BJRS

BRAZILIAN JOURNAL
OF
RADIATION SCIENCES
09-02B (2021) 01-16

Reliability and Redundancy Allocation Analysis Applied to a Nuclear Protection System

Alexander Lucas Busse, João Manoel Losada Moreira

Amazônia Azul Tecnologias de Defesa S.A

alexlucasb@gmail.com

ABSTRACT

Brazil is building, with national technology, two small nuclear reactors for propulsion and for the production of radioisotopes with thermal powers between 20 and 50 MW. These nuclear reactors fit more into the small modular reactor (SMR) class than the large nuclear power plant class. In this article, we apply the SMR design approach to propose a reactor protection system architecture for the small reactor under construction in the country. For this, the probabilistic analysis of the architecture of a protection system of a nuclear reactor is evaluated to determine the sensitivity of the components through a modeling of Reliability Block Diagram. The modification of the architecture and the addition of redundancies were evaluated when using components with a lower useful life than the components normally used for this purpose. The results showed that after one year of operation, the reference RPS system has a failure probability of 0.17%. The modified system, with components with a shorter life span, presents a point reliability value only 0.070% lower than the reference, but this difference grows exponentially with time, and in 10 years of operation it can reach values above 95%. The use of equipment with shorter life characteristics implies a greater number of redundancies and, in addition, a greater number of maintenance procedures and spare parts. Therefore, this technical feasibility analysis should consider RAM simulation as well.

Keywords: **reliability, protection system, SMR.**

ISSN: 2319-0612
Accepted: 2021-05-28

ACRONYMS

DAS	Diverse Actuation System
DIV	Processor Division
ESFAS	Engineered Safety Features Actuation System
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
GA	Genetic Algorithms
HMI	Human Machine Interface
MTBF	Mean Time Between Failures
PDF	Probability Density Function
PES	Programmable Electronic Systems
PSO	Particle Swarm Optimization
RAM	Reliability, Availability and Maintainability
RBD	Reliability Block Diagram
RPN	Risk Priority Number
RPS	Reactor Protection Systems
RTS	Reactor Trip System
SMR	Small Modular Reactor
VOT	Voter

1. INTRODUCTION

Operating an industrial plant in a safe, sustainable and financially viable manner are basic objectives of any industrial sector. The difficulties in achieving these goals are accentuated because many aspects are competing. In the nuclear sector, for example, the safety aspect to ensure the safe shutdown of the reactor can be seen in the high technical requirements and in the numerous redundancies [1]. A recurring feature of the nuclear plant industry is the requirement for technical certifications to mitigate failures and distribute responsibilities to suppliers. The perspective of analysis by certifying and reporting agencies has changed from the 1980s to today, with a focus on

quantitative techniques for safety analysis and life cycle analysis of the product under certification [2].

Brazil is building, with national technology, two small nuclear reactors for propulsion and for the production of radioisotopes with thermal powers between 20 and 50 MW. These nuclear reactors fit more into the small modular reactor (SMR) class than the large nuclear power plant class [3]. Herder et al [4] reinforce the importance of probabilistic reliability analysis for the protection architecture of critical control systems in an industrial process. They consider that it is essential to mitigate catastrophic failures to avoid not only financial expenses, but also damage to workers' health, the environment and society.

Karydas et al (1999) [2] summarize that the analysis for PES certification (Programmable Electronic Systems) should be divided into the following aspects:

1. Architecture (how each block is related);
2. Hardware failure modes and failure rate;
3. Systematic failure modes (analysis of systematic fault tolerance during the life cycle including human errors);
4. Reliability modeling (simulation techniques, RBD, FTA and Markov);
5. Reliability assessment (after raising the reliability characteristic curves, compare with the acceptance requirements for the architecture).

In the nuclear industry, the reactor safety function has “Reactor Protection Systems” (RPS) and these to meet the criteria of reliability and operational availability, have components with high MTBF (Mean Time Between Failures) and many processing redundancies and activation [1] The main functions of protection systems are to shut down the reactor, thus preventing overheating, damage to the reactor core and, finally, preventing the release of radioactive material into the environment. They are basically composed of sensors, logic, actuators and HMI dedicated to protection systems. Therefore, a catastrophic failure for the RPS would be the non-shutdown of the nuclear reactor and the failure to act to contain the release of radioactive material into the environment.

The need to analyze RPS from the point of view of reliability to determine the likelihood of catastrophic failure depends on the security context [2]. This security context allows to evaluate the system's reliability performance through reliability allocation analysis to determine the overall reliability impact, increasing redundancies using equipment with higher failure rates [3]. Such an

approach, while ensuring compliance with safety requirements, allows not only cost reduction, but also, in many situations, the feasibility of carrying out the project, since many countries have barriers to import systems, equipment and nuclear components.

