A nested Petri Net – Fault Tree approach for modelling complex failure behaviour in engineering systems

Silvia Tolo & John Andrews
Resilience Engineering Group, University of Nottingham, UK

Fault Trees (FTs) lack the capability to model complex features of engineering systems, e.g., complex maintenance strategies or asset management, that introduce dependencies between basic failure events.

The D2T2 methodology [1] overcomes such limitations through the tailored integration of Petri Nets (PNs) and Markov Models (MMs) with the Fault Tree framework. Such combination is provided maximizing modelling flexibility, while minimizing the size of more sophisticated models, which are restricted to the only dependent events [2].

Nevertheless, the modelling of dependencies involving entire subsets of components, as often encountered in real-world applications, may require the construction of large Petri Nets or Markov Models, putting strain on the analysist.

This research focuses on the generalization of the D2T2 methodology, aiming at simplifying the dependency modelling of multiple components. The approach consists of the computation of subtrees involved in the dependency and the subsequent input of the analysis results into a PN model capturing the dynamic of their relationships. This is in turn computed and the results fed back into the FT framework, resulting in a nested PN-FT framework.

The solution proposed is described and demonstrated through its application to a simple case study involving a safety critical subsystem.

REFERENCES

[1] Andrews, J. and 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, p.108959.

[2] Tolo, S. and Andrews, J., 2022. An integrated modelling framework for complex systems safety analysis. Quality and Reliability Engineering International, 38(8), pp.4330-4350.