BJRS

BRAZILIAN JOURNAL
OF
RADIATION SCIENCES
08-03A (2020) 01-11

Modeling dynamic scenarios for safety, reliability, availability, and maintainability analysis

Cesar Augusto Gabe, Luciano Ondir Freire, Delvonei Alves de Andrade

Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)

luciano.ondir@gmail.com

ABSTRACT

Safety analysis uses probability combinatorial models like fault tree and/or event tree. Such methods have static basic events and do not consider complex scenarios of dynamic reliability, leading to conservative results. Reliability, availability, and maintainability (RAM) analysis using reliability block diagram (RBD) experience the same limitations. Continuous Markov chains model dynamic reliability scenarios but suffer from other limitations like states explosion and restriction of exponential life distribution only. Markov Regenerative Stochastic Petri Nets oblige complex mathematical formalism and still subject to state explosions for large systems. In the design of complex systems, distinct teams make safety and RAM analyses, each one adopting tools better fitting their own needs. Teams using different tools turns obscure the detection of problems and their correction is even harder. This work aims to improve design quality, reduce design conservatism, and ensure consistency by proposing a single and powerful tool to perform any probabilistic analysis. The suggested tool is the Stochastic Colored class of Petri Nets, which supplies hierarchical organization, a set of options for life distributions, dynamic reliability scenarios and simple and easy construction for large systems. This work also proposes more quality rules to assure model consistency. Such method for probabilistic analysis may have the effect of shifting systems design from "redundancy, segregation and independency" approach to "maintainability, maintenance and contingency procedures" approach. By modeling complex human and automated interventional scenarios, this method reduces capital costs and keeps safety and availability of systems.

Keywords: **Safety Analysis, Reliability availability and maintainability (RAM) analysis, Petri Net.**

ISSN: 2319-0612
Accepted: 2020-07-18

1. INTRODUCTION

As shipping has a contribution to greenhouse gases emission [1], future regulations may create more taxes on crude oil, rising transport tariffs. As maritime transport accounts for 95% of goods transportation [2] [3], decarbonization effort would affect severely the global economy. An alternative to fossil fuels is nuclear power for merchant ships propulsion [4], especially for large container ships with shaft power in range of 60 to 80MW [5].

For Mobile Nuclear Power Plants (MNPP), due to their mobile nature, there is no grid power, so they need to rely on the own power for operation and safety. To meet current core damage frequencies, the probability of long-term station blackout must be lower than 10^{-5} reactor-year. Adopting probabilistic analysis methods like fault and event trees, a MNPP would need to have large redundancy on diesel generators. However, the same order of long-term station blackout probability can be obtained, with less diesel generators, by the adoption of more realistic scenarios like passive redundancy, replacement of spares, permissibility of short deterministic outage periods before core heat up, etc. Given most part of these scenarios is proven to be realistic, the current methods of probability analysis as fault trees are too conservative.

On the other hand, utilities need reliability, availability, and maintainability (RAM) analysis to make economic decisions, but the use of reliability block diagram (RBD) experience the same limitations of fault trees. In real life, long term unavailability is a critical event as well as accidents. The critical events must have their probability measured for adequate risk management. Systems have repairable failure modes and non-repairable failure modes in the case only short-term unavailability is acceptable because prolonged period for repair is not allowed.

When repairable and non-repairable failure modes are presented on a system, this system is called Partially Repairable Systems (PRS). The reference [6] adopted a repair rate factor which is the repairable failure rate over the total failure rate, to describe this maintainability limitations. When redundancy is presented, it is not possible to measure reliability or failure probability with RBD and fault tree analysis. To measure reliability on redundant PRS, the analysis needs to use an approach of state space models, like Markov chains or Petri Nets [6].

