frontiers in Energy Research

BRIEF RESEARCH REPORT
published: 26 June 2018
doi: 10.3389/fenrg.2018.00060

Sequential Failure Modeling and Analyzing for Standby Redundant System Based on FTA Method

Min Zhang[1]*, *Zhijian Zhang*[1]* and *Gangyang Zheng*[1,2]

[1] *Fundamental Science on Nuclear Safety and Simulation Technology Laboratory, College of Nuclear Science and Technology, Harbin Engineering University, Harbin, China,* [2] *NeUtron eXploration Team, Beijing, China*

Fault Tree Analysis (FTA) has been a well-established and widely used method to deduct system failure scenarios for large complex systems like Nuclear Power Plants (NPPs). Redundant design is usually adopted in NPPs to improve system reliability, including parallel design and standby design. Sequential failures exist among the modules in a standby redundant system, which have not been detailed considered in FTA in industry, leading to an overestimation of system failure probability. Then if FTA is used to compare the reliability of the two designs, it will be found that parallel design is more reliable than standby, which is just the opposite of the conclusion from Reliability Block Diagram (RBD) analysis. To solve this problem, an improved Fault Tree methodology is proposed in this paper, using Priority-AND (PAND) gate and Condition-AND (CAND) gate to model the sequential failures. And the Boolean laws of logic is extended correspondingly for qualitative analysis, as well as the mathematic formulas for quantitative analysis. A case study is also presented to demonstrate the process and benefits for using the proposed approach.

Keywords: fault tree analysis, standby redundant system, sequential failure, Priority-AND gate, Condition-AND gate

OPEN ACCESS

Edited by:
Jun Wang,
University of Wisconsin-Madison, United States

Reviewed by:
Carlos Antonio Sartin,
Universidade de São Paulo, Brazil
Keyou Mao,
Purdue University, United States

***Correspondence:**
Zhijian Zhang
zhangzhijian_heu@hrbeu.edu.cn
Min Zhang
zhangmin@hrbeu.edu.cn

Specialty section:
This article was submitted to Nuclear Energy, a section of the journal Frontiers in Energy Research

Received: *06 May 2018*
Accepted: *06 June 2018*
Published: *26 June 2018*

Citation:
Zhang M, Zhang Z and Zheng G (2018) Sequential Failure Modeling and Analyzing for Standby Redundant System Based on FTA Method. Front. Energy Res. 6:60. doi: 10.3389/fenrg.2018.00060

INTRODUCTION

Fault Tree Analysis (FTA) is a widely used method in system reliability analysis (Lee et al., 1985; Guimarães and Ebecken, 1999), and has been applied to nuclear power industry since early 1970s (NUREG, 1975).

It is a deductive methodology, which connects Top Event (system failure) with a set of Intermediate Events and Basic Events (component failures, human errors, etc.) by logic units like AND/OR gates. System failure paths and contributions of components/events to system failure can be located by FTA results (Vesely et al., 2002).

Redundancy is an effective measure to improve system reliability, including parallel redundant and standby redundant.

Figure 1 shows a typical two-redundant system design, in which the blue parts are unique to standby redundant design while the others for both. In parallel design, A and B are activated simultaneously. While in standby, A will be activated firstly, and then B by switching unit S if A fails.

The Minimal Cut Sets (MCSs) of the two systems are:

Parallel: $A \bigcap B$
Standby:$A \bigcap B, A \bigcap S$

With "no failure in standby" assumption, the standby system failure probability from FTA is bigger than the other, and the conclusion is opposite to that from Reliability Block Diagram analyzing (Bilintion and Allan, 1992). Detailed analysis about the MCSs of the two redundant systems is carried out, and it is found that the FTA has overestimated the failure probability of standby system, by involving two failure paths which should not be considered. They are: (1) B fails before A, which should not happen because B is in standby before A fails; (2) S fails after A, which may happen but should not lead to system failure as B should have been activated before S fails.

These are so called sequential failure problems in this paper, and are defined as:

1) Sequence-Dependent Failure (SDF)—the sequential failures of switching unit and redundant units. It means that the system fails or not depends on the failure sequence of these two types of units; and
2) Condition-Dependent Failure (CDF)—the sequential failures of redundant units. It means that the failure of the former unit is the prerequisite for the later one to fail, as the later unit will not fail until the former one fails.

