BJRS

BRAZILIAN JOURNAL
OF
RADIATION SCIENCES
10-03A (2022) 01-17

SBPR
Sociedade Brasileira de Proteção Radiológica

Risk-based design of electric power systems for non-conventional nuclear facilities at shutdown modes

Borsoi[a] S. S., Baroni[b] D. B., Mattar Neto[c] M., Oliveira[c] P. S. P., and Maturana[d] M. C.

[a] *University of São Paulo - USP, 05508-000, São Paulo, SP, Brazil*

[b] *Navy Technological Center in São Paulo - CTMSP, 05508-000, São Paulo, SP, Brazil*

[c] *Nuclear and Energy Research Institute – IPEN-CNEN, 05508-000, São Paulo, SP, Brazil*

[d] *Analysis, Evaluation and Risk Management - LABRISCO, 05508-970, São Paulo, SP, Brazil*

e-mail address of the corresponding sadborsoi@usp.br

ABSTRACT

The work presents a methodology for assessing the safety of electrical system designs for non-conventional nuclear facilities in shutdown. The methodology adopts the core damage frequency as the main risk measure to assess the different architectures of power systems in a non-conventional nuclear facility. Among the reasons is the absence of a specific regulatory basis for this type of installation. The adoption of standards for nuclear power plants by non-conventional nuclear facilities does not take into account the functional and operational particularities of these installations, imposing criteria that are often overestimated, which can even lead to an increase in the financial risk for carrying out the projects. Safety probabilistic analyzes become essential tools for the facilities design and licensing. The modeling and quantification of systems failures in charge of ensuring the nuclear safety of non-conventional nuclear facilities are carried out in the CAFTA software environment. In these studies, the analysis of electrical system configurations and their influence on the overall risk of the installation stand out.

Keywords: **Safety probabilistic analysis, risk-based design, core damage frequency, non-conventional nuclear facilities.**

ISSN: 2319-0612
DOI: https://doi.org/10.15392/2319-0612.2022.2063
Submitted: 2022-05-16
Accepted: 2023-01-18

1. INTRODUCTION

Electric power systems reliability is of paramount importance for safe operation of nuclear power plants (NPPs) and impacts the probability of occurrence of a Station Blackout (SBO) event, which is characterized by the loss of all alternating current power supply to plant safety busbars. Since the Fukushima Daiichi accident in 2011, there has been an increase in nuclear scientific community's perception of the need to improve electric power supply reliability level to ensure safe shutdown of nuclear reactors [1-2].

In Brazil, non-conventional nuclear facilities, such as onshore prototypes of a nuclear reactor for naval propulsion and shipyards that support nuclear submarines, do not have specific normative design basis defined by the nuclear regulatory authority. Consequently, for these non-conventional facilities, codes and standards applicable to NPPs have been used, imposing rigorous safety requirements and impacting projects financial feasibility. To comply with GDC 17, established by the U.S.NRC in Appendix A of 10CFR50 [3], power supply from transmission system must be guaranteed by at least two transmission lines (TLs) distributed in different towers. Assembling TLs in isolated and difficult to access places, such as hills and slopes, may lead to high deployment costs. In addition, transmission systems are subject to transient phenomena that can be induced, for example, by atmospheric discharges, activation of inductive loads (motors and transformers), switching capacitors, sustained power failure etc. Problems associated with monitoring, events location and corrective maintenance are also factors to be highlighted. Based on quality indicators provided by the Brazilian National Electrical System Operator (ONS) [4], it is observed that TLs contribute, approximately, with 70% of the failures attributed to loss of offsite power.

It is important to mention that loss of offsite power, which may involve transmission systems, is not considered an accident initiating event (IE) for non-conventional nuclear facilities that, at power mode, operate isolated from offsite power systems. For these facilities, power generated from nuclear reaction supplies electric power to plant internal systems. Therefore, a reactor trip induced by loss of offsite power is not a credible event for this operating mode. On the other hand, during shutdown mode, non-conventional nuclear facilities depend on offsite power sources to supply their safety busbars and loss of offsite power is considered an accident IE for the safety analysis of these

facilities. In addition, loss of offsite power is a contributor to an SBO scenario, imposing operational restrictions that may increase plant overall risk. Thus, alternative design solutions must be implemented and submitted to the licensing authority, to prove that such solutions are reliable and may increase electric power availability up to a level compatible with the electric power system architecture established in GDC 17 [1]. This work aims to present a probabilistic approach to assess electric power systems safety for non-conventional nuclear facilities during shutdown mode, in particular for refuelling outage. Based on the results of this assessment, the risk associated with loss of long-term residual heat removal in the reactor and loss of cooling in the spent fuel storage can be determined.

2. MATERIALS AND METHODS

2.1. General aspects of non-conventional nuclear facilities at shutdown modes

Onshore prototypes of nuclear reactor for naval propulsion have operational and design characteristics similar to those of a submarine, since at power mode they operate isolated from the offsite power grid and the reactor is inside a metallic hull. On the other hand, shipyards that support nuclear submarines are facilities where there are not reactors. However, when a nuclear submarine berths for refueling or high-level maintenance (reactor in shutdown mode), nuclear safety responsibility is transferred to the shipyard operating organization.

According to NUREG-1499 [5], the low power and shutdown regime of a nuclear facility comprises the period in which the reactor is in a subcritical state or in a transition state from subcriticality to power operation up to 5% of the rated value. In addition, NUREG-1499 [5] contains evaluations only for conditions in which the fuel is inside the Reactor Vessel (RV). Thus, the guide addresses all aspects of the Nuclear Steam Supply System (NSSS), containment and NSSS support systems. Moreover, the assessment performed in NUREG-1499 [5] does not include events that involve handling of the fuel outside containment and the fuel located in the storage building. In this work, the analysis will not be limited to the fuel inside the RV but will cover the fuel located in the Spent Fuel Storage Pool (SFSP) during refueling outages. The movement of spent fuel from the RV to SFSP is carried out by means of the Fuel Exchange Machine (FEM). Figures 1 and 2 illustrate, respectively, the nuclear reactor section of an onshore prototype for naval

propulsion and the shipyard structures involved during refueling outages of a nuclear submarine. Structures used during the refueling outage are the same for the two facilities.

