up Instrumentation**

This temporary instrumentation is required during the initial reactor start-up to monitor the neutron flux over the range from the spontaneous fission flux level to the sensitivity level of the permanent ion chambers. After start-up, this instrumentation is removed and is not required for subsequent start-ups, unless a prolonged shutdown, more than 30 days, occurs. In this case, the residual flux, due mainly to photoneutron production, decays beyond the sensitivity of the ion chambers. Two sets of triplicated fission chambers are used. One set covers the very low flux range ($10^{-14}$ to $10^{-10}$ of full power). The second set covers the flux range from $10^{-11}$ to $10^{-6}$ of full power and overlaps the ranges of both the first set and the permanent ion chamber instrumentation.

**Ion Chamber System**

Three ion chambers are employed in the reactor regulating system, for measuring neutron flux in the range from $10^{-7}$ to 15 per cent of full power. Compensation is not required, since adequate discrimination against gamma rays is achieved by employing appropriate materials in the detector and by gamma shielding in the construction of the ion chamber housings. These ion chambers are located in housings at one side of the core. In addition to one ion chamber for the reactor regulating system, each housing also contains an ion chamber and shutter for shutdown system number 1. Each of the three channels consists of an ion chamber and amplifier unit. The solid state amplifiers upgrade the ion chamber outputs to suitable input signal levels for processing in the control computers. Three similar ion chambers, mounted on the other side of the core, provide inputs to shutdown system number 2.

**Self-powered In-core Flux Detectors**

In the high power range (above 15 per cent power), self powered in-core flux detectors provide the required spatial flux information not available from the ion chambers.

Two types of in-core detectors are used in the reactor. One type uses platinum as the sensitive emitter material, while the other uses vanadium. The sheaths of both types are made of Inconel. The platinum detectors are fast-acting, sensitive to both neutrons and gamma rays, and because of their prompt response to flux changes are used in the reactor regulating system and in the two shutdown systems. The vanadium detectors are sensitive to neutrons, but because of a relatively slow response to flux changes, are used only in the flux mapping system.

The in-core flux detectors of the regulating system and of shutdown system number 1 are mounted vertically in the core, while those of shutdown system number 2 are mounted horizontally in the core.
Light Water Zone Control Absorbers

Light water ($H_2O$) is a neutron absorber (poison) in the heavy water cooled and moderated CANDU 6 reactor. The liquid zone control system takes advantage of this fact to provide short-term global and spatial reactivity control in the CANDU 6 reactor core.

The liquid zone control system in the reactor consists of six tubular, vertical zone control units that span the core. For flux control the zone control units are located such that 14 zone control compartments are formed and are distributed through the core. Each zone control unit can comprise either of two or three zone control compartments. Flux (power) in each zone is controlled by the addition or removal of light water from the liquid zone control compartment in that zone.

Mechanical Control Absorbers

Four mechanical control absorbers, mounted above the reactor, can be driven in or out of the core at variable speeds, or dropped by gravity into the core, between columns of fuel channels, by releasing a clutch. These absorbers are normally parked out of the core; they are driven in to supplement the negative reactivity from the light water zone control absorbers, or are dropped to effect a fast reduction in reactor power (stepback). When inserted, the mechanical control absorbers also help to prevent the reactor from going critical when the shutoff rods of shutdown system 1 are withdrawn, and are interlocked, in this inserted position, until the shutdown system number 1 is energized and available.

Adjusters

Adjusters are cylindrical neutron absorbing rods. A CANDU 6 reactor typically has 21 vertically mounted adjuster rods, normally fully inserted between columns of fuel channels for flux shaping purposes.

Removal of adjusters from the core provides positive reactivity to compensate for xenon buildup following large power reductions, or in the event that the on-power refuelling system is unavailable. The adjusters are capable of being driven in and out of the reactor core at variable speed to provide reactivity control. The adjusters are normally driven in banks, the largest bank containing five rods.

Adjusters are usually fabricated from stainless steel. In some CANDU plants the adjusters are made from cobalt, and are used to produce cobalt 60 for medical and industrial purposes.

Poison Addition and Removal

A reactivity balance can be maintained by the addition of soluble poison to the moderator. Boron is used to compensate for an excess of reactivity when fresh fuel is introduced into the reactor. Gadolinium is added when the xenon load is significantly less than equilibrium (as happens after prolonged shutdowns).

An ion exchange system removes the poisons from the moderator. Addition and removal of poison is normally controlled by the operator. However, the reactor regulating system can also add gadolinium, in special circumstances.
**Hardware Interlocks**

The reactivity mechanisms are subject to a number of interlocks, external to the control computers, which limit the consequences of erroneous operation of these mechanisms.

When the reactor is in a tripped state (i.e., shutdown system 1 and/or shutdown system 2 inserted) these interlocks prevent withdrawal of the adjusters and mechanical control absorbers. Poison removal from the moderator is also inhibited to prevent increases in reactivity.

The interlocks remain active, preventing reactor startup, until shutoff rods are fully withdrawn and available for reactor shutdown. There are further interlocks to prevent more than a limited number of high worth adjusters from being withdrawn at the same time. This limits the rate of positive reactivity insertion.

With the exception of the light water zone controllers, which are controlled only from the computer, the reactivity control units can also be manually controlled from the control room panels.
Feedwater System

Feedwater from the regenerative feedwater heating system is supplied separately to each steam generator. The feedwater is pumped into the steam generators by three 50 per cent capacity multi-stage feedwater pumps with the flow rate to each steam generator regulated by feedwater control valves. A check valve in the feedwater line to each steam generator is provided to prevent backflow in the unlikely event of feedwater pipe failure. An auxiliary feedwater pump is provided that can supply four per cent of full power feedwater requirements during shutdown conditions, or if the main feedwater pumps become unavailable.

The chemistry of the feedwater to the steam generators is precisely controlled by demineralization, deaeration, oxygen scavenging and pH control. A blowdown system is provided for each steam generator that allows impurities collected in the steam generators to be removed in order to prevent their accumulation and possible long-term corrosive effects.

Steam Generators and Main Steam Systems

Reactor coolant (heavy water) flows through small tubes, arranged in an inverted, vertical, U-tube bundle, within each of the four steam generators and transfers heat to the re-circulated water outside the tubes, producing steam. Moisture is removed from the steam by steam separating equipment located in the drum (upper section) of the steam generator. The steam then flows via four separate steam mains, through the reactor building wall, to the turbine where they connect to the turbine steam chest.

