COMPARING THE RISK OF THE PRESSURE TUBE-SCWR TO THE CANDU USING PROBABILISTIC RISK ASSESSMENT TOOLS

COMPARING THE RISK OF THE PRESSURE TUBE-SCWR TO THE CANDU USING PROBABILISTIC RISK ASSESSMENT TOOLS

BY

IMA ITUEN, B. Eng

A THESIS

SUBMITTED TO THE DEPARTMENT OF ENGINEERING PHYSICS

AND THE SCHOOL OF GRADUATE STUDIES

OF MCMASTER UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

Master of Applied Science (2011) McMaster University

(Engineering Physics) Hamilton, Ontario, Canada

TITLE:	Comparing the risk of the Pressure Tube-SCWR to the CANDU using Probabilistic Risk Assessment tools
AUTHOR:	Ima Ituen Bachelor of Engineering in Petroleum Engineering University of Port Harcourt, Port Harcourt, Nigeria
SUPERVISOR:	Dr. David Novog
NUMBER OF PAGES:	xvi, 144

Just for You, my Song thru the nights.

Abstract

In the next few decades, the nuclear industry worldwide is expected to launch a set of reactors with advanced reactor designs. Generation-IV (GEN-IV) reactors are to display superior safety by incorporating additional passive safety concepts as well as improving accident management and minimization of consequences. Canada is in the early stages of conceiving its GEN-IV reactor design – the Supercritical Water Reactor (SCWR). The proposed design is based on the existing CANDU configurations and is expected to offer significant advances in thermal efficiency, fuel cycle sustainability, and relative cost of energy. Of particular interest is the reactor's ability to use inherent or passive safety concepts which will translate to the reactor being walk-away safe in an accident.

Steam generators in CANDU remove decay heat by thermosyphoning in a loss of Class-IV power accident. This natural circulation process was a passive feature in GEN-II and GEN-III CANDUs. The SCWR's direct thermodynamic cycle implies steam generators are no longer incorporated into the design. This thesis examines how the SCWR compensates for the removal of a passive safety system element and the difference to the overall safety of the reactor following accidents. These results will be compared to the traditional CANDU's response in accidents to demonstrate the added value of this new reactor in maintaining the goal of no widespread core damage.

Comparisons were also made between the SCWR and similar GEN-IV reactors in terms of design and response to various initiating events.

Probabilistic Risk Analysis is used in this thesis to assess the SCWR design options. Although the SCWR is in the pre-conceptual design phase, the results of such risk assessment studies could affect the design, operation, and licensing of this new reactor. Future studies can build on this work to conduct more detailed analyses to characterise the SCWR's safety and reliability.

Acknowledgements

My deepest and most profound gratitude to Dr. Novog who's been incredibly patient, terribly understanding, and immensely generous. I am so glad I did the journey with you, Dr. Novog. I continue to say, you are Mac's best kept secret. Thanks to Dr. Luxat for patiently answering my questions and graciously giving of your time so I could understand more clearly the safety operations of a nuclear power plant.

And then there's the Nuke Group... What a bunch of folk! I appreciate each one of you and I'm thankful for the input you've made into my career and my life. It's been fun times. Thanks so much.

Family, you rock the best. Wouldn't have come this far if not for you. The deepest places of my heart say it all: You're the best – *ultra imus*!

Notation and abbreviations

ADS	Automatic Depressurization System
AECL	Atomic Energy of Canada Ltd.
AFS	Auxiliary Feedwater System
AOO	Anticipated Operational Occurrence
ASDV	Atmospheric Steam Discharge Valve
ATWS	Anticipated Transients Without Scram
BCS	Bleed Condenser System
BDBA	Beyond Design Basis Accident
BDBE	Beyond Design Basis Event
BWR	Boiling Water Reactor
CANDU	CAnada Deuterium Uranium
CD	Core Damage
CDF	Core Damage Frequency
CVR	Coolant Void Reactivity
DBA	Design Basis Accident
DBE	Design Basis Event
ECC	Emergency Core Cooling
ECCS	Emergency Core Cooling System

EPS	Emergency Power System
ESBWR	Economic Simplified Boiling Water Reactor
FTSD	Failure To Shutdown
GEN-II	Generation-II
GEN-III	Generation-III
GEN-IV	Generation-IV
GIF	Generation-IV International Forum
HEC	High Efficiency Channel
HPCI	High Pressure Core Injection System
HPI	High Pressure Injection
HPLWR	High Performance Light Water Reactor
HTS	Heat Transport System
ICS	Isolation Condenser System
JSCWR	Japanese Supercritical Water Reactor
LBLOCA	Large Break Loss Of Coolant Accident
LCD	Limited Core Damage
LCI	Low-pressure Core Injection
LOCA	Loss Of Coolant Accident
LOECC	Loss Of ECC
LOSP	Loss of Offsite Power
LPCI	Low Pressure Coolant Injection System
LPI	Low Pressure Injection
LRV	Liquid Relief Valve
LWR	Light Water Reactor

MCS	Moderator Circulation System
MPI	Medium Pressure Injection
MPS	Moderator Passive circulation System
NPP	Nuclear Power Plant
OPEX	OPerating EXperience
PRA	Probabilistic Risk Assessment/Analysis
PSA	Probabilistic Safety Assessment
RCP	Reactor Coolant Pump
RHRS	Residual Heat Removal System
RIH	Reactor Inlet Header
ROH	Reactor Outlet Header
RPS	Reactor Protection System
SBLOCA	Small Break Loss Of Coolant Accident
SBO	Station Blackout
SCWR	Supercritical Water Reactor
SDC	Shutdown Cooling
SDCS	Shutdown Cooling System
SDS 1	Shutdown System 1
SDS 2	Shutdown System 2
SLCS	Standby Liquid Control System
SLWR	Super Light Water Reactor

Contents

List of Figures

Chapter 1

Introduction and Problem Statement

Nuclear power represents a source of low CO_2-emitting energy, and it generates 51% of the electrical energy in Ontario and 14.6% of Canada's electricity [1]. The existing power reactors in Ontario are largely considered as Generation-II designs (with Generation-I being the early prototype and demonstration reactors). Generation-III reactors are currently being considered for construction in many jurisdictions with the goal that these designs provide an evolutionary improvement in safety and economics as compared to existing Generation-II stations. Beyond Generation-III, new and revolutionary designs entitled Generation-IV reactors are being considered with a focus on sustainability, economics, safety, and proliferation resistance. The objective of this thesis is to examine the potential improvements in safety of a specific Generation-IV design which utilizes water coolant at very high pressures and temperatures. The scope of this work includes a review of the current pressure tube-based pre-conceptual design, a review of existing regulatory requirements for such a design, and finally a

quantitative analysis of some of the improvements expected in safety using accepted probabilistic risk assessment tools.

1.1 The Generation-IV International Forum

The Generation-IV International Forum (GIF) was formed in 2001 to foster international collaboration as well as research and development. As its name implies, the GIF focuses on the next generation of reactors – the advanced reactors termed "Generation IV (GEN-IV)" reactors. This international forum is aimed at producing the research that is necessary to test the feasibility and performance capabilities of the GEN-IV reactors. The goal is that these systems will be deployable by 2030 or earlier [2]. The goals of the GEN-IV plants are to improve:

1. Sustainability
    - By generating energy sustainably and promoting the long-term availability of nuclear fuel
    - By effective fuel utilization and minimization of waste
2. Economics
    - Mainly by competitiveness with respect to other energy sources in terms of financial risk
    - By having a life cycle cost advantage over other energy sources
3. Safety and reliability
    - By excelling in safety and reliability

- Having a very low likelihood and degree of core damage, exemplified by the lack of need for offsite emergency response, and

4. Proliferation resistance and physical protection

   - Being a very unattractive route for diversion or theft of weapons-usable materials
   - Preventing terrorist acts by providing increased physical protection [3]

The focus of this thesis is exploring the potential safety improvements (i.e. the third goal) in Canada's GEN-IV reactor design.

The 6 generic systems the GIF chose to pursue are the Gas-cooled Fast Reactor (GFR), Molten Salt Reactor (MSR), Lead-cooled Fast Reactor (LFR), Sodium-cooled Fast Reactor (SFR), Super-Critical Water Reactor (SCWR), and the Very High Temperature Reactor (VHTR).

1.1.1 Canada's Role in GIF

Canada officially launched its GEN-IV National Program in 2006. Specifically, Canada has chosen to pursue research in the SCWR and the VHTR reactors. The three near-term needs the National Program wants to address are: a) Design and Integration, b) Materials and Chemistry, and c) Thermalhydraulics and Safety [4]. These are the broad areas over which the GEN-IV research is being conducted.

VHTR research is focussed on materials and fuel development which will be implemented in the SCWR. The SCWR is to be based on the CANDU™technology, and so the current CANDU infrastructure can be used to develop Canada's SCWR. The decision to focus on these two reactors is seen as a logical evolution from Canada's

expertise in nuclear reactors and research. The SCWR is seen as having the potential to fulfill all four of the GIF metrics using the pressure-tube reactor concept, and utilizes existing fossil-based technologies for the out-of-core components.

1.2 SCWR Basics and Pre-conceptual design description

Canada's SCWR can be considered as an advance of the heavy water-moderated, pressure tube reactor design, with the most important difference being the operating conditions, the fuel design, and the coolant type. The SCWR will still be a pressure tube-type reactor using low-temperature heavy water (Deuterium oxide) as the moderator, but will use light water as coolant. It is expected that the next generation design will have a higher thermal efficiency and improve the economics of the reactor, primarily through capital cost and construction schedule reduction. Like the other GEN-IV designs, the SCWR will also attempt to employ passive systems to the greatest extent practicable and supplement these systems with active components where necessary.

Table 1.1 below highlights some of the Canadian SCWR's properties. The SCWR design under consideration will be direct cycle, similar in some respects to a boiling water reactor. Since there will be no change of state in the coolant owing to the fact that full power operation will be above the thermodynamic critical pressure, the design eliminates the need for a pressurizer, steam generator and related secondary systems. These simplifications improve the costs while also removing some potential failure modes, and hence improve safety.

Parameter	**Value**
Thermal Power	2540 MW
Thermal Efficiency	45-50 %
Coolant	Supercritical light water
Coolant inlet temperature	350°C
Coolant outlet temperature	625°C
Operating pressure	25 MPa
Coolant Specific Heat at Inlet	6978 J/kg-K
Coolant Specific Heat at Outlet	2880 J/kg-K
Coolant Thermal Conductivity at Inlet	0.481 W/m-K
Coolant Thermal Conductivity at Outlet	0.107 W/m-K
Average discharge burnup	>40 MWd/kg
Linear element rating	<60 kW/m
Coolant void coefficient	Negative
Coolant temperature coefficient	Negative

Table 1.1: Pressure tube-SCWR design parameters

Water's supercritical temperature and pressure is 374 °C and 22.1MPa. The SCWR coolant will be above these conditions (i.e. system pressure of 25MPa and outlet temperatures up to 625°C) and will employ a mixture of existing materials and technologies for the Balance of Plant components, and new core designs for the reactor components. A preliminary sketch of the SCWR with its components is presented in Fig. 1.1.

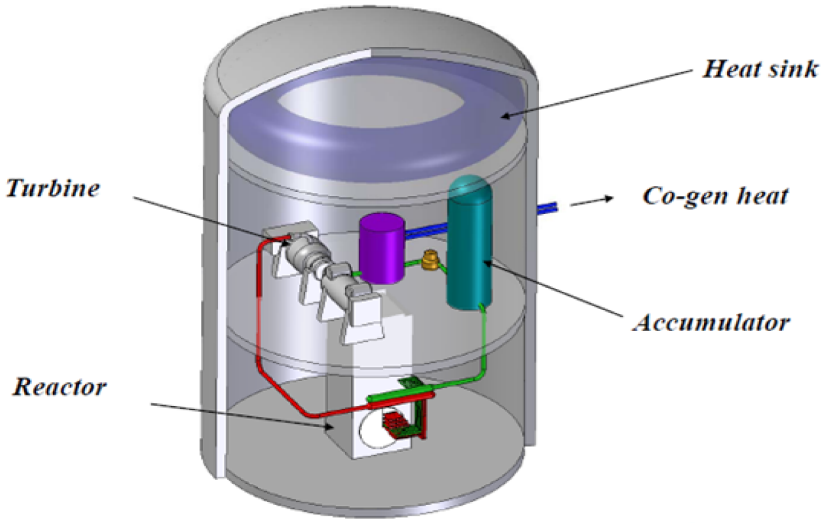


Figure 1.1: SCWR concept [5]

A key component of this thesis is the evaluation of potential failures in the pre-conceptual SCWR and their impact on the probabilities for core damage. From this respect, passive safety systems are desirable because they are based on natural phenomena like gravity, compressed gas, or compressed springs, and hence do not rely on external power, operator intervention, or any other active means. 'Passive system' may not need electric power nor mechanical forced power such as pumps. Therefore, passive systems are expected to have higher reliability and functionality. It is anticipated that as a GEN-IV reactor, the SCWR will have passive safety features such as natural circulation for decay heat removal. Simplification, in terms of reduced numbers of major components, valves, and pumps is also expected to improve safety by reducing the potential failure modes in the design. However, passive safety systems produce challenges of their own in terms of testing them to ensure they have the required performance reliability, and they have some unreliability due to "functional failures" (i.e. failures where the system may respond passively but where uncertainties

and performance are insufficient to meet the safety acceptance criteria). Hence while passive systems on the surface appear more reliable than active systems, a detailed analysis is required to prove this since the uncertainties in passively driven systems and therefore the probability of a functional failure tend to be larger than those for active systems.

1.3 Risk-Informed Design

The SCWR is still in the pre-conceptual design stage, hence detailed probabilistic risk assessments (PRAs) are not possible. However, Risk-Informed Design, wherein risk analysis tools are used to define the sensitivity of the risk to certain assumptions and limits from the proposed pre-conceptual layout, is applied. It is necessary to use risk assessment data and tools within the design phase so as to focus the efforts and design provisions to the areas where there is the greatest risk to the public, workers or the environment, or where the design exhibits excessive sensitivity to particular failures. For many components in the core (e.g. fuel channels, sheaths, etc.) little or no failure data may be available under relevant design conditions and assumptions. Therefore, judgements will need to be made for the risk calculations. As a result, the absolute value of the risk outputs may have high uncertainty; however the results can still be used to judge the design improvement against a similarly calculated CANDU, or they may be used to determine which safety features are the most sensitive to equipment or functional failures.

1.4 Objective

This work examines the safety of a pre-conceptual SCWR design with a focus on determining the relative improvements in risk as well as the particular design or component sensitivities. The approach first requires an in-depth look at the inherent and engineered safety features of the reactor. With this information, and testing the reactor's response to various abnormal operating scenarios and assumptions of equipment performance, one can identify the possible vulnerabilities in the safety systems and systems important to safety. Finally, risk assessment tools can be employed to estimate and quantify the risk in the pre-conceptual design.

The objective of this work is to use probabilistic methods to compare the response of the SCWR to the response of the CANDU under a variety of accident scenarios, and to perform a preliminary quantification of those improvements. This work will assess a combination of passive and active systems in the pre-conceptual design.

The thesis is divided into the following chapters: The second chapter will discuss the pre-conceptual reactor design and highlight some of the revolutionary changes it exhibits. Furthermore, the basis of risk and safety analysis is presented in that chapter. Chapter 3 outlines the approach used in this study (probabilistic risk analysis) and the accidents and dataset used for the analysis. Chapter 4 describes the accidents that are used as a basis of comparison between the response of the SCWR and the CANDU, and thereafter presents the results generated from the analysis. Chapter 5 contains the summary and conclusions from this study and provides suggested future work to build on this thesis. In the Appendix, some of the Canadian regulatory standards are examined for their applicability to the SCWR.

Chapter 2

Literature Review of SCWR and SCWR Safety

This chapter describes the design of the SCWR and compares it to the design of other supercritical water-cooled reactor designs. The second section discusses the special safety systems of the CANDU and describes some of the SCWR's safety systems, particularly those that are different from the CANDU's. The final section introduces the basis of risk and safety analysis.

2.1 Description of the Supercritical Water Reactor

The pressure tube-SCWR is a revolutionary reactor design. The design retains some aspects of existing CANDU™technology (such as a separate moderator and pressure tube concept, and being heavy water-moderated) with several new concepts and features aimed at improving safety, economics, sustainability, and proliferation resistance.

A nuclear reactor like the SCWR that operates with supercritical heat transport fluid has not been built yet but the concept and balance of plant equipment has been successfully deployed in the coal power industry. Therefore, the materials required are well known from that industry as are the thermodynamic cycles. For example, companies such as Mitsubishi Heavy Industries, Siemens AG, and GE build supercritical steam turbines and boiler feed pumps. ABB is also able to supply these high pressure turbines, whose materials are rated at over 700°C. As stated previously, it is expected that the designers of the SCWR will adopt the existing technology used in supercritical coal power for balance of plant equipment, but novel approaches will need to be adopted for the in-core components and safety systems.

2.1.1 Design

The SCWR will be a vertical reactor. Instead of having inlet headers and feeders like the CANDU does, the coolant will enter the core through an inlet plenum made from steel. The bottom of the plenum is the tubesheet; it has holes roughly the size of the pressure tubes [6]. The pressure tubes will be joined to the tubesheet using rolled joints [6]. Fig. 2.1 below shows a cross-section of the SCWR core.

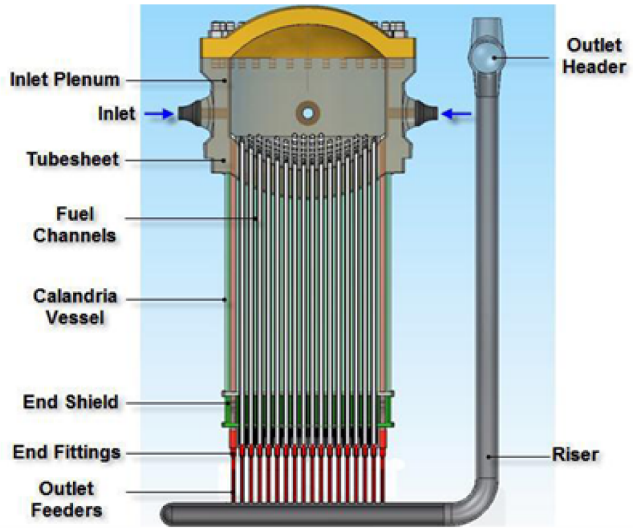


Figure 2.1: Cross-section of SCWR core [5]

The fuel channels comprise the pressure tubes and the fuel bundles within the pressure tubes. The fuel channels used in the SCWR will be insulated, both for safety reasons and due to restrictions arising from the materials. A limiting factor in choosing the structural materials is the high temperature and pressure of the coolant, particularly during accident scenarios. In order to use zircaloy pressure tubes in the SCWR, the pressure tube has to be insulated from the coolant. A zircaloy pressure tube is desired because it has a very low thermal neutron absorption cross-section compared to some other materials such as alloys of chrome, cobalt, iron or titanium. The latter alloys can resist the high temperature and pressure conditions but have much higher neutron absorption cross-sections – up to factors of ten or more [6]. Section 2.2 will give further details on the fuel channel design.

Similar to the CANDU, the SCWR will have a calandria which surrounds the core. The calandria is a cylindrical vessel which contains the heavy water moderator. The calandria vessel is closed by an end shield as well as by the continuously circulated

moderator fluid. The end shield has an inner and outer tubesheet and a peripheral shell, filled with carbon steel balls and cooling water. The end shield shields the external environment from radiation and also supports the fuel channels.

The end fittings are at the end of each fuel channel, providing a connection from the pressure tubes to the outlet header. This connection is via the outlet feeder pipes.

The following table, Table 2.1, shows some of the properties of the SCWR and compares them to the CANDU's. The reactor is still in its pre-conceptual design phase and so these dimensions and other parameters are not yet fixed.

Parameter	**SCWR**	**CANDU™**
Electric Power	1220 MWe	666-785 MWe
Thermal Power	2540 MWth	2064 MWth
Thermal Efficiency	45-50%	28-30%
Thermodynamic cycle	Direct	Indirect
Pressure at Inlet/Outlet	25.8 / 25 MPa	11 MPa /10 MPa
T_{in} / T_{out} Coolant	350 / 625 °C	290 / 310 °C
Coolant	Supercritical Light water	Heavy water
Moderator	Heavy water	Heavy water
Fuel	Enriched/Thorium	Natural uranium
Number of fuel channels	300-336	380
Core radius	335 cm	380 cm
Refuelling Method	3-batch refuelling	Online refuelling
Coolant Flow direction	Unidirectional	Bidirectional
Core orientation	Vertical	Horizontal
Cladding material	Ni alloy (stainless steel)	Zircaloy-4
Lattice Pitch	25.0 cm	28.6 cm
Average Burnup	40 MWd/kg	7.5 MWd/kg
Maximum Linear Element rating	37 kW/m	55-60 kW/m
Elements per bundle	78 + 1	37
Elements in rings 1, 2, 3 (4)	0, 15, 21, 42	12, 18, 24

Table 2.1: Comparing SCWR properties to CANDU's

Another significant departure from the traditional CANDU™designs is the use of

vertical fuel channels and batch refuelling. It would be very difficult, if not impossible, to perform online refuelling at 25MPa pressure in terms of fuelling machine integrity, seal robustness, and for safety reasons. Therefore, off-power batch refuelling has been selected for the SCWR. Studies have shown that the vertical orientation proves beneficial because it eliminates pressure tube sagging [7]. Furthermore, fuel loading from the top of the core provides easier access than from the sides and can minimize containment volumes.

2.1.2 Challenges

The SCWR is expected to generate a lot of interest since it boasts higher thermal efficiency, lower cost per MW, and better safety characteristics, but the reactor is not without its challenges. One of the challenges to the current design is choosing the materials for in-core components. The high temperatures, oxidation and corrosion characteristics, as well as the radiological constraints, make material selection a difficult task. Supercritical water has been used successfully in the coal industry, but that industry does not have the unique property of its operation causing high flux irradiation on the materials, thereby limiting its lifespan as it experiences neutron damage. At present, the usual Zircaloy-4 cladding material for CANDUs is not going to be used in the SCWR because the material shows corrosion and creep at SCWR temperatures [7]. Since surface temperatures of the cladding can reach up to 850°C [10] at which Zr's strength is greatly reduced, stainless steel is the material that has been selected for the fuel cladding [11]. The use of stainless steel for sheath material is consistent with the SCWR designs from Japan and Europe [12], [13].

A primary safety goal in a nuclear power plant is the prevention of radioactive

releases, to minimize worker dose, and to minimize the spread of contamination within the plant (as this leads to achieving the previous goals). One part of the prevention process is to control water chemistry to minimize corrosion and the transport of corrosion materials and radionuclides. Operations from fossil-fuel supercritical water plants indicate that there is a great risk of corrosion products being deposited on fuel cladding surfaces [36] which in turn will reduce its heat transfer capability, thereby increasing the likelihood of fuel failures. Moreover, the release of these corrosion products can increase the production of radioactive species from neutron activation, and thus increase the "out-of-core radiation fields and worker dose" [7].

The steam generator has typically been the repository for the material such as particulate that circulates with the coolant. The material originates from the corrosion on the primary side, and the material is usually deposited on the steam generator tubes. To combat the dissolution of iron, the CANDU heat transport system (HTS) pH specification has been set to 10.2-10.8 [14]. Such transport and deposition is common in BWR reactor designs where the direct cycle turbine requires additional shielding and confinement due to corrosion product deposition. Various institutions are studying the effects of SCWR water radiolysis in order to predict and mitigate its effects in the reactor [7].

A significant issue in SCWR design and safety is that the database of experimental data is small, for example in corrosion of materials, heat transfer from fuel, and material wear. To assist in solving this problem, supercritical test loops are being constructed in various places [9] [8]; the data they provide would prove invaluable to the development of this reactor as it relates to heat transfer properties. These programs are running in parallel with materials testing research and the conceptual

design activities. For the purposes of this work, the high-level design features and performance details are not required, but rather the design is evaluated at the system level to illustrate its strengths and weaknesses.

2.1.3 Other Supercritical Water-Cooled Reactor designs

Japanese Supercritical Water Reactor (JSCWR)

The Japanese version of the SCWR design is called the Super Light Water Reactor, Super LWR or SLWR. This reactor is a pressure-vessel type reactor and also operates a direct cycle with core pressure of 25MPa, while the core inlet and outlet temperatures are 280°C and 500°C respectively [15]. The reactor's pressure vessel and control rods are to be similar to those of PWRs while the containment and safety systems resemble the BWR's [12]. A pressure vessel is used rather than pressure tubes. As in the SCWR, since the heat transport cycle of the Super LWR is a once-through direct cycle at supercritical conditions, the reactor does not need the steam-water separators, dryers, and recirculation system of a BWR, nor does it require the pressurizer, primary coolant loop, and steam generators of the PWR [12]. Fig. 2.2 below illustrates how the Super LWR coolant loop is a simplified version of the LWR concept.

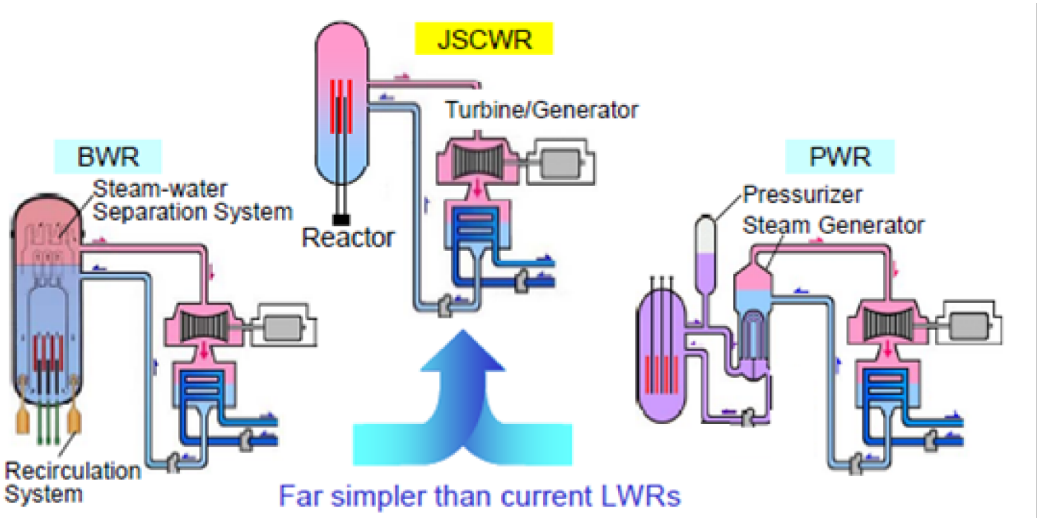


Figure 2.2: Comparison of primary circuits between JSCWR, BWR and PWR [16]

The priority in the JSCWR is to maintain the coolant flow at all times. For emergency core cooling, the ECCS is used. The ECCS of this reactor comprises the auxiliary feedwater system, low pressure core injection system (LPCI), and the automatic depressurization system (ADS). These systems are usually actuated sequentially following reactor scram. The safety relief valves act as the ADS to discharge coolant when required [12]. The design resembles modern BWR GEN-III designs in that high pressure core injection systems are not employed; rather the ADS system provides blowdown cooling for a period of time until the system reaches a low enough pressure such that LPCI or gravity-fed systems can be employed.

