2021 International Nuclear Atlantic Conference – INAC 2021
Virtual meeting, Brazil, November 29 – December 2, 2021

ISBN: 978-65-594-1256-3

Use of PSA Data for the Performance Specification of Safety Control Systems in Nuclear Power Plants

F. L. A. Schweizer[1], B. N. Warth[1], M. C. Maturana[1]

[1]*fernando.lage@marinha.mil.br*
bruno.napoli@marinha.mil.br
marcos.maturana@marinha.mil.br
Directorate for Nuclear Development of the Navy (DDNM)
São Paulo – Brazil

1. Introduction

Probabilistic Safety Assessment (PSA) is a fundamental part of a Nuclear Power Plant (NPP) licensing process, as license applicants must present the PSA results in Chapter 19 of the Safety Analysis Report, consistent with applicable codes, standards and legislation, to the regulatory body [1, 2]. PSA considers the development and updating of probabilistic models to estimate the risk associated with the operation, allowing the risk monitoring, from the plant design to the plant decommissioning [3]. The Reliability Assurance Program (RAP) complements the overall plant safety assessment and uses the PSA as a basis for cost/benefit analysis and optimization of safety processes during the design phase [4]. In addition, an RAP provides a sound basis for establishing systems technical specifications.

This paper discusses a methodology for specifying the maximum acceptable probability of failure on demand (PFD) and the maximum spurious operation frequency (SOF) of a NPP's Safety Control System (SCS) by exploiting the data presented in its Probabilistic Safety Assessment (PSA) Level 1 [5]. The application in a preliminary case study showed this methodology potential contribution to the specification of an SCS.

2. Methodology

This methodology is presented in four main steps: 1) Isolation of impacting initiating events (IE) – result of PSA; 2) Evaluation of the IE detection, data processing and actuation types, as presented in the plant design; 3) Definition of Risk Acceptance Criteria (RAC), and; 4) Integrated evaluation of SCS reliability performance characteristics. Next section discusses the results of a simplified case study where this methodology was applied.

3. Results and Discussion

In this simplified case study, the SCS and the SCS Diverse (SCS-D) – a system redundant to the SCS, which fulfills some of its critical functions – were considered, as part of an NPP with a Pressurized Water Reactor (PWR), which can be categorized as a Small Modular Reactor (SMR). As this analysis only considers the critical functions indicated by the PSA Level 1 of the plant, it is being considered that, if the SCS fails on demand, the SCS-D will act and control the plant's safety systems.

From the impacting IE data isolated from the PSA Level 1, and from the evaluation of the plant response to this IEs (detection, data processing and actuation) – as presented in the plant design –, it was possible to analyze the PFDs of the SCS and SCS-D.

Preliminary analysis of the PFD for the SCS and the SCS-D

In order to the control systems fail, the SCS failure and the SCS-D failure must occur. Assuming that these systems are independent, the event of failure in the systems demand has its probability calculated below (based on the data presented by the manufacturer):

$$PFD([SCS\ failure\ and\ SCS\text{-}D\ failure]) = 1E\text{-}04 * 1E\text{-}03 = 1E\text{-}07 \quad (1)$$

This data was used to estimate the Core Damage Frequency (CDF) of the plant, considering the IE that involve the performance of the SCS/SCS-D and that were presented in the plant's PSA Level 1. This estimate considers that the probability of failure of other safety systems is null. The frequency of IE considered and their contribution to the CDF are presented in the Table I.

Table I: SCS and SCS-D contribution to the CDF.

IE	***Frequency*** *[/yr]*	***PFD(SCS and SCS-D)***	***CDF*** *[/yr]*
LOOP (Loss of Offsite Power)	7.13E-01	**1.00E-07**	7.13E-08
Loss of Main Feedwater	1.62E-01	**1.00E-07**	1.62E-08
Medium LOCA (Loss-of-Coolant-Accident)	4.68E-04	**1.00E-07**	4.68E-11
Excessive LOCA	6.14E-07	**1.00E-07**	6.14E-14
Small LOCA	5.29E-04	**1.00E-07**	5.29E-11
Steam/Feedline Break	1.19E-02	**1.00E-07**	1.19E-09
Reactor/Turbine trip	6.60E-01	**1.00E-07**	6.60E-08
Steam Generator Tube Rupture	3.25E-03	**1.00E-07**	3.24E-10
Very Small LOCA	1.20E-03	**1.00E-07**	1.20E-10
Large LOCA	1.22E-06	**1.00E-07**	1.22E-13
Total CDF:			1.55E-07

Even assuming as null the failure probabilities of the other safety systems, the Total CDF presents a value in the order of 1E-07, as calculated in Table I. The calculation above can be refined for each IE, considering typical failure probabilities of safety systems (in addition to the failure of the control systems). For the case of IE Loss of Offsite Power (LOOP), the largest contributor to the CDF (among those considered in Table I), the typical PFD for a Diesel Generator Group (DGG) can be assumed to be 2.5E-02 [6]. The plant features 4 emergency DGG, leading to a PFD of 3.91E-07 for the set (all DGGs failure). Thus, the probability of the safety systems failure event, considering the I&C failure (considering independence between the SCS and the SCS-D) or failure in the emergency power system, disregarding the portion of failure probability of all systems (I&C and all the DGGs), is calculated below:

$$PFD([SCS\ failure\ and\ SCS\text{-}D\ failure]\ or\ 4\ DGG\ failure) = (1E\text{-}04 * 1E\text{-}03) + 3.91E\text{-}07 = 4.91E\text{-}07 \quad (2)$$