The steam pressure is normally controlled by the turbine governor valves that admit steam to the high pressure stage of the turbine. If the turbine is unavailable, up to 70 per cent of full power steam flow can bypass the turbine and go directly to the condenser. During this operation, pressure is controlled by the turbine bypass valves. Auxiliary bypass valves are also provided to permit up to 10 per cent of full power steam flow during low power operation.

Steam pressure can be controlled by discharging steam directly to the atmosphere via four atmospheric steam discharge valves which have a combined capacity of 10 per cent of full power steam flow. These valves are used primarily for control during warm-up or cool-down of the heat transport system.

Overpressure protection for the steam system is provided by four safety relief valves connected to each steam main.
Key to Diagram

1. Diesel room
2. Water treatment plant *
3. Crane hall
4. Turbine building
5. Turbine building crane
6. Generator
7. Condenser
8. Battery room
9. Boiler feed water tank
10. Deaerator storage tank
11. Deaerator
12. Reactor building
13. Dousing tank
14. Dousing water supply pipes
15. Dousing water valves
16. Dousing water spray nozzles
17. Steam pipes
18. Steam generators
19. Pressurizer
20. Crane
21. Heat transport pumps
22. Bleed condenser
23. Bleed cooler
24. Hatch
25. Reactor vault
26. Pressure relief pipes
27. Reactivity mechanism deck
28. Reactivity mechanism guide tubes
29. Calandria
30. Poison injection nozzles
31. Poison tanks
32. Ion chambers
33. Fuel channel assemblies
34. End shield
35. Headers
36. Feeder pipes
37. Fueling machine bridge
38. Bridge support column
39. Fueling machine
40. Catenary
41. Fuel channel end fittings
42. Steam generator support column
43. Feeder pipe insulation cabinet
44. Fueling machine vault door
45. End shield cooling
46. Fueling machine track
47. Moderator inlet pipe
48. New fuel handling machine
49. New fuel port
50. Fueling machine service ports
51. Rehearsal facility
52. Spent fuel port
53. Spent fuel elevator
54. Entrance to spent fuel area
55. Airlock
56. Crane
57. Spent fuel shipping area
58. Spent fuel handling area
59. Spent fuel bay gantry
60. Spent fuel bay
61. Spent fuel transfer baskets
62. Spent fuel transfer trolley
63. Spent fuel storage baskets
64. Fueling machine maintenance area
65. Decontamination room
66. New fuel storage
67. Tool crib
68. Vapour recovery equipment
69. Office
70. Control room *
71. Control equipment room
72. Computer room

* Some items have been moved for clarity.

Technical Data

<table>
<thead>
<tr>
<th>Reactor</th>
<th>Type</th>
<th>PHWR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thermal output (PHTS)</td>
<td>2064 MW(th)</td>
<td></td>
</tr>
<tr>
<td>Coolant flow rate (PHTS)</td>
<td>7.7 Mg/s</td>
<td></td>
</tr>
<tr>
<td>Design temperature (RIH)</td>
<td>279°C</td>
<td></td>
</tr>
<tr>
<td>Design pressure (RIH)</td>
<td>12.9 MPa(g)</td>
<td></td>
</tr>
<tr>
<td>Operating temperature (RIH)</td>
<td>286°C</td>
<td></td>
</tr>
<tr>
<td>Operating pressure (RIH)</td>
<td>11.7 MPa(abs)</td>
<td></td>
</tr>
<tr>
<td>Design temperature (ROH)</td>
<td>316°C</td>
<td></td>
</tr>
<tr>
<td>Design pressure (ROH)</td>
<td>10.7 MPa(g)</td>
<td></td>
</tr>
<tr>
<td>Operating temperature (ROH)</td>
<td>310°C</td>
<td></td>
</tr>
<tr>
<td>Operating pressure (ROH)</td>
<td>10.0 MPa(abs)</td>
<td></td>
</tr>
</tbody>
</table>

| Fuel Channels | Pressure tube inside diameter (cold, unpressurized) | 103.38 mm |
|               | Core Length (between calandria tubesheets) | 5.94 m |
|               | Number of pressure tubes | 380 |
|               | Coolant flow (nominal) | 24 kg/s |
|               | Est. pressure drop ~ 12 bundles | 838 kPa |
| Fuel | Length of bundle | 495.3 mm |
|      | Outside dia. of bundle (over bearing pads) | 102.4 mm |
| Weight of bundle (nominal) | 23.7 kg |
| Weight of uranium per bundle (nominal) | 19.2 kg |
| Sheath outside dia. (cold) | 13.1 mm |
| Sheath thickness (average) | 0.4 mm |
| Sheath material | Zircaloy - 4 |
| Elements per bundle | 37 |
| Fuel material | Natural UO₂ |
| Fuel bundles in core | 4500 |
| Fuel bundles per channel | 12 |
| Heat Transport System | Number of loops | 2 |
| Primary coolant | D₂O |
| Reactor inlet temperature | 286°C |
| Reactor outlet temperature | 310°C |

| Reactivity Control Units | Power control | 14 light water compartments |
|                         | 21 stainless steel rods |
|                         | 4 cadmium rods |
| Safety shutdown | 28 cadmium rods (vertical) |
|                     | 6 gadolinium nitrate injection tubes (horizontal) |
### Materials
- **(out of core)**: Stainless steel, zircaloy/stainless steel/cadmium
- **(in core)**: Zircaloy/stainless steel/cadmium

### Steam Generators
- **Type, number of units**: Vertical U-tube, 4
- **Steam flow for 4 steam generators**: 1033.0 kg/s
- **Steam pressure at full power**: 4.7 MPa(abs)
- **Steam temperature at full power**: 260° C
- **Maximum moisture**: 0.25%
- **Feedwater temperature**: 187° C

### Reactor Coolant Pumps
- **Number**: 4
- **Motor/type**: AC vertical, TEWAC induction
- **Rated capacity**: 2228 l/s
- **Rated head**: 215.0 m

### Containment
- **Type**: Prestressed cylindrical concrete
- **Inside diameter**: 41.46 m
- **Height Above Grade**: 46.02 m
- **Total Inside Containment**: 65,500 m³

### Turbine
- Single shaft tandem compound steam turbine directly coupled to 828 MVA generator. Steam turbine consists of one double flow high pressure cylinder, two external moisture separator/reheaters and three double flow low pressure cylinders.

### Generator
- Rated 828 MVA at 0.9 power factor and 414 kPa(g) hydrogen pressure. 1800 rpm with terminal voltage of 22,000 volts, 60 Hz.