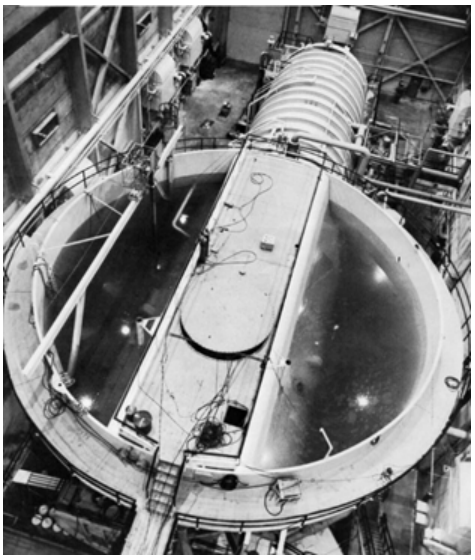

Figure 1: *Nuclear reactor section of an onshore prototype for naval propulsion*
Source: http\\ans.org [6]

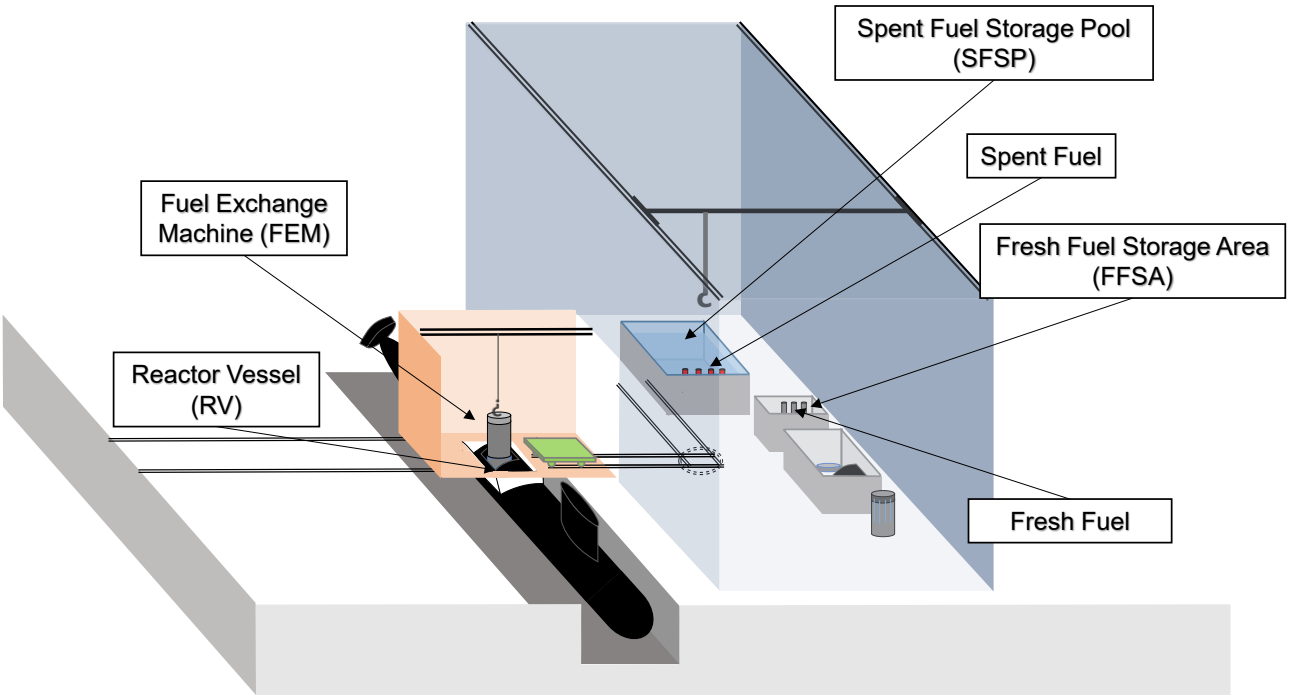

Figure 2: *Shipyard structures used during refuelling outages.*

2.2. Plant configurations at shutdown mode

The methodology proposed in this study consists of assessing the impact of modifications in the electric power systems configuration on the risk associated with a non-conventional nuclear facility during shutdown mode in refueling outages. For this purpose, the Probabilistic Safety Assessment (PSA) previously developed for this facility will be used. In this case, the measure to be adopted to assess the risk is core damage frequency (CDF) and the PSA considered in this study is a Level 1 PSA for internal events and shutdown mode. The shutdown PSA included the modelling of plant structures, systems, and components that are relied upon to maintain plant parameters within a safe-stable state during refueling outages. This involved the following front-line systems: Residual Heat Removal System (RHRS) and Primary Fuel Pool Cooling System (PFPCS). Additionally, Safety Water System (SWS), Primary Component Cooling System (PCCS), Secondary Fuel Pool Cooling System (SFPCS), and AC and DC Electrical Systems serve as secondary/support systems for the success of the core decay heat removal function.

During shutdown mode, some distinct plant configurations may be considered, depending on the activities performed during fuel movement in the core and the maintenance procedures. Therefore, the shutdown PSA developed for refueling outage may cover five distinct phases, as shown in Table 1:

Table 1: Phases of plant shutdown mode.

Phase	Description	Fuel Location	Front-line System	Duration (days)
I	Core cooldown	RV	RHRS	15
II	Spent fuel movement/offload	RV/SFSP/FEM	RHRS/PFPCS	5
III	Full spent fuel unload	SFSP	PFPCS	20
IV	Fresh fuel movement/reload	FFSA/FEM/RV	-	5
V	Preparation to restart with fresh fuel	RV	-	15

As shown in Figure 3, refueling outage for the facility under study is assumed to last 40 days, starting in phase I after reactor shutdown, and ending in phase V when the reactor can be restarted with fresh fuel placed in the core.