Continuous Markov chains model dynamic reliability scenarios, both analytically and by numerical simulations. Figure 1 presents an example of availability model of redundant systems. Each circle presents a readiness state of the two redundant systems (for instance, circle 1 shows both systems are available, circle 2 shows one is available and the other is unavailable and undergoing maintenance). The arcs present the failure rates or the repair rates and define how much the system transition from one state to another. In case of redundant PRS, failure takes place only both systems fail at the same time, which becomes quite rare when the repairable failure modes are majority. Markov chains suffer from limitations like states explosion and the restriction of being able to use only exponential life distribution. Markov Regenerative Stochastic Petri Nets oblige complex mathematical formalism and still subject to state explosions for large systems.

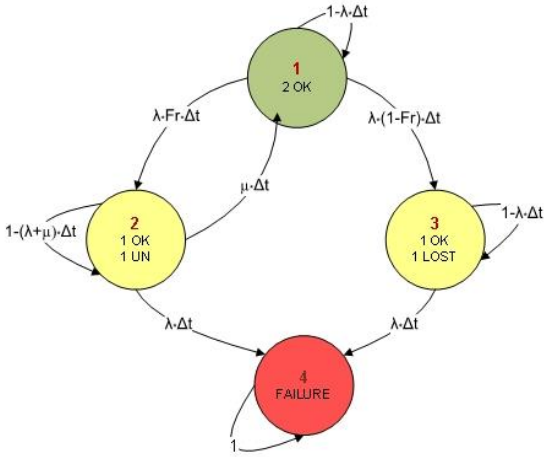

Figure 1 -Example of Markov chain modelling reliability of two redundant systems in parallel [6]

Finally, the Stochastic Colored class of Petri Nets supplies hierarchical organization and include a set of options for transition duration distributions. Because of such characteristics, this work proposes its use for modelling dynamic reliability scenarios as construction of models for large systems is simpler and easier. Petri Nets use places (shown as circles, in this case model a system availability status) and transitions (shown as rectangles). Between places and transitions there are oriented arcs, which define how tokens (shown as black dots) change of position from one place to another through the transitions. A transition can only happen if the input arcs have tokens and when the transition happens, it transfers the tokens to the output arcs. Figure 2 shows a simple Stochastic Colored Petri Nets to measure the reliability and availability of a simple fully repairable part.

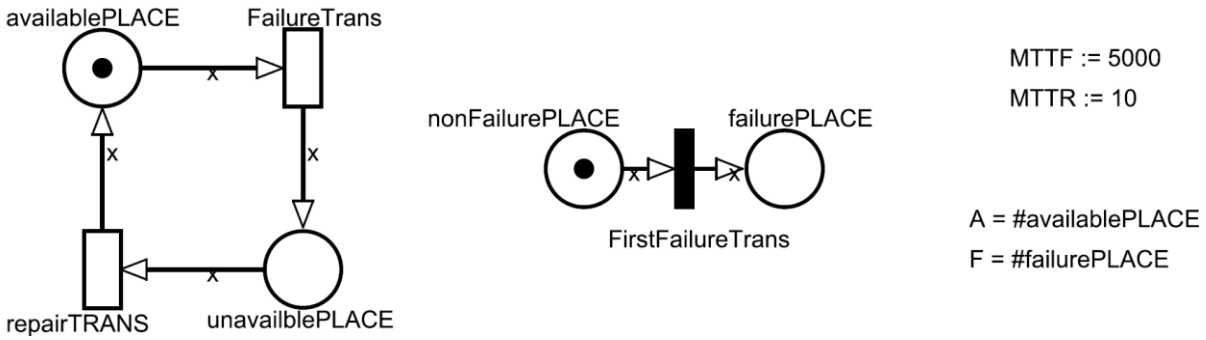

Figure 1 – Example of Stochastic Colored Petri Nets

From an organizational point of view, in the design of complex systems, distinct teams make safety and RAM analyses, each one adopting tools better fitting their own needs. Typically, a Safety Team uses fault tree and event tree analysis and an Integrated Logistic Support (ILS) Team uses reliability block diagrams. It is still worthy to note that design team (people in charge of defining the technical architecture) is also typically distinct of safety and ILS teams. The use of different tools turns obscure the detection of problems and make their correction is even harder, besides creating a burden on configuration management. Whenever there is a change in the technical solution, both safety models (fault and event trees) and ILS models (RBD) need updates. This work aims to improve design quality, reduce design conservatism, and ensure consistency by proposing a single and powerful tool to perform both safety and RAM analysis.

