International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

Use of Reliability Block Diagram and Fault Tree Techniques in Reliability Analysis of Emergency Diesel Generators of Nuclear Power Plants

Vanderley de Vasconcelos*, Wellington Antonio Soares, Antônio Carlos Lopes da Costa, Amanda Laureano Raso
Centro de Desenvolvimento da Tecnologia Nuclear – CDTN/CNEN, Belo Horizonte, Brasil
**Corresponding author*: vasconv@cdtn.br

(Received April 8, 2019; Accepted May 8, 2019)

Abstract
Nuclear power plants (NPPs) are subjected to events such as equipment failures, human errors and common-cause failures, in an environment of complex maintenance, inspection and testing managements. These events will affect the reliability of safety-related systems, as well as the risk level of the plant. Reliability block diagram (RBD) is often used to analyze the effect of item failures on system availability, taking into account their physical arrangement in the system. Fault tree (FT) is a commonly used technique for analyzing risk and reliability in nuclear, aeronautical and chemical industries. It represents graphically the basic events that will cause an undesired top event. Loss of electrical power is one of the main events that influences safe operation of NPPs, as well as accident prevention and mitigation. In case of unavailability of offsite power, emergency diesel generators (EDGs) supply onsite electrical power. This paper carries out reliability analyses of EDGs of NPPs using both RBD and FT techniques. Each technique has its own advantages and disadvantages, allowing a variety of qualitative and quantitative analyses. Outcomes using these two techniques are compared for a typical NPP EDG system.

Keywords- Reliability block diagram, Fault tree, Emergency diesel generator, Nuclear power plant, Reliability.

1. Introduction

The so-called station blackout of a nuclear power plant (NPP) occurs if fail both offsite and onsite power supplies. Loss of electrical power in an NPP impacts its availability and the ability to support safe conditions during shutdown. Typical power sources of NPPs are designed according to the single failure criterion, in such a way that a single event will affect only one source, for instance, through the physical and electrical isolation of their systems. Thus, the likelihood of station blackout occurrence in NPPs must be reduced as low as reasonably achievable, both due to operational safety issues and plant availability (IAEA, 2016).

Failures of emergency diesel generators (EDGs) have a significant role in unavailability of safety-related systems. Thus, reliability requirements of EDGs are design basis for onsite power source systems of NPPs. There are several studies of reliability analysis of EDGs demonstrating their importance for electric power availability and their impact on risks (Battle and Campbell, 1983; Wong, 1984; Sharma et al., 2016). These studies have identified the major contributors for EDG unavailability for different types of NPPs. They include mechanical failure of EDGs, failure in auxiliary systems, common-cause failures (CCFs), human errors (in operation, calibration, maintenance and testing tasks), design failures, shared environmental stresses, etc. Based on these analyses, critical parameters have been identified and more resources have been focused on the most critical contributors to system performance and the availability could be increased.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

Many techniques are suitable to reliability analysis of EDGs in NPPs, mainly in the scope of probabilistic safety analysis (Vasconcelos et al., 2019). Qualitative and quantitative assessments of system reliability can be carried out using, for instance, a reliability block diagram (RBD) or a fault tree (FT). This paper compares these two techniques, which can be used to model and analyze similar types of logical configurations required for EDG reliability analysis. EDGs have usually a configuration of active or standby redundancies, being called into service in case of unavailability of offsite power supply. The advantages and disadvantages of RBD and FT in the assessment of reliability characteristics of this kind of systems are analyzed according to the goals to be achieved. The integrated capability for RBD and FT analyses required by the assessments available in a reliability computer code is also analyzed.

2. Methodology

RBD and FT techniques are compared and their capabilities to assess the reliability characteristics of a typical EDG configuration of onsite electric power generation of an NPP are analyzed. The system to be analyzed as well as RBD and FT techniques are also briefly described.

