Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Petri Net Framework For Modelling Standby Dependencies In Fault Trees

Francesco Pugliese [a], Darren Prescott[a], & John Andrews[a]

[a] *University of Nottingham, Nottingham, United Kingdom*

Organiser use only: Received date; revised date; accepted date

Keywords: Standby systems; Dynamic and Dependent Tree Theory method; Fault Tree Analysis; Petri net modelling;

It is widely recognised that the Fault Tree Analysis (FTA) method stands as a cornerstone in the field of reliability engineering and safety assessment, providing a systematic and structured approach to evaluate the potential failure modes within complex systems (Ruijters & Stoelinga, 2015). Specifically, FTA emerges as a powerful tool for identifying, quantifying, and mitigating risks.

However, like any analysis method, it comes with its own set of limitations, especially those associated with standby systems. Standby systems often incorporate redundancy to enhance reliability. Therefore, modelling redundant components and standby configurations in fault trees can lead to complex diagrams, making it challenging to manage and analyse. The increased complexity may obscure important insights and make the fault tree difficult to interpret. Furthermore, fault trees are inherently static, and they may not capture the dynamic behaviour of standby systems adequately. The interactions between active and standby components, state transitions, and the timing of events may not be fully represented.

In addition, FTA often assumes that events are independent (Kabir, 2017), but in standby systems, the failure of one component often affects the reliability of others. This assumption of independence may not be held in complex systems with interdependent components.

Recently, a Dynamic and Dependent Tree Theory (D^2T^2) algorithm has been introduced to enhance FTA, addressing previously mentioned constraints (Tolo & Andrews, 2023). This innovative approach overcomes the typical limitations associated with traditional FT methods by incorporating Petri Nets (PNs), Markov models, and Binary Decision Diagrams (BDDs). Notably, PNs and Markov models enable the development of a complete dynamic model. Conversely, the use of BDDs represents FTs, brings increased efficiency and accuracy, and avoids any computational burden.

Nonetheless, such a D^2T^2 algorithm has not yet been explored to simulate standby systems.

As a result, this study explores the application of Petri net frameworks as a powerful modelling tool for standby systems. Standby systems are prevalent in various domains, including critical infrastructure, telecommunications, and manufacturing, where reliability and efficiency are paramount. PNs, known for their capacity to represent concurrency, synchronisation, and system dynamics, offer a structured and intuitive approach to modelling complex interactions within standby systems. In this research, a detailed analysis of how Petri nets can effectively capture the inherent characteristics of standby systems, such as redundancy, fault tolerance, and system transitions, is presented.

The objective of this research is to establish a robust framework capable of representing the functionality and characteristics of standby systems within a fault tree and subsequently converting this fault tree into an equivalent PN for quantitative analysis. The study focuses on a straightforward standby system, where a fault tree is constructed, and the conversion to an equivalent PN is systematically conducted through a modular approach.

The standby system under consideration is a pump system designed to ensure the continuous flow of lubrication fluids within a bearing lubrication system. This pumping system consists of two streams, each requiring continuous operation. Each stream includes a motor-operated valve (MOV), an electrical pump (P), and a non-return valve (NRV). A sensor (S) located at the system's outlet transmits flow status to a control unit (CON), responsible for activating the MOV and pump in the active stream. In the event of a loss of flow in the active stream, the CON deactivates it, cutting power to the MOV and P, and activates the backup stream.

Fig. 1 shows the pumping lubrication system.

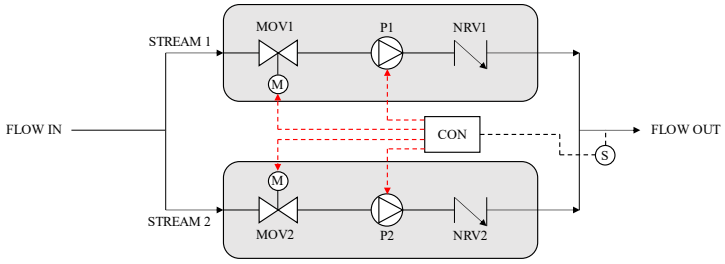

Fig. 1 Pumping Lubrication system

Initially, an FT is developed to elucidate the factors contributing to the failure of each stream and the standby operation. This FT considers various aspects, including the behaviour of active components (e.g., P1, P2) that are electrically powered, receive input from the control system and may encounter failure during warm standby in this scenario. Furthermore, it considers the prioritisation of a specific stream following a system failure and a shared duty cycle, wherein the operation of streams alternates regularly to uphold uniform wear across them.

Consequently, PN modules are devised to depict the functionality outlined in the fault tree. Figure 2 illustrates a part of the Fault Tree representing the failure of a periodic switch between streams, representing a shared duty cycle, and the corresponding PN modules.

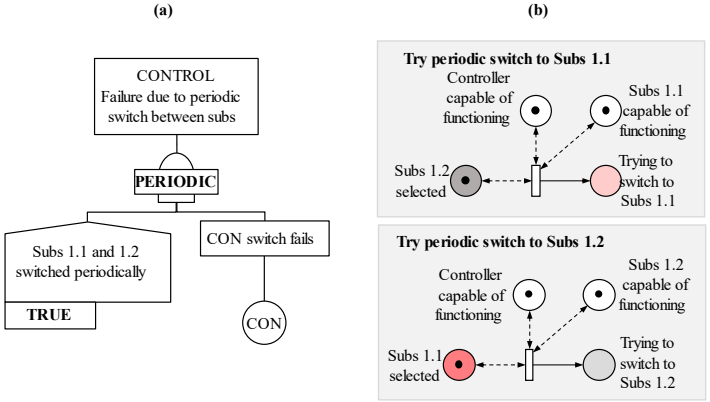

Fig. 2 (a) Fault Tree and (b) Petri net modularisation of the standby system

The modularisation of Petri Nets (PNs) for simulating the Standby system provides the flexibility to be seamlessly integrated into the FTA through the D^2T^2 method. Alternatively, such PN modules can operate independently, serving as standalone modules that can be used to determine the probabilities of FT intermediate events, which represent the failure of standby systems.

Acknowledgements

This work was supported by the Lloyd's Register Foundation, a charitable foundation in the U.K. helping to protect life and property by supporting engineering-related education, public engagement, and the application of research.

References

Andrews, J., Tolo, S., 2023. Dynamic and dependent tree theory (D^2T^2): A framework for the analysis of fault trees with dependent basic events. Reliab. Eng. Syst. Saf. 230, 108959. Author_3, I. year. Title of book. Publisher, City.

Ruijters, E., & Stoelinga, M., 2015. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review, 15, 29-62.

Kabir, S., 2017. An overview of fault tree analysis and its application in model based dependability analysis. Expert Systems with Applications, 77, pp.114-135.