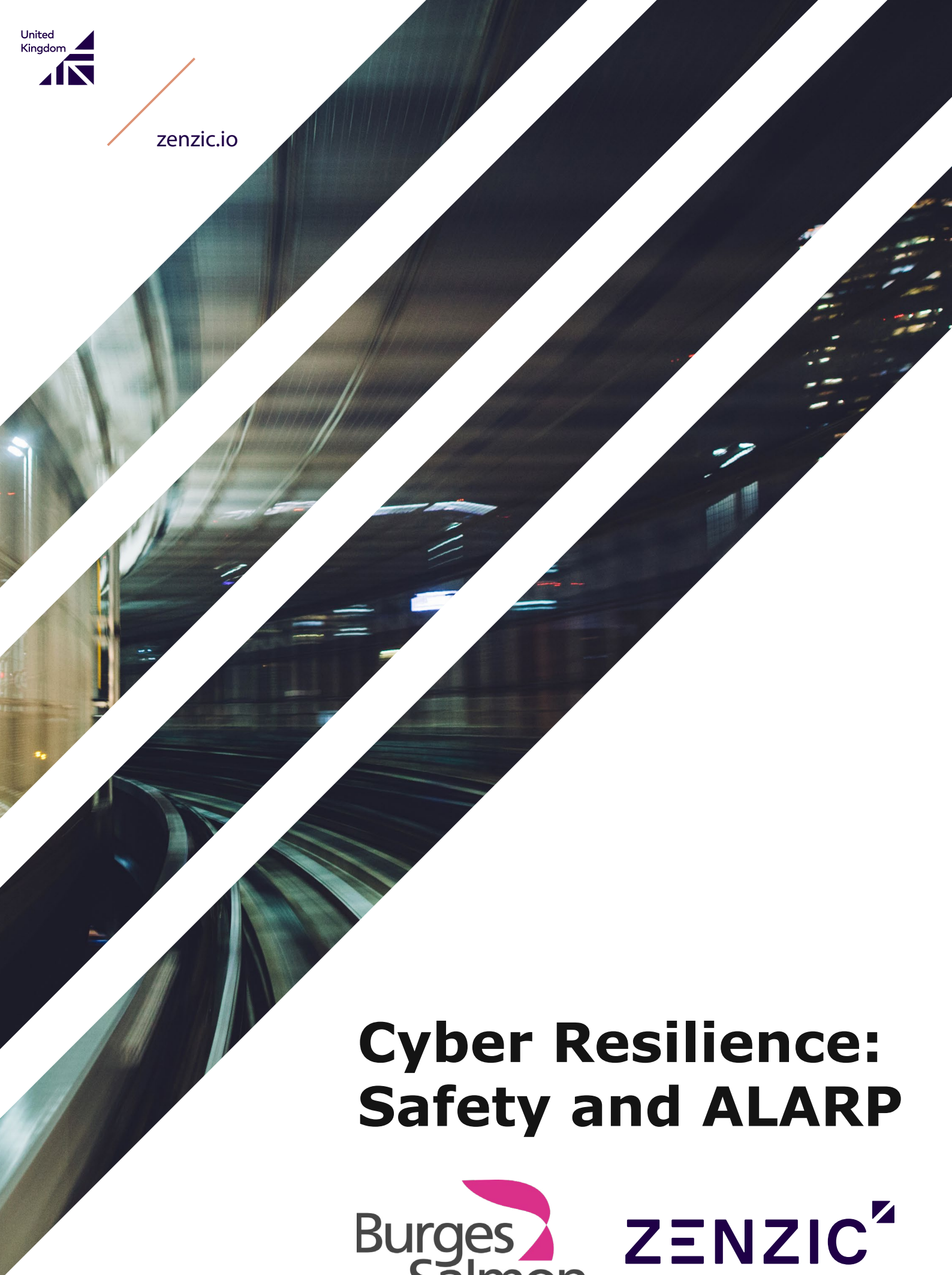
United Kingdom

zenzic.io



Cyber Resilience: Safety and ALARP

Burges Salmon

ZENZIC

SELF-DRIVING REVOLUTION

OBJECTIVE

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

This is provided in the context of the ResiCAV+ project, which is supported by Zenzic, where the project partners intend to demonstrate its CyRes methodology on a vehicle braking system.

SUMMARY

1 Braking systems are a safety-critical vehicle sub-system and functional requirement of modern vehicles. They are a core part of the vehicle type approval frameworks that currently apply to vehicles in the UK (whether EU, UNECE or GB).

2 The type approvals framework prescribes those braking systems that are deemed safe enough by design and construction for use in relevant markets. Demonstrating conformity with type approval requirements is a basic requirement of vehicle safety. Type approval requirements also set technical expectations so far as industry 'state of the art' and understanding go and therefore are relevant to whether or not products may be considered defective in the context of product liability claims.

3 Increasingly sophisticated braking systems and in particular their cyber-physical nature, are being reflected in type approval requirements (for example UNECE regulations on Electronic Stability Control, Anti-lock Braking Systems and Autonomous Emergency Braking).

4 As vehicle systems, including braking systems, develop in terms of design and the ways in which they are maintained and updated, it is clear that as well as encompassing new technology (e.g. Automated Lane Keeping Systems) there is awareness that type approval requirements must increasingly provide for cyber security in the face of cyber attacks. This is demonstrated in particular through UNECE Regulations 155 and 156 and guidance emanating from within both the EU and UK particularly in respect of in-life software updates, enduring cyber resilience and novel threat response.

5 These current and incoming requirements increasingly extend monitoring of type approval into a form of continuous market surveillance after initial placing of vehicles onto the market. Material failures in cyber resilience (particularly in safety-critical systems and sub-systems) will call into question not just design and construction requirements in the relevant vehicle approvals but also the fitness for purpose of type approval requirements.

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

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

8 The dynamic and emergent nature of cyber threats and the material risk that novel cyber attacks will be successful pose particular challenges as regards hazard identification and mitigation measures. Enduring cyber resilience may require technologies and design

methodologies and frameworks that ultimately require systems to take automated decisions in real time to respond to such threats to mitigate risk or fail safe. Notwithstanding automated decision-making, it is expected that automotive OEMs deploying such systems would remain responsible for the performance and decisions taken by their cyber security system.

9 The concept of reducing risk "As Low As Reasonably Practicable" or "ALARP" refers to a very specific legal term of art that applies to the general legal framework (the Health and Safety at Work, Etc. Act 1974 or "HSWA") governing health and safety law in the UK and has a highly technical meaning that is separate, and different to that which might otherwise be understood on a literal reading. In practice it imposes (and links to) a high threshold legal test subject to a reverse criminal law burden of proof which is in principle applicable to a very broad ambit of activity. Guidance issued by UK safety regulators on the level of obligation states that a dutyholder must prove that it has done everything practicable to reduce risk apart from any steps that are **grossly disproportionate** to take. It has not (by regulatory enforcement policy only) historically been applied to issues of road automotive design, construction and engineering. As a legal test. ALARP is also not a stated requirement of current vehicle type approvals relating to vehicle cyber security and its risk assessment.

10 However, the rapid move from a single driver or single vehicle emphasis to integrated roads systems is now attracting greater attention on system based safety issues as well as investigation and enforcement. For example a coroner has recently referred a death on a smart motorway to the CPS and the Office of Rail and Road whilst strictly not the safety regulator for roads (only rail) has been looking closely also at smart motorways on a system safety basis. It is conceivable therefore that the HSWA criminal investigation and enforcement may extend in the near future to road and vehicle system safety issues including cyber vulnerabilities. That itself would have potentially quite wide ranging (and potentially unintended) consequences for the development of new automotive technologies.

11 Notwithstanding its historic limited direct relevance to individual vehicle braking systems, the ALARP framework has some utility in illustrating how thorough the process of risk assessment, the selection and deployment of mitigation measures, the documentation of the same and the monitoring and auditing of safety risks and performance are undertaken in other industries. In particular, it would require consideration of all available mitigation measures relative to known and anticipated threats (including methodologies for automated decision making) and deployment of any or all of them so far as they are not grossly disproportionate to the risks in terms of time, money and effort. Notwithstanding that current and future type approval requirements may not mandate such an approach, it is probable that internal application of an ALARP approach would result in risk assessments and deployment of mitigation measures that would meet (or indeed exceed) type approval requirements given how stringent the ALARP approach/test is conventionally stated to be, and consequently increase the "defensibility" of engineering choices as regards cyber security.