However, this approach presents difficulties that require caution [4]. This type of solution has impacted such as loss of efficiency by not using equipment dedicated to such functions, more frequent maintenance procedures and a greater number of equipment and components for maintenance. In this regard, Herder et al. [4] points out that with the largest number of equipment and maintenance procedures, the system or part of it will be inoperable; moreover, not all maintenance activities will actually be effective in increasing reliability. Another important caveat is that the system reliability analysis, as done in this document, does not assess the project life cycle and that a set of coherent standards to support nuclear safety has yet to be applied.

In this work, we performed a sensitivity analysis of the general reliability of the RPS system with dedicated and certified equipment and evaluated the possibility of achieving the same reliability objective with equipment and components with a reduced life characteristic. Reliability requirements are pursued through changes in architecture specifications and redundancy.

2. METHODS AND DATA

2.1. Reactor protection system and reliability assesment models

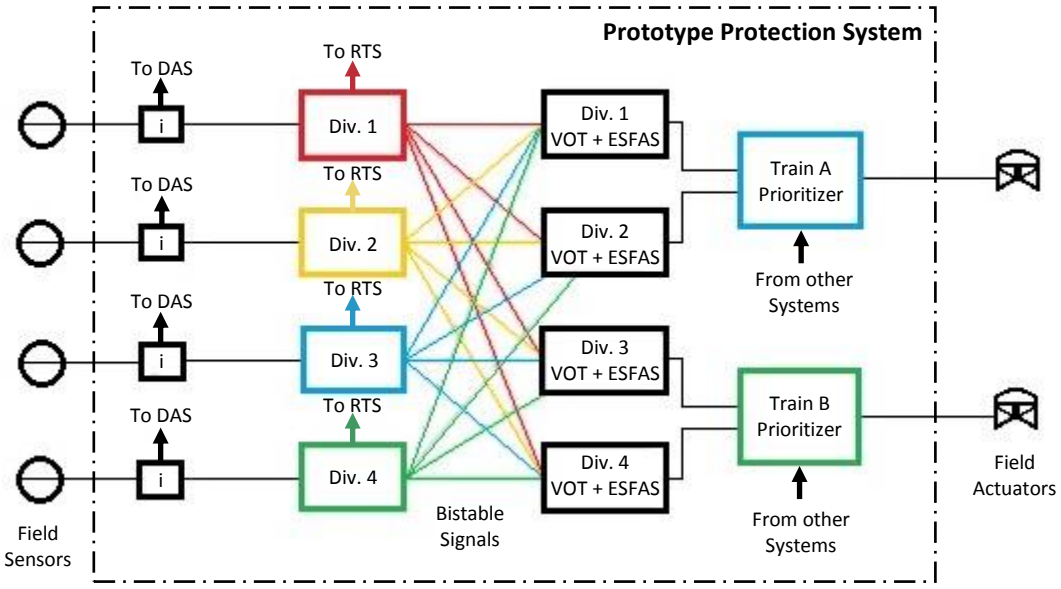
The reactor protection systems cover the following systems: The Reactor Protection System (RPS) and the Engineering Safety Resources Actuation System (ESFAS) [5]. Typically, these systems can be digital, with processed process-generated emergency shutdown signals (TRIP signal), or analog, with emergency shutdown signals generated from analog relay signals. Field information can be digital and analog [5].

The RPS is the system that initiates the shutdown of the reactor quickly when the values of the important parameters of the plant exceed the safety levels, these parameters are configurable and characteristic of the design of each plant. This system also initiates the action of ESFAS.

Figure 1 shows an RPS architecture, including ESFAS activation, for a nuclear power reactor. The RPS consists of 4 redundant processing rooms that process the field signals from the sensors and compare them with predefined security setpoints. If a division of the RPS considers that the field

variable has exceeded the value of the predefined setpoint, this division will send a reactor trip signal to voters. The trip signals of the four divisions must be voted, in logic 2oo4, to avoid spurious tripping. If there are two divisions indicating the triggering of the reactor, the ESFAS will be activated and the safety signal will be sent to the prioritizer (example: closing / opening of specific valve). The prioritizer is a digital processor that operates in a hot-stand-by situation and is close to the equipment that will be activated. This equipment will be activated with the ESFAS signal being routed by at least one of the redundant signal routing trains.

