OVERVIEW OF SOME CHALLENGES IN PSA REVIEWS FOR EXISTING AND NEW NUCLEAR POWER PLANTS IN CANADA

Guna Renganathan and Raducu Gheorghe
Canadian Nuclear Safety Commission
Ottawa, Canada

Yolande Akl, Director,
Canadian Nuclear Safety Commission
Ottawa, Canada

Abstract

The paper briefly describes the existing international and Canadian practices and guidance in the area of computer-based control and Digital I&C Systems. The paper presents the situation where the lack of information was experienced, how the situation was handled, and the type of information expected from the international community, if any. This paper also highlights the international activities in progress, for a better understanding of some of the cases considered in the discussion.

In Canada, Probabilistic Safety Assessments (PSAs) are being developed to demonstrate compliance with the safety goals, to identify plant vulnerabilities, for operation management, risk informed decision making, configuration management, testing and maintenance planning and optimization, safety upgrading programmes, and cost impact assessment. A post-Fukushima event review provided additional insights into the treatment of external events.

The Canadian Nuclear Power Plants (NPPs) are Pressurised Heavy Water Reactors (PHWR). However, vendors have submitted Pressurised Water Reactor (PWR) designs for review by the Canadian regulator (Canadian Nuclear Safety Commission (CNSC)). Review of PSAs for operating, refurbished plants, and new reactors revealed the need of new guidance. For instance, computer based control systems are part of the new designs, digital instrumentation and control is part of upgrades, refurbishment and in new NPP designs for many systems. The differences in international guidance in such areas require reliance on expert judgement. There is also need of guidance relating to treatment of software and hardware failure in the PSA models and their quantification, as well as the scope and treatment of external events.

1. INTRODUCTION

Since the commissioning of the first commercial Nuclear Power Plant (NPP) in the early 1950’s, until the publication of WASH-1400 studies in 1975, the deterministic approach was solely considered in evaluation of the safety cases. The WASH-1400 publication was the beginning of the use of PSA in the nuclear industry. The first PSA was issued in 1987 for the multi-unit Darlington plant.

PSA was used in a more or less formal manner in the past. In 2005, the CNSC published the PSA requirements in the regulatory standard S-2942 [1]. The regulatory standard [1] considered both

---

1 We acknowledge the valuable review comments provided by Smain Yalaoui, Michael Xu and Chantal Morin of the Canadian Nuclear Safety Commission.
international practices [2] and IAEA guidance [3, 4]. At the same time, the CNSC had been developing the Risk-Informed Decision Making (RIDM) approach for nuclear power reactor activities. In this approach, PSAs were recognized as a valuable tool for bringing insights that complemented the traditional deterministic safety approach. The requirements for the new NPP design are provided in the Regulatory Document RD-337 [5]. The PSA requirements for the new NPPs are directed through S-294 in RD-337.

Regulatory Document (RD)-337 [5] defines the safety goals and the safety system failure probability for new plants in Canada. The reliability program requirements, the guidance to set the reliability targets for the Systems Important to Safety (SIS), are defined in the regulatory standard RD/GD-98 [6].

2. SCOPE

The objective of this Technical Meeting is to serve as an international forum for presentations and discussions on the current practices in Member States pertaining to the development of PSA for new NPP designs. The emphasis will be on insights related to methodological aspects of Level 1 and Level 2 PSA for new NPP designs.

From the list of proposed topics for this technical meeting, this paper presents some of the gaps in guidance identified for the following areas:
- Computer-based control and Digital I&C Systems,
- Internal and external Hazards and PSA for shutdown modes, and
- Lessons learned from Fukushima event.

This paper includes some insights from the recent PSA review experience of operating and new NPP design.

The scope of this paper is rather limited to selected aspects related to the topics mentioned above.

From the PSA review and the lessons learned from Fukushima event, the revision being done in the regulatory requirements and guidance in the areas of internal and external hazards are discussed in this paper. The comprehensive list of PSA related aspects to be addressed as part of the evolving regulatory requirements (including guidance) is out of the scope of the present paper.

