Next Generation Prediction Methodologies and Tools for System Safety Analysis

Welcome to the first edition of our NxGen Project Newsletter

Our team in the Resilience Engineering Research Group at the University of Nottingham are leading a challenging project to develop a new generic methodology for improved system safety analysis.

Informed by our industrial partners in the aerospace, rail, and nuclear sectors, this 5 year project, funded by Lloyd's Register Foundation, proposes a step change in modelling capabilities, to represent more accurately modern engineering systems, which are rapidly increasing in size and complexity.

In this first project newsletter, we hope to outline the project objectives and introduce our developing modelling framework - **Dynamic and Dependent Tree Theory (D^2T^2)**. Our aim is to spark discussion and collaboration, share our findings, and encourage feedback.

To get involved contact the NxGen Team

NxGen Key Information:

Duration: 5 years

Funder: Lloyd's Register Foundation

Project Lead: Prof John Andrews

Academic Collaborators: Prof Ali Mosleh (UCLA), Prof Antoine Rauzy (NTNU)

Industrial Case Study Partners: Rolls Royce (aerospace and nuclear), High Speed 1 (HS1), Rail Safety and Standards Board (RSSB)

John Andrews - NxGen Project Lead
Professor of Infrastructure Asset Management
University of Nottingham

NxGen Website

NxGen Project Overview

Background:

The foundations of current risk assessment tools and methodologies for safety critical systems were established in the 1970's. Technology has advanced, and system designs, their operational conditions and maintenance strategies, are now significantly different to the types of systems that existed 50 years ago. This can limit the capability of current prediction methods to adequately represent their failure performance where; dependencies exist between components; components degrade over time; and complex asset management strategies are employed.

The Project:

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 this in a software tool that has the potential for wide distribution and impact. The tool could be adapted by users to reflect the needs of their individual system assessment characteristics.

Modern Engineering System Features:

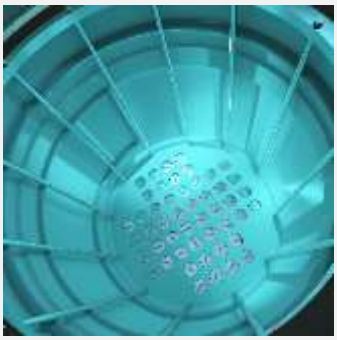
- An increased use of new technologies
- Operational regimes which restrict the opportunity for maintenance
- Operation of an engineering system beyond its planned design lifetime
- An increased exploitation of condition based maintenance
- The use of complex, phased maintenance strategies

System Threats:

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

Our Key Objectives

As a consequence of employing the new tools it is expected that the quality of the decisions made to control the risks associated with the operation of hazardous systems and infrastructure will improve, and there will be:



- Better informed decision making to avoid or mitigate accidents
- A reduced risk of fatalities to the public and workforce
- Reduced risk of incidents which cause damage to infrastructure
- A reduced risk of environmental pollution
- Optimising the most cost effective use of limited resources available
- Increased productivity
- Increased knowledge in the community

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

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: independent basic events, constant failure and repair rates for components, and only a limited ability to represent modern maintenance strategies.

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.

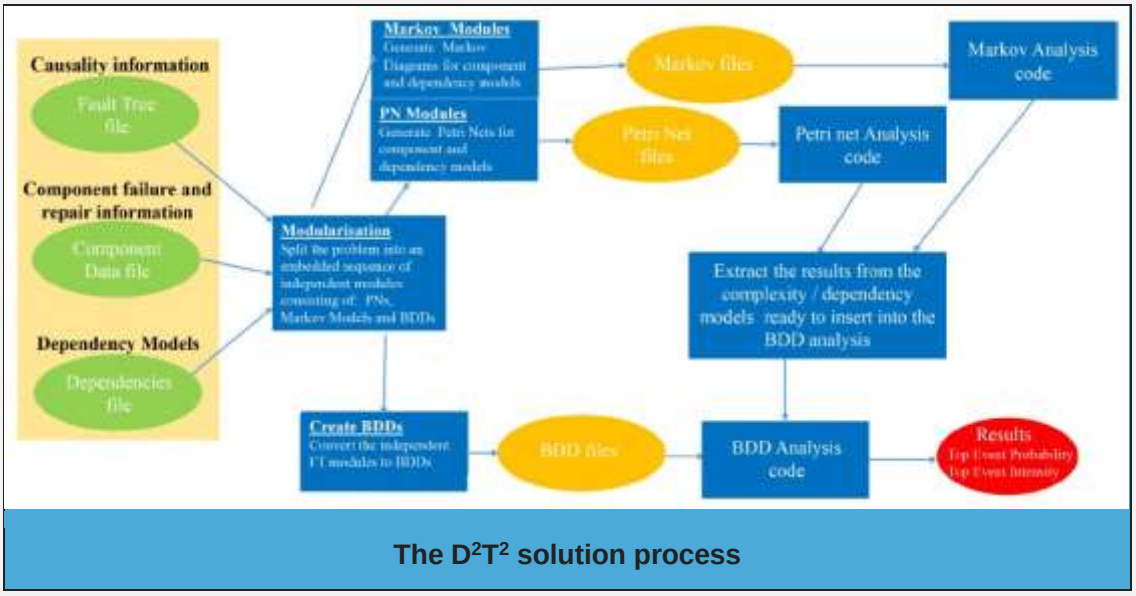
The D^2T^2 framework offers a practical generalised solution, with the following objectives:

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.