Figure 1*: Reference architecture*



2.2. Reliability analysis through Reliability Block Diagram

The Reliability Block Diagram (RBD) methodology assumes that it is possible to predict the system's reliability by modeling the sub-items that comprise it. Thus, the correct modeling of the life distribution of each subitem and the relational organization between the subitems are vital to obtain a correct forecast of the system. Each sub-item must be modeled as a block and the interface between these blocks as a diagram. Each block has its own independent distribution of life and properties. The most commonly found diagram configurations are serial, parallel, mixed, complex, split load and waiting block. Various mathematical methods have been developed to solve these configurations, as

described and commented on by [6]: Decomposition method, Event space method and Path tracking method.

Optimizing the allocation of redundancies is a complex and often competitive problem, as it involves several factors such as technical feasibility, costs, physical space and others. Therefore, several techniques to try to find the solution to improve have been developed in the last decades, although proving that the solution found is the most optimized is not always easy or possible [7]. The most commonly used optimization techniques include: dynamic programming, integral programming, integral-mixed and non-linear programming and heuristics [8, 7, 9]. A literature review on the problem is presented by Ramirez-Marquez et al [7] and Coit et al [8].

Redundancy optimization analysis becomes a combinatorial optimization problem for many problems where there is abundant information, such as component reliability, costs, component alternatives, well-defined constraints and so on. In these cases, the redundancy optimization analysis becomes an important tool for making investment and security decisions. Mettas [10] describes a solution using a nonlinear cost function methodology to find the solution taking into account predetermined constraints such as cost, technical feasibility, etc., after finding the system's global reliability equation using the Reliability Block Diagram (RBD).

Other approaches to problem solving, such as redundancy allocation, have been the use of Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) [11, 12, 7]. However, as emphasized by Ramirez-Marquez et al [7], the use of GA requires specific coding and adjustment of parameters, but cannot guarantee the optimal solution. Garg et al [12] presented good optimization results applied in the pharmaceutical industry.

The problem of allocating reliability and allocating redundancy are fundamentally different. For the reliability allocation problem, the system architecture is fixed and the reliability of the subsystems are the variables to be optimized, taking into account the restrictions imposed (cost, technical feasibility and so on). Coit et al [8] and Yadav et al [9] provide some examples and reviews of the literature on the problem. On the other hand, the problems of allocation of redundancies consider the analysis of increasing the number of redundancies in parallel to increase the general availability of the System.

Several approaches to the reliability of treatment allocation have been developed to determine the weighting functions for optimization. Some authors use methods based on failure mode and effect

analysis (FMEA) using the risk number (RPN). Others address the problem by introducing Lagrangian multipliers as part of the objective function to ensure that restrictions are satisfied [9]. Brian Krover (1994) [13] details the use of the Monte Carlo method to find reliability values for complex systems. Similar to the redundancy allocation analysis, Mettas [10] addresses this problem with a nonlinear weight function that includes restrictions determined by the method.

2.3. Cases studied and data

This work is divided into three main cases to achieve the mentioned objectives. We started with Case 1 to build reference RPS. First, a review of the literature will be carried out on articles and technical documents to find the reference values of the failure rate for the electronic components that make up the RPS of Figure 1. Next, an RBD modeling will be performed to find the global reliability equation. of the system for different periods of operation. The architecture resulting from the RBD modeling is presented in Figure 2. This RPS reliability modeling will be taken as a reference for all analyzes of this work. The failure rate data for components are shown in Tables 1 and 2.

Case 2 is similar to case 1, but considering characteristic life values reduced by 50% for the sake of sensitivity, and an assessment of the location of redundancies, according to the methodology of the cost function described by Mettas [10]. The failure rate data for components are shown in Table 1.

Case 3 is built by adding a redundant processing division to Reference Case 1. The new RPS architecture is built using the characteristic life values of the components reduced by the 50% factor of the reference, but incorporating the result of the analysis of the redundancy location. That is, a field sensor, a I/O card and a redundant processing division will be added to the architecture. This addition of yet another processing division in the architecture implies a change in the voting logic to 3oo5. The new architecture is shown in Figure 3. The component failure rate data is shown in Table 1.

Case 4 is similar to case 3, where the architecture shown in Figure 3, but the split post-processing signal has been changed to logic 2oo5. This means that in a 2oo5 logic, if 2 divisions fail or indicate reactor firing, the system will determine the emergency shutdown signal. The failure rate data for components are shown in Table 1.

Case 5 adds a complete redundant travel path to the RPS. Unlike cases 3 and 4, case 5 considers the addition of a complete redundant trip path and not just the addition of a field sensor and processing

division. The new RPS architecture modeled for case 3 is presented in Figure 4. Case 5 also considers the use of the characteristic life values of the components reduced by the factor of 50% of the reference. Similar to case 3, case 5 considers the voting logic of the 3oo5 post-processing signal. The failure rate data for components are shown in Table 1.