2.1 Description of System and Techniques

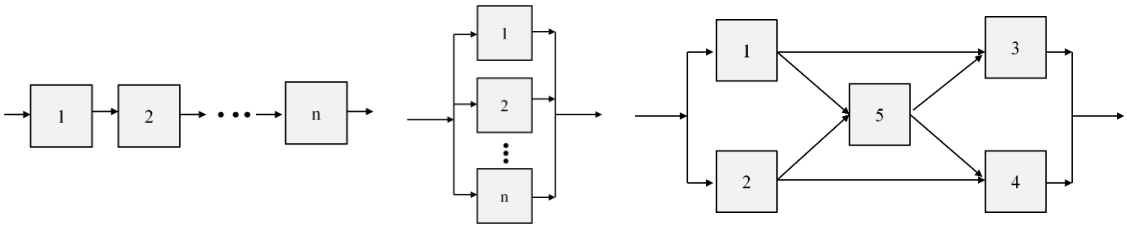
The single failure criterion is extensively used in NPPs in the design of the power sources in order to avoid the loss of nuclear electrical generation, improve safety, and minimize financial impacts. Among the main components of electrical power systems can be highlighted: generators, transformers, and batteries. These components are connected in such a way that provide the most reliable service to the electrical load demands of the facility. In general, EDGs supply emergency power in case of loss of offsite external power (IAEA, 2016).

Typical configurations of onsite power systems in NPPs consist of two redundant, independent and isolated trains, in order to meet the single failure criterion. This is not always achievable, as in the case of interconnections of buses on separate networks. Some of the main functions of EDG systems in NPPs are: provide the safe shutdown of the reactor, feed the emergency heat removal system of the reactor, and enable a safe maintenance of the reactor during shutdown, upon the loss of offsite power. The main components of EDGs with ability of automatic starting and loading are: batteries, control circuits with power supply by independent batteries, diesel engine, generator, cooling system, air and fuel systems, among others (Battle and Campbell, 1983).

2.2 Reliability Block Diagram (RBD)

Reliability block diagram is a graph of system components connected according to their logical relation of reliability. Each component is represented by a box that is assumed to be in operating or failed states. This model enables the analysis of the effect of component failures on different system configurations, as can be seen in Figures 1(a), 1(b) and 1(c), representing RBDs for series, parallel and “bridge” systems, respectively (Vasconcelos et al., 2018).

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064



(a) (b) (c)

Figure 1. Reliability block diagrams for series (a), parallel (b) and "bridge" (c) systems

The reliability of a system with n components in series configuration, R_s, is the probability that all components succeed, as given by Eq. (1):

$$R_s = P(a_1 \cap a_2 \cap \ldots \cap a_n) = P(a_1)\, P(a_2|a_1)\, P(a_3|a_1a_2) \ldots P(a_n|a_1a_2 \ldots a_{n-1}) \quad (1)$$

where a_i is the event "success of component i",
$P(a_i)$ is the probability of success of component i,
$P(a_i|a_1a_2a_3 \ldots a_{i-1})$ is the conditional probability, and
$\cap$ is the intersection symbol taken from set theory.

In parallel configuration, at least one component must succeed in order the whole system succeeds. It is a way to implement redundancy, in order to improve safety and reliability. Probability of failure of system with n parallel components, the system unreliability, U_p, is the probability that all components will be simultaneously in the failure state, as given by Eq. (2):

$$U_p = P(A_1 \cap A_2 \cap \ldots \cap A_n) = P(A_1)\, P(A_2|A_1)\, P(A_3|A_1A_2) \ldots P(A_n|A_1A_2 \ldots A_{n-1}) \quad (2)$$

where A_i is the event "failure of component i";
$P(A_i)$ is the failure probability of component i, and
$P(A_i|A_1A_2 \ldots A_{i-1})$ is the conditional probability.

For the more complex "bridge" systems, the mathematical expressions for reliability are obtained by combinations of Eqs. (1) and (2).

