United Kingdom

Compliance Report

A HORIBA COMPANY MIRA THALES WMG THE UNIVERSITY OF WARWICK

ZENZIC SELF-DRIVING REVOLUTION NOVA MODUS Burges Salmon AESIN AUTOMOTIVE ELECTRONICS INNOVATION

Authors

Dr Alastair Ruddle Paul Wooderson Dr Garikayi Madzudzo	HORIBA MIRA Ltd.

Executive Summary

Current vehicle regulations focus on certification prior to vehicle launch, achieved using the process known as Vehicle Type Approval, but provide limited ongoing assurance over the vehicle lifetime. In future, however, it is expected that vehicle software will be subject to through-life updates, which are likely to include the implementation of mitigations for previously undetected or emerging cybersecurity vulnerabilities.

The ResiCAV+ project follows previous initiatives, including the original ResiCAV project and the development of the CyRes methodology in the AESIN Security Workstream:

- CyRes Proposed methodology to achieve vehicle cybersecurity resilience
- ResiCAV Innovate UK project to investigate how the mobility industry can respond to emerging cybersecurity threats (2020)
- ResiCAV+ Innovate UK project to investigate the feasibility of applying the CyRes Methodology (2021-2022)

The original ResiCAV project in 2020 identified the need to move to more continuous and dynamic forms of regulation in order to assure the cyber resilience of future vehicles, and introduced the CyRes Methodology. The ResCAV+ project continues this work, developing demonstrator tools for the “Significant Difference” element of the CyRes Methodology, together with the use of a Dynamic Distributed Ledger (DDL) as a supporting framework to store and inspect legally sustainable assurance arguments. This “Compliance Report” addresses the suitability of the developed methods and DDL and the associated sustainable arguments in the context of current and potential future regulatory compliance environments.

The ability of the developed methods to support compliance to the recently enforced UN R155 and UN R156 has been evaluated. A core requirement for the type approval of vehicles is “conformity of production” (CoP), which aims to ensure that the entire production run maintains the same performance criteria as at the initial type approval. There may be potential for conflict between current CoP requirements and the vehicle differentiation that is envisaged in the CyRes methodology. As such, considerable care would be needed to ensure (and document) that the “engineered significant differences” do not impact on the specific performance characteristics that are subject to type approval regulations, as failure to do so would result in the loss of type approval.

A key element of the CyRes methodology is to proactively update software frequently to mitigate detected issues. It should be noted that in addition to the intended changes, software updates could

also have unintended impacts on other vehicle performance characteristics that may appear unrelated at first sight and are difficult to predict, such as EMC. Care therefore needs to be taken when applying the methodology under the current UNECE regulatory system to ensure that a software update does not inadvertently invalidate the type approval regarding any of these performance characteristics, particularly when an individual vehicle may diverge from other members of its type.

The ALARP principle is often used in health and safety risk management, and has been investigated through the ResiCAV+ compliance workshops in terms of its suitability for use in cybersecurity risk management. The ALARP principle requires demonstrable selection of the most effective mitigation or combination of mitigations, unless the resulting cost is grossly disproportionate to the associated risk. The cybersecurity environment, however, is radically different from the health and safety environment, the former being driven by human ingenuity exploiting technological changes. This makes it particularly challenging to estimate cybersecurity risk sufficiently accurately to enable it to be compared with the cost of the candidate mitigations.

The use of a DDL to record and inspect evidence of decisions made as part of the CyRes methodology to support compliance to UN R155 and UN R156 has been investigated. The DDL can facilitate demonstrating compliance with many aspects of UN R155 and its requirements for conformity of production, provision of data to support the forensic analysis of events and manufacturer reporting of incidents. 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.

The benefits of using the DDL extend beyond the current regulations, 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. The stakeholder workshops conducted as part of the ResiCAV+ project highlighted that 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.

The responsibility and sign-off requirements for such automated tools were explored during the compliance workshops. It was noted that automated decision-making would also include any automation as part of a cyber resilient system, in which the automated tool would be part of a mitigation that would need to be balanced against other possible mitigations. The approval for the deployment of such tools would replace the more established sign-off of vehicle design documents,

and organisational processes would need to be adapted to enable this sign-off based on sufficient understanding of the automated tool, requiring appropriate competence and authority.

The benefits of the methodology and tools for cyber resilient operation developed as part of ResiCAV+ have potential to provide the assurance arguments required for many aspects of UN R155 and R156, subject to some potential conflicts with the constraints of the current regulatory process. The scale and automation are expected to offer particular benefits for new assurance schemes such as CAVPASS and should be promoted internationally in order to establish a basis for future dynamic regulatory compliance initiatives, including future revisions of UN R155 and R156.

Abbreviations

AA	Approval Authority
ABS	Anti-lock Braking System
ACC	Adaptive Cruise Control
ALARP	As Low As Reasonably Practicable
ALKS	Automated Lane-Keeping System
CAV	Connected and Automated Vehicle
CAVPASS	Connected and Automated Vehicles Process for Assuring Safety and Security
CoP	Conformity of Production
CSMS	Cyber Security Management System
CyRes	Proposed methodology to achieve vehicle cybersecurity resilience
DDL	Dynamic Distributed Ledger
ECWVTA	EC Whole Vehicle Type Approval
EMC	Electromagnetic Compatibility
GNSS	Global Navigation Satellite System
HSE	Health and Safety Executive (UK)
ISO	International Standards Organisation
MoT	Ministry of Transport (annual vehicle safety test)
OBD	On-Board Diagnostics
OTA	Over-the-Air (i.e. wireless)
PTI	Periodic Technical Inspection (see R156 [16])
ResiCAV	Innovate UK project to investigate how the mobility industry can respond to emerging cybersecurity threats
ResiCAV+	Innovate UK project to investigate the feasibility of applying the CyRes Methodology
RXSWIN	Regulation X Software Identification Number
SAE	Society of Automotive Engineers (US Learned Society)
STU	Separate Technical Unit
SUMS	Software Update Management System
TS	Technical Service
UNECE	United Nations Economic Commission for Europe
VCA	Vehicle Certification Agency (UK Vehicle Type Approval Authority)
VM	Vehicle Manufacturer

Key Definitions

Approval Authority	Body empowered to grant vehicle type approval in a particular jurisdiction (e.g. VCA in the UK).
ALARP	"ALARP" means "as low as reasonably practicable". Reasonably practicable involves weighing a risk against the trouble, time and money needed to control it. Thus, ALARP describes the level to which the UK HSE expect to see workplace risks controlled.
Assurance	Justifiable grounds for confidence that the risks of using a product, process or service are acceptable to the stakeholders [1].
Certification	The provision of an official document attesting that a supplier has collated or provided convincing evidence that appropriate measures have been successfully implemented to ensure that the risks of using a product, process or service are acceptable to the stakeholders [1].
Conformity of Production	Every vehicle, equipment or part approved pursuant to a UN Regulation annexed to the 1958 Agreement shall be so manufactured as to conform to the type approved by meeting the requirements of UN E/ECE/TRANS/505/Rev.3 [8] and of the said UN Regulation.
Cyber attack	Any attempt to gain unauthorized access to and/or control of the data held within, received by (from sensors and/or communications), or transmitted from (via actuators and/or communications) a product, process or service, including both intentional and unintentional interference with the normal operation of the product, process or service [1].
Cybersecurity Management System (CSMS)	A systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber attacks, to comply with the requirements for management of cybersecurity of UNECE Regulation 155 [15].
Cybersecurity resilience	Ability to ensure the continued execution, or timely resumption, of the essential functions of a system, safely and securely, accommodating/mitigating foreseeable safety hazards and other potential threats (operational, financial, privacy) resulting from cyber-related failures or interference with the normal operation of a product, process or service, and enabling a graceful degradation of performance otherwise [1].
Cybersecurity	Freedom from unacceptable risk of fraudulent financial transactions, compromised privacy, impaired system services, and physical injury or damage to health, property or the environment that could result, either directly or indirectly, from unauthorized monitoring and/or control of the data entering, leaving, or held within a product, process or service [1].

EC Wole Vehicle Type Approval	Process by which passenger cars, goods vehicles, buses and coaches, motor caravans, trailers, and their systems and components, are approved for sale in the EU [3].
Operational assurance	Justifiable grounds for confidence that the risks of continuing to use a product, process or service remain acceptable to the stakeholders throughout its life [1].
Over-the-Air (OTA) update	Data transfers achieved by any wireless method, instead of using a cable or other local connection [16].
RX Software Identification Number	A dedicated identifier, defined by the vehicle manufacturer, representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N° X type approval relevant characteristics of the vehicle [16].
Software update	A package used to upgrade software to a new version including a change of the configuration parameters [16].
Software Update Management System (SUMS)	A systematic approach defining organizational processes and procedures to comply with the requirements for delivery of software updates according to UNECE Regulation 156 [16].
Technical Service	Organisation designated by Approval Authorities to carry out assessment to specified UNECE standards for vehicle type approval purposes.
Threat	Potential source of damage to the stakeholders, in terms of compromised safety, privacy, financial or operational performance, that could result from the exploitation of one or more vulnerabilities of a product, process or service by a threat agent in order to achieve a particular attack objective [1].
Vehicle Type	In the context of Type Approval, a Vehicle Type is a group of vehicles produced by a vehicle manufacturer that do not differ significantly in terms of essential aspects regarding certain specified performance standards.
Vehicle Type Approval	Process providing confirmation that production samples of a type of vehicle, vehicle system, component or separate technical unit will meet certain specified performance standards.

Contents

Page

1. Introduction

Current regulatory regimes focus on certification prior to vehicle launch, achieved using the process known as Vehicle Type Approval, but provide limited ongoing assurance over the vehicle lifetime. In future, however, it is expected that vehicle software will be subject to through-life updates, which are likely to include the implementation of mitigations for previously undetected or emerging cybersecurity vulnerabilities, as well as implementing new or enhanced vehicle functionality. These changes will therefore need to be assessed to ensure that they do not compromise the type approval.

The ResiCAV project (March 2020) identified the need to move to more continuous and dynamic forms of regulation in order to assure the cyber resilience of future vehicles, recommending [1]:

> "research into methods and frameworks needed to provide continuous assurance throughout the lifecycle of vehicles and the mobility ecosystem, as well as new models of regulation that can be applied beyond start of production and allow for more dynamic forms of type approval."

In addition, the ResiCAV project included an evaluation of the technical and economic feasibility of implementing the CyRes Methodology, outlined in ResiCAV Deliverable 2 [2]. This report considers the applicability of the CyRes approach, together with the use of a Dynamic Distributed Ledger (DDL) as a supporting framework, in:

- achieving cybersecurity resilience in the automotive domain,
- demonstrating due diligence on the part of the vehicle manufacturer in the legal domain.