12 Notwithstanding the position above, should ResiCAV+ partners wish to demonstrate a route to a legally defensible argument hypothetically using ALARP principles and processes, we have considered and set out in this paper the steps that the Health and Safety Executive or "HSE" (the main HSWA prosecutor) would likely take to verify that risks had been reduced ALARP. This iterative approach (page 15) requires:

(a) Assessment of risks;

(b) Assessment of sacrifice;

(c) Undertaking cost-benefit analysis;

(d) Selection and implementation of mitigations; and

(e) Monitoring and evaluation of risks and data.

13 Against each step, we have indicated what ResiCAV+ would have to demonstrate and document to satisfy HSE that risks were being managed ALARP if required to do so. Adopting this format and approach would permit ResiCAV+ partners to justify and explain their

processes and methodology on an ALARP basis including its use of the significant difference and distributed ledger approach. Combined with onboard collection of incident data that could be forensically examined, this provides a route to thinking through what would be required to justify not just decision-making but the underlying system choices and architecture that led to it.

EVOLUTION OF THE BRAKING SYSTEM AND ITS REGULATION

Braking systems have – naturally – been considered a safety-critical system of motor vehicles for practically as long as motor vehicles have existed. For the very first vehicles, being heavy, inefficiently powered and travelling at less than walking speed, brakes were less of an issue. However as more powerful production models came into being on increasingly busy roads, brakes have been a defining safety feature and function of motor vehicles.

From wooden blocks and directly applied force to hydraulic and disc brakes, braking systems have continuously evolved to improve the safety performance of braking relative to the power and speed of the vehicles they are embedded in. All however fundamentally translated through actuators the decision-making and action of human drivers into mechanical braking force. Human decision-making (and indeed organisational decision-making) is a variable that the law exists to affect, incentivising some behaviours, and disincentivising others through punishment or other consequence/sanction.

The advent of increasingly sophisticated automotive electronic systems (e.g. Electronic Stability Control or **ESC**) and Anti-lock Braking Systems (**ABS**)) introduced electronic assistance into the braking function. For example, recognising that overly hard application of brakes by human drivers (in particular at high speed) could in fact cause wheels to lock and lose traction and/or steering, an ABS system utilises speed sensors to detect the risk of wheel lock and then automatically varies and controls braking pressure to mitigate the risk. This is a technique often taught to and applied by skilled and advanced human professional drivers, however, ABS is able to replicate this function with highly rapid response times and independently of the pressure being applied to the brake pedal by the human driver. Similar technology over time has been deployed increasingly to assist drivers in optimising braking performance once initiated. Often the assistance is imperceptible to drivers.

The increasing complexity of automotive electronic systems continues to offer ever more system data, assistance and control of motor vehicles including to the braking system. Systems such as Autonomous (or Advanced) Emergency Braking (**AEB**) or Adaptive Cruise Control (**ACC**) are able to use sensors to trigger braking function either to maintain stopping distances between moving vehicles without driver input, warn drivers of collision risk or to bring a vehicle to an emergency stop if a driver fails to brake hard enough or in time.

The safety benefits of these systems are potentially very significant. In one study commissioned by Euro NCAP and ANCAP, it was found that low speed AEB technology had led to a 38% reduction in real-world rear end crashes[1]. Indeed AEB is now required as standard for a maximum score on Euro NCAP safety tests and, from 2022, the EU will make AEB and other advanced assistance features mandatory[2].

However, the increasingly connected nature of the braking system to the overall vehicle electronic system and of that system to the wider world also introduces cyber vulnerabilities into the braking systems of individual vehicles that were not present before.

The scale of the potential opportunity and risk in the connected vehicle system today was demonstrated simultaneously in 2018 when Tesla became aware of poor braking performance issues upon a test review on its Model 3 sedan. In a matter of days, Tesla had pushed out a firmware update

[1] *Effectiveness of low speed autonomous emergency braking in real-world rear-end crashes*, Accident Analysis & Prevention, Volume 81, August 2015 pp24-29 (Elsevier).

[2] 1 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (Regulation (EU) 2019/2144)

"over-the-air" to thousands of vehicles in the market, dramatically improving the emergency braking performance of its vehicle[3]. In October 2021, Tesla similarly used over-the-air updates to thousands of customers to review phantom braking issues experienced by approved drivers to whom it had granted access to its trial "Full Self Driving" software. In doing so, it reportedly even temporarily deactivated the AEB system and Forward Collision Warning system without informing users[4]. The same rights accessed by a malicious actor could have very different and serious consequences.

THE FUTURE OF BRAKING SYSTEMS

The electronic complexity inherent in modern vehicle braking systems will increase further as it becomes linked to ever more advanced driver assistance systems such as Automated Lane Keeping Systems[5] (**ALKS**). However, it is expected to undergo a paradigm shift in the future with the advent of true Automated Driving Systems; that is to say a system of "*hardware and software that are collectively capable of performing the dynamic driving task on a sustained basis, regardless of whether it is limited to a specific operational design domain*"[6].

The complexity of decision-making involved in a true Automated Driving System is likely to require bespoke legislation as to the safety assurance and approval of such systems and their performance – including as to the data and accountability of system decision-making. These issues have been under consideration for some time including by the Law Commission of England and Wales and the Scottish Law Commission[7] and the Centre for Connected and Automated Vehicles[8]. For the purposes of this report, however, we focus on the cyber security of current modern vehicle braking systems, not strictly those of future automated vehicles.

THE RISKS TO THE BRAKING SYSTEM PRESENTED BY CYBER VULNERABILTY

The way in which the braking system of a modern motor vehicle is integrated with other vehicle subsystems and the particular cyber risks that this entails are presented in the ResiCAV paper *"Breaking the Brakes: Vehicle Braking as a Connected Cyber Physical System"*.

In summary:

1 The braking system is a safety-critical system which continues to be engineered up to the requirements of Automotive Safety Integrity Level D (**ASIL D**) reflecting automotive hazard analysis, risk assessment and expected safety measures at their highest level so as to avoid "*unreasonable risk due to hazards caused by malfunctioning behavior of electrical or electronic systems*"[9]. ASIL-D designation implies the potential for High Exposure operational situations (i.e. more than 10% typical operational time) where a malfunction can lead to High Severity harm (i.e. death or major bodily harm) with very Low Controllability (i.e. less than 90% of average drivers or other traffic participants are able to avoid harm). This would reflect a scenario, for example, where brakes failed catastrophically at high speed.

2 As a matter of automotive engineering, verifying the integrity of the braking system to ASIL D requirements is not straight-forward given the highly interconnected nature of the modern vehicle subsystems. In particular the mechanical brakes are integrated into advanced driver assistance systems such as ABS, ESC, AEB and ACC and are equipped throughout with an array of processors, sensors (internal and external), actuators and controllers. All of which are powered by electrical systems and millions of lines of software code including analytical

[3] https://arstechnica.com/cars/2018/05/how-a-software-brake-upgrade-won-tesla-a-consumer-reports-endorsement/ https://www.theverge.com/2018/6/2/17413732/tesla-over-the-air-software-updates-brakes

[4] https://www.latimes.com/business/story/2021-11-03/teslas-handling-braking-bug-in-public-self-driving-test

[5] On which the UK Government has been consulting (https://www.gov.uk/government/consultations/safe-use-of-automated-lane-keeping-system-on-gb-motorways-call-for-evidence) and which is already the subject of a UN Regulation No. 157

[6] Per BSI CAV Vocabulary - Version 3 (2020) https://www.bsigroup.com/en-GB/CAV/cav-vocabulary/

[7] https://www.lawcom.gov.uk/project/automated-vehicles/

[8] https://www.gov.uk/government/groups/expert-advisory-panel-for-cavpass-programme

[9] ISO 26262 - Road vehicles — Functional safety (the definition of which is the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems")

algorithms. Furthermore, vehicle electronic systems increasing allow for connectivity with third party devices (e.g. on-board infotainment or navigation interfaces) as well as external communication with other vehicles or infrastructure (including for example over-the-air firmware upgrading or mandated systems for safety such the "e-Call" emergency system).