2.3 Fault Tree (FT)

Fault tree is a graphical and logical technique that looks for the possible causes of the top event, usually an undesired state of a system that is critical under safety, reliability or availability viewpoint. FT is a model of logical combinations of basic events, such as component failures and human errors, that will lead to the top event. Fault trees can be analyzed qualitatively or quantitatively. Qualitative analysis includes the identification of the combinations of basic events, which will result in the top events, the so-called "cut sets". The "minimal cut sets" (MCSs) are the most critical "cut sets", i.e., the smallest combinations of basic events that lead to the top event. They are the main events or component sets of the system, which should be prioritized in terms of inspection, maintenance or design modification, when considering the reduction of occurrence likelihood of a specific top event. Quantitative analysis of FTs is the assessment of occurrence probability of the top event, when the basic events probabilities are known. This results in numerical estimations of reliability and availability, including uncertainty assessments. Figures

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

2(a) and 2(b) show, respectively, fault trees for series and parallel systems, using basic events (circles), intermediate events (rectangles) and logic gates ("AND" and "OR" symbols).

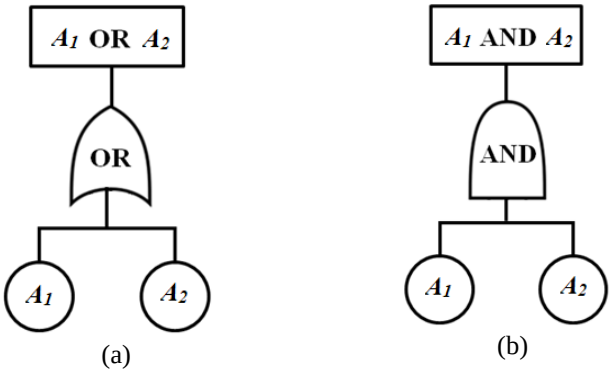


Figure 2. Fault trees for series (a) and parallel (b) systems

Using the set theory concepts (Vasconcelos et al., 2018), the equation for the probabilities of the "OR" and "AND" gates of the fault trees in Figures 2(a) and 2(b), are given by Eqs. (3) and (4), respectively:

$$P(A_1 \text{ or } A_2) = P(A_1 \cup A_2) = P(A_1) + P(A_2) - P(A_1 \cap A_2) \quad (3)$$

$$P(A_1 \text{ and } A_2) = P(A_1 \cap A_2) = P(A_1 | A_2)\, P(A_2) = P(A_2 | A_1)\, P(A_1) \quad (4)$$

where $P(A_1)$ and $P(A_2)$ are the independent probabilities of the basic events, A_1 and A_2, respectively, and $P(A_1 | A_2)$ and $P(A_2 | A_1)$ are the conditional probabilities. The symbols "∪" (union) and "∩" (intersection), taken from set theory, are equivalent to the "OR" and "AND" logic gates, respectively.

Modeling of "bridge" systems as fault trees is a more complicate task that depends on the use of duplicate events, because "OR" and "AND" gates can only depict series and parallel components. Inspecting the "bridge" system shown in Figure 1(c) reveals that any of the following combinations of component failures will cause the system to fail: 1 and 2, 3 and 4, 1 and 4 and 5, and 2, 3 and 5. After this analysis, which is equivalent to get the minimal cut sets from the fault tree, the failure probability of the "bridge" can be obtained using Boolean algebra and the probability laws applied to these combinations of failures (Reliasoft, 2015).

3. Comparison of RBD and FT Features

Table 1 summarizes some features of RBD and FT techniques, highlighting their similarities, differences, advantages and disadvantages. Both RBD and FT are symbolic, analytical and logical techniques that can be applied in analyzing reliability and related characteristics. Most of the logical constructions in FT can also be modeled with an RBD. According to Keisner (2003), RBD and FT provide essentially the same kind of information. In addition, these techniques have limited capacity of modeling systems whose component failures do not have sequential relationships with the system failure as a whole. They do not have capabilities to model reliability interactions among

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

components or subsystems, or to represent system reliability configuration changing (dynamics), such as: active redundancy (sometimes involving load-sharing, a reliability degradation in active parallel systems), standby redundancy (items that are inactive and available to be called into service when active item fails), and other types of interferences, such as dependencies and CCFs. To overcome this lack, the concepts of dynamic FT (DFT) and dynamic RBD (DRBD) were created, extending the original concepts of FT and RBD (Distefano and Puliafito, 2007). These extended concepts enable modeling the time-dependent failures and their analytical and computational implementations.