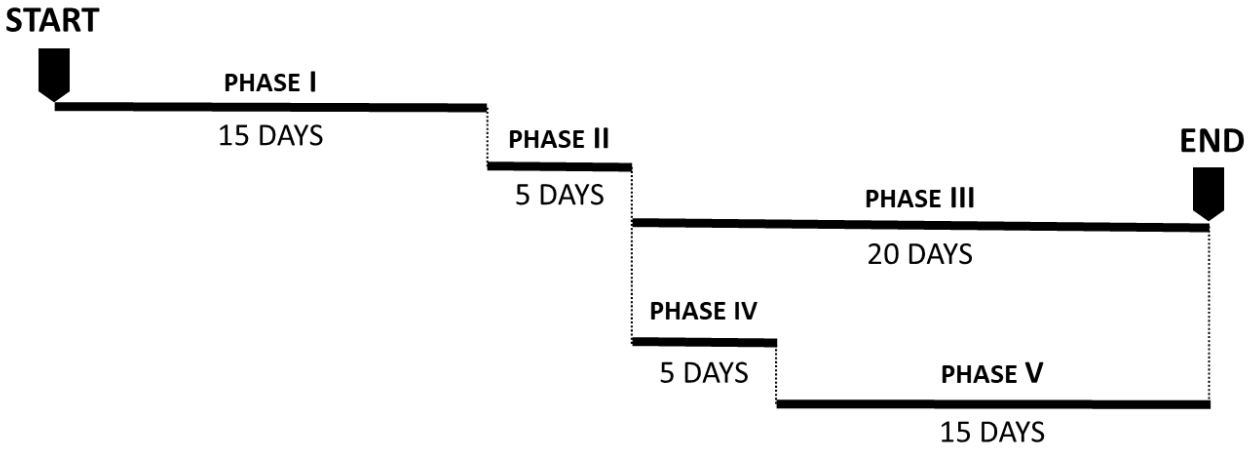

Figure 3: *Chronological sequence of refuelling outage phases.*

An accident with fresh fuel may be assumed unlikely, as well as an accident during the spent fuel movement from RV to SFSP, since the FEM transports only one fuel element at a time. It is noteworthy that the analysis performed for Phase III shall comprise the time taken during Phases IV and V. The risk analysis associated to any other plant operation mode except the ones shown in Figure 3 was out of scope of this work.

2.3. Application of Level 1 PSA methodology

The Shutdown PSA considered in this work was developed in accordance with the procedures for development and application of Level 1 PSA recommended in IAEA Specific Safety Guide No. SSG-3 [7]. The main steps of the analysis included: (1) identification of IE; (2) event tree analysis; (3) fault tree analysis; (4) accident sequences quantification; (5) data and human reliability analysis; and (7) results analysis. Besides, modifications to the models originally developed for the facility were evaluated to reflect proposed changes in electric power systems configuration. Therefore, these modifications comprised, mainly, revision of systems fault tree models so that they could represent new configurations proposed for the electric power systems. Review and updating of electric power systems component data, including component failure rates/probabilities and factors associated with common cause failures, were important tasks performed. Revised and updated values were incorporated into the PSA model implemented in CAFTA [8], which was the computer code used in this study. Thus, new estimates for the reliability of electric power systems were

obtained, impacting both the failure probability of support functions performed by these systems during an accident sequence as well as the frequency of occurrence of accident IE caused by loss of electric power. Reliability data incorporated in this PSA are mainly based on generic data published on U.S.NRC website (https://nrcoe.inl.gov/) [9].

Components of the PSA model implemented in CAFTA [8] were those of a generic onshore prototype of nuclear reactor, which are similar to those used in shipyards. The difference lies on the shielding pool in the prototype, as when the submarine is in a dry dock, there is no water around the reactor section. However, a very similar system formed by pumps, heat exchangers and valves also perform the cooling of the residual heat removal system from the reactor in the case of a docked submarine.

The Shutdown PSA was based on detailed fault tree models for systems that were considered in the event tree logic developed for shutdown operations. These fault trees included the modeling of support systems, such as power supply and cooling systems, which are necessary for the operation of the front-line systems. These support systems were also analyzed in specific detailed fault trees. These detailed fault tree models were then used to generate cut sets for the master fault tree top event.

Table 2 lists the IE identified for the shutdown PSA model. IE frequencies were calculated using system-specific fault tree models, representing an average frequency of this static model. Each IE name was incorporated as a flag event in the appropriate model, with probability set to 1.0. Then, to calculate each specific IE frequency, the system logic that was under an AND gate in conjunction with the IE was quantified to determine the gate frequency.

Table 2: Initiating event (IE) for the shutdown PSA.

Event Name	Event Description
%T1	Total Loss of RHRS
%T2	Total Loss of PFPCS

The development of the logical sequence of events after the occurrence of the initiating event requires the determination of plant systems that perform the safety functions in the specified accidental scenarios. The systems required to maintain the facility in a safe-stable shutdown state are shown in Figures 4 and 5, where CD means core damage and OK means that the accident sequence was successfully mitigated.

The front-line systems RHRS and PFPCS, considered in the event trees initiated by %T1 and %T2 are shown in Figures 6 and 7, respectively. The PFPCS can be configured so that, in order to accomplish its mission, one of the pumps of Train 1 may operate in combination with one of the heat exchangers of Train 2 and vice versa. In addition, the valves associated with this equipment are included in the modeling of the PFPCS pump and heat exchanger systems.

