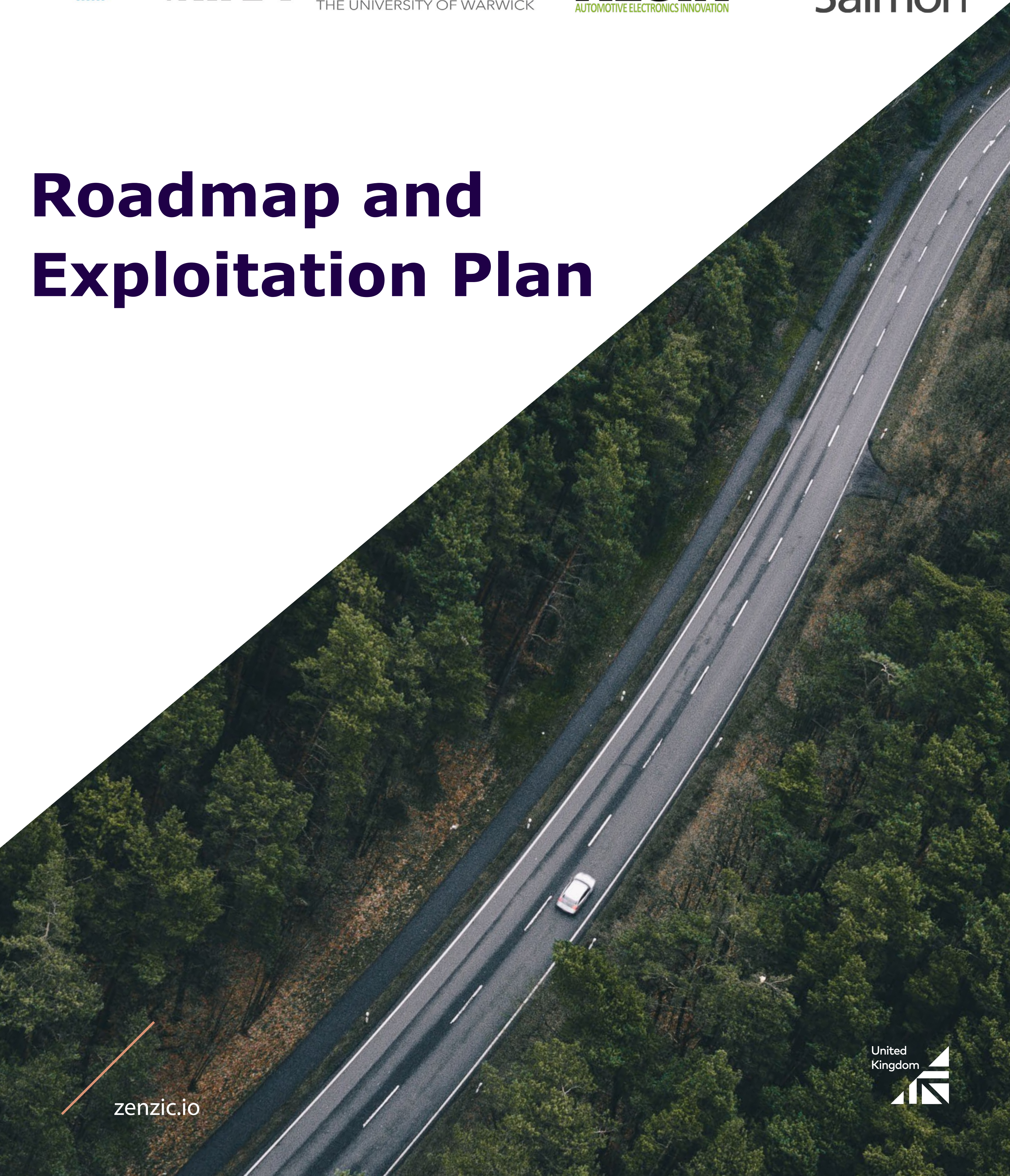
Roadmap and Exploitation Plan



zenzic.io

THALES UK LIMITED

350 Longwater Avenue Reading RG2 6GF
Tel. +44 0)118943 4500
www.thalesgroup.com

The ResiCAV+ contributors would like to acknowledge

ZENZIC
SELF-DRIVING REVOLUTION

Centre for Connected
& Autonomous Vehicles

Innovate UK

About Us

Thales - Together. Safer. Everywhere

Thales plays a role whenever critical decisions need to be undertaken. In all the markets we serve – aerospace, space, ground transportation, security and defence – our understanding of the Critical Decision Chain helps customers to decide and act in a timely fashion and obtain the best outcomes.

World-class technologies and the combined expertise of 65,000 employees in 56 locally based country operations make Thales a key player in assuring the security of citizens, infrastructure and nations.

Thales UK Limited, Research and Technology

Thales UK's Reading-based research and technology facility is the UK arm of the Thales corporate research centre. Activities focus on providing solutions: Security and Communication Systems, Galileo and Position-Based Systems and Enhanced Digital Environments. These are based on the key technologies of IP Networks and Network Security, Wireless Communications, Sensors and Signal Processing, and Navigation and Positioning. The facility offers a wide range of consultancy and development services to European Government Agencies and to industry throughout the world.

Executive Summary

The goal of ResiCAV was to explore the technological and economic feasibility of developing, implementing and operating a sustainable UK Cybersecurity Engineering capability; to ensure the cyber resilience of future mobility.

> ***This is an ambitious goal considering the size and complexity of the issue, but at the same time a very necessary target when we consider the possible risk of catastrophic failure in moving from Connected and Autonomous Vehicle (CAV) demonstrations to mass deployment if new methods are not developed to protect, detect, understand and react to emerging threats.***

Thus, the electronic systems of future vehicles, as well as the intelligent transport systems that they interact with, will need to exhibit a high degree of resilience to a wide range of threats.

Building on the results of ResiCAV, the goal of ResiCAV+ is to create a demonstration tool testbed in order to:

- Support development of the CyRes capability
- Allow systems, services and applications e.g. CAVs to be integrated together
- Support development and demonstration of CyRes scalability
- Demonstrate the production of court admissible evidence to support the CyRes arguments.

To enable the testbed to meet this purpose, the following requirements had to be met:

- Modular integration capability, such that inclusion of a new component does not impact other components
- Include a distributed ledger as a system of systems data store and allows systems to interact
- Provide an evidential chain of information
- Provide interfaces to allow systems, services, applications, and components to integrate into the system of systems
- Enable simulators or real systems to be integrated for development, demonstration and experimental purposes
- Possess visual interfaces to demonstrate the CyRes concepts and methods.

ResiCav+ is making actionable conclusions in the areas of Intellectual Property, Effective Use of Research Institutes, Common Tool Pool, National Security and Freedom of Action, Skills, Regulation and Law.

The ResiCAV+ study is documented in 5 Reports:

- **Report 1: Prototype Tool Suite** (software/documentation/skills training course). Including worked Examples of their use to provide cyber resilience in real-world automotive systems. It should be noted that OEM/Tier1 specifics may need to be redacted from any released version.