### Condenser
- Single tube sheet shells. Each shell is connected to the three LP turbine exhausts. Two 100% main condensate extraction pumps and one auxiliary condensate extraction pump. Three 50% main steam generator feedwater pumps and one auxiliary steam generator feedwater pump.
The system consists of a turbine generator unit, and associated condensing and feedwater heating systems.

Steam produced in the steam generators enters the high pressure turbine and its water content increases as it expands through this high pressure stage. On leaving this stage, the steam passes through separators where the water is removed; it then passes through reheaters where it is heated by live steam taken directly from the steam mains. The reheated steam then passes through the low pressure turbines, into the condenser where it condenses to water which is then returned to the steam generators via the feedwater heating system.

Steam Turbine

The steam turbine is a tandem compound unit, directly coupled to an electrical generator by a single shaft. It comprises one double flow, high pressure cylinder followed by external moisture separators, live steam reheaters and three double flow, low pressure cylinders. The turbine is designed to operate with saturated inlet steam. The turbine system has main steam stop valves, governor valves, reheat intercept and emergency stop valves. All of these valves close automatically in the event of a turbine protection system trip.

Generator

The generator is a three-phase, four-pole machine. The generator typically operates at 1800 r.p.m. to serve 60 cycle electrical systems, and at 1500 r.p.m. to serve 50 cycle systems.

The associated equipment consists of a solid state automatic voltage regulator controlling a thyristor convertor which supplies the generator field via a field circuit breaker, generator slip rings and brush gear.

The main power output from the generator to the step-up transformer is by means of a forced air cooled, isolated phase bus duct, with tapoffs to the unit service transformer, excitation transformer and potential transformer cubicle.

Condensing System

The turbine condenser consists of three separate shells. Each shell is connected to one of the three low pressure turbine exhausts. Steam from the turbine flows into the shell where it is condensed by flowing over a tube bundle assembly through which cooling water is pumped. The condenser cooling water typically consists of a once-through circuit, utilizing water from an ocean, lake or river. The condensed steam collects in a tank in the bottom of the condenser called the “hot well”. A vacuum system is provided to remove air and other non-condensable gases from the condenser shells. The condenser is designed to accept turbine bypass steam to permit the reactor power to be reduced from 100 per cent power to 70 per cent if the turbine is unavailable. The bypass can accept 100 per cent steam flow for a few minutes, and 70 per cent of full power steam flow continuously.
**Feedwater Heating System**

On its return to the steam generators, condensate from the turbine condenser is pumped through the feedwater heating system. First it passes through three low pressure feedwater heater units, each of which contains two heaters fed by independent regenerative lines. (This permits maintenance work to be carried out on the heaters with only a small effect on the turbine generator output.) Two of the heater units incorporate drain cooling sections and the third a separate drain cooling stage. Next, the feedwater enters a deaerator where dissolved oxygen is removed. From the deaerator the feedwater is pumped to the steam generators through two high pressure feedwater heaters each incorporating drain cooling sections.
Electric Power System

Turbine Generator
The turbine generator system (described on page 30) consists of a turbine generator unit and associated condensing and feedwater systems. The power transmitted from the generator terminals to the main output transformer and the unit service transformer is at the generator nominal operating voltage.

Main Transformer
The main transformer steps up the generator output voltage to the same level as the switchyard transmission voltage. The transformer is rated to meet the generator output requirements and site environment. It is equipped with all standard accessories and the necessary protective equipment.

Switchyard
The switchyard, located near the turbine hall, contains the automatic switching mechanism, including the breakers and disconnects, which is the interface between the station and the power grid transmission lines. There are at least two incoming lines which are synchronized under normal conditions. However, the switchyard electrical equipment allows transmission of full station power through any one of the incoming lines.

Unit Service Transformer
During normal station operation the station services power is supplied by both the unit service transformer and the system service transformer. However, either transformer can provide the total service load in the event of a failure of one supply. The transformer is fed from the output system of the turbine generator.

System Service Transformer
The system service transformer is similar to the unit service transformer.

It supplies half of the plant services power requirements under normal operating conditions and is able to provide the total service load when necessary. This transformer is fed from the switchyard and supplies all plant loads during the start-up of the plant, or when the turbine generator is unavailable. It is located outdoors and feeds the station services located in the electrical equipment rooms.

Both the unit service and station service transformers are designed to automatically maintain voltage in the station services.

Qinshan Phase III, Units 1 and 2
Power Classification

The station services power supplies are classified in order of their levels of reliability requirement. The reliability requirement of these power supplies is divided into four classes that range from uninterruptible power to that which can be interrupted with limited and acceptable consequences.

Class IV Power Supply

Power to auxiliaries and equipment that can tolerate long duration interruptions without endangering personnel or station equipment is obtained from Class IV power supply.

This class of power supply comprises:

- Two primary medium voltage (MV) buses, each connected to the secondary windings of the system service and unit service transformers in such a way that only one bus is supplied from each transformer.
- Two MV buses supplied from the secondary windings of two transformers on the primary MV buses. These buses supply the main heat transport pumps, feed pumps, circulating water pumps, extractor pumps and chillers.

Complete loss of Class IV power will initiate a reactor shutdown.

Class III Power Supply

Alternating current (AC) supplies to auxiliaries that are necessary for the safe shutdown of the reactor and turbine are obtained from the Class III power supply, which comprises:

- Two medium voltage buses supplied from the secondary windings of the two transformers on the Class IV primary MV buses. These buses supply power to the pumps in the service water system, emergency core cooling system, moderator circulation system, shutdown cooling system, heat transport system feed lines, steam generator auxiliary feed line, and the air compressors and chillers.
- A number of low voltage buses.

Class II Power Supply

Uninterruptible alternating current (AC) supplies for essential auxiliaries are obtained from the Class II power supply, which comprises:

- Two low voltage AC three phase buses which supply critical motor loads and emergency lighting. These buses are each supplied through an inverter from a Class III bus via a rectifier in parallel with a battery.
- Three low voltage AC single phase buses which supply AC instrument loads and the station computers. These buses are fed through an inverter from Class I buses, which are fed from Class III buses via rectifiers in parallel with batteries.

In the event of an inverter failure, power is supplied directly to the applicable low voltage bus and through a voltage regulator to the applicable instrument bus. If a disruption or loss of Class III power occurs, the battery in the applicable circuit will provide the necessary power without interruption.

Class I Power Supply

Uninterruptible direct current (DC) supplies for essential auxiliaries are obtained from the Class I power supply, which comprises:

- Three independent DC instrument buses, each supplying power to the control logic circuits and one channel of the triplicated reactor safety circuits. These buses are each supplied from a Class III bus via a rectifier in parallel with a battery.
- Three DC power buses which provide power for DC motors, switchgear operation and for the Class II AC buses via inverters. These DC buses are supplied from Class III buses via a rectifier in parallel with batteries.