Table 1. Comparison of RBD and FT Features

Reliability Block Diagram (RBD)	Fault Tree (FT)
Represents the successful pathways of system functions or operation.	Represents the logical relationships of the occurrence of the basic events that can result in the top event (an undesirable event or system failure).
Works in the “success space”, facilitating the computation of system reliability from component reliabilities.	Works in the “failure space”, facilitating the computation of the probability of top event using component failure rates or probability data of basic events.
Models and assess statistically configurations of independent components in series, parallel or combinations of them.	The probability of the top event can be computed by applying the Boolean expressions to the basic events of the fault tree.
Usually is difficult to convert an RBD into an FT, especially complex configurations, e.g., “bridge” configurations.	In general, an FT can be easily converted into an RBD.
Human errors, CCFs, and environmental events outside system boundary are not explicitly included and analyzed in RBD.	Human errors, CCFs and environmental events can be explicitly incorporated into the FTs for quantitative analysis.
Facilitates the computation of reliability characteristics and elucidates the role of redundancy.	Facilitates the computation of importance measures and the investigation of weaknesses of a system using the identified MCSs.
May include time-dependent distributions for the reliability characteristics.	Traditionally it has been used to analyze probabilities in a certain time.
Complex RBDs, as "bridge" configurations, are easily implemented and analyzed.	Representation of “bridges” as FTs is difficult, since it requires the use of duplicate events, due to limitations of “OR and “AND” gates.

These analyses indicate that the FT technique is more flexible than RBD for taking into account human errors, CCFs and environmental events, which are important causes of unavailability of redundant systems such as EDGs. The choice of the best technique will be strongly dependent on dynamic features of the system, the objective of analysis and the available resources of the computer software used in analysis.

4. Evaluation of EDG Reliability

To develop a station blackout quantification model in NPPs it is necessary to describe the possible failure scenarios of onsite power failure after loss of offsite power. Assuming an onsite power system composed of two redundant EDG systems, there are many possible configurations of these systems to perform their intended functions. A comparison among the capabilities of the RBD and FT techniques in evaluating the reliability of an EDG system to perform its design function is done. RBD is used to evaluate two design alternatives of EDG systems in active and standby configurations. FT is used to qualitatively assess the unavailability of an EDG system, taking into account maintainability and CCFs.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

4.1 Use of RBD for Evaluating Redundancy Configurations of EDGs

Although redundancy enhances system reliability and availability, it will also increase weight, space requirements, costs, time to design, complexity and unscheduled maintenance. The increase in unscheduled maintenance can be reduced by design simplification and use of more reliable components (Li, 2016). However, if a redundant component is unavailable prior to the mission start, then the redundancy can be lost, reducing system reliability. Reliability engineering studies are needed for analyzing the use of active or standby redundancy. Active redundancy does not require external devices for checking availability or switching. At this configuration, the redundant component is always in operation to share the load of the system, and automatically pick up the load in case of component failure (load-sharing redundancy). On the other hand, standby redundant configuration requires a switching device, which is involved to detect the failed primary component and turn on the standby one. If this switching device fails while the primary component is operating, the system operates until this component fails. The switching device can also fail on demand when the primary component fails. This introduces a complexity of analysis of availability of standby redundant systems. Figures 3(a) and 3(b) show RBDs for two parallel EDGs, in active and standby redundant configurations, respectively.