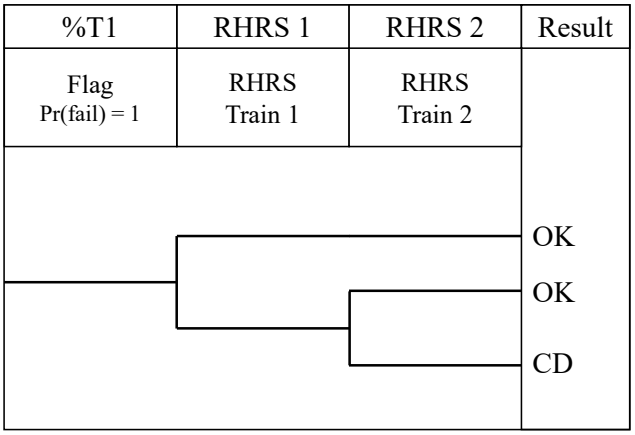

Figure 4: *Event tree %T1 of total loss of the RHRS*

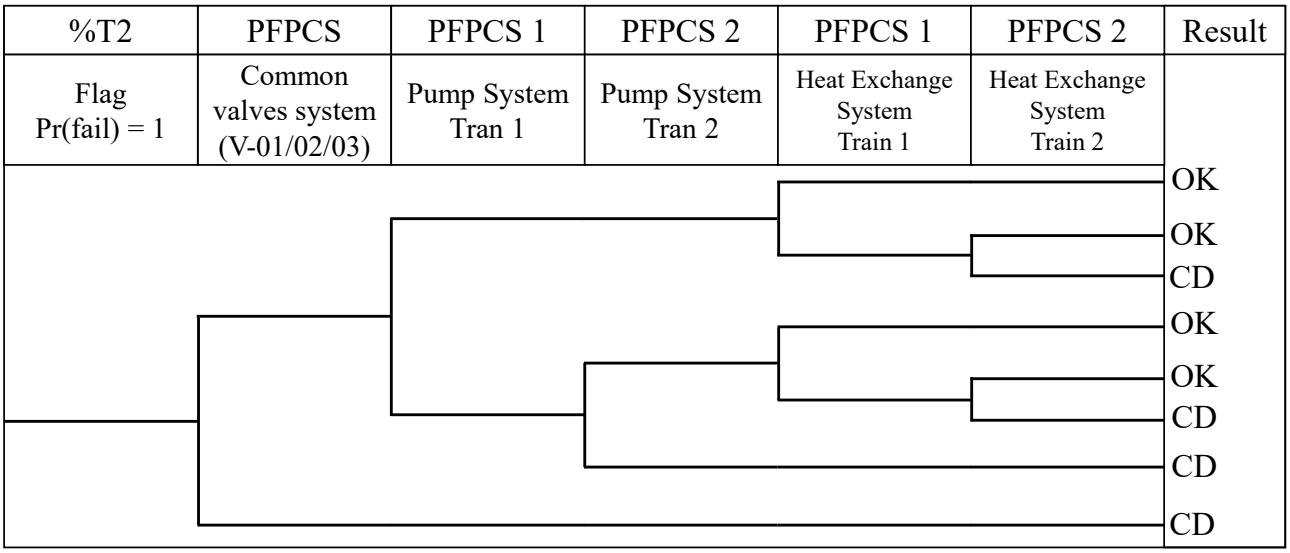

Figure 5: *Event tree %T2 of total loss of the PFPCS.*

It is worth mentioning that both initiating event and any other event of the accident sequence can be generated by intrinsic failures of front-line systems components, failures of support systems components, or as a result of the combination of failures in both types of systems. Failures in support systems may be characterized by failure of offsite power supply, failure of AC and DC electrical systems, and so on.

In Figures 6 and 7, an alphanumeric codification was used to identify equipment type and its functional classification. The letter code identifies the equipment type, e.g., P to pump, H to heat exchanger, and V to valve. Equipment that are common to both trains of the system have a sequential numerical code that starts with 0, e.g. valves V-01, V-02, and V-03 of PFPCS (Figure 7); Train 1 equipment are identified with number code 1, e.g. pumps P-11 and P-12 of RHRS (Figure 6); and Train 2 equipment are identified with number code 2, e.g. pumps P-21 and H-21 of PFPCS (Figure 7).