Case 6 is similar to case 5, but the split post-processing signal vote has changed to logic 2oo5. The failure rate data for components are shown in Table 1.

It should be noted that for all cases, the approximation of the exponential form of probability of failure for each subsystem was considered, as suggested by Mettas [10].

Figure 2: *Case 1 - RBD model of the reference architecture*

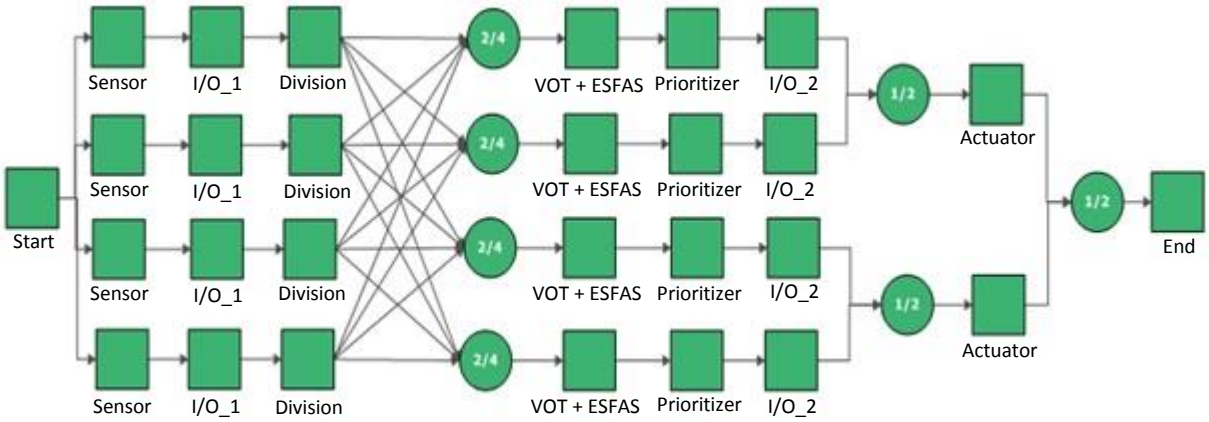


Figure 3: *Case 2 - RBD model plus redundant division*

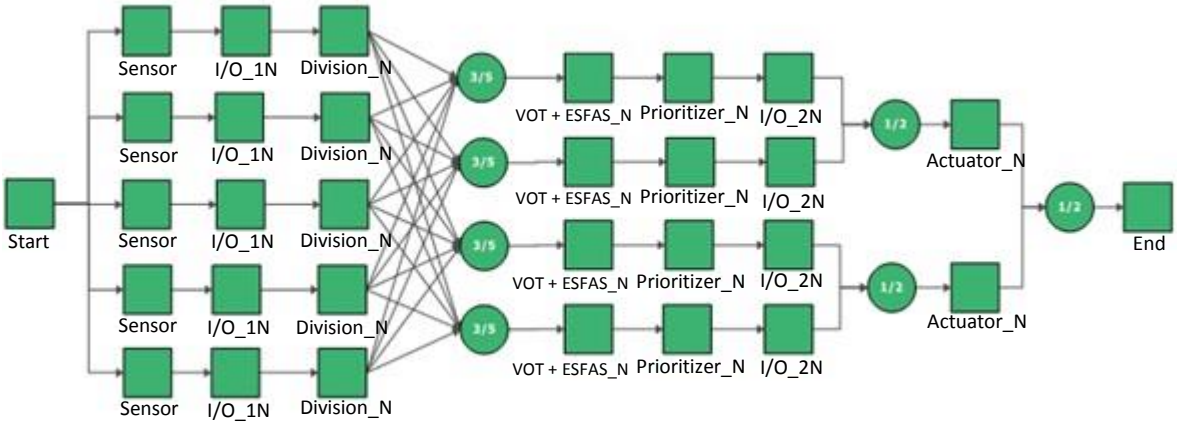


Figure 4: *Case 3 - RBD model plus a complete redundant trip path*

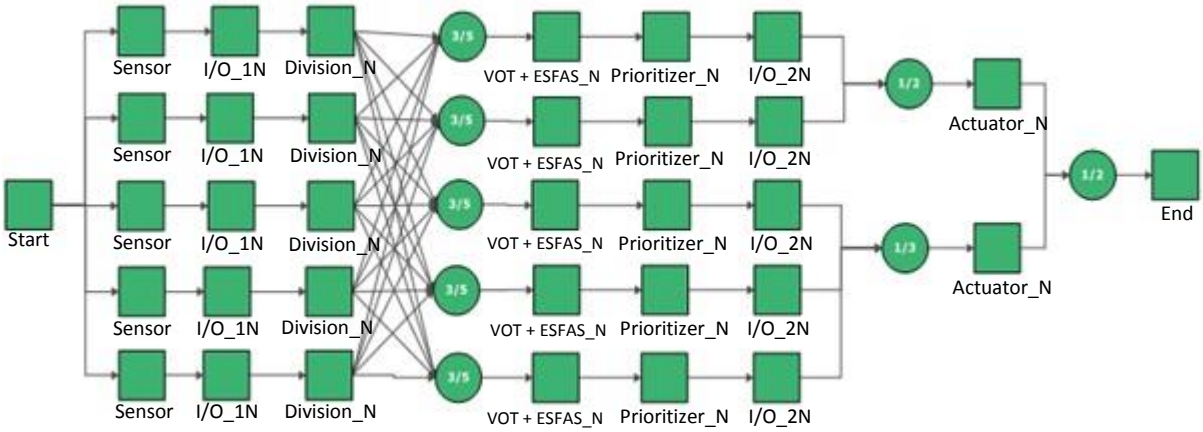


Table 1: *Summary of simulated cases*

Case	Architecture	Data failure rate	Comments
Case 1	Figure 2	Table 2	Reference
Case 2	Figure 2	(Table 2) x 50%	Reference
Case 3	Figure 3	(Table 2) x 50%	Add redundant division
Case 4	Figure 3	(Table 2) x 50%	Add complete redundant trip path
Case 5	Figure 3	(Table 2) x 50%	Add redundant division
Case 6	Figure 4	(Table 2) x 50%	Add complete redundant trip path

Table 2: *Data for failure rate for RPS components [7]*

Equipment	Failure rate	Life characteristic	Repair Time	Ref.
Pressure Sensor	1.1×10^{-6}/h	$9.0 \times 10^{+5}$/h	-	Sensor Pressure
I/O	4.2×10^{-6}/h	$238.0 \times 10^{+3}$/h	8h*	ECEFS