Automatic Transfer System

To ensure continuity of supply, in the event of a failure of either the unit or system power, an automatic transfer system is incorporated on the station service buses.

Transfer of load from one service transformer to the other is accomplished by:
- A manually initiated transfer of power under normal operating conditions, or an automatically initiated transfer for mechanical trips on the turbine.

- A fast open transfer of power, supplied automatically to both load groups of the class IV power supply system, when power from one transformer is interrupted. This fast transfer ensures that the voltage and phase difference between the incoming supply and the residual on the motors has no time to increase to a level that would cause excessive inrush currents.

- A residual voltage transfer, comprising automatic closure of the alternate breaker after the residual voltage has decayed by approximately 70 per cent. This scheme may require load shedding and could result in reactor power cut-back. It is provided as a back-up to the above transfers.

**Station Battery Banks**

The station battery banks are all on continuous charge from the Class III power supply and in the event of a Class III power disruption will provide power to their connected buses.

**Standby Generators**

Standby power for the Class III loads is supplied by two (or more) diesel generator sets, housed in separate rooms with fire resistant walls. Each diesel generator can supply the total safe shutdown load of the unit. The Class III shutdown loads are duplicated, one complete system being fed from each diesel generator. In the event of failure of Class IV power, the two diesel generators will start automatically.

The generators can be up to speed and ready to accept load in less than two minutes. The total interruption time is limited to three minutes. Each generator automatically energizes half of the shutdown load through a load sequencing scheme. There is no automatic electrical tie between the two generators, nor is there a requirement for them to be synchronized. In the event of one generator failing to start, the total load will be supplied from the other generator.

**Emergency Power Supply System**

The Emergency Power Supply System can provide all shutdown electrical loads that are essential for safety.

This system and its buildings are seismically qualified to be operational after an earthquake. The system provides a backup for one group of safety systems (shutdown system number 2, emergency water supply, secondary control area) if normal electric supplies become unavailable or the main control room becomes uninhabitable. The system comprises two diesel generating sets, housed in separate fire resistant rooms, which are self-contained and completely independent of the station’s normal services. There is adequate redundancy provided in both the generating distribution equipment and the loads.
Electric Power System Station Services

- Primary MV Buses
- Automatic Transfer Switch
- Turbine Services
- Reactor
- MV Buses
- Transformer
- Turbine Services Reactor
- Transformer Unit Service
- Inverters
- Batteries
- Rectifiers
- Motors
- Instrumentation
- Computers
- Safety Circuits Control Logic
- Motors
- Instrumentation
- Computers
- Motors
- Instrumentation
- Computers
Digital computers are used for station control, alarm annunciation, graphic data display and data logging. The system consists of two independent digital computers (DCCX and DCCY), each capable of station control.

Both computers run continuously, with programs in both machines switched on, but only the controlling computer’s outputs are connected to the station equipment. In the event that the controlling computer fails, the control of the station is automatically transferred to the “hot” standby computer.

Individual control programs use multiple inputs to ensure that erroneous inputs do not produce incorrect output signals. This is achieved by rejecting:

- analog input values that are outside the expected signal range
- individual readings that differ significantly from their median, average or other reference.

A spare computer is provided as a source of spare parts for the station computers. It is also used for:

- program assembling and checkout
- operator and maintainer training
- diagnosing faults in equipment removed from the station computers.

### Operator Communication Stations

These computerized stations replace much of the conventional panel instrumentation in the control room. A number of man-machine communication stations, each essentially comprising a keyboard and colour CRT monitor, are located on the main control room panels. The displays provided on the monitors include:

- graphic trends
- bar charts
- status displays
- pictorial displays
- historical trends.

Copies can be obtained from the line printers, of any display monitor the operator wishes to record.

### Automatic Transfer

A fault in any essential part of one computer results in automatic transfer of control to the other computer. If both computers fail, the station is automatically shut down.

### Alarm Annunciation

Alarm messages are presented on coloured display monitors (cathode ray tubes) which are centrally located above the station main control panels. Two line printers, one for each computer, provide chronological records of all alarm conditions.
Automatic Transfer Station Inputs

Digital Computer DCCX
- Reactor Control
- Heat Transport System Control
- Steam Generator Secondary Side Control
- Turbine Control
- Alarm Annunciation
- Alphanumeric Graphics Displays
- Fuel Channel Temperature Monitoring.

Digital Computer DCCY
- Reactor Control
- Heat Transport System Control
- Steam Generator Secondary Side Control
- Turbine Control
- Alarm Annunciation
- Alphanumeric Graphics Displays
- Fueling Machine Control.

Alarm Annunciation

Operator Communication Stations

Automatic Transfer

Station Control Outputs
Station instrumentation performs a number of monitoring, control and display functions. Nuclear instrumentation is provided to allow automatic control of reactor power and flux shape and to monitor local core behaviour. Conventional instrumentation provides signals for control and display of other plant variables.

The plant is automated to a level that requires a minimum of operator action for all phases of station operation. All major control loops employ the two computers as direct digital controllers. Conventional analog control instrumentation is used on smaller local loops.

The instrumentation required for the operation of the safety systems incorporates triplicated information channels that provide the system with a redundancy that ensures that single component failures will not cause spurious operation. The safety systems operate independently of the dual computers to avoid cross linked faults.

**Control Room**

The latest CANDU 6 control room is illustrated on the opposite page. The control room features an array of panels at the perimeter with two large central display screens, and the operations console. Information is provided on the panels and at the operations console to allow the station to be safely controlled and monitored.

The instrumentation and controls on the panels are grouped on a system basis, with a separate panel allocated to each major system. Coloured cathode ray tube (CRT) displays and advanced annunciation systems provide uncluttered control room panel layouts and excellent monitoring capabilities. The operator can call up information displays on the panel CRTs, the operating control console CRTs, and central display screens in a variety of alphanumeric and graphic formats via keyboards. All display annunciation messages are colour coded to facilitate system identification and the priority of the alarm.

Conventional display and annunciation instrumentation is provided for all safety related systems and to permit the station to be safely monitored in the event of dual computer failure, which automatically shuts down the reactor.