Chapter 2 outlines the underlying process of type approval, while chapter 3 gives an overview of assurance including assuring complex systems. Chapters 4 and 5 summarize the CyRes Methodology and DDL technology, respectively. Chapter 6 identifies current relevant regulatory requirements and chapter 7 considers the applicability of the CyRes Methodology and DDL technology for demonstrating compliance with the current regulatory requirements. Chapter 8 outlines the characteristics of operational assurance and potential future regulation. Finally, chapter 9 summarizes the conclusions and recommendations.

2. Vehicle Type Approval

In relation to Type Approval, a Vehicle Type is a group of vehicles produced by a vehicle manufacturer (VM) that do not differ significantly in terms of essential aspects regarding certain specified performance standards.

There are many different mandatory requirements for vehicles and components/separate technical unit (STUs) covering subjects such as gaseous (e.g. exhaust tail-pipe) emissions, braking, vision, lighting, and electromagnetic compatibility (EMC), amongst many others. For most components/STUs and for vehicles these are legal requirements and appropriate Type Approvals must be obtained before registration and/or sale. It should be noted, however, that this is an over-simplification, as there are circumstances where components/STUs do not require Type Approval.

Vehicle type approval therefore provides confirmation that production samples of a type of vehicle, vehicle system, component or STU will meet certain specified performance standards. This provides a mechanism for ensuring that the manufacturer can consistently produce vehicles that satisfy the approved specifications in relation to relevant safety, environmental (including EMC), and security performance requirements.

There is no central EU approval body: authorized approval bodies of member states are responsible for type approval, which will also be accepted in all other member states. The legislative instruments which govern automotive type approval schemes require third party approval – testing, certification and production conformity assessment by an independent body. A country may appoint an Approval Authority (AA) to issue the approvals and a Technical Service (TS) to carry out the testing to the relevant legislative instruments. Vehicle Type Approval is a formal process whereby the AA issues a certificate confirming that a given Type of vehicle, sub-assembly or component/separate technical unit (STU) meets an applicable requirement for use on the public road.

In Europe, there are presently two systems of Type Approval in operation: European Community Whole Vehicle Type Approval (ECWVTA) and United Nations Type Approval. Type Approvals must be obtained before registration and/or sale of the vehicle. In all cases these European Community directives (EC and EU) either require ‘e’ marking or ‘E’ marking to a delegated UNECE Regulation.

In the UK, the Vehicle Certification Agency (VCA) is the designated UK AA for automotive products and also a designated TS for type approval testing in the United Nations (UN) scheme. As the UK Type Approval Authority, VCA has responsibility to issue UK type approvals on behalf of the Secretary of State for Transport under the UN and the UK type approval schemes.

2.1 EC Whole Vehicle Type Approval

The European ECWVTA Directive (2007/46/EC [3], as last amended by 2017/2400/EU [4]) covers passenger cars, goods vehicles, buses and coaches, motor caravans, trailers, and systems and components. The directive also has schemes for low volume/small series manufacturers, operating in the EU or in individual member states, as well as for "individual vehicle approval" for making or importing a single vehicle or a very small number of vehicles in certain categories (passenger cars, goods vehicles, buses and coaches, trailers and special purpose vehicles, such as vehicles specially designed to hold a wheelchair).

There are also separate directives for motorcycles, tricycles and quadricycles (2013/168/EU [5], as amended), as well as agricultural and forestry vehicles (2013/167/EU [6], as amended).

2.2 United Nations Type Approval

The United Nations European Commission for Europe (UNECE) publishes a series of regulations (currently numbering 163) for systems and components. Type Approval to these regulations require 'E' marking. A number of the UNECE Regulations have been adopted by the EC Directives and replace former EC Directives covering the same subjects.

There is a long-term objective to replace vehicle type approval by country with a mutually recognized international vehicle type approval for vehicles. Currently, however, the UNECE has implemented this for vehicles of category M_1 only (i.e. passenger cars [7]), through UNECE Regulation 0 [8].

2.3 Conformity of Production

A mandatory prerequisite of type approval is that the manufacturer has appropriate measures in place to ensure that production samples will continue to meet the same performance requirements as the products originally examined. This is known as Conformity of Production (CoP).

CoP requires that every vehicle, equipment or part approved pursuant to a UN Regulation annexed to the 1958 Agreement shall be so manufactured as to conform to the type approved by meeting the requirements of UN E/ECE/TRANS/505/Rev.3 [8] and of the said UN Regulation.

Consequently, it is necessary for the manufacturer to control production such that all examples comply with all of the type approval requirements, and to establish that any products with deviations from the approved type remain compliant with the full set of requirements for that type approval.

There are also obligations on the AA to audit the CoP processes at regular intervals, and withdraw type approval if the results are not satisfactory.

CoP requirements are based around established quality systems principles and, in general, certification to ISO 9001 [9] is often an acceptable basis.

2.4 Type Approval Process

Both type approval systems are very similar, and the main steps involved in the process are:

- application by the vehicle or component manufacturer;
- identification of the relevant requirements;
- appropriate testing by a technical service;
- granting of the approval by an AA;
- Conformity of Production established by the manufacturer in agreement with the AA;
- Certificate of Conformity by the manufacturer for the end-user.

There are multiple methods available for type approval. For ECWVTA type approval of whole vehicles, manufacturers may select one of the following approaches:

- **Step-by-step Type Approval:** a vehicle approval procedure consisting in the step-by-step collection of the whole set of EC type-approval certificates for the systems, components and separate technical units relating to the vehicle, and which leads, at the final stage, to the approval of the whole vehicle.
- **Single-step Type Approval:** a procedure consisting in the approval of a vehicle as a whole by means of a single operation.
- **Mixed Type Approval:** a step-by-step Type Approval procedure for which one or more system approvals are achieved during the final stage of the approval of the whole vehicle, without it being necessary to issue the EC Type Approval certificates for those systems.
- **Multi-stage Type Approval:** the procedure whereby one or more Member States certify that, depending on the state of completion, an incomplete or completed type of vehicle satisfies the relevant administrative provisions and technical requirements.

The multi-stage type-approval approach, for example, could be used for complete vehicles that are converted or modified by another manufacturer.

3. Vehicles as Complex Systems

Over time, the technical solutions implemented in products tend to become increasingly sophisticated as a result of technological development. However, there are subtle but significant differences between solutions that are simply more *complicated*, and those that are more *complex*.

Systems become more complicated through the integration of additional subsystems to add further functionality, or the use of more sophisticated technologies to implement established functions. In a complicated system, however, the functions continue to be provided by specific subsystems. More complex systems are characterised by the implementation of functions that depend on the interaction of multiple subsystems, with the result that the functionality of the system is more than the sum of its parts.

Historically, the vehicle system has become increasingly complicated as more functions have been implemented using additional subsystems. Examples include the introduction of electronic ignition, engine management and anti-lock braking systems (ABS). The introduction of these subsystems made the vehicle more complicated, but their ongoing operational independence meant that the vehicle was not more complex. Now, however, the vehicle is also becoming a complex system, as subsystems increasingly interact in order to contribute collectively to the achievement of vehicle level functions.

For example, the adaptive cruise control (ACC) function relies on a situational sensor to monitor the target vehicle in front, ground speed sensors to monitor the vehicle speed, and control of the throttle and brake actuators to adjust the vehicle speed to maintain the distance to the target vehicle. Consequently, ACC is an example of a complex system because it utilizes the functions of a number of subsystems in order to achieve functions that could not be provided by any of the subsystems in isolation.

3.1 Cybersecurity as an Emergent Property of Complex Systems

A related characteristic of complex systems is the presence of *emergent properties* that were not specifically intended, but nonetheless become possible as a result of the interactions between systems. These emergent properties frequently arise from unintended functionality or missing functionality that inadvertently results from limitations of the system requirements and/or design. For example, some of the missing functionality should perhaps have precluded some of the unintended functionality.

In principle, the “implemented behaviour” should be identical to the “intended behaviour” that was identified in the user requirements. In practice, however, specification flaws, design errors and implementation defects may mean that not all of the intended behaviour is actually achieved, resulting in “missing behaviour”, while some of the behaviour that is implemented may be unwanted “unintended behaviour” (see Figure 3.1). The implemented system functionality then comprises the incompletely implemented intended behaviour together with any unintended behaviour.

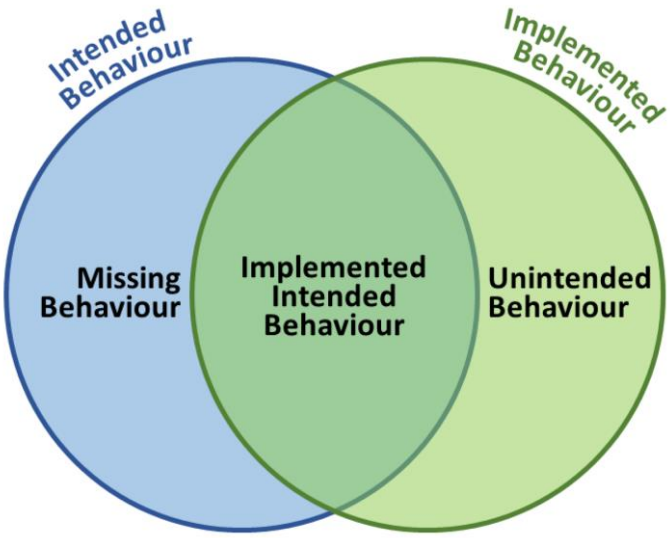


Figure 3.1 – Intended and implemented behaviour

Emergent properties can in some cases be beneficial. For example, it is not unusual for the users of a product to find ways to use it to undertake tasks that were never intended by the designers. However, emergent properties can also be exploited in a reckless or intentionally malicious manner if they have the potential to undermine safety properties, or can result in other types of harm, such as causing financial losses, compromised privacy, or deprivation of access to product functions or authorised services to others. Thus, cybersecurity vulnerabilities are prime examples of emergent behaviours that may be exploited for nefarious purposes.

The presence of a cybersecurity vulnerability does not constitute a threat in itself, but given the availability of a suitable exploitation mechanism and an attacker with the appropriate will, skills and resources then a threat may be associated with the vulnerability.

3.2 Prescriptive Assurance

Existing certification practices are based on prescriptive assurance approaches. These traditional methods of assurance are based on the use of regulations, standards and guidelines that must be complied with in order to establish whether a product can be considered suitable to be certified and placed on the market.

Prescriptive assurance approaches may be applied either to specific product features or to product development processes:

- **Product assurance standards** generally detail specific performance criteria that are required, as well as how they are to be demonstrated, and therefore reflect specific technologies, designs or features. Achieving assurance is then based on demonstrating compliance of the products with these requirements.
- **Process assurance standards** describe features of the process that is to be used in producing a product, rather than specific performance criteria or design features. Assurance is then based on establishing whether the process was followed, and often on the quality of the process and its outputs.

