Enhanced CANDU 6 Design Assist Probabilistic Safety Assessment Results and Insights

K.Torabi,R.Bettig, P.Iliescu, J.Robinson, P.Santamaura, B.Skorupska, A.K.Tyagi and I.Vencel

Candu Energy Inc.[1]
(keivan.torabi@candu.com)
2285 Speakman Drive, Mississauga, Ontario, Canada

Abstract

The Enhanced CANDU®[2] 6(EC6)is a 700 MWe reactor, which has evolved from the well-established CANDUline of reactors, which are heavy-water moderated, and heavy-water cooled horizontal pressure tube reactors, using natural uranium fuel. The EC6 design retains the generic CANDU design features, while incorporating innovations and state-of-the-art technologies to ensure competitiveness with other design with respect to operation, performance and economics.

A design assist probabilistic safety assessment (PSA) was conducted during the design change phase of the project. The purpose of the assessment was to assess internal events during at-power operation and identify the design improvements and additional features needed to comply with the latest regulatory requirements in Canada and compete with other reactor designs, internationally.

The PSA results show that the EC6 plant response to the postulated initiating events is well balanced, and the design meets its safety objectives. This paper summarizes the results and insights gained during the development of the PSAmodels for at-power internal events.

Introduction

The EC6reactor design has evolved from AECL's long experience with the CANDU reactor designs, components and materials, as well as the operating experience (OPEX) and feedback of owners and operators of the CANDU reactors. The EC6 design retains the proven strengths and features of CANDU reactors, while incorporating innovations and state-of-the-art technology.

The Enhanced EC6 is a Generation III, 700 MWe class heavy-water moderated and cooled pressure tube reactor. Heavy water (D_2O) is a natural occurring isotope of water that is used as a moderator to slow down the neutrons in the reactor, enabling the use of natural uranium as fuel. This feature is unique to CANDUreactors. The choice of D_2O as the moderator also allows other fuel cycles to be used in CANDU reactors.

The use of natural uranium fuel in EC6 reactors permits fuel cycle independence and avoids having to deal with complex issues such as fuel reprocessing and enrichment. Technology transfer for localizing fuel manufacture is simple and has been achieved very successfully in a number of countries, such as Argentina, China, India, Pakistan, South Korea, and Romania.

In general, the main advantages of the EC6 reactor design, in comparison to pressurized water reactors (PWRs) and boiling water reactors (BWRs), are the use of natural uranium, on-line refueling, excellent

safety performance, high capacity factor, and it is perfectly suited for small and medium sized electrical grids. The EC6 reactor can rely on either cooling towers, lake water, river or sea water, as the ultimate heat sink.

1. EC6 Design Concept

The EC6 design is based on horizontal fuel-channels surrounded by a heavy water moderator for thermalization of fission neutrons. This fundamental design concept is consistent among all CANDU reactors. A schematics diagram of EC6 nuclear design is shown in Figure 1. The design includes a heat transport system with two loops that can be isolated during loss of coolant accidents (LOCA), a pressurizer, and four steam generators. There are five safety systems in the EC6 design: two independent and diverse shutdown systems (SDS1 and SDS2), which are physically and functionally independent from each other and from the reactor regulating system; emergency core cooling system (ECCS); emergency heat removal system (EHRS) and a containment system, which includes a steel-lined concrete containment structure, passive recombiners,local air coolers and automatic isolation valves. The design includes a reserve water tank at the top of the containment, near the roof, that provides a passive source of water in case of emergency,that can be used as make up to several different systems.