3 However, existing design and safety frameworks focus predominantly on system faults (and fault tolerance), errors and failures as opposed to malicious cyberattack. In particular, given its characteristics, the modern vehicle braking system offers a very large 'attack surface' for cyberattacks. As cyberattacks have become more prevalent and novel and systems previously assumed to be closed have become integrated with others, it is becoming clear that, historically, design of system components and digital architecture may not have originally taken vulnerability to malicious cyberattack into account properly resulting in engineered vulnerability and risks[10].

Cyber attacks on vehicles and other Cyber-Physical Systems (**CPS**) are increasing. To date, fortunately, the majority of attacks on vehicle braking systems are 'white hat' attacks undertaken for research and feasibility purposes. However, the concept of 'hacking' the braking system using internal access or short range access or full remote external access has been demonstrated[11]. The cyber vulnerability of modern connected vehicles is a growing concern and a survey in 2020 from Uswitch found that reported cyber attacks were increasing significantly year on year, in particular for the purposes of theft either of personal data or keyless vehicles[12].

In the light of ever increasing complexity, integration of systems, hardware and software and the dynamic and continually emergent nature of cyberattack threats, traditional engineering design principles are insufficient as not all risks and threats can be known at the point of component and subsystem design. However, the distinct need to define and design for the cyber security aspect of vehicle CPS is recognised. In particular, in the following:

- SAE J3061_201601 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" (January 2016)
- HM Government "The Key Principles of Cyber Security for Connected and Automated Vehicles" (August 2017)
- BSI PAS 1885:2018 "The fundamental principles of automotive cyber security. Specification"
- BSI PAS 11281:2018 "Connected automotive ecosystems. Impact of security on safety. Code of practice"
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Regulation (EU) 2019/881)
- Zenzic "Cyber Resilience in Connected and Automated Mobility (CAM) Cyber Feasibility Report" (May 2020)
- ISO/SAE 21434 "Road vehicles – Cybersecurity engineering" (August 2021)

Principles and standards applicable to automotive cyber security engineering are however high level and do not prescribe or consider specific technology or solutions as to cyber security.

TYPE APPROVAL FRAMEWORK AND CYBER-SECURITY

As a result of withdrawing from the European Union, Great Britain has, since 1 January 2021, operated a Provisional GB Type Approval scheme (**GB Approval**) for certain categories of vehicles including

[10] "Breaking the Brakes: Spoofing and Denial of Service Attacks for Safety Critical Vehicle Components" (Shmyglya A., University of Bristol, 24 September 2020)

[11] Supra pp12-13

[12] https://www.uswitch.com/guides/car-insurance/data-security-in-connected-cars/

Passenger Vehicles (Category M) and Goods Vehicles (Category N). Vehicles approved under the EU Whole Vehicle Type Approval scheme must also obtain relevant GB Approval for new registrations of vehicles for GB roads. The provisional GB scheme will be replaced imminently with a Comprehensive GB Type Approval scheme.

As GB Approval currently only applies to whole vehicles, for now, the approval of vehicle systems, separate technical units and components continues to be in accordance with the relevant EU Type Approval (**"e"-type approval**) or UN Type Approval (**"E"- type approval**).

Whilst the type approval system in the UK is plainly undergoing transition, fundamentally the framework currently remains based on the principles of the EU / UN Type Approval system (in particular as expounded in Regulation (EU) 2018/858 as implemented by The Road Vehicles (Approval) Regulations 2020 and UN Regulations). Overseen by the Vehicle Certification Agency (**VCA**) the focus is on third party homologation assessment and ensuring the conformity of production of vehicles prior to placing vehicles on the market.

Certainly the legislation relating to vehicle braking systems remains currently based variously on:

1 Commission Directive 79/489/EEC of 18 April 1979 adapting to technical progress Council Directive 71/320/EEC on the approximation of the laws of the Member States relating to the braking devices of certain categories of motor vehicles and their trailers (Directive 79/489/EEC);

2 Commission Directive 85/647/EEC of 23 December 1985 adapting to technical progress Council Directive 71/320/EEC on the approximation of the laws of the Member States relating to the braking devices of certain categories of motor vehicles and their trailers (Directive 85/647/EEC);

3 Road Vehicles (Construction and Use) Regulations 1986 (as amended);

4 Commission Directive 88/194/EEC of 24 March 1988 adapting to technical progress Council Directive 71/320/EEC on the approximation of the laws of the Member States relating to the braking devices of certain categories of motor vehicles and their trailers (Directive 88/194/EEC)

5 UN Regulation No. 13 — Uniform provisions concerning the approval of vehicles of categories M, N and O with regard to braking [2016/194]

6 UN Regulation No. 13-H — Uniform provisions concerning the approval of passenger cars with regard to braking [2015/2364]

7 UN Regulation No 131 — Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking Systems (AEBS)

8 UN Regulation No. 139 — Uniform provisions concerning the approval of passenger cars with regard to Brake Assist Systems (BAS) [2018/1591]

9 UN Regulation No. 140 — Uniform provisions concerning the approval of passenger cars with regard to Electronic Stability Control (ESC) Systems [2018/1592]

10 Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (Regulation (EC) 661/2009)

Following Brexit, vehicle requirements in GB may potentially start to diverge from incoming and future EU legislation albeit that the Trade and Co-operation Agreement of 30 December 2020 between the EU and UK confirms the intention to stay closely aligned on automotive safety and standards. For now, so far as safety is concerned, we will assume that the UK whole vehicle type approval framework will remain broadly similar to the EU framework and that the UN system of type approval continues to

apply in any event as the UK is a signatory to the 1958 and 1998 UN Agreements (as revised) (UN Regulations).

Conventionally, these requirements focus on the condition and good working order of brakes and the technical efficiency and effectiveness of braking systems (service, secondary or parking) at the point of assessment prior to placing into the market. However, recent regulations are increasingly directed towards cyber security and software aspects of vehicle systems in particular:

11 UN Regulation No. 155 – Cyber security and cyber security management system

12 UN Regulation No. 156 – Software update and software update management system

13 UN Regulation No. 157 – Automated Lane Keeping Systems (ALKS)

14 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification

In addition, at the time of writing, there are a number of standards proposed or under development including:

15 ISO/PRF PAS 5112 "Road vehicles — Guidelines for auditing cybersecurity engineering" (under development)

16 ISO/SAE PWI 8475 "Road vehicles — Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF)"

17 ISO/PWI 8477 "Road vehicles — Cybersecurity verification and validation"

UN Regulation No. 155 will require manufacturers to establish and maintain a compliant and independently-audited[13] Cyber Security Management System (**CSMS**). This will be required in the EU from 2022 onwards to obtain EU Type Approvals and it is assumed that a similar position will apply for GB Type Approval. Amongst other requirements, UN Regulation No. 155 requires a whole lifecycle approach to cyber security and that the CSMS is able to deal with and addresses mitigations for specified types of cyber threats (these Annex 5 threats and mitigations are reproduced in the Appendix to this report).