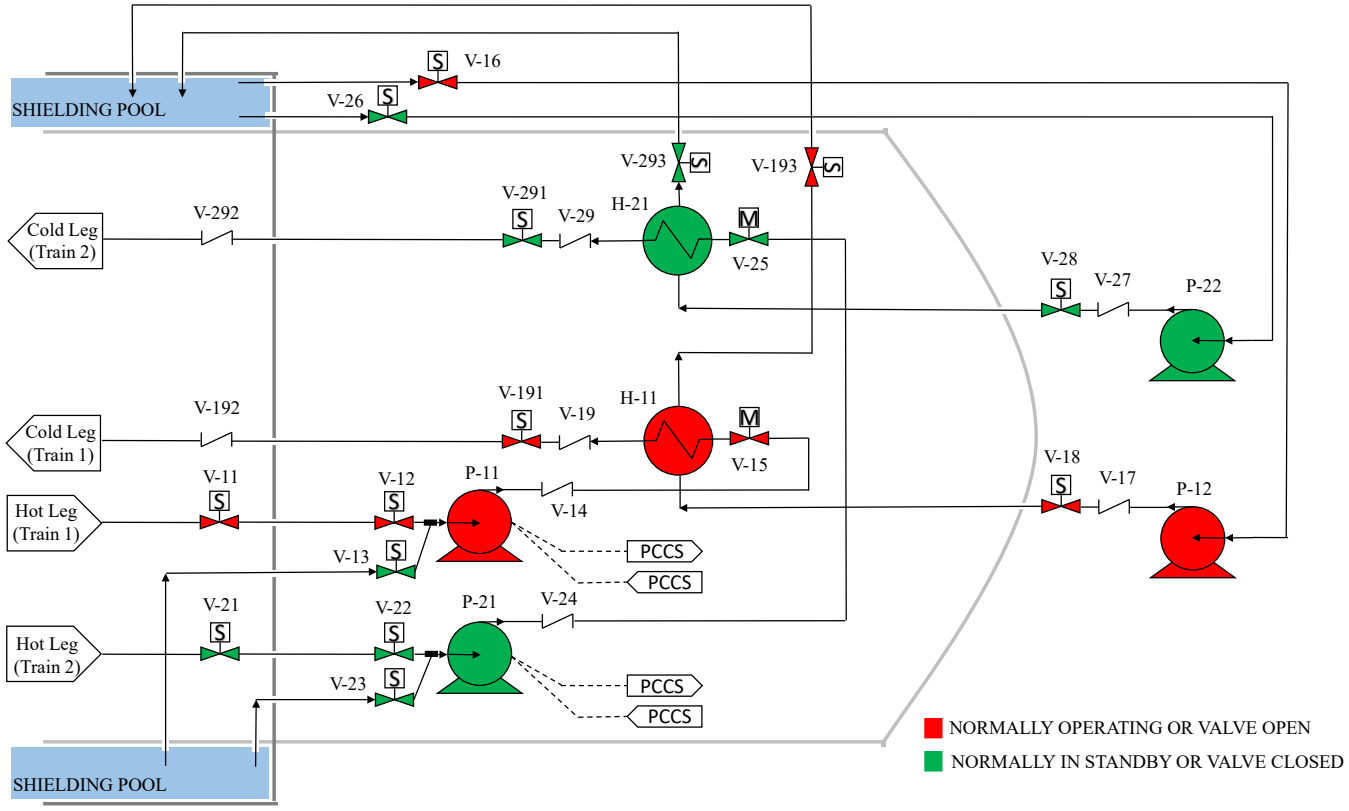

Figure 6: *Residual heat removal system (RHRS) process diagram.*

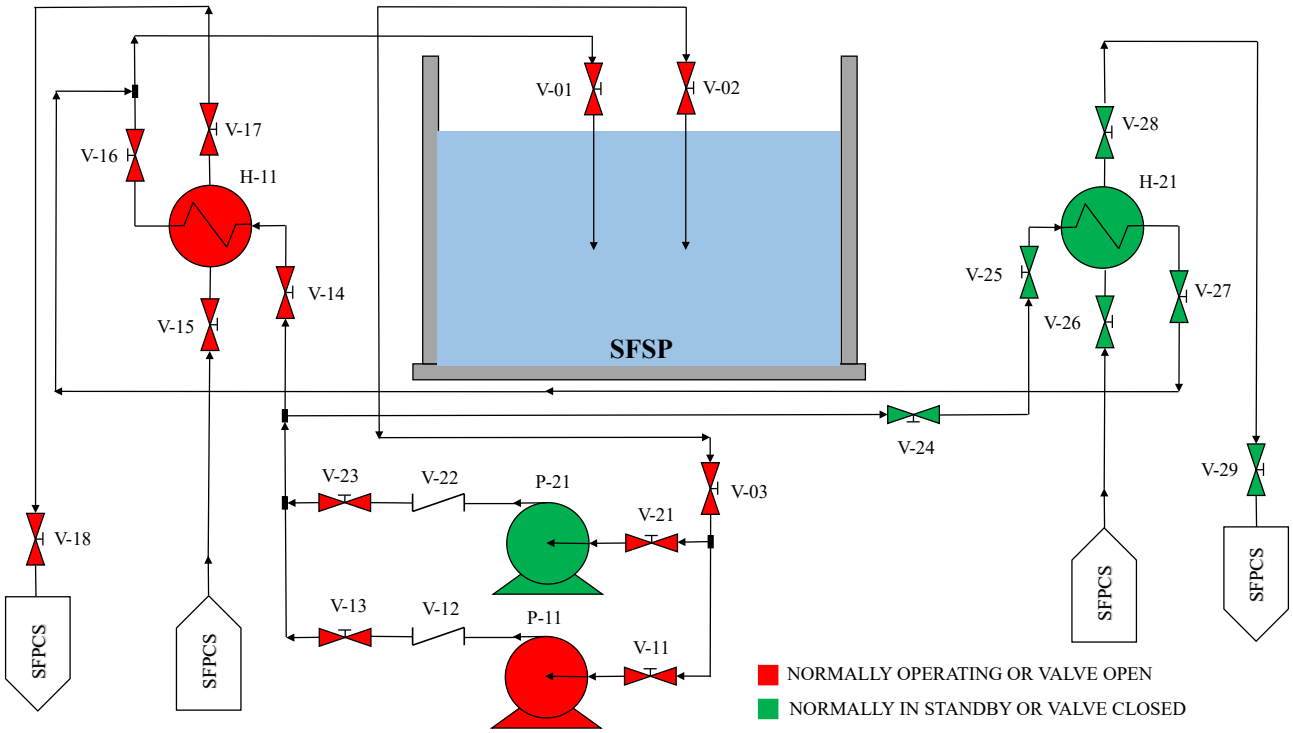

Figure 7: *Primary fuel pool cooling system (PFPCS) process diagram.*

A detailed fault tree model was developed for each system required during shutdown mode and considered in event trees %T1 and %T2. Dependencies between systems are represented by links in the fault trees, considering the support systems necessary for the successful performance of front-line systems. In this way, integrated fault tree models were developed that explicitly include all dependencies. Component failures as well as failures associated with testing and maintenance procedures were included in the fault trees. Top events of the master fault tree model are shown in Figure 8.