Some of the enhanced features of EC6 that contributed to the overall safety of EC6 are:

- A modern Distributed Control System (DCS) replaces the Digital Control Computers (DCC) used in previous CANDU reactors.
- New computer design for SDS1 and SDS2, which allows for more trip parameters to be implemented as necessary and monitored.
- Human factor engineering was fully involved in re-designing the state-of-the-art main and the secondary control rooms.
- Past 500 reactor years of CANDU experience and other feedbacks (including lesson learned from Fukushima) are incorporated in the design.
- Further hardening and improvements to the spatial separation of the safety systems.
- A computer-based safety monitoring system has been added to provide safety parameter displays in the main and secondary control rooms and in the technical support center.
- The containment has been made thicker and more reinforcing steel has been added to achieve a higher design pressure and lower leakage rate. These features provide additional margin in design and the thicker containment wall results in an increased protection against external threats, such as aircraft strike.
- In the event of hydrogen release into containment following a postulated accident, hydrogen mitigation is accomplished through the use of igniters and Passive Autocatalytic Recombiners (PARs).
- A new system is added to the EC6 design to prevent the core damage by backing up the moderator, and can also mitigate the damages and halt severe accident progression by filling the calandria vault with water. This system relies on independent sources of water and electrical power, and could be used in the case of loss of off-site power and other on-site AC power.