[13] Per above, at the time of writing, ISO/PRF PAS 5112 "Road vehicles — Guidelines for auditing cybersecurity engineering" is under development

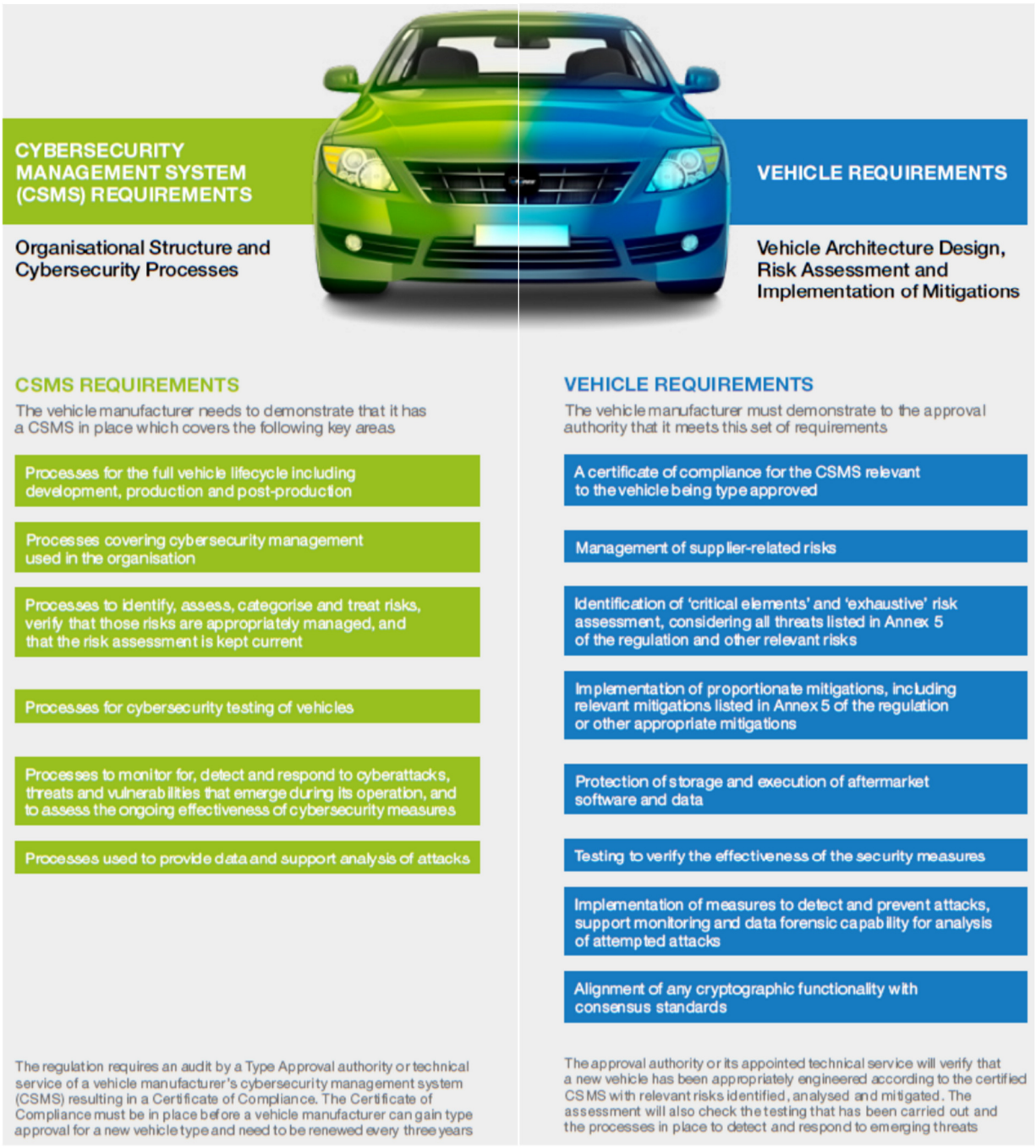


Figure 1 - UN Regulation No. 155 key requirements (source: HORIBA MIRA[14])

Given the dynamic nature of cyber security methodology, techniques and threats, this approach to the automotive CPS indicates potentially a much greater degree of ongoing engagement with approval authorities after initial approvals are secured than has historically been the case (including notification of modifications affecting the essential aspects of the electric/electronic architecture and external interfaces with respect to cyber security of the vehicle). Breaches of cyber security in the market would potentially become matters relevant to type approvals including as to whether an adequate CSMS continues to satisfy the likes of UN Regulation No. 155.

The recognition of the dynamic and uncertain nature of emergent cyber threats is also acknowledged in the EU in Regulation (EU) 2019/881 establishing an EU agency (ENISA) for the purpose of

[14] *"How to Navigate New Cybersecurity Type Approvals: A White Paper outlining how to meet UNECE Regulation 155"*, HORIBA MIRA, March 2021

administering cyber security certification. The regulation not only envisages that a cyber security certification scheme will be introduced for connected and automated cars but also acknowledges that:

"*Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation.*"

In the next few years, we are therefore likely to see significant development on uniform cyber security standards and independent certification / approval schemes of automotive CPS.

POST-SUPPLY SAFETY IN THE MARKET AND CYBER SECURITY

Once vehicles have been supplied into a market and are in use, where safety issues do not affect type approval, legislation[15] provides amongst other things for the regular testing of vehicles including the inspecting of the physical condition of the braking system through tests such as the MOT test.

Vehicle safety obligations are also enforced through the Driver & Vehicle Standards Agency (**DVSA**) as the competent authority designated under the General Product Safety Regulations 2005 (**GPSR**). However, for significant reported safety defects, the VCA may also be notified (e.g. serious safety defects requiring vehicle recalls or affecting type approval). Again, following Brexit, UK legislation may begin to diverge from the EU, however, the product and vehicle safety framework currently is that derived from EU legislation and is expected to remain closely aligned so far as motor vehicles go.

Broadly, so far as supply to consumers is concerned, the safety duty of vehicle producers is met through compliance with the type approval process. GPSR contains a general duty of safety applicable to producers and distributors of products. However, this is not applicable where sectors have specific EU safety requirements and where sector specific requirements have been met, products are deemed safe. Consequently, the safety duties of vehicle manufacturers and producers are generally met through the type approval and conformity process. The development of the type approval framework to encompass cyber security is therefore of critical importance to embedding cyber security into the vehicle safety framework. It is clear from the above that the emerging automotive cyber security framework and the assurance of systems over a vehicle's lifetime is going to require a degree of market surveillance after supply of vehicles that has not been common before.

In the historic absence of specific requirements relating to enduring cyber security in the vehicle approval framework, there has to date been a degree of debate as to what obligations producers and distributors have in respect of cyber security and software in cyber physical systems of vehicles placed on the market (particularly as a separate supply to the original vehicle) and whether such obligations fall within any general duties (such as those under GPSR).

Where a product issue has caused personal injury, damage to property or death in respect of consumers, claims may lie under the Consumer Protection Act 1987 (implementing Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products) (**CPA**) in respect of relevant defects. Generally speaking, a product is defective under CPA if it is not as safe as persons are generally entitled to expect taking into account the purpose for which the product has been marketed, any instructions for use or warnings and what might reasonably be expected to be done with the product at the time when the product was supplied. Where the product issue relates to a vehicles design and manufacture, by and large, demonstrable compliance with the comprehensive vehicle type approval framework offers a robust defence.

However debate as it relates to consumer liability has intensified with the increasing prevalence of connected vehicles and other 'Internet of Things' (**IoT**) devices. In particular, there has been debate

[15] Principally, the Road Traffic Act 1988

over aspects of the CPA which was not a law drafted with cyber physical products in mind. Concerns include:

1 The extent to which pure vehicle software is considered a "product" either supplied integrated or separately at the point of sale or afterwards. Linked to this would be the question of whether enduring cyber security is a product or a service (the latter of which is not covered by CPA)

2 The extent to which any software issues or vulnerabilities could be considered a "defect" at the time the product was supplied, including taking account of the emergent qualities of cyber threats which means that systems will always be exposed to novel threats during their lifetime

3 The identity of relevant producers if, for example, software is provided separately

4 The appropriateness of existing limitation dates (10 years after first supply) in the context of product lifecycles and products subject to software/hardware upgrades

5 The difficulty of establishing liability for software defects or cyber vulnerabilities – particularly where certain AI technologies (e.g. neural networks) are involved – and whether strict liability or reverse burdens of proof should apply

6 The applicability of product liability defences such as the "state of the art" defence and the determination of defects within products as at "the relevant time" for fast moving software-based technologies involved in the cyber security arena.

It is possible that cyber security software could be subject to a "contract to supply digital content" under the Consumer Rights Act 2015 (**CRA**) permitting claims for losses where digital content is not of "satisfactory quality" or "fit for particular purpose". However it is unclear, for example, whether or not this amounts to any obligation that or that there can be any reasonable expectation that digital content will be protected at all times from cyber attacks (malicious or otherwise).

