Development and Primary Application of a Level 2 PSA Methodology in a Small Nuclear Plant design

Nathalia Nunes Araujo[a], Maritza Rodriguez Gual[b], Ulisses Alves Maciel Neto[c], Marcos Coelho Maturana[d] and Marcelo Ramos Martins[e]

[abcde] Analysis, Evaluation and Risk Management Laboratory (LabRisco), São Paulo, Brazil,

[a] nathalia.nunes@labrisco.usp.br

[b] maritza.gual@labrisco.usp.br

[c] ulisses.neto@labrisco.usp.br

[d] marcos@labrisco.usp.br

[e] marcelo@labrisco.usp.br

Abstract: In the nuclear plant licensing process, a qualitative and quantitative analysis of the probability, progression, and consequences of transients and accident conditions must be performed to estimate the risk to public health. Probabilistic Safety Assessment (PSA) is a method widely used in the nuclear industry that numerically quantifies risk and is performed at three different levels. The Level 2 PSA addresses the phenomenological and physical events that can occur during the core meltdown to containment failure. The methodology of a Level 2 PSA must contain a clear definition of the steps, procedures, and reviews to be carried out in accordance with the standards and guidelines recommended by the International Atomic Energy Agency. This paper describes the development of a Level 2 PSA methodology for a small nuclear power plant design. Deterministic modeling of the accident progression is also considered, being essential for the construction of the sequence of events and subsequent management measures. Along with the development, a primary application of the methodology is being carried out to identify improvements.

1. INTRODUCTION

Nuclear reactor design trends have changed over the years. Small and medium-sized reactors (SMR) are expected to play a significant role in the future energy market. Electricity generation is the main objective of nuclear power plants but ongoing research has demonstrated the ability to use SMR in numerous other applications such as water desalination and floating nuclear power plant [1] [2].

Probabilistic Safety Analysis (PSA) of a nuclear power plant is a methodology used to study and manage risks related to accidents that degrade the reactor core and release fission products into the environment. PSA is performed at three levels; PSA Level 2 is responsible for analyzing the progression of sequences of damage to the core, providing data on the frequencies and consequences of damage.

A nuclear plant has two main operating states: full power and low power and shutdown (LPSD). Studies on the modeling of the nuclear plant in LPSD have shown that, in some cases, the risk of releasing fission materials into the environment is comparable to that associated with operating at full power [3] – even considering most of the operating time at full power. Level 2 PSA in LPSD is intended to determine the potential risk of loss of long-term decay heat removal systems during a plant shutdown for refueling and provide insights into potential plant vulnerabilities. The information obtained is used to develop risk management and accident control guidelines.

The development of a PSA is recommended by the International Atomic Energy Agency (IAEA) [4] and is required by many regulatory bodies as a complementary analysis to the Final Safety Analysis Report (FSAR). In Brazil, the Nuclear Regulatory Commission (CNEN) has PSA requirements and procedures to manage the plant under severe accident conditions [65] but has no specific standard or recommendation for SMR.

The main objective of the work is to define the scope of the modelling of a Level 2 PSA in the study of a loss of coolant circulation accident in the LPSD in an SMR. The reference SMR is a two-circuit pressurized water reactor (PWR) with an electrical capacity of 10 MWe. The description and initial steady-state conditions were presented in previous works [6][7].

2. METHODOLOGY

The development and application of the Level 2 PSA methodology is part of a program of qualification of specialists of the Laboratory of Analysis, Assessment and Risk Management (LabRisco) to carry out simulations and probabilistic analyzes of an SMR. The methodology developed and proposed for LPSD, described in detail in [8] and developed according to the specific literature [5], is divided into six steps:

Step 1: Selection of initiating events (EI);
Step 2: Grouping of possible accidents;
Step 3: Analysis of accident progression and development of event trees;
Step 4: Identification of therelease category (RC);
Step 5: Analysis of source terms (ST);
Step 6: Calculation of the Large Early Release Frequency (LERF).

3. IDENTIFICATION OF SEVERE ACCIDENT SCENARIO

A large number of sequences that can lead to core damage have been identified in Level 1 PSA [9] and grouped according to similarities and configurations of the plant and systems. Table 1 presents the grouping performed.

In LPSD, the reactor configuration changes as a function of time, unlike the full power state. Maintaining the cooling capacity of the reactor core and spent fuel pool (SFP) before and during fuel movement, reactor preparation, full discharge of spent fuel, refilling of the new fuel, and assembly and preparation for return to operation are considered.