Prescriptive standards provide a very useful mechanism to collate, preserve and propagate product knowledge and experience, as well as lessons learned from past failures and accidents. Well-established supporting processes have been developed within vehicle manufacturers and their suppliers, using familiar methods for engineering and assurance that are based on prior experience of incremental development to accommodate emerging technological developments.

However, the prescriptive approach works best for relatively simple systems, with a limited number of functions, which are implemented by discrete subsystems and based on established technologies that develop relatively slowly. This enables the multi-level type approval processes used in the automotive industry, where vehicle type approval can be achieved based purely on type approval of the subsystems that make up the vehicle.

The prescriptive approach may also lead to an excessive focus on simply passing the test, which can lead to the exclusion of wider performance considerations that the spirit or goal of the test is intended to be representative of, or even outright fraudulent activity. Furthermore, inherent inertia in the standards development process can result in technology-centric prescriptive standards struggling to keep pace with the adoption of new technologies. Thus, current approaches are expected to become unmanageable in future.

3.3 Assurance for Complex Systems

The introduction of complexity into vehicle systems weakens the applicability of the decomposition approach that has traditionally been employed in type approval and certification. Functions that rely on multiple subsystems cannot be reliably verified at individual subsystem level. Furthermore, it is only possible to generate prescriptive requirements for demonstrating functionality that is intended by the designer. In addition, the additional freedom that complexity facilitates, particularly when enabled through use of software, means that the mechanisms by which a particular function is achieved in different products may become increasingly divergent. Verification requirements therefore need to focus on establishing that the overarching goals of the function are achieved, rather than the details of how the function is implemented.

Traditional functional testing is very good at identifying missing behaviour (for example, the system does not produce the correct outputs for given inputs), provided that it is sufficiently comprehensive. However, unintended and emergent functionality are, by their nature, not specified and not readily predictable. Consequently, it is impossible to define prescriptive tests for such unknown functionality. As a consequence of this there is a much greater onus on the product developer to ensure that possible issues are avoided in the design phase, rather than simply relying on subsequent verification and validation activities to reveal defects.

3.3.1 Goal-Based Assurance

Goal-based assurance approaches focus on the achievement of desired, measurable outcomes, rather than required product features or prescriptive processes, techniques, or procedures. In the goal-based approach the certification authority specifies a threshold of acceptable performance, and often (but not always) a means for assuring that the threshold has been met. This type of standard sets a goal, which is often a risk target, usually without specific direction as to how to achieve the required result. The reliance on enhanced development processes to mitigate the impact of incomplete validation and verification coverage also leads to requirements relating to the quality of these processes. The automotive functional safety standard ISO 26262 [10] provides a very relevant example, encompassing both process assurance and risk-based target elements.

The main disadvantages of goal-based regulations are that this is far less familiar than simple prescriptive approaches, and less straight-forward to apply, requiring more involved assessment to judge whether the evidence presented truly supports the claims made by the developer. In addition,

the goal-based approach requires wider understanding of the system and sub-system functions as well as more extensive analysis activity from the system integrator.

The advantages, however, are significant. Goal-based regulations aim to be technology agnostic, not reflecting specific technological solutions, and are thereby more readily adaptable to technologies that are novel or untried in the application of interest, thus reducing the standards maintenance burden. They focus on the achievement of desired, measurable outcomes, with targets that are risk-based and therefore better suited to complex systems with high levels of sub-system interaction that provide richer levels of functionality, but which cannot be exhaustively tested. In addition, goal-based approaches have already been adopted in more recently emerging disciplines in the automotive industry (e.g. functional safety [10] and SOTIF [11]).

3.3.2 Risk-Based Approach

Historically, vehicle development activities have largely been focused on the “intended use” of the vehicle, which is taken here to include its assumed behaviour and operating environment. However, this represents only a subset of all possible uses, and is complemented by the “unintended uses” which can be considered in terms of those that are potentially “foreseeable” and those that will remain “unforeseeable”. A subset of the unintended uses includes “intentional misuses”, at least some of which will be reasonably foreseeable based on past experience (see Figure 3.2). In the cybersecurity context, a well-known case is eavesdropping on keyless entry transmissions to enable criminal access [12]. However, the emergence of the unforeseeable uses and misuses is inevitable, given the long operational lifetime of a car, human ingenuity, and the increasingly rapid pace of technological change.

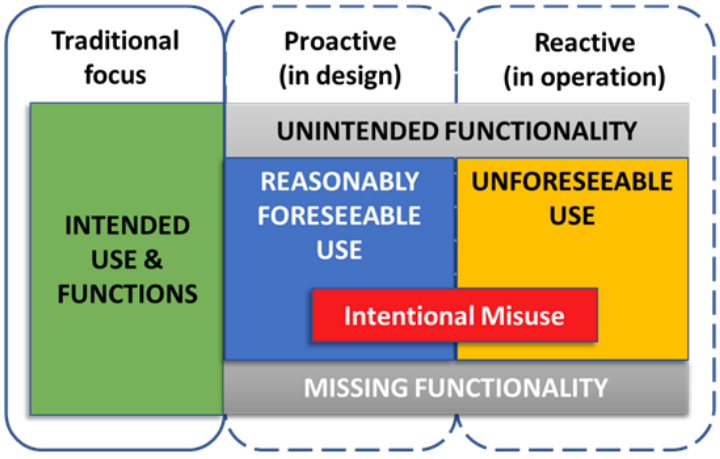


Figure 3.2 – Cybersecurity threats: unforeseeable and reasonably foreseeable misuse

To facilitate the setting of goals based on risk-based targets it is necessary to identify the potential threats to operation and then assess and categorize the resulting risks for the system stakeholders. In order to undertake such analysis, it is necessary to take a wide-ranging view of potential threats to identify and analyse the foreseeable threats, and hence mitigate those that are associated with the most significant risks.

In safety engineering a *safety hazard* is a source of possible *harm* to life, health, property or the environment. The *severity* is a measure of the expected degree of harm that may result from a hazard/threat in a specific situation. The associated *risk* is then a combination of the likelihood of occurrence of the source of harm and the severity of that harm, such that the risk increases with greater probability and/or severity. In some applications it is possible to quantify the likelihood and severity, using probability and cost for instance, with the result that the derived risk can also be quantified. In other applications, however, it is only possible to rank these measures in a qualitative manner. Such qualitative rankings often employ a classification based on order of magnitude differences.

In the security domain the source of harm is usually described as a 'security threat' and has other potential forms of harm beyond personal safety, such as unauthorized access to data or loss of privacy. As in safety engineering, it is recognised that eliminating all cybersecurity risks is not practicable, and that even if practicable it would be unaffordable. The pragmatic approach is therefore to identify the foreseeable threats, assess the associated risks, and apply appropriate mitigations to those that exceed broadly acceptable levels, such that the residual risks are at acceptable levels.

Risk assessment will also need to be applied to the analysis of unforeseen threats that emerge during operation in order to ensure that mitigation measures deemed to be necessary are appropriate to the risk associated with the threat.

In the cybersecurity context, assurance can be considered a means of establishing confidence that:

- the engineering of the product has taken cybersecurity into account and adequately addresses reasonably foreseeable threats;
- the implementation of the product achieves a residual level of security risk that is acceptable to the stakeholders; and
- appropriate processes are in place to monitor and respond to cybersecurity incidents identified during the operational lifetime and are effective in resolving emerging issues.

4. The CyRes Methodology

The CyRes Methodology has been developed to address the realisation that, for a trustworthy Connected and Autonomous future, we will need to practice a new 'Design for Cyber Resilient Operation' approach, leverage the best cross-sector practices and embrace 'Real Time' resilience as the new assurance paradigm. The CyRes methodology aims to reduce the probability that a random cyber event has catastrophic consequences. To achieve this, it extends the engineering V-model with innovative techniques that target design, manufacture, and operation. The CyRes model is illustrated in Figure 4.1 below.

Figure 4.1 – The CyRes model

The methodology is based on three key principles:

1. Increasing the probability of detection, understanding and timely reaction to cyber events;
2. Increasing the number of engineered significant differences;
3. Invoking a continuum of proactive updates during operation.

From the key principles, six certification arguments (shown in Figure 4.2) can be defined that can be used to justify the achievement of the principles and defend decisions made in legal or regulatory contexts.

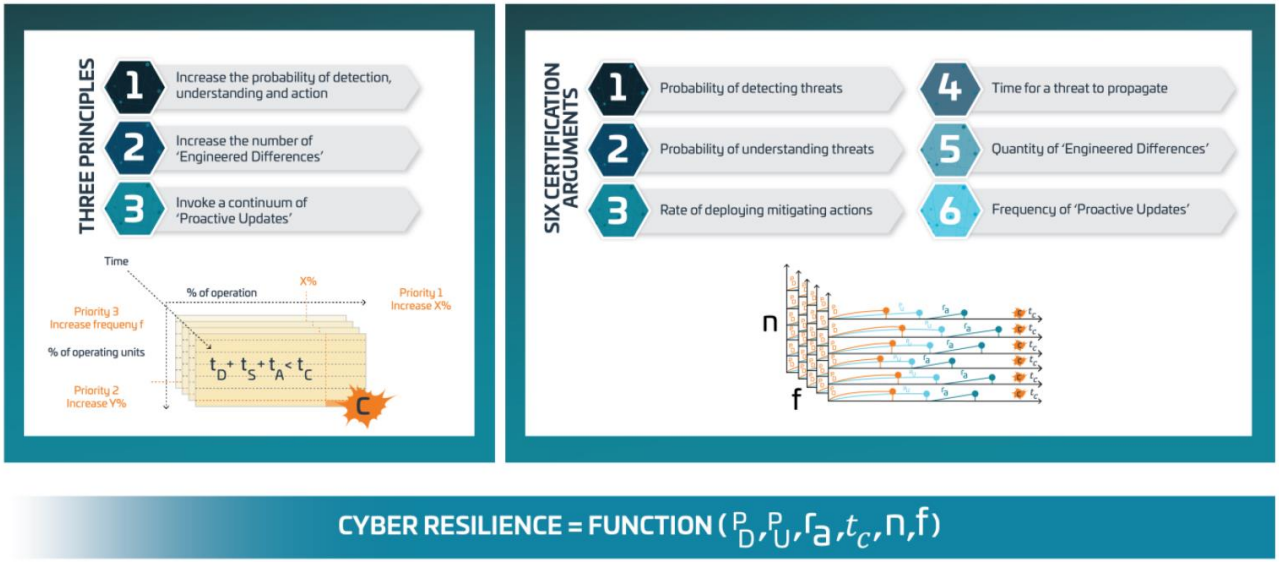


Figure 4.2 – The CyRes principles and certification arguments

The original ResiCAV project in 2020 described the CyRes methodology in detail and established its technical and commercial viability in Deliverable 2 [2]. The project also identified the need for further research and development of the key aspects of the CyRes methodology, in particular:

- new methods to increase the probability of detection, understanding and acting appropriately in response to attacks;
- methods to increase the number of 'Engineered Differences';
- methods to Invoke a continuum of 'Proactive Updates'; and
- sustainable legal and certification arguments to defend the sufficiency of the above.