If for any reason the control room has to be evacuated, the station can be shut down and monitored from a remotely located secondary control area.
Control Room LAN:
- Enhanced Annunciation Interrogation
- Work Management Access
- Electronic Procedures
- Equipment Status Monitoring

PDS LAN:
Home for Critical Safety Parameter and Safety System Monitoring

Soft Function Keypads
- Display Selection
- Digital Entries
- One per VDU Display
- 2nd from right switchable for Overview Display Control
- Flat touchscreen technology

Trackballs
- Cursor and selection control for direct VDU display interaction
- Left or right hand mounting (operator adjustable)

Additional Console features Controls for:
- Alarm Silence/Acknowledge/Reset
- RRS Hold Power and Setback
- SDS1 Reactor Trip
- Telephone and Paging
- Headset Communication Jacks
Digital computers are used to perform all the control and monitoring functions of the station. The system is designed to:

- handle both normal and abnormal situations
- be capable of automatically controlling the unit at startup and at any preselected power level within the normal loading range
- be capable of automatically shutting down the unit if unsafe conditions arise
- be tolerant of instrumentation failures.

**Control Programs**

The functions of the overall station control system are performed by control programs loaded in each of the two unit computers. The major control function programs are described below, but there are also programs for:

- Heat Transport System Control
- Moderator Temperature Control
- Turbine Runup and Monitoring
- Fuel Handling System Control.

**Reactor Regulation**

This program adjusts the reactivity control devices to maintain reactor power equal to its desired setpoint.

**Steam Generator Pressure**

This program controls steam generator pressure to a constant setpoint, by changing the reactor power setpoint (normal mode), or by adjusting the station loads (alternate mode).

**Steam Generator Level**

This program controls the feedwater valves in order to maintain the water level in the steam generators at a reactor power dependent level setpoint.

**Heat Transport System Pressure**

This program controls the pressurizer steam bleed valves and heaters to maintain heat transport system pressure at a fixed setpoint.

**Control Modes**

**Reactor following turbine**

In this mode of operation the turbine-generator load is set by the operator: the steam generator pressure control program requests variations in reactor power to maintain steam generator pressure constant. This control mode is termed “reactor follows turbine” or “reactor follows station loads”.

**Turbine following reactor**

In this control mode, “turbine follows reactor”, the station loads are made to follow the reactor output. This is achieved by the steam generator pressure control program adjusting the plant loads to maintain a constant steam generator pressure. This mode is used at low reactor power levels, during startup or shutdown, when the steam generator pressure is insensitive to reactor power. It is also used in some upset conditions when it may not be desirable to manoeuvre reactor power.

**Unit Power Regulation**

This program manoeuvres the unit power, by adjusting the turbine load setpoint, to maintain the generator output at the level demanded by the local operator, or by a generation control signal from a remote control centre.
**Typical Site Layout**

General site requirements for a nuclear power plant:

- Land must be provided for an exclusion area around the plant. A perimeter of 914 meters from all reactors, on the landward side, was provided for CANDU plants put into operation before 1990: for some newer plants this distance, known as the exclusion radius, has been reduced to less than 500 meters.

- The site should be located so as to be easily incorporated into the utility’s electrical grid system.

- A relatively flat shelf of sedimentary rock a few metres above high water level is an ideal site, as both construction costs and site preparation time are reduced.

- Suitable land access by rail and/or road to transport heavy equipment. If site is on a navigable water body, water access may be used to transport the heaviest equipment.

**Buildings and Structures**

**Reactor Building**

The reactor building houses the nuclear reactor and auxiliaries, primary heat transport system, fuel handling equipment, and instrumentation.

The reactor building’s major structural components are:

- pre-stressed concrete containment structure
- internal reinforced concrete structures
- reinforced concrete calandria vault.

The containment structure is separated from the internal structural systems. This provides flexibility in over-all building construction and no inter-dependence between the containment wall and other structures.

**Service Building**

The service building houses nuclear facilities which can be located outside of the reactor building. More general service facilities, e.g., equipment maintenance shops and laboratory facilities, are located in the common area of this building.

The layout of the rooms within the service building provides for safety and efficiency of plant operation in terms of traffic patterns, radiation zoning and the routing of services between the buildings of the proposed unit. The irradiated fuel storage facility is also located in the service building.

**Turbine Building**

The turbine building consists of a turbine hall, auxiliaries bay and two single story annexes. Space is provided in the auxiliaries bay for the electrical power distribution equipment. Water treatment plant and diesel generators are located at grade level in the annexes.

Overhead traveling cranes are provided in the turbine hall for erection and maintenance of the turbogenerator and some of its auxiliaries. The turbine building has a reinforced concrete substructure, steel framed superstructure, steel roof trusses and insulated metal walls and roof.
**Pumphouse**

The pumphouse consists of a reinforced concrete substructure containing the condenser cooling water pumps, raw service water pumps, fire pumps, screens, and racks and screen wash pumps. A steel framed superstructure provides housing for the pump motors. Roof hatches are provided for installation and maintenance of the pumps.
Overall Requirements

Like most metals, fuel sheaths weaken at very high temperatures. Fuel sheath integrity is therefore at risk if a component failure causes the cooling of the fuel to be reduced relative to the power it produces.

If such a failure occurs, the reactor process systems can often stop its course or moderate its effects. Backing these up are special safety systems. They are independent of the process systems and of each other both functionally and physically, and are not used in the day-to-day operation of the plant. They can, if needed, shut down the reactor (shutdown systems), refill the reactor fuel channels with coolant and remove residual or “decay” heat from the fuel (emergency core cooling system) and prevent release to the environment of radioactivity which may escape from the reactor (containment systems).

Supporting these special safety systems are systems that provide alternate sources of electrical power (emergency power supply system) and cooling water (emergency water supply system).

Shutdown Systems

There are two ‘full capability’ reactor shutdown systems, each able of shutting down the reactor during any postulated accident condition.

The two shutdown systems are functionally and physically independent of each other; and from the reactor regulating system.

- Functional independence is provided by utilizing different shutdown principles: solid shutoff rods for System number 1, direct liquid poison injection into the moderator for System number 2.
- Physical independence of the shutdown systems is achieved by positioning the shutoff units vertically through the top of the reactor and the poison injection tubes horizontally through the sides of the reactor.

Post-shutdown Safety Systems

The emergency core cooling system removes decay (post shutdown) heat produced in the fuel in the event that there is a break in the heat transport system; this serves to prevent radioactivity from being released from the fuel.

The containment system confines any activity released from the fuel and heat transport system to the reactor building during an accident. Along with the other special safety systems, it ensures that the dose limits for accidents, set by the Canadian regulatory agency, the Atomic Energy Control Board, and the local regulatory authority are not exceeded.

Safety Support Systems

These systems may be used for normal station operation and are also used to support the operation of the safety systems.

