EC6 Safety Enhancement - Including impact of Fukushima Lessons Learned

Stephen Yu, R. Zemdegs, S. Boyle and M. Soulard
Candu Energy Inc., Mississauga, Ontario, Canada
(stephen.yu@candu.com)

Abstract

The Enhanced CANDU® 6 (EC6) is the new Generation III CANDU reactor design that meets the most up to date regulatory requirements and customer expectations. EC6 builds on the proven high performance design such as the Qinshan CANDU 6 units and has made improvements to safety and operational performance, and has incorporated extensive operational feedback including Fukushima. The Fukushima Dai-ichi March 11, 2011 event has demonstrated the importance of defence-in-depth considerations for beyond-design basis events, including severe accidents. The EC6 design is based on the defence-in-depth principles and provides further design features that address the lessons learned from Fukushima.

1. Introduction

Proper application of defence-in-depth is the key in protecting the public against severe accidents, such as that which occurred at Fukushima. Two important aspects of defence-in-depth design provisions include: i) a high degree of robustness, which incorporates sufficient redundancy within the design and ii) a high degree of protection against a large range of accidents, including those whose probability is quite remote and which provide significant challenges for the reactor's ability to fulfill the key safety functions, namely to *control*, *cool*, *contain* and *monitor*. The CANDU design has been developed over many years and consists of attributes that i) prevent accidents, ii) if they occur, stop them and limit the consequences; iii) if they progress to core damage, provide protection and mitigate severe accident scenarios.

2. Proven CANDU Safety Features

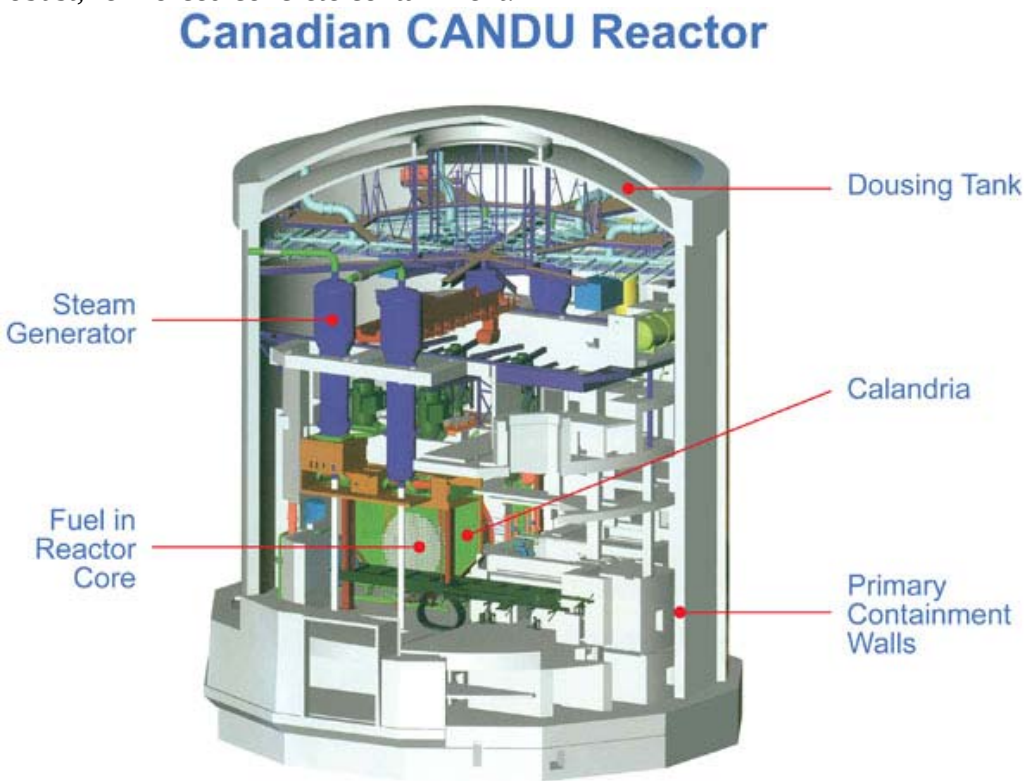
The CANDU 6 is a proven high performance design that has continued to evolve with improvements up to the Qinshan CANDU units built in China. It has an appropriate combination of inherent, passive safety characteristics, and engineered and administrative safety features. These characteristics and features prevent and mitigate severe accident progressions.