2. MATERIALS AND METHODS

The suggested tool is the Stochastic Colored Petri Nets, which supplies hierarchical organization and a set of options for life distributions. Such characteristics ease analysis of dynamic reliability scenarios and construction of models for large systems.

A Petri Net, PN, consists of places (drawn as circles) and transitions (drawn as bars), which are connected by input and output. Places may have tokens, which are drawn as black dots. A transition is said to be enabled in a marking if each input place contains at least many tokens as the multiplicity of the input arc, and no Guard condition (condition that inhibits the transition) is

satisfied. A transition fires by removing tokens from the input places and adding tokens to the output places. The transitions can be divided into immediate transitions firing without delay (drawn as thin bars) and timed transitions firing after a certain delay (drawn as rectangles). Immediate transitions have firing priority over timed transitions. Conflicts between immediate transitions are resolved by priorities and weights assigned to them. Firing delays of timed transitions are specified by deterministic delays or by random variables with time probabilities functions (drawn as uncolored rectangles). Transitions are only allowed to fire if they are enabled, which means that all the preconditions for the activity must be fulfilled (there are enough tokens available in the input places). When the transition fires, it removes tokens from its input places and adds some at all its output places. The number of tokens removed or added depends on the cardinality of each arc.

Petri nets are a promising tool for describing and studying systems that are characterized as being concurrent, asynchronous, distributed, parallel, nondeterministic, and/or stochastic. As a graphical tool, Petri nets can be used as a visual-communication aid like flow charts, block diagrams, and networks. In addition, tokens are used in these nets to simulate the dynamic and concurrent activities of systems. As a mathematical tool, it is possible to set up state equations, algebraic equations, and other mathematical models governing the behavior of systems.

To study performance and dependability issues of systems it is necessary to include a timing concept into the model. There are possibilities to do this for a Petri net; however, the most common way is to associate a firing delay with each transition. This delay specifies the time that the transition must be enabled before it can fire. If the delay is a random distribution function, the resulting net class is called stochastic Petri net. Distinct types of transitions can be distinguished depending on their associated delay, for instance immediate transitions (no delay), exponential transitions (delay is an exponential distribution), and deterministic transitions (delay is fixed). Sample application areas are communication systems, embedded systems, reliability evaluation, train control systems, manufacturing, supply chains and business processes.

The Stochastic Petri Net proposed is called Colored because each token can be unique (represented by a color), and conditions and measures can be applied for a specific token [7].

For reliability analysis, the MTTF is used as random delay to transition for a failure place. Immediate transitions are drawn as thin bars, useful for build the logical of the net. Deterministic transitions are drawn as black filled rectangles, in reliability, they can stand for any deterministic

event, for instance the time to start a cold stand-by redundant equipment. For example, deterministic transition is used to model the time that batteries can supply power for a system before their depletion. General transitions are depicted as rectangles, filled with gray. It can model uniform, triangular, truncated exponential and finite discrete distributions. It also models normal, lognormal and Weibull distributions, which are the most applied distributions on reliability studies.

Figure 3 presents an example of redundant system, measuring reliability and availability. The same petri net can be used to measure higher levels of redundancy by just increasing the number of tokens on available place.