Systems Grouping

To provide defence against low probability incidents such as local fires or missiles (turbine blades, aircraft strikes etc.), the station safety, post shutdown, and safety support systems are separated into two groups that are functionally and physically independent of each other. Each group is designed to provide the following functions:

- shut down the reactor
- to contain radioactivity in the process systems by assuring that decay heat is removed, or if the process systems are not intact, to prevent its release to the public
- supply the necessary information for post-accident monitoring.

The systems which provide these safety functions are:

- shutdown system number 1 or shutdown system number 2, to shut down the reactor
- the normal process systems, including normal electric power and service water systems; the emergency power supply and emergency water supply systems; and the emergency core cooling system, to remove decay heat
- the containment systems, to accommodate any accidental energy release and to contain the radioactivity that may be present in such a release
- the main control room or the secondary control area, for post accident monitoring.
**Shutdown System Number 1**

Shutdown system number 1 is the primary method of quickly shutting down the reactor when certain parameters enter an unacceptable range. This shutdown system employs a logic system, which is independent of those utilized by shutdown system number 2 and the reactor regulating system, which senses the requirement for reactor trip and de-energizes the direct current clutches to release the absorber element portion of the shutoff units, allowing them to drop between columns of fuel channels, into the moderator. Each shutdown rod is equipped with a spring that provides an initial acceleration.

The design philosophy is based on triplicating the measurement of each variable, and initiating protection action when any two of the three trip channels is tripped by any variable or combination of variables.

Typical variables (trip parameters) that can initiate a reactor trip through shutdown system number 1 are:

- high neutron power
- low gross coolant flow
- high heat transport pressure
- high rate log neutron power
- high reactor building pressure
- low steam generator level
- low pressurizer level
- high moderator temperature

**Shutdown System Number 2**

An alternate method of quickly shutting down the reactor is the rapid injection of poison (concentrated gadolinium nitrate solution) into the moderator through horizontal tubes that enter one side of the calandria and terminate as nozzles that span the calandria, between rows of fuel channels. There are six shutdown system number 2 poison injection nozzles in a CANDU 6 reactor. This shutdown system employs an independent logic system that senses the requirement for a reactor shutdown and opens fast-acting valves located in the line between a high pressure helium tank and the poison tanks. The released helium expels the poison from the tanks, through the injection nozzles into the moderator.

Similar trip parameters used to activate shutdown system number 1 also initiate a trip condition on shutdown system number 2. The instrumentation for these trips is however physically and electrically separate.
Emergency Core Cooling (ECCS)

System Operation

The emergency core cooling system provides ordinary water to the heat transport system to compensate for the heavy water coolant lost in a postulated Loss of Coolant Accident (LOCA), and recirculates and cools the heavy water/light water mixture that collects in the reactor building floor to the reactor headers to maintain fuel cooling in the long term.

The CANDU 6 ECCS has three stages of operation: high, medium and low pressure. System operation is triggered, on a loss-of-coolant accident (LOCA), when the heat transport system pressure drops to 5.5 MPa (800 psia) and a loop isolation system (independent of ECCS logic) closes the applicable valves to isolate the two HTS loops.

High Pressure (HP) Operation

The initial LOCA signal isolates the two HTS loops, opens the gas inlet, HP injection and the applicable heat transport system H₂O/D₂O isolation valves simultaneously and also initiates the rapid cooling of the steam generators: the latter is accomplished by opening the main steam safety valves on the steam generator secondary side, and discharging steam. Emergency coolant (ordinary water) is forced from the ECCS water tanks into the ruptured HTS loop when pressure in that loop falls below the injection pressure – 4.14 MPa (600 psia). This period to ECC injection can take about 10 seconds for a maximum pipe-size break. Coolant escaping from the ruptured circuit collects in the reactor building sump. Minimum time to empty the water (maximum break) is 2.5 minutes. The entire HP phase is initiated automatically.

When the ECCS water tanks reach a predetermined low level, the HP injection valves close automatically.

Medium Pressure (MP) Operation

The medium pressure stage consists of water supplied from the dousing tank, and delivered to the HTS headers via the ECC pumps. The valves connecting the dousing tank to the ECC pumps are opened on the LOCA signal, while the MP injection valves open on a delayed signal. The water in the dousing tank provided for MP ECC is sufficient for a minimum of 13 minutes operation with the maximum design basis HTS break.

There are two ECC pumps each capable of providing 100 per cent of the water needs at a pressure of 150 psia. Class IV electrical supply to the ECCS pumps is backed up by Class III power and the emergency power supply system.

Low Pressure Operation

As the dousing tank nears depletion, the valves between the reactor building floor and the ECC pumps open. Water collected in the reactor basement is returned to the heat transport system via heat exchangers, to provide long term fuel cooling.

The heat exchanger maintains the temperature of the coolant flow at about 49°C. Temperature of the water (D₂O and H₂O) from the sump would be about 66°C at the ECC pumps.

For small breaks decay heat is transferred to the steam generators and rejected via the main steam safety valves, which have a total steam flow capacity greater than that of the steam generators. For large breaks, the break itself acts as the heat sink in combination with ECC injection.
Undamaged HTS Loop

During the ECCS operating sequence decay heat in the undamaged HTS loop is transferred to the steam generators by natural circulation. Coolant losses from this circuit prior to its isolation will be less than 20 per cent. This inventory loss can be made up by opening the isolating valves to the feed circuit with the override control in the control room or, if the circuit pressure falls below that of the injection tanks, by the ECCS.

Backup Decay Heat Removal

In the very unlikely event that the emergency core cooling system fails during or following a LOCA, decay heat is transferred from the fuel to the moderator by radiation and conduction. The centre element of the CANDU 6 fuel bundle is only 50 mm from the cool heavy water moderator (see fuel channel section shown on previous page); hence decay heat removal from the fuel following shutdown is assured without melting the uranium dioxide, even if no coolant is present in the fuel channel.
Containment

Containment comprises a number of systems that operate to provide a sealed envelope around the reactor systems if an accidental radioactivity release occurs from these systems. The structures and systems that form containment are:

- a lined, post-tensioned concrete containment structure
- an automatic dousing system
- air coolers
- a filtered air discharge system
- access airlocks
- an automatically initiated containment isolation system.

Systems Operation

If a large break in the heat transport system occurred, the building pressure would rise and, at an overpressure of 3.5 kPa (0.5 psig), would initiate containment closure (if closure had not already been initiated by an activity release signal). Other sensors associated with the reactor would have caused a reactor trip and ECCS operation. The dousing system will start to operate automatically at an overpressure of 14 kPa (2 psig) and stops when the pressure drops to 7 kPa (1 psig). The operation can be continuous or cyclic, dependent on the size of the break.