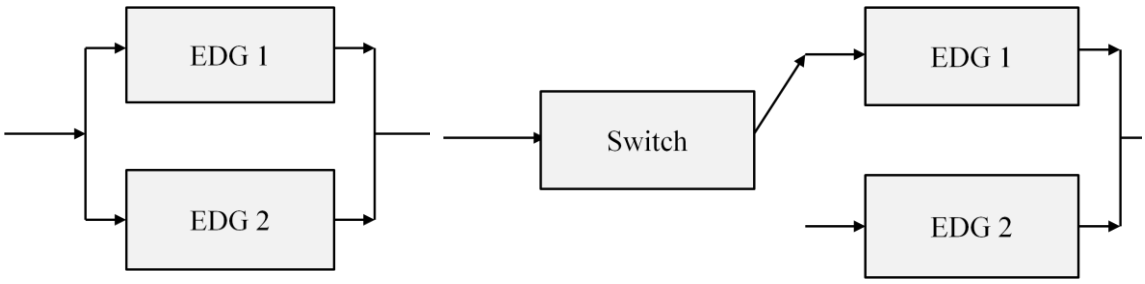


Figure 3. RBD for two EDGs in configurations of (a) “active redundancy” and (b) “standby redundancy” - based on Li (2016)

A reliability characteristic that can be used to compare these two configurations is the mean time between failures, *MTBF*, which can be estimated using Eq. (5):

$$MTBF = \int_0^\infty R(t)dt \tag{5}$$

where *R(t)* is the reliability at time *t*.

Considering an exponential distribution for the reliability function, *R(t)* is given by Eq. (6):

$$R(t) = e^{-\lambda t} \tag{6}$$

where λ is the failure rate of the EDGs.

For the active redundant configuration and non-repairable system, using Eq. (2) for parallel systems and assuming *MTBF* as defined by Eq. (5), results in Eq. (7):

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

$$MTBF = \frac{3}{2\lambda} \quad (7)$$

The reliability assessment of active and standby redundant configurations for repairable systems requires the use of dynamic models to represent system reliability configuration changing, as Monte Carlo method (Durga Rao et al., 2009) or Markov model (Li, 2016). For the standby configuration of non-repairable system, considering EDG 1 and 2 with the same failure rate (λ) and not taking into account the failure of switching device, *MTBF* is simply given by the sum of individual *MTBF* values, as shown by Eq. (8):

$$MTBF = \frac{2}{\lambda} \quad (8)$$

Based on these *MTBF* comparisons, the reliability improvements for the active and standby redundancies are very close. Then, the standby redundancy provides better results, once *MTBF* is nearly 33% greater than the active redundancy. More accurate calculations for different configurations, taking into account maintainability (repair rates), can be carried out using dynamic RBD implemented in computer programs as BlockSim® software with Markov module, developed by Reliasoft® Corporation (Reliasoft, 2015).

4.2 Use of FT for Unavailability Assessment of EDGs

Figure 4 illustrates a simplified fault tree for the top event "Failure of onsite power", used as a case study (IAEA, 1991). This fault tree describes the possible failure scenarios which can result in loss of onsite power.

A qualitative analysis of the fault tree can be carried out by looking for the minimal cut sets (MCSs), using Boolean algebra, specific algorithms, as Vesely-Fussell algorithm (Vesely et al., 1981), or computer codes, as BlockSim® software. As in the fault tree of the case study there are no repeated basic events, the MCS identification can be carried out simply by using Boolean algebra and combinatorial analysis. The MCSs obtained are: the single events A_7 and A_8 (first-order MCSs), and the combinations A_1A_4, A_1A_5, A_1A_6, A_2A_4, A_2A_5, A_2A_6, A_3A_4, A_3A_5 and A_3A_6 (second-order MCSs). The minimal cut set A_3A_6 can be eliminated, considering typical technical specifications of NPPs not allowing both EDGs to be in maintenance at the same time (IAEA, 1991). A qualitative analysis of the fault tree considers that the MCSs of lower orders are, in general, irrespective of their probability of occurrence, the most important contributors to top events. Thus "CCFs of EDGs to start" (event A_7) and "CCFs of EDGs to run" (event A_8) seems to be the highest contributors for the top event. This type of analysis can support the searching of most dominant failure modes that affect EDG systems and prioritizing preventive and corrective measures, improving design and operational procedures in order to increase availability of the onsite power. Based on this analysis, critical parameters can be identified and more resources can be focused on the most critical parameters, and system performance can be improved. These types of results can support EDG maintenance, inspection and testing programs with reliability focus. Independent verification tests are recommended in order to detect CCFs and verify the compliance with single failure criterion (IEEE, 2017).