CANDU reactors can be refuelled while operating, and incorporate safety features to respond to the safety requirements imposed by the Canadian Nuclear Safety Commission. Safety features include:

- a design that can use passive convection cooling for the primary systems to keep the reactor cool in the absence of power

[1] Registered trademark of Atomic Energy of Canada Limited, used under exclusive license by Candu Energy Inc. (Candu).

- the use of a storage tank high in the containment building that work on gravity, which can also be used to replenish secondary side inventory and refill the steam generators, as required, to continue heat release in the event of a loss of power
- use of ceramic uranium fuel pellets that tolerate high temperatures
- two independent and diverse shutdown systems
- calandria (reactor core) vessel that contains the fuel bundles and heavy water moderator
- water filled calandria vault for shielding
- robust, reinforced concrete containment.



A strong contributor to the robustness and redundancy of CANDU design is the two-group separation philosophy. This ensures a high degree of independence between safety systems as well as physical separation and functional independence in how essential safety functions are provided. Two-group separation provides two independent means of maintaining the essential safety functions for events which affect a limited area of the plant. Events with failure of a safety function in one group can be mitigated by the other group.

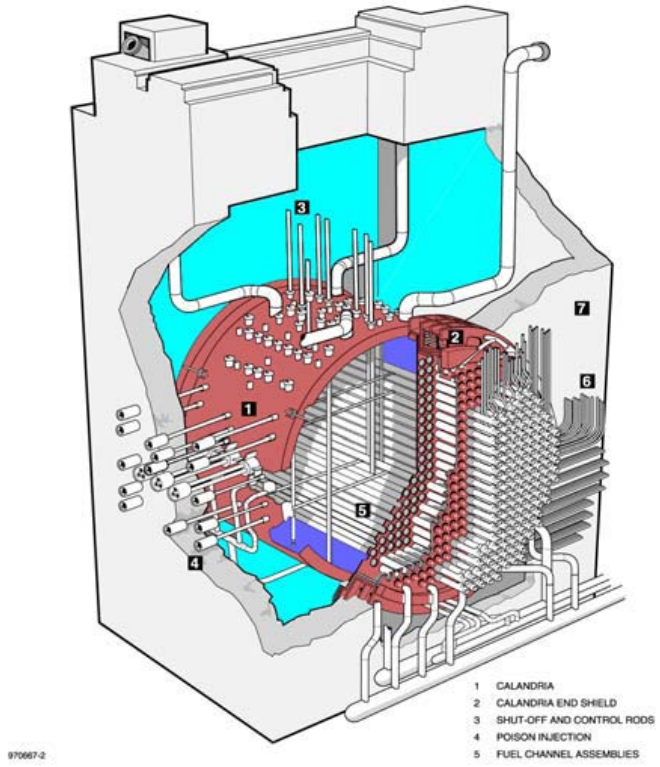
All CANDU reactors are designed with a number of barriers and protective systems that act to prevent releases of radioactive material into the environment. These include the fuel sheath, the heat transport system, the calandria tubes, the cool low pressure moderator, the cool low pressure shielding water in the calandria vault, the hydrogen control system and the containment building itself. The design measures taken result in a reactor that meets or exceeds regulatory requirements for the consequences of such accidents, with large margins that provide a high degree of robustness against accidents of even

greater severity and correspondingly more remote probability of occurrence. These safety features further support the defence-in-depth strategy in establishing accident prevention as the first priority, as outlined in IAEA guide on Defence in Depth [1].

CANDU reactors have large inventories of water within or connected to the reactor building that are available to provide passive cooling, even during accidents in which electrical power is not available and that involve earthquakes and flooding, such as was the case in the Fukushima event. These include the quantities of water in systems that can be used for backup cooling or water in mitigation systems such as emergency core cooling and dousing:

- the heat transport system as reactor coolant,
- the calandria vessel as moderator coolant,
- the calandria vault as shielding water
- the high pressure emergency core cooling tanks,
- the dousing tank (CANDU 6) / reserve water tank (EC6)

In the EC 6® design, for example, these different water sources together come to over 3,000 metric tonnes of water available for passive heat removal. The large water inventories surrounding the fuel can passively remove decay heat from the fuel and the reactor core for many hours after an accident, providing time and opportunity for operator intervention. This is an important inherent safety feature of the CANDU reactors. The low temperature, low-pressure moderator in the calandria vessel surrounding the horizontal fuel channels provides an effective heat sink under some accident conditions, allowing the fuel channels to maintain their integrity even when internal cooling is not available. The water in the calandria vault normally used for shielding will provide continuous cooling of the calandria vessel, which may contain the core debris (molten corium), as long as it is submerged in the large volume of water in the calandria vault. [2]