Table 1: Grouping of sequences of events

Group number	Event	Main characteristics	Frequency of CDF(/yr)	Percentage of CDF in the LPSD
1	Loss of coolant circulation in the SFP	Fuel transfer, part of the Fuel is in the SFP	2.54E-06	5.60%
2	Loss of coolant circulation in the SFP	All fuel in SFP	2.54E-05	55.98%
3	Loss of coolant circulation in the reactor core	All fuel is in the reactor core. Reactor vessel head closed	1.46E-05	32.14%
4	Loss of coolant circulation in the reactor core	Fuel transfer, part of the fuel in the reactor core. Reactor vessel head open	2.85E-06	6.28%

Group numbers 2 and 4 have been studied in [10] and [8], respectively. The analysis in this work corresponds to group 3, the second with the highest frequency of occurrence.

For LPSD with a closed reactor vessel and closed containment, the molten core accident phenomena are similar to the sequences that occur in full power mode. Therefore, under these conditions, the greatest risk would be attributed to the cold shutdown stage before refueling – due to the unavailability of high-pressure mitigation systems and reduced water inventory inside the reactor vessel in combinationwith the higher thermal decay power [11].

4. NUCLEAR SYSTEMS

To maintain the operational and safe conditions of the plant during the LPSD, the reactor cooling and safety systems must be in continuous operation. Figure 1 presents the components of the main systems required in this state. The accident of loss of coolant circulation in the reactor is caused by the total failure of the Residual Heat Removal System (RHRS).

4.1. Residual heat removal System (RHRS)

RHRS is designed to remove decay heat from fuel elements caused by the decomposition of fission products. The system starts operating when the reactor coolant reaches hot shutdown parameters. The RHRS is composed of two independent and redundant trains, each one connected to a hot leg and a cold leg of the primary circuit. Only one RHRS train is needed to remove the decay heat generated by the fuel in the reactor vessel, leaving the second train on standby.

Each RHRS train has a reactor coolant pump (B01/B02) and a heat exchanger (TC1/TC2), as shown in Figure 1. Pumps B01/B02 take suction from the hot leg, pass through the heat exchangers TC1/ TC2, where it is cooled, and then injected back into the reactor vessel through the cold leg. The TC1/TC2 heat exchangers are cooled by B03/B04 cooling pumps, which take suction from the shielding pool and discharge the heated water back to the shielding pool. The V01-V12 valves provide isolation, alignment, and control of the RHRS.

4.2. Reactor Cooling System (RCS)

The RCS provides primary cooling for the vessel and the reactor core, but in the LPSD some system components are isolated. In the LPSD, the reactor vessel is protected against overpressure during transients by two automatic depressurization system (ADS) valves, ADS1 and ADS2, installed on the pressurizer (PZR) and set to open at a pressure lower than the design basis of the plant. Both valves discharge into the relief tank.

4.3. Coolant Injection Subsystem (CIS)

The Coolant Injection Subsystem (CIS) is part of the Water Purification System (WPS) and provides replenishment of demineralized water to the reactor. The circuit is capable of replacing small leaks at a pressure greater than the opening pressure of the safety valves, ADS1 and ADS2. The CIS operates continuously throughout the entire operation and state of the nuclear plant.

4.4. H2 Inertization System (HIS)

The H2 Inertization System (HIS) consists of Passive Autocatalytic Recombiners (PAR), safety devices that combine hydrogen (H2) and oxygen (O2) to produce steam (H2O), providing H2 control and mitigation. PARs are designed to reduce the concentration of H2 accumulation below the safe concentration limit, providing inertization to the interior of the containment building and preventing explosions and combustions.

