

Automotive Cyber Resilience: Operationalizing, Standards and Research

Presenting the work of AESIN and the UK Automotive Council and Zenzic, supported by Queens University Belfast, University of South Wales, University of Edinburgh and the Turing Institute and with further support from BSI, this series of workshops is designed to:

- Present and discuss the limitations with existing standards in meeting the requirements of the Automotive and other mobility industries worldwide,, and
- Present the methodology proposed by AESIN, UK Automotive Council and Zenzic to achieve operationalizable and legally sustainable cyber resilience, and
- In the context of that methodology set out the research agenda and give examples of applying the outcomes of existing and potential research in support of the methodology

The Engineering 'V' is not Enough ...

Connectivity to complex systems within and beyond the vehicle, and the implementation of machine learning, both change the game entirely

Before

- Bounded scope
- System ownership
- Known interactions
- Predictable function
- Benign intent

Engineering V optimises design to known operating conditions

Connected & Automated

After

- Un-bounded scope
- No system ownership
- Un-knowable interactions
- Emergent function
- Nefarious intent

Engineering V cannot accommodate all operating conditions

Cyber Resilience

Three Principles

- 1) Increase the probability of detection, understanding and acting
- 2) Increase the number of 'Engineered Differences'
- 3) Invoke a continuum of 'Proactive Updates'

Six Certification Arguments

- 1) Probability of detecting threats
- 2) Probability of understanding threats
- 3) Rate of deploying mitigating actions
- 4) Time for a threat to propagate
- 5) Quantity of 'Engineered Differences'
- 6) Frequency of 'Proactive Updates'

Cyber Resilience = function ($P_{D,U}$, $P_{U,A}$, r_A , t_C , n , f)

What Do I Want My Security To Help Me Conclude?

THALES

Research Agenda

Static methods of approval and defence will not answer the threat of asymmetric nature of dynamic attacks either in their current form or when up-gunned in line with foreseeable technological advances. There is the need for the operationalisation of approaches to **resilience and survivability**. The research agenda should include work on:

- Malware propagation
- The economics of detection of significant cyber events
- The economics and understanding the significance of events
- The legal sustainability of actions to mitigate
- The introduction of significant difference to promote resilience
- Mathematical foundations that underpin cyber resilience
- The skill-base necessary to support the emerging technologies/methodologies

RITIOS



There are 4 workshops which are each limited to 50 attendees. At each site a different academic partner will highlight examples of applying the outcomes of existing and potential research in different areas in support of the methodology. The workshops will be held at:

4th Dec 2019 - ECIT, Queen's University of Belfast, Queen's Road, Queen's Island, Belfast, BT3 9DT

- QUB are the academic partner and will use research examples from hardware
- Click [here](#) for tickets

11th Dec 2019 - University of South Wales Conference Centre, CF37 1DL

- UoSW are the academic partner and will use research examples from Forensics
- Click [here](#) for tickets

8th Jan 2020 - NXP, Colvilles Road, Glasgow G75 0TG

- University of Edinburgh are the academic partner and will use research examples from Modelling
- Click [here](#) for tickets

15th Jan 2020 - Plexal, 14 East Bay Lane, Here East, Queen Elizabeth Olympic Park, London, E20 3BS

- The Turing Institute are the academic partner and will use research examples from mathematics and probability
- Click [here](#) for tickets

Who should attend?

This event is designed specifically for researchers with an interest in automotive cyber resilience and the application of security and other research outcomes, including PhD and other research students and their supervisors, early career researchers, representatives from industry, government and other defence and security-relevant NGOs.



...making excellence a habit™



plexal



THE UNIVERSITY
of EDINBURGH