Next Generation Prediction Methodologies and Tools for System Safety Analysis (NxGen) – A Project Overview

Kate Sanderson, University of Nottingham, Resilience Engineering Research Group, Kathryn.Sanderson@nottingham.ac.uk

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

Abstract

Modern engineering systems are rapidly increasing in size and complexity, posing greater safety and risk management challenges than ever before. In addition to this, the threats to these engineering systems are constantly changing and new hazards emerging.

Modern Engineering System Features

- An increased use of new technologies
- Operational regimes which restrict the opportunity for maintenance
- Operation of an engineering system beyond its planned design lifetime
- An increased exploitation of condition based maintenance
- The use of complex, phased maintenance strategies
- Use of autonomy

System Threats

- Component failure
- Human error
- Natural disasters
- Extreme weather conditions
- Climate change
- Terrorism
- Cyber attacks

Risk modelling methodologies need to adapt to keep pace with these changes and evolving threats in order to support the effective decision making needed to produce safe systems or facilities. However, the foundations of current risk assessment tools and methodologies for safety critical systems (established in the 1970s) remain unchanged, despite the considerable advances research has made in the capabilities of analytical techniques since then.

The challenge of this 5 year project is to account for all of these factors in developing a single methodology appropriate to meet the demands of modern industrial systems and to implement them in a software tool that has the potential for wide distribution and impact. The tool, accompanied by comprehensive documentation, could be adapted by users to reflect the needs of their system assessment.

This new, generic, approach to system failure modelling will enhance the traditional, currently used risk analysis methods: Event Tree Analysis and Fault Tree Analysis, which have limitations in terms of their applicability to modern systems resulting from the assumptions implicit in the modelling approaches such as:

i. Independent basic events

ii. Constant failure and repair rates for components

iii. Limited ability to represent modern maintenance strategies

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

The NxGen Project proposes a new fault tree analysis framework - Dynamic and Dependent Tree Theory (D^2T^2) which can overcome the restrictions and limitations of the traditional methods. Whilst retaining the fault tree structure to express the causality of the system failure, the internal calculation method is updated by exploiting features of Binary Decision Diagrams, Stochastic Petri Nets and Markov methods.

The D^2T^2 framework offers a practical generalised solution, with the following objectives:

1) To enable component failure and repair times to be represented by any probability distribution.

2) To incorporate the ability for dependencies of any type (due to system structure, operation or maintenance) to be accommodated between components or sub-systems.

3) To facilitate the representation of complex maintenance processes to represent the sophisticated asset management strategies employed on modern systems.

4) To permit dynamics in the form of event sequences to contribute to the system failure logic.

A key point is the retention of the fault tree structure, which is familiar to engineers and lends itself to visualisation of the system failure causes. This also facilitates transparency, peer review, and assessment by regulators, and enables fault tree models evolved over many years to be upwardly compatible with D^2T^2.

Project Partners

In addition to the contributions of our international academic partners on the project, (Professor Ali Mosleh - UCLA, and Professor Antoine Rauzy - NTNU), collaboration and input from our industrial partners is fundamental to the success of this research. Industry sectors involved in the project so far include:

- Nuclear: Rolls-Royce (Submarines), Rolls-Royce (Small Modular Reactors), Bhaba Atomic Research Centre (India), Indira Ghandhi Centre for Atomic Research (India)
- Aero: Rolls-Royce (Aero Engines), BAE Systems
- Railway: Network Rail, FirstGroup, High Speed 1, Rail Safety and Standards Board, Network Rail High Speed, High Speed 2

Development into new industry sectors includes: Maritime - Carnival Cruise Line, and Automotive - MIRA (Motor Industry Research Association)

This presentation will provide an overview of the project, describing our objectives, phases of work, demonstration through industrial case studies and its longer term impact. Particular attention will be given to our outputs, available reports and resources, industrial engagement, and our future plans for dissemination and collaboration.

https://www.nottingham.ac.uk/research/groups/resilience-engineering/nxgen-project/nxgen.aspx

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