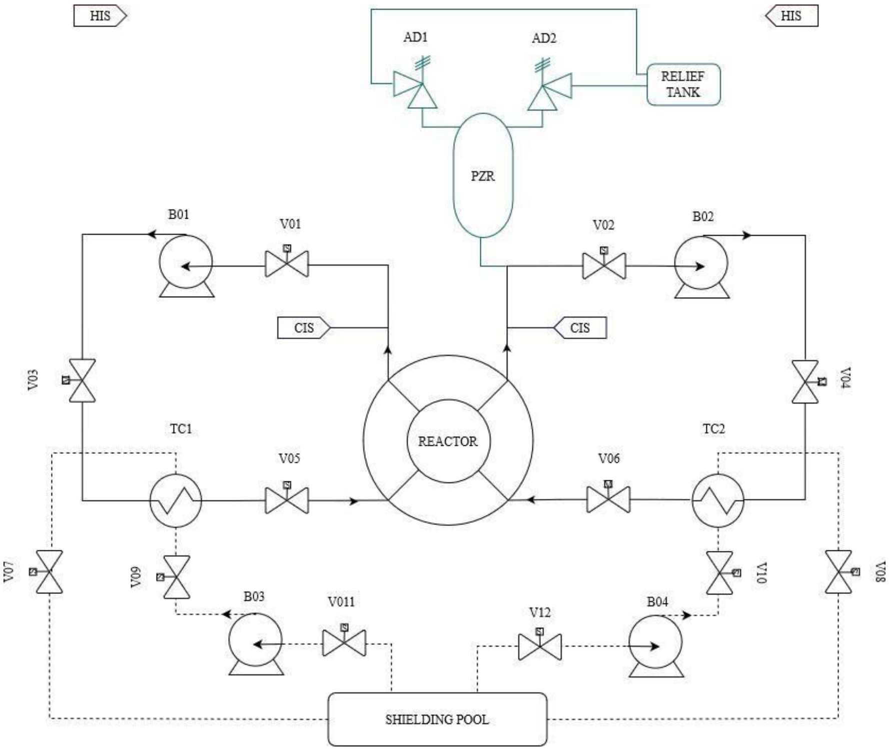


Figure 1: Systems diagram

5. RESULTS AND DISCUSSION

Data Analysis

Due to a lack of operating experience (e.g., reliability data), the database used for failure rates is composed of generic industry data, probabilistic risk assessment data from published similar nuclear power plants, and NUREG/CR-6928 [12]. All component failures are considered repairable. The average repair time is considered 18 hours. As the study develops, generic SMR data and data obtained from the reference SMR are added and incorporated into the model, generating more realistic results.

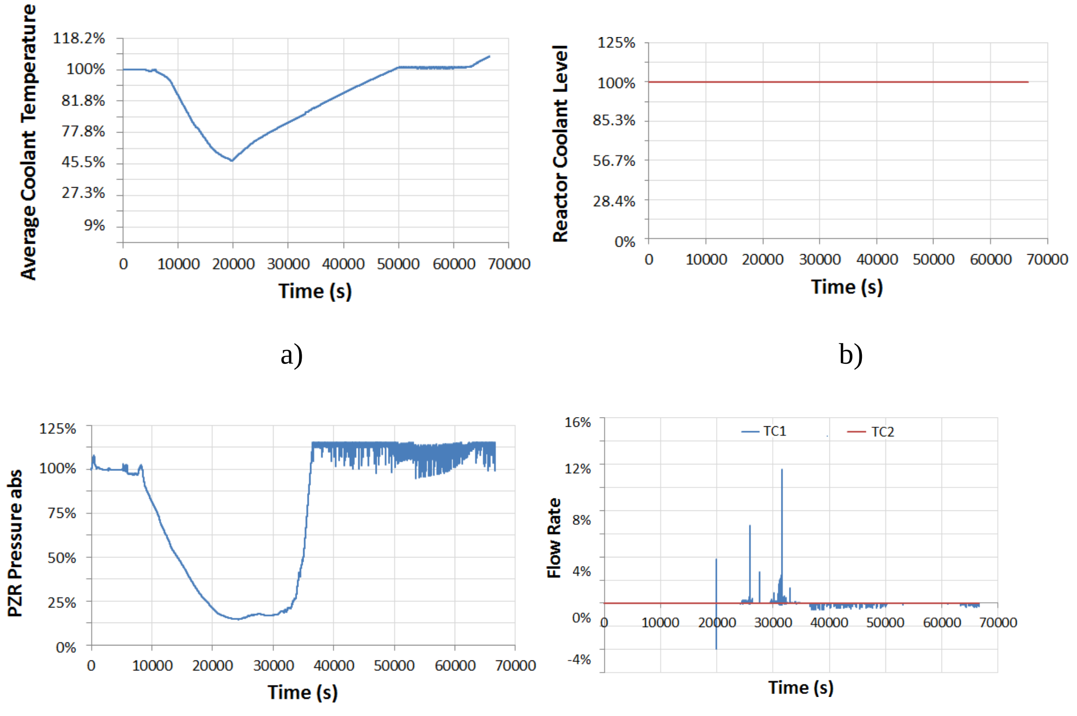
Common Cause failures (CCFs)

The RHRS is identified as the second-highest contributor with respect to core damage from the system in the LPSD (for the reference design). The top common cause of failure (CCF) is the RHRS pumps B01 and B02 failing to run. Since the success of decay heat removal during LPSD is dependent on the success of at least one RHRS train, a loss of both trains will lead directly to core damage.

