Fault Tree to Petri Net Conversion for the Analysis of a Standby System

Darren Prescott, University of Nottingham, darren.prescott@nottingham.ac.uk

Abstract

Although fault trees are widely used, their quantitative analysis is limited by the need for basic event independence. Dynamic and Dependent Tree Theory (D^2T^2) has been proposed to overcome this limitation and requires dependent system fault tree elements to be analysed using models such as Petri nets, with the results feeding into a wider analysis incorporating the dependent and independent elements. This study involved the development of a method to convert a standby system fault tree to a PN for quantitative analysis.

1 Introduction

Fault tree analysis (FTA) is commonly used for the study and analysis of the safety and reliability of engineering systems. Fault trees are relatively straightforward to construct and provide an excellent representation of how basic events (usually representing component failure modes) combine to cause the occurrence of a top event (representing a system failure mode). Quantitative FTA using Kinetic Tree Theory (KTT) can be used to determine top event probability or frequency. However, KTT is limited since it requires the fault tree basic events to be independent and this is often not the case due to maintenance, inspection and operational features. A common functional dependency, particularly in systems for which reliability is important, is the implementation of standby redundancy. This involves the use of primary and secondary subsystems, with the secondary subsystems used as backups for the primary subsystems in the case of primary subsystem failure.

Alternative reliability analysis techniques, such as Markov analysis or stochastic Petri nets (PN), can deal with the dependencies that make FTA problematic, but they often involve a less intuitive representation of the system failure mode. For this reason, a new FTA framework, Dynamic and Dependent Tree Theory (D^2T^2), has been proposed to overcome the limitations of FTA, taking advantage of the fault tree diagram to represent system failure causality, and using models including Markov models and PN to account for elements of the fault tree containing dependencies that would otherwise make standard methods of quantification impossible [1].

This study aims to provide the basis of a framework: 1. for the representation of standby system functionality and features within a fault tree; and 2. for the conversion of that fault tree to an equivalent PN for quantification. A simple standby system is considered, a fault tree constructed and the conversion of the fault tree to a PN form is carried out using a simple, modular process.

2 Standby system

Figure 1 shows a standby pump system (with structure motivated by systems detailed in [2]), which must ensure flow of lubrication fluid around a closed-loop bearing lubrication system. The system comprises two streams, one of which must be operational at all times, with the other stream acting as standby in case the first stream fails. Each stream consists of a motor-operated valve (MOV), an electrical pump (P) and a non-return valve (NRV). A sensor (FT) on the outlet of the system transmits the state of the flow to a control unit (CU), which ensures power is sent to the MOV and pump on the active stream. In the case that a loss of flow is detected in the active stream, the CU deactivates this stream, cutting the power to its MOV and P, and activates the other, backup stream.

3 Fault Tree Construction and Conversion to PN

A fault tree was constructed to represent the causes of the failure of each stream and also the standby operation. This fault tree accounts for features including: active component behaviour (e.g., P1, P2), which have a power supply, take a control system input and can fail on warm standby in this case; the prioritisation of a particular stream following a system failure; a shared duty cycle, with stream operation alternating regularly to ensure even stream wear.

Figure 1. A two-stream standby pump system forming part of a bearing lubrication system.

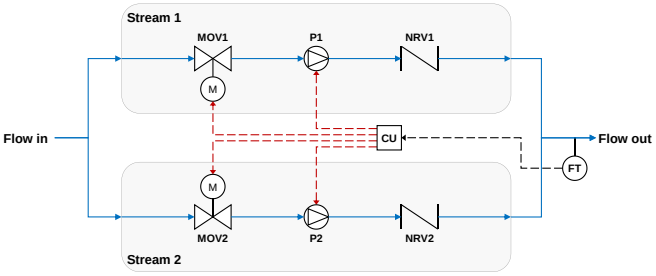
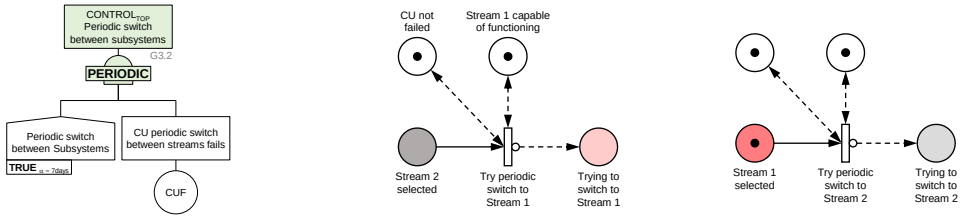


Figure 2 shows a portion of the fault tree constructed to represent the shared duty cycle and the PN modules that can be created to represent the functionality of such a structure. The key advantage of constructing the PN modules in this way is that they can be included or excluded from the overall PN system model depending on whether the particular feature is observed for the modelled system.

Figure 2. A fault tree event representing a periodic switch between streams and its PN module equivalents.



4 Conclusions

A method of converting a fault tree representation of the causes of standby system failure has been developed for an example pump standby system. The purpose is to provide a means to model standby dependencies within the D^2T^2 framework. The developed method is the first step to a general technique that will allow the modelling of any two-stream standby system.

Acknowledgements

This project is funded by the Lloyd's Register Foundation, an independent global charity that helps to protect life and property at sea, on land, and in the air, by supporting high quality research, accelerating technology to application and through education and public outreach.

References

1. Andrews, J., and Tolo, S. (2023) Dynamic and Dependent Tree Theory (D2T2): A Fault Tree Analysis Framework, *Reliability Engineering and System Safety*, vol. 230, 108959, https://doi.org/10.1016/j.ress.2022.108959.
2. Arsenie, A., Hanzu-Pazara, R., Varsami, A., Tromiadis, R. and Lamba D. (2015) A Comparative Approach of Electrical Diesel Propulsion Systems. In: Weintrit A. and Neumann T. (eds.) *Safety of Marine Transport*, CRC Press, Taylor & Francis.