Sequential failure problems are very common for process systems in which system/components may be placed in service orderly. And several solutions have been proposed to solve these problems in recent years. Representative works including:

- Pandora (Walker and Papadopoulos, 2006, 2009) based on Priority-AND gate to evaluate SDFs;
- Methodologies based on state transfer analysis involving CDF evaluation and other issues in analysis (Azaron et al., 2006; Wang et al., 2012; Hellmich and Berg, 2015);
- Event Sequence Diagram (ESD) (Swaminathan and Smidts, 1999a,b) to model failure of systems/components which are put in service orderly with a time delay; and
- Dynamic Fault Tree (DFT) (Manian et al., 1998; Cepin and Mavko, 2002) for risk evaluation for those systems whose comfiguration may change at different time points.

The first two kinds of methodology focus on only one sequential issue. DFT is designed with house event tables to take system configuration changes into consideration, but not to analyze the sequential issues discussed here. ESD is comprehensive in theory, but too complicated to construct a detailed model for large complex systems.

Hence, this research is to develop an FTA method to analyze both of the two sequential issues. The method suggested should be convenient to be implemented in model construction and computer aided analyzing.

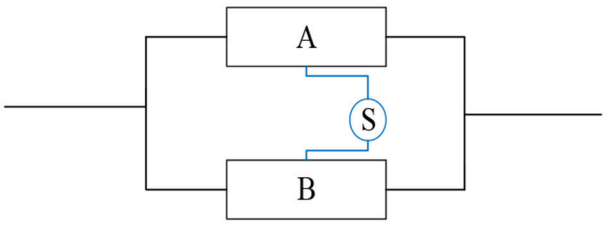

FIGURE 1 | Typical two redundant system.

SEQUENCE-DEPENDENT FAILURE MODELING AND ANALYZING

Priority-AND (PAND) gate is adopted to model the SDFs, which has been defined in Fault Tree Handbook (Vesely et al., 2002) but without qualitative and quantitative analysis laws.

The graphic symbol of PAND gate is shown in **Figure 2**, and the mathematic expression is written as$Q = A \forall B$, which means that event Q will occur if and only if:

1) B has occurred, following the occurrence of A; or
2) Both A and B occur simultaneously.

Most of the basic Boolean logic laws (Verma et al., 2010) are still available for Minimal Cut Sets Analysis for FTs involving PAND gates. For the convenience of reading, they are listed as follows:

Distributive Law:

$$(A \bigcup B) \forall (C \bigcup D) = (A \forall C) \bigcup (A \forall D) \bigcup (B \forall C) \bigcup (B \forall D)$$

Idempotent Laws: $A \forall A = A$
Absorption Law: $A \bigcup A \forall B = A \bigcup (A \forall B) = A$

But it should be noticed that the *Exchange Law* is no longer available for PAND gate, that is$A \forall B \neq B \forall A$.

And for *multiple SDF*, the extended Boolean Laws are:

$$(A \forall B) \forall C = A \forall B \forall C;$$

$A \forall (B \forall C) = (A \bigcap B) \forall C$, which means:

1) All of A, B and C should occur;

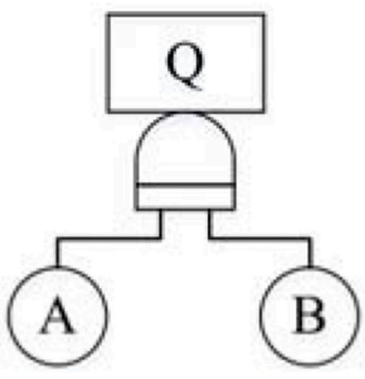

FIGURE 2 | PAND gate.

2) A should occur no later than the time when both B and C have occurred;
3) B should occur no later than C; and
4) A and B can occur in any order.

To calculate the probability of MCSs with SDFs, use

$$P\{A\forall B\forall C,t\}=\int_0^t f_C(t_3)\int_0^{t_3} f_B(t_2)\int_0^{t_2} f_A(t_1)dt_1dt_2dt_3$$

If B is an event with constant probability of Q_B, then

$$P\{A\forall B\forall C,t\}=Q_B\int_0^t f_C(t_3)\int_0^{t_3} f_A(t_1)dt_1dt_3$$

Where,$f(t)$ is the probability density function of an event—the probability that an event may occur at time t.

Any A, B, or C may be a combination of more than one events. If$A=A_1\bigcap A_2$, then

$$f_A(t)=\frac{dF(A_1\bigcup A_2)}{dt}=f_{A_1}(t)F_{A_2}(t)+F_{A_1}(t)f_{A_2}(t)$$

Where, $F(t)$is the distribution function of an event—the probability that an event may occur in time duration of t.

