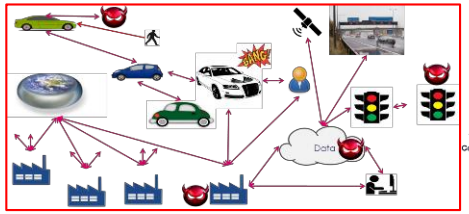
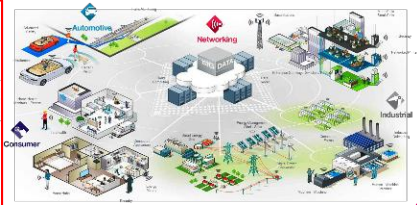
THALES





What Might I Achieve With Verified Software in Complex Automotive Systems?

Peter Davies
Director Security Concepts

with thanks to: automotive council UK, AESIN AUTOMOTIVE ELECTRONICS INNOVATION, ZENZIC

VERIFIED SOFTWARE WORKSHOP
25TH SEPTEMBER 2019

www.uk.thalesgroup.com

Who am I, Where do I Come from (why should I Listen)?

- I am
  - A Security Expert
  - Specialised in the convergence of Safety and Security
  - Leading Expert on
    - Countering Cyber Attacks targeted Supply Chain Infiltration
    - Cyber Physical Attacks
    - I have lead 2 Cyber Security aspects of C-CAV research activities
  - 30+ years of verifying security systems in hardware and software
- I do security where it can't afford to fail
- I advise organisations on their legal position

https://www.riscs.org.uk/2018/02/15/peter-davies-forward-security-for-emerging-problems/

Thales is a leading global provider of data protection and cyber solutions with more than 40 years' experience securing the world's most sensitive information. Our customers — businesses, governments, and technology vendors with a broad range of challenges — use Thales products and services to improve the security of applications that rely on encryption and digital signatures. By protecting the confidentiality, integrity, and availability of sensitive information that flows through today's traditional, virtualized, and cloud-based infrastructures, Thales is helping organizations reduce risk, demonstrate compliance, enhance agility, and pursue strategic goals with greater confidence

I Will Speak Today

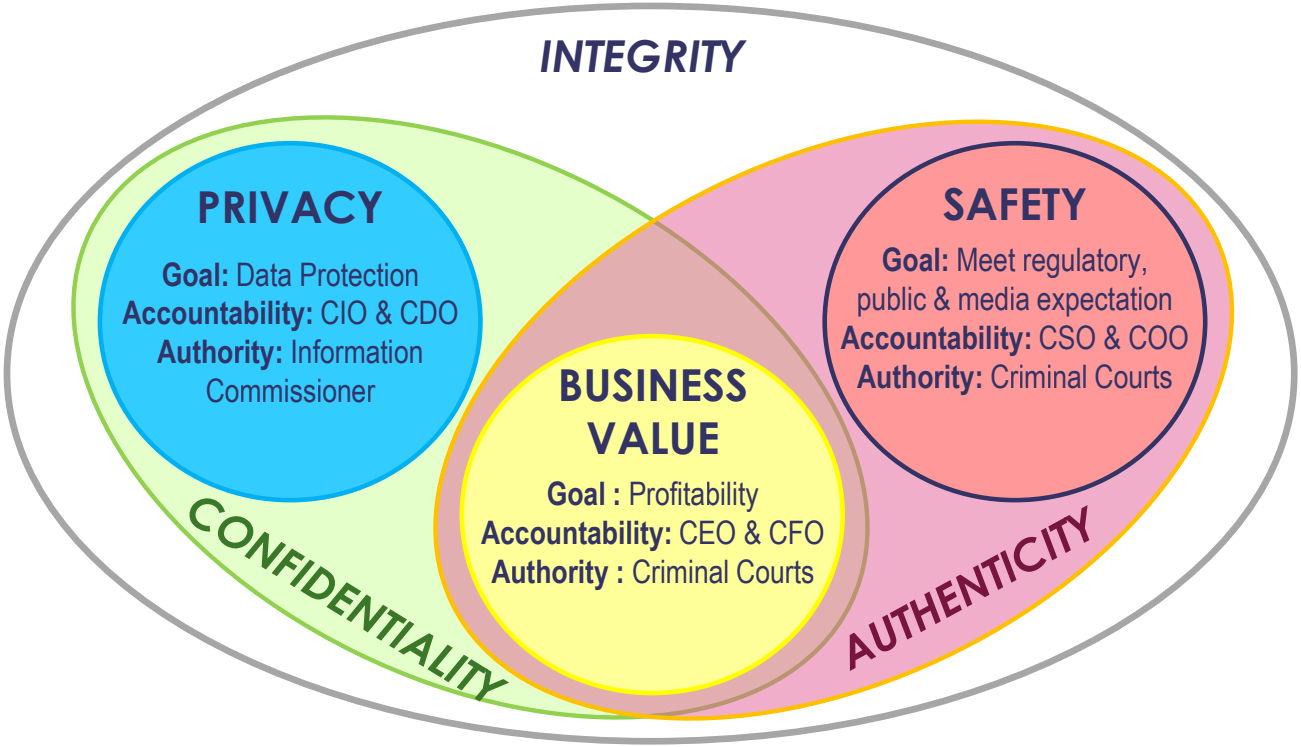
In the context of the Cyber Resilience Methodology being developed by the Auto Industry and the outcomes this methodology must achieve this talk will discuss:

- The nature of a cyber attack and the requirement for resilience

And in the context of verified and verifiable software its

- potential role
- effectiveness of as a means of countering cyber attacks
- contribution to the economics and some of the tools that may be required

Conflicting Objectives and Responsibility …

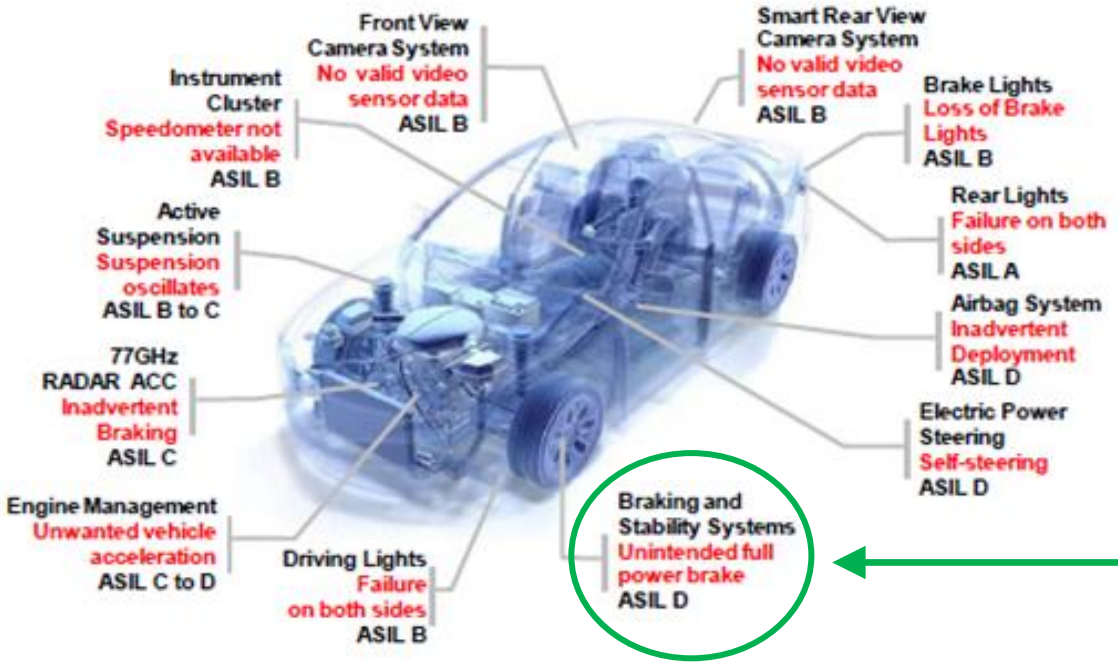


Cyber resilience is a board level responsibility with company integrity at stake

Most C-level executives share in the consequences of a breach

The Problem: Breaking the Brakes …

Braking used to be 'Simple'