ResiCAV+ continues this development focusing in particular on developing a demonstration of methods to implement, deploy and measure the significant difference in an automotive system (using the specific example of a braking system), and an approach to provide legally sustainable assurance and compliance arguments. The aspects covered in ResiCAV+ are illustrated in Figure 4.3.

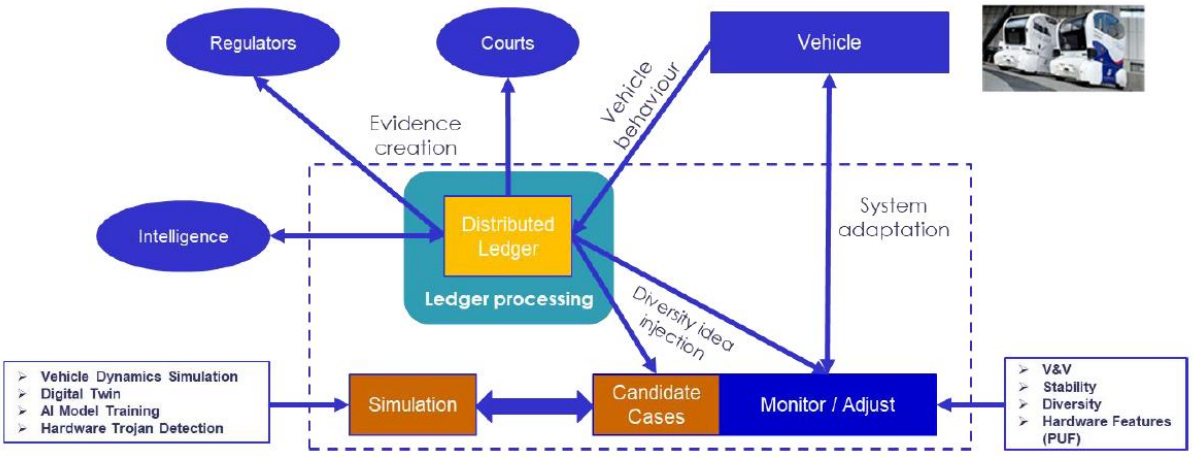


Figure 4.3 – Illustration of aspects of the CyRes methodology addressed by ResiCAV+

The lower part of the figure represents components of the Significant difference aspect of CyRes, in which parameters of a system such as its Stability and Diversity can be monitored and adjusted based on simulation of candidate responses in order to dynamically react to detected threats. The decisions leading to these parameter adjustments can be captured in a distributed ledger, which provides a trustworthy means of storing these decisions and can be used to provide evidence intended to be suitable for use in regulatory compliance and in courts.

In this “Compliance Report” we explore how the significant difference methodology and prototype tools developed in the ResiCAV+ project along with the use of the distributed ledger can be used to provide a route to the desired “Real Time” assurance arguments. The premise is that these assurance arguments can be used as evidence in current, proposed and future forms of regulatory compliance for connected and automated vehicles.

5. Dynamic Distributed Ledger

A distributed ledger is essentially an asset database that is shared and maintained simultaneously across a network of multiple sites, geographies, or institutions. Distributed ledger technology is based on proven cryptography and blockchain constructs to provide integrity and authenticity of the transactions recorded within it. The security and accuracy of the assets stored in the ledger are maintained cryptographically using 'keys' and signatures to control who can do what within the shared ledger.

These high integrity features ensure that events recorded in the ledger cannot be backdated, tampered with, or removed. All participants within the network will have their own identical copy of the ledger, and any changes to the ledger are reflected in all copies in minutes, or in some cases, in seconds. This fair access ensures every authorized participant has access to their complete data set without the need to request access to other databases. As such the distributed ledger can provide a trustworthy thread of evidence that can be relied upon to provide legally sustainable assurance arguments.

5.1 Application to Automotive Cybersecurity

Distributed ledger technology enables this evidence capture to be implemented in a way that is not dependent on human document creation and can be highly automated, meaning that it can be implemented at scale and provide per-vehicle assurance as opposed to traditional methods which focus on assuring at the less granular level of each vehicle type.

The distributed ledger proposed in ResiCAV+ is intended to be implemented and maintained by the vehicle manufacturer and used to store records of operational decisions made during the implementation of the CyRes methodology. The ledger can be used by different stakeholders as illustrated in Figure 5.1. The vehicle manufacturer's design and operation decisions (e.g. adjustment of significant difference parameters) would be entered into the ledger as records that could be inspected by a regulatory body carrying out a type approval assessment or other kinds of evaluation. The distributed ledger can also contribute to the ongoing reporting requirements of UN R155, which is described in more detail in section 6.

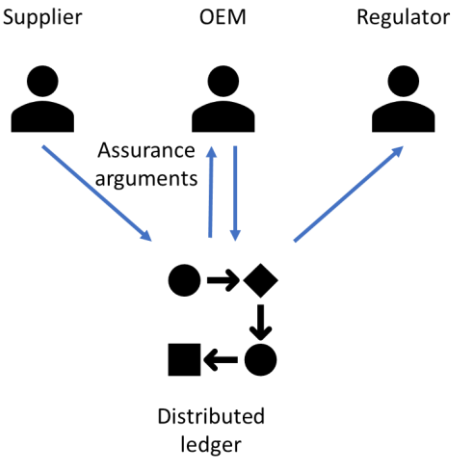


Figure 5.1 – Use of the distributed ledger to record and inspect assurance arguments

In another scenario, the vehicle manufacturer could also query the ledger to identify events such as a vehicle owner modifying their own vehicle's systems, potentially causing unsafe conditions, which may be captured in the ledger as changes to the vehicle systems. The distributed ledger can also support supply chain assurance, with possibilities for either a single distributed ledger with multiple parties able to contribute, or multiple ledgers across supply chains with interfaces to enable cross-querying between the ledgers. For example a vehicle manufacturer and its suppliers could each maintain their own ledger, with each ledger relying on entries in the other ledgers to accumulate evidence of decisions that have been made.

In the ResiCAV+ project, a specific distributed ledger implementation (see [13]) has been selected to demonstrate how this technology could be used to capture evidence based on the CyRes methodology, although other ledger implementations could also be used. The details of how the ledger is fed with information from the significant difference aspects of the methodology are described in other project deliverables [13]–[14].

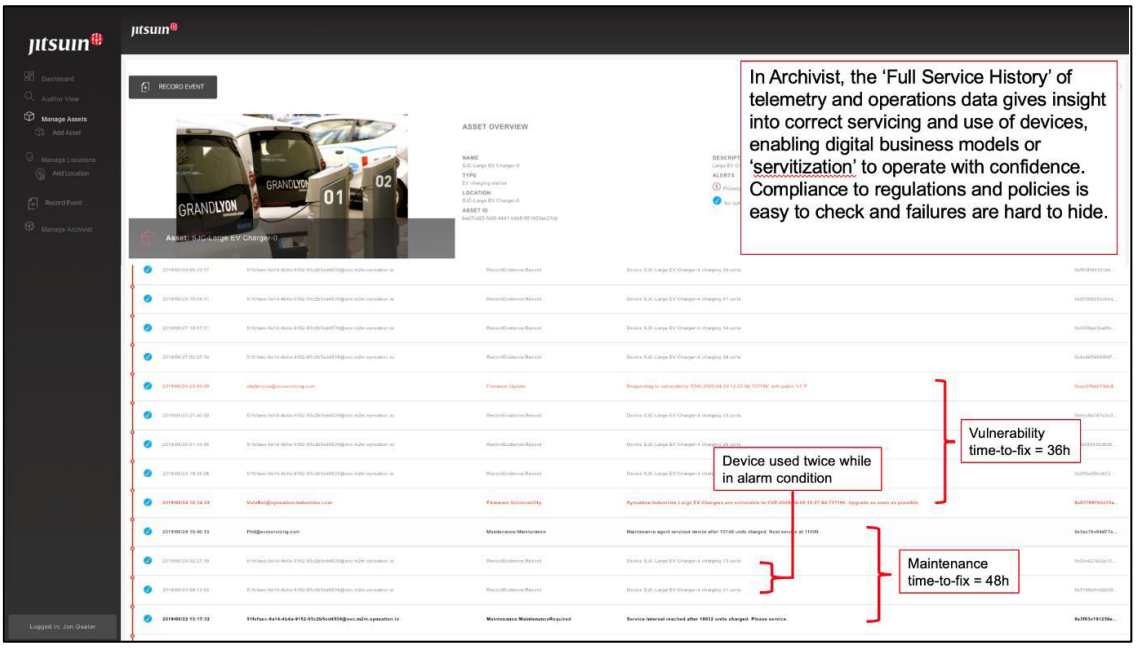


Figure 5.2 – Screenshot of RKVST distributed ledger used in ResiCAV+ demonstrator

5.2 Implementation Considerations

There are several ways in which a distributed ledger could be implemented in practice to enable combinations of the above use cases. The following practical considerations should be taken into account when specifying the solution:

5.2.1 Single or Multiple Ledgers

Should a single ledger be implemented it should store all artefacts related to a vehicle type, including each individual vehicle instance and all their parts. This single ledger would enable entries to be made by the vehicle manufacturer, their suppliers and potentially the vehicle itself when any changes to its systems, software or the environment are detected. Alternatively separate ledgers could be implemented by vehicle manufacturers and suppliers, but with the ability to interact and query entries of one ledger in another.

The most appropriate approach depends on several factors, for example, the suppliers may be supplying any or all of the following:

- parts that are unique to a single vehicle type
- variant parts that may be tuned to specific vehicle type(s) (with the implication that other variants are used in other vehicle types)

- commodity parts that are used “as is” in multiple vehicle types.

Any of these could potentially need modification to resolve a cybersecurity or other issue.

At first sight, a need to change a commodity part might be assumed to be the same for all vehicles that use it. But this is not necessarily the case. So either commodity parts are never modified (unless by the supplier) or they are allowed to spawn a variant at the vehicle manufacturer’s request. Hence the suppliers may need to maintain multiple ledgers for the “same” part.