Condensation, on the building walls, and operation of the building air coolers subsequently reduce the pressure from 7 kPa (1 psig) to about atmospheric. Vapour recovery dryers initially clean up the containment atmosphere when the dewpoint has reached about 16°C. This is followed by a fresh air purge that is discharged through the dryers and reactor building ventilation system filter train, removing the particulate and radioiodine activity prior to atmospheric release.

For a small break in the heat transport system the building coolers would condense discharging heat transport system coolant and maintain the building pressure at atmospheric level.

Gamma activity, if sensed in the ventilation discharge ducts and/or vapour recovery system will initiate signals that close the containment dampers and valves to prevent activity releases.

A fission product release in a fuelling machine room, caused by damaging one or more fuel elements, would be sensed in the ventilation discharge ducts and would initiate containment isolation.

The fuelling machine room, vaults and boiler room can be purged through the reactor building ventilation system filter train to remove the particulate and radioiodine activity prior to atmospheric venting.
The station is designed to prevent the loss of D$_2$O from the reactor systems. Special measures are taken to recover and upgrade D$_2$O which does escape.

Provisions ensuring optimum D$_2$O management are:

- use of welded joints, with the number of mechanical joints in heavy water systems is kept to a minimum
- heavy water and light water systems are segregated as much as possible
- a D$_2$O liquid recovery system is provided
- the building containing most heavy water systems is sealed and has a minimum through ventilation flow
- air entering and leaving the reactor building is dried to minimize D$_2$O downgrading and loss respectively
- air within the building is maintained dry by closed circulation and drying systems so that any increase in humidity can be readily detected. Heavy water vapour removed by the dryers is recovered and upgraded.

**Deuteration and De-deuteration System**

The spent resins from the ion exchange columns of the heat transport system and the moderator system contain D$_2$O. To recover the D$_2$O the resins are processed (de-deuteration – a downward flow of H$_2$O through the resin beds) in the deuteration and de-deuteration system.

Similarly when ion exchange resins are received from the suppliers they are also processed (deuteration – an upward flow of D$_2$O through the resin bed) to remove H$_2$O.

The ion exchange resins from the heat transport and moderator systems are processed separately and in both of the processes some D$_2$O is downgraded, collected and transferred to the D$_2$O cleanup system.

**Cleanup System**

The D$_2$O cleanup system purifies the downgraded D$_2$O collected in the station by removing most of the impurities, with the exception of H$_2$O.

The D$_2$O cleanup system contains three ion exchange columns, one charcoal filter and two feed pumps.

The ion exchange columns remove lithium, iron and boron ions and other corrosion products. The columns also remove fission products that may be present.

The charcoal filter removes any oil present in the heavy water, as well as impurities such as amines and carbonates. The clean downgraded D$_2$O is transferred to the D$_2$O upgrading system.

**Vapour Recovery System**

A D$_2$O vapour recovery system is provided in the reactor building to maintain a dry atmosphere in areas that may be subject to leakage. The areas are segregated into three groups, each group serviced by one portion of the system.

**Areas accessible only during reactor shutdown**

- fuelling machine operating areas
- boiler room, including shutdown cooler areas
- moderator room (exclusive of enclosure around equipment).

**Moderator areas**

- enclosure space around moderator equipment

**Areas accessible during reactor operation**

- fuelling machine maintenance locks
- fuelling machine auxiliary equipment room
- monitoring rooms.
**D₂O Collection System**

This system is designed to collect D₂O leakage from mechanical components that may occur in any area of the reactor building and to receive D₂O drained from equipment prior to maintenance.

The D₂O in the holding tank is transferred, by two pumps, to either the pressure and inventory control system or, if downgraded, to the D₂O cleanup system.

**D₂O Upgrading System**

The D₂O upgrading system separates a mixture of H₂O and D₂O into:
- an overhead distillate, richer in light water than the feed
- a bottom product, richer in heavy water than the feed.

The upgrading system accepts mixtures varying from 2 per cent to 99 per cent D₂O and upgrades them to reactor grade 99.8 per cent D₂O. The overhead distillate has a concentration of less than 2 per cent D₂O.

**D₂O Supply System**

The D₂O supply system receives D₂O from two sources:
- fresh D₂O is received from tank trucks or drums
- upgraded D₂O is received from the upgrading system.

The four storage tanks of the D₂O supply system contain inventory for one moderator or one heat transport system.

The four tanks also act as a high isotopic D₂O storage facility during normal reactor operation.
**Overview**

High neutron economy is the feature of the CANDU reactor that allows it to operate with a variety of low fissile content fuels. Several possible fuel cycles are illustrated in the following figure. These include natural uranium (NU cycle) and slightly enriched uranium (SEU cycle). Also, this feature of CANDU provides a unique synergy between CANDU and Light Water Reactors (LWRs) as there is sufficient fissile content in spent LWR fuel to provide new fuel in CANDU (Tandem cycle) as mixed uranium and plutonium oxide (MOX) fuel. Alternately, the recovered uranium from the LWR spent fuel can be used in CANDU without the plutonium (RU cycle) to operate in synergy with LWRs that recycle the plutonium.

In addition to burning the products of conventional LWR fuel reprocessing, the CANDU reactor can operate on LWR spent fuel, refabricated without chemical reprocessing (DUPIC Cycle), a process that is easier to safeguard against diversion of fissile material. This fuel cycle is particularly suitable for LWR owners and operators that do not have access to indigenous resources of uranium and conventional spent fuel reprocessing technology.

The option of recycling reprocessed LWR fuels in CANDU leads to higher energy output by 30 to 40 per cent compared with recycling using LWRs alone. Furthermore, the recycling of plutonium in the LWR is limited in capacity by otherwise unacceptable changes in the dynamic behaviour of the reactor. No such limitation exists with CANDU.

The high neutron economy of CANDU also has implications in the area of waste disposal, in particular, in the reduction of the radiotoxicity of spent fuel. There is sufficient fissile content in the mixture of plutonium and the higher actinides (a by-product of LWR spent fuel reprocessing) to be used as fuel in CANDU; no addition of uranium is required. The absence of uranium prevents the formation of plutonium. The fissile content of the transuranic mix depletes rapidly due to the lack of plutonium formation. As a result, the level of neutron flux increases rapidly in order to maintain reactor power at the rated level. The high level of neutron flux is instrumental in transmuting and annihilating the toxic material. The CANDU reactor can therefore produce energy through the destruction of toxic waste and without producing any such waste in the process, and falls into the category of “green” technology.