The *PFD (SCS failure and SCS-D failure)*, previously calculated for the IE LOOP, was replaced by the *PFD ([SCS failure and SCS-D failure] or DGG failure)* in Table I, obtaining a CDF of 4,34E-07/yr. In this refinement example, the impact of not considering the failures of safety systems can be seen. Considering only the failures in the DGG, there was an increase of 2.79E-7 in the Total CDF.

Integrated evaluation of SCS and SCS-D reliability performance characteristics

The refinement ideas discussed in the previous paragraph were applied to each critical IE extracted from the PSA, as illustrated in Table II – this table presents only a part of the analysis (related to the plant's operation at full power). The PSA events were detailed to consider the safety functions performed by SCS and SCS-D – see the first column of Table II.

Table II: Limits for PFD and SOF of SCS and SCS-D.

IE [/yr]		Engineered Safety Features and Auxiliary Systems (ESFAS)																CDF (partial) [/yr]
		Detection performed by (type):						Goal for SCS+SCS-D		Goal for CS		Actuation performed by (type):						
		SCS+SCS-D (automatic)		CS (automatic)		CS (manual)		PFD	SOF [/yr]	PFD	SOF [/yr]	SCS+SCS-D (automatic)			CS (automatic)	CS (manual)		
Inadvertent operation of the Residual Heat Removal Subsystem	1.44E-02	DP2	3.17E-09	DP2	3.17E-09	DP2	3.17E-09	5.17E-04	2.0E-01	5.17E-02	2.0E-01	A4	A6	A1	A2			9.99E-08
Increased feed water flow of a Steam Generator	3.99E-02	DP2	3.17E-09			DP2	3.17E-09	1.0E-05	2.0E-01	1.0E-03	2.0E-01	A4	A6	A1		A4	A6	3.23E-07
Excessive increase in steam flow	1.44E-02	DP2	3.17E-09			DP2	3.17E-09	4.36E-06	2.0E-01	4.36E-04	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Inadvertent opening of the Relief or Safety or Pressure Control Valve of a Steam Generator	1.31E-03	DP2	3.17E-09	DP2	3.17E-09	DP2	3.17E-09	8.47E-04	2.0E-01	8.47E-02	2.0E-01	A4	A6	A1	A2			2.72E-08
Failures in the piping of the steam system in or out of Containment (PWR)	1.30E-02	DP4	3.49E-09			DP4	3.49E-09	7.95E-06	2.0E-01	7.95E-04	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Loss of vacuum in Main Condenser	1.5E-01	DP4	3.49E-09			DP4	3.49E-09	1.0E-05	2.0E-01	1.0E-03	2.0E-01	A4	A6	A1		A4	A6	8.48E-07
Loss of turbine (auxiliary)	1.86E-01	DP4	3.49E-09			DP4	3.49E-09	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	1.16E-06
Loss of external electric power supply and loss of Auxiliary Turbo Generators in alternating current	2.42E-03	DP4	3.49E-09			DP4	3.49E-09	1.60E-04	2.0E-01	1.60E-02	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Loss of feed water from a Steam Generator	1.77E-01	DP2	3.17E-09			DP2	3.17E-09	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	1.11E-06
Breakage of feed water pipe (PWR)	1.9E-01	DP2	3.17E-09			DP2	3.17E-09	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	6.82E-07
Reactor flow loss due to loss of Reactor Coolant Circulation Pumps	2.61E-02	DP4	3.49E-09			DP4	3.49E-09	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	1.63E-07
Rotor locking of a Reactor Coolant Circulation Pump	2.61E-02	DP4	3.49E-09			DP4	3.49E-09	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	1.63E-07
Breakage of a Reactor Coolant Pump Shaft	2.61E-02	DP4	3.49E-09			DP4	3.49E-09	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	1.63E-07
Uncontrolled insertion of positive reactivity by a Control Rod from a sub-critical or low power condition	7.84E-03	DP1	5.42E-08			DP1	5.42E-08	3.20E-05	2.0E-01	3.20E-03	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Uncontrolled insertion of positive reactivity by a Power Control Rod	7.84E-03	DP1	5.42E-08			DP1	5.42E-08	3.20E-05	2.0E-01	3.20E-03	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Incorrect operation or operational error of the reactivity control process	5.75E-02	DP1	5.42E-08			DP1	5.42E-08	1.0E-06	2.0E-01	1.0E-04	2.0E-01	A4	A6	A1		A4	A6	3.63E-07
Control Rod ejection accident	7.84E-03	DP1	5.42E-08			DP1	5.42E-08	3.20E-05	2.0E-01	3.20E-03	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Incorrect operation or operational error of the Coolant Injection System	1.44E-02	DP2	3.17E-09			DP2	3.17E-09	4.36E-06	2.0E-01	4.36E-04	2.0E-01	A4	A6	A1		A4	A6	9.99E-08
Radiological consequences of tube rupture of a Steam Generator (PWR)	3.54E-03	DP7	3.51E-24			DP7	3.51E-24	2.8E-05	2.0E-01	2.8E-03	2.0E-01	A4	A6	A5		A4	A6	A1	9.99E-08
Loss of coolant accidents resulting from spectrum of postulated breakages of Pipes belonging to the pressure barrier of the Reactor Cooling System	2.40E-03	DP7	3.51E-24			DP7	3.51E-24	8.87E-05	2.0E-01	8.87E-03	2.0E-01	A4	A6	A5		A4	A6	A1	9.99E-08
Total CDF																		**2.85E-05**