5.2.2 **Automation**

A major strength of the distributed ledger solution is the ability to automate the recording of evidence from tools and systems that are part of the engineering and operation of a vehicle, enabling the solution to operate at scale on a per-vehicle basis. While a fully automated solution is desirable, it may not be achievable in a first implementation. Provided the ledger is implemented with the appropriate security controls, it could be proven using a small set of initial use cases with the evidence captured through manual entry.

6. Current Regulatory Requirements

Since the beginning of 2021 two new UNECE vehicle type approval regulations, R155 [15] and R156 [16], have been in force describing requirements for automotive cybersecurity and software updates, including by wireless “over-the-air” (OTA) methods, respectively. These regulations are currently being implemented in countries that are signatories to the UNECE WP.29 type approval regulations and R155, in particular, is expected to be applied to new vehicle type approvals starting from July 2022 in the EU, Japan and other regions.

Although these two regulations have clearly differing scopes, they inevitably have some significant overlaps and were therefore developed concurrently. In particular:

- the primary mechanism for the delivery and implementation of in-service mitigations for cybersecurity issues identified after launch is expected to be by software update;
- all software updates are required to be safely delivered and deployed;
- all software updates are required to be securely stored and delivered;
- all software updates are required to maintain compliance with all regulations relevant to the vehicle type approval;
- both regulations are based around the notions of through-life evolution of the vehicle system and ongoing assurance activities.

In addition, R155 requires the VM to maintain through-life monitoring of vehicles of the approved type, to identify cybersecurity events, to respond in a timely fashion to those that are deemed to require a response, and to provide regular reporting to the AA/TS regarding cybersecurity performance aspects.

The new regulations include requirements for the following activities:

- Mandatory audits by the responsible AA or designated TS of a VM’s cybersecurity management system (CSMS) and software update management system (SUMS), resulting in the issue of related certificates of conformity. These must be in place before a VM can seek type approval for a new vehicle.
- An assessment against the cybersecurity and software update requirements for new vehicle types. These assessments are expected to consist of the responsible AA verifying that a new vehicle has been appropriately engineered, with relevant risks identified, analysed and mitigated.

- Assessment of conformity control methods at least once every three years, to ensure compliance of the CoP production procedures with E/ECE/TRANS/505/Rev.3 [2]. The associated documentation must be retained for up to 10 years from when production is definitively discontinued. Type approval will be withdrawn if compliance with the regulations is not maintained.

In the context of cybersecurity and software updates, the Vehicle Type comprises a group of vehicles produced by a VM that do not differ in at least the following essential respects:

(a) the manufacturer's designation of the vehicle type [15]–[16];

(b) essential aspects of the electric/electronic architecture and external interfaces with respect to cyber security [15];

(c) essential aspects of the design of the vehicle type with respect to software update processes [16].

It should be noted that the VM's designation of the vehicle type will also reflect compliance with a much wider set of requirements that includes those of regulations that relate to the specific features of the particular vehicle type to as well as those of regulations that are mandated for all vehicles of the relevant vehicle category.

From a cyber resilience perspective, there is a risk that regulations can become part of the threat landscape, by imposing publicly available requirements that can be exploited by an attacker. For example, over-reliance on addressing only a specific set of threats (such as those in Annex V of UN R155) can mean that new threats or variants of the defined threats are not considered, and it is these that attackers will seek to realise.

6.1 UN Regulation 155 – Cybersecurity

Recognition of the potential for cybersecurity issues in vehicles that are becoming increasingly connected and automated has resulted in the development of a specific regulation for this aspect of vehicle performance. This regulation specifies requirements relating to cybersecurity on the VM and the AA or designated TS in a number of areas, including:

- Cyber Security Management System (CSMS) and associated processes
- Vehicle design and modification

- Reporting on cybersecurity monitoring and performance
- Modification and extension of the vehicle type
- Conformity of production

In addition, as part of the CSMS, the VM is required to implement processes to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

Furthermore, the VM is required to report to the AA (or their designated TS) at least once a year, or more frequently if relevant, regarding the outcome of their monitoring activities, including relevant information on new cyber-attacks identified and any additional actions taken, to confirm that the cyber security mitigations implemented for their vehicle types remain effective.

The specific requirements of R155 are detailed in Table 1 (see section 7.1).

6.2 UN Regulation 156 – Software Update

As vehicle functionality is increasingly dependent on software it is recognised that through-life software updates, including via OTA (i.e. wireless) delivery methods, will be used to mitigate unidentified and/or emerging cybersecurity vulnerabilities, to implement correction of identified defects, and also to enable new and/or enhanced vehicle functionality. This regulation specifies requirements relating to the safety and security of software updates on the VM and the AA or their designated TS in a number of areas, including:

- Software Update Management System (SUMS) and associated processes
- Vehicle type
- Modification and extension of the vehicle type
- Conformity of production

In addition, under R156 requirements VMs may also be subject to Periodic Technical Inspection (PTI) in addition to the more common inspection purposes associated with type approval, conformity of production, market surveillance, and recalls.

The specific requirements of R156 are detailed in Table 2 (see section 7.2).

6.3 ISO/SAE 21434

More recently (in August 2021), the new international standard ISO/SAE 21434 “Road vehicles – Cybersecurity engineering” [17] was published to support the practical implementation of UN R155. This document was developed by an ISO/SAE joint working group, established in October 2016, and the first standard to be developed under a joint standards development agreement between ISO and SAE.

ISO/SAE 21434 has been developed by experts from across the automotive industry including vehicle manufacturers, the tiered supply chain, cybersecurity consultants and government organisations. It is expected to be used by the automotive industry as the state-of-the-art for cybersecurity engineering, providing guidance on developing a CSMS and carrying out the cybersecurity activities needed to support compliance with UN R155.

However, it is recognised that the industry is at an early stage of maturity with respect to engineering for cyber resilience and that as experience and maturity increases, further best practice will be established and standards such as ISO/SAE 21434 will be further developed and supplemented with additional standards.

7. Applicability to Current Regulatory Requirements

In this section we consider how the proposed methodology can support compliance with the current regulatory requirements related to cybersecurity for vehicles.

7.1 Applicability for Demonstrating Compliance with UN R155

A mapping of how the CyRes methodology and DDL relate to the requirements of UNECE R155 is shown in Table 1 below.

Table 1 – UN R155 requirements mapped to the CyRes principles and DDL

Responsible Party	Requirement	R155 ref.	DDL/CyRes Applicability
Cyber Security Management System Requirements			
AA/TS shall	Verify VM has a CSMS in place.	7.2.1	DDL contributes to CSMS implementation
	Verify CSMS compliance with R155 requirements.	7.2.1	
VM shall	Ensure processes apply to the Development, Production and Post-production.	7.2.2.1	DDL is an evolving entity
	Ensure that security is adequately considered.	7.2.2.2	
	Ensure processes manage cybersecurity adequately.	7.2.2.2a	
	Ensure processes identify risks to vehicle types adequately.	7.2.2.2b	
	Take account of Annex 5, Part A, and other relevant threats.	7.2.2.2b	DDL provides evidence repository
	Ensure processes to assess, categorize and treat the risks identified adequately.	7.2.2.2c	
	Verify that the risks identified are appropriately managed.	7.2.2.2d	DDL provides evidence repository
	Ensure adequate testing of the cyber security of a vehicle type.	7.2.2.2e	
	Ensure that the risk assessment is kept current.	7.2.2.2f	DDL is an evolving entity
	Ensure processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.	7.2.2.2g	DDL provides evidence repository

Responsible Party	Requirement	R155 ref.	DDL/CyRes Applicability
	Ensure processes provide relevant data to support analysis of attempted or successful cyber-attacks.	7.2.2.2h	DDL provides evidence repository CyRes aims to improve detection and analysis
	Ensure processes mitigate cyber threats and vulnerabilities which require a response within a reasonable timeframe.	7.2.2.3	DDL provides evidence repository CyRes aims to improve detection and analysis
	Ensure processes continually monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types.	7.2.2.4	DDL provides evidence repository CyRes aims to improve detection and analysis
	Ensure processes monitor vehicles from first registration.	7.2.2.4a	DDL provides evidence repository
	Ensure processes analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs.	7.2.2.4b	CyRes aims to improve detection and analysis
	Ensure processes respect the privacy of owners and drivers.	7.2.2.4b	Access to DDL data can be controlled
	Ensure processes manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.	7.2.2.5	The entire supply chain can contribute to the DDL
Vehicle Design and Modification Requirements			
VM shall	Have a valid Certificate of Compliance for the CSMS relevant to the vehicle type.	7.3.1	
	Identify and manage supplier-related risks.	7.3.2	Entire supply chain can contribute to the DDL
	Identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type.	7.3.3	DDL provides evidence repository
	Treat/manage the identified risks appropriately.	7.3.3	DDL provides evidence repository
	Consider interactions with any external systems.	7.3.3	Entire supply chain can contribute to the DDL
	Consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.	7.3.3	DDL provides evidence repository
	Ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible, and	7.3.4	DDL provides evidence repository

Responsible Party	Requirement	R155 ref.	DDL/CyRes Applicability
	provide assessment of the technical feasibility to the AA.		
	Put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.	7.3.5	DDL provides evidence repository
	Perform appropriate and sufficient testing to verify the effectiveness of the security measures implemented.	7.3.6	DDL provides evidence repository
	Detect and prevent cyber-attacks against vehicles of the vehicle type.	7.3.7a	CyRes aims to improve detection and limit impact
	Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type.	7.3.7b	CyRes aims to improve detection and analysis
	Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.	7.3.7c	DDL provides evidence repository CyRes aims to improve detection and analysis
	Justify the use of cryptographic modules that are not in line with consensus standards.	7.3.8	DDL provides evidence repository
R155 Reporting Requirements			
VM shall	Report on the outcome of the cybersecurity monitoring, including relevant information on new cyber attacks.	7.4.1	DDL provides evidence repository
	Report on the effectiveness of the cyber security mitigations implemented for their vehicle types and any additional actions taken.	7.4.1	DDL provides evidence repository
AA/ITS shall	Verify the information provided.	7.4.2	
	Require the VM to remedy any detected ineffectiveness.	7.4.2	
	Withdraw the CSMS Compliance Certificate if the reporting or response is not sufficient.	7.4.2	
Requirements for Modification and Extension of the Vehicle Type			
VM shall	Notify the AA of every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in R155.	8.1	

Responsible Party	Requirement	R155 ref.	DDL/CyRes Applicability
AA shall	Either accept compliance or request a further test report relating to the modifications from the TS.	8.1.1,8.1.2	
	Communicate confirmation or refusal, specifying the alterations, to the VM.	8.1.3	
Conformity of Production Requirements			
VM shall	Ensure compliance of the CoP production procedures with E/ECE/TRANS/505/Rev.3 [8].	9.1	DDL provides evidence repository
	Record the results of CoP tests.	9.1.1	DDL provides evidence repository DDL is an evolving entity
	Retain the documentation for up to 10 years from when production is definitively discontinued.	9.1.1	DDL provides evidence repository
AA shall	Verify conformity control methods at least once every three years.	9.1.2	DDL provides evidence repository
	Withdraw type approval if R155 is not complied with.	10.1	

7.2 Applicability for Demonstrating Compliance with UN R156

A mapping of how the CyRes methodology and DDL relate to the requirements of UNECE R156 is shown in Table 2 below.

