AN INTEGRATED MODELLING FRAMEWORK FOR COMPLEX SYSTEMS SAFETY ANALYSIS: Case-studies

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 ever-increasing complexity of engineering systems has fuelled the need for novel and efficient computational tools able to enhance the accuracy of current modelling strategies for industrial systems. Indeed, traditional Fault and Event Tree techniques still monopolize the reliability analysis of complex systems despite their limitations, such as the inability to capture component dependencies or to include degradation processes and complex maintenance strategies into the analysis.
The current study investigates the application of a novel modelling framework for safety system performance which retains the capabilities of both Fault and Event Tree methods, but also overcomes their limitations through the circumscribed use of more exhaustive modelling techniques, such as Petri Nets and Markov Models. Five case-studies focusing on a simplified industrial plant cooling system are analysed: these cover a range of component dependency types and system settings which cannot be fully represented through the use of conventional fault and event trees.

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

1. Methodology

The novel approach adopted in the current study relies on the integration of traditional Fault and Event Tree (FT/ET) techniques with more flexible modelling strattegies such as Petri Nets (PNs) and Markov Models (MM). The proposed methodology can be broke down in five steps:

(1) *Components Reliability Computation*: the reliability information is calculated for each component according to the input failure mode. If traditional assumptions are not verified (e.g. non-constant failure rate, complex maintenance, etc.), the component lifecycle is simulated through the use of ad-hoc PN/MM models.
(2) *Dependency Groups Processing*: components that are mutually dependent on each other are grouped in closed sets. This isolated dependency groups are then analysed through PNs or MMs. The results obtained are reintegrated into the original FTs.
(3) *FTs computation*: independent FTs are identified and computed through the use of Binary Decision Diagrams Sinnamon and Andrews (1997). This involves the adoption of novel algorithms allowing for components dependencies Tolo and Andrews (Tolo and Andrews).
(4) *ET computation*: the information gathered from the previous step is used for the resolution of ETs. Dependencies among FTs are dealt with through Bayesian theory.

2. System Model and Case-Studies

A simplified power plant cooling system (see Fig.1) has been analysed. This embraces four subsystems, each represented by a FT: the primary system consists of two parallel pumps (P1 and P2) circulating the coolant from a tank T1 to the heat exchanger HX1; the secondary system, embraces a pump P3, a valve V1, a secondary tank (T2) and heat exchanger (HX2); the detection system, whose sensors S1 and S2 are in communication with a programmable logic controller (COMP), requests the activation of secondary cooling when needed; the fan system includes a fan (F) operated

Extended abstract collection of the 32nd European Safety and Reliability Conference.
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini and Simon Wilson

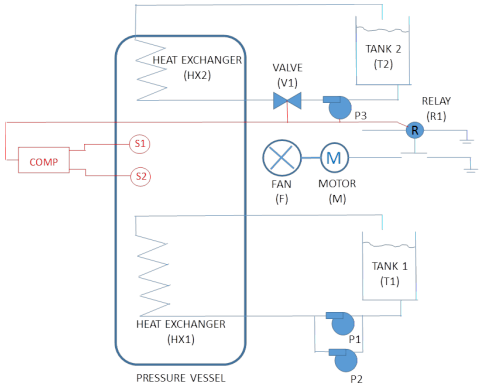

Fig. 1.: System model

by a motor (M) in turn activated by the relay R1.

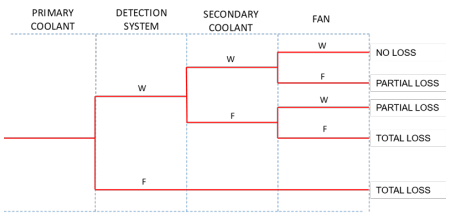

Fig. 2.: Event tree for the system in Fig. 1

Five simple case-studies characterised by different degrees of complexity have been analysed:

- Case Study A: relies on conventional assumptions such as full independence with no component degradation.
- Case Study B: investigates the inclusion of component degradation in the analysis, assuming components $T1$ and $HX1$ to have non-constant failure and repair rate. Their life-cycle is then simulated using PNs.
- Case Study C: focuses on dependencies resulting from shared basic events between two or more subsystems, assuming the secondary system to share pump P2 with the primary cooling system in place of P3. This requires the merging of the two relative FTs.
- Case Study D: investigates dependencies triggered by secondary procedures or processes (e.g. maintenance, load, etc.). P1 and P2 are assumed to be dependent since the failure of one increases the load on the other and its failure rate. The dependency is captured through a Markov model and the joint probability obtained processed in the converted Binary Decision Diagram.
- Case Study E: considers the overlapping of the assumptions in Case C and D, considering dependencies both within and between the FTs.

For each case study, the frequency of coolant losses were estimated according to the three categories shown in the event tree of Fig.2. The results are shown in Table 1.

Table 1.: Estimated frequency (h^{-1}) per loss type

	NONE	PARTIAL	TOTAL
CASE A	$1.161e^{-05}$	$2.136e^{-07}$	$8.074e^{-08}$
CASE B	$1.195e^{-05}$	$2.200e^{-07}$	$8.316e^{-08}$
CASE C	$1.441e^{-05}$	$7.469e^{-06}$	$2.426e^{-07}$
CASE D	$3.564e^{-05}$	$6.559e^{-07}$	$2.479e^{-07}$
CASE E	$3.961e^{-05}$	$3.093e^{-05}$	$8.723e^{-07}$

3. Conclusions

A novel methodology for the safety analysis of complex system was tested against five case-studies entailing a simplified industrial cooling system. The case-studies cover a range of component dependency types and system settings which cannot be fully represented through the use of conventional fault and event trees. The results obtained are compared to those achieved with existing techniques, in order to verify the accuracy as well as the computational efficiency of the implemented algorithms.

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

Sinnamon, R. M. and J. Andrews (1997). Improved accuracy in quantitative fault tree analysis. *Quality and reliability engineering international 13*(5), 285–292.

Tolo, S. and J. Andrews. Fault Tree analysis including component dependencies. *Currently Under Review*.