Processing Division	4.9×10^{-6}/h	$204.0 \times 10^{+3}$/h	8h	UCEAF
VOT+ESFAS	4.9×10^{-6}/h	$204.0 \times 10^{+3}$/h	8h	UCEAF
Prioritizer	3.4×10^{-6}/h	$204.0 \times 10^{+3}$/h	3h	RCEAF
Isolator	3.7×10^{-6}/h	$270.0 \times 10^{+3}$/h	8h*	UEYFO

Safety valve	7.0 x 10^{-3}/d	142/d	-	SOCG

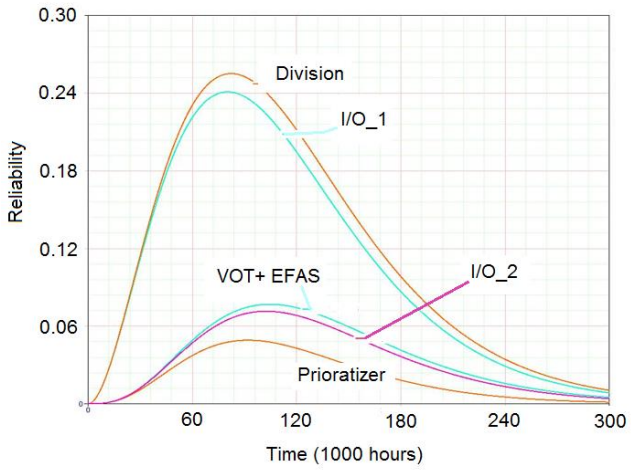
*Considered the same value as processing division = 8 h

3. RESULTS AND DISCUSSION

Before presenting the results themselves, it is important to note that the RBD diagrams are composed of the independent blocks that model the items in the architecture of Figure 1. The failure rate behavior of each item is modeled exponentially and increasing over time. That is, with the time of operation the probability of this item failing increases. In this way, it is possible to model the aging of the item. In turn, it is possible to obtain the global behavior of the RPS system, through a probabilistic resolution using Monte Carlo. Thousands of Monte Carlo generations are generated and failures of individual items are found and the RPS system as a whole is evaluated according to redundancy and voting paths. This is the reason why the system's life characteristic is no longer exponential as modeled on each item. With that in mind, section 3 presents the general results of the modeled cases.