The largest of these water inventories that can be used for heat removal is the water in the reserve water tank (2000 tonnes). This large volume of water is stored at high elevation and so can be used to provide water by gravity feed to the secondary side of the reactor's steam generators. This water will then boil away and be released through steam valves in the secondary side and in the process will remove the decay heat of the reactor core. This passive cooling of the reactor using water already available in close proximity can be established using no electrical power at all, if necessary. Use of all of these different sources of water allows for a period of several days during which the operator can

make use of emergency equipment such as portable diesel-driven pumps and electrical generators to maintain reactor cooling.
The water in the spent fuel storage bay is normally kept cooled by the bay cooling and purification system. On loss of power, the pool water will heat up and the fuel will continue to be cooled as long as the fuel bundles are submerged. There is significant time - about 16 days for operator to take corrective actions [3], and a small make-up rate of about 1kg/s will be sufficient to support evaporative cooling of the fuel in the storage bay.
Since CANDU reactors use natural (not enriched) uranium fuel, therefore light water can be used to provide cooling without concern for the fuel becoming critical. But for designs that use enriched fuel, appropriate chemical additions will be required to address criticality concerns.

3. Fukushima Events

On March 11, 2011, Japan suffered its highest recorded earthquake. A magnitude 9.0 earthquake struck off the eastern coast of Japan. It caused an immediate loss of offsite power. It also generated a series of large tsunami waves. The tsunami waves that hit the Fukushima Daiichi stations were much higher than had been considered in the plant design, and impacted both the normal and the mitigating systems.

At the time of the earthquake, Units 1-3 at the Fukushima Dai-ichi site were operating and Units 4-6 were in refuelling/maintenance outage. When the earthquake struck, all three operating reactors at the site shut down automatically and shutdown cooling commenced. All twelve of the available plant emergency diesel generators (EDG) started. Approximately 46 minutes after the earthquake, the first tsunami wave hit the site.
The flooding caused by the tsunami waves resulted in the loss of all nine available EDGs cooled by sea water and the loss of all but one of the three EDGs cooled by air. The remaining air-cooled EDG at Unit 6 was the only source of AC power at the six-unit site. All means of communication between the on-site Emergency Control Centre (OECC) and the on-site personnel executing recovery action was lost. The seawater pumps and motors located at the intake were destroyed; therefore the ultimate heat sink was lost.

4. Lessons Learned Identified from Major International and Canadian Reviews

The nuclear international community and regulatory organizations vigilantly reviewed the event to learn and improve nuclear safety. The common focus areas emerging from the compilation of lessons learned identified by the international organizations and regulatory bodies include external hazards, severe accident management and emergency preparedness.

The Japanese Reports by the Government of Japan [4] identified lessons learned to strengthen measures against earthquakes and tsunamis. In its mission report [5], the IAEA identified that response to a severe accident being outside normal design and operating provisions presents special resource, management, instrumentation and control arrangements, in particular when multiple plants are involved. Furthermore, the IAEA found that guidance regarding multi unit sites with respect to external hazards was lacking. Therefore many of the lessons learned and conclusions deal specifically

with common-cause failure for multiple unit sites – common to all three areas (external hazards, severe accidents and emergency preparedness). The IAEA review identified a '*lack of defence in depth*' and further a '*lack of consideration for diversity'* for the design of ultimate heat sinks. The USNRC has issued one high-level report and one detailed report on the lessons learned from the Fukushima event [6]. The latter made sweeping recommendations on design in the US, with a focus on external events and mitigation provisions.

The CNSC issued a Fukushima Final Report [7] and Action Plan [8] that identifies thirteen recommendations for (i) strengthening reactor defence in depth, (ii) enhancing emergency response and (iii) improving regulatory framework and process. These recommendations are applicable to current operating stations and new build designs. The CNSC Fukushima task team identifies '*extended defence in depth*' to be applicable to new build designs. Post-Fukushima, the Canadian Nuclear Safety Commission made a presentation to the Convention on Nuclear Safety on Canada's response, including re-affirming the CANDU two-group philosophy against common mode failure, and the presence of numerous, diverse heat sinks to manage severe accident conditions. Also noted was that Candu Energy (formerly AECL) would review lessons learned, and incorporate any necessary improvements into new build design.