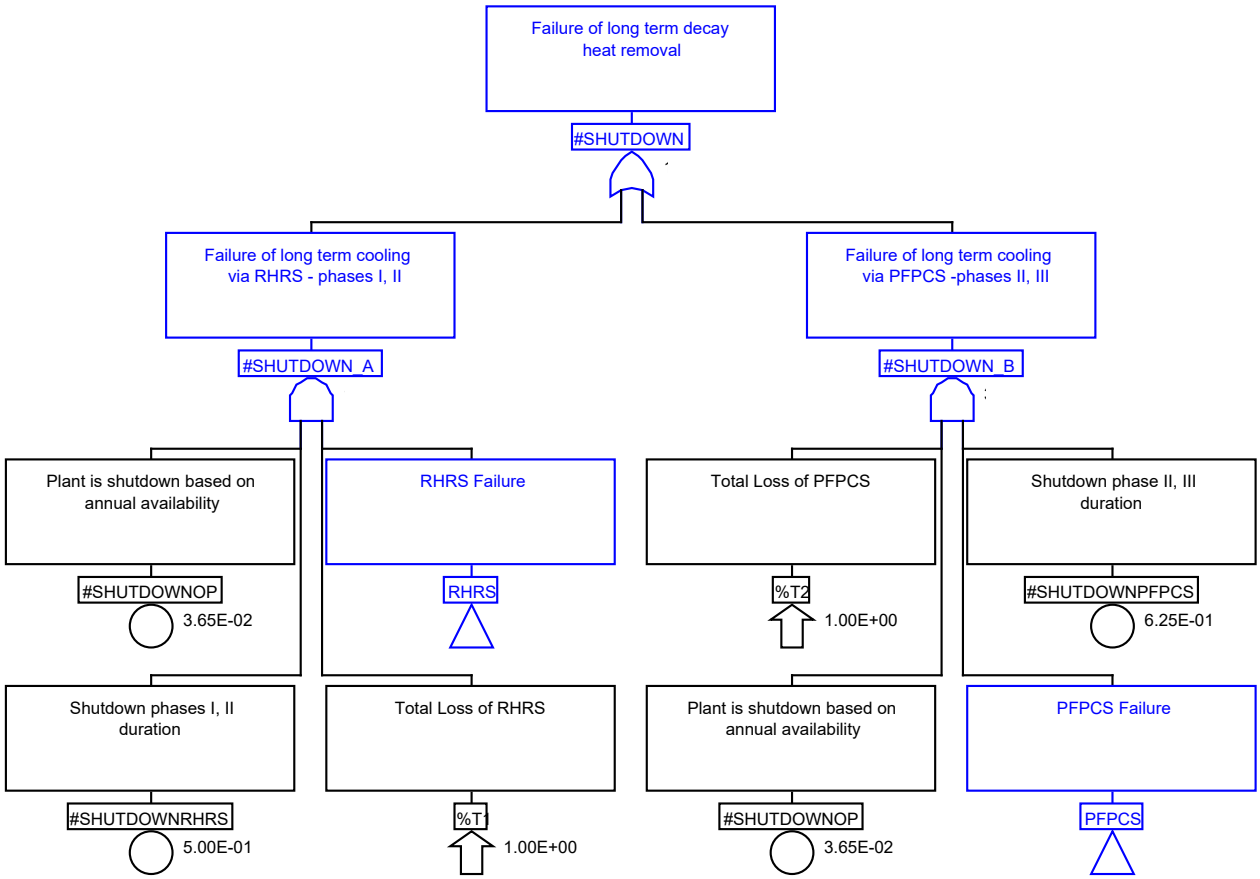

Figure 8: *Master fault tree model of the shutdown PSA.*

Combining the frequency of occurrence of an IE with the probability of the basic events in a given accident sequence provides the frequency of occurrence for that sequence. Due to IE and the various branches of event trees represented in fault trees, the total number of cut sets that could lead to core damage would be very high. Thus, a truncation frequency of 1E-11/year was selected, where only cut sets with a frequency of occurrence equal to or greater than this value was calculated.

The following assumptions used in the models may be highlighted:

- Refueling outages were assumed to last 40 days every 3 years (3.65E-2/yr.);
- Phases I and V were assumed to last 15 days (each), phases II and IV 5 days (each) and phase III 20 days. Therefore, the frequency of occurrence of phases I and V was estimated to be 3.75E-1/year, phases II and IV 1.25E-1/year, and phase III 5.00E-1/ year;

- Unavailability due to test and maintenance in PFPCS and in some other support systems were assumed to have an average value of 5.00E-3/yr. In particular, for diesel generators, an unavailability of 7.3 hours per month (1.00E-2/year) in periodic tests was considered;
- All components were considered repairable and a mean time to repair (MTTR) of 24 hrs. was assumed;
- Standby circuits operating time is defined to be 24 hours. Thus, the first system failure (the running component) can be considered as the initiator and the backup systems as the mitigation response;
- During an SBO, the operator is credited with aligning the alternate alternating current (AAC) source to supply power to the safety busbars. A value of 5.00E-2 is assigned to the human error probability in this operation; and
- Test and maintenance for two components that accomplish the same function in two redundant safety trains must not be performed simultaneously.

2.4. Electric power system modifications

Initially, a model for basic configuration of electric power systems based on NPP codes and standards was incorporated to the shutdown PSA previously developed for the facility. Then, some modifications in electric power systems configuration were proposed (Figure 9) and new analyses were carried out. The planned modifications led to three different electrical system designs, according to table 3:

Table 3: Electrical system design alternatives.

Electrical Configuration	Transmission Lines (TLs)	Emergency Generator by Electrical Safety Bus
A (NPP)	2	1
B	2	2
C	1	2

Note: Configuration C represents a configuration proposal for electric power systems adequate for a non-conventional facility with one TL.