The Super LWR is shut down by the reactor scram system; control rods are the main shutdown mechanism of this reactor. If all the control rods fail to be inserted to the core, an alternative shutdown system to bring the reactor to a cold shutdown state acts by injecting borated water. That is the standby liquid control system (SLCS) which is a backup shutdown system in the event of an ATWS. The SLCS is able to

bring the core to a cold shutdown state. The SLCS consists of a liquid storage tank, two pumps, two valves, and the associated piping that transfers the borated water to the core. This system is manually-initiated, however. Following the shutdown and depressurization phase, the LPCI is used to keep the reactor core cool.

Some of the abnormal transients that are anticipated to occur in this reactor include: (i) Partial loss of reactor coolant flow: This is an event where one of the reactor coolant pumps (RCPs) is assumed to trip. Each RCP is a 50% pump in the main coolant system, therefore if one pump fails, the main coolant flow will be at just about 50% of the rated flow. A trip of both RCPs simultaneously will result in a total loss of coolant flow. The trip of an RCP would initiate the scram signal. However, if there is a scram delay or the signal is not initiated, the cladding temperature would increase by 60°C [12] before decreasing due to the decrease in power. (ii) Loss of feedwater heating: Losing one stage of the feedwater heating will cause a drop of 35°C of the feedwater [12]. At the start of the transient, the inlet flowrate will decrease because of the coolant's density increase. With the fuel channel inlet flowrate decreased, the cladding temperature will increase (less than 30°C [12]) while the reactor power decreases. However, to maintain the reactor power at the power set point, the control system will withdraw control rods. The control system will also increase the coolant flow rate to maintain the main steam temperature at its initial value [12]. Thereby, the fuel channel inlet flowrate will be restored and the reactor power increases.

The European Union High Performance Light Water Reactor

The High Performance Light Water Reactor (HPLWR) is the European concept for a supercritical water-cooled reactor. The HPLWR will have a once-through steam cycle, with a net power output of 1000MWe and a net thermal efficiency 43.5% [17]. The inlet conditions are 280°C and 25MPa, while the steam will leave the reactor at 500°C and 24MPa.

As in the pressure tube-SCWR, the HPLWR will use both active and passive safety systems to perform safety-related functions.

Some of these safety systems and components are:

1. The two independent scram systems – control rod and boron injection
2. The safety relief valves for reactor pressure control and depressurization and the main safety injection valves for containment isolation
3. Residual heat removal system (RHRS) and low pressure coolant injection system for residual heat removal from the reactor pressure vessel and containment [18]

The safety relief valves can be actuated to provide an ADS [19] as is the case with the Super LWR.

Following an accident, the priorities would be to ensure the reactor shuts down and the pressure vessel is depressurized, coolant inventory is maintained to keep the core cool, while the containment is isolated and heat is removed from containment. Some of the failure modes being investigated for the HPLWR include: a) Large break LOCA, say a break in the steam line. In this event, the break could be detected by the difference between the feedwater mass flow rate and the steam flow rate to the turbine. When the difference is greater than 200kg/s [20], the signal for reactor

scram is sent. The MSIVs will close on a low pressure signal. Following scram, the power level decreases, however the decay heat in the core still needs to be dissipated. Inlet water is continually fed to the core from the feedwater tank at 1179kg/s [20], although the tank capacity will only last for roughly 4 minutes of feed at this rate. The reactor is being depressurized from the break, but analysis shows that the reactor pressure stays above 6MPa for over a minute and thus delays the start of the LPCI till roughly 90 seconds after the break [20]. When the pressure drops below 6MPa, the active LPCI is initiated [19], injecting cold water to the core. The feedwater can keep the core cool as long as there is a constant feedwater flow. b) Small break LOCA: Analysis for this event has shown that the auxiliary feedwater supply system will be adequate to maintain the HPLWR's core in a safe state following the reactor shutdown due to the LOCA [21]. However, the ADS can also be activated followed by other systems (such as LPCI and RHRS) if that decision is made. c) The uncontrolled withdrawal of an absorber from the bottom without SCRAM: In such an event, it is estimated that fuel melting will occur. Studies are currently underway to determine how this event can be prevented in the HPLWR. However, one idea is to apply lower reactivity worth to the control rods as compared to the shutoff rods [21].

Ref. [21] has identified a shortcoming of the LPCI system to be the high power that is required to operate the pumps. This active system requires either grid supply of electricity or, in emergency situations, supply from diesel generators. To avoid or reduce the demand for power for emergency cooling water, a passive high pressure coolant injection system (HPCI) is being investigated [22]. As illustrated in Fig. 2.3, this system will accelerate high pressured steam through a water nozzle, then through a valve (Valve 1), and into the steam injector. The control valve will be

slightly opened to allow steam go to the heat exchanger which is at the bottom of the core flooding pool. The steam injector starts shortly after depressurization, and once it starts, Valve 2 and the Relief valve both close. All the steam flow then goes to the heat exchanger where it is cooled and returned to the steam injector. When the pressure at the exit of the steam injector is high enough [22], the Check valve opens and the water is injected into the RPV via the feedwater line. Thus, the HPCI can provide core cooling until the system has depressurized sufficiently to initiate the LPCI.

The HPCI is proposed to be applied for any depressurization transient, for instance a loss of offsite power event. The HPCI would be a passive system design, (Category D passive system due to its valve operation and signal input), and so is expected to display high reliability. Further investigation into this strategy of employing HPCI followed by the LPCI is being conducted for safety analyses purposes [21].

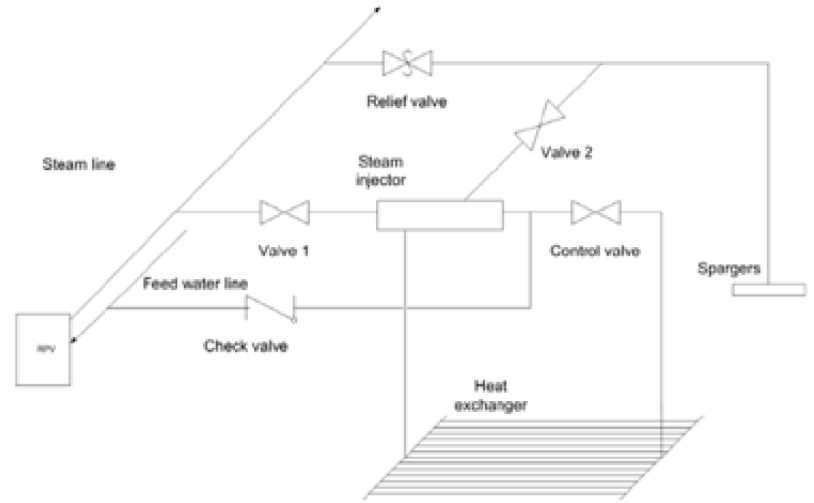


Figure 2.3: Passive HPCI system [22]

2.2 CANDU™reactor design and safety systems

The CANDU is a horizontal reactor with 380 fuel channels. Each fuel channel is designed to allow for online refuelling. This feature offers greater operational flexibility than offline refuelling such as being able to remove a defective fuel bundle without having to shut down the reactor. A cylindrical calandria surrounds the core and is closed on either side by end shields. The calandria contains the heavy water moderator, the fuel channel assemblies, and the reactivity mechanisms. The calandria itself is supported by a steel-lined concrete reactor vault [23]. Fig. 2.4 shows the CANDU assembly.

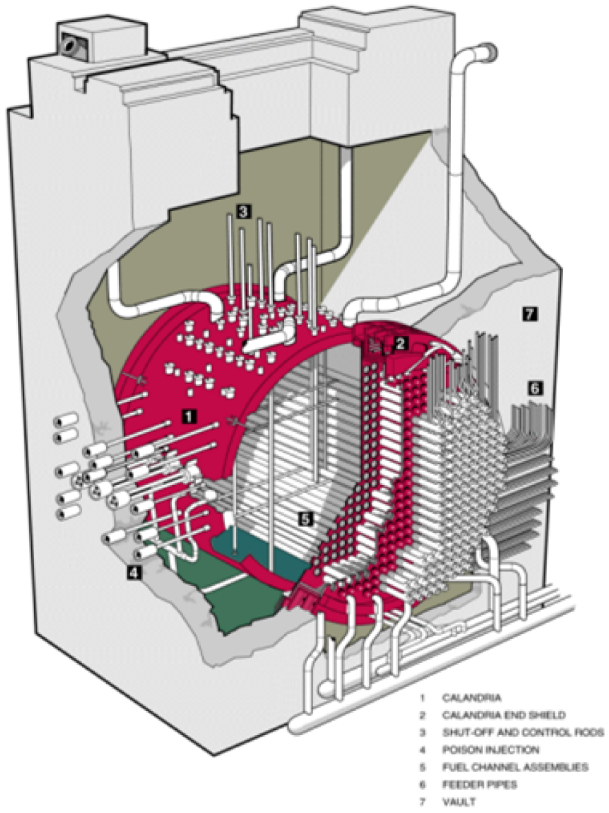


Figure 2.4: CANDU reactor assembly

The CANDU uses natural uranium fuel and each of the fuel bundles consists of 37 fuel elements. The fuel bundles are contained within a pressure tube, which is itself housed in a calandria tube, and each fuel channel has twelve fuel bundles. The heavy water coolant flows through the pressure tubes. The pressure tubes are thermally insulated from the moderator by the CO_2 annular gas that separates the pressure tube and the calandria tube. The fuel channel is illustrated in Fig. 2.5 below.

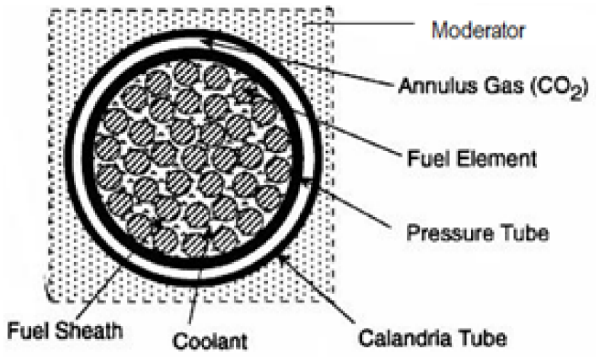


Figure 2.5: CANDU fuel channel

The CANDU HTS has two loops of 190 channels; coolant is circulated through the fuel channels to remove the heat produced from fission. Each of the loops consists of two steam generators, two pumps, two inlet headers, and two outlet headers. The CANDU also has a pressurizer as well as feed and bleed valves for pressure and reactor coolant inventory control and overpressure protection.

The moderator in the CANDU is heavy water at low pressure and temperature. Though both the coolant and the moderator use heavy water, the moderator system is entirely independent of the heat transport system. The moderator system is made up of the pumps and heat exchangers that circulate the moderator through the calandria and remove the heat that is generated during reactor operation [23]. The moderator

can also act as a backup heat sink when other heat removal systems are unavailable.

2.2.1 CANDU safety systems

The CANDU has four special safety systems: the two shutdown systems, the emergency core cooling system, and the containment system.

1. **Shutdown Systems, SDS1 and SDS2**: The two shutdown systems are fast-acting and independent of each other. They are each able to handle any design basis accident. They also have sufficient negative reactivity to ensure the reactor remains in a shutdown state after they are activated. Both SDS1 and SDS2 are Category D passive safety systems.

   Shutdown system 1 (SDS1) is a set of neutron-absorbing shutoff rods that fall vertically into the moderator. The rods are spring-assisted and gravity-driven; a trip signal will de-energize the clutches that hold the rod in place. Figure 2.6 illustrates the shutdown system. If there is a loss of power, this system will still function since it is not dependent on any form of power.

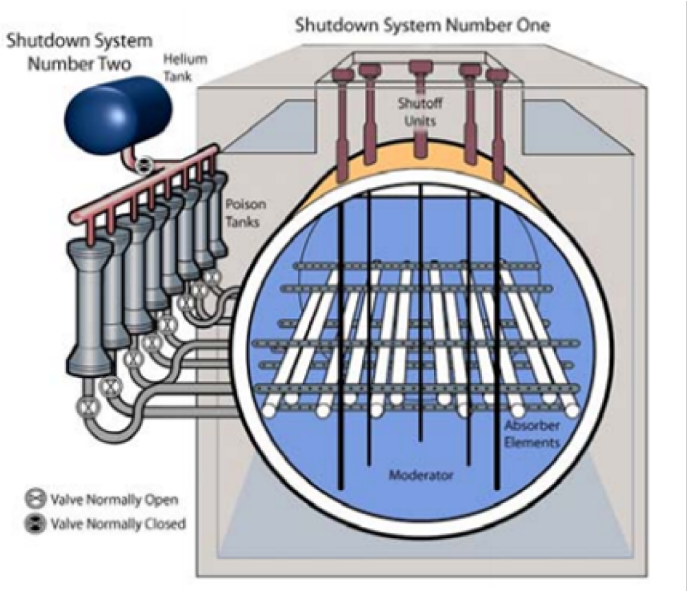


Figure 2.6: Shutdown Systems 1 and 2

As seen in Fig. 2.6, the Shutdown system 2 (SDS2) consists of horizontal perforated tubes inserted into the calandria. The tubes are connected to tanks containing liquid poison – so called because the liquid is a neutron absorber, and it therefore rapidly stops the nuclear chain reaction. As shown in the figure, the valves between the poison tanks and the calandria are left open, while the valves from the helium tank to the poison tanks are kept closed. When SDS2 is called upon, the quick-acting valves open and the helium pressurizes the contents of the poison tanks, causing them to inject the liquid poison at high pressure into the moderator. The poison used for SDS2 is a gadolinium nitrate solution. This shutdown system is a passive hydraulic system.

2. **Emergency Core Cooling (ECC) System**: The Emergency Core Cooling (ECC) System provides core refill and cooling following a small or large LOCA.

The ECC in CANDU has three stages: injection stage, intermediate stage, and recovery stage [24]. These correspond to the High Pressure Injection System (HPI), the Medium Pressure Injection (MPI), and the Low Pressure Injection (LPI) systems. During the injection stage, pressurized air injects water into the HTS from the ECC tanks (or at some stations it is via high pressure pumps). After the coolant pressure has decreased to a sufficient level, the intermediate stage begins wherein water is injected from the dousing water tank into HTS. When the water supply depletes and the pressure has further decreased, the recovery stage begins. The low pressure cooling is used for long-term recirculation and recovery. The water that collected in the reactor building sump during the accident and subsequent mitigation efforts is pumped back into the HTS through the emergency cooling recovery pumps.

3. **Containment**: The containment structure is made of a post-tensioned concrete with an epoxy liner. Under normal conditions, the containment is held at a slightly sub-atmospheric pressure. The containment system provides a sealed envelope around the reactor system if a release of radioactivity is detected; it will be automatically isolated on a high radioactivity signal. If the reactor building pressure rises to over 3.5kPa above atmospheric pressure, the automatic systems will initiate closure of all the containment penetrations. When an overpressure of 14kPa occurs in the building, the dousing system will automatically operate. The dousing tank is in the dome of the reactor building; its water is used not only for emergency dousing but also for emergency core cooling [23]. Other parts of the containment system include air coolers, a filtered air discharge system, access airlocks and an automatically-initiated containment isolation system.

2.3 Revolutionary design changes in the SCWR

Core damage is a key driver in GEN-IV designs, and the SCWR specifically, to demonstrate an improvement in safety. The SCWR design i) incorporates more passive safety systems, ii) simplifies the overall HTS system, and iii) provides more reliable equipment where needed as a way to improve its safety response. One method to examine the improvements in safety is to perform a conceptual-level risk assessment of the incremental risk improvements in the SCWR as compared to the standard CANDU™-type designs. In many nuclear power plants, risk of core damage (e.g. fuel melting and loss of geometry) is a metric used in the risk assessment. The reactor can demonstrate improvement by lower probability of severe accidents – evaluated by core damage frequency in Level 1 PRA, or by better mitigating the consequences of a severe accident – estimated by containment performance in Level 2 PRA. The focus of this thesis is to perform a preliminary Level 1 assessment of the relative improvement in core damage frequency for a pressure tube-SCWR.

The goal in the SCWR design is for inherent safety such that it is "walk-away safe" without core melt. A key feature used to achieve this objective is the implementation of the passive moderator heat removal system, which can remove heat from the core in the event that all active and normal heat sink methods are inoperable (e.g. in a station blackout). In order to assess this change, it is first important to highlight the major changes in core design in the SCWR. Some of the revolutionary changes made to the CANDU design that are being implemented in the SCWR include:

1. Fuel Channel Design

   Fig. 2.7 illustrates one of the possible SCWR fuel channel designs [5]. This AECL-proposed fuel channel design is called the High Efficiency Channel (HEC).

The calandria tube is eliminated and the pressure tube is always in contact with the moderator. As seen in Table 2.1, each SCWR fuel bundle has 79 elements though only 78 are fuel elements. The centre pin is used to displace coolant. It does not contain fuel but can be filled with air, solid material, or stagnant coolant [25].

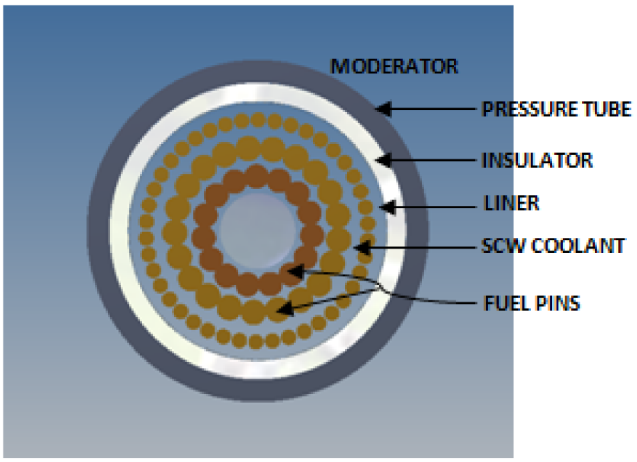


Figure 2.7: Conceptual SCWR High Efficiency Fuel Channel

A comparison is made between the CANDU's fuel channel and the SCWR's. In a CANDU, the calandria tube is in contact with the heavy water moderator. If cooling is not sustained to the fuel, the pressure tube undergoes thermal expansion into contact with the calandria tube. A heat transfer pathway is thereby formed to the much cooler (60°C) moderator. Pressure tube failure occurs for the moderator to act as a backup heat sink. Fig. 2.8 illustrates the pressure tube a CANDU accident.

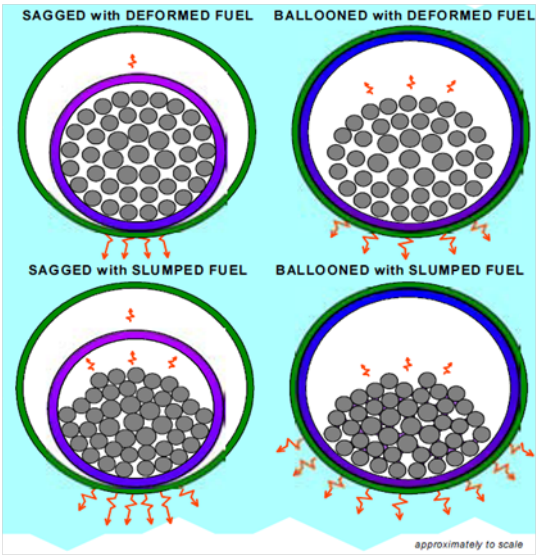


Figure 2.8: Pressure Tube Deformation in Accident – CANDU [26]

The HEC does not have a calandria tube; instead, the pressure tube is in direct contact with the moderator which is at about 100°C.The pressure tube is shielded from the hot coolant by a Yttrium-stabilised Zirconia insulator illustrated in Fig. 2.9. This porous material has a low thermal conductivity and very high corrosion resistance in SCW. Thus, the insulator provides a very good barrier to withstand thermal stresses and cycling. The insulated HEC design allows the CANDU pressure tube materials to be used in the SCWR since the zirconium alloy pressure tube operates below 100°C and hence can withstand the full HTS system conditions. This fuel channel design is unlike the CANDU's where the coolant flows are in direct contact with the pressure tube, and hence the pressure tube temperature is the same as the coolant's. The insulator provides the necessary characteristics such that the integrated effects of the pressure tube operating temperature and pressure can give greater than

a 30-year lifespan.

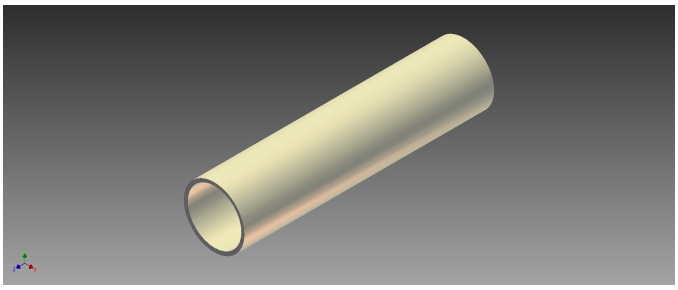


Figure 2.9: Insulator to be used in HEC fuel channel

The ceramic insulator in the HEC is a very important component. The insulator is porous such that the coolant can apply its full pressure to the pressure tube while retaining the temperature drop of over 500°C between the inside surface and the pressure tube [6]. A beneficial property of the insulator is that it is resistant to heat under the normal operating conditions of the reactor such that only a small amount of heat generated during fission is lost to the moderator (typically 3 to 5% of the thermal power).

However, at the high fuel and cladding temperatures typical of an accident such as a loss of heat sink, or LOCA with failure of low-pressure core injection (LCI), the elevated temperature of the fuel would radiate heat to the insulator. The inside edge of the insulator would heat up well beyond 500°C and subsequently the pressure tube would also heat up – albeit to a lesser extent due to conduction effects. Since the system under such scenarios would be depressurized, even the elevated temperature of the pressure tube would not pose a risk for fuel channel failure until its temperature became significantly high. As the pressure tube temperature rises, the heat transfer to the moderator would increase and the

passive moderator cooling system would act as a heat sink to remove the heat. Eventually, a steady state would be reached wherein the decay heat from the channel is perfectly balanced with the heat transferred from the pressure tube to the moderator, and then through the moderator heat sink. In theory, such a system could transfer all decay heat while precluding fuel and pressure tube failures in the channel. While the elevated fuel and pressure tube temperatures may pose an issue with respect to small geometrical distortions (e.g. bow) and return to service conditions may become an issue, the actual safety characteristics are excellent. Such a feature provides an ultimate heat sink capability that does not rely on flow in the channels and hence is superior to many severe accident mitigation features such as core catchers since it precludes core melt.

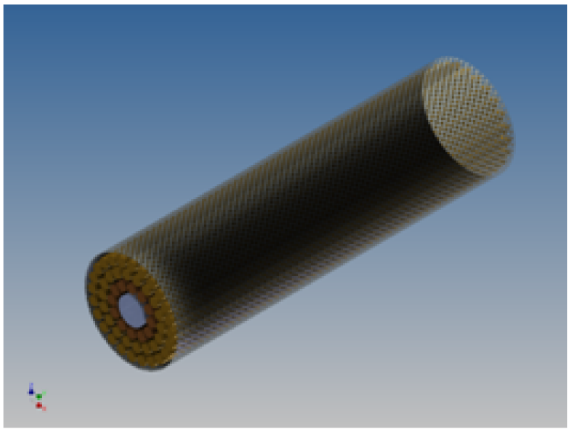


Figure 2.10: Liner to be used in HEC fuel channel

Initial design concepts for the SCWR retained the online refuelling feature of the CANDU, but have now been replaced by the batch fuelling concept. That design warranted the protection of a liner (illustrated in Fig. 2.10) for the insulator. The online refuelling in a CANDU-type reactor is done by i) having a fuelling

machine attach and seal itself to a channel closure plug, ii) remove the closure plugs, iii) provide cooling injection for that channel via the fuelling machine, iv) removing fuel either via flow assistance or by pushing new fuel on one side and removing fuel from the other, and v) replacing the shield plug and unsealing the machine from the channel. The equipment and procedures for fuelling become overly complicated at 25MPa, to the point where such activities are not cost-justified (especially given the fast refuelling times in BWR achieved during the last 5 years). In the end, batch-fuelled SCWR core can still: a) have quick refuelling outages about every 1 to 2 years; b) provide reactivity management by planning the batch fuelling and reuse of some assemblies; and c) still allow for flexible fuel cycle (e.g. some bundles with enriched uranium and some with thorium or actinide fuels). During the batch-refuelling, the liner will protect the insulator from scratches and damages that could have occurred by the removal and insertion of fuel strings.

2. Moderator Passive circulation System

   In the standard CANDU™, a severe accident occurs either by a LOCA plus loss of ECI, or a station blackout, or a reactivity-initiated accident plus Failure to Shutdown (FTSD). Fig. 2.11 below illustrates different pathways that could lead to a severe accident.

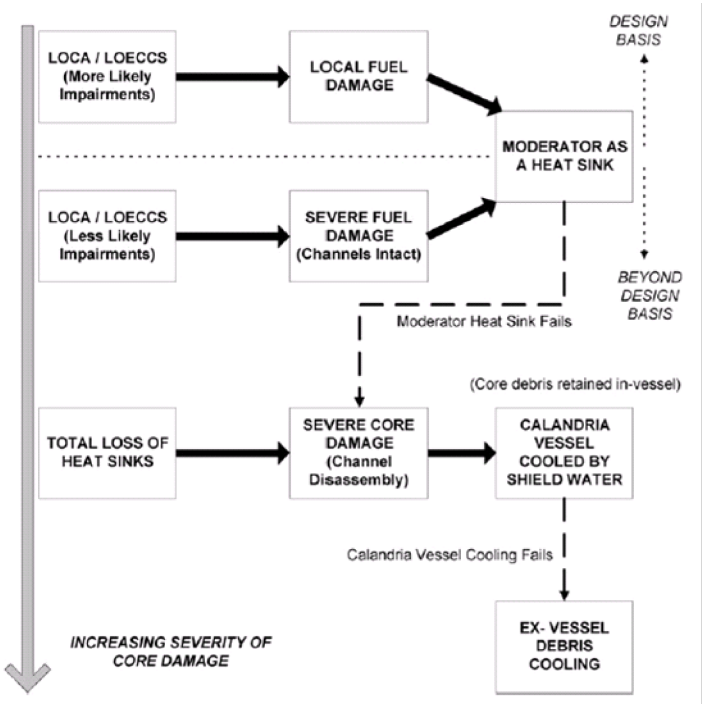


Figure 2.11: Core damage progression in CANDU [27]

A variety of systems (such as ECC, natural circulation mechanisms, and shutdown cooling) may play some role to either slow or terminate the sequence, depending on the initial failure. In the CANDU designs, some severe accident sequences can also be arrested or slowed by the moderator acting as a backup heat sink (and subsequently ensuring that the moderator inventory stays sufficient to maintain such a heat sink). However, the heat pathway to the moderator is formed only when the pressure tube deforms – either by ballooning sufficiently to overcome the annulus gas, or sagging – and contacts the calandria tube. Thus the pressure tube deformation must occur to establish the moderator as a backup heat sink.

The CANDU Moderator Circulation System (MCS) relies on active equipment

such as pumps and valves, and hence normal moderator cooling is dependent on power sources and equipment operation. In addition, moderator cooling can also be established by providing external water sources to the moderator (such as fire water).