4.1 Fukushima Lessons Learned for EC6

Following the Fukushima events, all sectors of the CANDU nuclear industry, including Candu Energy Inc. (formerly AECL) high-level teams reviewed the implications on the CANDU fleet of reactors. A specific task team was also set up to review the EC6 design. As the Fukushima event was a beyond design basis event, the focus of the latter review was on both the definition of design basis external events and on the capability of the station to handle beyond-design-basis external events.

5. EC6 Safety Enhancements

EC6 builds on the proven high performance design in the Qinshan CANDU 6 reactor, and has made generic improvements to safety, reliability and operational performance, and has incorporated extensive operational feedback, to meet the most up to date regulatory requirements and customer expectations.. As a Generation III design, the EC6 reactor builds on the defence-in-depth features of the CANDU design, and provides further improvements in accident prevention, accident mitigation, severe accident resistance and recovery, and post accident control and monitoring. [9]. The following is a summary of the assessments on how the reference EC6 design provisions addresses the different external hazards and beyond design basis events.

5.1 EC6 Provisions against External Hazards

The systems, structures and components (SSC) important to safety are designed to withstand or are protected from the effects of external events, without loss of the capability to perform their safety functions, or designed such that their response or failure is in a safe direction. External events include natural external hazards such as extreme weather conditions, earthquakes, external flooding, and man-made hazards such as aircraft crashes, hazards arising from transportation and industrial activities (e.g. explosion and release of toxic gases).

To increase the strength of EC6 against external events, some significant design enhancements have been made relative to the Qinshan reference plant:

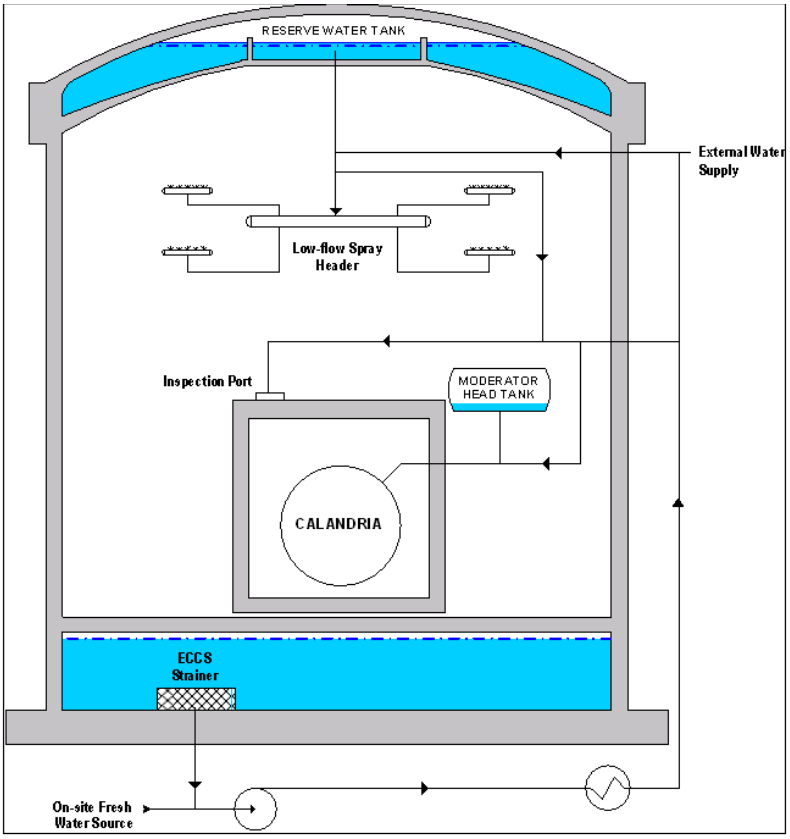
- The reference Design Basis Earthquake (DBE) peak ground acceleration has been increased to 0.3 g.
- The main control room (MCR) and secondary control area (SCA) are seismically qualified to operate during a DBE.
- Relocation of the SCA relative to the reference design for improved security and defence against localized events.
- Relocation of the Emergency Power Supply relative to the reference design for improved security and defence against localized events.
- The service building has been design-basis-tornado (DBT) qualified. This ensures that the emergency heat removal system gravity makeup from the reserve water tank to the SGs will not be rendered inoperable following a DBT, and
- The service building concrete thickness has been increased to improve defence against malevolent acts.

