Probabilistic Risk and Safety Assessments in Supercritical Water Reactors

I. Ituen
McMaster University, Hamilton, Ontario, Canada

Abstract

The Supercritical Water Reactor will introduce new avenues of risk that the Canadian nuclear industry has not dealt with before. For this reactor to be licensed for use in Canada, it will need to satisfy the safety standards of CNSC. Part of the licensing requirement is that a Probabilistic Safety Assessment is done on the entire plant to ensure the safety of the employees, the public, and the ecology in the nuclear plant's site. This paper will show some of the steps that can be taken in performing a complete risk and safety analysis on the plant.

1. Introduction

The Generation-IV International Forum (GIF) proposed a number of reactor designs that could be built in the next few decades. These new reactors are termed Generation-IV reactors, or GEN-IV reactors. These reactors are meant to have improved economics, improved safety, and be more sustainable [1]. The reactors differ in design; however, each of them must conform to certain standards given by GIF, for instance, they must all meet the increased level of safety, economics and sustainability. The reactor Canada is proposing to build is the Supercritical Water Reactor (SCWR).

It is expected that the next generation CANDU design will increase the thermal efficiency by up to 15% and improve the economics of the reactor, primarily through capital cost and construction schedule reduction. Like the other GEN-IV designs, it is expected that the SCWR will use more passive safety systems than the traditional CANDU. Although passive systems are usually preferred because they make use of proven natural phenomena such as convection and gravity, the system components still might fail. Moreover, passive systems can be difficult to test.

The SCWR will have operating conditions that are drastically different from Canada's traditional CANDU. For instance, this reactor will operate above the supercritical conditions of water, specifically 25MPa and 625°C, compared to the 10MPa and 325°C. Such conditions introduce new avenues of risk during operation and adequate safety measures must be implemented to prevent accidents. This reactor is expected to have enhanced passive safety systems, but even passive safety systems produce challenges of their own in terms of testing them to ensure they have the required performance reliability. This paper will consider some of the tools that can be used to analyse the safety of the SCWR during this design phase.

2. Risk Assessments

Risk is the possibility of loss or injury resulting from exposure to a hazard, while a 'hazard' is a condition that can cause an undesired consequence. This implies that there is danger from the exposure to a hazard. Identifying a risk reduces the probability of harm from the particular hazard since the hazard will then be avoided. However, each risk is an undesired event, and it is quantified as

$$Risk = Expected\ frequency\ of\ undesired\ event \times Expected\ damage \quad (1)$$

The operations undertaken in a nuclear power plant expose both the plant staff and the residents in the surrounding area to various risks. Therefore, prior to running the plant, a complete risk analysis must be conducted. This is so that all foreseeable hazards that can occur in the plant are identified. Then, mitigating systems or procedures can be introduced to slow or minimize the effect of the hazards. A Probabilistic Risk Assessment (PRA) is an analysis that can be used to quantitatively measure the level of risk an individual would be exposed to from the nuclear plant operations.

Risk assessment is necessary to determine the accident sequences that could lead to system failure and, if possible, remove the weakest links of the system [2]. Knowing the expected accident sequence allows an analyst to verify that the systems in the power plant that should mitigate the accident have a high enough reliability when called upon to act. Probabilistically speaking, the reliability of a component or system can be defined as its ability to operate under designated operating conditions for a designated period of time [3]. As a measure for probabilistic analysis, the reliability of a component or system is a reflection of its success at operating when required. Therefore, in order to mitigate an undesired event, a nuclear plant should be designed to have response systems with a high reliability. For accident scenarios that are even more severe or have worse consequences, the reliability standard should be much higher than for accidents of lesser consequence. (That is, the system should not be prone to failure.) This inference can be drawn from the definition of risk in eqn 1: to keep the risk low for a situation with a severe (highly hazardous) consequence, the frequency should be kept to a minimum.

Reliability of a component can be measured as a function of time from the following equation:

$$R(t) = 1 - F(t) \tag{2}$$

Where $R(t)$ is the reliability function at time *t*, and $F(t)$ is the probability that the component will fail before time *t*.