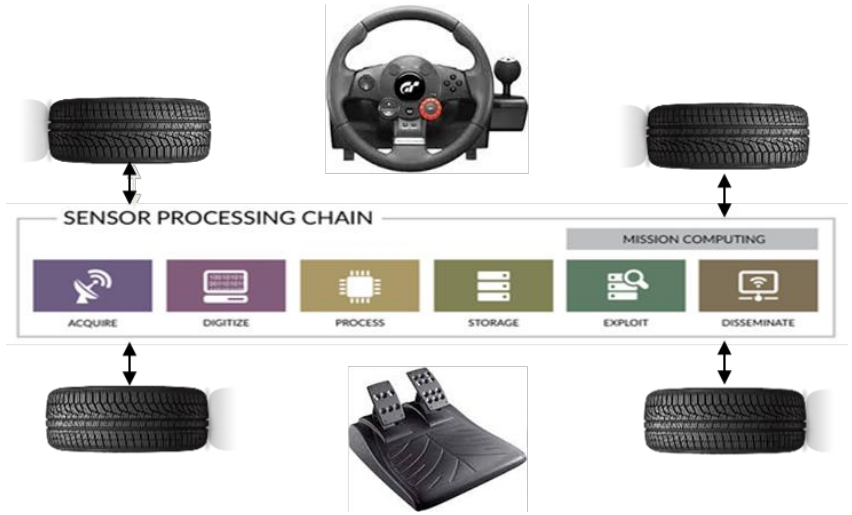
- The design rationale associated with Braking continues to call up ASIL-D;
- Implying simplicity, replication and zero to small numbers of lines of code

ASIL D, the highest classification of initial hazard (injury risk) defined in ISO 26262 (Road vehicles—Functional safety) represents likely potential for severely life-threatening or fatal injury in the event of malfunction

This was true for Fluid based Electromechanical systems

The Problem: Breaking the Brakes …

Braking has become Digital and 'Complicated'



The evolving Functional Braking System :

- ABS at City & Highway Speeds - Individual wheel braking, acceleration & steering
- Multiple sensors, often augmented by machine learning
- Data Fusion & algorithmic arbitration to optimise system
- Connected over a shared network infrastructure
- 10→23 Sensors; 1.5→3.5 million Lines-of-Code; Training Data sets …

Without direct connection between controls and function, our assumption of ASIL-D becomes questionable – even before malevolent attacks are considered

Cyber Resilience …

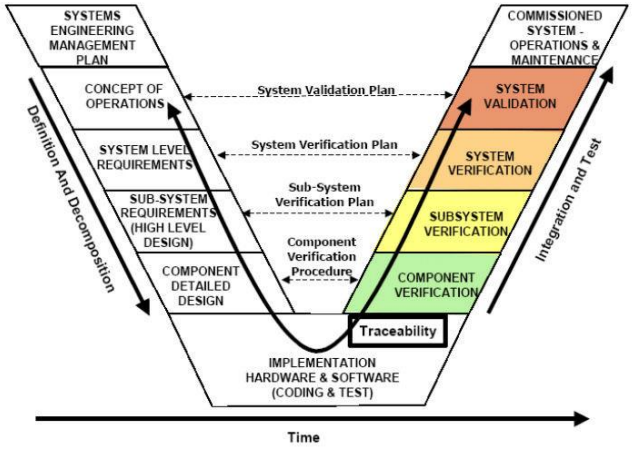
“A System is Cyber Resilient if, and only if,

there is justifiable and enduring confidence

that it will function as expected, when expected”

Something Fundamental Just Changed …

The Engineering 'V' Method has served us well for bounded, fully known systems, where time is given to prepare thoroughly for product launch and operation



We are justly proud of our progress in engineering more complex products, to higher standards, in shorter timespans using this trusted method

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

Connected & Automated

After

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

Engineering V optimises design to known operating conditions

Engineering V cannot accommodate all operating conditions

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

Connected & Automated

- **System becomes limitlessly complex**
- **Machine learnt contributions cannot be predicted**
- **Time to execute the Engineering V tends to Zero**