One example of a severe accident for existing CANDU's is a LOCA with failure of ECC system (represented as LOCA/LOECCS in Fig. 2.11). The progression of the accident is thus: i) a break occurs in the heat transport system; ii) the SDS1 and SDS2 shut down the reactor and power quickly drops to decay heat levels; iii) blowdown cooling may occur for some time (and at this point ECC injection should commence); iv) with no ECC injection, the fuel heats up and the bundles may begin to deform; heat is transported to the surrounding steam and then pressure tubes or through radiation; v) depending on the coolant conditions, the pressure tubes either sag or balloon into contact with the calandria tube; vi) the heat is finally removed by the moderator so long as sustained dryout does not occur on the calandria tube surface; vii) heat will continuously be removed so long as the calandria remains full and some form of moderator make-up (active) is available. However, if the active moderator system should be unavailable for any reason and make-up not achieved, when the fuel channels heat up and transfer their heat to the moderator, the moderator water will boil off. Eventually, if sufficient moderator boil-off occurs without further moderator make-up, the calandria tube will either dryout or become uncovered, at which point calandria tube failure may occur [27], [28], [26].

Another accident sequence that could lead to core damage is a sustained station blackout followed by loss of standby and emergency power sources and an

inability of on- and off-site response teams to restore power and/or flow to critical systems. Such event sequences occurred at Fukushima in March 2011 and resulted in large-scale core damage and offsite radiation releases. Depending on the nature of the loss of external power event, a CANDU may: a) continue to operate at reduced power and meet its internal power needs (provided adjusters, heat removal systems, etc. are operational); or b) it may shutdown, whether due to a process system response or due to the detection of a potential DBE. In the event that no offsite or onsite Class-IV power is available, the reactor will immediately shutdown on SDS1, SDS2 or on control system action. As a result, forced flow will be unavailable and the decay heat in the core still needs to be dissipated.

At this point in the accident sequence, the backup power and emergency power systems would normally be activated, restoring cooling and terminating the event. Furthermore, some passive decay heat removal (such as natural circulation in the HTS and steam generator inventory as a heat sink) may take place for a period of time. In this manner, the HTS pressure and temperatures are temporarily stabilized. However, since the steam generators and emergency steam generator injection inventories are finite, the natural circulation deteriorates once the steam generator tubes become uncovered [28]. The HTS pressure will rise again and when the liquid relief valve set point is reached, the valve will open to release pressure. The HTS inventory that is lost through the opening of the relief valves causes fuel bundles to be uncovered. Eventually, natural circulation will be lost unless the steam generator inventory can be replenished. Once the circulation is lost, the HTS inventory will boiloff and fuel will become

uncovered. This results in pressure tube heatup and eventual pressure tube to calandria tube contact. At this point, heat is removed into the moderator system and the moderator inventory begins to boiloff. Unless moderator make-up can be established, the calandria tube will eventually uncover and the calandria tube may fail, resulting in core damage.

In the SCWR, if an accident sequence occurs wherein the standard cooling systems and emergency cooling are unavailable, the pressure tube need not deform as it is already in contact with the moderator. As the pressure tube and fuel heat up, the heat is rejected to the moderator system. Since the moderator system employs completely passive circulation systems, heat removal takes place without core deformation. The goal of such a passive system would be to keep the sheath temperature less than some limit in the event of an accident with failure of ECC. Studies have shown that this system can remove decay heat and maintain the pressure tube and fuel temperatures below accident limits indefinitely (as long as the ultimate heat sink remains in place).

Fig. 2.12 illustrates how the SCWR is being designed to be a passive heat sink. The passive moderator system (Moderator Passive circulation System, MPS) uses natural circulation, and will be a flashing-driven system which provides much higher potential moderator flow rates than those achievable under single phase conditions (due to the much larger buoyancy forces). During both normal conditions wherein the power to the moderator is 5% of the operating thermal power, or in the case of an accident wherein the entire amount of decay heat (up to 5% must be removed) is removed by the moderator, the moderator behaves in a similar fashion. The moderator then becomes a two-phase fluid; the force

of the fluid as it flashes to vapour keeps it moving to the heat exchanger where the heavy water moderator fluid is cooled and returns to the calandria vessel. This system does not rely on active power such as pumps but uses natural and passive forces – gravity and density differences for instance – to maintain the circulation.

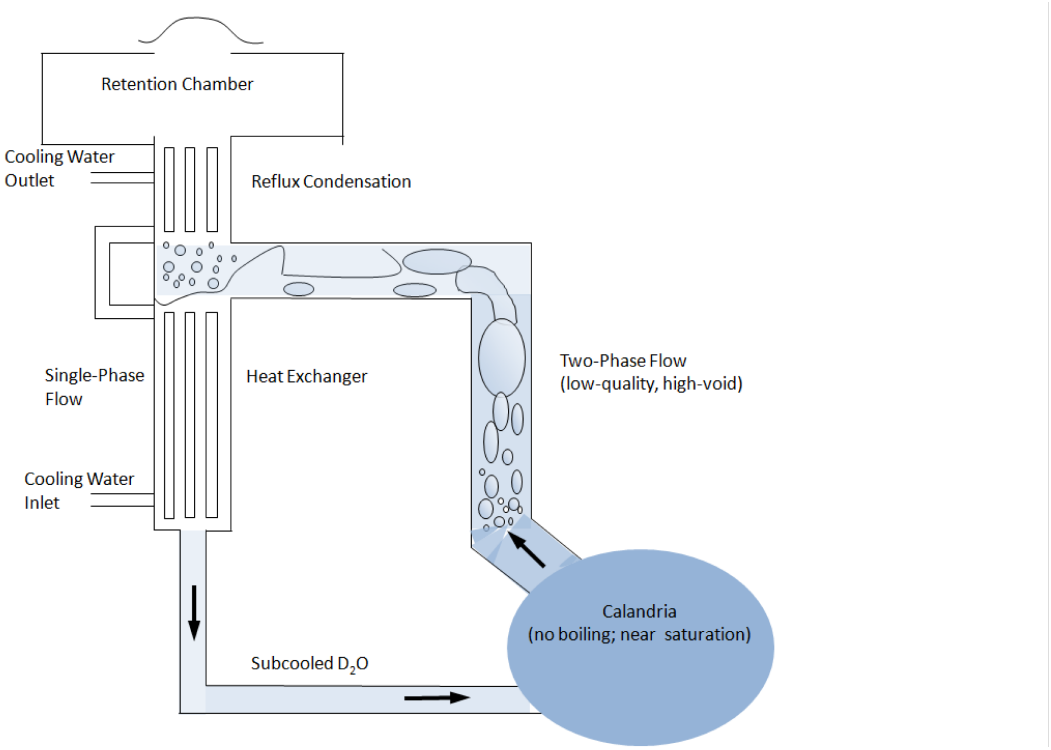


Figure 2.12: Moderator Cooling System of the SCWR

One of the issues that must be considered going forward is the water system or aire cooler that will supply cooling water for the heat exchange in the passive MPS. For the MPS to perform optimally achieving the high reliability expected of a passive system, the cooling water source should also be a passive. There also needs to be an avenue to discharge the heat from the heat exchanger, perhaps

to the atmosphere. Possibilities include the use of large-scale air-coolers, a large reservoir of water that can easily be replenished, on a ground source HEAT pipe (such as the reservoirs in the ESBWR or AP-1000).

3. Emergency Water System and Containment

   The Emergency Water System (EWS) will be a low-power and decay heat removal system similar in nature to the existing CANDU reactor shutdown cooling system which can be used as an emergency heat sink. The system is capable of cooling the reactor up to 3%FP at pressures and temperatures relevant to the SCWR system up to the point where the main heat transport system pumps can accommodate the process. The EWS might function like the AP-1000's In-Containment Refuelling Water Storage Tank (IRWST) that acts as a heat sink when the regular heat removal systems are unavailable. Alternatively, it may be active and take on characteristics of the safety-based shutdown cooling systems proposed for the Enhanced CANDU 6 (EC6™). The EC6 design follows similar principles as the ACR-1000.

   The ACR-1000 containment features an overhead reserve water tank that acts like a dousing spray in the event of a Large Break LOCA. (See Fig.2.13 below.) In the extremely unlikely scenario of a severe accident, the reserve water tank provides emergency backup to all ACR heat sinks i.e. moderator, steam generator, shield tank water, etc. [31]. This feature is expected to be carried on to the SCWR as a passive water tank to act as a backup heat sink for decay heat removal.

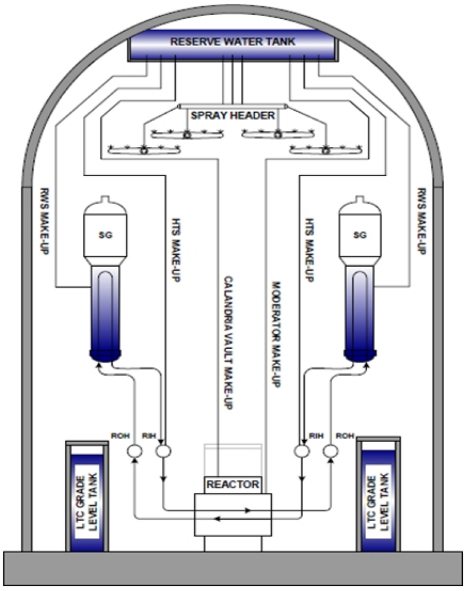


Figure 2.13: AP-1000 containment structure [31]

The containment safety system should be similar in nature to existing CANDU™designs which prevents and controls active material releases. Due to the more compact core and fewer in-containment components, it may be possible to significantly reduce the containment size and hence reduce costs. However, the reference SCWR design here considered the high pressure SCWR turbines to be housed completely inside containment, and as such the containment must be protected for events involving catastrophic turbine failure and subsequent missile loads. This containment is assumed to be designed to withstand the pressure, temperature, pipe whip and turbine disassembly forces for the potential SCWR design basis events while remaining structurally intact. It is also assumed that passive H_2 removal systems and a passive containment cooling system are included in the design. Similar to the ACR design, the containment will likely be a pre-stressed concrete structure with a steel liner.

4. Direct Thermodynamic Cycle

   Another revolutionary design change between the CANDU and the SCWR is the SCWR being a direct cycle reactor. This feature is possible due to the different coolant in the new reactor – super-critical water (SCW). Since it will not change phase but will remain as vapour, it can be used directly to generate electricity via the turbine-generator. Therefore, it will be unnecessary to have steam generators in a separate heat transfer loop, and may achieve 10% or more higher thermal efficiencies. The SCWR will have a direct cycle heat transport system with similar ex-core components and characteristics as a BWR or ESBWR. The exceptions will be materials, pipes and turbines being selected for supercritical water pressures and temperatures, possibly based on existing fossil equipment.

5. Core Orientation

   The orientation of the core – being vertical, not horizontal like the traditional CANDU™– is not in itself unusual for reactors since this is typical of almost all LWRs as well as the EU and Japanese SCWR designs. But for a CANDU-type reactor, it is a large design change. As mentioned earlier, the decision to go with the vertical core was based on various factors, not the least of them being the need for batch-refuelling which is much easier with a vertically oriented core. Further, since fuelling operations are from above, containment size and access will be improved.

6. Inlet Plenum/Eliminating inlet feeders

   The current design of the SCWR has a pressurized inlet plenum attached to the core. This differs greatly from the CANDU as the CANDU had inlet feederpipes

supplying coolant to the core. The coolant in the SCWR enters the plenum through inlet nozzles, and is then distributed to the fuel channels which are connected to the tubesheet just below the plenum. The individual channel flows will be tailored by using orifices either at the inlet or outlets. As the coolant descends in the channels, it becomes supercritical by the energy generated by the fuel [6].The inlet plenum is located on the top of the core and will be at pressures above supercritical, but at a temperature below the pseudocritical point. These conditions mean that the stress in this rather large vessel is reduced as compared to having a similar plenum at the outlet. The lower temperatures here also allow for greater material flexibility in construction and welding, and this is important since this is one of the larger pressure vessel features with the highest stresses in the design.

Having an inlet plenum means various components on the fuel channels are no longer needed e.g. the end fittings, the shield plug, the channel closure seal, and channel closure plug. Also, all the inlet feeder pipes are eliminated with this design. This decision has important ramifications in terms of economics as well as safety since replacing over 300 components (because of the over 300 fuel channels) reduces points of failure in that many components. This should directly reduce the frequency of a small break LOCA (SBLOCA), and remove the stagnation inlet feeder break event class from the design (all other things being equal). The outlet configuration uses very short feeder lengths which attach to several outlet pipe manifolds. The short outlet channel feeders have no bends and are designed for a 60 year lifespan. A large single outlet plenum on the reactor is not feasible since the pressures, temperatures and velocities

would require a very thick vessel, which if failed, would cause significant core damage. By having smaller diameter pipes and manifolds, no single failure would present a major safety concern, nor would the stresses and material limits be as problematic. The outlet pipe manifolds go to a main steam header and then to the high pressure turbines.

A ramification of the inlet plenum and outlet feeder design is that the control and shutoff assemblies must be inserted either horizontally into the calandria or at some angle to allow for gravity driven passive rod injection. The use of non-orthogonal or horizontal control and safety rods is a new concept in the CANDU design.

7. Emergency Core Cooling System

   If the SCWR follows the Super LWR, the emergency core cooling system would be comprised of the auxiliary feedwater system (or ICS in case of HPLWR), the low pressure core injection system, and the automatic depressurization system. The Automatic Depressurization System would be a revolutionary addition to the traditional CANDU™design. The Automatic Depressurization System (ADS) facilitates blowdown cooling and coolant recovery as well as system depressurization which subsequently enables a switchover to either the low power cooling system or a natural circulation or gravity-fed pathway. These features are a key part of the designs of GEN-III BWR such as the KARENA and ESBWR designs (in that they do away with the high pressure injection systems). A high pressure ECC system is difficult to envision since the temperatures and pressures of the SCWR would require very high pressure storage

tanks and pumps. Drawing from the BWR, the ADS is activated by opening valves connecting the system to the main HTS and provides a pathway for blowdown cooling flows to a suppression pool. Water from this pool is then eventually either gravity-fed or fed by the low-pressure ECC system back into the HTS under low pressure and temperature conditions. The SCWR design should include an ADS for rapid depressurization and LCI; this study assumes it present in the reactor.

8. Isolation Condenser System

   The Isolation Condenser System (ICS) is another passive safety system that we propose should be included in the SCWR design. Fig. 2.14 below illustrates the ICS. The system consists of a shell and tube heat exchanger which is immersed in a large pool of water. The ICS has four independent loops. Each loop contains two heat exchanger modules that condense the steam inside the tubes as well as transfers heat in the pool.

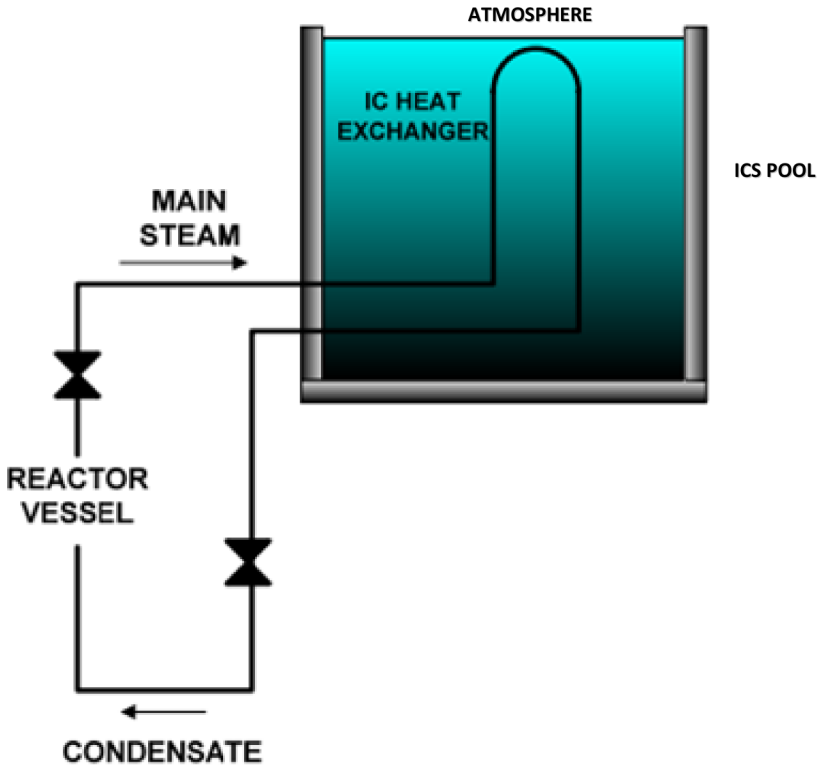


Figure 2.14: Isolation condenser cooling system [29]

The IC heat exchanger is isolated from the reactor during normal operations. In a situation where the reactor is to be isolated from the main steam line – for instance during a LOCA – the ICS can remove the core decay heat. The ICS can operate in all design basis conditions except medium- and large- break LOCA [30]. On ICS activation, a valve at the bottom of the IC opens to connect to the reactor, thus allowing water to fall by gravity to the core, while the steam rises to the pool. The heated water in the IC pool evaporates to the atmosphere. The steam is condensed in the tube section and the condensate drains to the core by gravity. Thus, the entire operation of the ICS is based on

natural circulation, with phenomena such as gravity flows, heat conduction, and condensation/evaporation employed for heat removal. The ICS is a Category D passive safety system.

In the ESBWR, the ICS initiates on signals such as high reactor pressure or MSIV closure. The IC pool in the ESBWR is in the upper part of the building; it is assumed here that the SCWR will likewise be located.

The special safety systems in the pressure tube-SCWR are a) Shutdown System 1, b) Shutdown System 2, c) Emergency Cooling System (consisting of pumped or gravity-fed LCI, ADS, reservoirs), d) Containment (containing a steel-lined concrete building, pressure suppression, H_2 mitigation, and passive containment cooling), and e) Moderator Passive circulation System.

2.4 Risk and Safety Analysis

A hazard is a condition which has the potential of causing an undesired consequence [32]. This implies that there is danger from exposure to a hazard. Risk can be defined as the possibility of loss or injury resulting from exposure to a hazard [33]. So risk connotes both the likelihood of some undesired event as well as the severity of the outcome or consequence. Mathematically, risk is defined as

$$Risk = Frequency \text{ (or probability)} \times Consequence$$

In a nuclear power plant facility, it is imperative to conduct risk and safety analyses due to the potential severity of accidents. Safety analysis would be beneficial for any undertaking or operation, regardless of the industry. But in the nuclear industry,

it can be considered especially important because, aside from usual accident consequences such as financial loss, fatalities, and man-hours lost, potential outcomes from these accidents include the deterioration of air and water quality.

A comprehensive risk analysis will answer the following questions:

1. What can go wrong that could lead to an outcome of hazard exposure?
2. How likely is it to happen?
3. If it happens, what consequences are expected?

To answer the first question, one should list the possible scenarios of events leading to a certain outcome. The next step is to estimate the likelihood of these circumstances occurring. These 'likelihoods' may be numeric estimations or calculations based on past experience. The third step can be dealt with by describing the consequence of each of the scenarios identified.

In other words, risk is a subset of three factors:

$$Risk,\ R = \langle S_i, P_i, C_i \rangle$$

Where S_i = Scenario of events leading to hazard exposure

P_i = Likelihood or probability of scenario i

C_i = Consequence of scenario i

This thesis deals only with the first two factors, the scenarios and the probability of events; the investigation into the consequences is listed as an area for future study.

Safety analysis is an integral part of the power plant operations. It is analytical in nature and can illustrate how the plant behaves under various operating conditions, or responds to a set of initiating events. Safety analysis can be deterministic or probabilistic.

The Canadian Nuclear Safety Commission (CNSC) is the nuclear industry regulator in Canada. It is responsible for ensuring that all nuclear-related activities are carried out safely and that the staff and citizens in the vicinity of a nuclear power plant (NPP) are not negatively affected. One of the ways the nuclear regulator in Canada enforces these safe conditions is by establishing guidelines for operation in the form of Standards, Guides, and Regulations. One of the standards of the CNSC is S-294; it gives the regulatory basis for risk-informed design. S-294 defines three levels of a Probabilistic Safety Assessment (PSA). They are:

1. "A Level 1 PSA identifies and quantifies the sequences of events that may lead to the loss of core structural integrity and massive fuel failures.

2. A Level 2 PSA starts from the Level 1 results, and analyses the containment behaviour, evaluates the radionuclides released from the failed fuel and quantifies the releases to the environment.

3. A Level 3 PSA starts from the Level 2 results, and analyses the distribution of radionuclides in the environment and evaluates the resulting effect on public health." [34]

This regulatory document also requires that a licensee perform a Level 2 PSA, and that the PSA model be updated every three years or sooner if the plant undergoes major changes [34]. The work documented in this thesis is a preliminary Level 1 PSA of the pre-conceptual SCWR design, and it represents the first such study available in Canada for the SCWR.

Safety analysis is an iterative process that occurs with the design process, performed to ensure that the design meets the relevant safety requirements. In Canada,

the requirements are set by the CNSC. Some of the CNSC regulatory documents have guidelines for the safety analysis that is to be carried out on nuclear power plants. For instance RD-310, entitled *Safety Analysis for Nuclear Power Plants*, gives the requirements for safety analysis methods, safety analysis documentation and review, as well as the requirements for selecting events that should be analysed. RD-310 is only for deterministic safety analysis of events. This implies that the analysis must be done based on predetermined rules and assumptions regarding the plant's operating state, as well as availability and performance of the systems. There are other regulations that speak specifically to PSA, for instance S-294 *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants*, and RD-337, *Design of New Nuclear Power Plants*. RD-337 discusses both deterministic safety analysis and PSA, and it lists several purposes of a PSA. Some of these purposes include:

- Identifying accident scenarios with the potential for significant core degradation
- Providing probability assessments for the occurrence of core damage states and major off-site releases
- Assessing the adequacy of plant accident management and emergency procedures
- Identifying systems for which design improvements or modifications to operating procedures could reduce the probability of severe accidents or mitigate their consequences [35]

Safety and risk assessments are invaluable exercises performed over the lifetime of the plant i.e. during siting, design, operation, and decommissioning. Not only

are the risks estimated of various hazardous situations, the results of such analyses can improve the design of the plant. This can occur through a risk-informed design process where risk analysts determine (perhaps probabilistically) the consequences of an event occurring in the plant as well as the response of the reactor to mitigate the event. If the analyst discovers that the response of the reactor is not suitable – for instance there are insufficient redundancies in place to arrest the accident, or the outcome of an event leads to radioactive releases which are beyond the limit set by the CNSC for such an event – this information can be fed back to the design team and modifications can be made to the design such that the reactor always stays within the acceptable criteria for these events. So risk-informed design is really an iterative process.

Risk-informed design will be critical for the design sequence of the SCWR. As a new reactor, all avenues for safety should be explored. Part of that entails examining credible accident scenarios, determining the risk of the accident, and reporting the reactor's response to the accident – if it does so within the acceptable limits for radioactive release or timeliness in stopping it, and if it produces minimal damage to the plant itself. The results of this analysis are reported back to the designers to ensure the plant design is robust. Another very valuable feature is to determine the sensitivity of the Level 1 PSA calculations to component level performance and reliability. This helps a designer to specify equipment and testing requirements which have the most impact on safety improvements.

The safety analysis is carried out over all four plant states to determine its performance, the plant states being Normal Operation, Anticipated Operational Occurrences (AOOs), Design Basis Accidents (DBAs), and Beyond Design Basis Accidents

(BDBAs) including events that could lead to a severe accident. An AOO is an operational process that deviates from the normal operation and is expected to occur once or more during the lifetime of the plant. But it does not cause significant damage to systems important to safety, nor does this event lead to an accident condition. A DBA is an accident condition against which a plant is designed already according to the established design criteria. In a DBA, the damage to the fuel and release of radioactive material are maintained within authorized limits. A BDBA is an accident that is less frequent but more severe than a DBA. It may or may not involve core degradation [36].

There are various approaches for studying risk. One method of categorizing the approaches is as deterministic or statistical:

1. Deterministic methods – Some deterministic methods of approaching risk are:

   (a) Maximum Credible Accident: In this approach, the worst-case credible accident is postulated. Then, the consequences of this accident are estimated. An example of a study using this approach is the WASH-740 done by the U.S. Atomic Energy Commission [37]. Although this approach can be beneficial for designing a new reactor, it can be difficult to determine what is 'credible', hence the analysis results would be a hard-sell to the regulator. The operator would have to prove that the worst-case scenario is being examined, and that indeed it is the worst event that could occur. This also leads to the problem of the description of the maximum credible accident being subjective. The approach would not be the best for a new reactor design since it is restrictive in analysis, not allowing a broad and rigorous test of the multiple fault areas possible in the reactor. Another shortcoming of this maximum credible accident approach

is that it may lead to conservative designs and hence higher costs, while not addressing the safety for lower consequence and higher probability events.

(b) Design Basis Accident: This approach is the traditional deterministic method used in nuclear safety. Herein, a plant is designed in such a way as to stand up to a specified list of failures. The postulated set of accidents (called Design Basis Accidents, DBAs) is based on past experience, knowledge of the plant, probability calculations, and engineering judgment [38]. When a licensee has proven that his plant can cope with this set of postulated accidents within the acceptance criteria, the regulator would grant the operating license. However, this approach can exclude provisions for safety that could have easily been incorporated while designing the reactors simply because such a scenario was not stated in the DBA list. This method differs from the Maximum Credible Accident method in that the latter bases its analysis on only one accident while the DBA method uses several accidents for the analysis.

Although the DBA approach to studying risk is not all-encompassing, it is useful as a first look to ensure the new plant will withstand some possible failures, especially failures that are known to have occurred in the industry. It could also be used in conjunction with one or more other approaches to risk and safety analysis. This method is not recommended to be used alone, however, as the prescriptive list of accidents can never be exhaustive. Examples of DBA's include loss of coolant, loss of pressure, loss of flow, continuous reactivity addition, and loss of electrical power incidents.

2. Statistical analysis methods – Some examples of this approach for studying risk are:

   (**a) Actuarial Analysis:** In this method, the frequencies of accidents are estimated from data obtained from large statistical databases. This is an approach commonly used by the insurance industry and formed the conceptual basis for PRA. One of the limitations of using actuarial analysis for safety analysis in the nuclear power industry is that a large empirical database is required [39]. There have not been so many accidents in the nuclear power industry on which to draw on for this method. However, this method can be used for component failures such as failure frequencies of valves. A drawback from this method is that if incorrect analysis is done on an accident, e.g. the root-cause analysis of an event, the report provides erroneous data to the database. Also, if incidents are not reported or not reported properly, it undermines the value of the database.

   (b) Probabilistic Risk Assessment (PRA): The PRA is an analytical tool to determine the frequency and consequences of an accident. In the safety analysis for nuclear plants, the accidents above a certain frequency of occurrence can be examined to ensure provision is made in the design to mitigate or protect against these accidents. The complete safety analysis would also define the acceptance criteria for the accidents and, after the PRA, show that the appropriate risk-based criteria are met. This method, like the one previous, relies on databases for failure rates. A difference between the PRA method and the actuarial analysis is that the former also analyses the outcomes of the accident – not only determining the frequencies of the accidents.