- **Report 2: Proof of Concept Demonstrator of Prototype Tool Suite.** A report on the tool suite covering how and in what form the tool suite might be made available for use by commercial and academic researchers, allowing them to start to integrate the CyRes methodology into existing practices.

- **Report 3: Legal Report.** A report providing a route to a *per vehicle* **legally defensible** argument that the cyber vulnerability of the braking system was reduced ALARP using this ***significant difference*** approach and based on the distributed ledger.

- **Report 4: Compliance Report.** A report providing a route to a *per vehicle* real-time compliance argument based on the use of the distributed ledger.

- **Report 5: Exploitation Plan. A**n updated roadmap outlining next steps to improve cyber-resilience of automotive systems using CyRes tools & methodologies, building on previous work by the team, including ResiCAV and work funded by NCSC as well as other projects. This includes:

  - A roadmap for continuing development and the funding required.

  - Plans to exploit and disseminate tools and methods on a global basis.

This report, the public part of Deliverable 5 outlines a roadmap to the commercial availability of tool and legal support for the CyRes (Cyber Resilience) methodology.

The goal of CyRes is to define an operational methodology, suitable for standardisation, for which:

1. **The methodology itself** is capable of being tested in court or by publicly appointed regulators.
2. **Operators** understand what evidence should be produced by it and are able to measure the quality of that evidence.
3. **The evidence produced** is capable of being tested in court or by publicly appointed regulators.

Typically, this will mean that the real-world system to which the methodology has been applied is capable of operating at all times and in all places with a legally acceptable value of negative consequence.

However, and unlike other Cyber Security methods for which the question is often ‘how much must I spend to be compliant’, the CyRes methodology is rooted in **economic advantage** with achieving the conditions for compliance being a by-product. One of the fundamental insights of CyRes is that **Cyber-attacks are ‘emergent properties’.** Much of the **value of the economy** is based on products and services created around emergent properties so by understanding and managing these in real time CyRes for the first time allows Cyber Resilience to sit firmly within the value creation rather than compliance chain.

The ResiCav+ programme, and the research by leading experts that underpins it, builds on prior work that demonstrated not only is the CyRes methodology is economically and technologically feasible but that operating in this way would allow the **direction of capital towards growth rather than compliance**. Under this programme

CyRes achieves this dynamic business advantage whilst at the same time developing evidence of Cyber Resilience that can be confidently brought to court if required. It is built around three principles and six certification arguments designed to provide **a mathematically well-founded index of resilience, including cyber resilience, in operational space**.

In considering the technological and economic feasibility of CyRes this study has concluded that all of the **resilience and economic benefits** are achievable by the UK in **3 years** subject to an **investment of £150m**. This conclusion is made on the basis that:

1. All of the elements necessary to operate CyRes exist today at a Technological Readiness Level (TRL) of 5-7.
2. Subject to an appropriate investment in tools of less than £20m over three years then the method could achieve TRL 9 and would be globally economically attractive.
3. Within three years the method could deliver a level of resilience with respect to emergent properties and cyber-attacks that would exceed current state of the art.

Whilst it was not the main purpose of this study the research conducted determined that **more than 25% of the cost of vehicles** was being spent in chips, software, V&V and compliance / type approval aimed at removing inherent diversity and turning them back into entities with inherent and increasing potential for global catastrophic outcomes; **much of this could be saved by using CyRes**.

Furthermore, collaborators at all levels of the supply chain reported that up to **5% of the cost of the digital vehicle** was being spent on Cyber Security with **little or no measurable outcomes** with respect to Cyber Resilience.

The techniques demonstrated by ResiCav+, which support the CyRes methodology and its operationalisation, provide an **academically well-founded baseline for understanding the cost of operation** together with an **academically well-founded baseline for understanding the effectiveness**. The acceptance of CyRes and this baseline together with the need to understand and improve it will provide a **springboard for innovation** for companies at all layers together with a **direction for and measure of academic research** in the coming decades.

Contents

Table of Figures

1. Introduction

The purpose of the demonstration testbed was to:

- Support development of the CyRes capability
- Allow systems, services and applications e.g. CAVs to be integrated together
- Support development and demonstration of CyRes scalability
- Demonstrate the production of court admissible evidence to support the CyRes arguments.

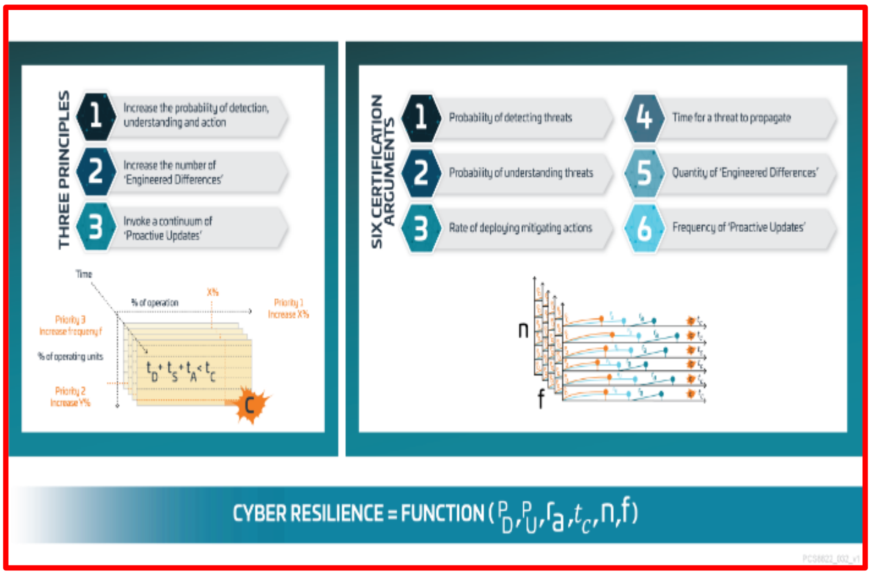
To enable the testbed to meet this purpose, the following requirements had to be met:

- Modular integration capability, such that inclusion of a new component does not impact other components
- Include a distributed ledger as a system of systems data store and allows systems to interact
- Provide an evidential chain of information
- Provide interfaces to allow systems, services, applications, and components to integrate into the system of systems
- Enable simulators or real systems to be integrated for development, demonstration and experimental purposes
- Possess visual interfaces to demonstrate the CyRes concepts and methods.

ResiCav+ has made actionable conclusions in the areas of Intellectual Property, Effective Use of Research Institutes, Common Tool Pool, National Security and Freedom of Action, Skills, Regulation and Law which are the content of this report.

2 Document Structure

Section 3: The Problem – based on previous research articulates the problem space for modern and future vehicles including CAVs including the 3 principles and 6 arguments that the CyRes methodology identified as fundamental to a coherent and defensible resilient system.