3. PSA REVIEW EXPERIENCE – CANADA

Canadian power reactors are constructed at three multi-unit sites and two single unit sites. Out of twenty-two power reactors, seventeen are currently in operation, two are at laid-up state, two are under start-up after refurbishment and one is undergoing refurbishment. In the past, Level 3 internal events at power and shut down PSAs were carried out for the multi-unit plants, and Level 2 internal events at power PSA was performed for a single unit plant. While PSAs are developed and used by the licensee in support of the safety cases for design changes and refurbishment, the PSA is considered to be one of the design assist tools for new designs.

---

2 Current regulatory standard S-294 is being revised and changed as Regulatory Document (RD-294)
The regulatory standard S-294 requires the licensees to develop a Level 2 PSA for any operating or the new NPP. At present, the licensees are in the process of complying with the S-294 requirements for the operating plants.

In Canada, at the request of the vendor, and by entering into a service agreement, the CNSC undertakes a pre-licensing review of a vendor’s reactor design. The pre-licensing review does not certify a reactor design, and does not involve the issuance of a licence. In the regulatory framework, the pre-licensing review is not required as part of the licensing process for a new nuclear power plant or small reactor.

The primary purpose of a vendor design review is to inform the vendor of the overall acceptability of the reactor design. This review provides the early identification and resolution of potential regulatory or technical issues in the design process, particularly those that could result in significant changes to the design or safety case. The CNSC conducts more detailed reviews of the design and safety case at the time of an application for a licence to construct and an application for a licence to operate.

Over the last few years, the vendors have entered in service agreements with CNSC for pre-design reviews of Advanced CANDU Reactor (ACR-1000), Enhanced CANDU 6 (EC6) and Advanced Pressurised Water Reactor 1000 (AP1000) designs. As part of the agreements, the vendors submitted a Level 1 PSA for full power and shutdown states and internal events, including limited flood analysis for new PHWR design, and EC6. For the AP1000 design, the information on the approach for the preparation of Level 1 and Level 2 PSA have been provided for regulatory review. Detailed PSAs have not yet been reviewed at this stage for new designs.

The Fukushima accident review has provided additional insights into the treatment of external hazards and expectations for existing and new designs.

3.1 DIGITAL CONTROL AND INSTRUMENTATION

International experiences indicate that digital system failures have the potential to contribute to the risk of the plant [7]. In Canada, the guidance to develop or review the probabilistic model (e.g., fault trees) of the digital I & C system has not been developed. Due to unavailability of failure data, the modeling details are not extended to the card or board level. As such, there is a need for guidance to determine usage of a specific model and guidance to include hardware, software, and their interaction.

Worldwide experience suggests that for systems with the multi-channel, defense-in-depth and fail-safe concept, the contribution from digital I&C is insignificant, viz., protective system. No special approach exists to model human error associated with the digital I & C. In addition, the Common Cause Failure (CCF) is only modeled under certain conditions.

Currently, the scope of the international activity [8] addresses some of these issues for Level 1 PSA (internal events). However, the NPP digital I & C for the new designs are expected to include the systems which provide supporting safety functions at all states of the plant, including design extended conditions. In the future, the treatment of digital components may require consideration for Level 2 and even Level 3 PSA.
In the area of digital I & C, international activities have been completed for: initial reliability modeling, methodology and acceptance criteria, defense-in-depth and diversity assessments for digital upgrades, dynamic modeling, identifying failure mode analysis, failure database development, developing insights on CCF, and software failure probability quantification. To develop taxonomy for failure mode, failure mechanism and CCF further activities are in progress. A guideline is being prepared by a Working Group on Risk Assessment (WGRISK) of Nuclear Energy Agency [8].

From the international comparative study of the available designs, it was noted that failure of processors, analog and digital input/output modules, and controller modules have not been considered in the PSA models. Dynamic interactions are also not addressed in the design aspects of PSA. This is an area that may require further consideration and guidance [9].

While participating on the international activities, CNSC reviewed the ongoing international activities in the areas of PSA for the digital I&C, and is in the process of deriving the strategy for developing a detailed guidance for a probabilistic model of the digital I&C system.