Table 2 – UN R156 requirements mapped to the CyRes principles and DDL

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
Software Updates Management System Requirements			
AA/TS shall	Verify SUMS compliance with R156 requirements.	6.4	
	Verify VM has a SUMS in place.	6.5	DDL contributes to SUMS implementation
VM shall	Ensure information relevant to this Regulation is documented and securely held at the vehicle manufacturer and can	7.1.1.1	DDL provides evidence repository

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
	be made available to an AA or its TS upon request.		
	Ensure information regarding all initial and updated software versions, including integrity validation data, and relevant hardware components of a type approved system can be uniquely identified.	7.1.1.2	DDL provides evidence repository
	For a vehicle type that has an RXSWIN, ensure information regarding the RXSWIN of the vehicle type before and after an update can be accessed and updated.	7.1.1.3	DDL is an evolving entity
	For a vehicle type that has an RXSWIN, ensure the ability to update information regarding the software versions and their integrity validation data of all relevant software for each RXSWIN.	7.1.1.3	Entire supply chain can contribute to the DDL
	For a vehicle type that has an RXSWIN, the vehicle manufacturer can verify that the software version(s) present on a component of a type approved system are consistent with those defined by the relevant RXSWIN.	7.1.1.4	DDL provides evidence repository
	Ensure any interdependencies of the updated system with other systems can be identified.	7.1.1.5	Entire supply chain can contribute to the DDL
	Ensure the vehicle manufacturer is able to identify target vehicles for a software update.	7.1.1.6	
	Confirm the compatibility of a software update with the target vehicle(s) configuration before it is issued. This shall include an assessment of the last known software/hardware configuration of the target vehicle(s) for compatibility with the update before it is issued.	7.1.1.7	DDL provides evidence repository
	Assess, identify and record whether a software update will affect any type approved systems. This shall consider whether the update will impact or alter any of the parameters used to define the systems the update may affect or whether it may change any of the parameters used to type approve those system (as defined in the relevant legislation);	7.1.1.8	DDL provides evidence repository
	Assess, identify and record whether a software update will add, alter or enable	7.1.1.9	DDL provides evidence repository

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
	any functions that were not present, or enabled, when the vehicle was type approved or alter or disable any other parameters or functions that are defined within legislation. The assessment shall include consideration of whether: (a) Entries in the information package will need to be modified; (b) Test results no longer cover the vehicle after modification; (c) Any modification to functions on the vehicle will affect the vehicle's type approval.		
	Assess, identify and record if a software update will affect any other system required for the safe and continued operation of the vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered;	7.1.1.10	DDL provides evidence repository
	Ensure that the vehicle user is able to be informed about updates.	7.1.1.11	
	Make the information according to paragraph 7.1.2.3. and 7.1.2.4. available to responsible AA or TS. This may be for the purpose of type approval, conformity of production, market surveillance, recalls and Periodic Technical Inspection (PTI).	7.1.1.12	DDL provides evidence repository Access to DDL data can be controlled
	Record and store documentation describing the processes used by the vehicle manufacturer for software updates and any relevant standards used to demonstrate their compliance.	7.1.2.1	DDL provides evidence repository
	Record and store documentation describing the configuration of any relevant type approved systems before and after an update, this shall include unique identification for the type approved system's hardware and software (including software versions) and any relevant vehicle or system parameters;	7.1.2.2	DDL provides evidence repository
	For every RXSWIN, there shall be an auditable register describing all the software relevant to the RXSWIN of the vehicle type before and after an update. validation data for all relevant software for each RXSWIN.	7.1.2.3	DDL provides evidence repository

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
	The RXSWIN register shall include information of the software versions and their integrity.	7.1.2.3	DDL provides evidence repository
	Record and store documentation listing target vehicles for the update and confirmation of the compatibility of the last known configuration of those vehicles with the update.	7.1.2.4	DDL provides evidence repository
	Record and store documentation for all software updates for that vehicle type describing: (a) The purpose of the update; (b) What systems or functions of the vehicle the update may affect; (c) Which of these are type approved (if any); (d) If applicable, whether the software update affects the fulfilment of any of the relevant requirements of those type approved system; (e) Whether the software update affects any system type approval parameter; (f) Whether an approval for the update was sought from an approval body; (g) How the update may be executed and under what conditions; (h) Confirmation that the software update will be conducted safely and securely; (i) Confirmation that the software update has undergone and successfully passed verification and validation procedures.	7.1.2.5	DDL provides evidence repository
	Demonstrate the process they will use to ensure that software updates will be protected to reasonably prevent manipulation before the update process is initiated.	7.1.3.1	DDL provides evidence repository
	Use update processes that are protected to reasonably prevent them being compromised, including development of the update delivery system.	7.1.3.2	
	Ensure that processes used to verify and validate software functionality and code for the software used in the vehicle are appropriate.	7.1.3.3	DDL provides evidence repository
	Ensure that processes and procedures they will use to assess that over the air	7.1.4.1	DDL provides evidence repository

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
	updates will not impact safety, if conducted during driving.		
	Ensure that processes and procedures they will use to ensure that, when an over the air update requires a specific skilled or complex action, for example recalibrate a sensor post-programming, in order to complete the update process, the update can only proceed when a person skilled to do that action is present or is in control of the process.	7.1.4.2	DDL provides evidence repository
Vehicle Type Requirements			
VM shall	Ensure that the authenticity and integrity of software updates shall be protected to reasonably prevent their compromise and reasonably prevent invalid updates.	7.2.1.1	
	Ensure that each RXSWIN shall be uniquely identifiable.	7.2.1.2.1	DDL provides evidence repository
	When type approval relevant software is modified by the vehicle manufacturer, the RXSWIN shall be updated if it leads to a type approval extension or to a new type approval	7.2.1.2.1	
	Each RXSWIN shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).	7.2.1.2.2	
	If RXSWINs are not held on the vehicle, the manufacturer shall declare the software version(s) of the vehicle or single ECUs with the connection to the relevant type approvals to the AA. This declaration shall be updated each time the declared software version(s) is updated. In this case, the software version(s) shall be easily readable in a standardized way via the use of an electronic communication interface, at least by the standard interface (OBD port).	7.2.1.2.2	
	Protect the RXSWINs and/or software version(s) on a vehicle against unauthorised modification. At the time of Type Approval, the means implemented to protect against unauthorized modification of the RXSWIN and/or software version(s) chosen by the	7.2.1.2.3	

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
	vehicle manufacturer shall be confidentially provided.		
	Ensure that the vehicle is able to restore systems to their previous version in case of a failed or interrupted update or that the vehicle can be placed into a safe state after a failed or interrupted update.	7.2.2.1.1	
	Ensure that software updates can only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).	7.2.2.1.2	DDL provides evidence repository
	When the execution of an update may affect the safety of the vehicle, the vehicle manufacturer shall demonstrate how the update will be executed safely. This shall be achieved through technical means that ensures the vehicle is in a state where the update can be executed safely.	7.2.2.1.3	DDL provides evidence repository
	Demonstrate that the vehicle user is able to be informed about an update before the update is executed. The information made available shall contain: (a) The purpose of the update. This could include the criticality of the update and if the update is for recall, safety and/or security purposes; (b) Any changes implemented by the update on vehicle functions; (c) The expected time to complete execution of the update; (d) Any vehicle functionalities which may not be available during the execution of the update; (e) Any instructions that may help the vehicle user safely execute the update; In case of groups of updates with a similar content one information may cover a group.	7.2.2.2	DDL provides evidence repository
	In the situation where the execution of an update whilst driving may not be safe, the VM shall demonstrate how they will: (a) Ensure the vehicle cannot be driven during the execution of the update; (b) Ensure that the driver is not able to use any functionality of the vehicle that	7.2.2.3	DDL provides evidence repository

Responsible Party	Requirement	R156 ref.	DDL/CyRes Applicability
	would affect the safety of the vehicle or the successful execution of the update.		
	After the execution of an update the VM shall demonstrate how the following will be implemented: (a) The vehicle user is able to be informed of the success (or failure) of the update; (b) The vehicle user is able to be informed about the changes implemented and any related updates to the user manual (if applicable).	7.2.2.4	DDL provides evidence repository
	The vehicle shall ensure that preconditions have to be met before the software update is executed.	7.2.2.5	
Requirements for Modification and Extension of the Vehicle Type			
VM shall	Notify the AA of every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in R156.	8.1	DDL is an evolving entity
AA shall	Either accept compliance or request a further test report relating to the modifications from the TS.	8.1.1,8.1.2	
	Communicate confirmation or refusal, specifying the alterations, to the VM.	8.1.3	
Conformity of Production Requirements			
VM shall	Ensure compliance of the CoP production procedures with E/ECE/TRANS/505/Rev.3 [8].	9.1	DDL provides evidence repository
	Record the results of CoP tests.	9.1.1	DDL provides evidence repository DDL is an evolving entity
	Retain the documentation for up to 10 years from when production is definitively discontinued.	9.1.1	DDL provides evidence repository
AA/TS shall	Periodically validate that the processes used and decisions made by the vehicle manufacturer are compliant, particularly for instances where the vehicle manufacturer chose not to notify the AA or its TS about an update. This may be achieved on a sampling basis.	9.1.3	DDL provides evidence repository
AA shall	Verify conformity control methods at least once every three years.	9.1.2	DDL provides evidence repository
	Withdraw type approval if R156 is not complied with.	10.1	

8. Operational Assurance and Future Regulation

Current regulatory regimes focus on certification prior to vehicle launch, but provide a limited element of ongoing assurance over the vehicle lifetime, where ensuring CoP is currently the primary ongoing activity. The recent regulations concerning cybersecurity [15] and software updates [16] depart from the traditional approach in that they identify the need for post-launch re-evaluations to ensure continuing compliance after software updates, as well as for in-service monitoring for the detection of potential cybersecurity events.

The ResiCAV project identified [1] the need to move to more continuous and dynamic forms of regulation based on "operational assurance" in order to assure the cyber resilience of future vehicles, recommending that:

> "research into methods and frameworks needed to provide continuous assurance throughout the lifecycle of vehicles and the mobility ecosystem, as well as new models of regulation that can be applied beyond the start of production and allow for more dynamic forms of type approval."