Quantitative assessment would require evaluating EDG common-cause failure statistics for the specific plants and the use of models and computer programs for complex repairable systems, as the mentioned BlockSim® software. The failure probabilities and component reliabilities used in the quantitative assessments can be obtained from historical data collected from Licensee Event

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 4, 814–823, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.4-064

Reports of NPPs and from operating experience information obtained from NPP licensees (Zubair and Zhijian, 2011).

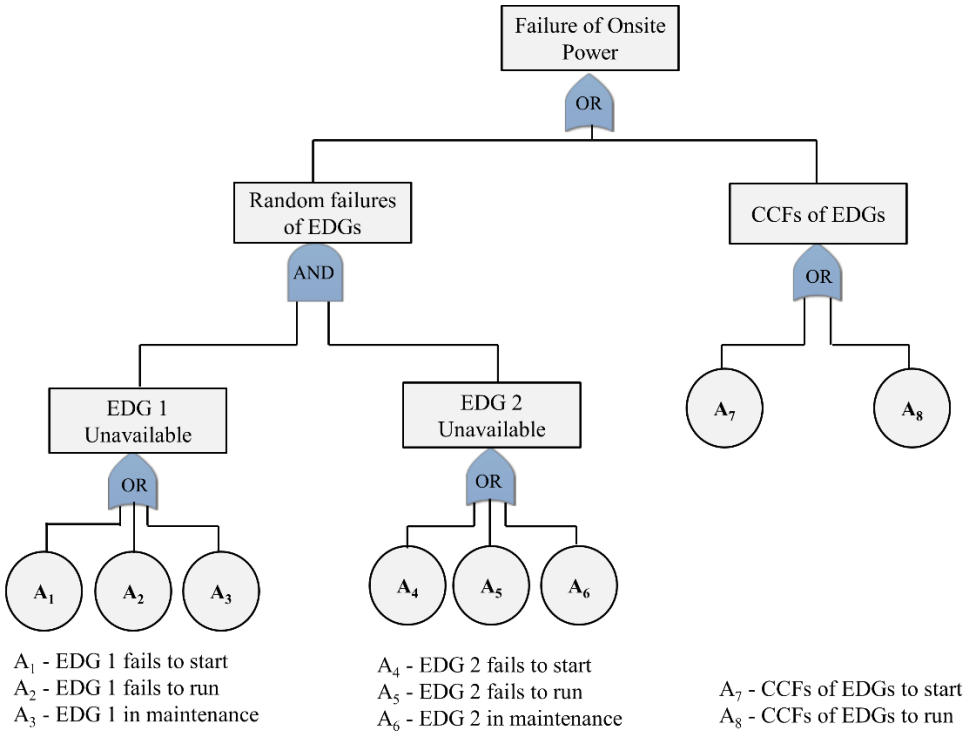


Figure 4. Fault tree for the top event "Failure of onsite power" - based on IAEA (1991)

5. Conclusion and Future Works

It can be concluded that FT technique is more flexible than RBD for taking into account human errors, common-cause failures and environmental events, which are important causes of unavailability of standby systems such as EDGs. The choice of the best technique will be strongly dependent on dynamic features of the techniques available on computer programs used to support the analyses.

RBD was used to evaluate two design alternatives of EDG systems, in active and standby configurations. It was concluded that, mathematically, the reliability improvements for these two configurations are very close, based on *MTBF* comparisons, indicating better results for the standby redundancy (nearly 33 % greater than active configuration). FT technique for the top event "failure of onsite power" was used to qualitatively assess the unavailability of an EDG system, considering start and run failures, maintainability and common-cause failures. Qualitative analysis of the minimal cut sets of the fault tree has identified to be the common-cause failures of EDGs, to start and to run, as the highest contributors to the top event. This qualitative analysis can be used to support the searching of most dominant failure modes that affect both EDG systems and prioritizing preventive and corrective measures, improving design and operational procedures, in order to increase the availability of the onsite power. This work can contribute to elaborate EDG

maintenance, inspection and testing programs of NPPs with reliability focus. In this case, independent verification tests are recommended in order to detect CCFs and verify the compliance with single failure criterion.