The PRA method for safety analysis is useful in that it can identify weaknesses in the design and provide quantitative measures for decision-making (such as risk-informed decision-making). PRA is also beneficial in that it provides a means for sensitivity and uncertainty studies that can highlight the best areas for improvements to safety. Again, like the actuarial analysis method, PRAs require reliable values of failure rates to ensure accurate results are produced, and to enable proper conclusions to be drawn. Another drawback is that that not every initiating event can be captured by this analysis method. It would be beneficial to the licensee to complement it with another method of safety analysis. The remainder of this study uses the PRA approach to studying risk.

Chapter 3

Methodology

This chapter describes the methods and tools used to estimate the incremental improvement in the pre-conceptual GEN-IV design relative to that of a standard heavy water CANDU™. First, the general probabilistic analysis theory is introduced, and the equations that form the basis of PRA are described. Next, the specific risk assessment tools used in this thesis are described along with the input data sources.

3.1 Probabilistic Risk Assessment

PRA may be summarized as one possible method for quantifying the risks inherent in a given engineered system and then used to compare such risks against those society encounters every day. Often, societal risks are discussed qualitatively or are judged independently from one another. By assessing the impact of the engineered system on a person's risk using PRA, knowing a person's risk tolerance and the benefits of such an engineered system, it is possible to provide quantitative and rational support for a power plant.

Risk assessment can determine the benefits of installing multiple redundant systems and assess potential common cause or functional failures. PRA can also be used to assess the strengths and weaknesses in a given design as well as assess the sensitivity of the risk to certain design or performance assumptions.

PRA can relate the plant risk to the factors that contribute to the risk, for instance operator action, equipment reliability, or plant operating procedures [40]. As a design tool, a PRA can give a numerical estimate of the risk the plant poses to the workers, public, and the environment following an accident. Finally, PRA can be used as input for risk-informed decision making such that the maximum benefit from design, construction or maintenance activities can be achieved.

The CNSC defines three safety goals for the frequency of core damage, small release, and large release frequency, namely:

1. **Core Damage Frequency:** The sum of frequencies of all event sequences that can lead to significant core degradation is less than 10^{-5} per reactor year

2. **Small Release Frequency:** The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} Becquerel of iodine-131 is less than 10^{-5} per reactor year. (The events in this category may lead to limited core damage and small releases; however, those releases are not significant. These accidents may require measures such as sheltering or short term evacuation of citizens in the vicinity of the plant [38].)

3. **Large Release Frequency:** The sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} Becquerel of cesium-137 is less than 10^{-6} per reactor year [35]

The methods and tools used in PRA rely heavily on knowledge of plant components and systems, their interactions and interdependencies, specific equipment failure modes, and statistics/probability theory. Probability theory is widely used in the field of reliability engineering to analyse the risk associated with a system, or to determine the reliability of a component. In reliability engineering, each component and system is described with a failure probability as well as a covariance (or common cause) factor which relates its operation to other systems, or its operation to other similar redundant devices. By examining each chain of a postulated event, in terms of a system's ability to meet its design intent, one can then determine the impact of such a fault on that sequence. Various components and systems have been so analysed and it is now possible to know their failure rate or probability of failure. A key component of PRA is to determine the various initiating events that may lead to core damage and assign a probability of such an initiating event occurring. Then the response of each important system and its probability of failure can be included to determine the overall integrated risk of the initiating event and the system's response leading to core damage. One shortcoming of PRA is that not all events can be assigned a frequency of occurrence and a consequence with surety. For instance an earthquake could be an event with a very low frequency, yet its outcome can have a very high severity. For example the probability of a Design Basis Earthquake as an initiating event may be set at 10^{-3} events per year for a certain magnitude quake, but there could be earthquakes (of other magnitudes) that occur on a rarer scale that have a potential for much higher consequence. The problem arises in setting not only its frequency value but its consequence for proper probabilistic analysis. A variety of methods are used to assess these situations:

1. Subdivision of events into sub-events (e.g. the division of LOCA into several categories that involve different break size ranges).

2. Assigning of conservative estimates for event occurrences. Note however that such a practice does not provide a true measure of risk and hence can lead to inappropriate conclusions for such a design.

3. Sensitivity and Monte Carlo analysis to determine the net impact or sensitivity of the assumptions related to severity and probability of occurrence.

Overall, the method to perform a PRA adopted in this thesis is as follows [6]:

- Define the acceptance criteria
- Generate a set of accidents to consider which span a wide range of possible initiating events
- Predict the frequency and consequences of the event
- Map the event progression by tracing all the critical equipment that may come into play that could: a) terminate the event sequence, b) cause the situation to worsen, c) affect other systems, d) cause another system to come into play. This is typically done by examining the timing of an event sequence, and at each stage of the accident where equipment might function, a "what-if" scenario is employed. i.e. "what if this system works" – then what happens; or "what if this system fails" – then what happens – keeping in mind failure does not imply catastrophic failure, but rather that a given equipment does not meet its design intent in some way (either due to run failure, demand failures, common cause or functional failures).

- Provide input on the performance of the systems and component failure probability
- Integrate the effects of initiating frequency and component failures to determine the net probability of core damage for each event sequence
- Prove that the appropriate risk-based criteria are met

To make the PRA a valuable tool, it must be updated over the life of the plant. This is done by continually reassessing the plant risks and potential events (e.g. DBA's) using the plant operation history to determine if the initial plant assessment remains current and correct. If not, the PRA should be redone. Furthermore, the CNSC demands that a PRA must be done every 3 years or sooner if there is a major change to the plant [34].

3.1.1 Probability Fundamentals

In PRA, the frequency and the probability of an event are the values most often quoted. Frequency refers to how often something happens, i.e. the events per unit time. However, probability is a measure of certainty about the truth of something and its unitless value is between 0 and 1. In PRA, the probability value is usually used to characterise component failures in the mitigating systems of the plant. Initiating events are normally expressed as frequencies, for instance the frequency of a loss of offsite power occurring at a plant. If necessary, the frequency value must be converted to a probability value before the PRA calculations.

To understand component failure probabilities and how they are derived in detail is beyond the scope of this thesis. Failure modes for each equipment are identified and

modelled such that the overall failure (or unavailability) of that piece of equipment can be identified and there are a number of probability models based on failures. These probability models may or may not be a function of time since manufacturing, and are typically modelled as either binomial, Poisson, or normal/lognormal. The models can be used to convert frequency information to probability values. These models can be classified into four categories: Demand Failures, Run Failures, Functional Failures, and Common Cause Failures. A single initiating event that results in the failure of multiple components or systems is termed a **Common Cause Failure**. Examples of common cause failures include a steam line rupture that affects nearby components [32], or natural dangers such as earthquakes initiating equipment failure.

Demand Failures arise in equipment that fail to start (or fail to open). Some of the systems that can experience demand failures are Auxiliary Feedwater, Shutdown Cooling, and Emergency Power. These are represented generally by the Binomial Distribution:

$$P\{r \text{ failures in N trials}|p\} = \binom{N}{r} p^r \left(1-p\right)^{N-r} \tag{3.1}$$

and P = Probability of failure for a single demand, and p = number of failures/no. of demands

where for M-out-of-N combinations:

$$\binom{N}{r} = \frac{N!}{(N-r)!r!} \tag{3.2}$$

Eqn. 3.1 can be used to convert frequencies of failures to probabilities. The probability of failure for a single demand then would just be "p."

Another failure type is the **Run Failures** [38]. This is for equipment that fails to run after a certain time, perhaps after running continuously in a harsh post-accident environment. For example a pump or generator operates from 0 to 100hrs and then fails either due to a lack of fuel, harsh local environments, or by some other mechanism. So these failures are time-related or time-dependent. Examples of continuous systems prone to run failures are diesel generators and auxiliary feedpumps. They are represented by the Poisson distribution:

$$P\left\{r \text{ failures in}(0,t)|\lambda\right\} = \frac{(\lambda t)^r e^{-\lambda t}}{r!} \tag{3.3}$$

where λ = probability of failure

The probability of one or more failures simplifies to the exponential:

$$P\left\{T_f < t|\lambda\right\} = 1 - e^{-\lambda t} \approx \lambda t(\text{ for small } \lambda t;\ \text{when } \lambda t < 0.1) \tag{3.4}$$

These are the relations used for component failure rates and event sequences given in terms of frequency.

For a series of independent events, the probability of them all occurring can be approximated by the sum of the individual probabilities of them occurring. That is, for a series of events $E_1, E_2, ...E_n$, the probability of them all occurring is:

$$P(E) = P(E_1) + P(E_2) + ... + P(E_n) - \prod i \overset{n}{=} 1\ P(E_i) \tag{3.5}$$

But for small probability values of the events, the last term can be neglected [41], approximating to

$$P(E) = P(E_1) + P(E_2) + ... + P(E_n) \tag{3.6}$$

3.1.2 Event Trees and Fault Trees

One of the first steps in developing a PRA is creating an Event Tree. An Event Tree is a graphical representation of the event sequence which outlines the systems that mitigate an accident and the result of the "what-if" scenarios discussed previously. The event tree displays the sequence of events that are involved in accident progression based on the success and/or failure of each component or system and accounting for the order in which systems will act. By looking at the tree, one can trace the event sequence progression and arrive at a conclusion as to the consequence of the incident, depending on the success or failure of the different systems involved. Each 'branch' of the tree represents a potential sequence of events that can lead to: a) a safe state with no core damage, b) a state where the core has some damage that is not a threat for major release, or c) severe core damage. A nuclear reactor is designed in such a way that if

1. A single component fails, various redundant but similar equipment may act to terminate the event.

2. An entire system fails, other independent systems will respond in such a way as to terminate the event.

The probabilities of the systems being involved in the event sequence are included in the event tree. Along each branch location (or at each what-if scenario), a probability can be assigned as to the system's likelihood to fail. These probabilities of

failure are a function of many variables such as the system design, the number of redundant components or "trains" within that system, its testing frequency, etc.

By following the event tree and multiplying the probability of each branch occurring – starting from the initiating event up to the end of that branch – the numerical probability of that specific end state can be determined. By summing up the probability from all branches that lead to a given end state (such as core damage), the end probability for that state can be determined (i.e. the Core Damage Frequency). One advantage of the event tree is that it is easy to quickly grasp the consequence of a system performing as designed, and it also demonstrates clearly the safety-related functions of the various systems – since the tree indicates if an accident is stopped by such a system failing or working properly.

The beginning of the event tree is called the Initiating Event. This is the accidental event from either internal or external failures that can lead to a possible breach of a safety barrier or to core damage. The sequence of all subsequent system actions that may be involved in that event are then shown in the event tree. There are two categories of initiating events:

- Internal Initiating Events: E.g. Loss of Coolant Accident (LOCA) which entails the failure of the pressure boundary in the cooling system which leads to a release of the primary coolant. It could arise from a stuck-open valve, a pipe break, or even a pump seal break. Other examples of initiating events include failure of the power control system; failure of the coolant pumps; failure of the moderator system cooling; support system failures such as instrument air or service water; or failure of the used fuel and new fuel delivery or storage systems. Such events may in turn propagate to other systems as in the case of

an internal fire.

- External Initiating Events: These typically originate from outside the plant, for instance earthquakes, floods, fires, or tornadoes [39]. Due to the potential random nature of such events, assigning a single event frequency is difficult and it is often determined uniquely for each site. Also, given the large variability in these events, it is also problematic to assign failure probabilities to equipment in the plant which are exposed to such events. Of particular difficulty is the common failure modes which may occur due to these external events. For example, during an earthquake, equipment which has not been seismically certified may fail, and hence several systems which are functionally and physically independent may fail simultaneously. Further, such events can lead to unrelated failures due to hazards which are a direct result (i.e. flooding from a tsunami which was caused by the original earthquake, or fires which are started due to a tornado).

In any case, either by internal or external events, some potential threat to the plant is postulated and the event tree is created. All system functions are indicated on the diagram as well as potential operator actions that may contribute to the final end state. It is up to the analyst preparing the PRA to define what a 'success' or 'failure' is. For example in the Loss of Class-IV power accident, a loss of power can be defined as the loss of power to the two 13.8kV buses or to only one of them (being conservative). Similarly, for the restoration of power following this event, success can be defined as starting the diesel generators to energize all of the Class III buses. If all are not powered, say powering two out of three is still success, or if for conservatism it is deemed a failure in the event tree sequence. Finally, the event tree will help

the analyst to estimate the probability of different end states for the accident – e.g. 'reactor kept cool', 'limited core damage', 'severe core damage' – and the frequencies thereof. Ultimately, the goal of the analysis of NPP accidents is to estimate the magnitude of the release of radioactive material. This can be determined from the fission products released to containment, their distribution within containment, and their leakage from the containment [32].

An event tree has headings above the tree which typically represent the systems called upon to arrest the incident progression, or the headings indicate the plant states (see Fig. 3.1). Each header section indicates a new system is being considered, and going from left to right, provides the order in which these systems would generally act. For instance, if after a LOCA the ECC is established, no further action will be needed; the end-state of the branch will be "OK". But if there is a failure of say the ECC, a subsequent system may be required, or the sequence could lead directly to core damage.

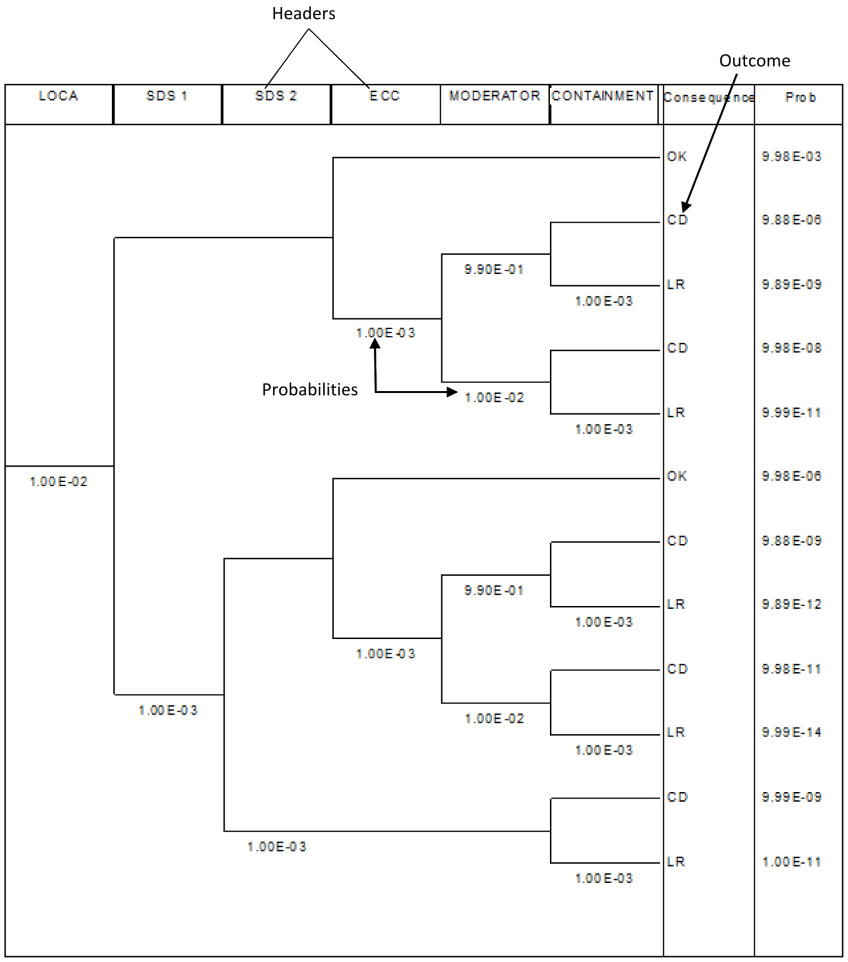


Figure 3.1: Sample Event Tree

Assigning the probability of the outcome of each system is also a very involved analysis process. At the fundamental level, each piece of equipment within a system can be analysed to determine its possible failure modes. Then, starting with these fundamental failure modes, the impact on the components using these failed systems can be determined. Next, the even higher level sub-systems will be examined for their sensitivity to the sub-systems below them; and so on until the net impact on the entire system is determined. This complete bottom-up approach is known as a fault tree and

it is described in the following sections. For other systems, a direct failure probability may be known either from experience, from comparisons to comparable equipment in the plant or in other plants and industries, or through statistical estimation (like Bayes' approach). Often, a PRA is composed of all these methods.

A fault tree is also a graphical illustration of the operation of a specific system in order to determine its failure probability. Fault tree analysis can be done on each of the main headings of the event tree to determine all the credible ways in which these systems can fail to respond, and it also uses probabilistic bases to calculate the final failure probability. Differing from the event tree, a fault tree uses a bottom-up approach that starts by examining the fundamental reasons and causes for individual components or systems to fail and then traces upwards to all systems it is connected to in order to see its impact.

Fault tree analysis allows the user to indicate if there are independent components in the system that could cause it to fail or if there are systems that are mutually dependent. In essence, it keeps asking 'why?' a component fails and the answers are displayed in the branches underneath. Fault trees can model the failure points of the components within a system or a system as a whole. It is also advantageous because it is easily grasped, being a graphical display in a top-down manner. In the fault tree, the Top Event is the undesired event. (This is the event that could be taken from the event tree as a system failure.) An example is shown in Fig. 3.2 below.

Another benefit of the fault tree is that it quickly shows which components are the largest contributors to a system failure – those with the lowest reliability. Thus, the weaknesses or vulnerabilities in the system are identified. By examining the potential changes in this probability on an event tree, one can then determine the net effect on

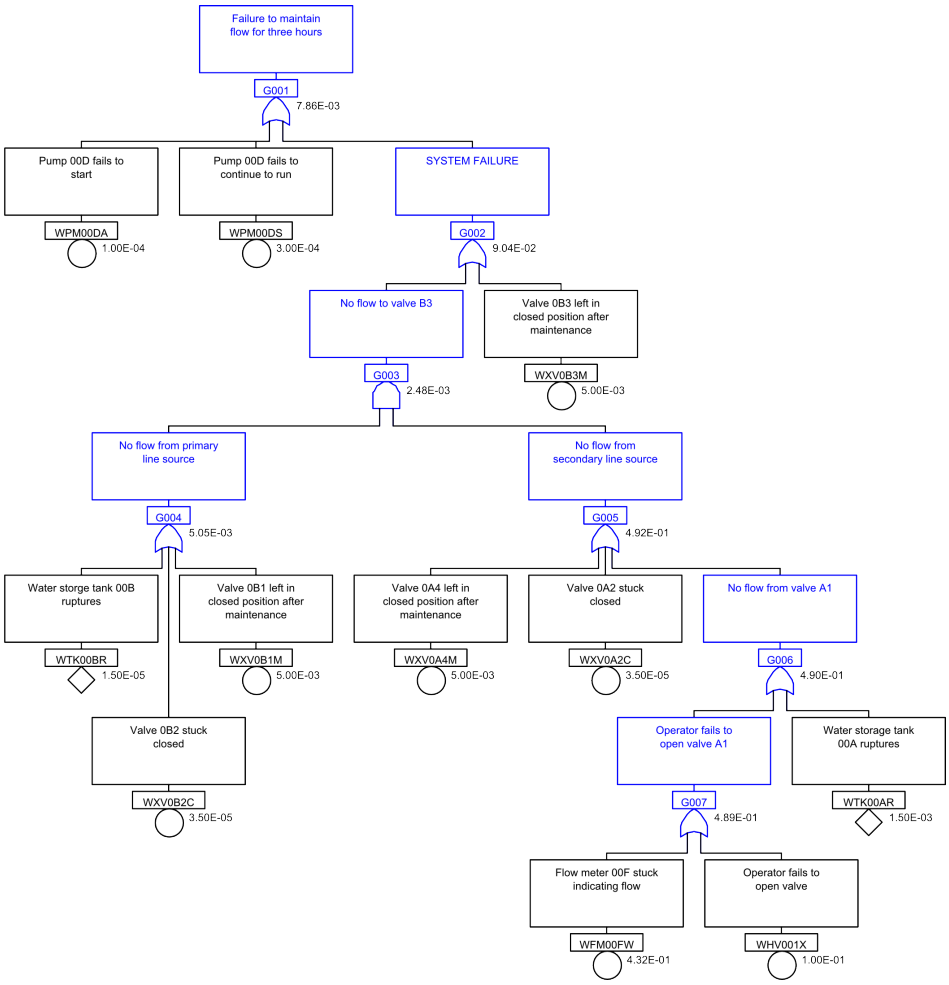


Figure 3.2: Sample Fault Tree

core damage frequency (CDF), or the sensitivity of CDF to the failure probability of a single component. And when doing root-cause-analysis, a fault tree could display the root causes for a system failure. With the fault trees showing which components are the weakest link, a designer may consider several options including system redesign, replacing that component with another which has a higher reliability, or including more redundancies in the system to improve its overall reliability.

When creating a fault tree the reasons for failure can be incessant. For instance, one can continue asking 'why' a component fails in order to discover the cause of the overall system failure. However, a point must be reached where this is cut off. In such cases, when modelling the fault tree, this cut off point is called a Basic Event. For example if it is determined that one of the failure modes of a component is a circuit board failure, it would be judicious of the analyst to stop the fault tree analysis at that point – instead of examining which part of the board failed.

For a fault tree to be effective and valuable, it must be constructed based on the way the system operates. Therefore, the fault tree analyst must have a good understanding of the system. For example, if crossties exist in the system, the person developing the fault tree should know where they are and their function so that the effect of these ties is incorporated into the probabilistic calculations.

3.1.3 Tools for Probabilistic Risk Assessment

There are numerous computer codes available to perform PRAs in the nuclear industry. These tools include *SAPHIRE* (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations) developed for the U.S. NRC and which is used in the U.S. by most utilities; and *CAFTA*(Computer Aided Fault Tree Analysis). Every

model, as well as the approach used for a PRA by a NPP licensee, must be approved by the regulator. This study was done using *CAFTA* v.5.3.

CAFTA is a computer software tool created by Electric Power Research Institute, Inc. (EPRI). *CAFTA* is a general tool for risk and reliability analysis [42], but EPRI also developed software for specialized analysis, e.g. *FRANX* used for fire PRA. As a reliability tool, *CAFTA* can be used to develop reliability models of large or even complex systems. This is done through fault tree and event tree building.

The program includes a reliability database for storing the basic event, failure rate, and gate information used in the models for each system in the plant. This database can be updated as required and the updated values in turn will be reflected in the output of the event trees and fault trees. Hence, the tool easily facilitates sensitivity studies because changing a single value in the input reliabilities will permeate all calculations simultaneously and provide the integrated result. A failure probability can be a function of the failure rate of the current event and a run or mission time. For instance recalling eqn. 3.4, the probability of a pump failing to run can be represented by

$$P(Pr) = 1 - e^{-\lambda t}$$

where

$P(Pr)$ = probability of failure for pump running

λ = failure rate per unit of time

t = required operational time (mission time)

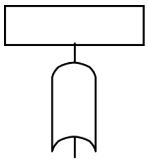
For each pump of that type, the failure rate for that event – failure to run – is always λ. However, if consideration is made of the pump's failure to run after operating for 1000hrs, the failure rate might be different than the generic 'failure to

run' rate of λ. Therefore, the reliability database could be kept updated corresponding to the type of event and failure.

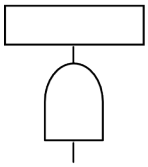
It is possible in the reliability database to specify what type of component failure is being modelled, for instance failure to start the diesel generator, or failure to run after 10hrs of continuous operation. The analyst would facilitate the traceablity of the components in the database by using a naming convention. *CAFTA* provides an interactive environment not only for creating and updating fault trees and event trees; it also allows a user to specify the format of values to calculate the overall system reliability. Therefore the failure of a component can be entered as a rate of a failure, i.e. per unit time, or it can be entered as a probability.

The solution of the fault tree and event trees is based on probability theory. The fault tree is based on AND/OR gates. The 'AND' represents the probability relations for independent events which must all occur for the failure to be realized or events that must occur simultaneously. If they are independent, $Pr(E_1 \bigcap E_2) = Pr(E_1).Pr(E_2)$ but if the events E1 and E2 are dependent, $Pr(E_1 \bigcap E_2) = Pr(E_1).Pr(E_2|E_1)$.

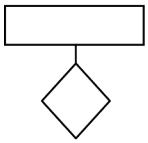
Some of the symbols that will be seen in the fault trees of this study are the following:



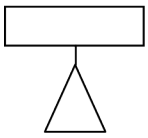
Or Gate: Logic for the union of input event. The fault occurs if at least one of the inputs fails.



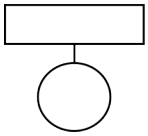
And Gate: Logic for the intersection of input event. The fault occurs if all of the inputs fail.



Undeveloped Event: This is an event that cannot be developed due to lack of information or it is not desired to be developed because it is of insufficient consequence.



Transfer Gate: This gate indicates that the tree is developed further, probably on another page. It connects other parts of the fault tree or can connect to another fault tree.



Basic Event: This is a fault that does not need any further development.

Figure 3.3: Symbols used in fault trees

3.2 Accident Analysis

3.2.1 Safety metrics and Accident Set:

One way to create the accident set is to examine the failure of each process system and look at how the reactor mitigates those failures. Or to assume the failure of a system combined with the unavailability or impairment of another system, such as a special safety system. Another option may be to postulate a failure plus an external event occurring, such as tornado, earthquake, fire, or aircraft crash: one could perform analysis to show probabilistically how the plant would withstand a LOCA followed by a design basis earthquake. Finally, one can identify initiating events from past practice, operating experience, regulatory documents, or even by reviewing the PRAs (and list of initiating events) from similar plants.

It might be difficult to surmise all the credible accidents that could occur at the NPP. Therefore, it would be beneficial to apply both deterministic and probabilistic methods to identify these incidents. This combination could be extremely valuable for a revolutionary system such as the SCWR.

Two accidents in particular were chosen for examination in this study – a small break loss of coolant accident (small LOCA) and a Loss of Class-IV power event. These two incidents present the opportunity to scrutinize the safety systems' behaviour in the reactors and the reliability of the systems to respond as needed. By comparing the PRA analyses for these events to similarly determined events for CANDU, the incremental improvement in safety can be estimated. It should be noted that station and licensing PRA analysis goes through a much greater level of detail as compared to the models shown here – in terms of its input data and fidelity, the

number of branches, and the number of initiating events. The intent of this thesis is not to replicate these PRAs but rather, for a given set of input reliabilities and with the improvements in the GEN-IV design, to do a consistent comparison between the reactors and assess the improvements. As such, deviations in input frequencies and input reliabilities, while important, do not play a significant role in the conclusions of this thesis.

3.2.2 Data Sources:

The fault trees and hence the event trees are populated by probabilities of failure of the corresponding components and systems. These failure rates are derived from various sources. One of them is using past data i.e. data from an operating plant, preferably a similar plant. Then, after the new plant has operated for a period of time, the failure database Bayesian updates can be applied to the PRA, using posterior knowledge. Another method is to use generic databases. Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995 [43] is one of the sources of data that could be used. However, these databases should also be updated with plant-specific data by Bayesian updating method. Bayesian updating produces posterior probability estimations to improve the prior probability. This is especially useful where there was only sparse generic data available initially; then the plant-specific data provides more accurate data. Plant-specific data can come from periodic test reports, failure reports, maintenance reports, or even control room logs.