5.2 EC6 Provisions Against Beyond-Design Basis Accident (BDBA) Events

One of the dominant common issues apparent from the review of Fukushima lessons learned is the need to improve availability of emergency cooling water and power supplies. The EC6 design has incorporated many improvements in the area of severe accident prevention and mitigation, particularly with respect to the availability of emergency cooling and backup power capability.

The EC6 design includes a Severe Accident Recovery and Heat Removal System (SARHRS). Depending on the accident scenario/sequence, the SARHRS may be used for a Limited Core Damage Accident (LCDA) or Severe Core Damage Accident (SCDA). The system is designed to enable light-water makeup of the calandria or calandria vault inventories in order to provide decay heat removal. The system provides cooling either passively through steaming by gravity from the reserve water tank, followed by an external water source make-up (if available) ; and then actively, by recovering water from the Reactor Building sump and cooling it using the SARHRS heat exchanger prior to recirculation. Provisions are also made for containment pressure suppression and fission product washout via a containment cooling spray. The spray function can be performed simultaneously with either calandria vessel or calandria vault makeup (depending on the circumstances of the accident) for steam condensation in order to maintain the containment pressure within allowable limits.

The major equipment for SARHRS include a unit specific containment heat removal pump and heat exchanger, and a cooling water pump for supplying the secondary side of the heat exchangers. To ensure that water makeup flow can be delivered under different plant conditions, secondary flow paths are provided which do not require any valves inside the reactor building to be opened. These valves and pumps are powered by a dedicated power supply, which is comprised of a seismically qualified, dedicated diesel generator and electrical distribution system, designed to be shared between two EC6 units. Therefore all necessary operations required for a seismic event are seismically qualified and the necessary equipment is located outside the reactor building for accessibility.



Severe Accident Recovery and Heat Removal System Diagram

5.3 EC6 Heat Sink Capability

The design includes numerous flow paths to the ultimate heat sink (local body of water and/or atmosphere) for normal operation, design basis events, and beyond design basis accidents. EC6 has numerous 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 and following design basis accidents. Additionally, the SARHRS system is a completely independent means of transferring decay heat to the ultimate heat sink following severe accidents. In the EC6 there is always at least one heat sink, passive or active, available at any stage of accident progression that will halt or delay progression of the accident, allowing time for other mitigating measures to be employed. For mitigation of beyond design basis accidents, the following design features are capable of delaying or halting progression of the event;

- Provision for make-up to the calandria vessel from the reserve water tank (RWT) allows heat removal by steaming from the calandria vessel, to extend the available time for an active heat sink to be restored.
- RWT inventory can be replenished by SARHRS drawing water from on-site water supply (lake or river). RWT inventory can be directed to the steam generators, the calandria vessel, the calandria vault, or the low-flow containment cooling sprays.

- Use of SARHRS to recover and cool water from the RB floor and restore it to the calandria vessel or the calandria vault. Cooling for the SARHRS heat exchanger is by a dedicated SARHRS cooling water pump, using inventory from the on-site water supply (such as water from lake intake or from sea intake).
- Engineered connections to allow calandria vault and vessel make-up from an external water supply, in the unlikely event that all of the above water sources are exhausted or unavailable.

5.4 EC6 Provisions for Station Blackout Coping Capability

The dominant initiator of the Fukushima event was the extended loss of all AC power that resulted in emergency heat removal systems being unable to prevent fuel damage at three of the six units. By design, the EC6 has incorporated improvements that help to prevent and mitigate consequences from a station black out event (SBO).

Station blackout involves a loss of off-site power concurrent with a turbine trip and failure of the on-site safety alternating current (AC) power system (both Class III standby diesel generators and emergency power). It should be noted that each unit has two Class III standby generators, capable of accepting loads within three and a half minutes, for a mission time of seven days. In addition, each unit is provided with a dedicated emergency power supply (EPS) system, discussed below. A separated and seismically qualified dedicated power supply is provided to support SARHRS. In the case of a seismic event or station blackout resulting from a seismic event, a seismically qualified uninterruptible power supply (UPS) is provided to supply loads required for heat sink.