The use of dynamic FT (DFT) and dynamic RBD (DRBD), including more accurate assessments of complex repairable active and standby systems, taking into account in the reliability analysis the failure of switching device, are suggestions for future works. Quantitative assessments using plant-specific failure rates and EDG common-cause failure statistics are also suggested for analyzing failure of onsite power of NPPs, considering complex repairable systems. Computer programs having DFT and DRBD resources implemented, as those provided by Reliasoft® BlockSim software with Markov module (Reliasoft, 2015), can support this type of implementation.

Conflict of Interest
The authors declare that there is no conflict of interest in this publication.

Acknowledgements
This work was supported by the following Brazilian institutions: Nuclear Technology Development Center (CDTN); National Nuclear Energy Commission (CNEN); Funding Authority for Innovation and Research (FINEP); and National Council for Scientific and Technological Development (CNPq).

References

Battle, R.E., & Campbell, D.J. (1983). *Reliability of emergency AC power systems at nuclear power plants - NUREG/CR-2989*. Nuclear Regulatory Commission, USNRC, Washington, D.C., USA.

Durga Rao, K., Gopika, V., Sanyasi Rao, V.V.S., Kushwaha, H.S., Verma, A.K., & Srividya, A. (2009). Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliability Engineering and System Safety, 94*(4), 872-883.

IAEA (1991). *Case study on the use of PSA methods: station blackout risk at Millstone Unit 3. IAEA TECDOC 593*. International Atomic Energy Agency, IAEA, Vienna, Austria.

IAEA (2016). *Design of electrical power systems for nuclear power plants. IAEA Specific Safety Guide Nº SSG-34*. International Atomic Energy Agency, IAEA, Vienna, Austria.

IEEE (2017). *IEEE standard for criteria for diesel generator units applied as standby power supplies for nuclear power generating stations. IEEE Std 387-2017*. IEEE Power and Energy Society, IEEE, New York, NY, USA.

Keisner, A. (2003). Reliability analysis technique comparison, as applied to the space shuttle. *AE8900 Special Project, School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA*.

Li, J. (2016). Reliability comparative evaluation of active redundancy vs. standby redundancy. *International Journal of Mathematical, Engineering and Management Sciences, 1*(3), 122-129.

ReliaSoft (2015). *System analysis reference: reliability, availability and optimization*. ReliaSoft Corporation, Tucson, Arizona, USA.

Sharma, P.K., Bhuvana, V., & Ramakrishnan, M. (2016). Reliability analysis of diesel generator power supply system of prototype fast breeder reactor. *Nuclear Engineering and Design, 310*, 192-204.

Vasconcelos, V., Soares, W.A., & Marques, R.O. (2018). Integrated engineering approach to safety, reliability, risk management and human factors. In *Human Factors and Reliability Engineering for Safety and Security in Critical Infrastructures* (pp. 77-107). Springer, Cham.

Vasconcelos, V., Soares, W.A., da Costa, A.C.L., & Raso, A.L. (2019). Deterministic and Probabilistic Safety Analyses. In *Advances in System Reliability Engineering* (pp. 43-75). Academic Press.

Vesely, W.E., Goldberg, F.F., Roberts, N.H., & Haasl, D.F. (1981). *Fault tree handbook - NUREG-0492*. Nuclear Regulatory Commission, USNRC, Washington, D.C., USA.

Wong, S.-M. (1984). *Reliability analysis for the emergency power system of a Pressurized Water Reactor facility during a loss of offsite power transient*. Ph.D. Thesis, Iowa State University, USA.

Zubair, M., & Zhijian, Z. (2011). Reliability data update method for emergency diesel generator of Daya Bay nuclear power plant. *Annals of Nuclear Energy*, *38*(11), 2575-2580.

Distefano, S., & Puliafito, A. (2007, January). Dynamic reliability block diagrams vs dynamic fault trees. In *2007 Annual Reliability and Maintainability Symposium* (pp. 71-76). IEEE.