Systems Risk, Reliability, Security and Resilience

Theme Lead: Dr John May

Reader in Safety Systems, University of Bristol
Contact: J.May@bristol.ac.uk

John's research focuses on the mathematics of risk and organizational structures for complex systems in safety contexts. New science and engineering is required to manage the safety and resilience of these systems as their complexity, and the responsibilities handed to them, grow.

Theme summary

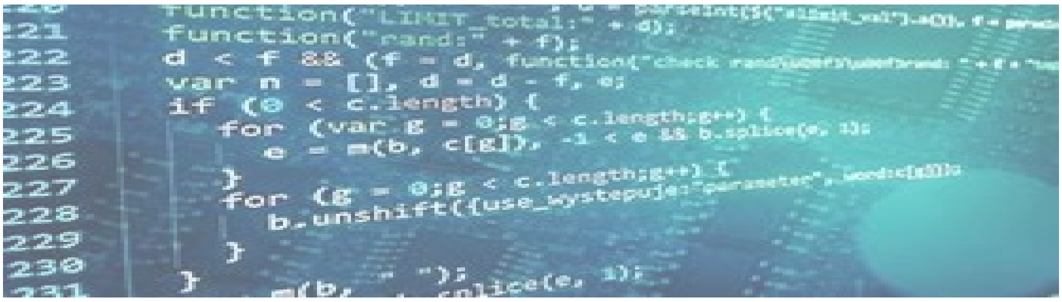
In low carbon energy production, increasingly competitive renewables are perceived as presenting few risks to human safety. To compete beyond baseload production, nuclear energy can reduce costs whilst maintaining public acceptance using cutting edge assurance techniques.

"Safety is our number one priority" EDF[1]

Risk, reliability, security and resilience research is developing deep assurance for new nuclear technologies, engaging both nuclear licensees and the regulator through research programmes: Control & Instrumentation Nuclear Industry Forum, the Energy Institute, RAEng Engineering-X, and the BEIS Nuclear Innovation Programme.

This research theme involves:

- Powerful new test methods for the safety and security of complex digital systems
- Objective J-value assessments for more accurate quantification of nuclear risks, allowing risk prioritisation to target effort where it is most cost effective
- Organisational resilience techniques predisposed to safety in human operations and human-autonomy cooperation



[1] 'Protecting the public' https://www.edfenergy.com/energy/safety-reporting (20.11.20).

Research capabilities

Control and Instrumentation Software Systems Testing

Key academics: Dr John May

New nuclear plants use significantly more software-based Control & Instrumentation (C&I) than in previous generations. This C&I is more complex, and we rely on it to a greater extent for safety. In addition to appearing in key protection, alarm (display) and control systems, software now appears in large numbers of sensors (‘smart devices’). A variety of hardware platforms such as processors and FPGA are used but, in all cases, new reliability modelling is required: the ‘design’, or ‘systematic’, failures exhibited by software are not random in the sense used by traditional models of reliable hardware.

This research has developed, and continues to evolve, a new *statistical testing* approach to reliability assurance of programmable digital systems, grounded in the scientific method. The aim is to ensure nuclear regulators can have the highest confidence in the most critical software, and to increase the level of reliability that can be claimed for these systems.

Case Study

Statistical testing (ST) for safety cases – ST won an ‘internationally leading’ impact rating in the 2014 universities REF assessment, after its use on Sizewell primary protection, Hunterston DPS, and a range of smart devices. ST is now incorporated into the UK’s regulatory framework in ONR’s SAPs (Safety Assessment Principles) and TAGs. The US, South Korea and China have initiated policy synthesis research investigating ST capability for C&I assurance.

Current activities include:

- Developing the fundamental theory to underpin higher C&I reliability claims
    - Massively parallel test acceleration using hardware simulation-based testing (hardware platform digital twins)
    - demonstrating diverse redundancy in multi-channel system architectures using fault injection.
- Ongoing policy synthesis: understanding where best to apply intensive techniques such as statistical testing, and the degree to which they should be applied (see BEIS NIP case study in box below).
- Tools and technical guidance to improve application e.g. the ST interface with PRA; test harness for probabilistic demand generation.
- Design for ST in future systems such as SMR/AMR/Fusion C&I

Contact: enquiries@southwestnuclearhub.ac.uk

SOUTH WEST NUCLEAR HUB

Case Study

BEIS Nuclear Innovation Programme - Research projects, led by Bristol with Fraser Nash Consultancy, are investigating future directions for C&I assurance, horizon scanning across new assurance techniques, studying the implications for assurance of software and system design, and the potential for new regulatory perspectives.

Organisational Safety Resilience

Key academics: Professor Richard Taylor MBE, Dr John May, Dr Graeme Collinson, Dr Neil Carhart, Richard Voke

Case Study – Developing 'Tools' to Achieve Greater Resilience to Organisational Accidents

The Energy Institute, and RAEng's Engineering-X initiative, have commissioned studies on behalf of member organisations, from the Universities of Bristol and Bath to provide 'best practice guidelines' and develop a diagnostic 'audit' tool, based on learning from historical major events. The work also targets systems models which can predict and control unintended consequences in organisational improvement.

For example, we have shown how well-intentioned interventions, such as enhanced incident reporting, can lead to significant departures from leadership intentions. Complexities in contractor relationships and the impact of a weakened safety culture on oversight, have also been modelled. Follow up research is now incorporating behavioural factors into the models, with the objective of building new tools to guide sustainable organisational change with effective measures of progress.

Credit: EDF

Cyber Security

Key academics: [Bristol Cyber Security Group]

The University of Bristol Cyber Security Group is part of the Academic Centre of Excellence in Cyber Security Research (ACE-CSR) at Bristol, and linked into key national security research programmes. The group's research focuses on three over-arching but interlinked strands: security of cyber-physical infrastructures, software security and human behaviours. As critical national infrastructure, nuclear plants are natural targets for attack and the increase of software and digital systems create more 'access' points, as well as opportunity for human error.

The next generation of plant, including SMRs and AMRs, are likely to use digital systems extensively and will be more ‘connected’ to the outside world. The highest security and safety requirements must co-exist, and human operators will need to be suitably trained to anticipate and mitigate risks.

Risk Analysis and Management

Key academics: Professor Philip Thomas, Professor Richard Taylor MBE

In every organisation, there is a need to balance the effectiveness of planned safety measures against their cost. Available resources must be used wisely, allowing the most important risks to be identified and then mitigated or reduced as far as possible.

Research in this area looks to improve on the official UK government measure, the Value of a Prevented Fatality (VPF), to balance safety spend against the extension of life expectancy it brings about.

The J-value method is an objective measure that indicates the maximum reasonable cost of a protection measure relative to the increase in life expectancy and the safety expenditure required. Applied to the effectiveness of mass relocation interventions following major nuclear events such as Chernobyl and Fukushima, the research has shown that the response has often gone beyond what might objectively be determined as cost effective whilst often not preserving or extending life expectancy.

Case Study

The J-value tool for assessing relocation strategies after major nuclear incidents

Of the 335,000 people evacuated away from the Chernobyl area after the power plant accident in 1986, the J-value shows that 80% to 90% of them ought to have been allowed to stay in their homes. This conclusion is based on the J-value being greater than one; where the people would have benefited more in terms of life expectancy by remaining in their homes rather than being relocated, often never to return.

This has been explored as a public health policy option by national and international bodies such as the US Federal Emergency Management Agency and France’s IRSN, as well as the UK Public Health Executive.

Contact: enquiries@southwestnuclearhub.ac.uk