A number of these issues were highlighted in the legal review project undertaken by the Law Commission of England and Wales and the Scottish Law Commission on Automated Vehicles[16]. Additionally, the EU's Expert Group on Liability and New Technologies – New Technologies Formation also considered the issue and reported in 2019. It concluded that whilst there was a baseline of existing product liability protection capable of encompassing such cyber-physical new technologies there was also scope to make it more consistent across the EU and to look at the specific challenges of emerging technology to reinforce obligations. It also recommended considering new joint and several liability or strict liability rules, reverse burden of proof regimes, new continuing duties to ensure safety in certain technologies after supply and reform of the "state of the art" defence in circumstances where producers are obligated to monitor and update[17].

Nevertheless, for now, it is clear that there would be significant legal challenges to making a claim under UK consumer protection law in respect of cyber security breaches affecting vehicle sub-systems – particularly as the result of novel cyber attacks.

Furthermore, both the UK and the European Commission has been working on and consulting on proposals in this area throughout 2021[18] and both are expected to legislate on this area of product liability and emerging technologies from 2022. However, these changes would only really have material relevance as regards vehicle cyber security systems to the extent that they are governed by general product safety law. As noted above, the sector-specific type approval regulations are adapting to encompass cyber security aspects and it seems tolerably clear that the direction of travel is to embed vehicle cyber security requirements into the sector-specific safety framework. These in turn will set

[16] https://www.lawcom.gov.uk/project/automated-vehicles/

[17] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[18] For example, see the UK Government's response to its call for evidence on product safety (November 2021) - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1032752/call-for-evidence-response-11-2021.pdf and Product Security and Telecommunications Infrastructure Bill https://www.gov.uk/government/news/new-cyber-laws-to-protect-peoples-personal-tech-from-hackers

the reasonable expectations that consumers can have of type approved production vehicles that they buy. Nonetheless changes to the general product safety framework may certainly affect those supplying, for example, third party or after market products and associated services.

"DEFENDING" CYBER SECURITY OF THE BRAKING SYSTEM IN LAW – FOR WHAT PURPOSE?

As far as defending the cyber security of a braking system in law goes, there are variety of applicable legal regimes (and specifically the enforcement and sanction aspects of those regimes) depending on the specific factual context, parties, breaches and losses involved and where different criteria would apply. For example, a breach of cyber security today relating to the braking system might conceivably lead (amongst other things) to:

1 Criminal charges by the police such as Corporate Manslaughter under the Corporate Manslaughter and Corporate Homicide Act 2007 if fatalities are involved;

2 Criminal enforcement action by the VCA in respect of any breaches of the type approval and conformity legislation;

3 Criminal enforcement action by the DVSA in respect of breaches of the general safety duty under the GPSR 2005 for matters that are not specifically covered in sector-specific legislation, albeit the residual scope as regards automotive safety would appear very limited (certainly for the vehicles as type approved and supplied);

4 Criminal enforcement action by the Health and Safety Executive in respect of the Health and Safety at Work, etc Act 1974 (**HSWA**) where vehicles have been provided by an employer in the context of work (regardless of whether people affected are employees or members of the public and consequently the ambit of this general legislation is extraordinarily wide);

5 Criminal enforcement action under Data Protection Act 2018 by the Information Commissioner's Office to the extent that any breach affected personal data protection;

6 Civil action by consumers on strict liability basis under CPA or on the basis of common law negligence and/or breach of contract

7 Civil action under the CRA

Criminal or regulatory actions are punitive or corrective in nature; civil actions are compensatory.

"Defending" the cyber security of the braking system in each of these contexts involves different arguments, criteria, thresholds and burdens of proof.

Moreover, as explained above, key legislation around vehicle type approval, conformity, product safety and liability are in flux. All are adapting to the challenge of cyber-physical systems and therefore there is a degree of uncertainty as to what the expectations in this area are going to be in the short to medium term. However, it appears to be relatively clear that:

1 Cyber security elements will increasingly become part of the vehicle type approval requirements applicable to the UK (and elsewhere)

2 Those approval requirements (based on emerging requirements and policy stances at approvals authority level) will be:

(a) sector-specific (and indeed system or component specific);

(b) require a whole lifecycle approach and management system for cyber security;

(c) require cyber security design to presume the occurrence of cyber attacks and anticipate and minimise impact; and

(d) nevertheless be system or technology 'agnostic' in the sense of not specifying a particular technology to achieve requirements.

3 An independent cyber security certification scheme is likely to be required and introduced for the purposes of approval of cyber security systems

4 Cyber security system aspects of motor vehicles will be, as with other automotive subsystems, prescribed predominantly by specific approval regulations, not general product safety regulations (e.g. not the residual safety duty under GPSR).

5 Unlike other Internet of Things devices and smart products therefore, we anticipate that automotive cyber security will in due course be prescribed by sector specific safety regulations. Consequently, reforms to civil liability for products proposed for emerging technology are likely to have limited impact on the safety regulation of vehicle systems. As it is today, the issue of vehicle safety is likely to refer back predominantly to type approval requirements. To the extent that producers breach their sector-specific statutory safety duties, civil claims may follow but this is likely to be limited to circumstances where type approval certification and assessment has not been fully complied with[19]. They are not therefore likely in the main to be under the general (strict liability) safety duty of the GPSR. And the same sector specific safety regulations will likely set the expectations that consumers may reasonably have under product liability law.

6 However other general legal frameworks such HSWA do apply and enforcement is potentially possible (in particular it is conceivable that they may be enforced where compliance with type approvals has not in fact been achieved or where there is an absence of specific or adequate type approval provision).

The objective of this legal report is to examine an approach to defensible arguments around ALARP which is a safety regulatory / criminal aspects (see below). In the circumstances, the assumption of this report is that defending cyber security in this context is to be taken in the context of position regulatory / criminal prosecution.

PARTY LIABILITY FOR AUTOMATED DECISIONS IN SYSTEMS

Organisations in the UK such as the Office for Artificial Intelligent, Cabinet Office and Central Digital & Data Office have been considering reforms in respect of automated decision-making including laws protecting individuals from the consequences of automated decision-making[20]. However, certainly so far as safety-critical products and systems are concerned, there is no indication that manufacturers, producers or retailers of cyber-physical products in future may not be legally responsible for the automated decision-making of those products. Indeed, from legal, societal and commercial perspectives, it is considered important for there to be clarity over legal liability (and associated insurance coverage) for the sake of consumer protection and confidence.

This debate is played out most obviously in the context of automated vehicles which is a future cyber-physical product that has captured the public imagination and debate prominently. Based on the Automated and Electric Vehicles Act 2018 and the direction of the Law Commissions' 3 year review into Automated Vehicles legislation, the focus has been on establishing clarity as to insurance coverage and legal liability for automated decision-making. For future automated vehicles, legal liability will focus in particular on the "Authorised Self-Driving Entity" (**ASDE**) which is the organisation that puts an automated vehicle forward for regulatory authorisation. This is the equivalent of vehicle manufacturers currently putting their vehicles forward for necessary type approval.

The integral nature of cyber security software in cyber physical products and the framework of the vehicle type approval system (which is fast adapting to include express cyber security elements) means that vehicle manufacturers are likely to be held responsible for the decision-making of the cyber security systems that they have designed or commissioned and installed as part of their type approved cyber physical vehicle system. Where the nature of emergent cyber threats means that automated decision-making may become an essential feature of a cyber resilient system this raises the need for, amongst other things, design, testing, simulation and validation to understand system responses to

[19] For example in the case of the 'Dieselgate' litigation and the alleged deploying of 'cheat devices' to secure approvals

[20] See: https://blog.burges-salmon.com/post/102gybs/automated-decision-making-by-public-bodies-government-guidance-published and https://techmonitor.ai/policy/privacy-and-data-protection/uk-algorithmic-decision-making-article-22-brexit

often unpredictable inputs and ensure that the 'behaviour' of the system nevertheless falls within a reasonably predictable range to allow for safe deployment.

"DEFENSIBILITY" IN THE CONTEXT OF REDUCING CYBER VULNERABILITY OF A BRAKING SYSTEM AS LOW AS REASONABLY PRACTICABLE USING SIGNIFICANT DIFFERENCE AND BASED ON THE DISTRBUTED LEDGER

For the purpose of this paper, we are asked to consider specifically a route to a per-vehicle legally defensible argument that the cyber vulnerability of the braking system was reduced to "as low as reasonably practicable" (**ALARP**) using the significant difference approach and based on the distributed ledger.