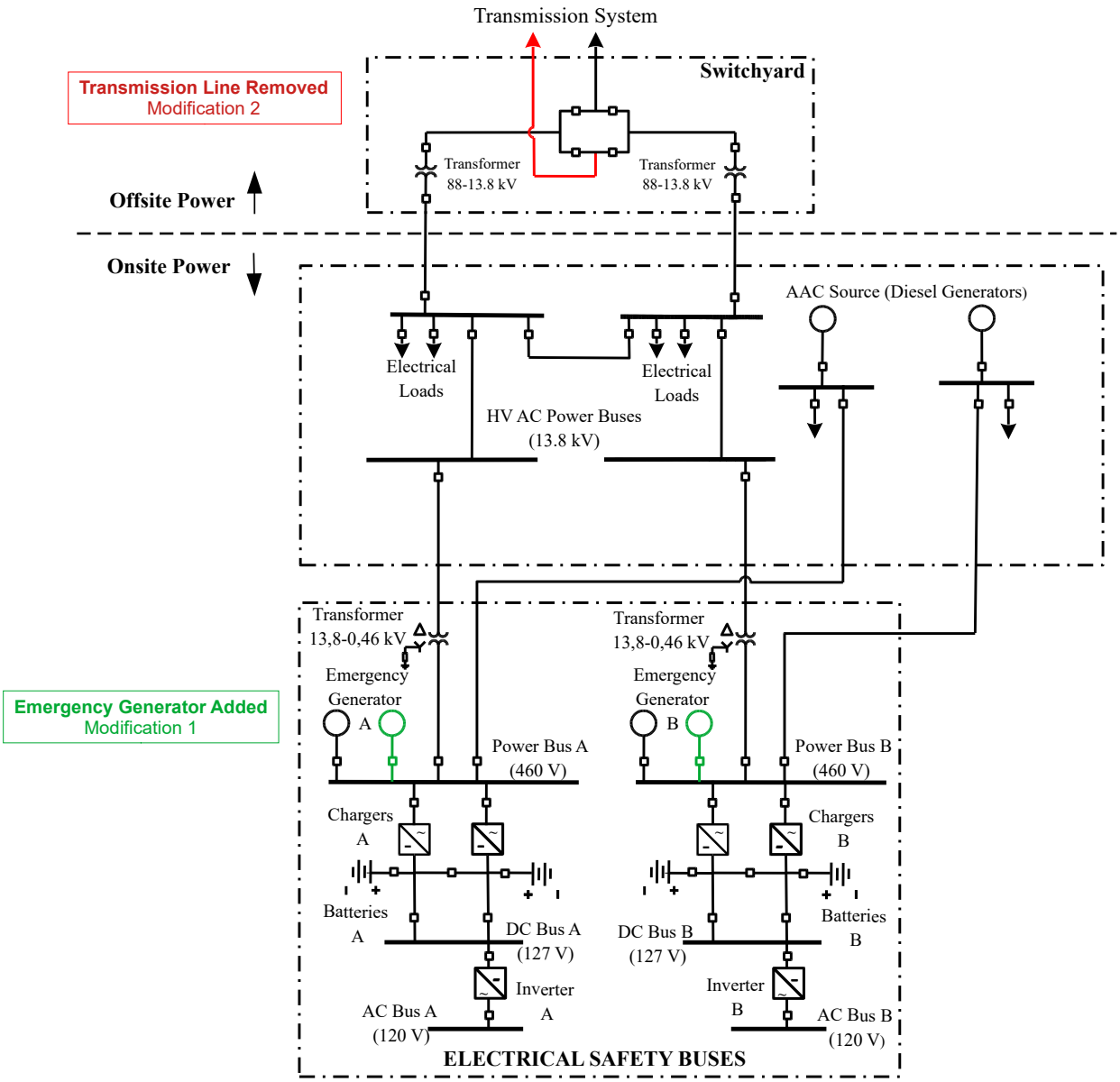

Figure 9: *Basic electrical configuration of a NPP with two modifications to represent the electrical configuration of a non-conventional facility with one TL.*

2.5. Electric power system design selection

Based on the Level 1 PSA results for the different electric power system configurations, the selection of the most appropriate design is carried out with regard to safety for the evaluated installation type. Thus, the variable ΔCDF was defined, which means the percentage of relative

variation of the CDF after the project was updated in relation to the original version. The risk associated with the project can be considered lower compared to the original project if ΔCDF is negative, while the risk is higher if ΔCDF is positive. The ΔCDF equation is defined by:

$$\Delta CDF = \frac{CDF_{updated} - CDF_{original}}{CDF_{original}} \times 100\% \quad (1)$$

It is noteworthy that ΔCDF is just a supporting variable in the project choice, as it does not take into account economic aspects, the functionality of the installation and the minimum reliability of the electric power system demanded by the project.

3. RESULTS AND DISCUSSION

The plant total CDF was estimated to be 1.28E-5/year for configuration A (original) of the electric power system, 1.24E-5/year for configuration B, and 1.25E-5/year for configuration C.

Table 4 shows the contribution of initiating events %T1 and %T2 to the accident. For all electric power configurations, it is evident that the total loss of RHRS (%T1) is the major contributor to a core damage accident during the refueling outage.

Table 4 – Installation core damage frequency

Electrical Configuration	CDF_{TOTAL} (/yr.)	CDF (/yr.)	
		%T1	%T2
A (original)	1.28E-5	1.04E-5	2.34E-6
B	1.24 E-5	1.02E-5	2.22E-6
C	1.25 E-5	1.02E-5	2.24E-6

Table 5 shows the SBO contribution to plant total CDF considering the three electrical system configurations. Total CDF and SBO reduction comparing configurations B and C with A (original) are presented in the two last column. Comparison between configuration A (basic NPP) and configuration C (adequate for non-conventional nuclear facilities) shows that there is a 2.33% reduction in total CDF and 98.72% reduction in SBO contribution to CDF.

Table 5: CDF estimates for different electric power systems configurations.