If the component operates up until timeτ, the reliability function can be defined as:

$$R(t) = \int_t^{\infty} f(\tau)\, d\tau \tag{3}$$

In performing the PRA of a NPP, the components and systems that are part of mitigating safety systems should be tested to ensure their reliability is maximized. Testing for reliability can be done using equations similar to (2) and (3) above. Also, the probability of failure of the components can be estimated from similar formulas. Usually, improving the performance of a structure, system, or component will reduce a risk. However, a risk analyst would need to know which systems or components are affected in the undesired event being planned against in order to know the system or component that needs improvement. One way to visualize the components that could be responsible for a failure is by using a Fault Tree.

A fault tree starts with ‘top event’ and then shows probable causes for the event or failure. The Fault Tree is made up of branches that can have another component, or structure, or system as a factor that causes the failure. Each element of the Fault Tree has an associated failure probability according to the mode of failure. For instance, the failure analysed in a Fault Tree could be the failure of feedwater to be delivered to the steam generator. A branch on the Fault Tree could be the feedwater pump failing. However, the pump would have different failure probabilities depending on its mode of failure, e.g. failure to continue pumping having already started, or failure to start pump when the signal to initiate the pump is received. For the former failure, the probability of occurrence

could be 0.001, while the probability of the pump not starting on receipt of the "start" signal could be 0.008. Since the failure modes have different failure probabilities, each event has to have a separate branch on the tree to do a proper failure analysis. A benefit of the Fault Tree is that it gives the opportunity to analyse the probable causes of a failure and also see the probabilities of such failures. Then, the probabilities of individual failures are calculated using the usual probability and statistics tools. Another value of the Fault Tree is that it can help to quickly recognize the most likely system failure modes.

As an example of the usage of Fault Trees for probabilistically analysing risk, Figure 1 shows a Fault Tree for the loss of Class-IV power in a CANDU-type SCWR. This was generated with the Risk Assessment software CAFTA.