As noted in Table II, the calculation of the partial CDF (associated with each IE) took into account:

a) *The frequency associated with the IEs*;

b) *The failure probabilities for the different types of detection*, both for systems that operate in an emergency (SCS and SCS-D) and for systems that operate normally (Plant Control System – CS) the types being considered: DP1 (radiation detection with 1 sensor with cable routed signal), DP2 (level detection with 1 sensor with cable routed signal), DP4 (temperature detection with 1 sensor with cable routed signal), DP7 (LOCA detection with 1 sensor with cable routed signal);

c) *PFD and SOF of the possible types of processing*: both systems that operate in an emergency (SCS

and SCS-D) and systems that operate normally – plant Control System (CS); and

d) *The failure probabilities for the different types of actuated equipment*, considering the types: A1 (Cooling), A2 (Injection), A4 (SCRAM), A5 (Containment Isolation) and A6 (Steam Generator Isolation). These probabilities were conservatively calculated for typical arrangements (e.g., for systems with triple redundancy for a given equipment an arrangement with double redundancy was considered). Figure 1 illustrates the typical arrangement considered for equipment type A1.

<table>
<tr><th colspan="3">Tertiary Circuit</th><th colspan="3">Secondary Circuit</th><th colspan="3">Primary Circuit</th></tr>
<tr><td rowspan="2">Heat exchanger</td><td rowspan="2">Pump</td><td>Valve</td><td rowspan="2">Heat exchanger</td><td rowspan="2">Pump</td><td>Valve</td><td rowspan="2">Heat exchanger</td><td rowspan="2">Pump</td><td>Valve</td></tr>
<tr><td>Valve</td><td>Valve</td><td>Valve</td></tr>
<tr><td rowspan="2">Heat exchanger</td><td rowspan="2">Pump</td><td>Valve</td><td rowspan="2">Heat exchanger</td><td rowspan="2">Pump</td><td>Valve</td><td rowspan="2">Heat exchanger</td><td rowspan="2">Pump</td><td>Valve</td></tr>
<tr><td>Valve</td><td>Valve</td><td>Valve</td></tr>
<tr><td colspan="9">Electric Power</td></tr>
</table>

Figure 1: Typical arrangement considered for equipment type A1.

4. Conclusions

Considering the Total CDF targets established for the plant (less than 1.00E-04/yr), it was possible to use Table II as an instrument for defining the PFD and SOF target associated with the SCS and SCS-D – i.e., which values would be acceptance limits. Thus, the reliability data submitted by the manufacturer were evaluated and compared to the plant design requirements.

It is noteworthy that this work is not considering the dependence between the SCS and the SCS-D. These systems, however, have a strong dependency (given the impossibility of installing additional sensors and actuators for the SCS-D in the plant). Therefore, the data presented by the manufacturer must consider these dependencies so that the verification reflects the real condition of the plant.

Another point to highlight is the consideration only of events internal to the plant that require the SCS/SCS-D – events such as fire, flood, earthquake, and other events external to the plant were disregarded.

Acknowledgements

The authors would like to acknowledge the Directorate for Nuclear Development of the Navy (DDNM) for supporting their participation in INAC 2021.

References

[1] USNRC, *Standard Review Plan: Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors, NUREG-0800, Section 19.0, Draft Revision 3,* United States Nuclear Regulatory Commission, Washington, DC, USA (2014).

[2] CNEN, *Licenciamento de Instalações Nucleares, CNEN NE 1.04,* Comissão Nacional de Eneria Nuclear, Rio de Janeiro, Brazil (2002).

[3] USNRC, *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, Regulatory Guide 1.200, Rev. 2,* United States Nuclear Regulatory Commission, Washington, DC, USA (2009).

[4] IAEA, *Reliability assurance programme guidebook for advanced light water reactors, IAEA-TECDOC-1264,* International Atomic Energy Agency, Vienna, Austria (2001).

[5] IAEA, *Design of Instrumentation and Control Systems for Nuclear Power Plants Specific Safety Guide, IAEA-SSG-39,* International Atomic Energy Agency, Vienna (2016).

[6] USNRC, *Station Blackout, Regulatory Guide 1.155*, United States Nuclear Regulatory Commission, Washington, DC, USA (1988).