Electrical Configuration	CDF_{TOTAL} (/yr.)	CDF_{SBO} (/yr.)	CDF_{SBO} (%)	ΔCDF_{TOTAL} (%)	ΔCDF_{SBO} (%)
A (original)	1.28E-5	7.26E-8	0.57	-	-
B	1.24E-5	6.89E-10	0.01	-2.70	-99.05
C	1.25E-5	9.27E-10	0.01	-2.33	-98.72

Considering the individual contribution of the systems to a core damage accident, Figure 10 shows the F-V importance measures (0 to 1) that order the systems with highest contribution to the accident. RHRS is the major contributor, independently of the electric power system configuration. The F-V importance measures for SFPCS and DC electrical system were in the order of E-5 and E-3, respectively, and for this reason, they had very low graphical representation. With the incorporation of an emergency diesel generator, in configurations B and C, there is a significant reduction in the AC electrical system contribution to the accident.

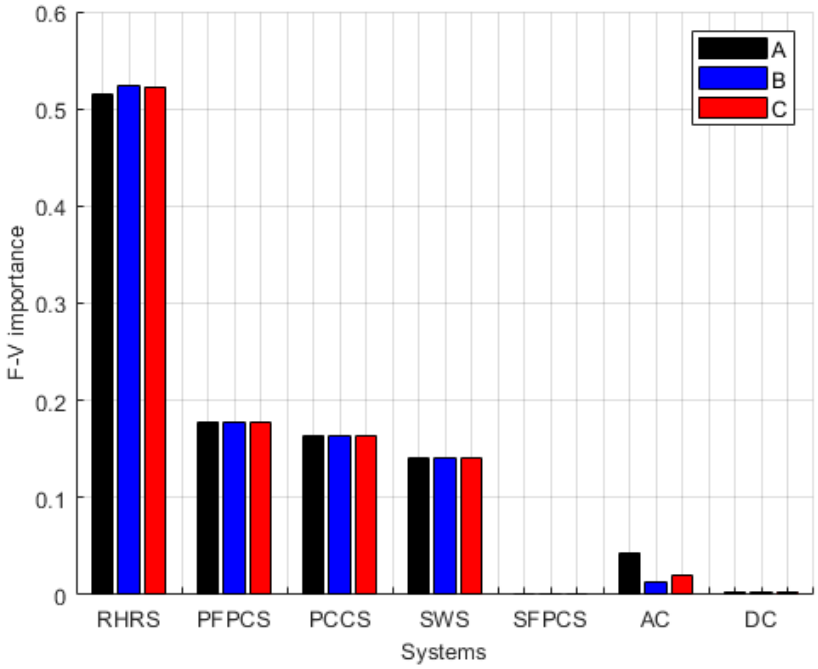

Figure 10: *Individual contribution of systems to the core damage accident.*

Considering the non-conventional nuclear facility operational specificities, configuration C proved to be more adequate than configuration A. The non-compliance with the requirement for a second TL can be justified by the increased level of safety demonstrated by the incorporation of local emergency diesel generators in the design of electrical systems.

4. CONCLUSION

CDF is an adequate risk metric for the objectives of this study and PSA methodology is an important tool to support decision making for the design as well as the licensing process of non-conventional nuclear facilities. In this work, PSA was used to support the selection of alternative configurations of electric power systems design, overriding the standard configurations required for NPPs. The Station Blackout event was emphasized because it is a critical event for the installation, imposing operational restrictions that even depend on operator interventions and, consequently, can trigger a significant increase in the risk to the installation caused by human error. Considering the functional and operational specificities of a non-conventional nuclear facility, the failure to comply with the requirement for a second TL, provided for in the conventional normative basis, can be justified by the increase in the level of safety obtained in a probabilistic evaluation, demonstrated by the incorporation of an additional emergency diesel generator by safety bus in the design of electrical systems. In accordance with the results, depending on the functional particularities, it is recommended to review the normative basis adopted by non-conventional nuclear facilities.

For future work, it is suggested a case study with application of the methodology that considers the recovery times of the systems, considering the time to which the core can be without effective cooling. Therefore, it will be necessary to estimate the residual heat of the spent fuel over time. The recovery times will provide a more detailed and less conservative analysis than that performed in this work. Another important aspect that must be studied in detail is human errors in critical events, such as Station Blackout events, which can considerably increase the risk to the installation.

ACKNOWLEDGMENT

Navy Technological Center in São Paulo (CTMSP), Nuclear and Energy Research Institute (IPEN-CNEN), and Analysis, Evaluation and Risk Management Laboratory (LabRisco) of University of São Paulo (USP).

REFERENCES

[1] Gjorgiev, B.; Volkanovski, A.; Kancev, D.; Cepin, M. Alternative off-site power supply improves nuclear power plant safety. **Annals of Nuclear Energy 71**, p. 304-312, 2014.

[2] Khatua, S.; Mukherjee, V. Application of integrated microgrid for strengthening the station blackout power supply in nuclear plant. **Progress in Nuclear Energy 118**, 2020.

[3] U.S. NUCLEAR REGULATORY COMMISSION. **Domestic Licensing of Production and Utilization Facilities**. Washington: U.S.NRC, 2017. (10CFR50).

[4] ONS. Operador Nacional do Sistema Elétrico. Available at: <http://www.ons.org.br/Paginas/resultados-da-operacao/qualidade-do-suprimento-paineis.aspx>. Last accessed: 18 Feb. 2020.

[5] U.S. NUCLEAR REGULATORY COMMISSION. **Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States**. Washington: U.S.NRC, 1993. (NUREG-1449).

[6] ANS. American Nuclear Society. Available at: https://www.ans.org/news/article-1635/they-harnessed-the-atom-the-first-navy-prototype-nuclear-plant/. Last accessed: 10 Ago. 2021.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY. **Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants**. Vienna: IAEA, 2010. (Specific Safety Guide No. SSG-3).

[8] CAFTA, Version 6.0b: **Fault Tre Analysis System Software**. Electric Power Research Institute (EPRI), 2014.

[9] U.S.NRC. U.S. Nuclear Regulatory Commission. **Reactor Operational Experience Results and Databases**. Disponível em: https://nrcoe.inl.gov/. Acesso em: 05 jun. 2021.