Then for the system in **Figure 1**, the MCS $A\bigcap S$ becomes$S\forall A$, and its probability is

$$P\{S\forall A,t\}=\int_0^t f_A(t_1)F_S(t_1)dt_1$$

CONDITION-DEPENDENT FAILURE MODELING AND ANALYZING

Condition-AND (CAND) gate is constructed to model CDFs. The graphic symbol is shown in **Figure 3**, and the mathematic expression is written as$Q=\langle A\,|B\rangle$, which means that:

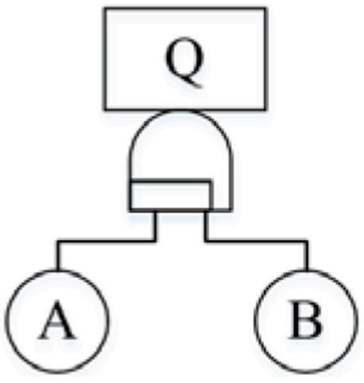

FIGURE 3 | CAND gate.

1) Event Q will occur if and only if both A and B occur; and
2) B never occurs before A.

The basic Boolean logic laws for CAND gate are as follows:

Distributive Law:

$$\left\langle (A\bigcup B)\,\middle|\,(C\bigcup D)\right\rangle=\langle A\,|C\rangle\bigcup\langle A\,|D\rangle\bigcup\langle B\,|C\rangle\bigcup\langle B\,|D\rangle$$

Idempotent Laws: $\langle A\,|A\rangle=A$
Absorption Law: $A\bigcup\langle A\,|B\rangle=A\bigcup(\langle A\,|B\rangle)=A$

Exchange Law is not available for CAND gate either.

And for *multiple CDF*, use the extended Boolean Law:

$$\langle\langle A\,|B\rangle\,|C\rangle=\langle A\,|\langle B\,|C\rangle\rangle=\langle A\,|B\,|C\rangle$$

To calculate the probability of MCSs with CDFs, use

$$P\{\langle A\,|B\,|C\rangle,t\}=\int_0^t f_A(t_1)\int_{t_1}^t f_B(t_2-t_1)\int_{t_2}^t f_C(t_3-t_2)dt_3dt_2dt_1$$

or

$$P\{\langle A\,|B\,|C\rangle,t\}=Q_B\int_0^t f_A(t_1)\int_{t_1}^t f_C(t_3-t_1)dt_3dt_1$$

Then for the system in **Figure 1**, the MCS $A\bigcap B$ becomes $\langle A\,|B\rangle$, and the probability is

$$P\{\langle A\,|B\rangle,t\}=\int_0^t f_A(t_1)\int_{t_1}^t f_B(t_2-t_1)dt_2dt_1$$

HYBRID LOGIC ANALYSIS

The two sequential logic gates discussed separately above usually exist simultaneously in one MCS for high-redundancy system, and the logic is hybrid.

Figure 4 shows a simplified typical composition of a standby triple-redundant system with function modules of A, B, and C. The switching unit is consisted by three sensors (S1–S3) and a processing modular (P). Sensors S1, S2, and S3 are used to monitoring the parameters out from A, B, and C correspondingly. P processes the parameters from sensors and then generates a signal to activate the standby unit orderly if necessary. There are three operation modes for this system:

Mode1: A is put in operation firstly, B and C will be activated one-by-one in order of B and C;
Mode2: B is put in operation firstly, A and C will be activated one-by-one in order of C and A;
Mode3: C is put in operation firstly, A and B will be activated one-by-one in order of A and B.

These modes are completely symmetrical. We assume that the system is operated in Mode1.

The possible hybrid logics and laws to do qualitative and quantitative analysis are:

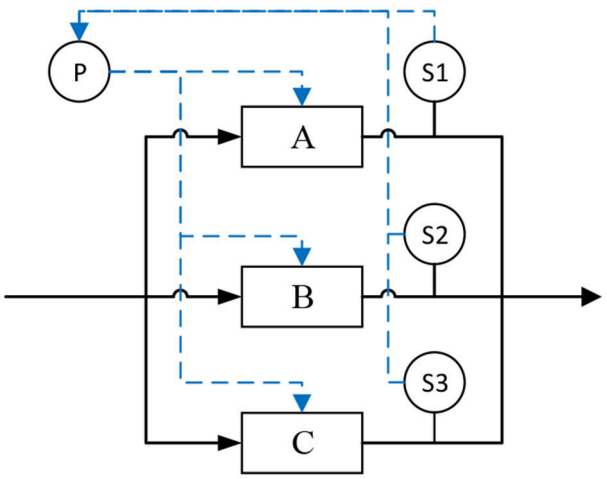

FIGURE 4 | Example of a Triple-redundant system.