3.1.1 ANALOG TO DIGITAL

The reviews of design change-over, from analog to digital revealed several challenges. The failure modes of the components of analog systems are identified by the Failure Modes and Effects Analysis (FMEA) and the Hazard and Operability (HazOp) analysis. There is no clear systematic approach employed to identify the failure modes for the digital systems. However, considering the fault tree approach and the level of detail applied, the failure mode identification is not a major issue in digital I&C modeling in existing CANDU reactors. The modeling methodologies and their acceptance criteria through conventional methods, the fault tree approach, may not yield satisfactory results for the digital I&C system interacting with the process systems. In addition, due to the complexity in the digital system, it is unlikely to test the system exhaustively, and therefore it is difficult to prove the reliability [10]. The identification and modeling of failure modes for the digital systems may require additional study and guidance. The installation and operation of similar / same manufacturer components in several systems for the purpose of improving the maintainability leads to common cause failure concerns related, for instance, to processors, controllers, and software. It departs from existing safety principles and implementation strategy. This may require detailed study and development of guidance.

3.1.2 USE OF COMPUTER BASED SYSTEMS

In the Canadian PSA model, the traditional fault tree model is considered for evaluating the computer based system failures. The failure modes considered are the ‘control program failure’ and the ‘signal failure’. Software failure is not considered in the model.

Internationally, the importance of simplicity to assure the reliability of computer based systems important to safety was discussed. “How simple is simple enough for safety application?” is not determined. At the same time, some analytical approaches were introduced, but did not succeed in providing quantitative values. This status has been left unchanged. International co-operation should help in obtaining the analytical measures [10].
To calculate the reliability of the computer based systems, an evaluation model has to be established in order to identify the necessary parameters (as early as possible) and to collect the related information and data continuously during the operation [10].

3.1.3 SOFTWARE

Software CCFs remain an unsettled technical and regulatory issue for both new plants and for digital upgrades at operating plants. Due to CCFs, there is a potential for disabling multiple equipment trains or systems using identical software-based components. The operating experiences of some Canadian plants [8] suggest that software is not a prominent contributor to potential and actual CCFs.

By definition, the software faults are design faults. This means that software is deterministic and its failure cannot be represented by “failure probability.” However, the faults in software cause system failure(s) only when the input sequence activates those faults [10].

In some situations, probabilistic treatment of the software is considered. For instance, during the refurbishment review, reliability target for the software running on the hardware of the programmable logic controllers of a safety system was considered as $10^{-4}$ with 50 % confidence level, instead of $10^{-3}$ with 95% confidence level. While it was noted that the reliability target of $10^{-4}$ with 99% confidence level is followed by other regulators, similar statistical approach requires guidance.

The software failures are treated as dependent failures for redundant components. The existing international guidance desires a supporting analysis to verify the treatment of the software failures [12]. The analysis methodology and the software-element failure mode may have to be determined for this.

3.2 TREATMENT OF INTERNAL AND EXTERNAL HAZARDS

The regulatory standard S-294 [1] requires the PSA to include both internal and external events for both at power and shutdown state. Currently, the CNSC is in the process of preparing regulatory guidance document on the interpretation of the PSA high-level requirements included in S-294 [1].

As per the standard [1], the external event may be excluded from the PSA, if in agreement with CNSC, an alternate analysis method to conduct the assessment is chosen. Based on the review experience on PSAs for external events for operating reactors, the CNSC defined the expectations regarding an acceptable analysis approach for External Events PSA, as well as the screening criteria. For these expectations available international guidance from [3-4], and [14-17] are used. The expectations are related to the scope, screening criteria and consideration of combined effects. From this expectation: the internal hazards should not be screened out; for external hazards: the seismic hazard, external floods, high winds, and human induced hazards should not be screened out; the minimum lists of external events that have to be considered in PSA are internal fires, internal floods, seismic events. The scope should include the L1 & L2 both at power and shutdown states.
During PSA review of the operating plants, the licensees have submitted requests to CNSC for exemption from detailed analysis of internal floods, internal fires and seismic events in shutdown PSA. These exemptions requests have been accepted based on an alternative approach prepared by CNSC. This alternative approach has been derived considering the international guidance [3, and 18-24].

