Next Generation Prediction Methodologies and Tools for System Safety Analysis

Welcome to the second edition of the NxGen 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. The project objectives and a more detailed introduction to the work can be found on our website.

In this newsletter we update you on our recent activities and outputs centred on 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)

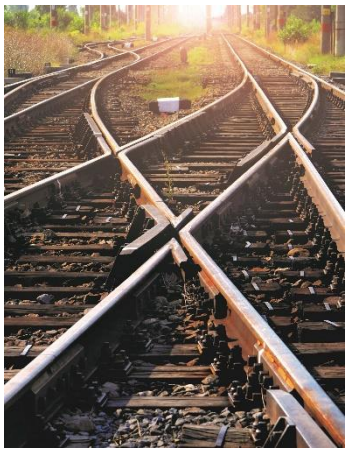
John Andrews - NxGen Project Lead
Professor of Infrastructure Asset Management
University of Nottingham

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

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, both of 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.

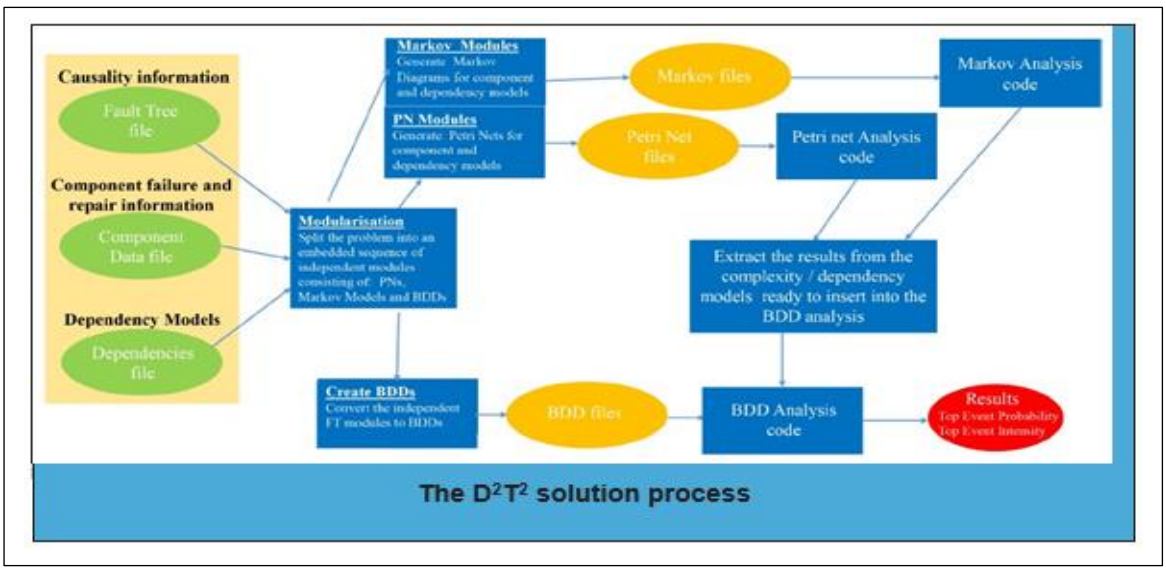
The D^2T^2 framework offers a practical, generalised solution, with the following objectives:

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.



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 .

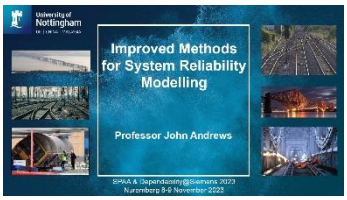
Dynamic and dependent tree theory (D^2T^2) : A framework for the analysis of fault trees with dependent basic events

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

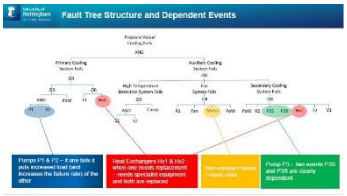
In this paper the key elements of the D^2T^2 algorithm are described in detail and the framework demonstrated through application to a case study example of a pressure vessel cooling system.

Access the pdf.

SPAA & Dependability@Siemens 2023 Nuremburg



Professor John Andrews gave the invited keynote speech in November at the Siemens best-practice sharing event on safety-relevant perception, autonomy, and AI together with dependability (SPAA & Dependability@Siemens 2023).