Expected event progression

After the normal shutdown of the reactor, the trip of the turbines, and the scram of the control/safety bars, the RHRS started its operation when the reactor reached the operating reference temperature and pressure. The total failure of the RHRS system causes a loss of coolant circulation in the reactor. Steam generators are not available for emergency cooling. Figure 2 shows the initial progression of the accident – first, the reactor temperature and pressure began to rise; then, the PRZ ADS valves began a continuous opening and closing process; after that, the coolant inventory was lost by opening and closing valves is replenished by the CIS.

The RHRS was considered to fail when it goes into operation - approximately 5-6 hours after normal plant shutdown, i.e. with the highest possible decay heat for a more conservative analysis.



a) b)

c) d)

Figure 2: a) Average coolant temperature, b) Reactor coolant level, c) PZR pressure abs c) Flow rate. Parameter values were normalized according to full power operation values (100%). Simulations performed in RELAP [13]

Event tree construction

An event tree graphically models the various accident scenarios that can occur as a result of an event, based on the success or failure of structures, systems, and components as the event progress – the preceding paragraphs show the designed event progression. The progression of the accident of loss of coolant circulation in the reactor core due to loss of RHRS was evaluated through an event tree, Figure 3, using the Computer-Aided Fault Tree Analysis (CAFTA) [14].

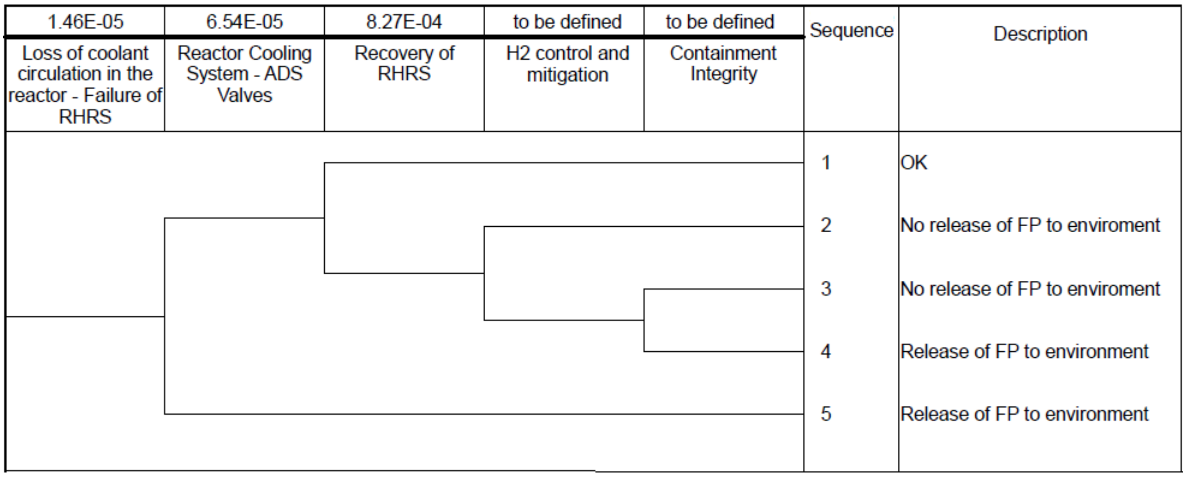

1.46E-05
6.54E-05
8.27E-04
to be defined
to be defined
Sequence
Description
Loss of coolant circulation in the reactor - Failure of RHRS
Reactor Cooling System - ADS Valves
Recovery of RHRS
H2 control and mitigation
Containment Integrity
1
OK
2
No release of FP to enviroment
3
No release of FP to enviroment
4
Release of FP to environment
5
Release of FP to environment

Figure 3: Event Tree

Fault tree analyses and quantification

Fault Trees use logic diagrams used to estimate the probabilities of event occurrences, both in risk analysis and in reliability calculations. They are used in addition to event trees, in assessing the probability of occurrence of each event in the accident sequences.