Figure 5 shows the importance of the reliability of each sub-item of the RPS system for the composition of the graph in PDF. It can be highlighted from the analysis the relative importance of the reliability for the following system the items: 1) Division of processing and 2) Input cards of reception of the signals of the sensors. The sum of the relative importance of these two items exceeds 50% of the overall reliability.

Figure 5: *Importance of Reliability vs. time applied to case 1*



This fact led us to justify the analysis of Cases 3 and 4, described in the section. 2.3, where only these two sub-items receive more redundancy (see Figure 3). In sequence, we performed Cases 5 and 6 (see Figure 4), where a complete trip path (sensor for the actuator) received redundancy so that we can compare the real gain with cases 1, 2, 3 and 4.

Figure 6 shows the reliability vs. time in two sets, cases 1, 2, 3 and 5 and cases 1, 2, 4 and 6. Figure 6 should be understood as the probability that the system will operate correctly within the specific operational conditions of the project. In addition, it can be used to generate Figure 7 through its complement (Note, the failure rate is the complement of Reliability). Both values can be used to determine the periodic maintenance periods and self-tests of the system.

Figure 7 shows the probability of failure vs. time through the accumulated density function (CDF) for the reactor protection system represented by the architecture of Figure 1 and modeled according to cases 1, 2 and 3. One of the advantages of the graphic CDF type is the possibility of directly reading the probability of system failure due to the time of operation in the interpolation of the axes.

Figure 8 shows the system failure rate vs. time as modeled according to Figure 2 and Figure 3. This figure shows the increasing behavior of the failure rate due to the aging of the components. Figure 9 shows the graph of the density probability of failure (PDF) function of the system as modeled according to Figure 2 and Figure 3. This figure is the result of the composition of the probability distribution forms of the various sub-items that make up the RPS system. It can be noted that the probabilistic form of failure of the RPS system is Lognormal.

Figure 6: *Reliability vs Time for cases: (1, 2, 3, 5) and (1, 2 ,4, 6)*

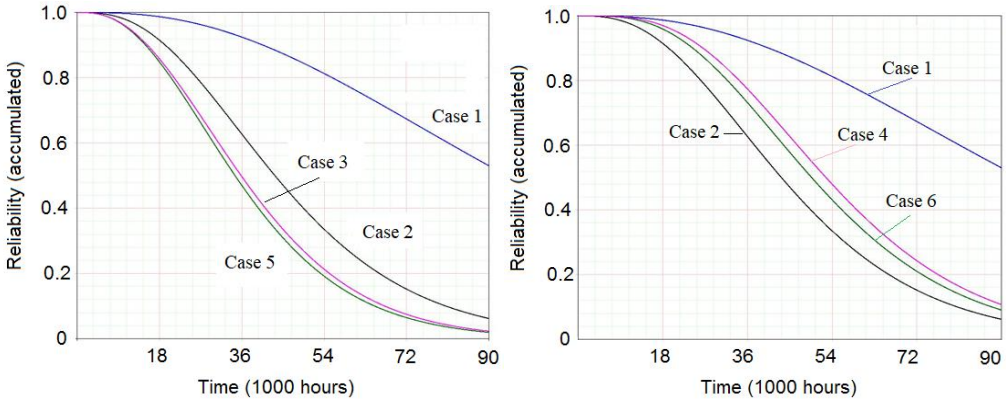


Figure 7: *Probability of Failure vs. Time for cases: (1, 2, 3, 5) and (1, 2 ,4, 6)*