This two day event (8th - 9th November 2023, Nuremburg) represented a unique opportunity for best-practice sharing for experts and practitioners from the entire Siemens group with an interest in safety-relevant perception, autonomy, and AI as well as development, engineering, and the management of dependable systems.

With a focus on dependability in general, which includes reliability, availability, maintainability, and safety (commonly abbreviated as RAMS), this event also covered additional aspects such as security, robustness and the resilience of systems and systems-of-systems. All these aspects are required to ensure - by means of analysis, design, reasoning, and evidence - that systems deliver services that can be trusted to meet expectations, in terms of safety and performance.

Contributions addressed fundamental concepts, best-practice, experiences, and novel approaches. The NxGen presentation, with a focus on rail, can be accessed here.

ESREL 2023 Special Session

John Andrews and Silvia Tolo led a Special Session at the European Safety and Reliability Conference (ESREL), held at the University of Southampton, 3rd - 7th September 2023. The NxGen session, under the topic of Mathematical Models in Reliability and Safety, highlighted the projects novel developments in methods to predict the failure probability or frequency of systems operating normal or phased missions.

Many modern engineering systems have features such as:

- Non constant failure and repair rates

- Dependencies between the component or sub-system failures
- Complex maintenance strategies

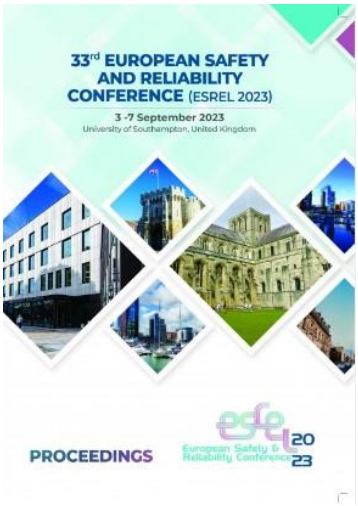
Commonly used methodologies, such as fault tree / event tree analysis, do not adequately analyse such systems. Dynamic and Dependent Tree Theory (D^2T^2) created by the NxGen project, can overcome the limitations in the currently accepted analysis methods, improving the quality of the decisions made to control the risks associated with the operation of hazardous systems and infrastructure.

The session generated awareness and discussion, and contributions addressed the development of methods to enable system wear-out, dependence, and sophisticated maintenance strategies to be accurately incorporated into a system analysis.

Key contributions:

"A nested Petri Net - Fault Tree approach for system dependency modelling", S. Tolo, J.D. Andrews.

"The extension of commonly used measures of importance for Dynamic and Dependent Tree Theory (D^2T^2)", S. Lunt, J.D. Andrews.

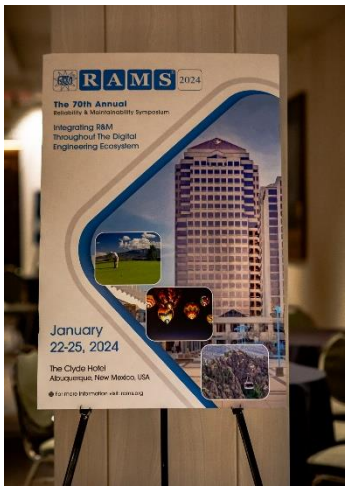


Proceedings of the 33rd European Safety and Reliability Conference (ESREL2023) Edited by Mário P.Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio. doi: 10.3850/978-981-18-8071-1_driver

ESREL 2024

The NxGen project team will be running a further two special sessions at the 34th European Safety and Reliability Conference, held this year at the Jagiellonian University, Cracow, Poland, 23rd - 27th June 2024.

RAMS 2024 Workshop



The Annual Reliability and Maintainability Symposium (RAMS®) is a world-renowned annual symposium alternating between east and west coast areas of the United States and has been continually held since 1954. Its purpose is to promote the Reliability, Availability, Maintainability and Safety professions and provide training, education, recognition, and advancement of these professions.

John Andrews and Silvia Tolo led invited Tutorial / Workshop sessions at RAMS 2024, the 70th Annual Reliability and Maintainability Symposium, 22nd - 25th January 2024, Albuquerque, New Mexico.