Encoding the outputs of the CyRes methodology in an extendable but unmodifiable DDL, enables automated recording of legally-defensible, per-vehicle, real-time assurance artefacts.

Nonetheless, the regulations as currently written remain in terms of achieving approval at a vehicle type, rather than individual vehicle, level. In addition, there may be potential for conflict between existing notions of CoP for the vehicle type and the implementation of significant engineered difference between vehicles that is proposed in the CyRes methodology. Thus, considerable care would be needed to ensure (and document) that the "engineered significant differences" do not impact on the specific performance characteristics that are subject to type approval regulations, as failure to do so would result in the withdrawal of type approval.

The DDL approach would provide a framework for documenting and recording evidence that the type characteristics are maintained through and/or despite software updates. However, further development of the regulations may be required to permit the use of an "individualised" type approval process for vehicles that are actually produced in large volumes.

A concern regarding the notion of a per-vehicle assurance approach is that it may become increasingly difficult, and perhaps ultimately unmanageable and unaffordable, to ensure that compliance with all relevant performance characteristics is maintained when each vehicle diverges from every other member of its type.

In order to explore the relevance of the proposed methodology to both current and future methods of regulatory compliance, two workshops were held in November 2021 and January 2022 between the ResiCAV+ project team and stakeholders from UK Government departments, including:

- Vehicle Certification Agency (VCA)
- Driver and Vehicle Standards Agency (DVSA)
- Centre for Connected and Autonomous Vehicles (CCAV)
- National Cybersecurity Centre (NCSC)

During these workshops the key principles of CyRes were reviewed and the following themes explored through group discussion. The outcomes of the two workshops are summarised as follows, with additional details in the Appendix.

1. Although the current UN R155 requires annual reporting by vehicle manufacturers of their monitoring activities, more dynamic forms of regulation are also desirable. The difficulties of realising this through existing mechanisms such as the MoT were noted.
2. The security assurance aspects of the new DfT CAVPASS scheme for assuring the safety and security of automated vehicles are at an early stage of development and the proposed methodology is expected to be of interest to this scheme.
3. The use of the dynamic distributed ledger to store and retrieve assurance artefacts was generally seen as helpful. The real-time, per-vehicle aspects were also seen as important and these would need to be automated in order to be able to apply them at scale. Additional uses of the ledger, for example to store safety-related failures, were also recognised.
4. Potential barriers to implementation of the proposed methodology include:
    a. Cost – the need to share the cost of implementation and operation of the solution.
    b. Consistency – the ability to capture decisions and their rationales in the distributed ledger.
    c. Competence – there is limited ability to upskill the automotive industry at the scale required when limited by manual processes, so the use of automation is critical.
5. The use of the ALARP principle is an established part of health and safety at work legislation, which may be invoked in the event of a cybersecurity incident which results in physical harm.

However ALARP is problematic when applied to security risk assessment due to the difficulty of accurately determining and comparing risks and cost of mitigation.

6. It was noted that responsibility for the decisions made by automated tools would include not only responsibility for the functional behaviour of automated driving systems, but also for decision-making as part of an automated system to mitigate cyber attacks.

9. Conclusion and Recommendations

This “Compliance Report” has considered the applicability of the CyRes approach, together with the use of a Dynamic Distributed Ledger (DDL) as a supporting framework, in:

- achieving cybersecurity resilience in the automotive domain,
- demonstrating due diligence on the part of the vehicle manufacturer in the legal domain.

The following conclusions can be drawn:

1. Current legislation is based around the concept of “type approval”, which involves demonstrating compliance of the vehicle type with relevant regulations (currently numbering 163 and rising) that relate to various aspects of vehicle system or component performance, ranging from generic for the underlying vehicle category as well as specific to the features of the particular vehicle type. The traditional approach for vehicles is based around a one-off certification activity prior to vehicle launch and generally provides only limited assurance activity over the vehicle lifetime, where ensuring “conformity of production” (CoP) is currently the primary ongoing assurance activity.

   Ensuring CoP is a core requirement for the type approval of vehicles, as well as vehicle systems, components or STUs, aiming to ensure that the entire production run maintains the same performance criteria. Consequently, there may be potential for conflict between current CoP requirements and the vehicle differentiation that is envisaged in the CyRes methodology. A similar concern arises in relation to the assurance of vehicles that make use of artificial intelligence technologies that exploit unsupervised learning for automating driving tasks.

   Thus, considerable care would be needed to ensure (and document) that the “engineered significant differences” do not impact on the specific performance characteristics of the vehicle that are subject to type approval regulations, as failure to do so would result in the withdrawal of type approval.

2. Although UN R155 and UN R156 inherently reflect a need for post-launch re-evaluations to ensure continuing compliance after software updates, as well as through-life monitoring for the detection of potential cybersecurity events, these regulations are still written in terms of achieving approval at vehicle type, rather than individual vehicle, level. Compliance at the level of individual vehicles is seen as desirable and the proposed methodology provides a route to such assurance,

while reducing the risk of prescriptive regulatory requirements becoming part of the threat landscape. However, one concern with a per-vehicle assurance approach is that:

It may become increasingly difficult, and perhaps ultimately unmanageable and unaffordable, to ensure that compliance with all relevant performance characteristics is maintained when each vehicle diverges from every other member of its type.

3. Software changes may result in unexpected impacts on the performance characteristics of the related vehicle systems and functions. However, it should be noted that software changes could also have impacts on other vehicle performance characteristics that may appear unrelated at first sight and are difficult to predict, such as EMC. For example, modifying control strategies could change the electromagnetic emissions characteristics of the associated electronic components, and changing signal processing techniques may potentially result in increased susceptibility to electromagnetic interference for the related monitoring system.

4. Software changes are not the only mechanism by which a system can be changed; it is also critical to consider changes to the environment that may be caused intentionally by an intelligent adversary. Often such changes will be deliberately crafted to occur outside the model assumed during the development of a system, especially if that model is known to the adversary.

The proposed methodology enables such changes to the environment to be detected and for per-vehicle decisions to be made, documented and queried at scale.

A large class of (often relatively easy to mount) attacks involve remotely manipulating the sensory input to vehicle environment monitoring systems, such as by denying, corrupting or falsifying these inputs (e.g. GNSS, radar, optical etc.). As such attacks require no access to on-board systems, software or data it is difficult to see how differences between vehicles that do not impact on specified performance criteria can provide resilience against these types of threat. The impact of such attacks is more likely to be revealed through anomalies in road traffic behaviour than by in-vehicle anomaly detection schemes.

The CyRes techniques that are to be used for increasing the probability of detection and understanding of cyber events will also need to include methods for the identification of possible confounding data sources.

For example, unintentional electromagnetic interference could also lead to events or anomalies that might otherwise be mistaken for cyber events. Failure to successfully identify such confounding sources could result in considerable effort being wasted in trying to understand, assess and mitigate effects that do not actually originate from malicious cybersecurity threat agents.

5. The ALARP principle originates from safety engineering where the operational environment is well defined and the systems have hitherto been relatively stable. The cybersecurity environment, however, is radically different, driven by human ingenuity exploiting technological changes. Furthermore, the perceived future of vehicles is one of evolving systems enabled by through-life software updates.

   The ALARP principle requires demonstrable selection of the most effective mitigation or combination of mitigations, unless the resulting cost is grossly disproportionate to the associated risk. Consequently, the ResiCAV+ Legal Report [18] cautions that if other viable alternatives are identified that are more cost effective, then the CyRes methodology should not be used.

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

   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.

   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. 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.

7. 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. The stakeholder workshops conducted as part of the ResiCAV+ project highlighted that more dynamic and continuous forms of assurance and associated regulatory mechanisms would be desirable.

   Furthermore, such dynamic forms of regulation would only be feasible if supported by appropriate tools that could operate at the scale and with the necessary automation.

8. 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 UN R156.

10. References

[1] ResiCAV Deliverable 1, “Requirements and timescales for CYB-R: the UK Centre of Excellence for Road Transport Cybersecurity Resilience”, HORIBA MIRA, 30th March 2020.

[2] ResiCAV Deliverable 2, “Economic and technological feasibility of the CyRes Methodology”, Thales, 30th March 2020.

[3] 2007/46/EC, “Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive)”, Official Journal of the European Union, No. L 263, 9th October 2007, pp. 1–160.

[4] 2017/2400/EU, “Commission Regulation (EU) 2017/2400 of 12 December 2017 implementing Regulation (EC) No 595/2009 of the European Parliament and of the Council as regards the determination of the CO2 emissions and fuel consumption of heavy-duty vehicles and amending Directive 2007/46/EC of the European Parliament and of the Council and Commission Regulation (EU) No 582/2011”, Official Journal of the European Union, No. L 349, 29th December 2017, pp. 1–246.

[5] 2013/168/EU, “Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles”, Official Journal of the European Union, No. L 60, 2nd March 2013, pp. 52–128.

[6] 2013/167/EU, “Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles”, Official Journal of the European Union, No. L 60, 2nd March 2013, pp. 1–41.

[7] UN ECE/TRANS/WP.29/78/Rev.3, “Consolidated Resolution on the Construction of Vehicles (R.E.3)”, Economic Commission for Europe (ECE), Inland Transport Committee, World Forum for Harmonization of Vehicle Regulations, United Nations Economic and Social Council (UNECE), 23rd January 2014.

[8] UN E/ECE/TRANS/505/Rev.3, “Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations”, Rev. 3, 20th October 2017.

[9] ISO 9001:2015, “Quality management systems — Requirements”, September 2015.

[10] ISO 26262:2018, “Road vehicles – Functional safety”, Ed. 2, 2018.

[11] ISO/PAS 21448:2019, “Road vehicles – Safety of the intended functionality”, 2019.

[12] A. Francillon, B. Danev and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars”, Proc. 18th Annual Network and Distributed System Security Symp. (NDSS Symposium 2011), San Diego, CA, USA, Feb. 2011

[13] ResiCAV+ Deliverable D2, “Proof of Concept Demonstrator of Prototype Tool Suite”, Thales, March 2022.

[14] ResiCAV+ Deliverable D1, “Prototype Tool Suite”, Thales, March 2022.

[15] UN Regulation 155, “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”, 22nd January 2021.

[16] UN Regulation 156, “Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system”, 22nd January 2021.

[17] ISO/SAE 21434, “Road vehicles – Cybersecurity engineering”, August 2021.

[18] ResiCAV+ Deliverable D3, “Legal Report”, Burges Salmon, 11th January 2022.