THREE PRINCIPLES

1 Increase the probability of detection, understanding and action

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

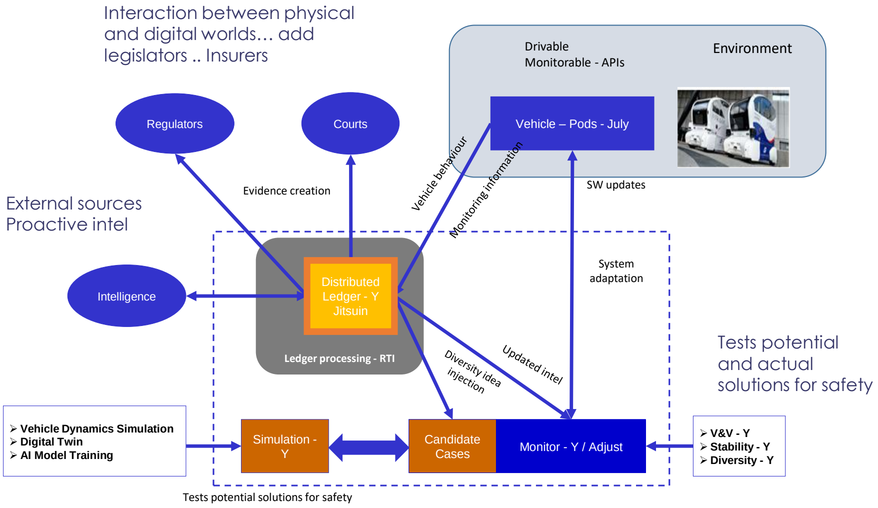
5 Quantity of 'Engineered Differences'

6 Frequency of 'Proactive Updates'

CYBER RESILIENCE = FUNCTION (P_D, P_U, r_a, t_c, n, f)

Existing automotive practice however is focussed almost entirely on the design rather than operation phase with a skill base rooted firmly in electromechanical systems and the experience of the past 50 years.

Section 4 What was Demonstrated – The ResiCAV+ technical approach sets out a feedback loop based around the collection of evidence relating to events and the decisions made with respect to those events that provides for the reinsertion of tested updates into vehicles at scale and within minutes. It operates on the basis that changes to the vehicle baseline must often be driven by changes necessitated by emergent properties in its environment rather than from controlled software updates. As such and given that the Technology Readiness Level (TRL) of an emergent property will often be 0 this toolset was created on the basis that Automotive systems will at all times be in a design phase crucially even when deployed.

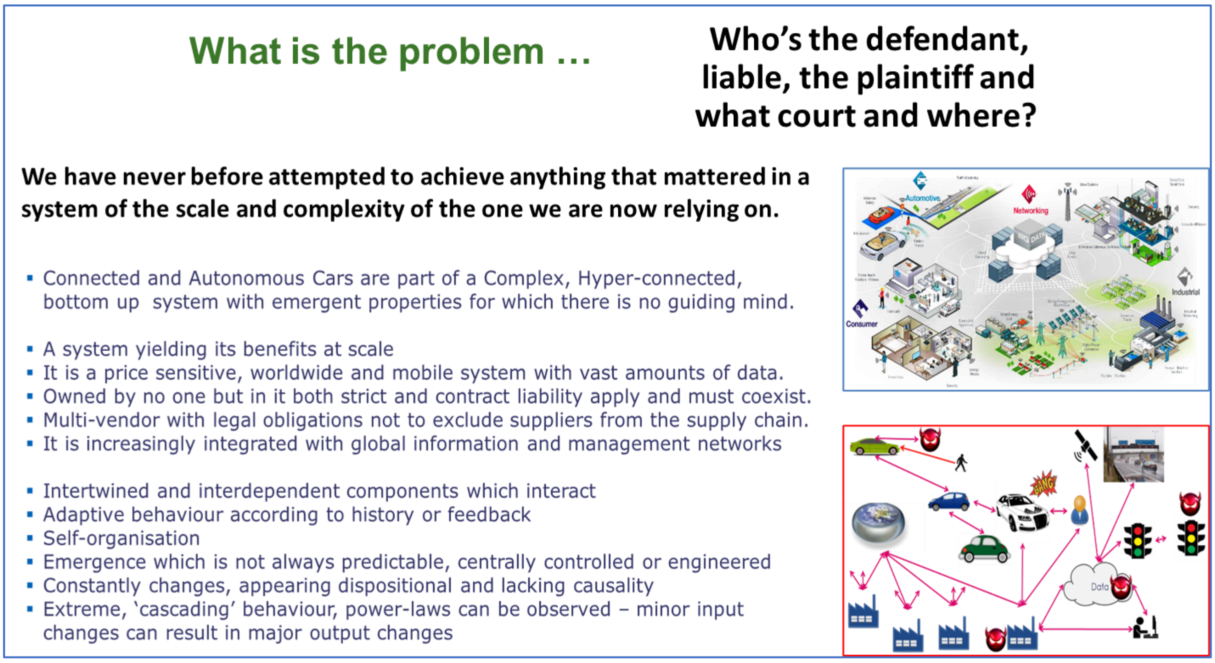


Section 5 The ResiCAV+ Roadmap Conclusions – This section documents some of the conclusions from the ResiCAV+ study particularly with respect to the tools and their suitability for use.

Section 6 Roadmap Table– This section contains a table showing the roadmap conclusions and when they must be acted on in order to yield the required benefits.

3 The Problem

Over the period since 2015 we have characterised every significant emerging system as having all, or at least most, of the characteristics shown below under the diagram 'what is the problem'



What is the problem …

Who's the defendant, liable, the plaintiff and what court and where?

We have never before attempted to achieve anything that mattered in a system of the scale and complexity of the one we are now relying on.

- Connected and Autonomous Cars are part of a Complex, Hyper-connected, bottom up system with emergent properties for which there is no guiding mind.

- A system yielding its benefits at scale
- It is a price sensitive, worldwide and mobile system with vast amounts of data.
- Owned by no one but in it both strict and contract liability apply and must coexist.
- Multi-vendor with legal obligations not to exclude suppliers from the supply chain.
- It is increasingly integrated with global information and management networks