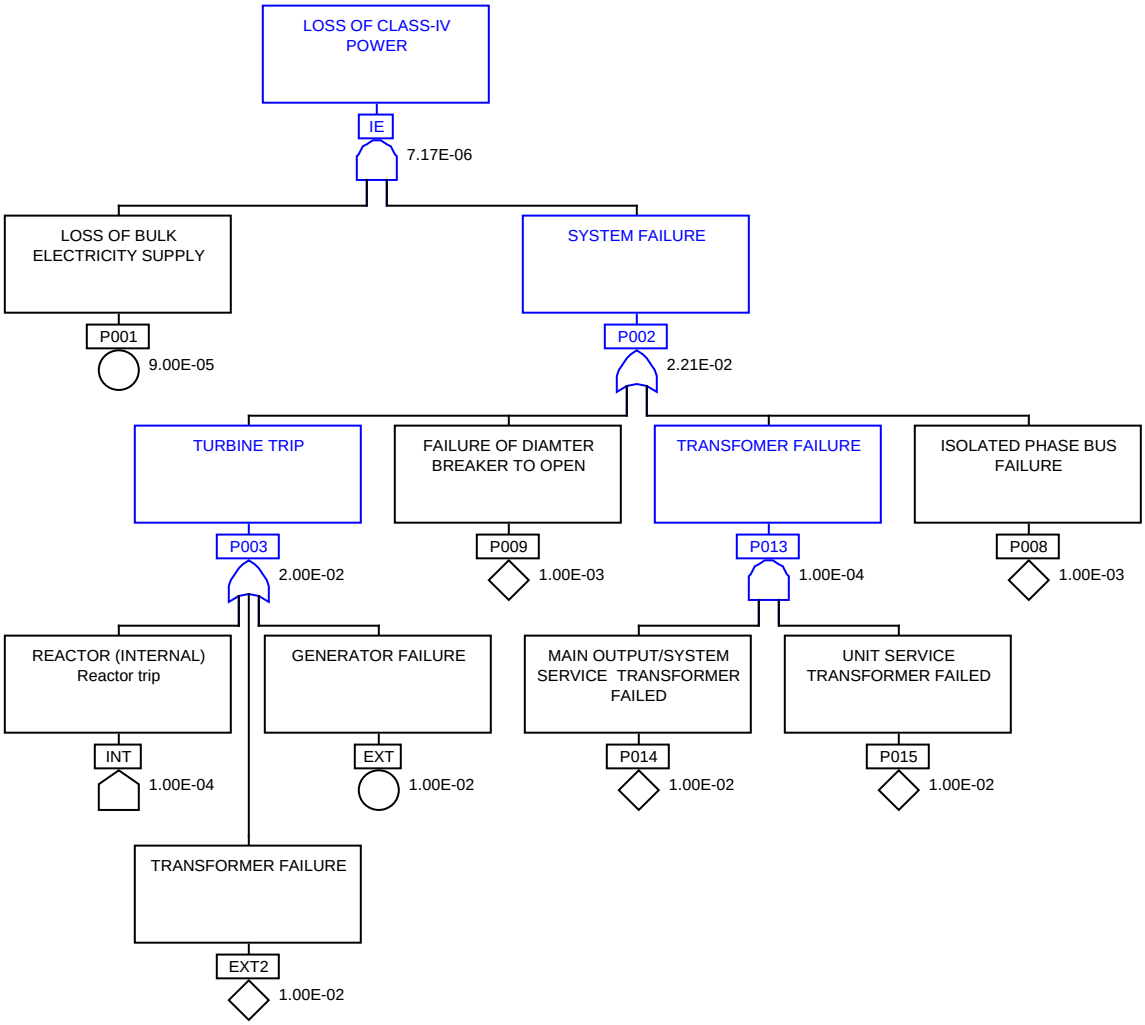

Figure 1 Fault Tree for causes of Loss of Class-IV Power.

The top event in the Fault Tree is the scenario that is to be prevented (or an incident that has occurred and troubleshooting is underway to determine the cause). From Figure 1, the NPP can lose Class-IV power if both the bulk electricity supply fails and a system failure occurs. Here, the system failure that could cause the loss of power is any of the four elements that branch from the System Failure box.

Analysis of a Fault Tree starts from the top and develops downward, as the risk analyst identifies more probable causes for the failure. The numbers beneath the component/system failure boxes are their probability of failure. Therefore, overall, if the only components and systems that the Class-IV power supply depended on are represented in Figure 1, the probability of a NPP experiencing a complete loss of Class-IV Power is 7.17×10^{-6}, or there is a 0.000717% chance of this occurring.

A PRA can be used to identify the types of accidents that could occur as well as their frequency of occurrence. In a nuclear power plant, the most important event being prevented is a large radioactivity release. Every NPP operator wants to prevent the release of fission products in the containment, and their leakage from containment. With the PRA, it is possible to find severe accident weaknesses in the system. Severe accidents will yield the release of radioactivity outside containment or result in core melt. Performing a PRA will allow designers to know what reliability components or systems need to have to prevent such events. A PRA is also a good tool for designers and decision-makers to generate quantitative results to plausible accident scenarios. In this way, the PRAs can feed back to the designers with advance requirements such as reliability data, to make the reactor design safer.

3. Safety Analysis

Another tool in analysing the safety of a reactor is a Probabilistic Safety Assessment (PSA). A PSA can be done by the use of Event Trees. There are three levels of PSAs [4]:

a) Level 1 – Identifies the events that could lead to core damage or massive fuel failure

b) Level 2 – Starts with Level 1 results and analyses the behaviour of the containment, evaluates the radionuclides that are released from failed fuel, and quantifies the releases to the environment

c) Level 3 – Starts with Level 2 results and models the release of radionuclides to the environment and their impact on the health of the public

The Event Tree displays probable outcomes of an “Initiating event”. The subsequent actions following the Initiating Event are also termed ‘events’. It is during a PSA that the subsequent events are analysed to anticipate the response of a system to an Initiating Event. In a NPP, there are structures and systems to compensate for any event that is outside the regular operation of the reactor. Some of the compensating systems are automatically initiated while others need to be started by the operators on duty.

Event Trees allow one to see which system would next mitigate the accident, minimizing the consequence of the accident. So one can know the progression of the accident and know which systems need to be available as well as possible consequences under various availabilities of the mitigating systems. For instance, if the Initiating Event is a turbine trip, the subsequent systems that will kick in for a CANDU include the Reactor Regulating System through a setback, the Emergency Stop Valves may close to prevent further steam going to the turbine, and the Condenser Steam Discharge Valves will open to send the excess steam to the condenser shell.