A detailed fault tree model was developed, using CAFTA [14], for the systems identified as needed during the course of the accident and quantified using PRAQuant version 5.2 [15]. Random failure, test and maintenance, and common cause failure events were modeled for each component as needed. Figures 4 and 5 show the fault trees of the RHRS and ADS valves system. The reliability of the CIS was not modeled, its operation is continuous in all states of operation of the reactor.

The reliability of the realignment of the RHRS recovery was obtained through the probability of human error presented in [16], considering the characteristics and cognitive processes of human actions associated with the execution of a procedure, and the use of information in situations other than that of obtaining knowledge. An application of this data (of human error probability) is found in [17].

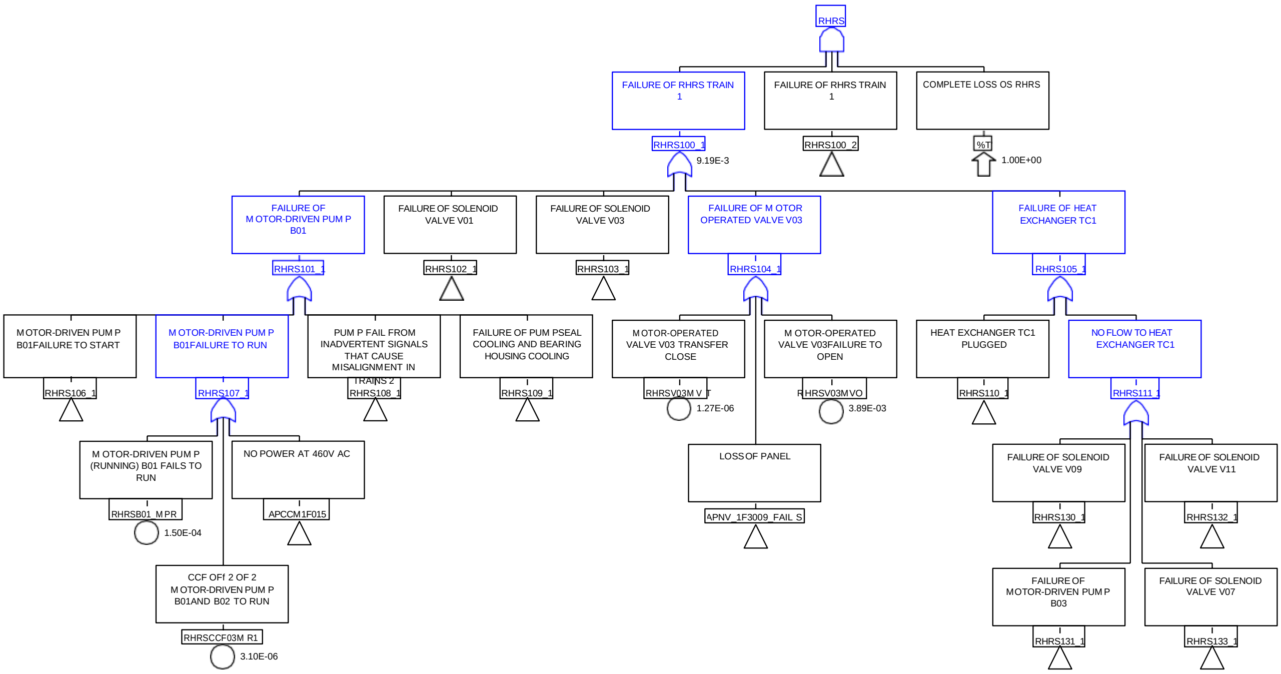

RHRS
FAILURE OF RHRS TRAIN 1
RHRS100_1
9.19E-3
FAILURE OF RHRS TRAIN 1
RHRS100_2
COMPLETE LOSS OS RHRS
%T
1.00E+00
FAILURE OF M OTOR-DRIVEN PUM P B01
RHRS101_1
FAILURE OF SOLENOID VALVE V01
RHRS102_1
FAILURE OF SOLENOID VALVE V03
RHRS103_1
FAILURE OF M OTOR OPERATED VALVE V03
RHRS104_1
FAILURE OF HEAT EXCHANGER TC1
RHRS105_1
M OTOR-DRIVEN PUM P B01FAILURE TO START
RHRS106_1
M OTOR-DRIVEN PUM P B01FAILURE TO RUN
RHRS107_1
PUM P FAIL FROM INADVERTENT SIGNALS THAT CAUSE MISALIGNM ENT IN TRAINS 2
RHRS108_1
FAILURE OF PUM PSEAL COOLING AND BEARING HOUSING COOLING
RHRS109_1
M OTOR-OPERATED VALVE V03 TRANSFER CLOSE
RHRSV03M V T
1.27E-06
M OTOR-OPERATED VALVE V03FAILURE TO OPEN
RHRSV03MVO
3.89E-03
HEAT EXCHANGER TC1 PLUGGED
RHRS110_1
NO FLOW TO HEAT EXCHANGER TC1
RHRS111_1
M OTOR-DRIVEN PUM P (RUNNING) B01 FAILS TO RUN
RHRSB01_M PR
1.50E-04
NO POWER AT 460V AC
APCCM1F015
LOSS OF PANEL
APNV_1F3009_FAIL S
FAILURE OF SOLENOID VALVE V09
RHRS130_1
FAILURE OF SOLENOID VALVE V11
RHRS132_1
CCF OFf 2 OF 2 M OTOR-DRIVEN PUM P B01AND B02 TO RUN
RHRSCCF03M R1
3.10E-06
FAILURE OF MOTOR-DRIVEN PUM P B03
RHRS131_1
FAILURE OF SOLENOID VALVE V07
RHRS133_1

Figure 4: RHRS Fault Tree

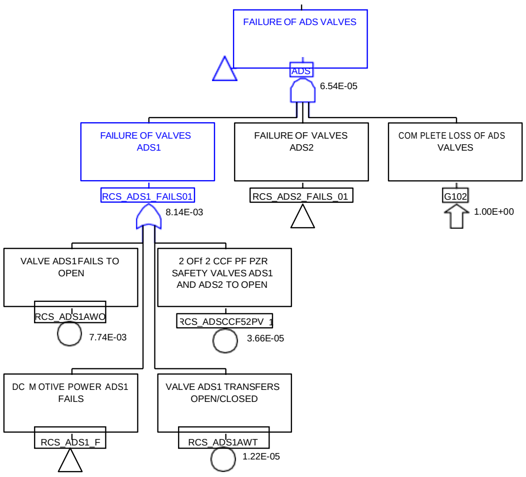