The SCWR is in the pre-conceptual stage of design and as such, there is no model from which to draw component failure rates. Therefore, for the SCWR's fault trees and event trees, the generic CANDU™(and in some cases LWR) failure probabilities

were used, derived from a variety of sources e.g.: NUREG/CR-2300, *Probabilistic risk assessment procedures guide* [44] and NUREG/CR-75/014 (WASH 1400) *Reactor safety study – An assessment of accident risks in U.S. commercial nuclear power plants* [45], IAEA-TECDOC *Component reliability data for use in probabilistic safety assessment* [46] and the *Savannah River Site Generic Database* [47]. A drawback in this study is that CANDU-specific data was not available for the public and so some estimations from databases were used. Further, no Bayesian updates were performed since plant data was not available.

The failure rate of a component or system was determined based on its mode of operation. For instance for safety valves like ASDV and LRV's, there is a different failure rate listed for them failing to open and for them failing to close and so the appropriate values were used. Also for the backup diesel generator, there is a failure probability for it to fail to run or for it to fail after having run for a period of time. For the purpose of this study, only the probability of it failing to start is necessary, so a demand failure is attributed to the backup diesel generator. Further, there are also probabilities for restoring offsite or onsite power within a given timeframe which were assumed for loss of offsite-power (LOSP) scenarios.

Since the databases only have components' failure rates, when the overall system failure probability was not known for input into an event tree, a fault tree was constructed to generate the system failure probability – the top event. This underscores the importance of understanding how the system operates, in order to know its modes of failure. A schematic of the system showing its connecting lines and paths for operation is therefore very useful in a fault tree. Some systems, however, had generic failure rates or else were known from common knowledge/public literature, e.g. the

CANDU shutdown system's failure probability of 1 in 1000 [48].

Chapter 4

Results

This chapter compares the responses and incremental improvements in risk for the SCWR and the CANDU for two significant DBA's. The assessment is limited in scope to two initiating events which have historically contributed to the core damage probability for nuclear power reactors. The main objective here is to examine the improvements in the SCWR design relative to existing technologies. The initiating events considered in this work are:

1. A small break Loss of Coolant accident wherein improved ECC reliability and potential moderator passive cooling may play an important role in reducing the risk of core damage for such an event, and may in fact negate most of the severe consequences of such an event. The selection of this initiator is driven by the so-called LOCA-LOECI sequence which is a dominant contributor to risk (i.e. loss of coolant accident followed by a complete failure of the emergency coolant injection system). Furthermore, the sensitivity of the results are examined to see the competing impacts of proposed simplification in piping for the SCWR

and the harsher system conditions (high pressure and temperatures leading to increased failure rates). For this work, the relative change in SBLOCA-induced core damage is assessed for both the SCWR and CANDU using a consistent but simplified methodology. In addition, a separate LBLOCA is assessed for the SCWR design to facilitate comparisons with other GEN-IV reactor concepts.

2. A Loss of off-site AC (Class-IV) power, which can lead to a Station Blackout (SBO) event wherein main, backup and emergency power systems may be lost. The 2011 Fukushima Daiichi accident illustrated the potential consequences of a SBO with sustained loss of heat sinks. For this event, passive moderator cooling in the SCWR design is expected to significantly reduce the CDF and post-accident consequences. It should be noted that common cause events (e.g. tsunami or earthquake) and operator errors are not modelled in this work.

4.1 Loss of Cooling Accidents

A small break loss of cooling accident (SBLOCA) can occur from a break in a small diameter piping (<10cm) [51], such as feeder pipe break in a CANDU. The features of a LOCA progression are dependent on size, location of break, and reactor initial conditions but in general involve detection of the LOCA, initiation of the special safety systems to shutdown the reactor, emergency core cooling injection and containment response. The details of the event considered are discussed below.

4.1.1 Loss of Coolant Accident (LOCA) in CANDU™

During normal operation the HTS provides a coolant pathway for heat to be transferred from the reactor fuel in the core to the steam generators. A schematic of the flow system is shown in Figure 4.1. The main circuit can be seen as two loops, with the coolant flowing in alternate directions in each fuel channel as the coolant passes through the reactor.

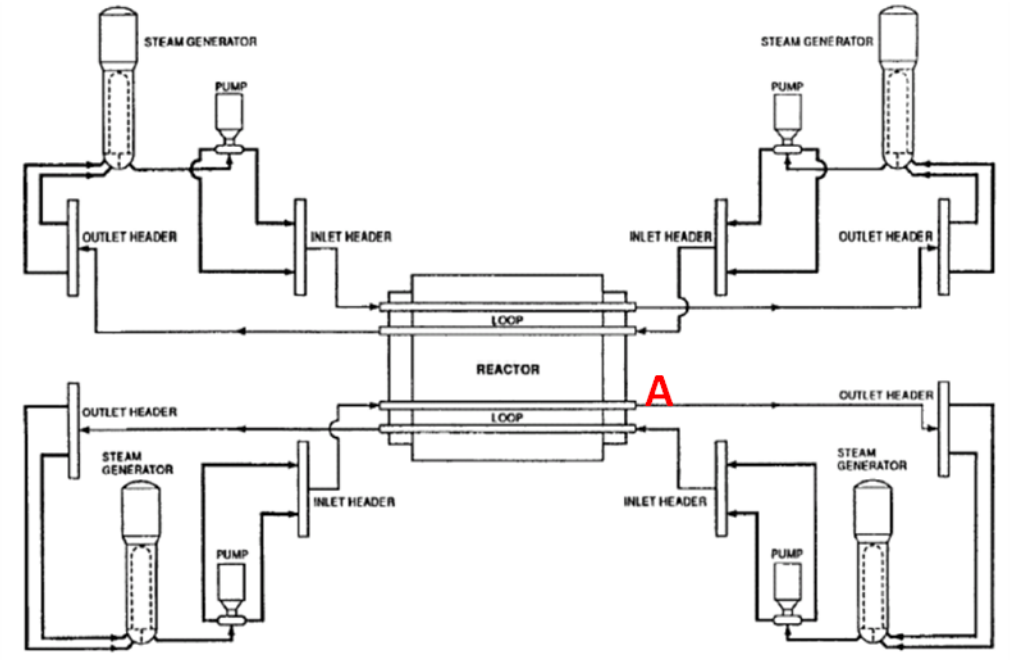


Figure 4.1: CANDU-6 HTS flow diagram [52]

Starting from point A in one of the loops, coolant emerges hot from the fuel channels. The feeders from a quarter of the fuel channels (about 95) are connected to the reactor outlet header (ROH) from which the hot heavy water coolant flows to the steam generators. In the steam generator, the heat from the reactor coolant is transferred to the light water on the secondary side. The heavy water coolant is now

cooled and enters the main HTS pumps which circulate water to the large distribution reactor inlet header (RIH). The RIH distributes the coolant to each of the feederpipes connected to it, sending the coolant to the inlet of the fuel channels flowing in the opposite direction from the earlier set. The coolant is heated once again as it flows past the fuel and emerges at the other end of the reactor flowing through the ROH, to the steam generator, and then the pump. The loop is completed by the coolant flowing thru the RIH back to the first set of fuel channels.

A small LOCA can occur in any of the high pressure piping in the HTS either by a break in the smaller feeder pipes or auxiliary pipes attached to the HTS, leaks in the steam generator tube piping, spurious valve discharge or breaks in the pressurizer, breaks in a pressure tube, and smaller cracks or openings in the pipes connecting the steam generators, headers and pumps. Once a small break has occurred, inventory will continuously be lost from the HTS and, depending on the break size, the control system may take action to terminate the event (if it detects a LOCA), or it may mask the event by attempting to increase flow from the inventory control system, increase pressure in the pressurizer, and/or regulate power due to increasing void. For many break scenarios, SDS1 and SDS2 may be activated to terminate the event. Prior to shutdown, the safety concerns are related to ensuring the fuel, sheath, and pressure tube temperatures stay within established limits. Post-shutdown, a primary concern is to ensure that a heat sink is established even considering a break in the HTS pathway. For some breaks, the ECC system supplies coolant from multiple locations in the loop such that the decay heat in the fuel can be removed. In the longer term, ECC recovery will collect the water ejected from the break from the sumps in containment and re-inject it into the HTS. ECC heat exchangers remove

decay heat such that a long term steady state cooling of the fuel is achieved.

Since LOCA event sequences are highly dependent on break location, size and reactor design/initial conditions, no single event tree can capture all of the potential pathways for CDF in a tractable manner. Therefore, in a PRA typically, a range of initial conditions and breaks is examined and a site- or design-specific PRA result generated. In order to analyze the improvements in the SCWR design, a "generic" LOCA sequence has been established wherein the major processes and safety systems are captured. This "generic" event sequence would consist of the following potential actions in a CANDU™design:

1. Break initiation with a frequency that depends on operating history and power, piping length, materials, and postulated break size.

2. Control system actions – either to reduce power if a LOCA is detected (through, for example, a stepback) or to initiate high feed flows to the HTS, minimize bleed flow, increase pressurizer demand, and/or liquid zone control level increase to counteract any coolant temperature/void feedback effects. In the event that the control system terminates the event prior to safety system actions, the likelihood of fuel overheating and core damage is negligible, although a long term heat sink is still required. If the control system does not terminate the event, any masking actions must be considered in the analysis which would delay the SDS1 and SDS2 trips.

3. SDS1 and SDS2 trips – the special safety systems for shutdown are designed to detect a LOCA and terminate reactions in the core. Depending on the specific design, initial conditions, and the size/location of the break, multiple instruments may detect the break and initiate the logic sequence which will activate

each SDS. In the event that none of the control systems, nor SDS1 and SDS2 shut down the reactor, fuel will eventually overheat and core damage will occur. Due to the multiple and redundant safety systems, equipment diversity, and physical separation within the design of each SDS, such a "failure to shutdown" scenario is of very low probability.

4. Post-trip cooling of the fuel then becomes a primary safety concern since prevention of fuel failures due to high temperature will prevent significant radiation release to containment. Beyond the normal heat sinks sich as SDC, the ECC system has various capabilities to cool the fuel in this event including high and low pressure injection systems which will cool the fuel. ECC is also equipped with heat removal systems powered by multiple redundant power systems such that a failure of Class IV power will not lead to degradation in ECC capabilities.

5. In the event of an ECC failure post-trip, fuel cooling may become degraded. First, the remaining coolant in the HTS will either be lost through the break and/or will be boiled off by the fuel. Once steam conditions exist in the fuel channels the fuel will heat up significantly and transfer some heat to the pressure tube. The pressure tube will also heat up and may either deform through sagging or ballooning into contact with the calandria tube.

6. For CANDU, once contact is made between the pressure tube and the calandria tube, heat is rejected to the moderator fluid in the calandria. As long as moderator fluid can be replenished and the heat loads to the moderator are not sufficiently high as to cause complete calandria tube dryout, a heat sink pathway is established to the moderator system and further deformation is precluded.

7. In the unlikely event that the moderator system is incapable of removing sufficient heat or cannot be replenished, core damage will eventually occur. In this process, the moderator boils off and channels in the upper elevation of the core begin to overheat, deform, and ultimately fail.

As a result of the event sequence above, and the availability of each of the process and safety systems involved, core damage may occur with a finite probability. The risk model adopted for this generic CANDU™sequence is shown in Figure 4.2. The event tree is initiated with a small LOCA frequency of occurrence assumed to be 0.01/yr [51]. The next actions are SDS1 followed by SDS2 with an assumed reliability of 99.9% based on the requirements set forth in licensing documentation [48]. (Control system action is not being credited in this work.) If neither SDS is operable, this results in the "failure to shutdown" (FTSD) type scenario which could lead to core damage, indicated as CD-FTSD in the figure. Given the high reliability and independence of both SDS1 and SDS2 as well as the low frequency of occurrence, the combined frequency of core damage is less than 10^{-8} from this sub-sequence.

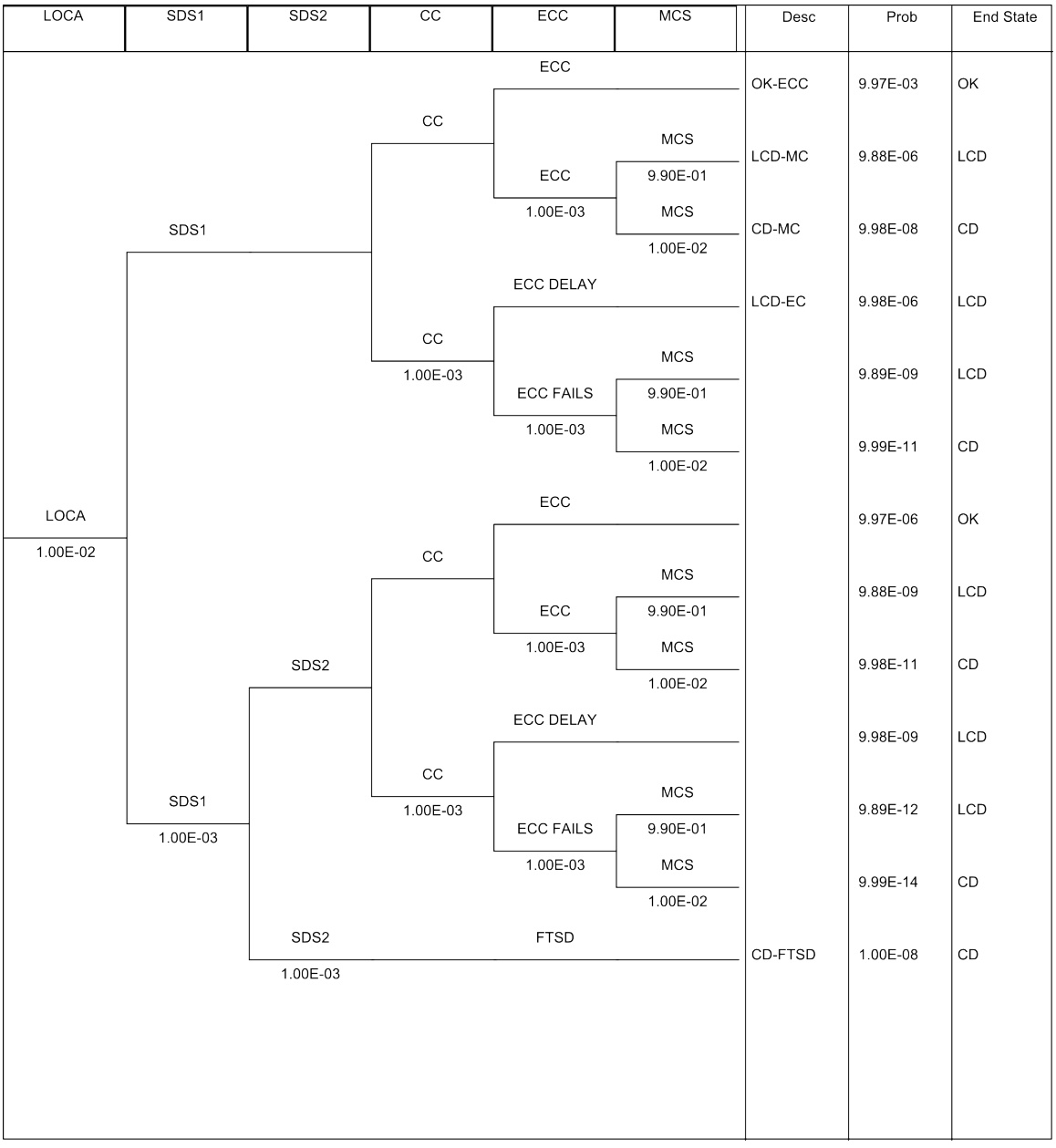


Figure 4.2: Event Tree of SBLOCA in CANDU™

In the event that SDS1, SDS2 and control system actions terminate power in the core, a heat sink must then be established. Depending on the size and break location

it may be possible to employ a low pressure heat sink process system such as SDC. However, the effectiveness of the SDC as a means for cooling and depressurizing the HTS, and ensuring that SDC flow, heat sink, and inventory can be maintained, is dependent on the specific nature of the LOCA. For the purposes of this study, the complicated actions involved in SDC operation post-LOCA are not modelled, and it is conservatively assumed that SDC could not be brought into service. Rather, the next available actions center on the availability of ECC High Pressure Injection (HPI), Medium Pressure Injection (MPI), and Low Pressure Injection (LPI). The combined reliability of these systems is estimated at 99.9% [38]. When ECC functions, the core is kept cool (OK-ECC).

Crash cooling of the steam generators is also credited in this event. If crash cooldown of the steam generators fails, the HTS temperatures and pressures will remain high. Therefore, the emergency coolant injection (ECI) will be delayed. When this happens, some fuel damage can be expected before emergency coolant is injected. If ECC is available then the event sequence is terminated with only small core damage (LCD-EC). In the event of ECC failures, fuel channel deformation will occur as outlined above and the moderator would act as a heat sink. As long as the moderator cooling system and/or inventory are maintained, the event should again be terminated with no fuel failures (but some fuel channel deformation) - given as LCD-MC in Fig. 4.2. Since the moderator system is process equipment, it is assigned an unavailability of 10^{-2} based on typical process system reliability. In reality the MCS system should be modelled with higher reliability, since even a combination of moderator inventory injection (via fire water for example) and moderator boil-off

could remove heat from the calandria tubes (with the heat sink being the environment within containment). Under such sequence, moderator as a heat sink would not require the moderator pumps, heat exchangers and other active equipment for use. Nevertheless, the more complicated actions required for sustained moderator heat sink in the absence of process system availability are not modeled in this work and are conservatively assumed to be unavailable. Core damage is expected to occur if moderator cooling fails (CD-MC).

In these event trees, 'OK' implies the cool is kept cool. 'LCD' refers to a limited core damage state wherein pressure tube deformation and/or damage to the fuel sheath. So there is deformation of local components, but no more. 'CD' is used in this thesis as a state in which substantial damage occurs to the core resulting in a loss of core geometry and radionuclide release from the fuel failures may occur.

The integrated result for this generic sequence for a SBLOCA gives a final CDF contribution on the order of 10^{-7}. In order to ascertain the most important contributors to safety in this sequence each of the assumed failure probabilities was individually perturbed one at a time by a factor of 50%. The sensitivity to individual system failure reliability was ranked and the result illustrates the following:

- The single largest sensitivity is to the functional availability of the ECC system, since there is no alternative heat removal capability within the model (in fact the event sequence should credit a finite probability for Crash Cooling and SDC heat removal).

- The next largest sensitivity resulted from the reliability assumptions on the moderator cooling system. Since there are multiple means for maintaining moderator inventory, it is probable that the moderator may act as a heat sink even

given that the MCS process systems are unavailable. However, since it is an active system and is not designated as a special safety system, the reliability included in this assessment limits its contribution to safety.

As a result of these observations, it becomes apparent that the proposed SCWR feature of passive moderator cooling will likely provide large quantitative improvements in risk since it both improves reliability of moderator heat removal through passive means as well as provides a high quality heat sink without fuel channel deformation or the need for active equipment.

4.1.2 Loss of Coolant Accident (LOCA) in SCWR

The generic event sequence discussed in section 4.1.1 is modified to account for the major design differences in the SCWR design. The fundamental changes that need to be considered are:

- Negative CVR: This means the SDS systems are generally not required to shutdown the core. Eventually the high void in the core will lead to shutdown and the FTSD scenario is removed. Hence, the role of SDS1 and SDS2 is to limit fuel and sheath temperatures during the transients such that the reactor is shutdown before fuel limits are breached and ensure that a timely trip occurs prior to excessive coolant loss. However, no events are considered where power remains high during a LOCA for an uninterrupted period.

- The use of ADS in lieu of HPI: As in similar GEN-IV designs and the ESBWR, it is assumed that a functioning ADS is capable of sustaining blowdown cooling for

a period of some 10s of seconds. Typical designs such as that in the ESBWR include several banks of ADS valves which are operated using independent means (e.g. spring-loaded relief valves, local pressure actuation valves, etc.) Since at this time detailed models are not available to assess the effectiveness of ADS blowdown cooling, it is assumed in this work that if ADS operates it will meet the design criteria (i.e. limit sheath temperatures to within acceptable accident limits). If the use of ADS in lieu of HPI is analysed and demonstrates ADS to be insufficient, the design may need to be revised to include a High Pressure Injection system.

- A low pressure ECI system with high reliability similar in design to the ESBWR gravity-fed system or the ACR active LPI/RHR system

- The use of a passive moderator cooling: As discussed previously, this passive moderator cooling system is the last line of defence to keep the core cool in accident scenarios where cooling capability is lost. While further measures may be available (moderator boil-off and inventory replacement), only the passive nature is conservatively modelled here. It is expected to greatly reduce the CDF and increase the overall safety of the reactor.

The sequence of potential events is similar to the CANDU, i.e:

- Break: The break probability must consider both the new operating conditions as well as the simplification in piping (less feeders, less pumps, less valves, no steam generator tubes etc.);

- Negative CVR: A loss of coolant in a CANDU is said to lead to positive coolant void reactivity (or positive CVR). In the SCWR, the moderator and the coolant

are still separated and so a loss of coolant does not involve a loss of moderator. However, a combination of properties such as the smaller lattice size in the SCWR, fuel enrichment, and the non-fuel centre pin are expected to lead to the SCWR having a negative CVR on coolant voiding. Another feature that has been introduced to the fuel channel design to ensure negative CVR is to increase the thickness of the pressure tube and insulator [69]. The centre pin in the SCWR fuel bundle can be a neutron absorber (poison) which will further reduce the CVR. Therefore, in a loss of coolant event in a SCWR, the negative CVR can be credited for slowing and eventually stopping the fission process;

- SDS1 and SDS2 activation to ensure a minimal loss of inventory prior to trip;
- ADS: The use a depressurization system stems from modern GEN-III+ designs such as the ESBWR. These GEN-III+ designs utilize the ADS system on the hot leg such that forward flow is always maintained irrespective of break location, hence avoiding flow stagnation. For the SCWR design, it is unclear if the ADS system will be required in a LOCA. For the reference case, it is assumed ADS is required to preclude core damage similar to the ESBWR concept;
- LCI: As mentioned earlier, this system initiates low-pressure core cooling and is part of the ECCS. The cooling fluid injected can be gravity-fed or pumped; and
- Passive moderator cooling: where heat is rejected to the passive moderator system through the specialized HEC channel.

The event tree is shown in Figure 4.3. The unavailability of the ADS is assumed to be in the order of 10^{-4} in this thesis, similar to the SLWR value [12]. The rationale for using this value is that its reliability should be comparable to that of other safety systems. Likewise, the reliability of the low pressure cooling injection system (LCI) is taken to be 10^{-3} based on existing active ECC systems. The failure probability for the MPS is derived from calculations in section 4.4. (Note that external moderator injection and boil-off can still be a potential heat sink in this case in the event that natural circulation is precluded – however this is not credited in this analysis). It is further assumed in this work that the long-term cooling system will be incorporated into the LCI as per the proposed ACR and ESBWR design. Other probabilities remain similar to CANDU; however it is expected that reliability improvements may be achieved in each stage within the SCWR design since it will incorporate lessons learned from previous failure information in GEN-II designs and OPEX. Such "technology" improvements in reliability are not modelled here.

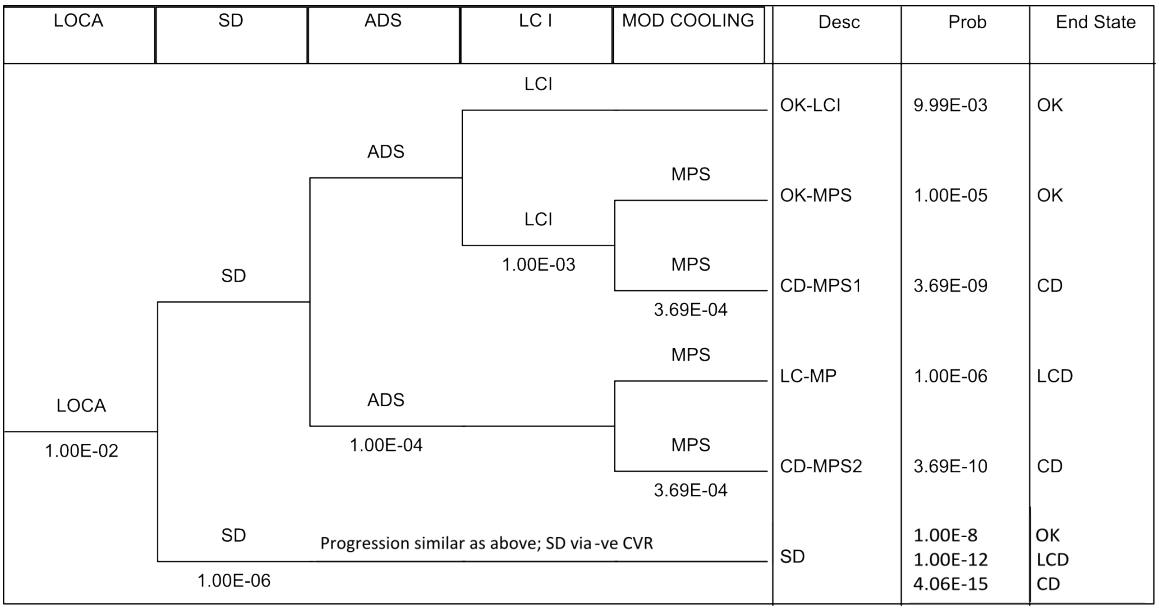


Figure 4.3: Event Tree of SBLOCA in SCWR

[1]

In Figs. 4.3 and 4.4, SD is a combination of the SCWR shutdown mechanisms. OK-LCI implies that the core gets continuous long-term cooling due to LCI. However, if LCI fails and the MPS is functioning, the core can still be kept cool (OK-MPS). The situation in which ADS fails yet the MPS works is estimated to lead to LCD due to the delay in cooling which will result (LC-MP). Core damage would ensue with the failure of MPS when either LCI and ADS fail (CD-MPS1, CD-MPS2). A sensitivity study similar to that discussed in Section 4.1.1 was also performed. The CDF was most sensitive to the ADS value, followed by that of the MPS, and then the low pressure ECC. Furthermore, as seen from the results in Table 4.1, the overall CDF is significantly improved in the SCWR.

OUTCOME	CANDU	SCWR
Cool core	9.99E-03	1.00E-02
Limited Core Damage	1.99E-05	1.00E-06
CD	1.02E-07	4.06E-09

Table 4.1: Probability of failures from Loss of Coolant accident

4.1.3 Large Break LOCA simplified behaviour in SCWR

A simplified key event sequence not examined above is large break LOCA (LBLOCA), and in fact for some SCWR designs such as the JSCWR, it is the dominant event leading to core damage [12]. For these other SCWR designs, a failure of ECC ultimately leads to core damage, while in the pressure tube-SCWR, a new passive heat removal system has been added. Hence we examine the event sequence for LBLOCA to demonstrate the potential robustness of the SCWR given the passive moderator heat removal system. The LBLOCA can be defined as a break in a large diameter piping (>10cm) of the primary HTS [51], such as would occur in the RIH or ROH. The failure probability of this event in a CANDU is in the range of 10^{-4} [51]. That same frequency is being assumed for this analysis.