Just as in the PRA’s Fault Trees, the reliability of mitigating systems and components must be determined in performing a PSA. That way, an analyst can know the probability of the failure of the mitigating components. In the example above, the probability needed will be the failure probability of the valves and the Reactor Regulating System. The final probability of the accident proceeding is

calculated using probability formulas. An Event Tree will display the end result of the accident given the success or failure of a mitigating system. Figure 2 shows an Event Tree for a loss of coolant accident in a SCWR.

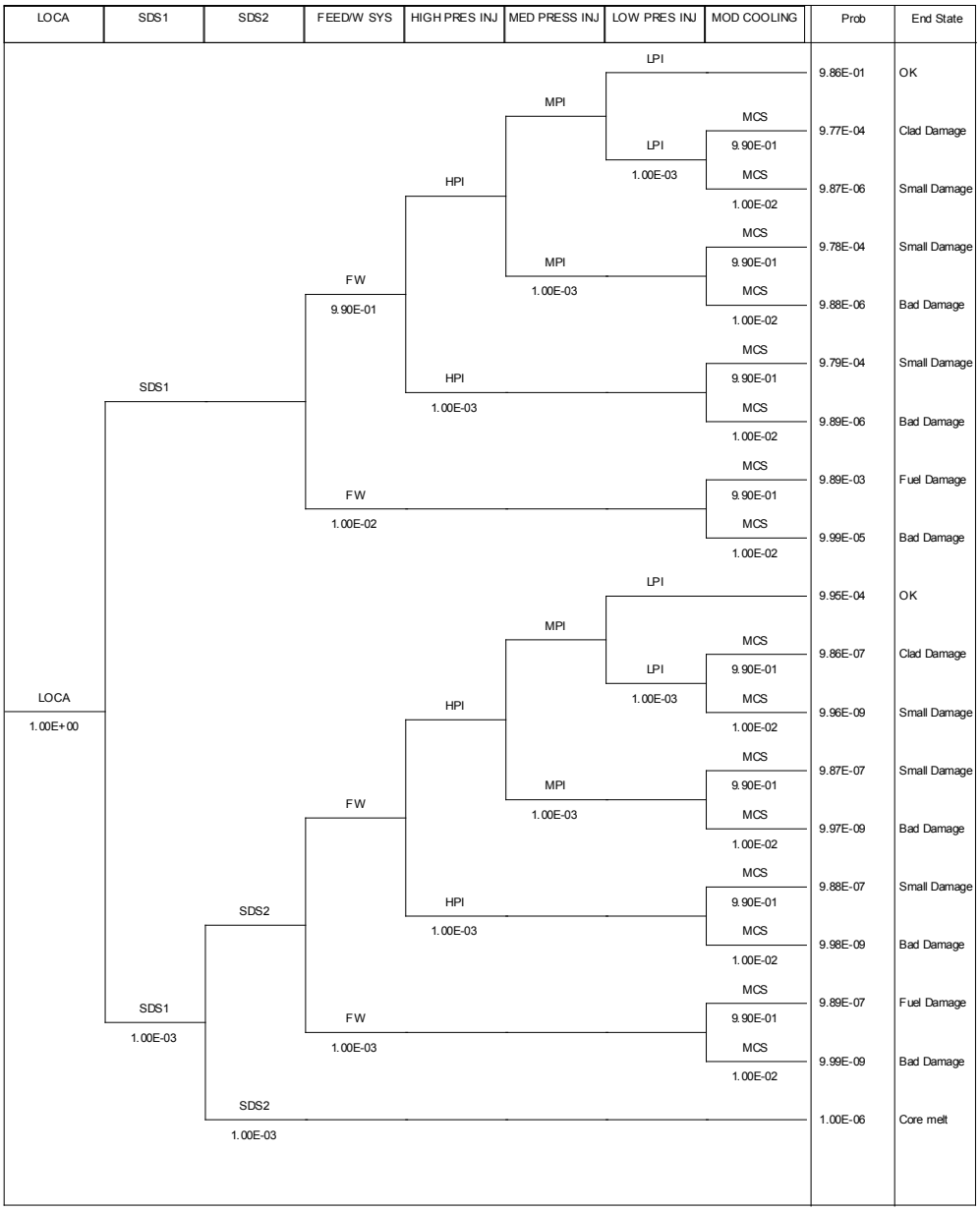

Figure 2 An Event Tree of a Loss of Coolant Accident.