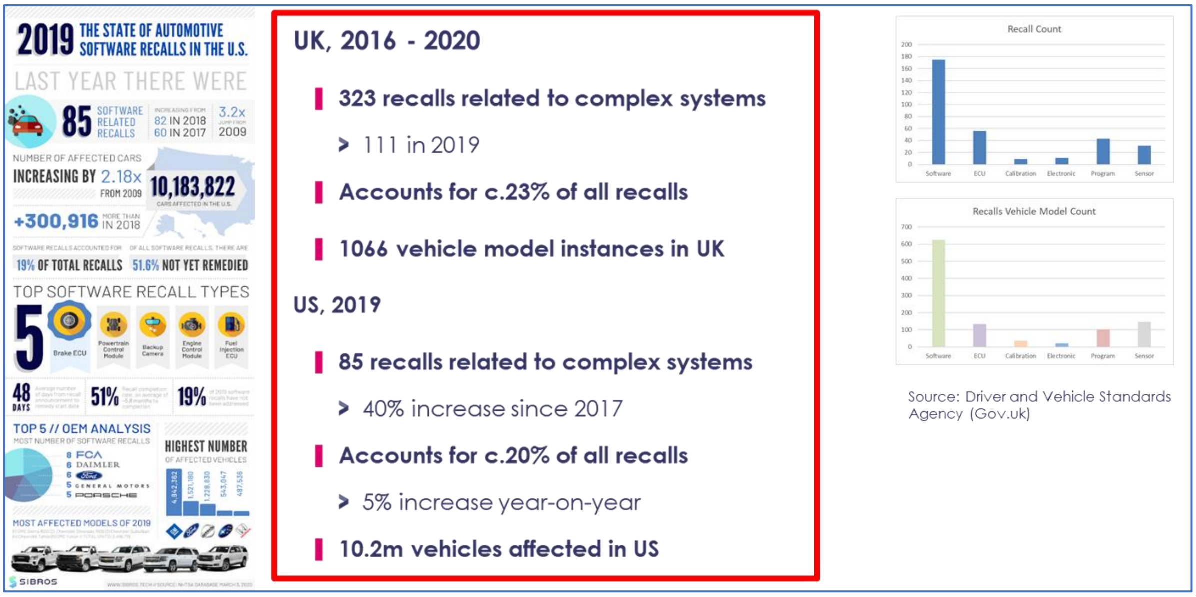
- Intertwined and interdependent components which interact
- Adaptive behaviour according to history or feedback
- Self-organisation
- Emergence which is not always predictable, centrally controlled or engineered
- Constantly changes, appearing dispositional and lacking causality
- Extreme, 'cascading' behaviour, power-laws can be observed – minor input changes can result in major output changes

Figure 1: The Problem is Extreme Complexity.

These systems can be stimulated to failure by cyber attacks. Whilst demonstrating the problem at the level of the global interconnected system we have also demonstrated it in secure chipsets and in systems including automotive braking, flight and energy control systems; all areas where the highest level of safety might be expected to apply and for which we are now demonstrating that the very engineering process being used for assurance are in fact the major contributor to the most catastrophic failures.

This problem is increasingly acknowledged and cited by C level business leaders and those of their supply chains, particularly in areas including Automotive and Medical where safety of life is a consideration. Evidence of this can be seen in the recent ministerial response to a Techworks letter with respect to the Automotive Transformation Fund and the Connected and Automated Mobility (CAM) Technology Acceleration Fund where the only subject explicitly now called out is Cyber Security.

As shown in the figure below complexity is fast becoming the principal cause of product recall in the automotive industry and given that it is growing at greater than 5% pa and vehicles are becoming increasingly complex with techniques including Artificial Intelligence (AI) / Machine Learning, approximate computing, smart sensors and edge / hybrid vehicles this is a trend that is increasingly set to dominate and will soon become unmanageable.



UK, 2016 - 2020

- 323 recalls related to complex systems
  - 111 in 2019
- Accounts for c.23% of all recalls
- 1066 vehicle model instances in UK

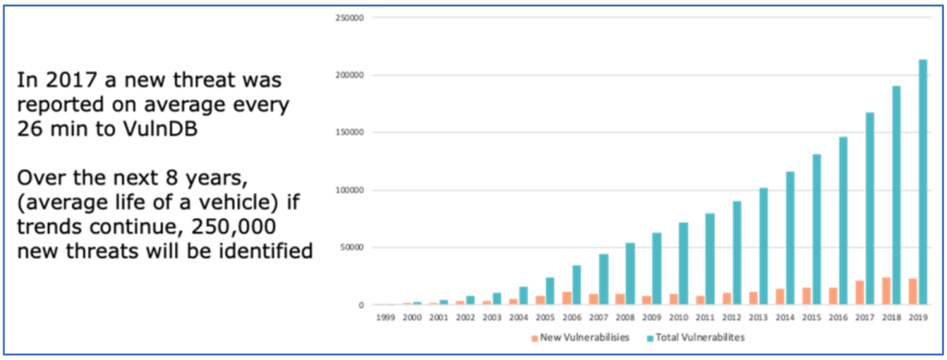
US, 2019

- 85 recalls related to complex systems
  - 40% increase since 2017
- Accounts for c.20% of all recalls
  - 5% increase year-on-year
- 10.2m vehicles affected in US

Source: Driver and Vehicle Standards Agency (Gov.uk)

Figure 2: Complexity Related Recalls

The cyber threat is often seen as exploiting well known IT vulnerabilities which in itself would likely result in ¼ million significant vulnerabilities for the automotive industry and connected cyber physical systems in general we are increasingly seeing the emergence of attacks exploiting 'emergence' as a method to attack the space outside the model analysed at design time. Cyber attacks in this context are just one type of highly targeted and inconvenient emergence showing no significant requirement for skill, opportunity or equipment



In 2017 a new threat was reported on average every 26 min to VulnDB

Over the next 8 years, (average life of a vehicle) if trends continue, 250,000 new threats will be identified

Figure 3: Emergence of Vulnerabilities.

Worse, as compared to electromechanical automotive systems which have a tendency to fail one at a time and are therefore insurable 'emergence' in modern automotive systems has the potential to fail globally as has already been seen in a number of IT examples including 'notpetya'; indeed cyber attackers including Miller and Valasek have observed[1] that only the most skilled attackers are able to target single vehicles which is the complete inverse of the experience from the electro mechanical space. Specifically, as illustrated in Figure 4, whilst practices such as ISO26262 normally presume that it is possible to conduct a risk analysis to justify the decision that a vehicle is 'fit for it's operating environment', the emergence of a cyber event having global effect would in some circumstances be expected to raise the vehicle from the central section of Figure 4 where 'pareto' arguments might apply and instead place the vehicle (all vehicles) in the top (red) where risk analysis methodologies do not apply or constitute a defence.

[1] Black Hat 2016

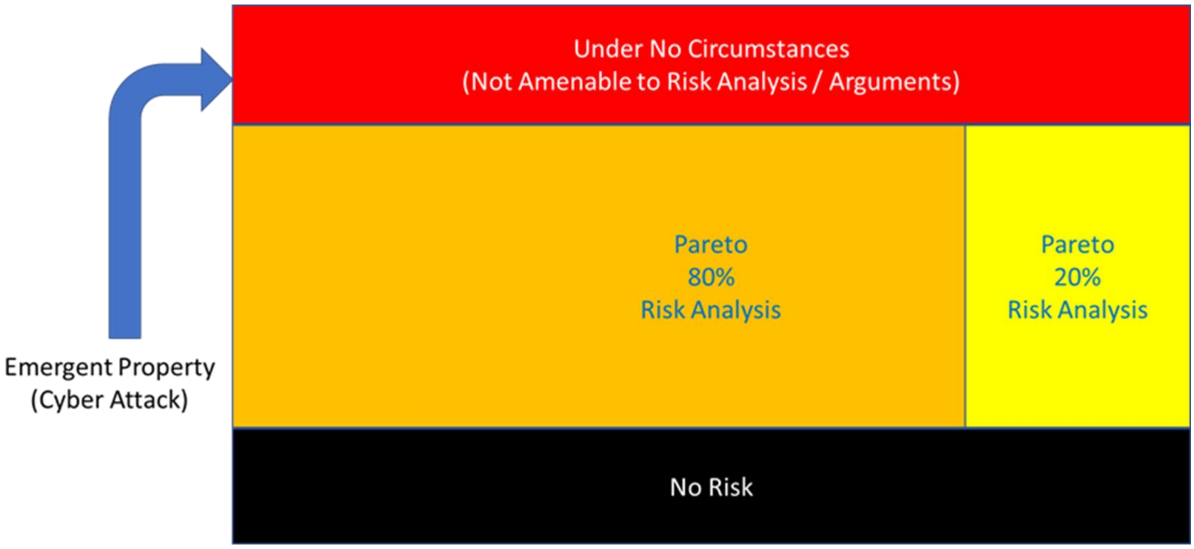


Figure 4: Problems with Risk in Cyber Physical Systems.