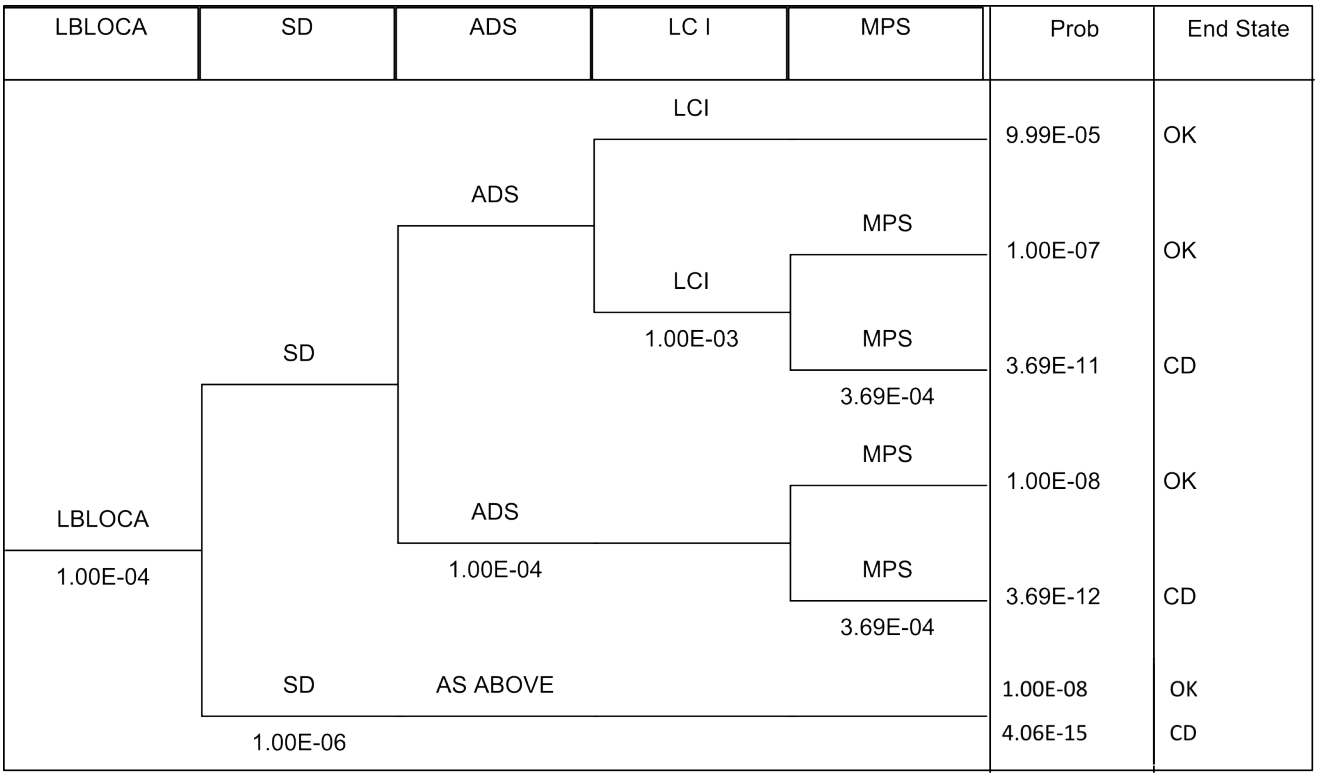


Figure 4.4: Simplified LBLOCA sequence in SCWR

In this figure, SD is the combined action of either SDS1, SDS2, and negative CVR to shutdown the core and control system which is not credited. ADS is needed here to maintain forward flow in the core and to ensure blowdown cooling until the LCI system can be effective. In the event that ADS fails, the last line of defence is the passive MPS for continued heat removal from the core. This differs from other GEN-III or GEN-IV designs (as seen in section 4.3.2) because having the MPS provides another level of defence-in-depth against a LOCA-LOECI sequence. The resultant CDF values for LBLOCA are much smaller than the SBLOCA case, and indeed much smaller than any other SCWR design [12]. Further discussions and comparisons of the LBLOCA event in SCWR and other GEN-IV reactors are contained in section

4.3.2.

4.2 Loss of Class-IV Power Accident

The Class-IV power system supplies all the large loads in the NPP e.g. motors for heat transport pumps, condensing cooling water, and other service water pumps. On-site standby diesel generators will supply Class-III loads in the event of a sustained loss of Class-IV power. The Shutdown Cooling System (SDCS) pumps, ECC pumps, boiler feedpumps, and heat transport feedpumps run on Class-III power. Critical station loads such as ECC may also be supplied by the Emergency Power System, which is physically separated from Class-IV and standby diesel generators. Loss of Class-IV power events can arise from several failure modes including load rejection or loss of offsite power coupled with loss of station-generated power. The event can also stem from a turbine or reactor trip and a failure of the transfer busses to switch to grid supplied power. A Loss of Class-IV power, a failure of the Class-III power supplies and failure of emergency power will lead to a station-blackout and subsequent loss of heat sink accident.

4.2.1 Loss of Class-IV Power Accident in CANDU™

AAssuming a turbine trip coincident with a total station disconnection is the considered in this Loss of Class-IV analysis. Fig. 4.5 is an event tree showing a possible sequence for the progression of this accident, for which the description is below:

1. On turbine trip, the reactor regulating system (whose failure rate is in the order of 10^{-2} [50]) initiates a stepback on detection of a load rejection, e.g. from

steam generator pressure or other means. If sustained, the reactor will shut down. *Events: Reactor Regulating System (RRS), Shutdown systems (SDS1/2)*

2. The heat transport pumps are run down, removing decay heat in the process. This takes 2-3 minutes and ensures a smooth transition to thermosyphoning which will last for some period of time (at least 15 minutes is demonstrated in the safety analysis) provided there is adequate steam generator inventory. By the end of this period of time, the diesel generators should start, supplying Class-III power. Hence, the Auxiliary Feedwater system will resupply the steam generator inventory and allow thermosyphoning to continue. In the event that thermosyphoning is not available, the system can be cooled and depressurized and SDCS (powered by SDG) can be brought into service. *Event: Standby Generators (SDG)*

3. If the diesel generators fail, the Emergency Power System (EPS) will be started. The EPS provides a seismically qualified source of electrical power to the systems important to safety if the normal power supplies are lost [24], [23]. The EPS would start automatically if both the Class- III and -IV supplies are lost. EPS supplies power to the emergency feedwater system (EWS) and when running, the EWS will ensure the secondary side of the steam generators stays full and thermosyphoning continues. Other heat sinks such as ECC are also available with Emergency Power.

4. If the EPS does not start then a station blackout situation will initiate. During this period, staff will attempt to restore power (from all available sources) as well as initiate emergency measures to supply moderator make-up in the event

the moderator may be needed as a heat sink. If power is not restored in a timely manner, then pressure tube-calandria tube contact will occur and the heat sink will become the moderator. If external pumps or power can be supplied for moderator make-up, it may act as the ultimate heat sink. If power is restored within 8 hours, it is assumed that no further damage to the core will occur. Another event is included for restoring power in half an hour, similar to the JSCWR PSA analysis. If power is restored in half an hour, this will prevent fuel channel deformation and terminate the event with no core damage. The probability for power restoration is taken to be same as in the JSCWR [12]. *Event: 8h PWR RESTRD, 0.5h PWR RESTRD, EWS*

5. Following a turbine trip, the condenser steam discharge valves would open and allow the steam to be discharged to the condenser. However, with the Loss of Class-IV power, the condenser pumps will not be available so condenser heat sink is lost. Therefore, the pneumatic atmospheric steam discharge valves (ASDVs) would open. However, the pressure in the system might be too large to be handled by the ASDVs alone [51] leading to the MSSVs opening on top of the steam generators. To avoid over-pressurization of the HTS, the liquid relief valves (LRV's) may open periodically during the transient to limit pressure rise in the main circuit. Failure of the LRVs to open would initiate a LOCA sequence due to overpressure damage. For the sake of simplification, this branch is not shown on the event tree.

6. If the standby diesel generators start, thermosyphoning and/or the SDCS can be used to cool the core coupled with heat sinks either in the steam generators (with auxiliary feedwater supply) or through the use of SDCS. *Event: FW2,*

AFW

7. With normal cooling of the core established, the LRVs can now close. If the LRV's fail to close, the coolant inventory will continue going to the Bleed Condenser System (BCS) and to the D_2O storage tank. The bleed condenser can be isolated so that HTS inventory is not lost to D_2O tank. Failure to isolate the BCS will cause an event similar to a small loss of primary coolant. This event is not mapped on the event tree however, for simplification. Other sub-events related to BCS and LRV actions and potential loss of coolants are not modelled in this work.

8. If the LRV and BCS fail to isolate the HTS, ECC needs to be initiated similar to a LOCA sequence. That means using Low Pressure Injection (LPI) to cool the core.

9. In the unlikely event that the Main Steam Safety Valves (MSSV's) fail, other safety relief valves such as the ASDV will discharge steam from the secondary side of steam generators. Alternatively, switching to SDCS or using the ECC heat exchangers is also an option. *Event: SDC/ECC.*

10. The Moderator Circulation System (MCS) may act as a heat sink if all other heat sinks have failed, i.e. SDG and EPS are not working and steam generator levels have boiled off. In this event, pressure tubes either sag or balloon into contact with the calandria tubes and heat is conducted to the moderator. Some pressure tube and fuel overheating may occur during this event. The moderator heat sink can accommodate at least 8hrs of heat load, after which inventory replacement is needed. Without external intervention (i.e. water supply or

power restoration), it is assumed core damage occurs after 8hrs. *Event: MCS*

The simplified accident sequence can be represented in the event tree shown in Fig. 4.5.

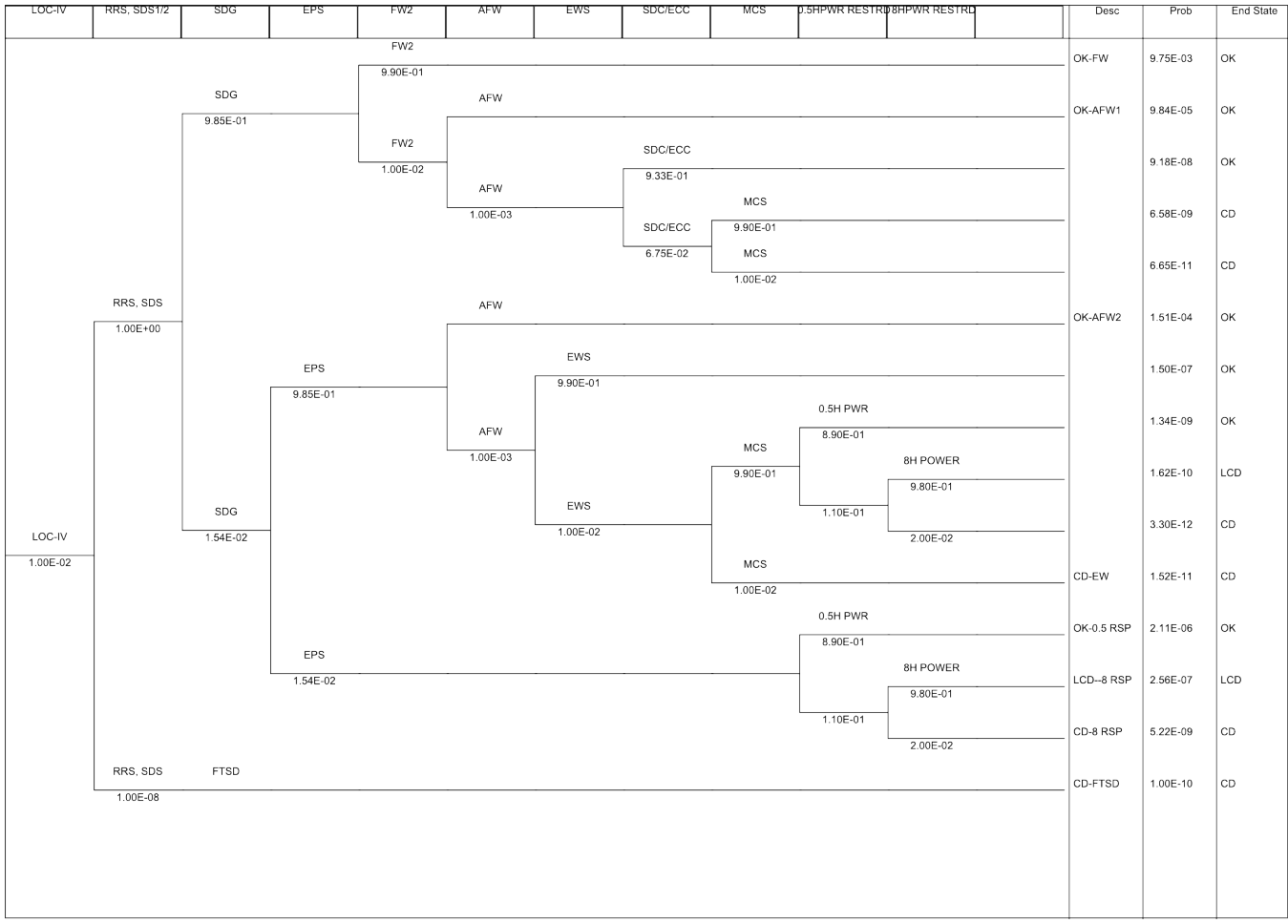


Figure 4.5: Event Tree of Loss of Class-IV Accident in CANDU™

As described in the previous chapter, the values used in the analysis came from various sources. The probability of power being restored was taken from NUREG-1784 [53] which gives the failure to restore power in 4 hours as $2.0\text{x}10^{-2}$. The same value was assumed for restoring power in 8 hours. For the equipment which would

have run failures, their probability of failure was calculated using eqn. 3.4 since the failure rates are usually given in the databases by the daily or hourly rate [44], [45], [46]. Another assumption made in the calculations is that the reactor was shut down for 28 days every 2 years, therefore a capacity factor of 0.96 was applied as an adjustment on the failure rate of each component taken from Ref. [46].

Using the descriptions in Fig. 4.5, OK-FW leads to an end state of a cool core. The event trees presented are simplified event trees of the sequence of the initiating events as they do not show a lot of the subsystems that would come into play in mitigating these events. For example if the standby diesel generators are available and the feedwater is available, the risk of core damage is very low due to multiple and redundant heat sink pathways being available. Therefore the event is truncated at this point.

OK-AFW1 and OK-AFW2 are similar to OK-FW. It is assumed that long-term heat sinks such as the SDC or the ECC's heat exchangers will be used to keep the core cool, or thermosyphoning continues. (Note that the combined reliability of the SDCS and the ECC is used on this branch – 6.65E-02 and 1.0E-3 respectively.) Failing these long-term systems, the decay heat will be rejected to the MCS after some pressure tube deformation and pressure tube-calandria tube contact.

If there is no emergency water supply, a loss of heat sink will occur leading to pressure tube deformation and heat rejection to the moderator through pressure tube-calandria tube contact. If moderator make-up is available, then boiling in the moderator will be an effective heat sink. With no make-up to the moderator, eventually boil-off will occur and core damage will initiate. The CD-EW reflects this pathway to damage.

If any power supply is restored within half an hour during the event progression, the main HTS pumps and heat exchanger, the SDCS or thermosyphoning will be available as heat sinks. That is the pathway represented by OK-0.5 RSP. But if all the backup power supplies fail, by the time power is restored in 8hrs, there will be limited core damage (LCD-8 RSP). If the reactor power is not restored in a timely manner following the station backup power supplies failing, moderator make-up will be needed to prevent core damage. Without make-up, core damage will ensue (CD-8 RSP). The final pathway leading to potential CD is if the reactor fails to shut down (CD-FTSD).

4.2.2 Loss of Class-IV Power Accident in SCWR

The progression of a loss of Class-IV power occurring in SCWR will deviate from the generic CANDU™sequence due to the direct thermodynamic cycle of the system. Upon turbine trip and loss of Class-IV power, the shutdown systems will need to activate. The ADS valves can be opened to depressurize the reactor system and initiate cooling. However, there is also the option to keep the reactor at pressure, after shut down, and have the decay heat removed until power is restored. This will be similar to the CANDU where decay heat can be removed via thermosyphoning using the steam generators. The ICS can passively remove decay heat when the normal heat removal systems are unavailable in the ESBWR [29], and this analysis assumes it will exist in the SCWR. On the loss of power, the heat exchanger tubes in the IC pool drain cold water to the core. Then, as the tubes empty, steam from the reactor is drawn in to the IC pool and is condensed. Thus, heat is transferred to the IC pool and the core is kept cool from the condensing water. (The heat in the IC pool is

transferred to the atmosphere outside of containment.) This passive system can keep the reactor cool for 3 days.

If the ICS fails or power is not restored within the 3 days, the ADS system could valve in and allow blowdown cooling. Thus the initial blowdown cooling is passive after the valve actuation of the ADS. After a period of time the pressure in the HTS will have decreased sufficiently, as well as an appreciable decrease in decay heat, to allow the LCI to initiate; it will circulate fluid from the suppression pool to the core. In the long term, liquid in the suppression pool will be cooled using a passive heat exchanger system to the environment. In the event of a failure of ADS and/or ECI and/or low power cooling systems modes, the heat sink may be maintained by the purely passive moderator system operating in its natural circulation mode. It is assumed that there will be a tank of water with a capacity to supply the MPS. If not, then moderator make-up supply of water (which has a high reliability) will be brought on to maintain core cooling via the MPS. Although it is not credited here, it should be noted that if the MPS stops functioning due to insufficient cooling water supply, there is still the opportunity to boil off the moderator and replenish the liquid as in the existing CANDUs. Fig. 4.6 is the event tree showing the sequence of loss of Class-IV power in a SCWR.

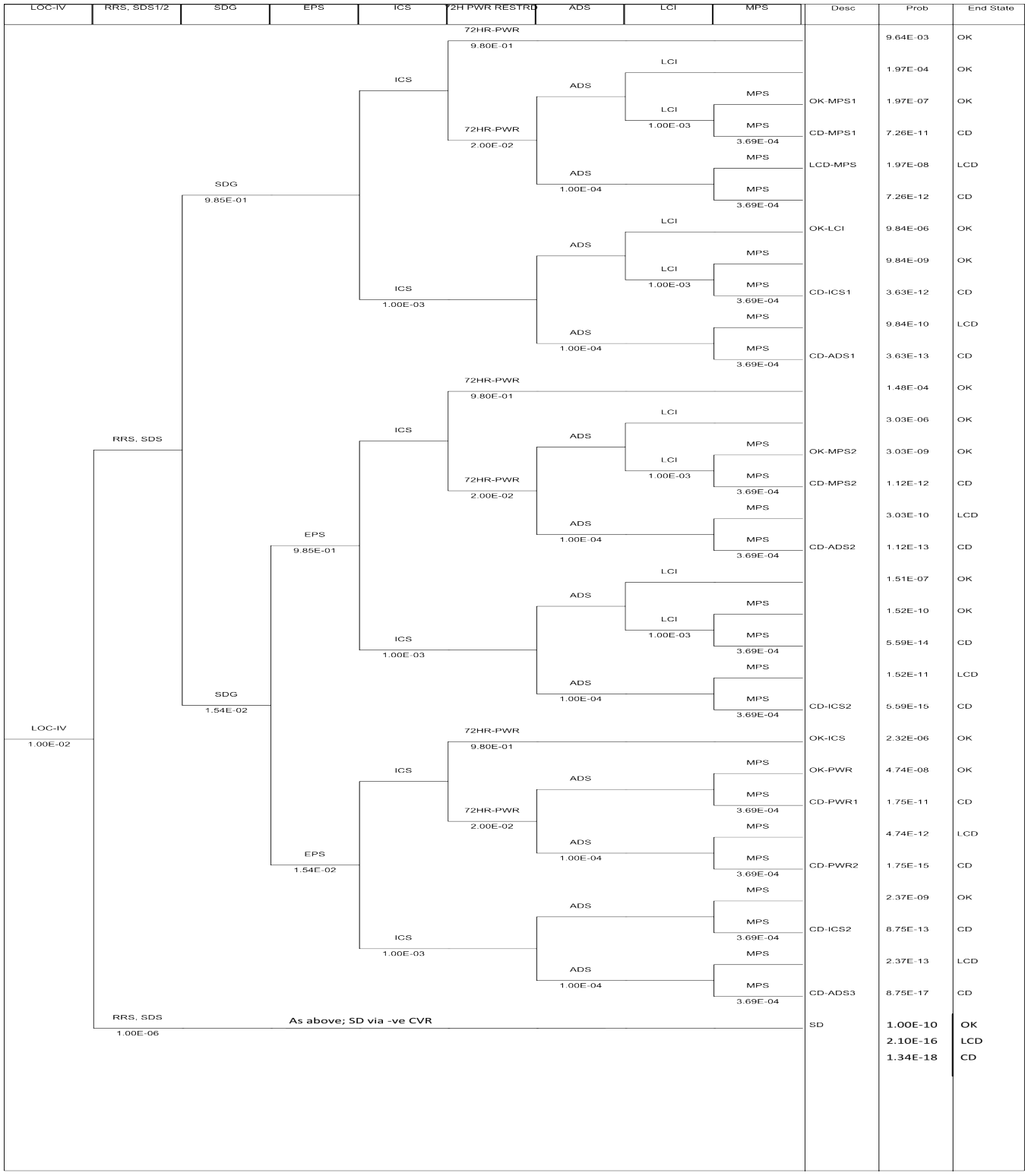


Figure 4.6: Event Tree of Loss of Class-IV Accident in SCWR

The Loss of Class-IV event is another incident that demonstrates the passive moderator cooling system's contribution to safety in the SCWR. If the standby diesel generators are running and ADS is initiated yet LCI fails to come on for long term cooling, the heat can be rejected to the moderator and the core will still be kept cool – OK-MPS1. As in the CANDU's Loss of Class-IV power event, terminating the event at 'OK' could mean that a further system for long-term cooling is initiated.

After the system is depressurized by ADS because power has not been restored within 72 hours, if the long-term cooling systems do not function, the MPS can also keep the core cool (OK-MPS2 or OK-MPS1). However, if the MPS fails at that point, the end state would be CD – CD-MPS1 or CD-MPS2. When the ICS fails and the system is depressurized, the LCI maintains the long-term cooling (OK-LCI). If the LCI fails at this point yet the MPS functions, the core can be kept cool. If the MPS fails, the end state will be core damage (CD-ICS1). When ADS does not depressurize the system, it will be over-pressurized and the high pressure could cause a pipe burst or other HTS breach. The MPS is still available to limit CD and remove heat, however some CD is assumed. Thus the end result of this overpressure scenario is LCD, as in LCD-MPS. It is recognized that the system depressurization following say a pipe rupture due to ADS failure could eventually allow LCI to be activated, and therefore the end state may not be LCD or CD. However, making conservative judgments, the outcome of this event is set at LCD. If the MPS fails following the ADS failure, CD ensues (CD-ADS1, CD-ADS2). If EPS works but the ICS and ADS do not, the reactor will remain at high system pressure. Limited core damage will occur if the MPS works, however core damage will result if the MPS does not function – CD-ICS2.

The proposed ICS is a passive system and so even if there is total station blackout, the core will be kept cool for the three days in which decay heat can be rejected to the ICS pool. If power is restored within the three days, no damage to the core results (OK-ICS). However, if power is not restored in the three days, the reactor is depressurized by the ADS and the core can be kept cool via the MPS (OK-PWR). Failure of the MPS at this juncture will lead to core damage (CD-PWR1).

Additional pathways for core damage from the loss of Class-IV power event are if the ADS and MPS fail when there is a complete station blackout (CD-PWR2), or if all backup power supply fails and the ADS and MPS fail (CD-ADS3), or if after the station backup power supplies fail and ICS fails, the MPS does not function though the ADS works (CD-ICS2). The core would also experience core damage if there is no water make-up to the moderator following the failure of the backup power supplies although this is not included in this model. Table 4.2 compares the outcomes of this accident occurring in a CANDU to that in the pressure tube-SCWR.

OUTCOME	CANDU	SCWR
Cool core	1.00E-02	1.00E-02
Limited Core Damage	2.56E-07	2.10E-08
CD	1.20E-08	1.34E-10

Table 4.2: Probability of failures from Loss of Class-IV power accident

One of the differences between the CANDU's and SCWR's Loss of Class-IV accident progressions is the CANDU core can be kept cool by means of thermosyphoning when continuous feedwater flow to the steam generator is established while the SCWR

requires the injection of cooling water to maintain a cool core. Furthermore, the outcomes for both accidents are different when the moderator is the backup heat sink: in CANDU, pressure tube damage ensues and some sheath damage may occur as well.

4.3 Comparison of results with other supercritical reactors

An attempt was made to compare the results to those obtained on the Japanese SLWR. The Loss of Class-IV accident in a SLWR was analysed in Ref. [12] using PSA tools; however the values of the failure rates of the safety systems are somewhat different from those used in this study. The authors' reasoning behind these values could not be determined because the sources of the data for their analysis were from papers that were in Japanese. Therefore, the only comparisons done here are of values of the reactors' reliability in withstanding CD following the accidents.

4.3.1 Small Break LOCA in SLWR

There is not much difference between the sequence of events and the outcomes of a SBLOCA in the SCWR and the SLWR. The reactor is shut down by the RPS on the LOCA signal, and negative reactivity is inserted for final shutdown. Therefore, the reactor is depressurized and the SLCS is activated to maintain the reactor in a shutdown state. Alternatively, the core can be depressurized by the ADS and cooled by the LPCI [12]. The last line of defence in the LOCA is the residual heat removal (RHR) system which has a failure probability of 4.44E-04.

The major differences between the SCWR and the response of the SLWR are:

1. The SLWR shuts down with the RPS (equivalent to the SCWR's SDS1), but rather than have a second shutdown system like SDS2, the reactor uses the standby liquid control system (SLCS). This system is a backup for shutdown. It injects borated liquid (from a tank) at high pressure into the system and so is like a combination of SDS2 and a high pressure ECI. The unavailability of this system is given as 2.7E-01 [12].

2. There is no passive moderator heat removal system as a last line of defence. The RHR is relied upon in order to avoid core damage, but it is an active system whereas the MPS is a passive system. Although the reliability of both systems is similar (both have unavailabilities on the order of 10^{-4}), the calculations for the MPS reliability might be conservative.

The final value for the core damage frequency from a small LOCA is 3.4E-8/yr [12], which is about an order of magnitude higher than the SCWR rate for a LOCA. The similar CDF value is to be expected given the similar systems used to arrest the event in both reactors.

4.3.2 Large Break LOCA in SLWR

When a LBLOCA occurs in the SLWR, the reactor depressurizes by the ADS. Then, negative reactivity is inserted through the RPS. In the long term, LPCI ensures continue core cooling. Of great importance in the SLWR is the location of the break and the size of the break. In this reactor design, the large upper plenum contains most of the coolant inventory. If there is a large break on the inlet side, coolant flow may either continue in the forward direction or it could reverse; it depends on the break size. For large breaks, there is a chance that the flow will reverse. Or,

also depending on the break size, there could be equal flow from the plenum which perfectly balances the pressure in the core. In that case, there will be no coolant flow to the core and a situation of flow stagnation arises.