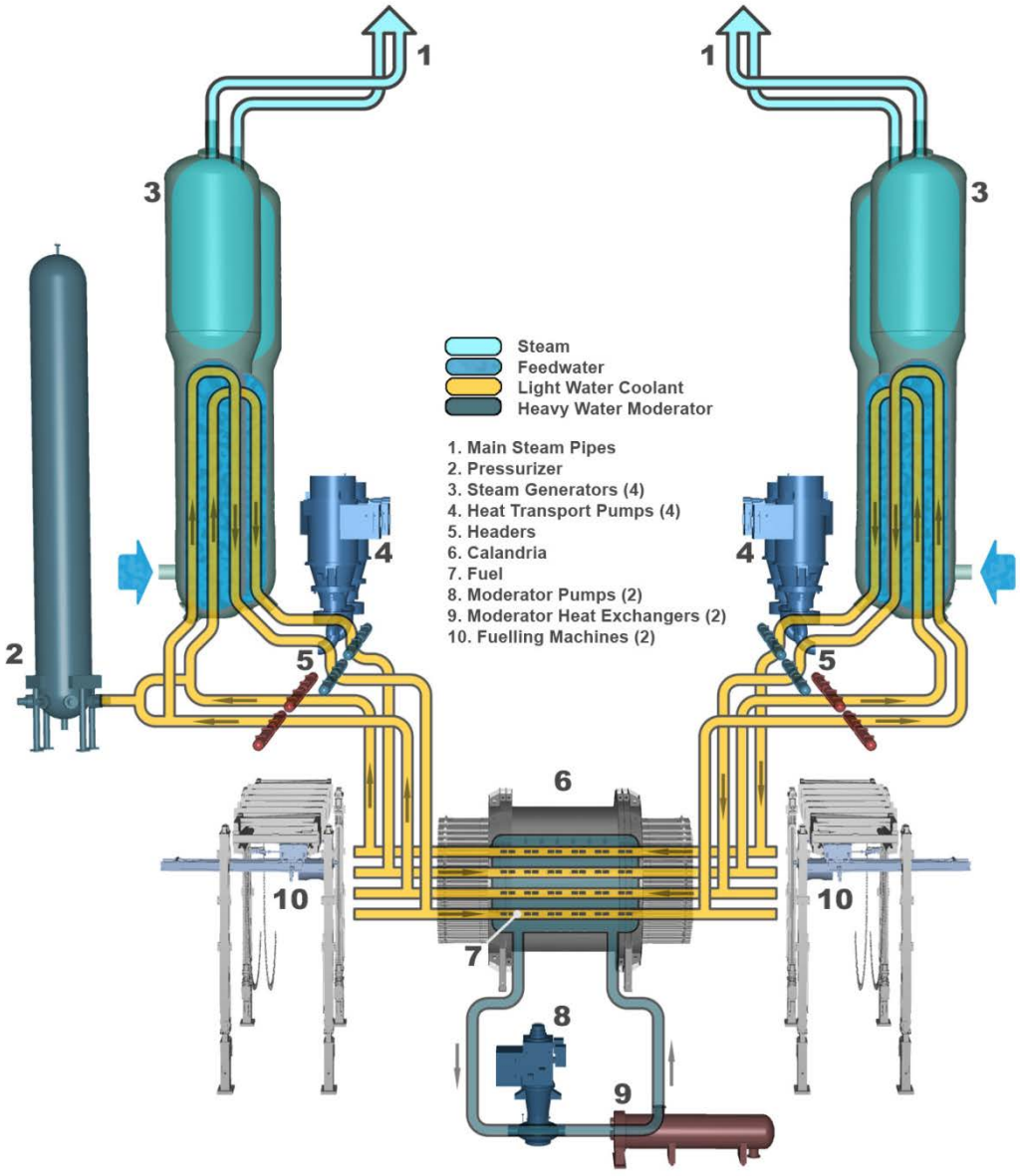

Figure 1Schematic Enhanced CANDU6 Design[3]

2. PSA Involvement in EC6 Design, Safety and Licensing

The potential for accidental release of fission products contained in nuclear fuel constitutes the main risk from a nuclear power plant. A risk assessment of nuclear power plants is necessary to identify the sequence of events that can lead to such a release when reactor is at-power and thus to assess and to quantify the risks.

[3]Source: Atomic Energy of Canada Limited. Licensed exclusively to Candu Energy Inc. All rights reserved.

As a new reactor design, the EC6 is required to meet the requirements enshrined in the Canadian Nuclear Safety Commission (CNSC) regulatory document RD-337 "Design of New Nuclear Power Plants" [1]. The regulator defines the acceptable safety goals, which includes the postulated frequencies of accidental radioactivity releases from the plant. Part of these requirements includes the safety goals for core damage frequency (CDF), small release frequency (SRF), and large release frequency (LRF). The goal for the CDF is below 1E-05 per reactor year.The PSA results must demonstrate that the design meets the regulatory requirements. The Level 1 PSA demonstrates the compliance with the CDF related safety goal, and the Level 2 PSA extends the results of Level 1 PSA to demonstrate the compliance with the SRF and LRF safety goals.

During the design change process and enhancement of the EC6 project, PSA was involved from the conceptual stages. The initial PSA input into the EC6 project was to determine what design improvements should be implemented in order to ensure the CNSC safety goals would be met and to ensure an adequate seismic capacity is achieved. The Level 1 and Level 2 PSA results from the existing CANDU PSAs were reviewed. Various design changes to address both internal and external events were assessed as to their impact on CDF and LRF. Out of this assessment, a number of design changeswere proposed to the project and were implemented.

As the EC6 design work during conceptual design phase progressed, another high-level assessment was conducted to provide confidence that the safety goals could be achieved, after implementing the proposed changes. The high-level assessment evaluated the applicable approved design changes to estimate the CDF from at-power and shutdown operation.

Finally, after the completion of the high-level assessment, a complete Level 1 PSA was launched to accurately calculate the CDF, develop the accident sequences, cutsets and quantify the contributions of initiating events and mitigating systems to the overall risk. The PSA role was development of the system fault trees, as they were going through the modifications, to ensure the safety goals are met.

3. PSA Findings DuringEvent Tree Development

Development of the accident sequences and event tree models were progressed in parallel with the conceptual phase of the EC6 design, making it difficult to have all of the required design information necessary for event tree analyses available ahead of time. Where possible, design information was taken from the existing plants. In other cases, where the reference plant design information was not applicable, or the design still progressing, a number of assumptions had to be made. The majority of the assumptions were related to system detailed design, operation, maintenance, or deterministic safety analysis. Process and instrumentation and control designers were consulted for related system design assumptions, available alarms and indications in the control rooms. Operational and maintenance assumptions were vigorously discussed and confirmed with the operation and maintenancedisciplines to ensure they comply with the outage plans. The deterministic safety analysis group provided information related to trip parameters and success criteria of the credited systems in the event trees.