In response to this problem and further observations with respect to complexity science, the nature of evidence and significant work has been done to define a method based on 3 principles and 6 arguments to move the development of assurance to the operational rather than design space.

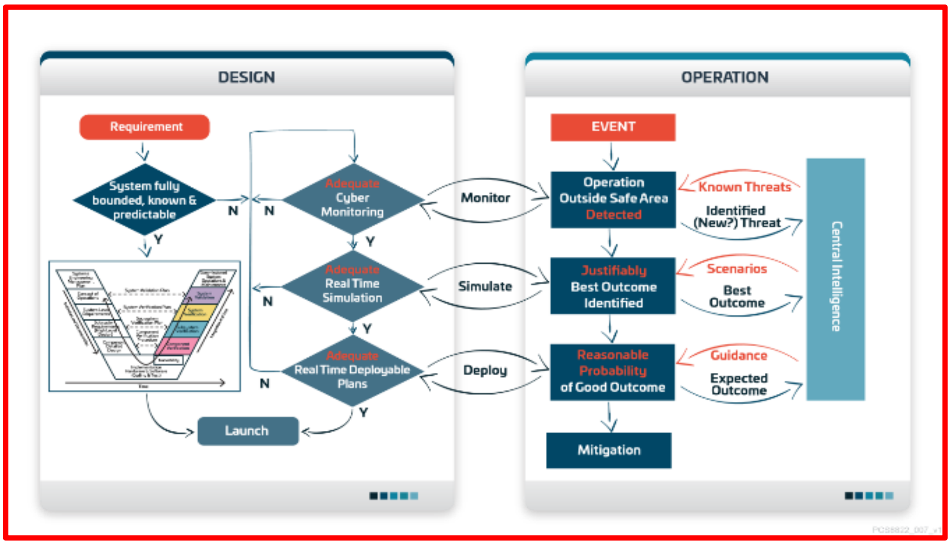
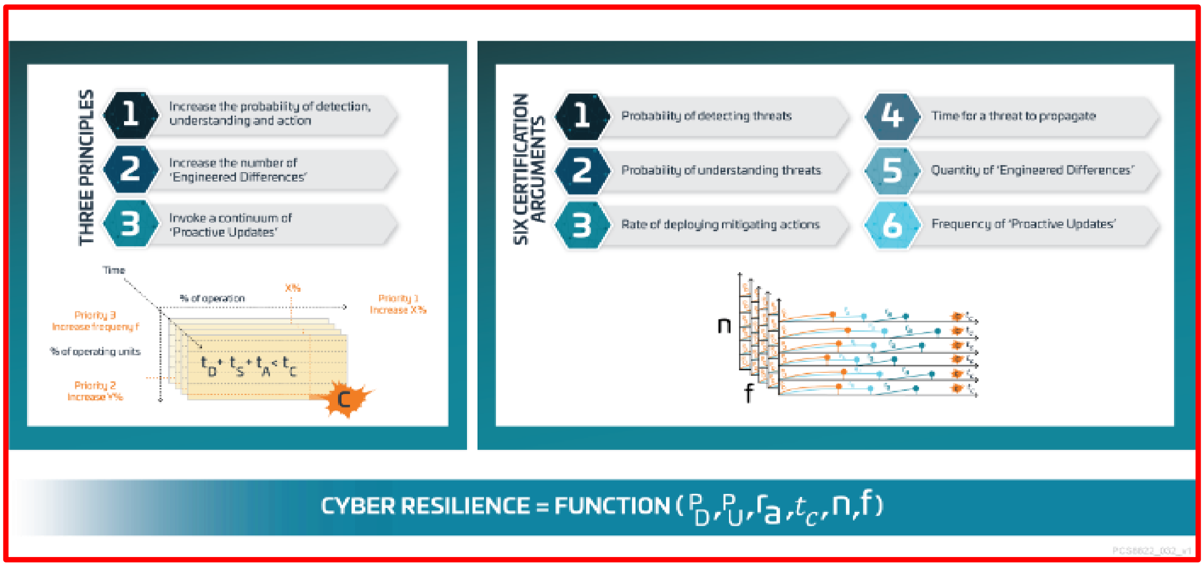

DESIGN
Requirement
System fully bounded, known & predictable
N
Y
Adequate Cyber Monitoring
N
Y
Adequate Real Time Simulation
N
Y
Adequate Real Time Deployable Plans
N
Y
Launch
Monitor
Simulate
Deploy
OPERATION
EVENT
Operation Outside Safe Area Detected
Known Threats
Identified (New?) Threat
Justifiably Best Outcome Identified
Scenarios
Best Outcome
Reasonable Probability of Good Outcome
Guidance
Expected Outcome
Mitigation
Central Intelligence

Figure 5: Resilience in Design and Operation.

In electro-mechanical systems, each system and platform is different and consequently each would be expected to be susceptible to failure in a different way and at a different time; the potential 'harm' arising from failure occurs with statistical probability, one device at a time. It is this principle that forms the basis of standard safety calculations. In digital systems it is possible that an identified fault could manifest in all digitally identical systems at the same time, thereby giving rise to global catastrophic failure. That is, at the level of the overall system of devices rather than at the level of the individual device.

Sharman et al. (2004), proposed functionality defence by heterogeneity as a paradigm for securing systems. This technique was inspired by the biological phenomenon of the human race surviving deadly viruses because of the diversity arising from heterogeneity. We use similar inspiration to create the concept of engineered differences. The approach is concerned with the deliberate introduction of significant differences between systems and platforms. These differences may be imperceptible to the user or operator but may prevent all systems being affected in the same way by cyber-attacks. At its most extreme one may suppose that a cyber physical system in which every entity was different would fail, and therefore be subject to calculation of harm, in the same way as an electro-mechanical system.



THREE PRINCIPLES

1 Increase the probability of detection, understanding and action

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)

Figure 6: The 3 Principles and 6 Arguments of CyRes.

Producing a system that exhibits significant differences in this way has been deemed economically infeasible on the basis that:

1. the need for V&V and product certification could not be borne on a per unit basis;
2. the economics of eg. chip design and manufacturing, together with the necessary ecosystem fabs, toolchains etc. favour a volume industry in which if you are not #1 or #2 then you are not likely to survive.