1) $\langle (S_1 \forall A) \,|(S_2 \forall B)\rangle$, and

$$P\left\{\langle (S_1 \forall A) \,|(S_2 \forall B)\rangle, t\right\} = \int_0^t f_A(t_1) F_{S_1}(t_1) \int_{t_1}^t f_B(t_2 - t_1) F_{S_2}(t_2) dt_2 dt_1$$

2) $\langle (S_1 \forall A) \,|(S_2 \forall B)\rangle = \langle [(S_1 \bigcap S_2) \forall A] \,|B\rangle$, if B is a failure on demand with a constant probability, and

$$P\left\{\langle (S_1 \forall A) \,|(S_2 \forall B)\rangle, t\right\} = Q_B \int_0^t f_A(t_1) F_{S_1}(t_1) F_{S_2}(t_1) dt_1$$

3) $\langle A \,|(P \forall B)\rangle$, with P as the unit shared by A and B. Then

$$P\left\{\langle A \,|(P \forall B)\rangle, t\right\} = \int_0^t f_A(t_1) \int_{t_2}^t f_B(t_2 - t_1) \int_{t_1}^{t_2} f_P(t_3) dt_3 dt_2 dt_1$$

4) For any A and B, $\langle A \,|(B \forall A)\rangle = B \forall A$.

CASE STUDY

Taking the system shown in **Figure 4** as an example to demonstrate the FTA process using the proposed methodology. And define events as follows:

1. SYS: System is failed.
2. Component name with*: All failures of the component;
3. Component name without*: The primary failure of component;
4. Component name-SW: Failed to activate the component;

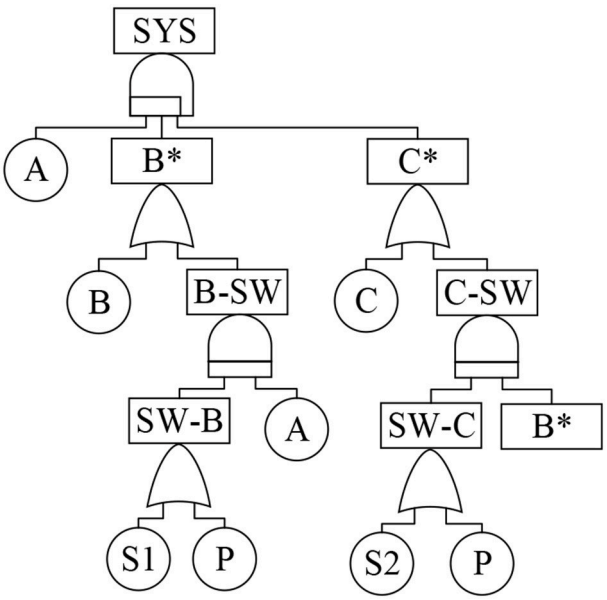

FIGURE 5 | FT for case study.

5. SW-component name: The component is not activated because of the failure of relative switching unit.

The FT is shown in **Figure 5**.

S3 does not appear in the FT. It is because that A and B have failed when C is activated and there would be no standby remained once C is also failed. Then S3 is only used to monitor system parameters and find whether system has failed or not, with no contribution to system function failure.

Apply the extended Boolean logic rules, then

$$\begin{aligned} SYS &= \langle A \,|B* \,|C* \rangle \\ &= \langle A \,|B* \,|C \rangle + \langle A \,|B* \,|C - SW \rangle \\ &= \langle A \,|B* \,|C \rangle + \langle A \,|B* \,|(SW - C \forall B*) \rangle \\ &= \langle A \,|B* \,|C \rangle + \langle A \,|(SW - C \forall B*) \rangle \end{aligned}$$

$$\begin{aligned} B* &= B + B - SW \\ &= B + (SW - B \forall A) \\ &= B + [(S1 + P) \forall A] \\ &= B + (S1 \forall A) + (\mathrm{P} \forall A) \end{aligned}$$