4. PSA Findings DuringFault Tree Development

Fault tree analysis was performed to assess the reliability of the safety and safety support systems. Not only this assessment determined the probability of failure, but also helped to identify any inherent design deficiencies and areas for improvement (e.g., singletons). Development of fault trees required inputs from the different design disciplines, as well as input from operations and maintenance. The resulting system reliability analysis demonstrated whether or not the system reliability was sufficient,

or if particular aspects of the design could benefit some improvements. The impact of the testing strategy was also revealed as to their effect on the system reliability, and whether or not the proposed strategy was acceptable. The regulatory document RD-337 also contains some reliability requirements placed on the EC6 safety systems. The safety systems are required to meet a probability of failure on demand of 1E-03. The failure on demand analysis, using the same fault tree modeling techniques, demonstrated that the safety systems meet this regulatory requirement.

Some examples of feedback based on system reliability analyses are as follows:

- While evaluating and reviewing the fault tree model for the digital control system, it was discovered an apparent single failure problem in the power supply, that could disable the associated mitigating system. The preliminary configuration of the control system could potentially have a scenario where a control system failure (either odd or even division), could be potential for failure of a single computer to block two redundant mitigating system pathways. A spurious signal from the odd or even voting computer to the components on the odd or even controller load list would result in failure to function. If the odd or even voting computer failed, this would lead to a single failure in the system. The singleton was identified and design was modified to eliminate the possibility of such failures.
- Some flow diversion scenarios were not accounted for during the preliminary phase of the system design. The flow diversion scenarios were identified and the design was changed to eliminate such scenarios. This modification included additional procedural and physical changes to the system.
- Another example was the feedback with respect to seismic qualification of systems, credited in the seismic assessments. One of the new systems, added to the EC6 design to address the necessity to have a dedicated system that caters to severe accidents and ensure that the regulatory safety goals are met, was not initially proposed to be seismically qualified. However, in order to meet the PSA safety goals, it was determined that the system should be seismically qualified. PSA input was a major driver to ensure that a seismically qualified heat sink was available to cater for a severe accident following a severe seismic event.

5. PSA Findings DuringAccident Sequence Quantification

Accident sequence quantification (ASQ) is performed in order to integrate initiating events, event tree sequences and systems fault trees, human reliability analyses results and quantify the dominant accident sequences and their frequencies. This provides insights into which initiating events and accident sequences contribute the most to overall plant risk. Unlike the individual system fault tree reliability assessments that can help to identify deficiencies in that system, ASQ can be useful in identifying deficiencies within the entire set of inter-related systems and their dependencies on each other. The ASQ results can also provide insights into what systems, components, and human actions are most risk-significant. This information can be useful in helping to determine what equipment or human errors should receive the most attention in order to maximize the benefit of additional design or analysis.

A few significant observations based on the ASQ results and importance measures are as follows:

- Heating ventilation and air conditioning: During the integration it was identified that the battery and inverter rooms are cooled by a single air conditioning unit, so that on loss of cooling

to the unit, or failure of the associated damper in the closed position, the battery room would overheat. This could affect the Class I and II electrical equipment due to the build-up of heat in the room and could lead to unavailability of the Class I and II power supplies, during mission.

- Additional automatic trip control logic: For some event sequences, it was identified that having additional automatic trips would have significant impact on the event sequences risks. A design change to make the auto trips more reliable was introduced.
- Some post-accident operator actions were identified that could have significant impact on the results. Those actions were identified and included in the operating procedures.
- The Severe Accident Recovery and Heat Removal System (SARHRS) provides the last line of defense to prevent severe core damage by recirculating cooled water into the calandria vessel and maintaining the integrity of the fuel channels. As SARHRS was credited as the last defense, it was expected that it would be a risk-significant system, and PSA results confirmed that.
- Class III electrical distribution systems, including the diesel generators, power a large number of mitigating systems. A significant number of related components are shown to be risk-significant, which confirms that the Class III power system is an important system with respect to preventing core damage.
- The importance measures of an operator action to open an isolation valve for make-up water supply showed significant impact.