These CNSC expectations have already been presented to the Canadian industry, and once finalised, they will be included in the regulatory guidance for S-294. Given that S-294 [1] is applicable to both the existing and new plants, the guidance will reflect the scope of this regulatory standard.

The S-294 [1] is being revised to include all potential site-specific initiating events and potential hazards. These include, internal initiating events caused by random component failures and human error; internal hazards (e.g., internal fires and floods, turbine missiles) and external hazards, both natural (e.g., earthquakes, high winds, external floods) and human-induced, but non-malevolent (e.g., airplane crashes, accidents at nearby industrial facilities). Also, the scope of the PSA should include potential combinations of external hazards. Examples are seismic, floods, or fire. The screening criteria of hazards shall be acceptable to the CNSC. However, an alternative analysis method to conduct the assessment of external events (internal hazards and external hazards) is acceptable subject to the acceptance by CNSC.

Regarding the quantitative thresholds used in the screening criteria, they need to be aligned with the safety goals for the new plants as defined in RD-337 [5].

3.3 FUKUSHIMA AFTERMATH

The Japanese government concluded that the fundamental cause of the incident was a failure to identify the appropriate magnitude of the tsunami hazard. From the early results of the international task force reports, all external events (not just seismic and tsunami) relevant to NPPs must be identified and the selection of appropriate magnitude for the events must be verified [25].

After the Fukushima event, CNSC convened a Task Force to evaluate the lessons learned and the operational, technical and regulatory implications for Canadian NPPs, and to develop a strategy for prioritization and implementation of corrective measures. The CNSC Fukushima Task Force submitted a report [25] which encompasses actions including, the improvement of the regulatory framework and processes. An action plan was initiated to implement the tasks. As part of the action plan, applicable regulatory documents are being revised. One of the regulatory documents being revised is the S-294 [1]. This revision provides additional requirements and guidance required for upcoming refurbishments and new builds.

The criteria of the S-294 revision are to include:

- A Level 1 and 2 PSA to cover irradiated fuel bay events and multi-unit considerations, as well as plant-wide internal fires, internal floods, seismic events and other external events.
- specific mention of:
the purpose for the PSA methodology and computer codes that are required to be accepted by CNSC and the means by which it may be achieved;
the PSA methodology will verify that the safety goals in RD-337 are met;
the PSA methodology is required to identify dominant contributors to risk, plant vulnerabilities and provide insights into the management of severe accidents;
the means by which sensitivity and uncertainty analysis are to be performed.

4 CONCLUSIONS:

As a direct result of the experience gained from the regulatory review of Canadian PSAs, and participation in international activities in the areas of PSA for the digital I&C, the CNSC initiated the process of deriving the strategy for developing a detailed guidance for probabilistic model of the digital I&C system.

For the computer based systems, the level of simplicity, the model and the inputs for PSA, and the database may have to be defined.³

Regarding the internal and external hazards, the CNSC is defining the expectations for the analysis approach for External Events PSA, the screening criteria, the rationale for exclusion of internal fires, internal floods and seismic events from detailed analysis in the shutdown PSA. This will be part of the regulatory guidance associated with the regulatory standard S-294.

After the Fukushima event, the CNSC regulatory standard for PSA is being revised to include:

- irradiated fuel bay and multi-unit considerations, as well as plant-wide internal fires, internal floods, seismic events and other external events;
- To specifically mention some of the requirements on PSA methodology and the means by which it may be achieved and the means by which sensitivity and uncertainty analysis are to be performed.

The S-294 revision based on CNSC Fukushima Task Force report provides additional requirements and guidance required for upcoming refurbishments and new builds.

REFERENCES AND BIBLIOGRAPHY:


³While international activities are in progress/in place for many of the activities, they may have to be coordinated to integrate for use. Activities have to be triggered for those not having actions in place.