Key EC6 mitigative design features for this event are:

- Gravity injection of water to steam generators (SGs) from the RWT.
- Batteries to ensure at least 24 hours of capability to support make-up from the RWT to the SGs.
- SARHRS is capable of refilling the RWT with water taken from the on-site cooling water source (lake or river). Alternative supply for refilling of RWT is possible via engineered connections.

In the extreme event that all engineered features are unavailable, the inventories in the steam generators, the calandria vessel, and the calandria vault will slow event progression. At any stage of the event, off-site water supplies may be established (using provided connections) to halt event progression.
Following a SBO event, if the motorized valves from the RWT to the SGs do not open automatically, the operator will have approximately 2.9 hours from the start of the event before heat-up of the fuel. With make-up from the RWT to the steam generators available, there is sufficient capacity to keep the fuel cool for over three (3) days.
After 24 hours, extended coping strategies are in place to provide core and SFB cooling, and HTS and containment integrity. These strategies rely on portable equipment which is safely stored onsite and protected from external events. This extended coping time will be sufficient for use of pre-planned and pre-staged offsite resources for maintaining core and SFB cooling, and HTS and containment integrity.

5.5 Emergency Power Supply System

Each unit is provided with a dedicated system comprising emergency power generators (EPGs), batteries as the uninterruptible power supply (UPS), and equipment distributing power from those sources. EPS is seismically qualified. EPS starts up automatically when required and is an alternate power source to selected safety and systems important to safety such as ECC, containment cooling, and emergency heat removal system. The EPS generator location has been reviewed in terms of grouping and separation from the other diesel generators and their margins to potential flooding scenarios.

In case of a seismic event or station blackout (SBO) resulting from a seismic event, the seismically qualified UPS supply loads required for heat sink. At the onset of a Class III failure, the EPS batteries are in a fully-charged state capable of supporting the EPS loads for up to 24 hours for severe accident scenarios (motorized valves for water supply from reserve water tanks).

5.6 Maintaining Cooling to Spent Fuel Bay

The Fukushima accident identified the need to ensure cooling of spent fuel pools in case of loss of all power. Spent fuel bays in CANDU reactors are located outside the reactor buildings at grade elevation to prevent interaction between events in containment and events in the SFB. They are not elevated. Provisions are in place for the EC6 design to ensure monitoring and cooling of spent fuel bay by additional make-up.

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 during normal operation. 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.

5.7 EC6 Provisions for Severe Accident Management and Mitigation

The Fukushima lessons learned have identified the importance of proper planning and preparatory measures for severe accident management. In particular, the Fukushima lessons learned have highlighted the importance of the role of a robust containment design, hydrogen mitigation provisions and adequate provisions for control and monitoring during accident conditions.

One of the pertinent improvements for the EC6 design is an improved containment structure, which provides additional margin in maintaining containment integrity following severe accident events and provides additional time for emergency response. The EC6 containment structure provides an environmental boundary, biological shielding, and a pressure boundary in the event of an accident.

The containment includes design enhancements that have been made for the EC6:

- The design pressure of the reactor building has been increased from operating CANDU plants
- 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.

5.7.1 Hydrogen Mitigation to Minimize Off-Site Releases

Containment atmospheric hydrogen control is achieved by passive autocatalytic recombiners (PARS) and active igniters that limit the concentration of hydrogen in the reactor building atmosphere to below the threshold limit at which rapid deflagration or detonation could occur. In the event of severe accidents where the quantity and rate of production of hydrogen may be high, active igniters placed at strategic locations in the containment supplement the action of the passive recombiners.

5.7.2 Improved Safety Parameters Monitoring Functions Following a Severe Accident

The EC6 design includes a number of improvements to the computer control systems, including post accident controllability. The EC6 safety monitoring system (SMS) performs the function of safety parameter display system that provides safety system monitoring during normal plant operation and post-accident monitoring functions following an event. This is achieved by providing information on the critical safety functions for supporting the proper operation of the reactor including detection and diagnosis of malfunctions to allow mitigation of these conditions.

Within the SMS envelope for the EC6 design are the critical parameters and the parameters required for post accident monitoring. Post accident monitoring (PAM) including monitoring of severe accidents, provides plant operators with information to monitor DBA and/or BDBA conditions in the plant and to assist the operators in making decisions regarding other systems that shutdown, cool and contain the unit in a safe state.