In addition:

3. it has been found to be technologically difficult to determine that one system or component is in fact significantly different from another.

For the engineering of significant difference to be a viable technique it must be possible to address each of the three points above.

In 'Technological and Economic Feasibility of the CyRes Methodology' [Thales 2020] drawing on areas including *Approximate Computing*, *CMOS Variability Modelling and Prediction*, *Nanoelectronics Devices and Modelling*, *Significant Difference* and *Appropriate Level of Resilience and Risk Management* to demonstrate that *Significant Difference* is economically and technologically beneficial and is feasible. Further it was shown that the investment currently made to turn inherently analogue systems into digital is creating significant vectors for catastrophic failure, diminishing the anticipated associated benefits that have driven the industry of the past decades.

Resting on the work of many of the ACE-CSRs and all of the NCSC supported RIs, 'Technological and Economic Feasibility of the CyRes Methodology' did significant amounts of the scientific groundwork and suggested a set of tools which over a 3-5 year period could allow the economically feasible operationalisation of future methods to combat cyber and complexity attacks against our most important products and systems.

ResiCAV+ has set out to demonstrate a basis of an extensible framework into which those tools might be integrated and that these tools could form the basis of a legally defensible and adoptable engineering methodology for the Automotive industry throughout its supply ecosystem.

4 What was Demonstrated

ResiCav+ demonstrated the principles of a scalable ‘Tool Framework’ for detection based around recording of evidence and decision making.

In the context of this ‘Tool Framework’ ResiCav+ has demonstrated the automatic / semi-automatic use of tools in the context of CyRes to provide both system resilience and evidence for courts or regulators in a way that could feasibly and beneficially be integrated into OEM and Tier supplier processes. Application in this way would transform a design time only activity into one capable of operating both effectively and economically through life.

ResiCav+ has also shown a scalable methodology that can be used to capture and react appropriately to emergence from wider environmental conditions moving forward significantly from the current position that restricts concern to environmental changes caused by software.

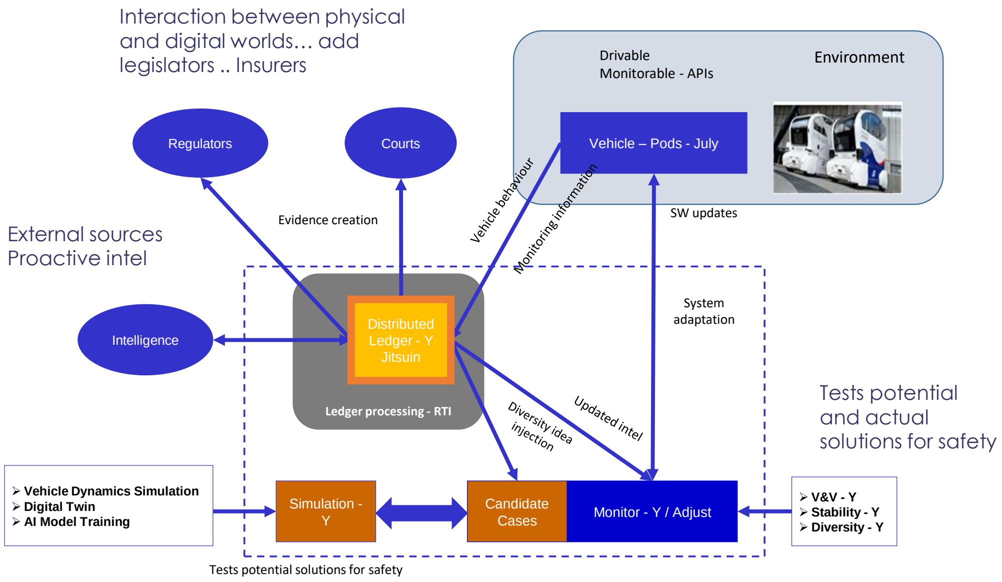


Figure 7: Scalable, Evidential Quality Feedback to Operation.

The ResiCav+ solution used multiple simulations of various aspects of the vehicle, against candidate uses cases, to predict how the system will behave. These use-cases and the model are bound within a set of assumptions about the range of inputs & behaviours in the deployed system – these are the constraints of the simulation.

Feedback from the deployed system in the vehicle recorded anomalous events, inputs & behaviours. Those inputs and behaviours outside of the constraints of the simulation need to be assessed – possibly by widening the inputs to the simulation to cover these new found scenarios. With these update simulations the system can assess of these previously unexpected inputs are suitably handled, and we probably extended the input data and therefore the constraints to reflect this new found information. Or the simulation identifies the system does not behave as desired and some other course of action is required.

Using this tool chain, ResiCav+, work previously conducted on the CyRes methodology and predecessor projects as well as the self-funded work of the project partners and their academic and industrial partners the project partners sought to answer the question ‘who might take advantage of such a framework and tool chain’ by consulting with potential industrial and academic users.

In the case of potential academic sources of tools, the intention of this consultation was to determine whether:

a. the framework made it more feasible to bring ‘tools’ and concepts developed as part of academic research to market.
b. integration with such a framework might positively or negatively impact the long term future for such research.

Examples of academic partners consulted on this project included University of Warwick (a project partner) and University of Bristol and Imperial College.

In the case of industrial sources of tools, the intention of this consultation was to determine whether:

a. the framework was consistent with making effective use of funding models.
b. integration with such a framework might positively or negatively impact the long term exit strategies including prospects for sale of such companies.

Examples of industrials consulted on this project included Thales UK (a project partner) and Jitsuin.

In addition, ResiCAV+ consulted with representative members of the automotive eco system to determine whether the ResiCAV+ toolchain might advantageously be incorporated into their engineering / business processes, what impediments there might be to achieving this ad what advantages or disadvantages there might be were this to be achieved.

Finally, ResiCAV+ consulted with representative members of the vehicle standards and regulatory communities to determine whether the availability of a real-time tool chain capable of understanding, recording and acting to deliver evidential quality and actionable updates to deliver continuous, through life safe and resilient operation.

5 The ResiCAV+ Roadmap Conclusions

Actionable conclusions were made in the following areas:

5.1 Finance

1. During ResiCAV+, in discussion with both our academic and industrial respondents, the team had the opportunity to estimate the cost per tool and the likely number of tools to develop an adequately complete toolchain together with the likely Return on Investment. Whilst it was concluded that successfully developing the necessary tools in the UK could be worth in excess of £5bn per annum to the UK economy. It was concluded however, following consultation with the commercial financial community, that the probability of being able to raise the necessary finance in the UK would be low. ResiCAV+ suggests that the UK government should consider providing adequately targeted funding; models to consider might include the British Business Bank or other special purpose vehicle.

5.2 A Tools Framework.

2. In consultation with both academic and industrial sources of tools the 'Framework' demonstrated by ResiCav+ needs to be developed and refined so that it may act as the core for a developing ecosystem of tools from the UK and more widely. This should be complete to industrial quality by March 2023.