The ‘end state’ in Figure 2 represents the consequence of the accident, depending on how the mitigating system functioned. The Event Tree allows a decision-maker to quantitatively estimate the consequence of a component or system that is important to safety not performing as it should. Thus, there can be feedback to the designers to incorporate further safety features to stop the progress of an accident, if for instance, a particular availability criteria was being designed towards. Each scenario represented in the Event Tree is a realistic though approximate guess of how a system will

respond. The values for the failure/success probabilities are based on either plant history, or data from the plant history of a similar plant. In situations where exact plant data cannot be accessed, expert judgement can be used, and an element of conservatism included to design the plant towards fewer failures, even at the cost of less availability. (Availability here is used in the nuclear industry term of being the percentage of time the plant is operational or is capable of being put into operation for the electricity demands [5].) Another source of failure probabilities is IAEA's *Component Reliability Data for use in PSA* [6]. This document provides the probabilities of certain safety system failures and describes their consequences.

These methods of obtaining failure probability data described above will be very important for the SCWR as it is still in design phase. There needs to be close communication between the PSA/PRA analysts and the designers. The designers make their design based on availability requirements. As the PSA/PRA analysts discover systems or components that are very susceptible to failure and might increase the failure probability of a system, they could give feedback to the designers so the designers either replace the component, or create a compensating system to make up for the lapse. There is great opportunity in the design stage of the SCWR to use data of failures from plants that currently exist. However, as the operating temperatures and pressures far exceed those used currently for nuclear power generation, some data might be taken from the fossil fuel industry which already uses supercritical water systems for power generation. Furthermore, different materials might be required for the SCWR, since fuel claddings, fuel bundles and other in-core elements that are used in the CANDU might not withstand the high temperatures and pressures the SCWR components will be subjected to. Finally, when the SCWR is built, the failure data specific to the reactor can be incorporated in future PSA's. Canadian Nuclear Safety Commission (CNSC) – the nuclear industry's regulator in Canada – mandates that a Level 2 PSA be done on al NPP's every 3 years [4]. So after a while of operating, plant-specific data will be available to update the PSA.

4. Conclusion

The SCWR is a GEN-IV reactor that could be built in the next few decades. Its high temperatures and pressures are causes of concern in terms of safety. Two very good tools at analysing the safety of components and systems are PSA and PRA. This paper has demonstrated the value of PSA and PRA to the analysis of NPP's and the SCWR in particular. A PRA is very beneficial as its results provide a comprehensive assessment of the NPP. The plant's design can be scrutinized, and the reliability of each component and system can be examined and quantified. This has tremendous benefit to the SCWR that is not yet built as the PRA will identify possible weaknesses in the design and help to prevent severe accidents. Furthermore, a PSA should be a very cost-effective tool if it is used as a design tool as it will point out systems that need strengthening to avoid large releases of radioactivity.

5. References

[1] Nuclear Energy Advisory Committee and GIF, "GEN-IV Roadmap: Description of candidate water-cooled reactor systems report, GIF-015-00", Dec. 2002, p.9.

[2] N.J. McCormick, Reliability and risk analysis, Academic Press, 1981.

[3] M. Modarres, M. Kaminskiy, and V. Krivtsov, Reliability engineering and risk analysis: A practical guide, 2nd ed., CRC Press Taylor & Francis Group, 2010.

[4] Canadian Nuclear Safety Commission, "S-294: Probabilistic safety assessment (PSA) for nuclear power plants", Apr. 2005, pp.8,10.

[5] J.R. Lamarsh and A.J. Baratta, Introduction to nuclear engineering, 3rd ed., Prentice-Hall Inc., 2001.

[6] IAEA, “Component reliability data for use in probabilistic safety assessment”, 1998.