Appendix – Compliance Workshop Outcomes

Workshop 1 – November 2021

This first workshop introduced the ResiCAV+ project, the significant difference element of the CyRes methodology and the topic of dynamic per-vehicle assurance offered by the DDL. The workshop discussion was structured around the following questions:

1. **What are the perceived limitations of current static pre-SOP regulatory model?**
2. **Are more dynamic models of regulation considered desirable?**
    - It was noted that although UN R155 provides requirements for vehicle type approval prior to production, it does also contain provision for ongoing assurance in that vehicle manufacturers have to report at least annually to their type approval authority about their monitoring activities, including attacks they have detected and whether the mitigations are still effective.
    - It was recognised that the pace of technological change is a potential problem, in that regulations cannot keep up with technology or changes in the threat landscape.
    - Any future dynamic assurance model should consider continuous methods of approval as well as periodic inspections (e.g. MOT) if possible. However, the practical challenges of implementing cybersecurity related MOT checks at the scale needed should not be underestimated.
    - A question was also raised about what should happen to vehicles still on the road after their end of life. For example, should it still be possible to pass an MOT if they are no longer supported from a cyber resilience perspective?
3. **How does the proposed approach fit with CAVPASS?**
    - CAVPASS is a new safety and security assurance process for connected and automated vehicles, with the security aspects starting to be addressed now.
    - CAVPASS targets all connected and automated vehicles, including ALKS equipped vehicles.
    - The security assurance aspects of CAVPASS are at an early stage of development, however the proposed methodology is expected to be of interest to the further development of the CAVPASS scheme.

4. **Is fine grained per-vehicle assurance desirable?**

    - It was noted that a form of per-vehicle assurance would be of interest, for example through the MOT, but it is not clear how this would work in practice and should not be the only means of providing this assurance.

5. **Is the "irrefutable" nature of the assurance artefacts stored by the distributed ledger desirable?**

    - In general this was considered desirable and could also be useful for storing safety-related failures, not just cybersecurity issues.
    - The approach was seen to be similar to aircraft "black boxes" but the data could be streamed in real-time rather than examined after the event.
    - It was highlighted that it would be important to be able to justify decisions on a per-vehicle basis and that decisions made by a system at this scale would need to be automated.
    - The question was raised as to whether the proposed distributed ledger would be based on single or multi-layer technology? The implementation in the current ResiCAV+ demonstrator is based on a single layer ledger but it could in principle also be implemented as multi-layer.

6. **What would be the barriers to implementing such an approach?**

    - Several barriers were identified by the group:
    - ***Cost*****:** Which party or parties would bear the cost of getting the data from the vehicle, given the cost of providing continuous connectivity to and from vehicles?
        - It was recognised that this cost should be shared between the manufacturers of vehicles and off-board systems in order for implementation to be realistic.
    - ***Consistency*****:** How could the generation of the real-time, per-vehicle assurance artefacts be done in a consistent way to benefit all but still achieve close to real-time performance?
        - The prototype tools include a set of "sliders" that can be used to adjust the parameters affecting significant different, for example Stability and Diversity, and record the reasons for such adjustments within the distributed ledger.
        - It is also possible to choose to apply system changes or updates to a limited number of vehicles rather than to the whole fleet.

- ***Competence*:** Knowledge and understanding are required to consistently interpret the artefacts stored in the ledger. This would apply not only in a court setting but also among different manufacturers and regulatory compliance processes.
  - It is becoming clear that we cannot upskill the automotive industry with the necessary cyber resilience competences at the scale needed.
  - Scarce cybersecurity competence needs to be focussed on ensuring tangible outcomes that lead to increased assurance.
  - This highlights the need to develop appropriate tooling and automation, although some level of upskilling will still be needed, including competence in operating/understanding the proposed methodology.

Workshop 2 – January 2022

The second workshop focussed on the role of the ALARP principle in security risk management and the use and defence of automated decision making tools to construct legally sustainable assurance arguments. These aspects are investigated from a legal perspective in the ResiCAV+ Legal Report [18] and are also considered here from a regulatory compliance perspective.

1. ALARP

The ALARP principle that residual risk shall be reduced 'as low as reasonably practicable' is often used in health and safety risk management. ALARP involves assessing the risk associated with an undesirable event against the cost of its mitigation. Such an assessment usually takes the form of a cost-benefit analysis and the ALARP principle implies that all possible mitigations are to be considered other than those that are grossly disproportionate.

ALARP has not seen common usage for security risk management to date, but the question explored is whether the principle has a role when assessing the impact of cyber-attacks on safety? The following areas were explored during the workshop:

a) Is the use of ALARP feasibly at the scale required, for example 250,000 cyber incidents over 8 years and 40 million vehicles?

b) ALARP requires balancing mitigations against risks (cost-benefit analysis) but is it feasible to estimate risk for cyber-attacks with sufficient accuracy to perform such an analysis?

Probability or frequency of cyber-attacks are problematic to estimate given that their occurrence is determined by the motivations of human adversaries, and past occurrence is not a reliable indicator of future occurrence. It was suggested that the UN R155 reporting provisions may allow these estimations to be improved over time, as more data becomes available about detected threats and attacks, although relevant parts of this data would need to be shared appropriately to enable such improvements to be realised.

c) How can we judge as part of a compliance process whether all possible mitigations have been considered in this cost-benefit analysis?

Vehicle manufacturers and their suppliers would have to prepare evidence of how candidate mitigations were considered or dismissed based on their proportionality and cost-benefit versus the risks, and this would have to be assessed in each case by the regulatory body. Sufficient competence would have to exist in both manufacturers and regulators for the preparation and assessment of these arguments.

2. Automated Tools

A key aspect of the CyRes methodology is the use of automated tools to make decisions and record evidence for a decision made by the vehicle, instead of relying on design documents signed off by a responsible individual. The workshop explored how, when using such automated tools, the context-specific legal responsibility for that decision can be established.

a) What is the responsibility of the OEM for the decisions made by the automated systems they have deployed and in particular when, to whom and for what are they responsible?

It was noted during the workshop that this would include not only responsibility for the functional behaviour of automated driving systems, but also for automated decision-making as part of a cyber resilient system, in which case the automated tool would be part of a mitigation that would need to be balanced against other possible mitigations.

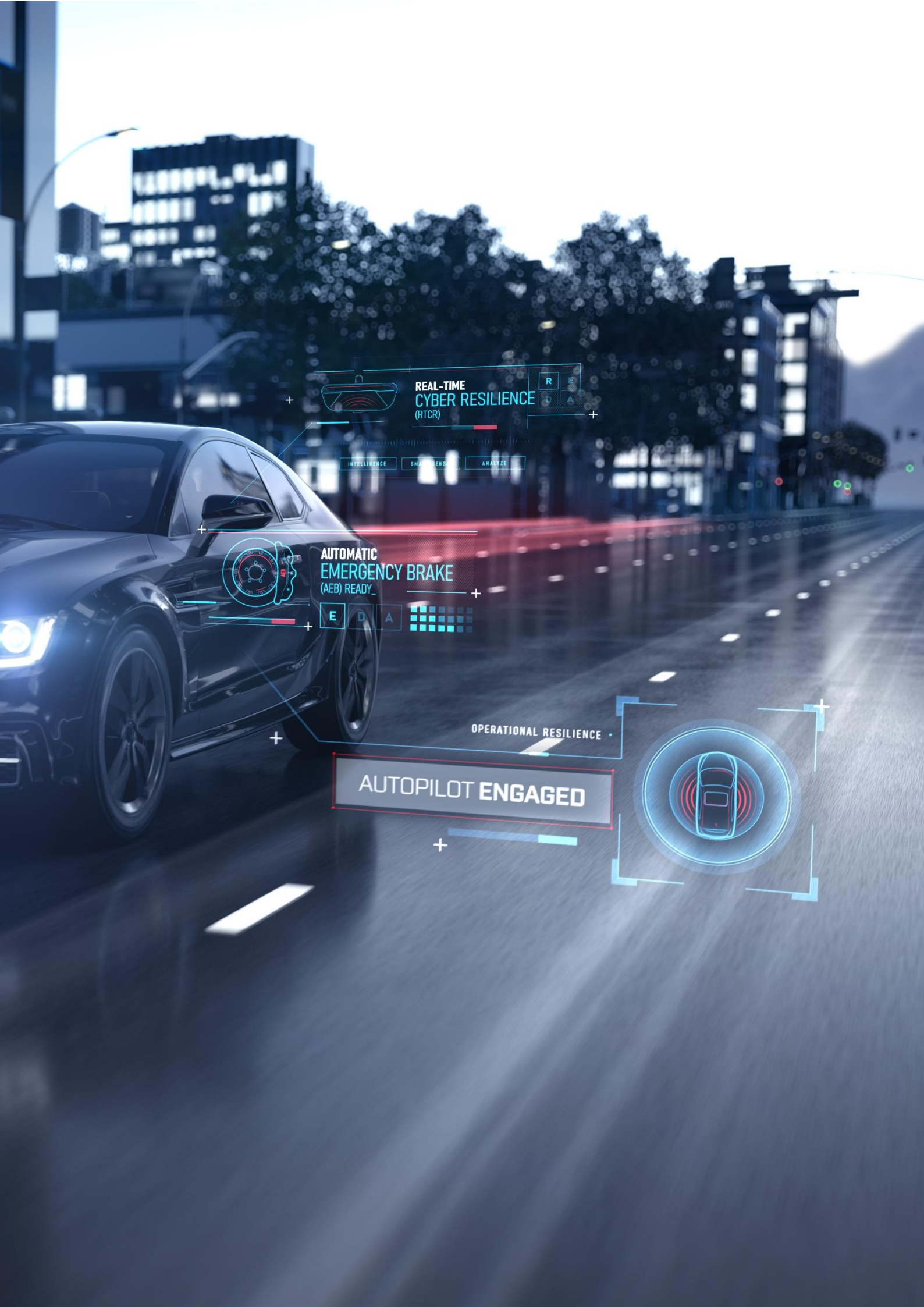
b) What would be required of a regulatory process to be able to assess the output and effectiveness of such automated tools? What would an organisation need to do to fulfil that obligation?

It was noted that without considering the context and variables of liability, system flaws and adverse unintended effects would inevitably be designed into both the regulatory and legal processes, and (as a result) the operational parts of the system.

c) If automated tools are to replace human design or operational decisions, how would such decisions be approved and signed-off?

Essentially, the necessary approval would be for the deployment of the tools and organisational sign-off processes would need to be adapted to enable this sign-off based on sufficient understanding of the automated tool, requiring appropriate competence and authority.

Produced by HORIBA MIRA Ltd.


REAL-TIME
CYBER RESILIENCE
(RTCR)
R
E
D
A
INTELLIGENCE
ANALYZE
AUTOMATIC
EMERGENCY BRAKE
(AEB) READY_
E
D
A
OPERATIONAL RESILIENCE
AUTOPILOT ENGAGED

ZENZIC

SELF-DRIVING REVOLUTION

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