Under flow stagnation conditions, it will be difficult to inject any coolant to the core. Perhaps it might not even be possible to inject the low pressure ECI. Therefore, ADS is required (in the LBLOCA of an SLWR) to create a vent on the downstream side so that flow can continue. Having the ADS action in a LOCA situation guarantees that stagnation flows do not occur and cooling can therefore continue in the core. Therefore, in the SLWR sequence for a LBLOCA, failure of the ADS leads to immediate core damage as reflected in the sequence in the event tree of Fig. 4.7. The ADS is the only mitigating system for a LBLOCA, unlike the SCWR which can rely on the passive moderator cooling if the ADS fails completely. Hence, it is expected that the SCWR design will show significant improvement in safety when assessing the LBLOCA pathway. The CDF due to LBLOCA in the SLWR is given as $2.3\text{x}10^{-7}$/yr [12] while the SCWR has a CDF that is about $4\text{x}10^{-11}$/yr.

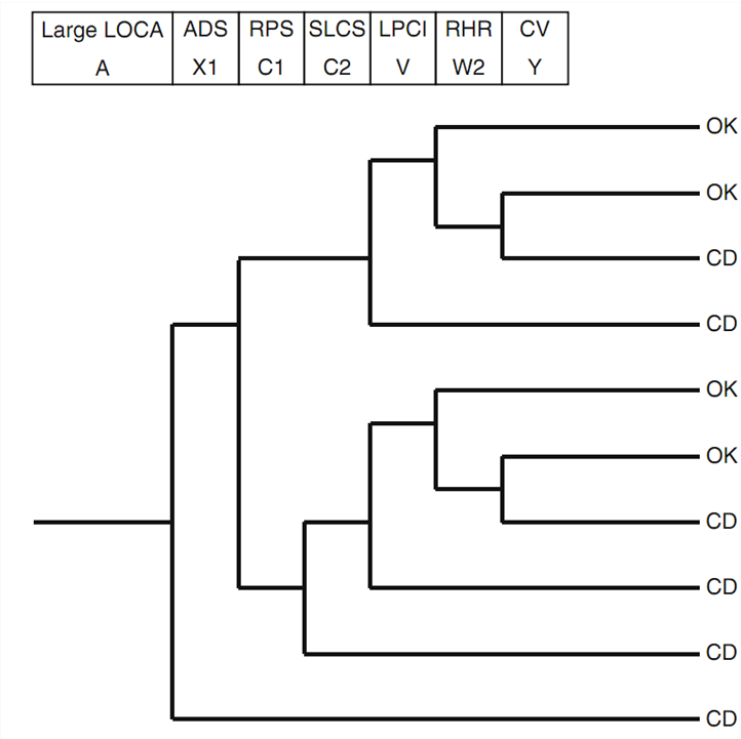


Figure 4.7: Event tree of LBLOCA in SLWR [12]

4.3.3 Loss of Offsite Power in SLWR

The sequence for the loss of Class-IV power in the Super Light Water Reactor is shown in the event tree in Fig. 4.8 below. (The list of system unavailabilities used in their failure analysis is given in Table B.1 while Table B.2 gives a brief description of some of the acronyms used in the Event Tree.) At the loss of power, the turbine trips and hence the turbine-driven reactor control pumps are not available. If the RPS operates successfully, it is possible to maintain core cooling at supercritical pressure using the auxiliary feedwater system. For longer term cooling, the LPCI will be used. However, if after 8 hours neither emergency nor offsite power is restored, core damage will ensue because the decay heat cannot be removed by the LPCI alone when the

auxiliary feedwater system (AFS) is no longer available [12]. But if the emergency diesel generators are available, long term cooling can continue via the LPCI. If the AFS fails, the reactor can depressurize via the ADS and then core cooling by the LPCI can start. Similarly, if the RPS fails, the AFS can still initialize but the system will be depressurized by the ADS and the core kept cool by the LPCI or RHRS, instead of attempting to avoid core damage without depressurization, as is the case when the RPS operates. If both the RPS and AFS fail, the reactor must be immediately depressurized by the ADS [12], and core damage can be avoided by having the SLCS and LPCI systems maintaining core cooling. Some scenarios where core damage could occur in the SLWR following the Loss of Class-IV power include i) if RPS and AFS were successful but no long-term cooling system was available, or ii) if AFS was not available and neither the diesel generators nor offsite power was restored in 8 hours, or iii) if ADS failed, or iv) if RPS, AFS and ADS all failed.

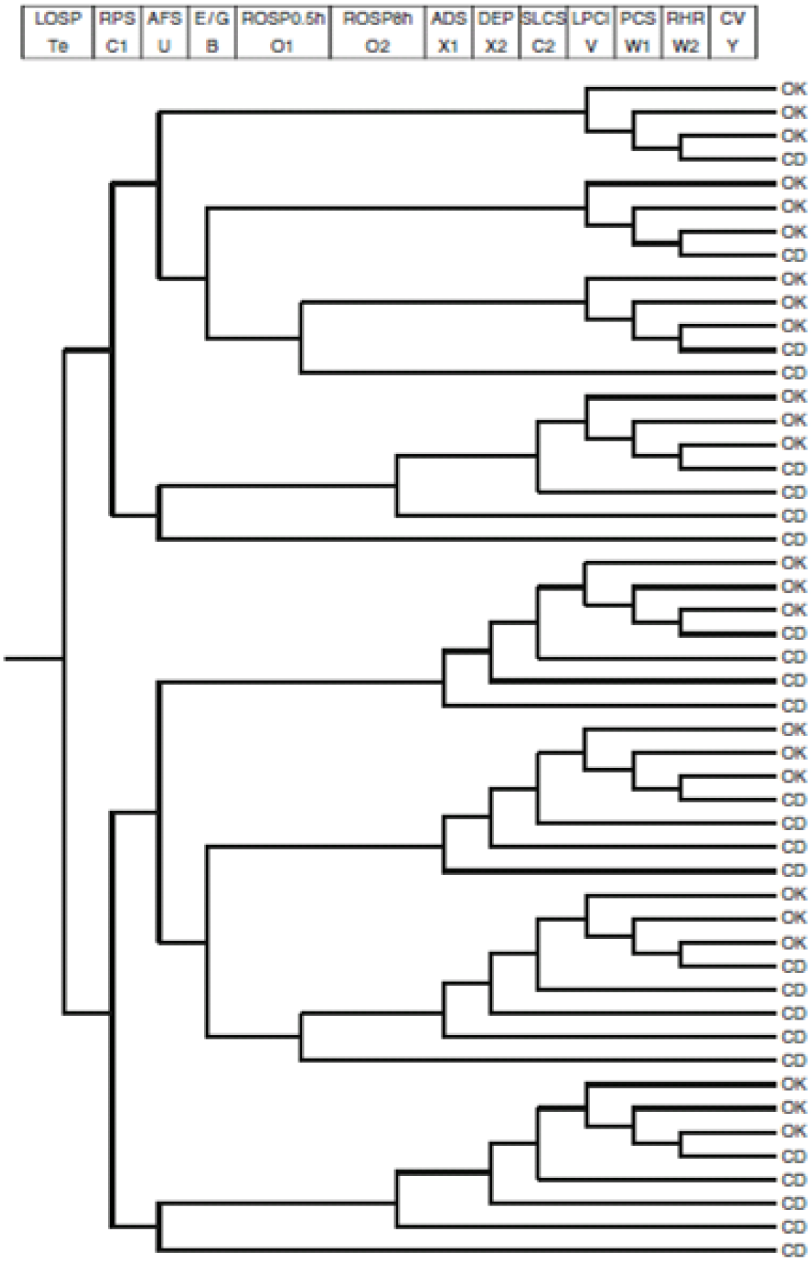


Figure 4.8: Loss of Class-IV power event in Super Light Water Reactor [12]

The core damage frequency for a loss of station power was estimated as 7.5E-8/yr [12]. It should be noted that for the JSCWR analysis, the transients are assumed to be

followed by turbine-driven reactor coolant pumps also tripping. Hence core damage is mainly due to failures of the systems that are tasked with supplying coolant to the core. Also, in comparing the JSCWR to the pressure-tube SCWR, it can be seen that the JSCWR accident sequences terminate at the failure of the ADS, and the consequence is core damage. However, in the pressure-tube SCWR, there is another option following the failure of the ADS or loss of all heat sinks and that is the passive moderator cooling system. Therefore, event pathways that would normally lead to core damage now have a safe end state with the core remaining cool.

There were no comparisons made between the responses of the HPLWR with the SCWR because although safety analysis work has been done on the HPLWR for such DBA's, no probabilistic analysis of these accidents was found in the literature.

4.4 Fault Trees for safety systems

For systems comprising various components without generic failure rates, the system's overall failure rate was derived from the fault trees constructed. For instance, the failure rate of the SCWR's MPS was calculated from the fault tree in Fig. 4.9, giving 3.69E-04/yr.

1. Moderator System: Based on the operation of the SCWR's passive moderator cooling system, the fault tree for this system failing is illustrated in Fig. 4.9. The main causes for the MPS to fail are assumed to be moderator leakage, lack of cooling water to the heat exchangers, or calandria leakage. Fig. 4.9 expands on these failures, illustrating the root causes of some of the main causes for the MPS failure. Further sources of these failures include pipe and tank breaks or

unavailability of cooling water. None of these causes are from active systems or components.

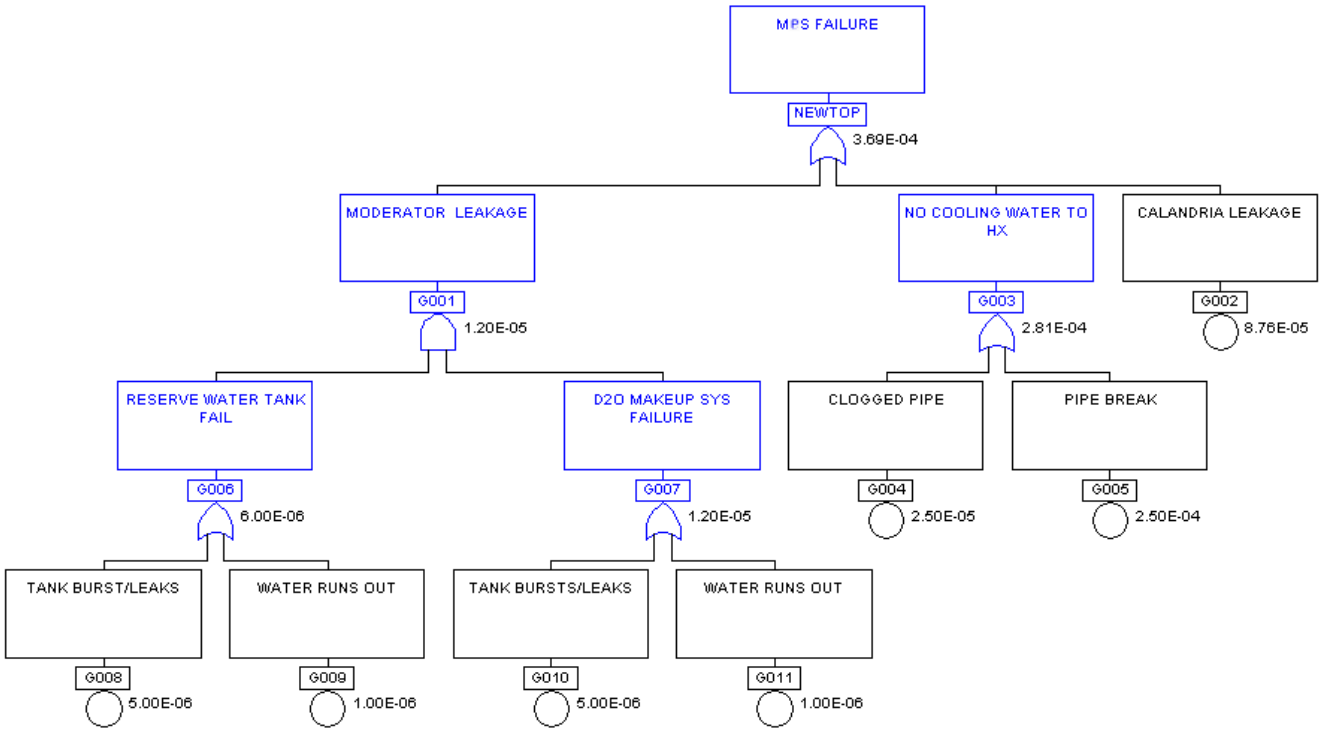


Figure 4.9: Fault Tree for SCWR Moderator Cooling System

2. Shutdown Cooling System: The Shutdown Cooling System (SDCS) is a system for long-term decay heat removal. It is able to remove 100% maximum core decay heat, being a shutdown pathway after a reactor trip [52]. The SDCS must be started manually, however. The SDCS can cool the HTS from full system pressure and temperature and maintain the system at a low temperature indefinitely [52]. The SDCS has two 50% pumps, two 50% heat exchangers, and the associated valves and pipes. The flow diagram of the SDCS is shown in Fig. 4.10. The failure probability of the SDCS was estimated as 6.65×10^{-2}

from the fault tree in Fig.4.11.

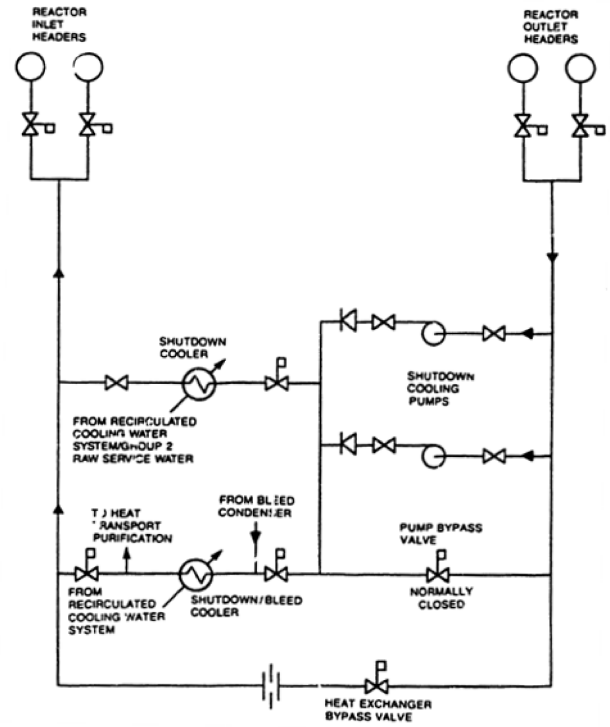


Figure 4.10: Shutdown Cooling System flow diagram

Drawing from the flow diagram, some of the main sources of the SDC failure could be lack of cooling water, operator failing to initiate the system, or the pump bypass valve left open. It is observed that several root causes of the SDC's failure are active components failing, such as pumps and valve failure. It can also be observed from the fault tree in Fig. 4.11 that the pumps and the heat exchangers are the least reliable components of the SDCS. Operator action is included as a root cause in the analysis since this system is initiated manually.

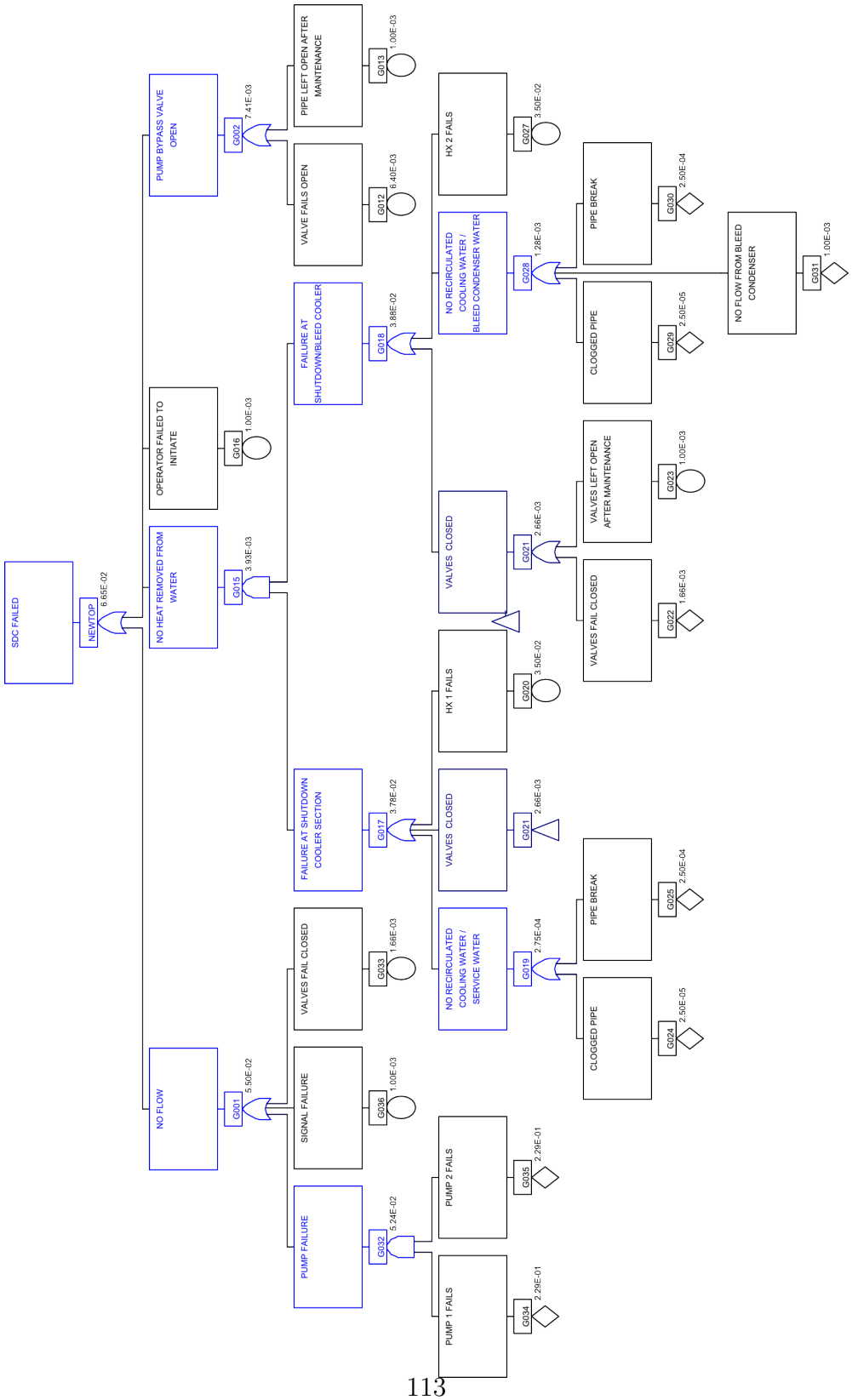


Figure 4.11: Fault Tree of Shutdown Cooling System

Chapter 5

Summary and discussion

This chapter will highlight some of the conclusions made from the risk analysis on the CANDU and SCWR, and then give a summary the entire study. Extensions of the thesis are also proposed

5.1 Conclusion

A preliminary risk assessment of the SCWR was performed, comparing the outcome of loss of coolant and loss of Class-IV power accidents in the traditional CANDU to that in the next-generation pressure tube-SCWR. The tool used for the analysis was Probabilistic Risk Assessment (PRA) using CAFTA. This tool allows one to assess the sensitivity of the system to certain design or performance assumptions in order to determine which components have more of an impact on the overall system's reliability.

The preliminary analysis proved that, compared to the CANDU, the SCWR does have fewer avenues to core damage from these accidents, in large part because decay

heat can be rejected to the moderator without significant structural deformation. An inherent assumption made in this risk assessment is that for the MPS to work, the HEC integrity is maintained and that margins within the fuel channel are not exceeded during accidents. Overall, the moderator system and ICS being passive leads to a higher reactor reliability. However, subsequent work should address the common-cause potential failure of the HEC and MPS since a failure in one channel will compromise the MPS.

In order to ensure the risk-based design criteria were met in the SCWR (e.g. the safety goal of CDF being below 10^{-5}/yr), an Isolation Condenser System was proposed as a system to be included in the SCWR design. It was necessary to include the Isolation Condenser System as a backup heat sink because the analysis proved that in its absence, the SCWR had a higher probability of core damage than the CANDU. [1] The Isolation Condenser System will be a source of passive decay heat removal thus providing another layer of protection to the reactor core during a station blackout. Alternatively, a High Pressure Injection System can be incorporated into the design so as to stay within acceptable accident limits.

A LBLOCA accident was examined to compare the response of Canada's SCWR to a GEN-IV design developed elsewhere. A significant conclusion drawn from the pressure vessel-based designs is that they are almost solely reliant on the ADS availability for LBLOCA. This is why such vessel designs have CDF dominated by the LBLOCA pathway, not the SBLOCA nor LOSP event: the design relies on a single

[1] Initiating event frequencies are the same between the CANDU and the SCWR for these events because we made the decision to freeze them to allow direct comparison. However, it is expected that there would be different initiating frequencies due to the simplification in design as well as the higher pressures and temperatures in the SCWR.

system to mitigate the LBLOCA accident. The pressure tube-SCWR has two independent systems (i.e. ADS and ECC, backed up by passive moderator heat rejection) to mitigate this accident, and therefore the failure frequency is reduced by at least two orders of magnitude.

While these CDF and relative improvement indicate a potential large reduction in risk, the following assumptions should be noted:

1. External events and operator failures are not included

2. Simplifications have been made in the event tree

3. While the reliability has been assigned to each system, no safety analysis has yet been performed to demonstrate that these systems meet their design criteria. For example

- Since ADS is used for blowdown cooling for LOCA followed by LCI, there is no analysis to assess fuel and sheath integrity for these transients. Hence, a HPCI system may eventually be required.

- The MPS system has not been fully analysed to determine that it can remove decay heat and keep fuel sheath temperatures within acceptable limits. Further, the ultimate heat sink for MPS has not been determined.

- The potential for common mode failure between the MPS and the fuel channel was not included in the analysis. In particular, if the HEC overheats, or the insulator fails as a result of an accident or as a result of high temperatures or creep-induced stresses, then there is a potential that MPS may fail entirely.

5.2 Event trees, Fault trees, and Sensitivity Results

The event tree models showed that following a LOCA, the Limited CD and CD frequency is 1.00E-06/yr while for the CANDU it is 1.99E-05/yr. In a Loss of Class-IV accident, the probability of limited or core damage was 2.11E-08/yr for the SCWR and 2.68E-07/yr in a CANDU. These results are significant given the SCWR will not have a steam generator as a backup heat sink in accidents.

The fault tree analysis of the SDCS demonstrated that the pump and heat exchanger were the components most likely to fail, having failure probabilities in the order of 10^{-2} as opposed to most other components that were two or three orders of magnitude less likely to fail. A limitation of the work was the lack of plant-specific data used in the calculations – both for the CANDU and the SCWR. LWR failure probabilities were hence substituted when required.

An extremely low value of likelihood of occurrence does not mean that an accident cannot occur; therefore further research should be conducted to test the SCWR's behaviour under additional abnormal conditions. The analyses will be more complete and give more accurate results when the input data reflects the plant's operation. Future work will incorporate such data into the analysis in order to generate more credible results.

A sensitivity study was conducted on the contributors to CDF for the SBLOCA accident in the two reactors. It demonstrated that the largest sensitivity is to the availability of the ECC system in the CANDU, followed by that of the MCS. For the SCWR, the largest sensitivity was from the ADS's reliability, followed by the MPS's,

and then the LCI's.

5.3 Discussions

Each GEN-IV reactor is to achieve certain criteria, namely improvements in sustainability, safety and reliability, economics, and proliferation resistance. The SCWR is being planned to meet these criteria: it will meet the sustainability and non-proliferation goals by using more advanced fuel cycles, reducing waste, and having advanced storage [5]. This will enable the reactor to reduce the stewardship burden of future generations and not be attractive for diversion of its fuel for weapons. The financial metric will be met by the increased thermal efficiency (almost 50%) as well as by decreased capital and operation & maintenance cost – realized by the simplified design, elimination of certain components, and replacing the more expensive heavy water coolant with light water. The reactor will fulfil the improved safety and reliability requirements by having enhanced safety features that will significantly reduce the possibility for core melt.

Many design changes will be made to the SCWR before the system goes into operation. However, that does not invalidate the results of this thesis' risk and reliability assessment. Such analysis as conducted in this thesis assist in providing feedback regarding vulnerabilities identified in the design model. For example, at one stage it was proposed that the passive MPS may replace all need for LPI or HPI, but risk results do not support this simplification. Also, until recently, the RHR or ICS was not factored into the pressure tube SCWR design. However, the results from this PSA for station blackout indicate the system will be required to demonstrate improved safety. The insights generated from the risk analysis will play a vital role in revising the

design, identifying redundancies and other safeguards necessary in order to make the plant more robust. Thus, the PRA has the potential to strengthen the plant before it is built. It is also cost-effective when used as a design tool. Ultimately, it will be the combination of regulatory dictates, operating experience, collective understanding of the thermalhydraulic and physical processes, and the accident risk and sequence that determines how the new reactor design will be analysed.

5.4 Future Work

This section presents some ideas for continuing this work to enhance the study on the safety and reliability of the SCWR's safety systems.

5.4.1 Human Reliability Analysis:

One of the factors that can enhance the safety and risk assessment of the plant is to account for operator action in arresting accidents. For instance a system that can be used for long-term cooling following a loss of Class-IV power incident is the Shutdown Cooling system. This is a manually operated system, although the goal of the system design is to avoid human actions. If the SCWR design includes a separate shutdown cooling system as the CANDU does, operator action should be credited in the analysis and Human Reliability Analysis (HRA) should be considered as part of the overall safety analysis. HRA will also be necessary for other comprehensive accident sequences in which operator action is required. Similar to the way in which systems were credited to either fail or succeed in the event trees created, the two outcomes HRA gives are the probability that a person will act correctly and perform

the required task or will fail at it (due to an error of commission or omission perhaps). There are various methods to characterize human error e.g.

- Errors in problem detection
- Errors in problem diagnosis
- Errors in execution
- Errors external or internal to the individual
- Limits to the memory or attention span and decision making [39]

The further study that incorporates HRA could look at some of these areas for better understanding of the causes of the human failure.

5.4.2 Safety Analysis to determine effectiveness of ECC, ADS, MPS, ICS, AND LCI:

Of prime importance to assure the improvement in CDF of the SCWR is to ensure the special safety systems and systems important to safety have a high reliability. The new safety systems not in the CANDU that will be found in the SCWR are the ADS, MPS, and ICS. The ADS and ICS have been tested for other LWRs and shown high reliability, though their successful integration into the SCWR design needs to be confirmed. However, the MPS is unique to the SCWR. This system will require further study to demonstrate it will achieve the availability values required to mitigate accidents when called upon. The LCI (part of the ECC system) will also play an important role in arresting accidents and maintaining long-term cooling of

the core. Therefore, future work should include rigorous component reliability testing of these systems to verify their effectiveness in reactor operations.