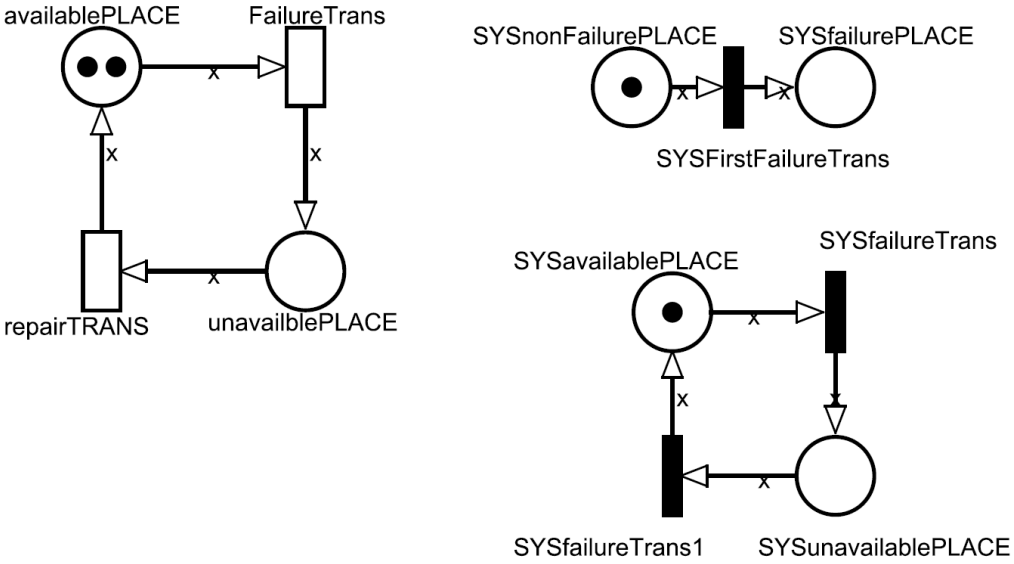

Figure 3 – SCPN for redundant system

This work also proposes quality rules to assure model consistency, as follows:

- Design team should define the Petri Net model because the architects have the best knowledge about the technical characteristics of the systems, including failure modes, failure rates and degraded modes.
- Both safety and ILS make a quality control on the models checking consistency with design documents, completeness of outputs and methods.
- Design team run the calculations to find design basis accidents frequencies and plant availability.

- If results are not satisfactory, design team performs sensitivity analysis to find the cheapest (in lifecycle cost) way to meet criteria or improve lifecycle costs.
- If design needs an architectural change to meet criteria, restart at step 1.

3. RESULTS AND DISCUSSION

This work proposes to use the Stochastic Colored class of Petri Nets (SCPN) [7], which are useful to model complex stochastic events, allowing to solve availability and safety assessments. SCPN include arbitrary attributes on the tokens, allowing distinct treatment for diverse types of tokens. Therefore, the model needs to define attributes of tokens, resulting in colors or types of tokens and transition firings may depend on token attributes and change them. Transitions may have more than one mode of enabling and firing, depending on input tokens.

Taking an example of a standby diesel generating system for a nuclear power plant (NPP), it has only one maintenance team, two redundant diesel generators and a backup battery. The maintenance team can only work on a single diesel generator at a time and the battery has a limited endurance before becoming depleted. Both diesel generators are partially repairable, meaning they have a probability of failing and taking a long time (longer than the safety scenario) to restore its normal function. Also, after losing completely the electrical power, the NPP blackout scenario starts at once, but only after a given time, damage starts as the primary circuit has thermal inertia.

Such situation would require a fault tree analysis considering the global probability of failure of both diesel generators during the mission and the common cause failure modes. Batteries duration, maintenance team interventions and repair rate factor would not enter in the model, resulting in a conservative result (Figure 4). Worse, such analysis ignores the importance of maintenance requirements and crew training.