$$\begin{aligned} \langle A \,|B* \,|C \rangle &= \langle A \,|[B + (S1 \forall A) + (\mathrm{P} \forall A)] \,|C \rangle \\ &= \langle A \,|B \,|C \rangle + \langle A \,|(S1 \forall A) \,|C \rangle + \langle A \,|(\mathrm{P} \forall A) \,|C \rangle \\ &= \langle A \,|B \,|C \rangle + \langle (S1 \forall A) \,|C \rangle + \langle (P \forall A) \,|C \rangle \end{aligned}$$

$$\begin{aligned} &\langle A \,|(SW - C \forall B*) \rangle \\ &= \langle A \,|\{SW - C \forall [B + (S1 \forall A) + (\mathrm{P} \forall A)]\} \rangle \\ &= \langle A \,|\{(S2 + P) \forall [B + (S1 \forall A) + (\mathrm{P} \forall A)]\} \rangle \\ &= \langle A \,|(S2 \forall B) \rangle + \langle A \,|[S2 \forall (S1 \forall A)] \rangle + \langle A \,|[S2 \forall (P \forall A)] \rangle \end{aligned}$$

$$
\begin{aligned}
&+\langle A\,|(P\forall B)\rangle+\langle A\,|[P\forall(S1\forall A)]\rangle+\langle A\,|[P\forall(P\forall A)]\rangle\\
&=\langle A\,|(S2\forall B)\rangle+(S2\bigcap S1)\forall A+(S2\bigcap P)\forall A\\
&+\langle A\,|(P\forall B)\rangle+(S1\bigcap P)\forall A+P\forall A\\
&=\langle A\,|(S2\forall B)\rangle+(S2\bigcap S1)\forall A+\langle A\,|(P\forall B)\rangle+P\forall A
\end{aligned}
$$

$$
\begin{aligned}
SYS=&\langle A\,|B\,|C\rangle+\langle(S1\forall A)\,|C\rangle+\langle A\,|(S2\forall B)\rangle\\
&+(S2\bigcap S1)\forall A+\langle A\,|(P\forall B)\rangle+P\forall A
\end{aligned}
$$

Ultimately, there are six MCSs for system failure:

1	$\langle A\,\|B\,\|C\rangle$	Failures of A, B and C, in order of A-B-C.
2	$\langle(S1\forall A)\,\|C\rangle$	Failures of A, S1 and C, in order of S1-A-C.
3	$\langle A\,\|(S2\forall B)\rangle$	Failures of A, S2 and B, in order of A-B and S2-B.
4	$(S2\bigcap S1)\forall A$	Failures of A, S1 and S2, in order of S1&S2-A
5	$\langle A\,\|(P\forall B)\rangle$	Failures of A, P and B, in order of A-P-B.
6	$P\forall A$	Failures of A and P, in order of P-A.

The MCSs of a classical FT are:

1	A.B.C	Failures of A, B and C.
2	A.S1.C	Failures of A, S1 and C.
3	A.S2.B	Failures of A, S2 and B.
4	A.S1.S2	Failures of A, S1 and S2.
5	A.P	Failures of A and P.

Using the same failure rate of 1E-04 h^{-1} for all the components in system, then the system failure probability in 24 h evaluated by the proposed FT method is 2.8892e-06, while the value of classical FT is 5.8013e-06, which is almost twice as much as the former.

From the case study, it is very clear that:

1) Usually, the failure scenarios of a standby redundant system obtained from the classic FT are too extensive (e.g., MCS A.B.C), including the scenarios which shouldn't occur or won't lead to system failure even if occurred;
2) Sometimes, failure scenarios may be omitted by the classic FT (e.g. MCS$\langle A\,|(P\forall B)\rangle$); and
3) System failure probability would be overestimated by the classic FTA, as the mission time of components used in calculation are longer than actual values.

And also it should be reasonable to suspect the accuracy of importance analysis result of the classic FT.

The proposed FT method provides a new perspective to avoid the issues above. It has been applied to an NPP system, under a Project on NPP risk monitor. The qualitative analysis to generate MCSs is implemented manually, and MATLAB program is used to do the quantitative calculation. And a software tool to do a complete analysis is under development.

CONCLUSION

It has been recognized for many years that the order in which the components may fail will affect system behavior in a standby redundant system. But, this issue has not been comprehensively considered yet in industry. The study of this paper aims to find a way to take account of this issue based on FTA methodology.

Firstly, the issue is divided into two categories:

1) Components can only fail in certain order;
2) Components may fail in any order, but only those failures in certain order will lead to a system failure.