Figure 5: ADS Fault Tree

Final Sequences

In sequence 1 there was no core damage and fission products (FP) released to the environment. With the RHRS recovered, the reactor cooling was successful. The RHRS recovery becomes more effective in cases where the RHRS failure occurs hours after the start of its operation, i.e., the reactor heat has already decayed significantly. The data obtained in this paper allowed the preliminary calculation of the frequency of sequence 1, 1.30E-05 /yr. From this data, it is possible to determine that the sum of the frequency of the other sequences is less than 1.56E-06/yr, which represents important information to the large early frequency release (LERF).

In sequences 2 to 4, with the failure to recover the RHRS, the ADS valves opening and closing process continued until the CIS flow was not enough to replace the lost inventory. Without the action of other protection and safety systems, the reactor core was uncovered and H2 was produced due to the oxidation of the cladding. HIS are essential to prevent combustion, helping to maintain containment integrity. In the event of a failure in the HIS, explosions and combustion can occur, challenging the integrity of the containment. Other severe accident phenomena can also challenge containment, such as increased pressure in containment, and direct heating by corium. These phenomena have been integrated in a simplified way in the event tree.

Accidental sequence 5 occurred at high pressure, due to the failure of the ADS valves to open. Due to high reactor pressure, the RHRS system cannot operate when recovered. The reactor vessel quickly fails and releases radioactive material into containment. In such cases, ejection of the molten core at high pressure can cause direct containment heating and failure.

6. CONCLUSION

This study identified the possible combinations of RHRS failures that could lead to the release of FP into the environment. These results are preliminary, considering the methodology is under development, and for future studies, the event and fault trees will be improved to generate more results and expand the research.