6. PSA Feedback to Human Factors Engineering

Risk significant operator actions identified during the PSA were discussed with the human factor engineering staff for conducting and prioritizingoperator task analyses, and to ensure there are provisions in the design to allow for operator to properly follow the emergency operating procedures and complete the tasks. As a result of the human factors task analysis of the risk significant operator actions, there are possibilities for changes in the arrangement of the alarms, indicator and switches on the control rooms control panels, or even modifying the indicators. In turn, those operator actions may be reassessed and the associated human error probabilities used in PSA can be re-quantified, and task analysis information can be used as a feedback to PSA human reliability analysis.

7. Results and Discussions

The Level 1 PSA for the EC6 were performed by employing methods that are widely used and accepted in the nuclear industry, domestically and internationally, and which mainly involve the identification of the initiating events, development of event trees, fault trees, human reliability analysis common cause failure and accident sequence quantification.A systematic review of the plant design was conducted to identify postulated events. Event tree analysis was conducted for the initiating events. The events trees were developed to show mitigating system plant response and assign reactor damage states for each sequence. The analysed event tree involved fault tree modelling of the EC6 mitigating systems as well as quantifying operator actions failure probabilities. A comprehensive human reliability analysis was conducted to systematically quantify probabilities of human error in the plant. Each event sequence in an event tree terminates at an end statewhich is a successful reactor shutdown

with adequate decay heat removal capability, or where mitigating system failures occur, resulting in some degree of fuel damage in the reactor core.

These PSA results are obtained by integrating the initiating events, fault tree analysis models, event tree analysis models and human reliability analysis probabilities. The accident sequences are grouped into categories called reactor damage states. There are twelve reactor damage states defined for EC6. These damage states are further subdivided into local, widespread fuel damage or core damage consequences. The localand widespread fuel damage consequences are those that can potentially reach or exceed the prescribed small release threshold. A limited fuel damage accident is represented by severe single channel events that involve subsequent failure of a single pressure tube due to severe fuel overheating. A widespread fuel damage accident is defined as one that affects the core and results in fission product release due to fuel overheating, but does not result in consequential fuel channel failures. The severe core damage accidents are defined as the ones in which a rapid or late loss of fuel channel structural integrity occurs. The severe core damage accidents are characterized by a loss of heat sinks leading to rupture of multiple fuel channels. The primary objective of a Level 1 PSA is to estimate the core damage frequency (CDF). The severe core damage accident sequences are collected and then summed to calculate the CDF. Likewise, the widespread fuel damage frequency (WFDF) sequences are quantified and added together.

The quantification of risk and the integration of the models was conducted using the widely used computer codes (i.e., CAFTA [2] and PRAQUANT [3]). The sum of all CDF event sequences from 45 initiating events is estimated to be 1.1E-06 per reactor year. The sum for the local fuel damage frequency and WFDF are 8.1E-04 and 9.2E-06, respectively. The contribution of the initiating events to the overall CDF and WFDF are shown Figures 2 and 3. A Monte Carlo simulation was also used to assess the uncertainty associated with the estimates.