After

While the Engineering V remains useful for bounded sub-systems
We need an additional design method that can adapt in real time operation

The Nature of Failure has Changed …

Unconnected, Manually Controlled, Electro-Mechanical Systems

- Can be tested for all failure modes
- Fail one at a time on a statistical basis
- Each attack takes expertise
- Each system needs a separate attack

Connected & Automated

Connected, Automated Digital Systems

- Cannot be tested for all failures
- Fail globally and unpredictably
- Only the first attack takes time and expertise
- Attack only needs to succeed once

Beyond a certain level of complexity, the choice is no longer 'How not to fail' …
… but 'How to fail'

Cyber Resilience …

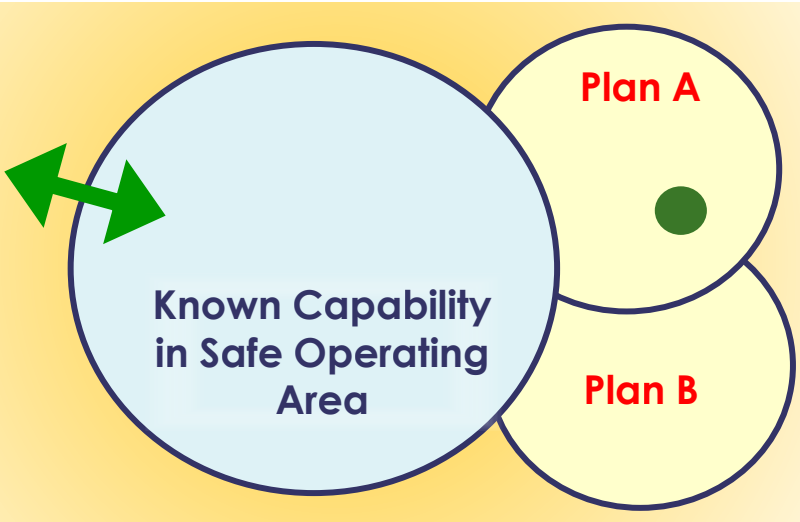
Agreeing the Design Limit for Safe Operation, and the Mitigation when Unsafe, are the new Sign-Off and Certification judgements

Certification requires a 'Sustainable Argument' that gives 'Justifiable Confidence' of a 'Good Outcome' in the face of an Emerging System Failure

Cyber Resilience …

Agreeing the Design Limit for Safe Operation, and the Mitigation when Unsafe, are the new Sign-Off and Certification judgements

Design Limit covers a 'Reasonable' operating area governed by 'Well-Founded' theories