The base assumption here is that the key risk that has come to pass in this hypothetical example is that a cyber attack causes a malfunction in the braking system whilst a vehicle is in operation so as to lead to an accident involving fatalities, personal injuries and/or damage to property. The assumption is that resulting loss of control has been total and therefore there are no issues of driver or third party contributory fault. We are also not therefore focussing on other peripheral outcomes such as loss of personal data (notwithstanding that arguments as to mitigations adopted to minimise cyber vulnerability may be similar).

ALARP

First and foremost, it is important to recognise that the concept of reducing risks ALARP is one that derives solely from health and safety law, in particular the general duties under the HSWA and certain specific duties under Regulations made under the HSWA. In that context it is **a very specific legal term** evolved from case law in this area and that arguably does not reflect what might be considered to be a layman's interpretation of the phrase. It is linked with, uniquely in criminal law, a 'reverse burden of proof'. The organisation whose undertaking gives rise to the risk must prove that risk had been reduced so far as is reasonably practicable (**SFAIRP**)[21]

Interpretation[22] of the obligation to reduce risks "as low as is reasonably practicable" so far as health and safety law goes rests in particular on the following regulatory expositions of the ALARP principle (emphasis added):

1 "*... in every case, it is the risk that has to be weighed against the measures necessary to eliminate the risk. The greater the risk, no doubt, the less will be the weight to be given to the factor of cost.*"; and

2 "'*Reasonably practicable' is a narrower term than 'physically possible' and seems to me to imply that a* ***computation*** *must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a* ***gross disproportion*** *between them - the risk being insignificant in relation to the sacrifice - the defendants discharge the onus on them.*"

Consequently demonstrating ALARP is in particular dependent on an understanding of risks, the available counteracting measures, the relative cost of those measures (in time, money and effort) and cost-benefit calculation between them. This can be particularly challenging where designing for emergent risks for which there is currently an absence of data and where the state of the art in cyber security technology is continually changing. The difference between what is merely 'disproportionate' and what is 'grossly disproportionate' is not defined but is linked to the level of perceived risk and societal level risk. Consequently, measures aimed at cyber threats to individual vehicles compared to cyber threats to entire systems or connected fleets would be viewed differently.

As noted above, ALARP, as applied to health and safety law in the UK under Section 40 HSWA, is also characterised by the application of a reverse burden of proof. Establishing that risks have been

[21] SFAIRP is the formulation used in the HSWA 1974. ALARP is the terms used in resulting regulatory guidance. ALARP and SFAIRP are regarded generally as being synonymous in meaning. We have used ALARP from her onwards for brevity.

[22] Based in particular on *Edwards v National Coal Board* [1949] 1 KB 704; [1949] 1 All ER 743

reduced ALARP requires a defendant to prove on the balance of probabilities that it was not reasonably practicable to do more than was in fact done. It is therefore considered a very high threshold and evidential burden of proof not least since all measures are potentially reasonable other than those that are grossly disproportionate. The conviction rate for HSWA charges brought is consequently typically over 90% each year. HSWA offences permit unlimited fines for corporate defendants and imprisonment for individuals convicted.

ALARP has not conventionally been enforced (as a matter of policy choice) in practice in respect of automotive engineering notwithstanding that the scope of HSWA is so wide that it likely applies to many situations in which vehicles are used. So far as production vehicles go and where production vehicles are supplied by employers in a work context, it generally suffices as regards matters of design and construction to demonstrate that the vehicle is suitable for its purpose and type approved. Whilst the HSWA applies, due to a scale of resource policy choice, enforcement against drivers or other parties has fallen not to the Health & Safety Executive (**HSE**) but to other agencies using other legislation. The HSE as the primary enforcement agency under the HSWA, has produced only limited guidance on cyber security and only in the context Electrical, Control and Instrumentation systems in the Onshore Chemicals, Explosives and Microbiological Sectors[23].

However, the rapid move from a single driver or single vehicle emphasis to integrated roads systems is now attracting greater attention on system based investigation and enforcement. For example a coroner has recently referred a death on a smart motorway to the CPS[24] and the Office of Rail and Road (**ORR**) whilst strictly not the safety (HSWA) regulator for roads (only rail) is looking closely also at smart motorways on a system safety basis[25].

It is quite conceivable therefore that HSWA criminal investigation and enforcement may extend in the near future to road and vehicle system safety issues including cyber vulnerabilities, particularly where they demonstrate connected system impacts or impacts of relevance to many vehicles and/or systems.

Comparison of ALARP against existing safety through homologation

The current system by which braking systems is regulated is through type approval regulations and assessment/certification of conformity. Conforming to applicable regulations *prima facie* meets vehicle safety requirements notwithstanding that requirements can sometimes be high level. Even when general requirements apply in relevant regulations, they are expressed and assessed as goals without any reverse burden of proof.

For example, Article 5(1) of Regulation (EC) No 661/2009 includes in addition to the general obligation to type approve new vehicles, a general requirement that manufacturers *"shall ensure that vehicles are designed, constructed and assembled so as to minimise risk of injury to vehicle occupants and other road users"*. That, however, is some way short of a HSWA ALARP obligation and burden of proof.

Similarly, incoming UN Regulation No. 155 on cyber security, as well as listing specific threats and mitigations has general provisions that relate to cyber security being *"adequately considered"*, mitigation within *"a reasonable timeframe"*, *"proportionate mitigations"*, *"proportionate measures"* and being in line with *"consensus standards"*. This is again not equivalent to ALARP which actually contemplates the undertaking of what might be considered 'disproportionate' measures as long as they are not 'grossly' so.

Whilst vehicle type approval regulations are being developed and the regulatory framework for certifying cyber security within those are being considered, and we note the wider trends toward a wider system-based view of road safety (see comments above), we are not aware of moves to apply an ALARP test to automotive cyber security. As we have seen in the Report of the Expert Group on Liability and New Technologies commissioned by the EU, there is some talk of reverse burdens of proof or even strict liability in some circumstances in respect of civil product liability for emerging

[23] https://www.hse.gov.uk/eci/cyber-security.htm

[24] https://www.zurich.co.uk/news-and-insight/highways-england-referred-to-cps-over-smart-motorways

[25] See for example : https://www.orr.gov.uk/search-news/analysing-data-and-evidence-all-lane-running-motorways

technologies. However, there is no immediate indication that this is expected to apply to cyber security of automotive systems or apply to criminal liability in respect of safety compliance.

Consequently, application of an ALARP approach to test and construct defensible legal arguments on cyber security would represent a 'belt and braces' test that is likely to be above what is currently visible at least as mandated. As with the existing type approval framework, safety requirements are likely to be mandated at a level that will not necessarily dictate specific methodologies or technologies that manufacturers may adopt and put forward for certification / approval. Automotive cyber security systems are then likely to be deemed safe and resilient if they are certified / type approved properly. Crucially, in future, this aspect of cyber security is likely to involve materially greater involvement of regulators post-initial approval to ensure that enduring system resilience requirements of type approval will be and remain demonstrated in real world conditions.

Nevertheless we have considered here how a route to a legally defensible argument using ALARP under HSE enforcement could be navigated by the ResiCAV+ technical team.