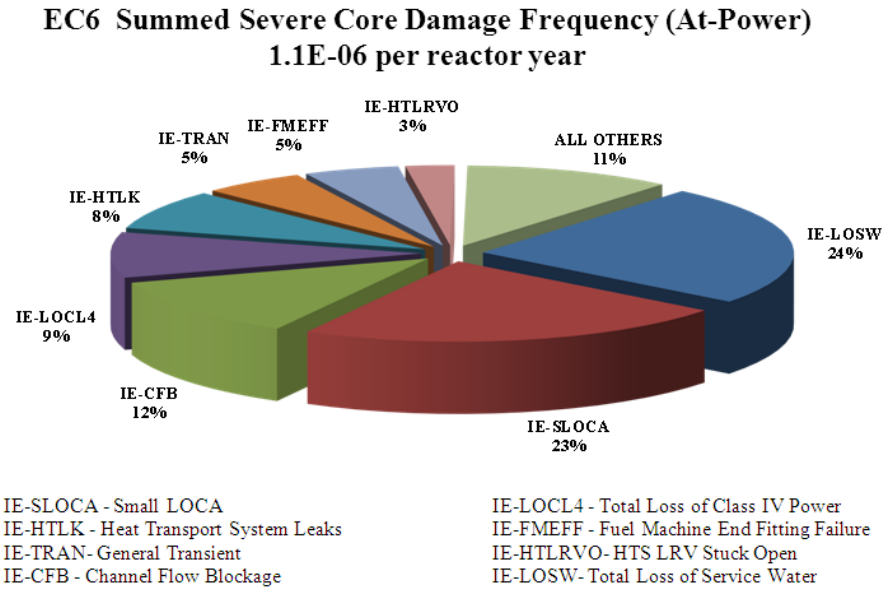

Figure 2 EC6 Core Damage Frequency by Initiating Events

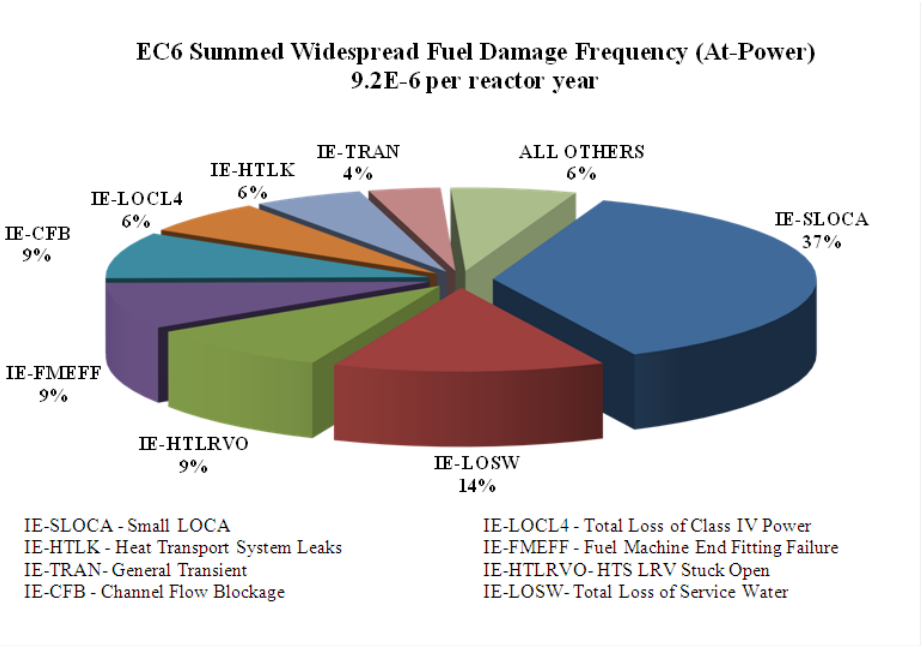

Figure 3 EC6 Widespread Core Damage Frequency by Initiating Events

8. Conclusions

Having the design modification and PSA activities progressing in parallel, allowed for early implementation of the PSA results in the plant design before the final design stage. This helped eliminating risks and expenses of design modifications later on during detailed design phase and construction.

The EC6 includes three different categories of reactor damage, which include local, widespread fuel damages, and severe core damage. Many events in the EC6 design can be stopped at fuel damage level and be prevented from progression to a reactor core damage state. The PSA provides insights for different risks and consequences. The risk of CDF of an EC6 unit, during normal at-power operation, due to internal events is estimated to be 1.1E-06 per reactor year.

It was determined that about half of the risk is due to support systems and half is related to loss of coolant accidents. Overall the contributions are well balanced and no single event dominates the risks.

Based on the results of the interim Level 1 PSA for EC6 internal events, at-power, the contribution to the overall CDF is low enough such that it is expected that the CNSC safety goal of 1E-05 can be met, once shutdown and external events PSAs are completed.

9. References

[1] RD-337, Regulatory Document titled “Design of New Nuclear plants”, Published by the Canadian Nuclear Safety Commission, November 2008.

[2] CAFTA, Software Manual, EPRI, Palo Alto, CA, 2009.

[3] PRAQUANT, Software Manual, EPRI, Palo Alto, CA, 2008.