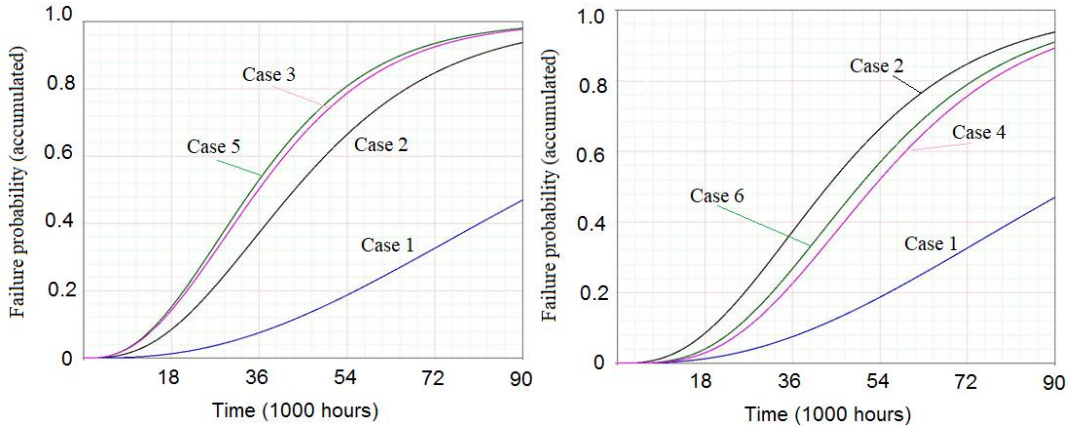


Figure 8: *Failure rate vs. Time for cases: (1, 2, 3, 5) and (1, 2 ,4, 6)*

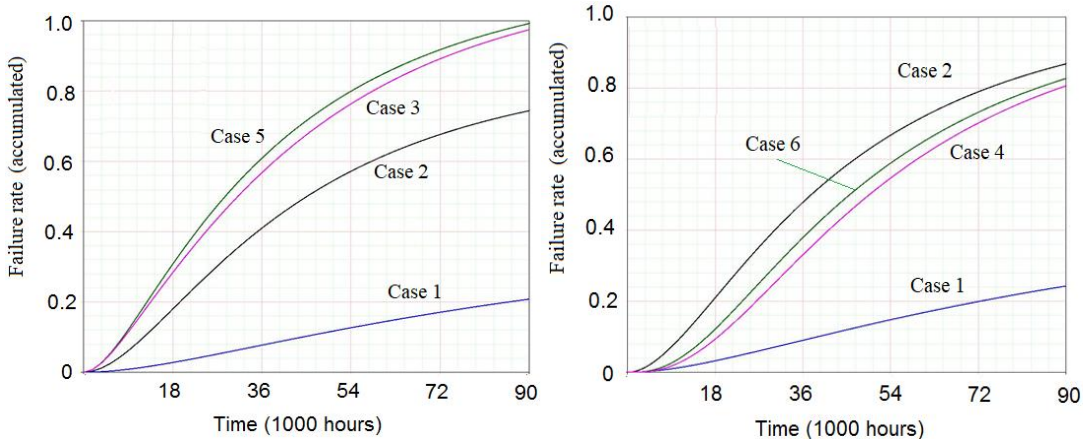


Figure 9: *Probability density function vs. Time for cases: (1, 2, 3, 5) and (1, 2 ,4, 6)*

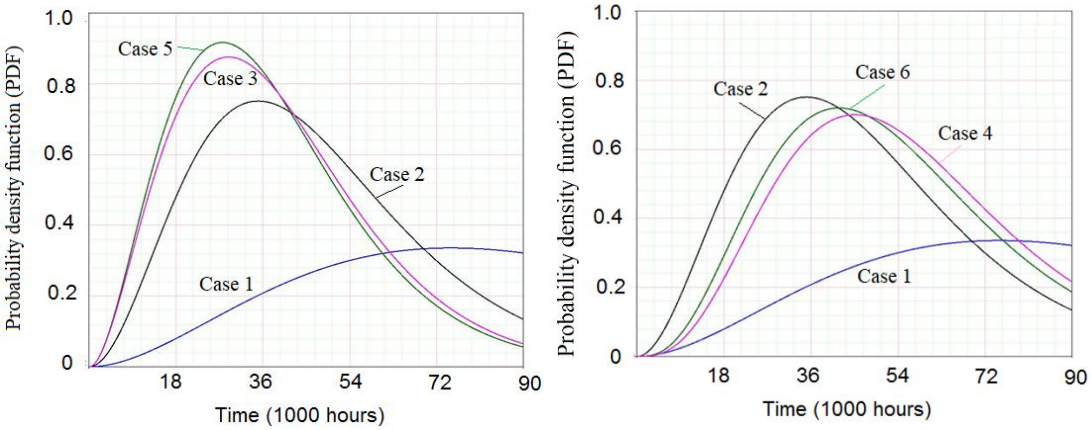


Table 3 shows the result of the failure rate of the simulations for each of the studied cases considering the operating times equal to one, one and a half and ten years. In this table it is possible to verify the influence of the value of the failure rate on reliability at the end of the simulated operating time.

