The Dynamic and Dependent Tree Theory (D^2T^2) methodology Developed for Fault Tree Analysis

John Andrews, University of Nottingham, Resilience Engineering Research Group, john.andrews@nottingham.ac.uk

Silvia Tolo, University of Nottingham, Resilience Engineering Research Group, silvia.tolo@Nottingham.ac.uk

Abstract

Fault Tree Analysis (FTA) has its origins back in the 1960's with the mathematical framework, known as Kinetic Tree Theory (KTT) added at the end of the decade by Vesely. In KTT the analysis of the fault tree is performed in two stages. The first stage performs a qualitative analysis producing minimal cut sets. The second, quantitative stage, then calculates the system failure mode probability or frequency, along with importance rankings to identify the most significant contributors to the system failure mode. To perform the analysis using KTT requires assumptions to be made about the component failure events such as the independence of all basic events. Also, in most commercial packages, the models employed to evaluate the component failure probabilities assume constant failure and repair rates with limited means of representing the, often complex, asset management strategies employed. These restrictions limit the ability of FTA to represent modern engineering system performance.

This paper describes the D^2T^2 framework which enables Dynamic and Dependent Fault Tree analysis overcoming all of the limitations described above by integrating the capabilities of Binary Decision Diagram, Petri net and Markov modelling methodologies.

1 Introduction

The new fault tree analysis framework known as Dynamic and Dependent Tree Theory (D^2T^2) [1] addresses eth following restrictive assumptions in traditional fault tree analysis:

- Component independence
- Component constant failure and repair rates
- Simplistic maintenance strategies

This is achieved using the capabilities of Binary Decision Diagrams (BDDs) to give an effective, disjoint, structure to the logic function within which the probabilities of the dependent and independent component failures can be accommodated. The probabilities of the dependent failure events are calculated using either Petri Nets or Markov models. The means of expressing the system failure causality retains the conventional fault tree representation with the internal calculation procedures updated to calculate the top event probability and frequency.

2 Dynamic and Dependent Tree Theory (D^2T^2)

The D^2T^2 framework is illustrated in Figure 1. The input data provided includes the fault tree structure and component failure and repair data, similar to conventional fault tree packages, but where failure and repair times are not receptive to exponential distribution. An additional file is required to specify the dependencies which exist between components and the models (Petri Net or Markov) which are used for their analysis.

For an effective analysis process there are two further requirements of the D^2T^2 framework:

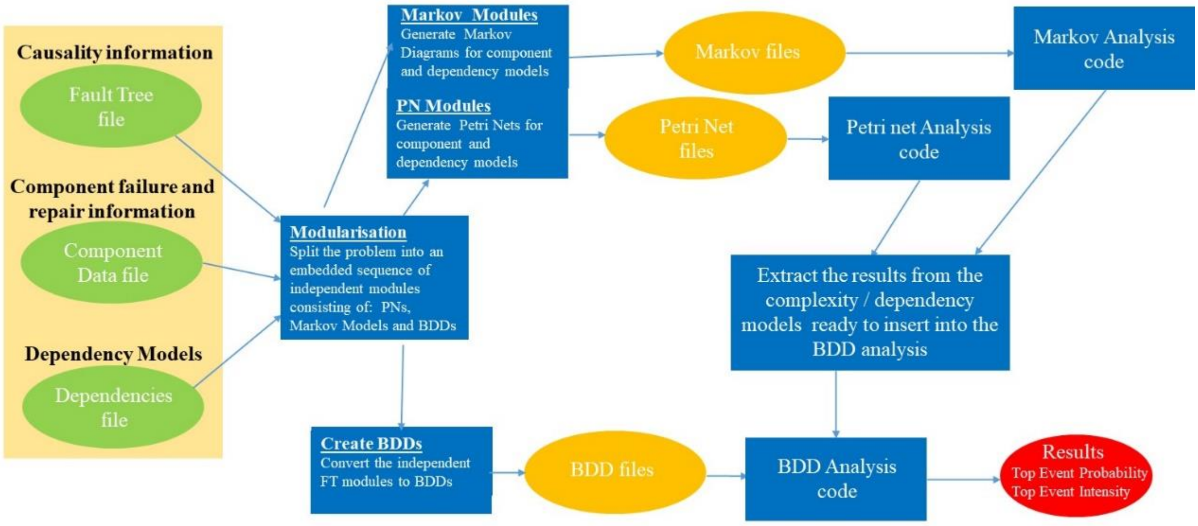
- The dependency models need to be the smallest possible size and consider only the dependent components and no others from the system.

- The BDDs should be made as small as possible by utilising effective variable ordering heuristics and an effective modularisation approach.

Having accepted the input data the algorithm the next phase in the process is to modularise the fault tree int its smallest subtrees, Petri Nets and Markov models. This is achieved by using methods based around the fault tree reduction approaches of Platz and Olsen [2] and Dutuit and Rauzy [3] with appropriate modifications to enable the dependent events to be included.

The modularised sections are then solved suing the appropriate BDD, Petri net or Markov solver and then recombined to give the fault tree top event results.

Figure 1. *D^2T^2 Framework*



This presentation will focus on the modularisation algortihm employed throiugh itsdemonstration to a fault tree with depndencies which represents the failure causes of a a pressure vessle cooling system.

3 Conclusion

The D^2T^2 framework is presented which can be used to analyse fault trees which have dependencies between basic events, components where failure rates or repair fates are not constant and for systems which employ complex asset management strategies.

Acknowledgement: 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.

Refereneces:

1. Andrews, J.D, Tolo, S., (2023), Dynamic and Dependent Tree Theory (D^2T^2): A Framework for the Analysis of Fault Trees with Dependent Basic Events, *Reliability Engineering and System Safety,* Vol 230, 108959
2. Platz, O. and Olsen, J.V. (1976) FAUNET: A program package for evaluation of fault trees and networks, Riso Laboratories Report No 348. DK-4000 Roskilde.
3. Duituit E. and Rauzy, A. (1996) A linear-time algorithm to find modules in fault trees, IEEE Trans Relaibility, 45 No 3, 422-425.