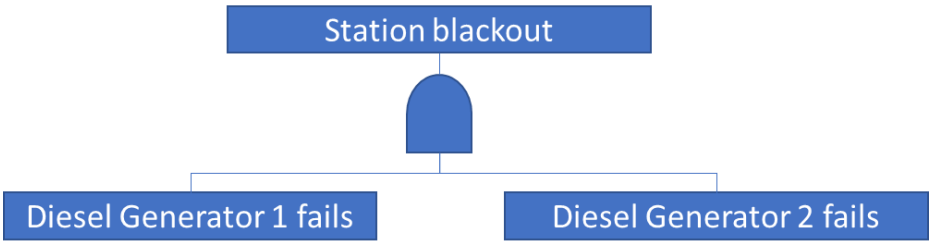

Figure 4 – Reliability model of two redundant diesel generators using fault tree analysis

The proposed alternative is to create a SCPN model like Figure 5 considering availability of maintenance team, repair rate factor and time on battery before start of station blackout.

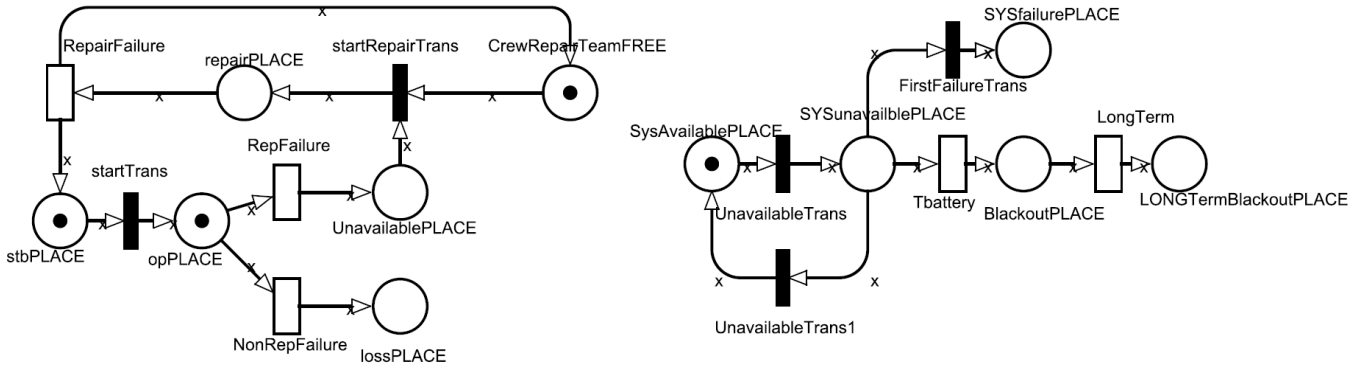

Figure 5 – Reliability model of redundant generating systems (with battery backup) with one maintenance team

Such method for probabilistic analysis may have the effect of shifting systems design from "high-quality components, redundancy, segregation and independency" approach to "maintainability, maintenance and contingency procedures" approach.

This means regulators would pay more attention to crew training and ability and systems maintainability than to classical architectural or design approach. Once the crew is a common cause failure to all systems, the proposed approach should make the MNPPs safer. An effect would be reduction of number of redundancies and high-quality systems (reducing overnight costs along capital costs). A drawback would be higher costs on personnel qualification during the MNPP life and more maintainability requirements towards suppliers, increasing costs a bit.

SCPNs require numerical simulations as analytical solutions are impossible. The typical method is Monte Carlo (simulation of millions of cases to see the overall probability of accidents or availability), which has limitations, like:

- Issues when working in large models: exceptionally large models may require large memory or parallel processing to enable the solution.
- Imprecisions at small probabilities: as current regulations require probabilities in range of $1e^{-6}$ or $1e^{-7}$ per year, Monte Carlo simulations have difficulties to assure precision at such low figures.
- Computation time: associated with model size and high precision of probabilities, Monte Carlo method requires considerable number of simulations meaning large computation times.

The verification and validation effort from the point of view of nuclear authority would increase because the proposed tool requires more input data than the current tools. However, the models would assure greater transparency on design assumptions. Beyond the model verification, nuclear authority would also need to check the model stability and numerical convergence. During the MNPP life, nuclear authority needs to verify if assumptions (mean time to failure, mean time to restore and repair rate factor) matches design assumptions. Besides, that, personnel capability would require constant verification, as it would become a fundamental element on nuclear safety demonstration.