Route to a per vehicle legally defensible argument that the cyber vulnerability of the braking system was reduced ALARP using the significant difference approach and based on the distributed ledger

Notwithstanding the position above, should ResiCAV+ partners wish to demonstrate a route to a legally defensible argument hypothetically using ALARP principles and processes, we have considered the steps that the HSE would likely take to verify that risks had been reduced ALARP. Against each, we have indicated what ResiCAV+ would have to demonstrate and document to satisfy HSE that risks were being managed ALARP:

#	ACTION	REQUIRED INPUTS / EVIDENCE	NOTES
1	<u>Assessment of risks</u> Undertake a "suitable and sufficient" risk assessment of all risks presented by cyber vulnerability of the braking system (hazard, probability, severity of impact)	A suitable and sufficient risk assessment within a defined and implemented Cyber Security Management System	Assessment needs to include all known and probable risks. However given the emergent nature of cyber threats should also quantify risk of unknown but anticipated emergent threats. General risk assessment guidance from HSE to be reviewed and complied with as well as specific provisions (e.g. as to "*exhaustive risk assessment*" in UN Regulation 155 including all threats in Annex 5 and National Cyber Security Centre Cyber Assessment Framework (**NCSC CAF**)
2	<u>Assessment of sacrifice</u> Against all available risk mitigation measures assess the cost in terms of money, time and trouble	As part of risk assessment or as separate document, identify available mitigations and assess the cost and feasibility of each	Assessment of sacrifice may only be limited relevance as regards any mandatory mitigations (e.g. all mitigations required by Annex 5 in UN Regulation No. 155). However it may be relevant if different technologies and methodologies are available to achieve a high level mandatory mitigation in which case each to be assessed

3	Undertake cost-benefit analysis For each risk and set of potential mitigations, undertake a cost-benefit analysis to understand the cost of action relative to the risk reduction gain	Analysis of cost-benefit for all potential mitigations to reduce or eliminate respective risks	Evidence of how any mitigations may have been identified and assessed as being "grossly disproportionate" and therefore dismissed from selection
3.1	Consider whether wider societal concerns over risk might affect balancing exercise		Certain risks in terms of scale of public potentially affected or damage to public confidence or other policy priorities may be so severe as to warrant seemingly disproportionate costs to reduce or eliminate
3.2	Consider applicable regulations / guidance	Evidence that all mandatory regulations as to cyber security and mitigations have been complied with. Evidence of voluntary guidance and standards compliance.	All mandatory regulations (e.g. UN Regulation No. 155) to be complied with as a minimum (whatever the cost). In due course, the cyber security system may also need to be independently certified for type approval and so guidance from any certification authority will also need to be complied with. Other guidance and standards that may not be mandatory (e.g. NCSC CAF, Zenzic, ISO/SAE 21434) should be complied with also unless there is good reason to justify a compliance gap.
4	Selection and implementation of mitigations Once grossly disproportionate measures have been eliminated all other measures are open for selection. At that point, the HSE requires that measures which reduce risk the most are selected and implemented regardless of cost (since none are grossly disproportionate)	Evidence that based on risks assessments and cost-benefit analysis, the most effective mitigation or combination of mitigations have been selected and deployed.	We note that the project seeks to put forward its CyRes methodology including use of significant difference and distributed ledger technology. In practice, if they are not grossly disproportionate and are assessed from the available options to offer the most effective mitigation of identified risks, then selection can be justified. However, if the process has identified other viable alternatives that are more effective, these other mitigations should be used. ALARP requires demonstrable selection of the most effective mitigation or combination of mitigations, unless the sacrifice

			and cost are grossly disproportionate.
5	Monitoring and evaluation of risks and cyber security data Safety-relevant data must be captured and processed as part of monitoring and evaluation of safety risks (including cyber) Risk assessments and risk mitigations must be continuously reviewed in the light of new external data and internal performance data and analysis	A Cyber Security Management System that has robust procedures to review emergent risks, monitor and evaluate performance and safety data from vehicles routinely and trigger changes as necessary Vehicle data system that captures accurately, stores securely and makes data available on a trustworthy and accessible form for continuous safety monitoring and analysis. This will include data required to demonstrate forensically the facts and decision-making pertaining to individual vehicle incidents in manner that is verifiable and trustworthy.	At all points, if emerging data indicates that new risks or existing risks are not being managed ALARP then the system must be capable of adapting in a timely manner. This is challenging where emergent characteristics of cyber threats mean that assumptions may change very quickly. Methodologies that are able to contain and deal with emergent threats, maintain safe operation and buy time for comprehensive response are positive features of system resilience. In respect of data capture, regulatory requirements (including provisions around any future Road Collision Investigation Branch[26] or future regulator of automated vehicles) and insurance requirements may introduce standard data capture and reporting in any event. However, even outside the context of 'incidents', data that may be relevant to improving safety and cyber security must be captured accurately, securely and processed or analysed so that real-time or near real-time identification of emergent threats can be demonstrated – as well as the system or vehicle response resulting from it.

[26] https://www.gov.uk/government/news/government-launches-consultation-on-road-collision-investigation-branch

Appendix - Annex 5 UN Regulation No. 155

List of threats and corresponding mitigations

1. This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.

2. Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.

3. The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.

4. The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:

   (a) Safe operation of vehicle affected;

   (b) Vehicle functions stop working;

   (c) Software modified, performance altered;

   (d) Software altered but no operational effects;

   (e) Data integrity breach;

   (f) Data confidentiality breach;

   (g) Loss of data availability;

   (h) Other, including criminality.

Part A. Vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table A1.

Table A1
List of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
4.3.1 Threats regarding back-end servers related to vehicles in the field	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (**insider attack**)
			1.2	**Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	**Unauthorized physical access** to the server (conducted by for example USB sticks or other media connecting to the server)

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	2.1	**Attack on back-end server stops it functioning**, for example it prevents it from interacting with vehicles and providing services they rely on
	3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1	Abuse of privileges by staff (**insider attack)**
			3.2	**Loss of information in the cloud**. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
			3.3	**Unauthorized internet access to the server** (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			3.4	**Unauthorized physical access to the server** (conducted for example by USB sticks or other media connecting to the server)
			3.5	**Information breach** by unintended sharing of data (e.g. admin errors)
4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	**Spoofing of messages** by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
			4.2	**Sybil attack** (in order to spoof other vehicles as if there are many vehicles on the road)
	5	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	5.1	Communications channels permit **code injection**, for example tampered software binary might be injected into the communication stream
			5.2	Communications channels permit **manipulate** of vehicle held data/code
			5.3	Communications channels permit **overwrite** of vehicle held data/code
			5.4	Communications channels permit **erasure** of vehicle held data/code
			5.5	Communications channels permit introduction of data/code to the vehicle (write data code)
	6	Communication channels permit untrusted/unreliable messages to be accepted or	6.1	Accepting information from an **unreliable or untrusted source**
			6.2	**Man in the middle** attack/ session hijacking

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
		are vulnerable to session hijacking/replay attacks	6.3	**Replay attack**, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway
	7	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	7.1	**Interception of information** / interfering radiations / monitoring communications
			7.2	Gaining **unauthorized access** to files or data
	8	Denial of service attacks via communication channels to disrupt vehicle functions	8.1	**Sending** a large number of garbage **data** to vehicle information system, **so that it is unable to provide services** in the normal manner
			8.2	**Black hole attack**, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles
	9	An unprivileged user is able to gain privileged access to vehicle systems	9.1	An unprivileged user is able to **gain privileged access**, for example root access
	10	Viruses embedded in communication media are able to infect vehicle systems	10.1	**Virus** embedded in communication media infects vehicle systems
	11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious **internal** (e.g. CAN) **messages**
			11.2	Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
			11.3	Malicious diagnostic messages
			11.4	Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)
4.3.3. Threats to vehicles regarding their update procedures	12	Misuse or compromise of update procedures	12.1	Compromise of **over the air software update procedures**. This includes fabricating the system update program or firmware
			12.2	Compromise of **local/physical software update procedures**. This includes fabricating the system update program or firmware
			12.3	The **software** is **manipulated before the update process** (and is therefore corrupted), although the update process is intact

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
			12.4	**Compromise** of cryptographic keys of the software provider **to allow invalid update**
	13	It is possible to deny legitimate updates	13.1	Denial of Service attack against update server or network to **prevent rollout of critical software updates** and/or unlock of customer specific features
4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack	15	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack	15.1	Innocent victim (e.g. owner, operator or maintenance engineer) being **tricked into taking an action** to unintentionally load malware or enable an attack
			15.2	**Defined security procedures** are not followed
4.3.5 Threats to vehicles regarding their external connectivity and connections	16	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications	16.1	Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile
			16.2	**Manipulation of vehicle telematics** (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)
			16.3	Interference with **short range wireless systems** or sensors
	17	Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems	17.1	**Corrupted applications**, or those with poor software security, used as a method to attack vehicle systems
	18	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection
			18.2	Media infected with a **virus** connected to a vehicle system
			18.3	**Diagnostic access (e.g. dongles in OBD port)** used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)
4.3.6 Threats to vehicle data/code	19	Extraction of vehicle data/code	19.1	Extraction of copyright or proprietary software from vehicle systems (product **piracy**)
			19.2	Unauthorized access to the **owner's privacy information** such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.
			19.3	Extraction of cryptographic keys