5.7 Further Assessment of Fukushima Lessons Learned for EC6

The accident itself, as well as international and industry-wide preliminary lessons learned from the event, was analyzed in order to identify any gaps or opportunities for improvement in the EC6 design. The generic plant safety topic areas arising from Fukushima that vendors and operators are addressing worldwide include:

- Robustness to design basis and beyond design basis earthquakes and floods
- Fire protection, including fires in conjunction with seismic or flood events
- Response to prolonged station blackout
- Ability to restore and maintain cooling to a damaged core
- Management of hydrogen generation/release
- Supply of services and protection to on-site staff managing a severe accident
- Robustness of spent fuel management systems (wet and dry storage).

Many of the design features incorporated in the reference EC6 described in the section above, which were originally enhanced to meet the safety requirements stated in latest CNSC requirements in RD-337, address the key themes emerging as lessons learned from the Fukushima event, in particular protection against severe external events such as i) seismic, ii) flooding and iii) station blackout (SBO) mitigation capability. The evaluation completed has identified areas for further assessment of event sequences from severe external events, which are characterized by consequential loss of power and/or loss of heat sink and hence present the most challenge. Additional enhancement of accident response is being considered in the current EC6 Development project for the management of heat sinks and severe accident management. These include the use of portable equipment, such as engineered connections for portable water make-up and portable diesel generator, mulit-unit post accident considerations, and enhancements to spent fuel bay and for post accident monitoring. The application of the Fukushima lessons learned will further strengthen the lines of defence.

6. Conclusion

The Enhanced CANDU 6 (EC6) is the new Generation III CANDU reactor design that meets the most up to date regulatory requirements and customer expectations. EC6 builds on the proven high performance design such as the Qinshan CANDU 6 reactor, and has made improvements to safety, operational performance, and has incorporated extensive operational feedback meeting Generation III requirements. The Fukushima Daiichi March 11, 2011 event has demonstrated the importance of defence-in-depth considerations for beyond-design basis events, including severe core damage accidents. The EC6 design is based on the defence-in-depth principles and provides further design features that address the lessons learned from Fukushima. The CANDU design, including EC6, has an appropriate combination of inherent, passive safety characteristics, and engineered and administrative safety features. These characteristics provide the proper balance to effectively mitigate and prevent severe accident progressions. The design has been developed over many years and consists of attributes that i) prevent accidents, ii) if they occur, stop them and limit the consequences; iii) if they progress to core damage, provide protection and mitigate severe accident scenarios. The application of the Fukushima lessons learned will further strengthen the lines of defence for beyond design basis events.

7. References

[1] “Defence in Depth in Nuclear Safety”, INSAG 10-1996, IAEA, June 1996.
[2] CFD Model of CANDU Calandria Vessel Retention During Severe Accidents, by F. Song, B.Lekakh and K. Hau, The 14th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, Toronto, Ontario, Canada, 2011 September 25-29.
[3] Spent Fuel Response after A Postulated Loss of Spent Fuel Bay Cooling Accident, by H.Z. Fan, R. Aboud, E. Choy, W. Zhu, and H. Liu, 33rd Annual Conference of the Canadian Nuclear Society, Saskatoon, Saskatchewan, 2012 June 10 – 13.
[4] Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety – “The Accident at TEPCO's Fukushima Nuclear Power Stations”, Nuclear Emergency Response Headquarters; Government of Japan, June 2011, and Additional Report in September 2011.

[5] IAEA International Fact Finding Expert Mission Of The Fukushima Dai-Ichi NPP Accident Following The Great East Japan Earthquake And Tsunami" Tokyo, Fukushima Dai-ichi NPP, Fukushima Dai-ni NPP and Tokai Dai-ni NPP, Japan 24 May – 2 June 2011, June 16, 2011.
[6] Charles Miller et al., "Recommendations for Enhancing Reactor Safety in the 21st Century - The Near-Term Task Force Review of Insights from the Fukushima Dai-Ichi Accident", US Nuclear Regulatory Commission, July 12, 2011
[7] CNSC Fukushima Task Force Report, INFO-0824, October 2011.
[8] CNSC Staff Action Plan on the CSNC Fukushima Task Force Recommendations, INFO-0828, March 2012.
[9] The EC6 – An Enhanced Mid-Sized Reactor with Fuel cycle Applications by M. Soulard, S. Yu, J. Hopwood and I. Hastings, International Conference on Future of HWRs, Ottawa, Ontario, Canada, October 2-5, 2011