CANDU fuel cycle options of current interest include: natural uranium (NU), slightly enriched uranium (SEU), recovered uranium (0.9 per cent U\textsubscript{235}) (RU), direct use of spent LWR fuel in CANDU (DUPIC), the thorium/U\textsubscript{233} cycles and the transuranic mix. The fuel cycle options are illustrated in the following figure, and are discussed further in the following sub-sections.

An important feature of CANDU’s versatility is that alternate fuel cycles can be implemented in operating CANDU reactors, with little or no equipment change. As a result, fuel cycle benefits do not require a big investment in new designs. This versatility also allows “reversibility” of fuel cycle options. Even if a CANDU has been optimized for a particular fuel cycle, the operator can convert to alternate fuel cycles, if required. This is a major attraction of the advanced fuel cycles, since it preserves the option of national independence of enrichment supply even while using the advanced fuel.

The ability to switch to alternative nuclear fuels that become available in the global market allows CANDU to take advantage of global fuel availability, thereby reducing cost and providing increased security of fuel supply.
LWR

Enrichment

Dry Processing

Reprocessing

Uranium Mine

Thorium Cycle

Plutonium Cycle

Actinide Burning

Direct Use
0.9%U 0.6%Pu

Recovered Uranium 0.9%

Slightly Enriched Uranium (0.8 to 1.2%) Fuel

Enriched Uranium Fuel

LWR

Natural Uranium 0.7%

Natural Fuel

CANDU fuel cycles (current and future)
Natural Uranium Fuel Cycle

CANDU Nuclear Power Plants now in operation or under construction utilize natural uranium (NU) fuel. The ability to burn natural uranium is a direct consequence of the excellent neutron economy provided by CANDU.

Historically, the ability to use NU fuel has had many benefits to CANDU owners, including low fuelling costs compared to other nuclear power plants, no reliance on supply of uranium enrichment or fuel reprocessing, and low uranium resource consumption.

These benefits, coupled with competitive capital cost, have made natural uranium fuelled CANDU reactors a competitive electricity supply option. Although CANDU spent fuel volumes are greater than for LWRs, the economic impact is offset by the lower specific activity and the absence of criticality concerns in handling and storage. Thus, on-site dry spent-fuel storage has been implemented with relative ease at operating CANDU plants. The dry storage technology is also applicable to the alternative fuel cycles mentioned above.

Short Term Advanced Fuel Cycles – RU & SEU

The short-term SEU and RU cycles involve very little development and can be implemented into existing CANDU plants as no significant hardware changes are required. The choice of the enrichment level for the SEU fuel is dictated primarily by the limit placed on fuel discharge burnup.

There is a specific enrichment level (and burnup) that maximizes the utilization of the natural uranium which is the starting material for the SEU fuel. This enrichment level is approximately 1.2 wt per cent U$_{235}$. This is due to the opposing effects of enrichment and the production rate of plutonium (which is the source of more than 50 per cent of the energy generated by natural uranium CANDU fuel). The enrichment reduces the production rate of plutonium but it also extends the fuel life in the core, which tends to increase the total energy contribution of the plutonium. A burnup of 22 MWd/kgU, which requires 1.2 wt per cent enrichment to achieve, minimizes uranium resource requirement. The spent fuel volume is reduced to 33 per cent of that of the natural uranium cycle as the burnup is increased by three times.

The RU cycle essentially uses a waste product of LWR spent fuel reprocessing since only the plutonium from the spent LWR fuel is currently recycled into the LWR; Therefore the cost of the RU fuel material is potentially low. The exit burnup of this fuel in CANDU is between 14 and 18 MWd/kgU (depending on the U$_{235}$ content of the RU which varies between 0.8 to 1.0 wt per cent). The additional energy obtained in CANDU is approximately 40 per cent of initial LWR fuel burnup. The reduction in CANDU spent fuel volume with the RU cycle is approximately 50 per cent that of the natural uranium cycle.

DUPIC Cycle

The DUPIC cycle facilitates the use of spent LWR fuel in CANDU without the need for chemical reprocessing, via relatively simple fuel refabrication technologies.

The DUPIC cycle is particularly suitable for countries that have spent LWR fuel and which do not have reprocessing technology, due to the simplified refabrication technology utilized by the DUPIC process.

The DUPIC cycle offers strategic benefits, such as security of supply and protection from uranium and enrichment price changes. The development of LWR-CANDU fuel cycles, such as DUPIC, transforms spent LWR fuel inventory from a “waste-disposal” cost into a valuable energy resource. A mix of LWRs and CANDUs incorporating the DUPIC fuel cycle would generate electricity utilizing 40 per cent less uranium resources than LWRs alone.

The DUPIC cycle has important non-proliferation advantages; fissile plutonium is never separated from the remaining heavy metals, so that no stream of material exists which could be diverted to non-peaceful use.
Thorium Cycle

Thorium, which is abundant in many areas of the world, is a fertile material and produces a fissile material, U\textsubscript{233}, by neutron capture. Hence, thorium can largely displace uranium in CANDU operation.

Some fissile material is required to initially (fresh core) make the reactor critical. This fissile material can be NU fuel, SEU fuel, RU fuel or DUPIC fuel. Once the process of neutron capture in thorium has started, significant quantities of U\textsubscript{233} are produced and fissioned during the life of the thorium fuel in CANDU. The production of U\textsubscript{233} is highly efficient (more so than the production of plutonium in the natural uranium cycle). There is, under optimum circumstances, almost one atom of U\textsubscript{233} produced per atom of U\textsubscript{233} destroyed. This makes the CANDU reactor a near-breeder as it breeds most of its own fuel.

There are essentially two types of thorium/U\textsubscript{233} cycles that can be used in CANDU, one without reprocessing spent fuel and one with reprocessing and recycling of the U\textsubscript{233} that is extracted. The reprocessing option results in more efficient fuel utilization but fuel cost depends on reprocessing cost. The fissile fuel production efficiency of the CANDU thorium/U\textsubscript{233} cycle ensures security of resources almost indefinitely.

Another advantage of the thorium/U\textsubscript{233} cycle is the lower radiotoxicity (by a factor of 10 to 100, compared with the uranium based cycles) of the spent fuel. This simplifies spent fuel disposal significantly. The lower radiotoxicity of the spent fuel is a result of the absence of U\textsubscript{238} which is the starting material for the production of the transuranic actinides, the main contributors to long-lived radiotoxicity of the spent uranium fuel.

The thorium fuel cycles are of immediate interest to countries that have thorium reserves while lacking significant uranium reserves and are of general interest to all countries as the price of uranium increases.