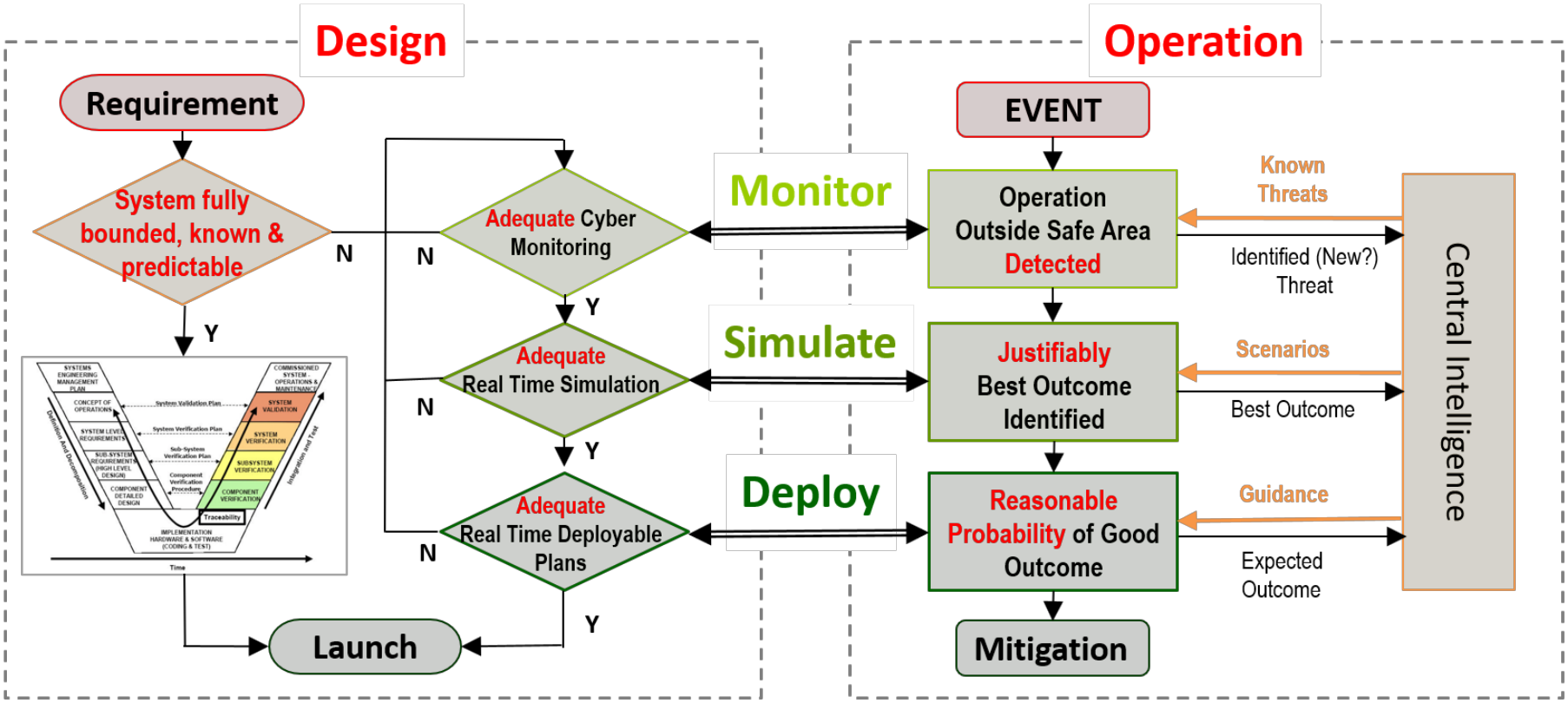


Mitigation Plans with 'Reasonable' probability of a 'Good Outcome' are deployable at point of need

Certification requires a 'Sustainable Argument' that gives 'Justifiable Confidence' of a 'Good Outcome' in the face of an Emerging System Failure

Could This Work … ?

A Framework for the 'Design for Cyber Resilient Operation'



Monitoring

What	• Real time cyber monitoring to detect abnormal events not considered within 'Design Limits' • Observing emergence and propagation of potential new or known threats • Interfaces at system boundary with other systems and wider system-of-systems
Why	• Support 'Mitigation Plan' deployment decisions in the expectation of imminent failure • Update real world understanding to continuously improve system design and operation

How	• Highly automated real time methods (with human oversight to identify new requirements)
	  • Theorem proving to classify events inside and outside 'Design Limits'
	  • Cryptographic techniques to identify incorrect data and communications
	  • Probes & viral techniques to monitor and prove system is responding as expected

Highly automated real time theorem proving methods underpin threat monitoring

Simulation

What	• Multi-dimensional (attribute) simulation of all operationally relevant aspects of system • Real time combination of Game Theoretic & Model Theoretic simulation methods • Simulation of high level (eg. Data Bus) and low level (eg. Compute Cycles) as relevant

Why	• Provide understanding about possible future effects, particularly based on Game methods
	  • How close to 'Design Limit' might future operating state become ?
	  • Under what conditions might a failure occur ? … How likely are these conditions ?

How	• Game Theoretic methods will follow self-learning pathways to find outcomes • Model Theoretic models used to provide an accelerated testing environment • Primarily off-board due to computational demands. Limited on-board simulation.