As the same model outputs safety results (top event probabilities) and availability results, overall work during design is smaller and more consistent. Moreover, if designers do the modelling, they also may make sensitivity analysis on RAM parameters, perfecting life cycle costs. Such approach would impose greater number of competencies of designers, which in turn implies in higher human capital and higher pay. However, as the number of models is cut by half, analysis effort (in work hours) should also be cut by half. This means pay could double for people involved without increasing design costs. Considering the major advantage is a MNPP with better RAM characteristics (and lower capital costs) and that design is a small fraction of the cost, it seems reasonable to assume the proposed approach gives a good return on investment.

4. CONCLUSION

This work aimed at three objectives: 1) to improve design quality, which means to assure consistency between safety and Integrated Logistic Support (ILS) models output and system

architectures; 2) reduce design conservatism, meaning to consider human interventions like corrective maintenance activities during safety scenarios; and 3) to ensure consistency between safety and ILS models, meaning that both analysis should adopt the same input data and assumptions. This proposal reached the first goal by giving the analysis task to the system designers, which in turn, generated an issue about effort and time to a single person to develop two distinct models. Proposing a single and powerful tool to perform any probabilistic analysis (safety and ILS alike), this work solved the second and third goal while mitigating the effort issue. The suggested tool was the Stochastic Colored class of Petri Nets, which supplies hierarchical organization, a set of options for life distributions. This tool may model dynamic reliability scenarios for large systems, considering ILS parameters like repair rate factor, maintenance team availability and conditional deterministic events. This work also proposed quality rules to assure model consistency, giving the task of model checking to separate safety and ILS teams, working transversally in all systems, assuring standard procedures. Such method for probabilistic analysis may have the effect of shifting systems design from "high-quality, redundancy, segregation and independency" approach to "maintainability, maintenance and contingency procedures" approach. By modeling complex human and automated interventional scenarios, this method may reduce capital costs while it kept safety and availability of systems. Although such method would demand higher technical capabilities from designers, net effort may reduce, design quality and life cycle costs may improve.

REFERENCES

[1] EYRING, V. et al. Transport Impacts on Atmosphere and Climate: Shipping, Atmospheric Environment. **Journal of Atmosphere and Environment**, v. 44, n. 37, p. 4735-4771, 2009. ISSN 1352-2310. Disponivel em: <http://www.sciencedirect.com/science/article/pii/s1352231009003379>.

[2] ROYAL ACADEMY OF ENGINEERING. **Future Ship Powering Options Exploring alternative methods of ship propulsion**. Royal Academy of Engineering. United Kingdom. 2013.

[3] ONDIR FREIRE, L.; DE ANDRADE, D. A. Historic survey on nuclear merchant ships. **Nuclear Engineering and Design**, n. 293, p. 176–186, 2015. ISSN 0029-5493.

[4] ONDIR FREIRE, L.; DE ANDRADE, D. A. The Role of Nuclear Power from a System Engineering Standpoint. **World Journal of Nuclear Science and Technology**, v. 07, n. 03, p. 167-188, 2017. Disponivel em: <http://dx.doi.org/10.4236/wjnst.2017.73015>.

[5] FREIRE, L. O.; DE ANDRADE, D. A. Economically Feasible Mobile Nuclear Power Plant for Merchant Ships and Remote Clients. **Nuclear Technology**, 2018. ISSN 1943-7471.

[6] SOUZA, G. F. M.; GABE, C. A. **Reliability modeling of partially repairable systems applied on electrical power system**. Annual Reliability and Maintainability Symposium (RAMS). Orlando: IEEE. 2017. p. 1-6.

[7] HAAS, P. J. Colored Stochastic Petri Nets. In: _____ **Stochastic Petri Nets. Springer Series in Operations Research**. New York, NY: Springer, 2002. p. 385-445. ISBN 978-0-387-21552-5.