The D^2T^2 solution process

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 .

Lloyd's Register Foundation

Lloyd's Register Foundation is an independent global charity that supports research, innovation, and education to make the world a safer place.The charitable mission of the Foundation is "To secure, for the benefit of the community, high technical standards of design, manufacture, construction, maintenance, operation and performance for the purpose of enhancing the safety of life and property at sea, on land and in the air. The advancement of public education including within the transportation industries and any other engineering and technological disciplines". Lloyd's Register

Foundation are engineering a safer world by focussing on the biggest safety challenges facing society. To find out more visit lrfoundation.org.uk

Meet the Team

Professor John Andrews - Project Lead

John Andrews is Professor of Infrastructure Asset Management in the Faculty of Engineering at the University of Nottingham, and a member of the Resilience Engineering Research Group. Prior to this he worked for 20 years at Loughborough University where his final post was Professor of Systems Risk and Reliability. Full profile.

Dr Silvia Tolo - Senior Researcher

Silvia Tolo gained an MSc with honours in Energy and Nuclear Engineering from the University of Bologna in 2012, and a PhD in 2016 with the Institute for Risk and Uncertainty at the University of Liverpool. She worked as a research associate at the same Institute, on the UK national research programme Digital Reactor Design in 2018 before moving to Nottingham. Full profile.

Dr Sally Lunt - Researcher

Sally Lunt gained a PhD in Risk and Reliability assessment in 2002 from Loughborough University. She spent many years in education before returning to research as a research associate with the University of Nottingham in 2022. Her work is focused on developing efficient computational methods to quantify phased mission systems, and importance measures.

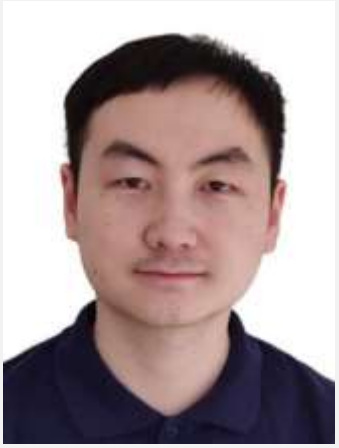
Dr Francesco Pugliese - Researcher

Francesco Pugliese is a civil engineer and recipient of an EPSRC Doctoral Prize Fellowship at the University of Nottingham, where he has focussed on the development of optimised approaches for improving the asset management of ageing critical infrastructure. He gained his PhD in risk and uncertainty applied to civil engineering from the University of Liverpool. Full profile.

Kate Sanderson - NxGen Project and Impact Manager

Kate is the Lloyd's Register Foundation NxGen project coordinator, managing all administrative and organisational aspects of the research. Kate is responsible for developing and monitoring pathways to impact for the methodologies and tools developed.

Dr Derek (Rundong) Yan



Dr Derek (Rundong) Yan is an Assistant Professor in System Risk and Reliability Modelling at the University of Nottingham. He graduated with an MEng from Imperial College London, UK in 2015, and completed a PhD in Control and Reliability at Loughborough University in 2020. Full profile.

Dr Darren Prescott

Darren Prescott is an Assistant Professor in Risk and Reliability Engineering in the Resilience Engineering Research Group at the University of Nottingham, where he has worked since 2010. Prior to this, he worked as a Lecturer at Loughborough University where he previously gained BSc and MSc degrees before being awarded a PhD in 2006 for his research on the application of Monte Carlo simulation techniques for the reliability analysis of degraded redundancy operation in aircraft. Full profile.

Key Outputs

Our aim is to share our work as widely as possible, open access and open source, for the benefit of all. To explore the development and findings of our research, through the publications, reports, and presentations produced to date, visit the "Outputs and Publications" page of our website. Our current key outputs are accessible below:

Dynamic and dependent tree theory (D^2T^2) : A framework for the analysis of fault trees with dependent basic events

John Andrews, Silvia Tolo. *Reliability Engineering & System Safety*, Vol. 230, February 2023, 108959.

This paper proposes a new fault tree analysis framework which can overcome these restrictions. Whilst retaining the fault tree structure to express the causality of the system failure, the internal calculation method is updated by exploiting features of the Binary Decision Diagram, Stochastic Petri Net and Markov methods. The key elements of the D^2T^2 algorithm are described in detail and the framework demonstrated through application to a case study example of a pressure vessel cooling system.

Access the pdf.

Next Generation Fault Tree Analysis Methods - A Tutorial

John Andrews, Silvia Tolo. January 2023.

Access the text document.

Access the presentation slides.

Get Involved

Our aim is to develop a community of industry practitioners, risk analysts, engineers, researchers, and academics, with an interest in safety risk management challenges, across a diverse range of industrial sectors. If you are interested in joining our network to learn how our methodologies and tools could enhance your work please contact us.

Contact the Team

Our mailing address is:
kathryn.sanderson@nottingham.ac.uk

.