Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_driver

A nested Petri Net – Fault Tree approach for system dependency modelling

Silvia Tolo

Resilience Engineering Research Group, University of Nottingham, UK.
E-mail: silvia.tolo@nottingham.co.uk

John Andrews

Resilience Engineering Research Group, University of Nottingham, UK.
E-mail: john.andrews@nottingham.co.uk

The Dynamic and Dependent Tree Theory (D^2T^2) provides a safety analysis framework able to model complex features of engineering systems, such as dynamic behaviour, complex maintenance strategies or components dependencies which cannot be represented in traditional Fault Tree methods. This is achieved through the tailored integration of flexible modelling techniques, such as Petri Nets and Markov Models, within the Fault Tree framework: differently from similar approaches (e.g., Dynamic Fault Trees), the D^2T^2 methodology does not impose any restriction on the location or type of dependencies. However, when these involve multiple components, such as in the case of redundant trains, the resulting Petri Nets or Markov Models can become rapidly large and convoluted, putting strain on the analyst. This work proposes a generalization of the D^2T^2 methodology based on the nesting of Petri Nets and Fault Trees models: the use of the first is extended to represent dynamic or complex relationship involving entire sets of components (e.g., trains or subsystems represented by section of the main Fault Tree) rather then merely individual ones, dramatically reducing the complexity of the user-defined models. A simple case study is proposed to demonstrate the approach, and the results obtained investigated throughout together with the potential for automatic generation of the dependency models.

Keywords: Fault Trees, Safety Analysis, Component Dependency, Degradation, Markov Models, Petri Nets

1. Introduction

Risk analysis methodologies commonly applied to real-world engineering systems, such as Fault and Event Trees, lack the capability to model realistically the dependencies existing between system components. This limits the accuracy of the prediction of system behaviour due to the need for simplifying but often unrealistic assumptions. The Dynamic and Dependent Tree Theory (D^2T^2) [Andrews and Tolo (2023)] was designed to overcome such limitations and offer a more realistic modelling of system behaviour through the integration of traditional Fault and Event Tree with more flexible techniques such as Petri Nets and Markov Models. These are applied to the modelling of dependencies or complex behaviour (e.g., non-standard maintenance models, dynamic features) of individual components, and the information obtained reintroduced in the initial Fault Tree model in order to proceed with its computation [Tolo and Andrews (2022)]. However, in real-world applications, dependencies often involve entire subsets of components rather than individual ones: this may imply the construction of large Petri Nets or Markov Models representing individual components dependencies and may result challenging for the analysts. This study offers a generalization of the D^2T^2 methodology aimed at simplifying the dependency modelling of subsystems or trains by-passing the representation of their individual components. The suggested approach relies on the identification of the components trains governed by the dependency relationship, and the extraction of the relative sub-trees in the Fault Tree. These sections are then analysed regardless their implicit dependency. The results obtained are then combined into the construction of a Petri Net entailing the independent failure mechanisms of the components in the subsets as well as their dependent relationship.

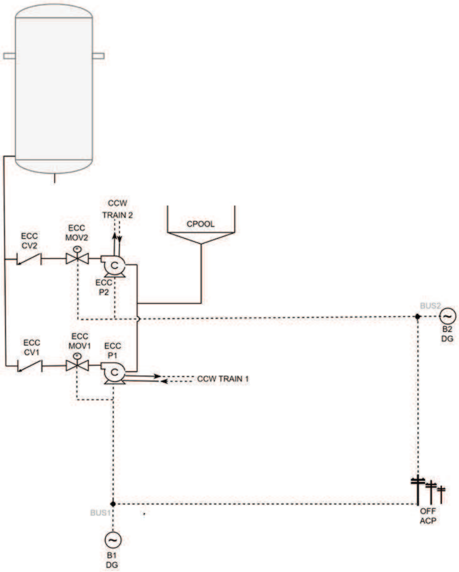

Fig. 1. Overview of the system

2. Case Study

The proposed approach is applied to the Emergency Core Cooling (ECC) system of a Boiling Water Reactor (BWR), consisting of two redundant trains, as shown in Fig.1. Each train includes a circulation pump, a motor operated valve and a non return valve. The two trains, labelled 1 and 2, are fully redundant: train 2 is requested only if train 1 has failed, while it is automatically back in standby when train 1 is repaired (i.e., train 1 has priority). In addition to this activation mechanism, the dependent relationship between the two trains is further complicated by the mutually exclusive servicing (i.e., the two trains cannot be simultaneously in maintenance), and by their dependency to external subsystems, such as power trains 1 and 2, condensation pool (CPOOL in Fig.1) and the Component Cooling Water (CCW) system trains 1 and 2.

3. Application

The proposed approach consists of seven phases, summarised as followed:

(1) **Identification** of relevant sub-trees interested by complex relationships (i.e., sections associated with ECC trains 1 and 2);
(2) **Extraction** of common, explicit source of dependencies (e.g., servicing, power sources, condensation pool etc.) from the sub-trees identified in phase 1;
(3) **Analysis** of the modified sub-trees over a selected time interval and extraction of the resulting failure and repair probabilities;
(4) **Implementation** of the dependency Petri Net modelling the relationship existing between the identified sub-trees. The results obtained from step 4 are adopted, together with the initial input, to capture the independent failure and repair behaviour of the trains/subsystems under study, while the dependencies are explicitly represented by the network;
(5) **Simulation** of the Petri Net dependency model and collection of the converged results, expressed as joint probability of the dependent model sub-sections;
(6) **Re-integration** of the Petri Net output (i.e., joint probabilities) in the initial Fault Tree framework;
(7) **Resolution** of the initial Fault Tree through BDD conversion (including dependencies) according to the D^2T^2 algorithm.

The approach is applied to the system in Fig.1 for demonstration purposes, and the results discussed throughout together with the potential and limitations of the proposed methodology.

Acknowledgement

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. and S. Tolo (2023). Dynamic and dependent tree theory (d2t2): A framework for the analysis of fault trees with dependent basic events. *Reliability Engineering & System Safety 230*, 108959.

Tolo, S. and J. Andrews (2022). An integrated modelling framework for complex systems safety analysis. *Quality and Reliability Engineering International 38*(8), 4330–4350.