Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Modelling Complexity In System Safety: Generalizing D^2T^2 Methodology

Silvia Tolo, John Andrews

University of Nottingham,Nottingham,U.K.

Keywords: system safety, dependencies, dynamic analysis, fault tree, petri nets

The Dynamic and Dependent Tree Theory (D^2T^2) (Andrews and Tolo, 2023) offers theoretical and mathematical tools to include realistic complex features (e.g., dynamic dependencies, component wear-out, complex asset management strategies etc.) in the safety modelling of complex systems, while retaining the familiarity and efficiency of traditional techniques, such as Fault Tree (FTs) and Event Trees (ETs). This is achieved through the tailored integration of dynamic modelling techniques (e.g., Markov Models, Petri Nets, etc.) within the traditional FT/ET framework, using purposely developed algorithms (Tolo and Andrews, 2023).

However, the current formulation of the D^2T^2 methodology considers complex features, i.e., dependencies, involving individual basic events. In engineering practice, dependencies often involve entire sets of components (for instance in the case of emergency systems trains) or subsystems: in this case, the original D^2T^2 approach can require the implementation of convoluted dynamic models, putting strain on the analysts and hence deluding the very aim of the methodology.

This study offers a generalization of the D^2T^2 approach, modified according to the modelling hierarchy of reference. In common practice, systems modelling for safety analysis purposes is developed on multiple 'layers':

- The overall system behaviour during an accident sequence is modelled through the use of Event Trees: these hence capture the interaction between subsystems and their failure or working states.
- The failure mechanism of individual subsystem is modelled by Fault Tree, which may include sets of multiple components working in accordance towards a common task. These are generally referred as subsystem trains and appear in the FT as intermediate events, and hence sub-trees.
- Any 'measurable' event relevant for the safety of the system, such as the failure of individual components, is represented in the FT as a basic event: this represent the very brick of the overall safety analysis, as well as its numerical input.

The application of the D^2T^2 methodology hence changes according to the 'modelling layer' on which the complex features lie. An overview of the different procedures developed for the application of the D^2T^2 approach at any level of the safety analysis modelling is presented and discussed throughout.

The original formulation of the D^2T^2 methodology and its applications (Tolo and Andrew, 2022) addresses the modelling of complex features (e.g., dependencies, dynamic relationships, complex maintenance strategies) involving multiple basic events. This is achieved through the modelling of such features through the use of dynamic models including the basic events involved and resulting in the computation of the joint probability associated with the possible combination of states of the latter. The joint probabilities are then re-introduced in the analysis through the computation of Binary Decision Diagrams (BDDs) using purposely developed algorithms (Tolo and Andrews, 2023), and hence integrating the dynamic models results in the initial FT/ET framework.

In the case of complex features or dependencies involving FT intermediate events (e.g., subsystem trains failure), the original formulation of the D^2T^2 would still require the factorization of such feature over the basic events enclosed by the relative subtrees. In order to prevent the implementation of large dynamic models, a

preliminary step is introduced in order to reduce the modelling of intermediate events complexities to that of basic events previously discussed. This is achieved according to the following steps:

- The top event failure probability ($\mathbf{Q_x}$) and intensity ($\mathbf{Ix}$) of any intermediate event X included in the complex feature is calculated at n intervals of the mission time domain, such that:

$$\mathbf{Qx} = \{q_x(t_0), q_x(t_1), \dots, q_x(t_n)\}, \quad \boldsymbol{Ix} = \{i_x(t_0), i_x(t_1), \dots, i_x(t_n)\} \tag{1}$$

- The values previously obtained are converted into the failure ($\boldsymbol{\lambda_x}$) and repair ($\boldsymbol{\nu_x}$) (if applicable) rates for the same time values, according to:

$$\lambda_{\boldsymbol{x}}(t_i) = \frac{i_x(t_0)}{1-q_x(t_i)}, \ \nu_{\boldsymbol{x}}(t_i) = \frac{i_x(t_0)}{q_x(t_i)} \tag{2}$$

- Assuming the failure and repair rates to be constant within any i-th time interval considered (t_i), empirical failure ($\mathbf{Fx}$) and repair probability distributions ($\mathbf{Rx}$) for any intermediate event X are constructed over the probability values ($f_x(t_i)$ and $r_x(t_i)$ respectvely) computed at the different time interval considered such as:

$$\boldsymbol{Fx} = \{f_x(t_0), f_x(t_1), \dots, f_x(t_n)\} \, where \quad f_x(t_1) = 1 - \exp(-\lambda_{\boldsymbol{x}}(t_i) \cdot t_i)$$
$$\boldsymbol{Rx} = \{r_x(t_0), r_x(t_1), \dots, r_x(t_n)\} \, where \quad r_x(t_1) = 1 - \exp(-\nu_{\boldsymbol{x}}(t_i) \cdot t_i) \tag{3}$$

- The intermediate events involved in the complex feature are substituted by complex basic events characterized by the equivalent failure and repair distribution expressed in (3). The original D^2T^2 procedure as described in Section 1 can then be applied over the equivalent complex basic events.

Multiple FTs may result dependent on each other, due for instance to shared resources (i.e., supply subsystems in the case under study) or components. The approach adopted in this case relies on the principle of D-separation, as generally known for Bayesian Network application. This consists of 'blocking' the dependency through conditioning, that is instantiating the source of such dependency.

For instance, let assume subsystems A and B to both rely on a third subsystem C. This configuration of course introduces a dependency between A and B, through C. However, if the state of C is known, the dependency between A and B is removed. This can be expressed as:

$p(\text{A,B|C}) = p(\text{A|C})q(\text{B|C})$

Hence, as far as all sources of dependencies between two subsystems are explicitly instantiated, the resulting conditional probability of failure of the two subsystems result independent.

The application of such principle to the analysis of dependent FTs, implies the computation of the top event probabilities of the latter conditional to the state of the dependency sources (being those components or external subsystems). This translates into the analysis of the subsystems failure under predefined scenarios, which are determined by the state of the dependency sources. From a numerical point of view, such conditional probability can be calculated from the analysis of the converted BDD, grouping the BDD paths which include the specific scenarios, and hence the associated dependency sources state.

Acknowledgements

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., 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.

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

Tolo, S., Andrews, J. 2023. Fault Tree analysis including component dependencies. IEEE Transactions on Reliability.