Simulation is a mission critical enabler with high strategic & commercial value

Deployment

What	• Time critical strategic application of 'Mitigation Plans' across product range to reduce negative impacts of new or known events and threats • Withdrawal of deployed actions if impact is not desirable • Traceable log of all decisions, actions and supporting evidence
Why	• Initial set-up and pro-active update of product to improve operational resilience • Manage propagation or impact during an event, up to & including managed shut down • Retain or restore safe operation in response to abnormal event
How	• Secure verifiable software delivery • (Re-)Configuration of some or all products or their components • A culture of proactive continuous learning and improvement

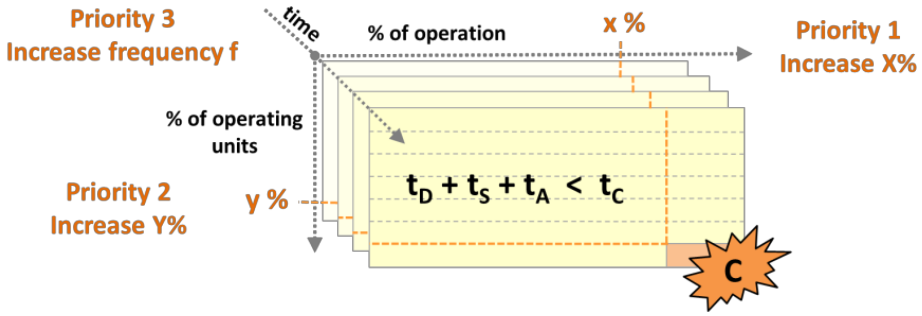
Strategic response to events to maximise safe operating capability

THALES

Cyber Resilience

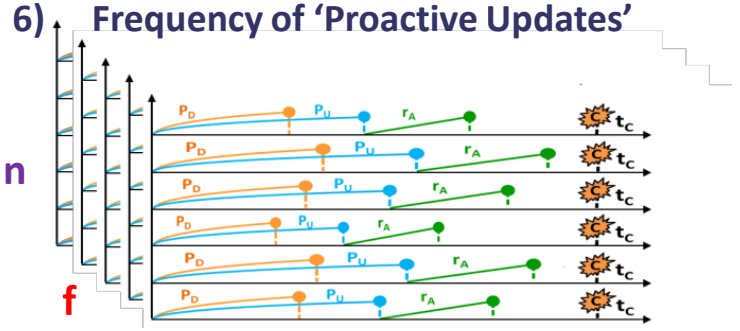
Three Principles

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, P_U, r_A , t_C, n, f)

Making It Reality …

There are two things we need to stop doing …

1) **The common supply chain that underpins the automotive sector creates a likelihood of global catastrophic failure - we now need to 'Engineer Difference'**
2) **Current regulatory framework requires confidence that static requirements are met – guaranteeing that when failure occurs it will be catastrophic, and now need to mange confidence in dynamic environments and 'proactive updates'**

We have a unique opportunity to invest and re-imagine the future of resilient systems across multiple sectors to the economic advantage of the UK

Making It Reality …

There are four things we need to do …

1) Engineering Principles & Methods – Establish the new Industry protocol
2) Research – Inter-disciplinary research is critical to provide the intellectual underpinning for emerging methodologies, leveraging areas in which the UK is or aspires to be in the top-three globally
3) Legislation & Certification – Update by executive order or legislative changes
4) Skills – Inspire and direct the next generation

We have a unique opportunity to invest and re-imagine the future of resilient systems across multiple sectors to the economic advantage of the UK

In Summary …

We have fundamentally reorganised engineering knowhow and methods to be fit for Connected & Autonomous Mobility

- **We can numerically describe and defend a complex digital system – including emergent and non-deterministic behaviour (cyber attacks) – in a legal setting**
- **Forming the basis for a new definition for type approval of CAM**
- **Enabling investments in technologies that can bring quantifiable benefits**
- **Identified areas where actions and improvements are required**

We have a unique opportunity to invest and re-imagine the future of resilient systems across multiple sectors

In Summary …

And in the context of verified and verifiable software its

- **Potential role: in cutting down search space for events**
- **Effectiveness of as a means of countering cyber attacks: Is questionable**
- **Contribution to the economics and some of the tools that may be required:**
  - **Theorem provers**
- **Identified areas where actions and improvements are required**

Thank you

peter.davies@uk.thalesgroup.com