5.3 Tools.

3. Following a study involving a wider stakeholder group, a reference work defining a complete set of industrial quality tools necessary to operationalise the conclusions of this study within the framework at 1.1.1 above should be developed and, once endorsed by the stakeholder community, be maintained. An initial version of this reference must be available by December 2022 with an endorsed version available no later than Mar 2023.

4. The cost to develop tools cannot, and should not, be borne by 1 party alone. As OEM 3 noted were they to develop this for their own use then every other OEM and tier supplier would need to do the same. This would both result in high, unnecessary, and ongoing cost but would also run the significant risk of a 'wild west' in which key elements were tied up by one party to the detriment of others. Accordingly, a fund of not less than £150m over 3 years, with an additional £100m available over the subsequent 2 years, available to tool developers generating IPR in the UK should be set up by the UK Govt to support the development of a world leading tool ecosystem.

5. Tools developed or adapted for the 'Framework' and either publicly funded or using a significant contribution from public funding should be made available for licencing through the UK IPR Pool. The licencing terms must ensure that residual rights are retained in the UK in the event that the tool or IPR is sold.

5.4 Intellectual Property.

6. **UK IPR:** Thales will create a company limited by guarantee (available to others and in agreement with NCSC) to licence techniques eg data science algorithms identified under this programme to those in the UK committing to the maintenance of this for an initial period of 5 years.. It is intended that by retaining residual UK right in the event of a sale the developing 'basket' of rights will ensure that we do not develop a method which we then can't use and by ensuring that it can be used in the UK will help to attract inward investment.
7. **UK IPR Pool:** it is intended that the company limited by guarantee, if successful, should within the next 5 years form the basis of a sovereign IPR fund ensuring:
    a. The freedom for UK cyber companies to operate in emerging markets from CNI, through health and mobility where safety and security are a consideration,

    b. inward investment to the UK (in order to access that IP),
    c. additional levers to prevent offshoring of high value skills and jobs
    d. HMG value for money for research and other investments made.

5.5 Effective Use of Research Institutes.

8. **Cyber Centre of Excellence and UK Research Institutes:**
    a. there are a significant number of proposals eg. under the current **RITICS** (Research Institute in Trustworthy Interconnected Cyber Physical Systems) funding round that could be accelerated by allowing them to participate in this tool chain.
    b. The existence of the outcomes from ResiCAV+ help to add purpose to appropriate but what might otherwise be unconnected research activities significantly increasing impact.
    c. **T**he work of ResiCAV+ will help influence countermeasures to the type of data science based attacks currently being developed by QUB and **RISE** (Hardware Security Institute) which would be expected to be significantly impactful to static assurance in the near term.

5.6 Skills.

9. The net outcome of UN regs with respect to cyber has been to increase the skills deficit in an environment where the projected requirement is unachievable, and were it achievable unaffordable, and were it both achievable and affordable ineffective at scale. ResiCav+ has demonstrated that the requirement to reskill and the type of skills could be achievable, affordable and effective by prioritising the industrialisation of cyber resilience instead of trying to grow a highly paid cottage industry. It is important that this transition is achieved over the next 3 years before the cost of meeting regulations in the current manner makes this unaffordable.

5.7 Regulation and Law.

10. ResiCav+ has demonstrated that it is feasible to scale a tool based cyber resilience methodology in a complex system with emergent properties such that it could operate at a per vehicle (and per subsystem) level. It has demonstrated that this tool-based method is not inconsistent with the current international regulatory framework and could be used by regulators in the next step of their forward planning.

11. Regulation and Law. ResiCav+ demonstrated and articulated a framework for the evidence that must be collected to withstand prosecution and also identified that in the absence of adequate and well-founded regulation prosecution under eg HSWA with all of its onerous characteristics remains an option [even if that reg exists]. ResiCav+ therefore set out a map for continuous vehicle control that should be onward developed with the UK regulators

12. The use of a dynamic distributed ledger to record and inspect evidence of decisions made as part of the CyRes methodology enable a trustworthy trail of sustainable assurance evidence, which can support not only the defence of those decisions in court, but also regulatory compliance assessments.

13. The assurance arguments captured in the distributed ledger can support various aspects of current vehicle regulation, in particular UN R155 for cybersecurity and UN R156 for software updates.

14. The distributed ledger can facilitate demonstrating compliance with UN R155 and its requirements for conformity of production, provision of data to support the forensic analysis of events and manufacturer reporting of incidents.

15. The dynamic nature of the ledger also means that decisions leading to the delivery of software updates to vehicles and their impact on existing type approved systems can also be

captured and inspected, as required by UN R156, even if those software updates are deployed at higher frequencies in the future than typically seen today.

16. The benefits of using the distributed ledger extend beyond current forms of regulation, with the scale and automation provided by the technology enabling decisions and the associated arguments to be captured more dynamically and on a per-vehicle basis.

17. The stakeholder workshops conducted as part of the ResiCAV+ project highlighted that this more dynamic and continuous forms of assurance and associated regulatory mechanisms would be desirable. Furthermore, they would only be feasible if supported by appropriate tools that could operate at the scale and with the necessary automation.

18. The methodology and tools developed as part of ResiCAV+ provide this scale and automation and are expected to offer particular benefits for new assurance schemes such as CAVPASS, which focuses on safety and security assurance of increasingly connected and automated vehicles. These benefits should also be promoted internationally in order to establish a basis for future more dynamic regulatory compliance initiatives, including future revisions of UN R155 and R156.

19. Type approval requirements that are fit for purpose in respect of vehicle cyber security are crucial because of the pivotal role that type approval plays in setting vehicle safety expectations, aligning industry standards and supporting consumer confidence. Enforcement against failures of design or construction of highly technical cyber security systems through general product safety, general health and safety or product liability legislation is not satisfactory for either consumers, regulators or the automotive industry. This is particularly so since these general legal frameworks themselves continue to evolve to catch up with the increasing cyber physical nature of products (some of the key frameworks originate from a pre-internet age). Historically, these general legal frameworks have tended only to be enforced in respect of as products or vehicles are operated, maintained and deployed by users or otherwise fail to conform to relevant type approvals.

20. There is recognition in the evolving and emerging type approval framework that cyber threats are dynamic, and that cyber security actively involves an element of anticipating novel cyber threats and, ultimately, the probability of successful cyber-attack from novel threats. However, beyond high level requirements to assess these risks and mitigate them, specific cyber security technologies and methodologies are not prescribed in detail.

21. The dynamic and emergent nature of cyber threats and the material risk that novel cyber attacks will be successful pose particular challenges as regards hazard identification and mitigation measures. Enduring cyber resilience may require technologies and design methodologies and frameworks that ultimately require systems to take automated decisions in real time to respond to such threats to mitigate risk or fail safe. Notwithstanding automated decision-making, it is expected that automotive OEMs deploying such systems would remain responsible for the performance and decisions taken by their cyber security system.