Accordingly, two gates, Condition-AND gate and Priority-AND gate, are adopted in this study. The former gate is new constructed, while the later one has been defined in Fault Tree Handbook but not applied because of the lack of qualitative and quantitative analysis rules in the Handbook.

Then, the extended Boolean logic laws are proposed to implement the qualitative analysis of a FT, generating the MCSs with sequential characteristics. The mathematical formulas to calculate MCS probability (quantitative analysis) are also developed, as well as the variations in application.

Finally, a case study is presented to demonstrate the modeling and analyzing process using the improved FTA method. Compared with the results from classical FTA, it is found that the proposed method can lead to more realistic failure scenarios and reduce the conversation of classical FTA.

The future work will focus on how to improve the efficiency of the method for applying to large complex system (e.g., NPP system) when combined with other problems like common cause failure. Also, it is necessary to develop a software to do analysis automatically.

AUTHOR CONTRIBUTIONS

ZZ found the engineering problem and proposed to do this research. MZ was in charge of and implemented the research to find the reason and solution of the problem. GZ helped to verify the method in a industrial system.

ACKNOWLEDGMENTS

This study was supported by the National Science and Technology Major Project Research on Living PSA and Online Risk Monitoring and Management of NPPs [2014ZX06004-003].

REFERENCES

Azaron, A., Katagiri, H., Kato, K., and Sakawa, M. (2006). Reliability evaluation of multi-component cold-standby redundant systems. *Appl. Math. Comput.* 173, 137–149. doi: 10.1016/j.amc.2005.02.051

Bilintion, R., and Allan, R. (1992). *Reliability Evaluation of Engineering System.* New York, NY: Springer.

Cepin, M., and Mavko, B. (2002). A dynamic fault tree. *Reliab. Eng. Syst. Safety* 75, 83–91. doi: 10.1016/S0951-8320(01)00121-1

Guimarães, A. C. F., and Ebecken, N. F. F. (1999). FuzzyFTA: a fuzzy fault tree system for uncertainty analysis. *Ann. Nucl. Energy* 26, 523–532. doi: 10.1016/S0306-4549(98)00070-X

Hellmich, M., and Berg, H.-P. (2015). Markov analysis of redundant standby safety systems under periodic surveillance testing. *Reliab. Eng. Syst. Safety* 133, 48–58. doi: 10.1016/j.ress.2014.08.007

Lee, W. S., Grosh, D. L., Tillman, F. A., and Lie, C. H. (1985). Fault tree analysis, methods, and applications: a review. *IEEE Trans. Reliab. R*-34, 194–203. doi: 10.1109/TR.1985.5222114

Manian, R., Bechta Dugan, J., Coppit, D., and Sullivan, K. J. (1998). "Combining various solution techniques for dynamic fault tree analysis of computer systems,"in *Proceedings Third IEEE International High-Assurance Systems Engineering Symposium* (Washington, DC), 21–28.

NUREG (1975). *WASH 1400 (NUREG-75/014), Reactor Safety Study*. Washington, DC: NRC.

Swaminathan, S., and Smidts, C. (1999a). The mathematical formulation for the event sequence diagram framework. *Reliab. Eng. Syst. Safety* 65, 103–118. doi: 10.1016/S0951-8320(98)00092-1

Swaminathan, S., and Smidts, C. (1999b). The event sequence diagram framework for dynamic probabilistic risk assessment. *Reliab. Eng. Syst. Safety* 63, 73–90. doi: 10.1016/S0951-8320(98)00027-1

Verma, A. K., Srividya, A., and Karanki, D. R. (2010). *Reliability and Safety Engineering*. London: Springer.

Vesely, W. E., Stamatelatos, M., Dugan, J. B., Fragola, J., Minarick, J., and Railsback, J. (2002). *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance, USA.

Walker, M., and Papadopoulos, Y. (2006). Pandora: the time of priority-and gates. *IFAC Proc.* 39, 237–242. doi: 10.3182/20060517-3-FR-2903.00134

Walker, M., and Papadopoulos, Y. (2009). Qualitative temporal analysis: towards a full implementation of the Fault Tree Handbook. *Control Eng. Prac.* 17, 1115–1125. doi: 10.1016/j.conengprac.2008.10.003

Wang, C., Xing, L., and Amari, S. V. (2012). A fast approximation method for reliability analysis of cold-standby systems. *Reliab. Eng. Syst. Safety* 106, 119–126. doi: 10.1016/j.ress.2012.06.007

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.