"An Introduction to Fault Tree Analysis" - Tutorial 7,
John Andrews, Sally Lunt
Access the text document Access the presentation slides

"Next Generation Fault Tree Analysis Methods" - Tutorial 8,
John Andrews and Silvia Tolo.
Access the text document Access the presentation slides

The NxGen Project 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 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.

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

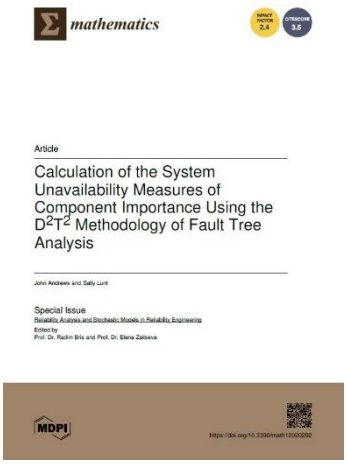
Darren Prescott is an Assistant Professor in Risk and Reliability Engineering in the Resilience Engineering Research Group at the University of Nottingham, where he has worked since 2010. Prior to this, he worked as a Lecturer at Loughborough University where he previously gained BSc and MSc degrees 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.

Latest Outputs and Webinars

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:

Calculation of the System Unavailability Measures of Component Importance using the D^2T^2 Methodology of Fault Tree Analysis

John Andrews and Sally Lunt, *Mathematics: Special Issue - Reliability Analysis and Stochastic Models in Reliability Engineering* , 12(2) 292.



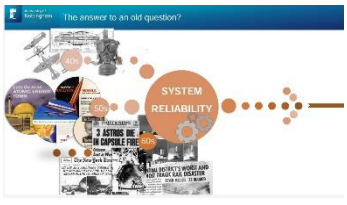
This paper proposes methods which extend the current capability of the D^2T^2 framework to calculate component importance measures. Birnbaum's measure of importance, the Criticality measure of importance, the Risk Achievement Worth (RAW) measure of importance and the Risk Reduction Worth (RRW) measure of importance are considered. This adds a vital ability to the framework, enabling the influence that components have on system failure to be determined and the most effective means of improving system performance to be identified. The algorithms for calculating each measure of importance are described and demonstrated using a pressure vessel cooling system.

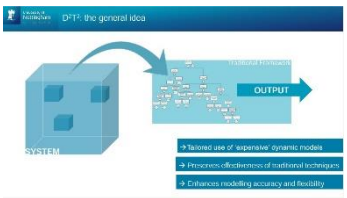
Access the pdf.

Modelling Modern Systems Safety: The Dynamic and Dependent Tree Theory (D^2T^2)

Silvia Tolo, invited webinar presentation Safety and Reliability Society (SaRS). March 2024.

Access the presentation slides

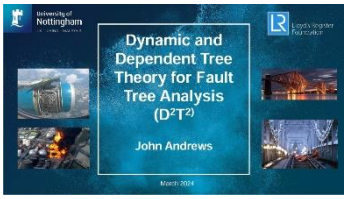


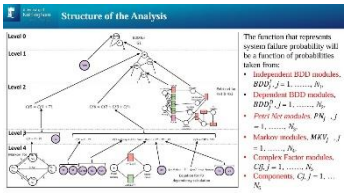


Dynamic and Dependent Tree Theory for Fault Tree Analysis (D^2T^2)

John Andrews, invited webinar presentation Nuclear Safety Inspectors (HSE), March 2024.

Access the presentation slides





Useful Links

ESRA - European Safety and Reliability Association

A non-profit organization dedicated to promoting and advancing the fields of safety and reliability engineering in Europe and beyond. ESRA brings together professionals, researchers, and practitioners from various disciplines to exchange knowledge, collaborate on research projects, and foster innovation in the areas of risk assessment, safety management, and reliability analysis.

Learn more about ESRA's mission, activities and events

ESReDA - European Safety, Reliability and Data Association

ESReDA was established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability and a focus for specialist expertise.

See more information on ESReDA, it's aims and objectives

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

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

University of Nottingham
UK | CHINA | MALAYSIA