22. The rapid move from a single driver or single vehicle emphasis to integrated roads systems is now attracting greater attention on system-based safety issues as well as investigation and enforcement. It is conceivable that the HSWA criminal investigation and enforcement may extend in the near future to road and vehicle system safety issues including cyber vulnerabilities which would have potentially quite wide ranging (and potentially unintended) consequences for the development of new automotive technologies.

23. Should ResiCAV+ partners wish to demonstrate a route to a legally defensible argument hypothetically using ALARP principles and processes, we have considered and set out in this paper the steps that the Health and Safety Executive or “HSE” (the main HSWA prosecutor)

would likely take to verify that risks had been reduced ALARP. This iterative approach requires:

a. Assessment of risks;
b. Assessment of sacrifice;
c. Undertaking cost-benefit analysis;
d. Selection and implementation of mitigations; and
e. Monitoring and evaluation of risks and data.
a. Against each step, we have indicated what ResiCAV+ would have to demonstrate and document to satisfy HSE that risks were being managed ALARP if required to do so. Adopting this format and approach would permit ResiCAV+ partners to justify and explain their, processes and methodology on an ALARP basis including its use of the significant difference and distributed ledger approach. Combined with onboard collection of incident data that could be forensically examined, this provides a route to thinking through what would be required to justify not just decision-making but the underlying system choices and architecture that led to it.

5.8 Simulation based Verification.

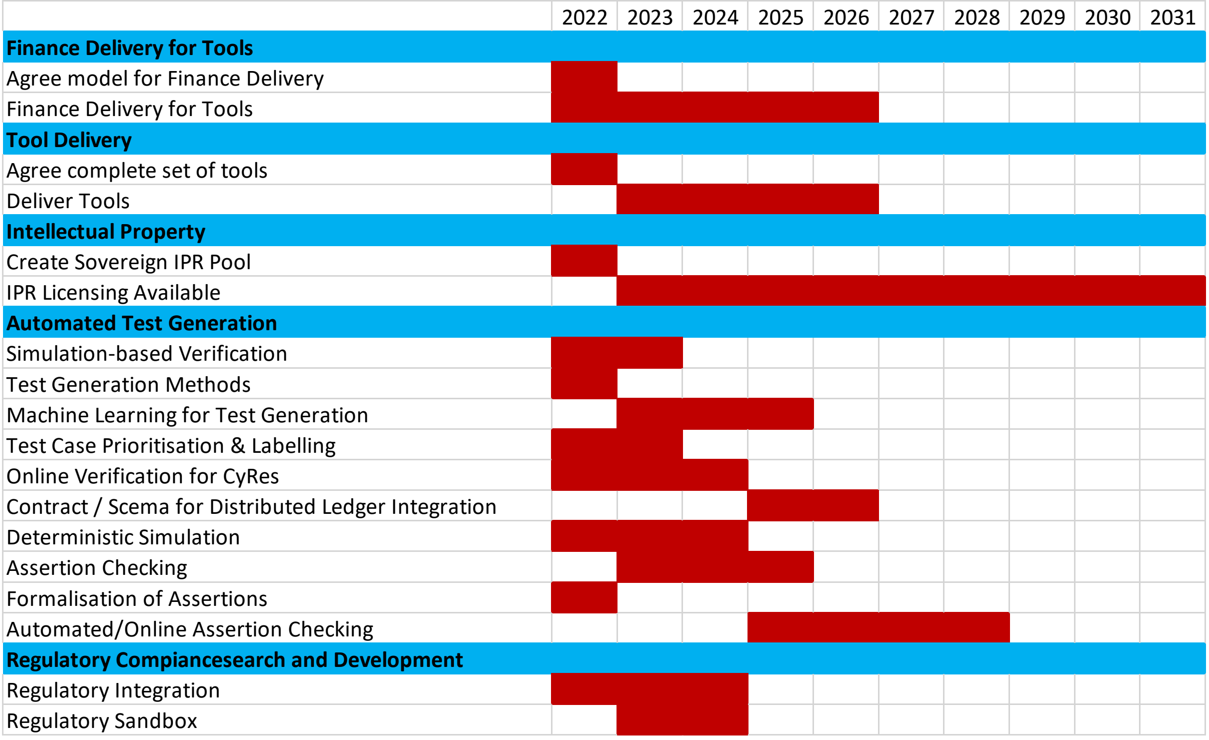
24. **The Fallacious arguments.** CyRes demonstrated the very severe limits of simulation in drawing functionality and safety conclusions particularly when not used as part of an overall methodology to control harm such as CyRes. ResiCav+ demonstrated where simulation, constraints and AI / ML might be used in an ongoing way to produce the necessary evidence for compliance and legal sustainability. It will be important that this becomes part of the regulatory understanding over the next 2-3 years if the industry is not to risk having its methodologies questioned in court.

25. **Assertion based real time V&V.** ResiCav+ explored and demonstrated the need for Assertion Checking, Formalisation of Assertions and Automated/Online Assertion Checking in order to support real time V&V. To support the emergence of the necessary automation and tools to enable CyRes Formalisation of Assertions must be completed during 2022, Assertion Checking during the 3 years from 2023 to 2025 and Automated/Online Assertion Checking during the period from 2025 to 2028.

5.9 National Security, Freedom of Action.

26. The UK currently has an excellent position with respect to advanced automotive cyber security / resilience. A national IPR pool should be established, available to organisations operating from the UK, to ensure inward investment and prevent UK suppliers being either driven overseas or purchased by overseas competitors. This requirement is even more important given the applicability of the techniques outside the Automotive sector and therefore the criticality to both high value jobs, the trading position, and the national wellbeing of the UK.

6 Roadmap Table



	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
Finance Delivery for Tools										
Agree model for Finance Delivery	🟥									
Finance Delivery for Tools	🟥	🟥	🟥	🟥	🟥					
Tool Delivery										
Agree complete set of tools	🟥									
Deliver Tools		🟥	🟥	🟥	🟥					
Intellectual Property										
Create Sovereign IPR Pool	🟥									
IPR Licensing Available		🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Automated Test Generation										
Simulation-based Verification	🟥	🟥								
Test Generation Methods	🟥									
Machine Learning for Test Generation		🟥	🟥	🟥						
Test Case Prioritisation & Labelling	🟥	🟥								
Online Verification for CyRes	🟥	🟥	🟥							
Contract / Scema for Distributed Ledger Integration				🟥	🟥					
Deterministic Simulation	🟥	🟥	🟥							
Assertion Checking		🟥	🟥	🟥						
Formalisation of Assertions	🟥									
Automated/Online Assertion Checking				🟥	🟥	🟥	🟥			
Regulatory Compiancesearch and Development										
Regulatory Integration	🟥	🟥	🟥							
Regulatory Sandbox		🟥	🟥							

Figure 8: Table of Roadmap Activities

Acknowledgements

The ResiCAV+ contributors would like to acknowledge

ZENZIC
SELF-DRIVING REVOLUTION

Centre for Connected
& Autonomous Vehicles

Innovate UK

in making this study possible.

ZENZIC

SELF-DRIVING REVOLUTION

To find out more, please email info@zenzic.io

zenzic.io