Dependent and Dynamic Tree Theory (D^2T^2) for Event Tree Applications

Silvia Tolo, University of Nottingham, silvia.tolo@nottingham.ac.uk

John Andrews, University of Nottingham, john.andrews@nottingham.ac.uk

Abstract

The demand for innovative and effective computational tools able to improve the accuracy of present modelling methodologies has been fuelled by the ever-increasing complexity of engineering systems. In spite of their shortcomings, such as their inability to account for component interconnections or to incorporate degradation processes and intricate maintenance plans into the analysis, classic Fault and Event Trees are still the dominating methodologies of choice for reliability analysis of complex systems.

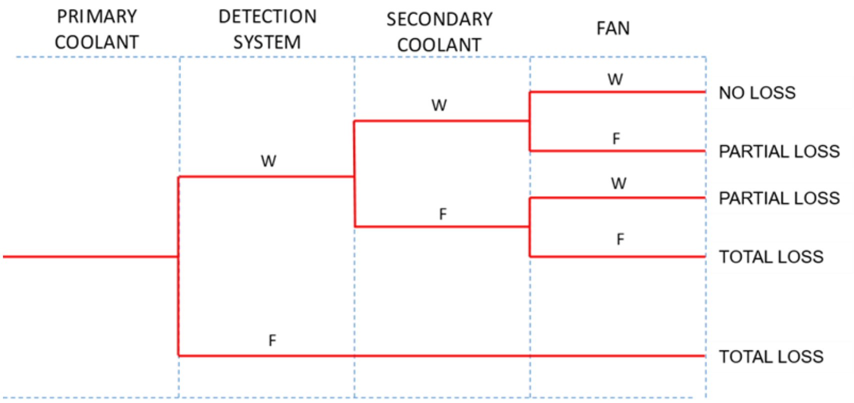
The D^2T^2 methodology was proposed to target the limitations of traditional Fault Trees (FT) through the tailored integration of more flexible modelling options, such as Markov Models (MM) and Petri Nets(PN). This allows to include in the analysis component's dependencies and dynamic features of system behaviour, without renouncing the familiar modelling language of Fault and Event Trees (ET). This work follows the application of the D^2T^2 methodology to a simple case study, investigating how such approach deals with different levels of modelling complexity.

Introduction

The D^2T^2 methodology allows to combine conventional FT/ET with PNs and MMs, ensuring computational viability as well as modelling accuracy. The system setup (in the form of traditional FTs and ETs as well as component failure modes) and, when appropriate, PN/MM models describing complex system features (e.g., components' maintenance strategies or dependencies), make up the input that the analyst is expected to provide.

The approach consists of first locating and isolating independent modules within the FTs provided that contain Dependency Groups. These are intended as closed sets of components whose failure events are interdependent. The Dependency Groups, and associated complex features, are then modelled by means of distinct PNs or MMs (either provided by the user or automatically generated) and analysed. The results obtained by simulation are then reintegrated into the initial FT structure in the form of joint probabilities, through the use of Binary Decision Diagrams. These are finally analysed through custom algorithms able to include in the analysis dependencies in the form of joint probability, resulting in the calculation of the top event probability. Finally, the results are used for the calculation of the ET input.

Figure 1 Event Tree for the system in Figure 2



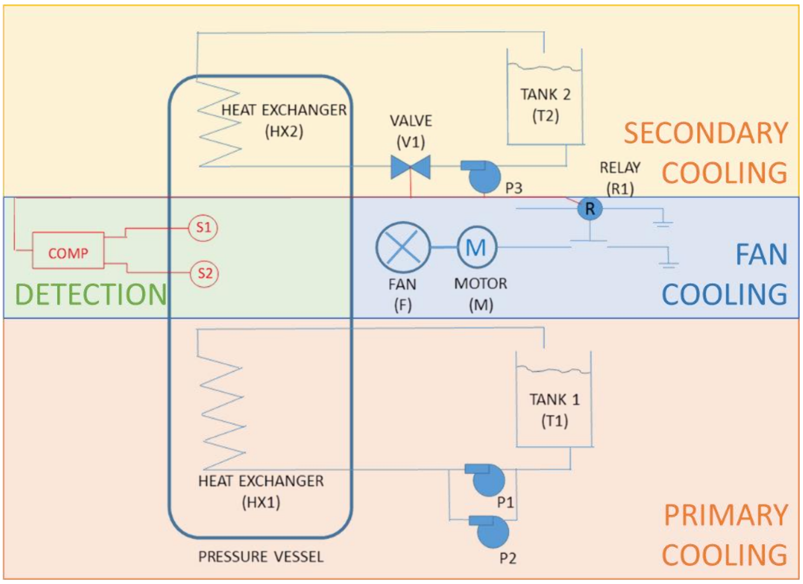
Application

The complexity of the analysis depends on the location and type of dependencies. In order to provide a complete overview of the potential of the methodology, a simplified industrial cooling system (see Figure 2) is analysed. This consists of 4 subsystems potentially contributing to the system failure as shown by the ET in Figure 1: primary cooling, secondary cooling, detection system and fan cooling.

Different assumptions characterised by an increasing degree of complexity are adopted, and summarised by four main case studies:

- Case-study A: component deterioration is taken into account, assuming the tank T1 and heat exchanger HX1 to have non-constant rates of failure and repair. Basic, automatically generated PNs are used to simulate their life cycle and to extract the reliability metrics required for the analysis.
- Case-study B: basic events shared between two or more FTs in input are considered, assuming the secondary system to share pump P2 with the primary cooling system (i.e., in place of P3 in Figure 1). This requires the merging of the two relative FTs, with consequences on the ET computation.
- Case-study C: secondary failures (i.e., triggered by previous failures) are modelled. As the failure of one increases the strain on the other and its failure rate, P1 and P2 are assumed to be dependent on one another. A Markov model is used to capture such dependency.
- Case-study D: the assumptions introduced in Cases B and C are adopted, taking into account dependencies both inside and across the FTs.

Figure 2 Overview of the simplified system under study



Acknowledgement

This work 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., & Tolo, S. (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.

[2] Tolo, S., & Andrews, J. (2022). An Integrated Modelling Framework for Complex Systems Safety Analysis: Case-Studies.