Table 3: *Overall failure rate (R) for the different cases*

Models	R (h^{-1}) 1 year	R (h^{-1}) 1.5 year	R (h^{-1}) 10 years
Case 1	5.6×10^{-7}	1.0×10^{-5}	1.4×10^{-4}
Case 3	8.0×10^{-5}	1.5×10^{-4}	6.9×10^{-4}
Case 4	1.0×10^{-5}	4.0×10^{-5}	4.9×10^{-4}
Case 5	8.0×10^{-5}	1.4×10^{-4}	6.8×10^{-4}
Case 6	1.0×10^{-5}	3.0×10^{-5}	4.8×10^{-4}

We observed that for 8,760 h (1 year) of operation the reliability of the reference model (Figure 2) is 0.9983, that is, the probability of a system failure occurring would be 0.17%. The occurrence of this failure means a catastrophic failure, that is, the RPS will fail with the reactor shutdown function. For the other cases, the best behavior was presented by case 6, the lowest reliability value of - 0.070% in relation to the reference. And in the worst case (case 3), a lower reliability value - 2.5%. This difference increases over time, reaching values greater than 95% difference when considering 10 years of operation.

Another piece of information we can get from Figure 7 is that the occurrence of at least one catastrophic failure or an unsecured failure becomes close to 80%, probably close to 150,000 hours of operation. For cases 3 and 5, the probability of 80% occurs close to 60,000 hours of operation.

4. CONCLUSION

The approach taken in this article can be applied to national projects for two small nuclear propulsion and radioisotope production reactors, since these nuclear reactors fall more into the Small Modular Reactors (SMR) class than in the large nuclear power plants class. . . A generic RPS model that can be used in these reactors was evaluated using real reliability values. After the construction of cases 3, 4, 5 and 6, which analyzed the sensitivity of the general reliability of the system when using

equipment and components with characteristic half-life, it was possible to demonstrate that it is possible to approach the global reliability value of the system by adding redundancies.

Reliability values over 10 years of operation demonstrated that the difference between the cumulative reliability between the cases (3, 4, 5 and 6) in relation to the reference (case 1) increased exponentially. However, this divergence can be monitored through periodic self-test procedures, inspections and preventive maintenance to detect simple failures, since the catastrophic failure would only occur if the various redundancies were inoperative at the same time. The use of spare parts in the cases (3, 4, 5 and 6) will be considerably higher than the reference, as we can see through the average life values presented in Table 3. For a more complete analysis of technical feasibility, we have to suggest that a RAM (Reliability, Availability and Maintenance) must be implemented.

ACKNOWLEDGMENT

The authors thank the Universidade Federal do ABC and Amazônia Azul Tecnologias de Defesa S.A. company for the technical and financial support for this research.

REFERENCES

[1] Cameron RF. Willers A. Use of Risk assessment in the nuclear industry with specific reference to the Autralian situation. Reliability Engineering and Safety 2001; 74:275-282.

[2] Karydas DM, Brombacher AC. Reliability certification of programmable electronic systems. Reliability Engineering and Safety 1999; 66:103-107.

[3] Busse A.L., Moreira J.M.L. Avaliação sistêmica de tolerância a falhas em sistemas de proteção de reatores nucleares. R. Tecnol. Soc., Curitiba, v. 16, n. 42, p. 58-74. jul/set. 2020. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/9780.

[4] Herder PM, Van Lujik JA, Bruijnooge J. Industrial application of RAM modeling Development and implementation of a RAM simulation model for the Lexan plant at GE Industrial, Plastics. Reliability Engineering and Safety 2008; 93:501-508.

[5] HEYCK, H.; SALM, M. Short Communication: Development of a Digital Reactor Control and Protection System. Reliability Engineering and System Safety. Vol. 27, p. 257-266, 1990.

[6] Ghofrani, M. B.; Damghani, S.A. Determination of the safety importance of systems of the Tehran research using a PSA method. Annals of Nuclear Energy 29, pp. 1989-2000, 2002.

[7] Ramirez-Marquez JE, Coit DW. Optimization of system reliability in the presence of common cause failures. Reliability Engineering and Safety 2007; 92:1421-1434.

[8] Coit DW, Zio E. The evolution of system reliability optimization. Reliability Engineering and Safety, 2018;

[9] Yadav OM, Zhuang X. A pratical reliability allocation method considering modified cricality factors. Reliability Engineering and Safety 2014; 129:57-65.

[10] Mettas, A., Reliability Allocation and Optimization for Complex Systems, Proceedings of the Annual Reliability & Maintainability Symposium, 2000.

[11] Cao D, Murat A, Chinnam RB. Efficient exact optimization of multi-objective redundancy allocation problems in series-parallel systems. Reliability Engineering and System Safety 2013; 111:154-163.

[12] Garg H, Sharma SP. Reliability-Redundancy allocation problem of pharmaceutical plant. Journal of Engineering Science and Technology. Vol 8, No.2 (2013) 190-198.

[13] Korver B. The Monte Carlo method and software reliability theory, http://www-cs-students.stanford.edu/briank/BrianKorverMonteCarlo.pdf, February 1994.