Although the results are preliminary, the analysis of the loss of coolant circulation in the reactor core due to the failure of the RHRS with all the fuel in the reactor core and in the closed reactor vessel head in an SMR project demonstrated the need for further investigation in the study of RHRS and safety and emergency systems

The focus of this study is to acquire knowledge on the application of PSA to new SMR projects, but it can be used for other purposes, such as supporting the updating of reactor safety analysis reports with useful information about systems and components. Posteriorly, with the experience gained in this study – resulting in a better understanding of the phenomena involved in the accident and of the working with CAFTA – the researchers will simulate different types of accidents, to study the action of safety important equipment system and how to mitigate the consequences of the accident. In addition to bringing these preliminary results, this work is also important due to the lack of information available on level 2 PSA dedicated to an SMR designed with an electrical capacity less than 10 MWe.

Acknowledgements

The authors would like to thank Mr. Pedro Maia Vinhas for his support in the deterministic analysis ofthe accidents.

References

[1] D. T. Ingersoll, Z. J. Houghton, R. Bromm, C. Desportes. "*Integration of NuScale SMR With Desalination Technologies*" Proceedings of the ASME 2014 Small Modular Reactors Symposium.
Washington, DC, USA, 2014.

[2] S.E. Hirdaris, Y.F. Cheng, P. Shallcross, J. Bonafoux, D. Carlson, B. Prince, G.A. Sarris, C*onsiderations on the potential use of Nuclear Small Modular Reactor (SMR) technology for merchant marine propulsion*", Ocean Engineering, volume 79, pp 101-130, 2014.

[3] International Atomic Energy Agency, "*Advances in Small Modular Reactor TechnologyDevelopments*", Advanced Reactors Information System, 2020.

[4] International Atomic Energy Agency, "*PSA for the shutdown mode for nuclear power plants*",
Proceedings of a Technical Committee meeting, 1992.

[5] International Atomic Energy Agency, "*Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*", Specific Safety Guide No. SSG-4, 2010.

[6] Brazilian National Commission of Nuclear Energy, *Quality Assurance for Safety in NuclearPower Plants and Other installations* - CNEN-NN-1.16, 2000.

[7] N. N. Araújo, M. C. Maturana, M. R. Gual, "*MELCOR steady state calculation of the generic PWR of 40MWth*", Brazilian Journal of Radiation Sciences, Vol. 8, No. 3A, 01-19, 2020.

[8] N. N. Araujo, M. R. Gual, M. C. Maturana, M. R. Martins, "*Unmitigated severe accident analysisfor a PWR using MELCOR*", Progress in Nuclear Energy, Vol 128, 103461, 2020.

[9] H. C. Romberg, N. N. Araujo, M. R. Gual, M. C. Maturana, M. R. Martins, "*Shutdown Level 2 PSA Methodology for a Small Modular Reactor*", Proceedings of International Topical Meeting on Probabilistic Safety Assessment and Analysis, 2021.

[10] M. R. Martins, P. F. F. Melo, M. C. Maturana, "*Methodology for system reliability analysis during the conceptual phase of complex system design considering human factors*". Proceeding of the ANS PSA 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis, 2015.

[11] N. N. Araújo, M. R. Gual, M. C. Maturana, "*Spent fuel pool severe accidents modeled with MELCOR to support a PSA level 2*" Phenomenology, Simulation and Modelling of Accidents in SpentFuel Pools, IAEA-TECDOC-1949, 2021.

[12] H. Löffler, E. Raimond, “*Final guidance document for extended Level 2 PSA*”, Technical reportASAMPSA_E / WP40 / D40.7 / 2017-39, Vol 1, 2016.

[13] U.S. Nuclear Regulatory Commission, “*Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*”, NUREG/CR-6928 (INL/EXT-06- 11119), U.S., Washington, DC, 2007.

[14] U.S. Nuclear Regulatory Commission, “*The RELAP5 Development Team – RELAP5/MOD3 Code Manual; Volume 1: Code Structure, Systems Models and Solution Methods*”,NUREG/CR-5535; INEL-9510174, 1995.

[15] Electric Power Researc Institute, Fault Tree Analysis System CAFTA Software Manual, Version 5.4, 2009.

[16] Electric Power Researc Institute, PRAQUANT Software Manual, Version 5.2, 2015.

[17] M. C. Maturana, “*Application of Bayesian Networks in the human error contribution analysis of collision accidents*”, Thesis, Polytechnic School of the University of São Paulo, 2010.

[18] M. R. Martins, M. C. Maturana, “*Application of Bayesian Belief networks to the human reliability analysis of an oil tanker operation focusing on collision accidents*”, Reliability Engineering& System Safety 110, 89-109, 2013.