5.4.3 Dose Calculations:

Another important area to be considered is the calculation of the radiological hazard from the postulated accidents. For the non-critical group of the public that is expected to receive the greatest exposure, the average dose can be estimated using existing numerical relations. This will enable the designers to see how close the doses are to the regulatory limits. As has been discussed earlier, each class of accidents – AOO's, DBA's, and BDBA's – has a radiological dose limit. For instance an AOO and a DBA respectively have a dose limit of 0.5mSv and 20mSv [35]. The SCWR design should be assessed in detail to ensure it meets the dose limit set by the CNSC following such incidents by a large margin. While CDF improvements have been noted in this thesis, the drive for higher burn-up and enrichment would need to be considered in dose impacts. Perhaps there will be revisions made to the existing CNSC standards and regulations that will cater specifically to the SCWR and these might adjust the dose acceptance criteria for the new reactor.

5.4.4 Sensitivity and Uncertainty studies:

Sensitivity analysis allows one to determine which variables, models, or assumptions lead to the greatest change in the PRA results. Thereafter, proposals can be made to use alternative models or to modify the scope of the PRA in order to reduce the uncertainty in these most sensitive elements. Although this thesis and ref. [56] had a simple sensitivity analysis included, further component level reliability testing

should be done to determine the effect on the plant's overall reliability when certain components of systems are replaced or enhanced. Furthermore, uncertainty analysis of the PRA should be carried out as it will give a numeric value of the uncertainties (perhaps originating from the model chosen, the parameters, or the incompleteness of the model) in the risk calculations. This will assist the designers in deciding if further testing and research is needed to reduce the uncertainties. Another outcome could be that the regulatory oversight is increased [55].

5.4.5 Multiple failure analysis and external events:

An idea that arose before converting my degree to a Master's might be interesting for future research: to determine if one failure in an SCWR would affect another component, and the cascading effect this causes, either arising from internal events (potential cascade of failures from burst pressure tube) or from external events (DBE or BDBE). The question is in the spirit of the CNSC's R-8 regulation that stipulates the failure of a system should not reduce the effectiveness of the shutdown system. An idea would be to determine how/if a failing pressure tube would affect other systems important to safety. Ideally, one component's failure should not propagate to other components and cause further damage. But if the pressure tube fails, would the energy of the failed tube actually fail others in its vicinity? Or would there be an explosion in the calandria?

5.5 Contributions to knowledge

Refereed Conference Proceedings

Ituen, I. and Novog, D.R., Risk assessments and regulatory Concerns for Canada's GEN-IV reactors, *2nd Canada-China Joint Workshop on Supercritical Water-Cooled Reactors*, Toronto, Canada, 2010.

Ituen, I. and Novog, D.R., Analysing Supercritical Water Reactor's (SCWR'S) Special safety systems using probabilistic tools, *5th International Symposium on Supercritical-Water-Cooled Reactors* (ISSCWR-5), Vancouver, Canada, 2011.

Ituen, I. and Novog, D.R., Assessing the applicability of Canadian regulations to the Supercritical Water Reactor, *5th International Symposium on Supercritical-Water-Cooled Reactors* (ISSCWR-5), Vancouver, Canada, 2011.

Malik, M.M., Ituen, I., Luxat, J.C., and Novog, D.R., Fault Tree Analysis and FMEA of High Efficiency Channel in a CANDU-SCWR, *American Nuclear Society 2011 Annual Meeting*, Hollywood, U.S.A., 2011

Non-Refereed Conference Proceedings & Presentations

Ituen, I., Probabilistic Risk and Safety Assessments in Supercritical Water Reactors, *34th Canadian Nuclear Society / Canadian Nuclear Association Student Conference (Poster Presentation and Paper)*, Montreal, Canada, 2010.

K. Heckman, I. Ituen, F. Bao, J. Spencer, B. Statham, P. Szymanski, and D. Novog, Thermal-hydraulic Analysis and Experiments Improving Operating Margins, *CANDU Owners Group (Poster Presentation)*, Ottawa, Canada, 2010

K. Heckman, M. Ball, M. Chatharaju, I. Ituen, K. Leung, M. McDonald, A. Morreale and D. Novog, Benchmarking, Uncertainty Analysis, Fuel Recycling and the Super-critical Water Reactor, *CANDU Owners Group (Poster Presentation)*, Ottawa,

Canada, 2010

Ituen, I. and Novog, D.R., Risk assessment of Canada's next generation nuclear reactors using probabilistic tools, *Current Research in Engineering, Science, & Technology (CREST) Meeting (Presentation)*, Hamilton, Canada, 2011.

Malik, M.M., Ituen, I., Luxat, J.C., and Novog, D.R., Analysis of Fuel Channel Design in the CANDU SCWR, *Ontario Research Fund for Research Excellence Funding Student Seminar (Presentation)*, Hamilton, Canada, 2011.

Ituen, I., Reviewing the Environmental Statutes of Canadian Nuclear Regulations and their Impact on the Generation-IV Reactor, *35th Canadian Nuclear Society / Canadian Nuclear Association Student Conference (Poster Presentation and Paper)*, Niagara Falls, Canada, 2011.

Appendix A

Appendix

A.1 Review of Modern Standards for SCWR

This section gives an overview of the research done on the applicability of CNSC standards to the SCWR. The following is mainly drawn from the publication from earlier this year [56]. The regulations set out by the CNSC are applied to the nuclear power reactors that are in Canada. But as new types are built, these regulations may have to change. With the CANDU-SCWR, new regulations might be needed. That notion is what this section examines. It has been recognized that since this reactor design is first of its kind, the current standards, policies, and regulations issued by the regulatory authorities would not have accounted for unique features of the SCWR.

The regulations are to ensure the public is kept safe from ionizing radiation generated during the plant's operations or other power plant accidents. The following sub-sections examine the Canadian regulations pertinent to licensing a new reactor to determine if they would be applicable to the SCWR.

Regulations

A.1.1 RD-346: Site evaluation for new nuclear power plants

RD-346 provides general criteria for site evaluation. The regulation states that the main objective for site evaluation is that the NPP will not "create unreasonable risk to the public or to the environment" [57]. The licensee is responsible for identifying and prioritizing the risks associated with the site's characteristics and external events, for example the SCWR's turbine being in containment would necessitate a new load to containment and internal structures.

In this Regulatory document, some of the criteria for evaluating an NPP site are:

1. Evaluation against safety goals
2. Consideration of evolving natural and human-induced factors
3. Evaluation of the hazards associated with external events
4. Determination of the potential effects of the NPP on the environment
5. Consideration of projected population growth in the vicinity of the site, and emergency planning that takes those projections into account.

Overall, RD-346 is a comprehensive and relevant regulation for the planned SCWR. It is entirely applicable to the SCWR, and no areas need to be changed to accommodate this new reactor.

A.1.2 RD-310: Safety analysis for nuclear power plants

The CNSC expects this regulation to be applied in new-build submissions. This regulation is for the deterministic safety assessment of an NPP. Events to be analysed are classified into three classes of events based on probabilistic studies and engineering judgement – AOO's, DBA's, and BDBA's.

Apart from the quantitative references for the events, the operator needs to establish the qualitative acceptance criteria for the event. That way, the analyst will know (following the safety analysis) if the plant systems meet the target set. The ultimate goal is that the integrity of physical barriers is maintained and release of radioactive material is prevented following an AOO or DBA. The regulation suggests that quantitative (derived) acceptance criteria should be used for AOOs and DBAs to demonstrate that the qualitative acceptance criteria are met. These numerical targets are obtained from other experimental data prior to performing the safety analysis.

A licensee has to review the safety analyses to ensure they meet the set objectives. The safety analyses are to be periodically reviewed and updated to account for changes in NPP configuration, conditions (including aging), operating procedures, research findings, and advances in knowledge and understanding of physical phenomena. Finally, if a different hazard is realized long after the initial analysis is done, these differences should be incorporated into the next 'periodic update' to keep the Safety Analysis Documentation current.

Overall, RD-310 is relevant to the SCWR since the plant must undergo Safety Analysis, and the design method will incorporate results from this form of safety analysis (deterministic safety analysis).

A.1.3 RD-337: Design of new nuclear power plants

RD-337 specifies the CNSC expectations for new water-cooled NPP designs. The CNSC drew on the principles in IAEA document NS-R-1 Safety of Nuclear Plants: Design [58] in writing this regulation, and adapted those principles to align with Canadian practices. Since RD-337 is intended to be technology-neutral, it is anticipated that most of the regulation will be applicable to the SCWR concept.

The regulation states that an independent peer review of the safety assessment would be performed before the design is submitted. The basis of the safety assessment, as the regulation informs, is the data derived from the safety analysis, operational experience, research, and proven engineering practices.

The SCWR should definitely be built around the stipulations in this regulation. It provides beneficial guidelines for the operation and reliability of the safety support systems. Following these rules in design could contribute to the SCWR being a safer and more reliable reactor.

A.1.4 R10: The use of two shutdown systems in reactors

This regulation mandates that each reactor shall incorporate two independent protective Shutdown Systems (SDSs), unless CNSC approves otherwise. The issue of two SDSs was introduced to counter the effect of positive coolant void reactivity in CANDU. The positive coolant void reactivity means that in a LOCA, the reactivity of the core would increase thereby increasing power in the reactor. The immediate response necessary would be to shutdown the reactor to prevent damage to the core or structures. The second SDS was needed to ensure the CANDU reactor would have a high certainty of shutting down within a few seconds in accident scenarios.

The SCWR in its current pre-conceptual design stage is to have a negative coolant void reactivity. In that case, the requirement for two SDSs to compensate each other is muted because power will decrease on void of coolant. The change in fuel and moderation characteristics may affect coolant density feedback effects.

Two fast-acting safety shutdown systems may not be required since LOCA power pulse and failure to shutdown issues may not apply to the SCWR design. The SCWR might only require one fast-acting SDS, and this would greatly simplify the design, maintenance and testing requirements.

R-10 might not be directly applicable to the SCWR. Perhaps meeting the requirements of regulations such as RD-310 and RD-346 is sufficient.

A.1.5 R8: Requirements for shutdown systems for CANDU nuclear power plants

R-8 is also written for the CANDU NPP and so refers to two SDSs. Some of the regulation's requirements imply that if two SDSs are used for the SCWR, the combined unavailability will have to be less than 10^{-6} years per year. Another R-8 requirement is that the design shall be such that it is not readily possible for an operator to prevent actuation of a SDS when such actuation is required. This is in line with the philosophy of the SCWR – being built with passive safety concepts. The regulation also demands that the failure of any component of the SDS cannot impair the system from meeting its minimum allowable performance standards under accident conditions.

The SCWR is a CANDU-type reactor and so the directives of this regulation could be incorporated into the SCWR's design without modification.

A.1.6 S-294: Probabilistic safety assessment for nuclear power plants

Items of note in this regulatory standard are the PSA requirements. They include

- The NPP must perform a facility-specific Level 2 PSA
- PSA models should be as good a representation as possible of the plant as built and operated
- PSA models must be developed using assumptions and data that are realistic and practical
- The CNSC must accept the methodology and computer codes used for the PSA
- The PSA models must be updated every three years, or sooner if the facility undergoes major changes

This Standard is relevant to the SCWR as part of its safety analysis will be done using PSA, adopting a risk-informed design process from the outset.

A.1.7 S-98 Rev.1: Reliability programs for nuclear power plants

S-98 is a document that describes CNSC requirements for systems' and components' reliability, and for the programs which are implemented at operating stations to track these issues [59].

As part of the drive to improve safety in the GEN-IV designs, the systems important to safety in the SCWR will need to show an increased level of reliability. This

regulatory document urges that a Reliability Program be established. Such a reliability Program should be established in the SCWR operations, especially as there is not a lot of data on the response of this plant at the conditions it will operate at.

This standard would be useful during all the phases of the reactor life cycle. Therefore it should be incorporated into the design and operation of the SCWR.

A.1.8 G-144: Trip parameter acceptance criteria for the safety analysis of CANDU nuclear power plants

This Guide focuses most of its attention on fuel sheath dryout and post-dryout effectiveness in existing CANDU's [60]. This is because dryout can be taken as an acceptable alternative to fuel failure, and the resulting pressure tube failure, for safety assessments and monitoring. This Guide is written for CANDU NPP's, and though the SCWR is to be a CANDU-type reactor, some of its characteristics differ greatly from the traditional CANDU. For instance the SCWR will operate with supercritical water as coolant and so the fuel channels will not experience dryout. As such, fuel sheath dryout need not be a trip parameter in this new reactor. Therefore, a new trip effectiveness parameter must be defined.

One method of developing alternate trip parameter criteria for the SCWR is to first of all identify the mechanisms for fuel failure. Some of the fuel failure mechanisms are melting, fuel fragmentation, strain, and oxidation. Therefore, some alternate trip criteria which should be considered are Strain level and Oxidation and Hydriding.

In lieu of the complexity of determining sheath strain during all possible DBAs, it is likely that a more practicable limit be proposed for the design which ensures a large margin to fuel and pressure tube failures. It is proposed that such a criteria be based

on a given fuel power ramp rate limit, a maximum sheath temperature, and for full power operation. Under start-up and low power operation it is likely that additional criteria will be required which can accommodate the sliding start-up-like procedures, low power cooling requirements, and maintenance. For the sheaths being considered the likely criteria will be 800°C for normal operation and 1260°C for accidents [11].

A.1.9 G-149: Computer programs used in design and safety analyses of nuclear power plants and research reactors

It is imperative that the analysis conducted to support the design, or licensing of a new design, be conducted using tools and methods that are qualified for that purpose. For example the mathematical equations used in a computer program must sufficiently reflect the phenomena and processes of the physical system they model.

G-149 provides guidelines for computer programs used in designing NPPs and used for analysing operational transients, incidents, or accidents. The guidelines cover such phases as the development phase of the computer program, the design phase, the code verification phase, the program integration phase, and the computer program performance validation stage [61].

G-149 is applicable to the design and safety analysis of the SCWR as following the guidelines provided herein could lead to robust programs being used for the development of this new reactor.

SUMMARY Most of the regulations – in their current form – were found to be acceptable to cover the SCWR for licensing. Table A.1 below summarises the regulations reviewed and their applicability to the SCWR, specifying if any modification is necessary for this new reactor.

Ref.	**Regulation**	**Application**
RD-346	Site Evaluation for new Nuclear Power Plants	Yes
RD-310	Safety Analysis for Nuclear Power Plants	Yes
RD-337	Design of new Nuclear Power Plants	Yes
S-98.1	Reliability programs for nuclear power plants	Yes
R-8	Requirements for Shutdown Systems for CANDU Nuclear Power Plants	Meets Qualitative goals
R-7	Requirements for Containment Systems for CANDU Nuclear Power Plants	Yes
R-10	The Use of two Shutdown Systems in Reactors	Maybe
P-223	Protection of the Environment	Yes
S-294	Probabilistic safety assessment for nuclear power plants	Yes
G-144	Trip parameter acceptance criteria for the safety analysis of CANDU Nuclear Power Plants	No
G-149	Computer programs used in design and safety analyses of nuclear power plants and research reactors	Yes

Table A.1: Applicability of Regulations to the Supercritical Water Reactor

Appendix B

Appendix

Table B.2 below contains the systems unavailabilities used in the failure analysis of the JSCWR. Table B.3 explains the acronyms used in the event tree Fig. 4.9.

Mitigation system	**Unavailability (demand^{-1})**
RPS	1.26E-06
SLCS	2.7E-01
RCP	1.0E-02
ADS	1.7E-04
DEP	2.9E-03
AFS	4.2E-03
LPCI	2.4E-03
PCS	1.86E-02
RHR	4.34E-04
CV	3.7E-02
E/G	2.5E-02
ROSP 0.5 h	1.1E-01
ROSP 8 h	2.1E-02

Table B.2: Unavailabilities of mitigation systems [12]

Function	**Mitigation system or action**	**Abbreviation**
Negative reactivity insertion	Reactor protection system	RPS
	Standby liquid control system	SLCS
	Manual depressurization for initiating SLCS	DEP
Core cooling	Reactor coolant pumps (both turbine-driven and motor-driven)	RCP
	Auxiliary feedwater system	AFS
	Automatic depressurization system	ADS
	Low pressure core injection system	LPCI
Containment cooling	Power conversion system	PCS
	Residual heat removal system	RHR
	Containment vent	CV
Electricity	Emergency diesel generators	E/G
	Recovery of offsite power in 0.5 h	ROSP 0.5 h
	Recovery of offsite power in 8 h	ROSP 8 h

Table B.3: Acronyms used in Event Tree for Super Light Water Reactor [12]

Bibliography

[1] Industry Canada, "Power mix," *IC*, Accessed from http://www.ic.gc.ca/eic/site/mse-epe.nsf/eng/home, July 2011.

[2] GIF, "GIF 2009 Report," *GIF*, Accessed from www.gen-4.org, July 2011.

[3] GIF, "GIF Objectives," *GIF*, Accessed from www.gen-4.org, June 2011.

[4] D. Brady, R. Duffy, H. Khartabil, R. Sadhankar and S. Suppiah, "Generation IV reactor development in Canada," *Proceedings of the 3rd International Symposium on Supercritical-Water-Cooled Reactors – Design and Technology*, Shanghai, China, March 2007.

[5] R. Duffey, L.K.H. Leung and I. Pioro, "Design principles and features of Supercritical Water-cooled Reactors to meet design goals of Generation-IV nuclear reactor concepts", *Technical Meeting On Heat Transfer, Thermal-Hydraulics And System Design For Supercritical Water*, Pisa, Italy, July 2010.

[6] M. Yetisir, B. Diamond, L. Leung, D. Martin and R. Duffey, "Conceptual mechanical design for a pressure-tube type Supercritical Water-Cooled Reactor," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[7] D. Brady, D. Guzonas, W. Zheng and L.K.H. Leung, "Research and Development Initiatives in Support of the Conceptual Design for the CANDU Supercritical Water-Cooled Reactor," *Proceedings of the 31st Annual Conference of the Canadian Nuclear Society*, Montreal, Canada, May 2010.

[8] G. Wu, Q. Bi, Z. Yang and M. Li, "Experimental investigation on heat transfer of supercritical pressure water in annular channel," *Proceedings of the 2nd Canada-China Joint Workshop on Supercritical Water-Cooled Reactors*, Toronto, Canada, April 2010.

[9] L. Jeddi, K. Jiang, S. Tavoularis and D. Groeneveld, "Preliminary tests at the University of Ottawa Supercritical CO2 heat transfer facility," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[10] W. Zheng, J. Luo, M. Li, D. Guzonas and W. Cook, "Stress corrosion cracking of SCWR candidate alloys: A review of published results," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[11] M. McDonald and D. Novog, "Analyses of hot channel fuel conditions and loss of regulation accident for CANDU-SCWR fuel channels," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[12] Y. Oka, S.Koshizuka, Y. Ishiwatari, and A. Yamaji, *Super Light Water Reactors and Super Fast Reactors - Supercritical-Pressure Light Water Cooled Reactors*, Springer, New York, NY, 2010.

[13] T. Schulenberg, C. Maraczy, W. Bernnat and J. Starflinger, "Assessment of the HPLWR thermal core design," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[14] D.F. Spratt, T.F. Lin and J.A. Peters, "The ignition and combustion of Zircaloy-4," *American Nuclear Society Transactions*, Vol. 99, pp.488–489, 2008.

[15] Y. Oka, S. Morooka, M. Yamakawa, Y. Ishiwatari, S. Ikejiri, Y. Katsumura, Y. Muroya, T. Terai, K. Sasaki, H. Mori, Y. Hamamoto, K. Okumura, T. Kugo, T. Nakatsuka, K. Ezato, N. Akasaka and A. Hotta, "Research and development of Super Light Water Reactors and Super Fast Reactors in Japan," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[16] K. Yamada, S. Sakurai, Y. Asanuma, R. Hamazaki, Y. Ishiwatari and K. Kitoh, "Overview of the Japanese SCWR concept developed under the GIF Collaboration," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[17] C. Koehly, J. Starflinger, T. Schulenberg, M. Brandauer, D. Lemasson, R. Velluet, and H. Herbell, "Draft layout of the HPLWR power plant," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[18] D. Bittermann, T. Schulenberg, M. Andreani, "The safety concept of the HPLWR," *Proceedings of the 4th International Symposium on Supercritical-Water-Cooled Reactors*, Heidelberg, Germany, March 2009.

[19] M. Andreani, D.Bittermann, Ph. Marsault, O. Antoni, A. Kereszturi, M.Schlagenhaufer, A.Manera, M. Seppala, J.Kurki, "Evaluation of a preliminary safety concept for the HPLWR," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[20] J. Kurki and M. Seppl, "Thermal Hydraulic Transient Analysis of the High Performance Light Water Reactor Using APROS and SMABRE," *Proceedings of the 20th International Conference on Structural Mechanics in Reactor Technology, SMiRT 20*, Espoo, Finland, August 2009.

[21] J. Starflinger, T. Schulenberg, D. Bittermann, M. Andreani and C. Maraczy, "Assessment of the High Performance Light Water Reactor concept," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[22] B. de Marsac, T. Schulenberg and M. Schlagenhaufer, "Residual heat removal system of the HPLWR," *Proceedings of the International Students Workshop on High Performance Light Water Reactors*, Karlsruhe, Germany, March 2008.

[23] AECL, "Enhanced CANDU 6™(EC6™) design description: IAEA advanced water cooled reactors web-based report," *Atomic Energy of Canada Ltd.*, 2009.

[24] AECL, "CANDU 6 Technical Outline," *Atomic Energy of Canada Ltd.*, 2005.

[25] P. Boczar, W. Shen, J. Pencer, B. Hyland and R. Dworshak, "Reactor physics

studies for a pressure tube Supercritical Water Reactor (PT-SCWR)," *Proceedings of the 2nd Canada-China Joint Workshop on Supercritical Water-Cooled Reactors*, Toronto, Canada, April 2010.

[26] IAEA, "IAEA-TECDOC-1594: Analysis for Severe Accidents in Pressurized Heavy Water Reactors," *International Atomic Energy Agency*, 2008.

[27] J.C. Luxat, "Thermal-hydraulic aspects of progression to severe accidents in CANDU reactors," *Nuclear Technology*, Vol. 167, pp.187–210, 2009.

[28] P.M. Mathew, W. Kupferschmidt, V. Snell, and M. Bonechi, "CANDU-specific severe core damage accident experiments in support of Level 2 PSA," *Proceedings of the 16th International Conference on Structural Mechanics in Reactor Technology, SMiRT 16*, Washington DC, U.S.A., August 2001.

[29] IAEA, "IAEA-TECDOC-1624: Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants," *International Atomic Energy Agency*, 2009.

[30] J. Beard, "ESBWR Overview," *GE*, Presentation accessed from http://www.ne.doe.gov/np2010/pdfs/esbwrOverview.pdf, 2006.

[31] AECL, "ACR-1000 technical summary," *CD-ROM*, 2007.

[32] N.J. McCormick, *Reliability and risk analysis*, Academic Press, New York, NY, 1981.

[33] M.Modarres, *What every engineer should know about reliability and risk analysis*, Marcel Dekker Inc., New York, NY, 1993.

[34] CNSC, "S-294: Probabilistic safety assessment (PSA) for nuclear power plants," *Canadian Nuclear Safety Commission*, 2005.

[35] CNSC, "RD-337: Design of new nuclear power plants," *Canadian Nuclear Safety Commission*, 2008.

[36] CNSC, "RD-310: Safety analysis for nuclear power plants," *Canadian Nuclear Safety Commission*, 2008.

[37] USAEC, "WASH-740: Theoretical possibilities and consequence of major accidents in large nuclear plants," *U.S. Atomic Energy Commission*, 1957.

[38] V.G. Snell and W. Garland, "EP716 Course notes: Nuclear Reactor Safety Design," *McMaster University*, 2009.

[39] Electric Utility Consultants Inc. (EUCI), "Nuclear power Probabilistic Risk Assessment (PRA)," *Course on PRA at Arlington, USA*, March 2010.

[40] V.G. Snell and R. Jaitly, "CANDU Safety #20 – Probabilistic Safety Analysis," *CANTEACH*, Presentation accessed from http://www.canteach.candu.org.

[41] M.Modarres, M. Kaminskiy, and V. Krivtsov, *Reliability engineering and risk analysis: a practical guide*, 2nd ed., CRC Press, New York, NY, 2010.

[42] Electric Power Research Institute, Inc. (EPRI), "CAFTA, Software Manual, Software Product ID #1015513," *CD-ROM*, Palo Alto, CA, 2007.

[43] USNRC, "NUREG/CR-5750: Rates of Initiating Ivents at U.S. Nuclear Power Plants: 1987 - 1995," *U.S. Nuclear Regulatory Commission*, 1999.

[44] USNRC, "NUREG/CR-2300: Probabilistic risk assessment procedures guide," *U.S. Nuclear Regulatory Commission*, 1982.

[45] USNRC, "NUREG-75/014: Reactor safety study – An assessment of accident risks in U.S. commercial nuclear power plants (WASH-1400)," *U.S. Nuclear Regulatory Commission*, 1975.

[46] USNRC, "IAEA-TECDOC-478: Component reliability data for use in probabilistic safety assessment," *International Atomic Energy Agency*, 1988.

[47] B.N. Roy, "WSRC-TR-93-262: Savannah River site generic data base development," *Westinghouse Safety Management Solution*, 1998.

[48] AECB, "R-10: The use of two shutdown systems in reactor," *Atomic Energy Control Board*, 1991.

[49] P. Yang, L. Cao, H. Wu, and C. Wang, "Core design study on CANDU-SCWR with 3D neutronics/thermal-hydraulics coupling," *Nuclear Engineering and Design*, DOI:10.1016/j.nucengdes.2011.03.036, 2011.

[50] D. Meneley, "Course notes, Nuclear Safety and Reliability: Week 11," *CANTEACH*, 2003.

[51] USNRC, "NUREG/CR-6065:Systems analysis of the CANDU 3 reactor," *U.S. Nuclear Regulatory Commission*, 1993.

[52] G. Bereznai, "Nuclear power Probabilistic Risk Assessment (PRA)," *Course notes, Nuclear Power Plant Systems and Operation*, 2005.

[53] USNRC, "NUREG-1784: Operating experience assessment – effects of grid events on nuclear power plant performance," *U.S. Nuclear Regulatory Commission*, 2003.

[54] I. Ituen and D. Novog, "Assessing the Applicability of Canadian Regulations to the Supercritical Water Reactor," *Proceedings of the 5th International Symposium on Supercritical-Water-Cooled Reactors*, Vancouver, Canada, March 2011.

[55] USNRC, "NUREG-1860 Vol. 2: Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," *U.S. Nuclear Regulatory Commission*, 2007.

[56] I. Ituen and D. Novog, "Assessing accident risks and responses in Canada's Supercritical Water Reactor," *Proceedings of the 19th International Conference on Nuclear Engineering, (Accepted)*, Chiba, Japan, May 2011.

[57] CNSC, "RD-346: Site evaluation for new nuclear power plants," *Canadian Nuclear Safety Commission*, 2008.

[58] IAEA, "Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1," *International Atomic Energy Agency*, 2000.

[59] CNSC, "S-98 Rev.1: Reliability programs for nuclear power plants," *Canadian Nuclear Safety Commission*, 2005.

[60] CNSC, "G-144: Trip parameter acceptance criteria for the safety analysis of CANDU nuclear power plants," *Canadian Nuclear Safety Commission*, 2006.

[61] CNSC, "G-149: Computer programs used in design and safety analyses of nuclear power plants and research reactors," *Canadian Nuclear Safety Commission*, 2000.