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	20	Manipulation of vehicle data/code	20.1	Illegal/unauthorized changes to **vehicle's electronic ID**
			20.2	**Identity fraud.** For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend
			20.3	Action to **circumvent monitoring systems** (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)
			20.4	Data manipulation to **falsify vehicle's driving data** (e.g. mileage, driving speed, driving directions, etc.)
			20.5	Unauthorized changes to **system diagnostic data**
	21	Erasure of data/code	21.1	Unauthorized deletion/manipulation of **system event logs**
	22	Introduction of malware	22.2	Introduce **malicious software** or malicious software activity
	23	Introduction of new software or overwrite existing software	23.1	**Fabrication of software** of the vehicle control system or information system
	24	Disruption of systems or operations	24.1	**Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
	25	Manipulation of vehicle parameters	25.1	Unauthorized access of **falsify the configuration parameters** of vehicle's key functions, such as brake data, airbag deployed threshold, etc.
			25.2	Unauthorized access of **falsify the charging parameters**, such as charging voltage, charging power, battery temperature, etc.
4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26	Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short **encryption keys** and long period of validity enables attacker to break encryption
			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems
			26.3	Using already or soon to be deprecated **cryptographic algorithms**
	27	Parts or supplies could be compromised to permit vehicles to be attacked	27.1	**Hardware or software, engineered to enable an attack** or fails to meet design criteria to stop an attack

High level and sub-level descriptions of vulnerability/ threat			*Example of vulnerability or attack method*	
	28	Software or hardware development permits vulnerabilities	28.1	**Software bugs**. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present
			28.2	**Using remainders** from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit access to ECUs or permit attackers to gain higher privileges
	29	Network design introduces vulnerabilities	29.1	**Superfluous internet ports left open**, providing access to network systems
			29.2	Circumvent **network separation** to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages
	31	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the **car changes user** (e.g. is sold or is used as hire vehicle with new hirers)
	32	Physical manipulation of systems can enable an attack	32.1	**Manipulation of electronic hardware**, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack **Replacement of authorized electronic hardware** (e.g., sensors) with unauthorized electronic hardware **Manipulation of the information** collected by a sensor (for example, using a magnet to tamper with the Hall effect sensor connected to the gearbox)

Part B. Mitigations to the threats intended for vehicles

1. Mitigations for "Vehicle communication channels"

   Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10 M6	The vehicle shall verify the authenticity and integrity of messages it receives Systems shall implement security by design to minimize risks
5.2	Communication channels permit manipulation of vehicle held data/code	M7	Access control techniques and designs shall be applied to protect system data/code
5.3	Communication channels permit overwrite of vehicle held data/code		
5.4 21.1	Communication channels permit erasure of vehicle held data/code		
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code)		
6.1	Accepting information from an unreliable or untrusted source	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.2	Man in the middle attack / session hijacking	M10	The vehicle shall verify the authenticity and integrity of messages it receives
6.3	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway		
7.1	Interception of information / interfering radiations / monitoring communications	M12	Confidential data transmitted to or from the vehicle shall be protected
7.2	Gaining unauthorized access to files or data	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example of Security Controls can be found in OWASP
8.1	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	M13	Measures to detect and recover from a denial of service attack shall be employed
8.2	Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles	M13	Measures to detect and recover from a denial of service attack shall be employed

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
9.1	An unprivileged user is able to gain privileged access, for example root access	M9	Measures to prevent and detect unauthorized access shall be employed
10.1	Virus embedded in communication media infects vehicle systems	M14	Measures to protect systems against embedded viruses/malware should be considered
11.1	Malicious internal (e.g. CAN) messages	M15	Measures to detect malicious internal messages or activity should be considered
11.2	Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	M10	The vehicle shall verify the authenticity and integrity of messages it receives
11.3	Malicious diagnostic messages		
11.4	Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)		

2. Mitigations for "Update process"

   Mitigations to the threats which are related to "Update process" are listed in Table B2.

Table B2
Mitigations to the threats which are related to "Update process"

Table A1 reference	*Threats to "Update process"*	*Ref*	*Mitigation*
12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	M16	Secure software update procedures shall be employed
12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware		
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact		
12.4	Compromise of cryptographic keys of the software provider to allow invalid update	M11	Security controls shall be implemented for storing cryptographic keys
13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	M3	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP

3. Mitigations for "Unintended human actions facilitating a cyber attack"

   Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack" are listed in Table B3.

Table B3
Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

Table B4
Mitigation to the threats which are related to "external connectivity and connections"

Table A1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	M20	Security controls shall be applied to systems that have remote access
16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)		
16.3	Interference with short range wireless systems or sensors		
17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection	M22	Security controls shall be applied to external interfaces
18.2	Media infected with viruses connected to the vehicle		
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	M22	Security controls shall be applied to external interfaces

5. Mitigations for "Potential targets of, or motivations for, an attack "

Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

Table B5
Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack"

Table A1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
19.1	Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
19.2	Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
19.3	Extraction of cryptographic keys	M11	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules
20.1	Illegal/unauthorised changes to vehicle's electronic ID	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
20.2	Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend		
20.3	Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP. Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information
20.4	Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)		
20.5	Unauthorised changes to system diagnostic data		
21.1	Unauthorized deletion/manipulation of system event logs	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
22.2	Introduce malicious software or malicious software activity	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
23.1	Fabrication of software of the vehicle control system or information system		
24.1	Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	M13	Measures to detect and recover from a denial of service attack shall be employed
25.1	Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	M7	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP

Table A1 reference	*Threats to "Potential targets of, or motivations for, an attack"*	*Ref*	*Mitigation*
25.2	Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.		

6. Mitigations for "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

   Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened" are listed in Table B6.

Table B6
Mitigations to the threats which are related to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"

Table A1 reference	*Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"*	*Ref*	*Mitigation*
26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption	M23	Cybersecurity best practices for software and hardware development shall be followed
26.2	Insufficient use of cryptographic algorithms to protect sensitive systems		
26.3	Using deprecated cryptographic algorithms		
27.1	Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack	M23	Cybersecurity best practices for software and hardware development shall be followed
28.1	The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity testing with adequate coverage
28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, …) can permit an attacker to access ECUs or gain higher privileges		
29.1	Superfluous internet ports left open, providing access to network systems		
29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages	M23	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity best practices for system design and system integration shall be followed

7. Mitigations for "Data loss / data breach from vehicle"

Mitigations to the threats which are related to "Data loss / data breach from vehicle" are listed in Table B7.

Table B7
Mitigations to the threats which are related to "Data loss / data breach from vehicle"

Table A1 reference	*Threats of "Data loss / data breach from vehicle"*	*Ref*	*Mitigation*
31.1	Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.

8. Mitigations for "Physical manipulation of systems to enable an attack"

Mitigation to the threats which are related to "Physical manipulation of systems to enable an attack" are listed in Table B8.

Table B8
Mitigations to the threats which are related to "Physical manipulation of systems to enable an attack"

Table A1 reference	*Threats to "Physical manipulation of systems to enable an attack"*	*Ref*	*Mitigation*
32.1	Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack	M9	Measures to prevent and detect unauthorized access shall be employed

Part C. Mitigations to the threats outside of vehicles

1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

Table C1
Mitigations to the threats which are related to "Back-end servers"

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
1.1 & 3.1	Abuse of privileges by staff (insider attack)	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack
1.2 & 3.3	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data

2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	M4	Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance
3.5	Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)	M5	Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP

2. Mitigations for "Unintended human actions"
   Mitigations to the threats which are related to "Unintended human actions" are listed in Table C2.

Table C2
Mitigations to the threats which are related to "Unintended human actions"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

3. Mitigations for "Physical loss of data"
   Mitigations to the threats which are related to "Physical loss of data" are listed in Table C3.

Table C3
Mitigations to the threats which are related to "Physical loss of data loss"

Table A1 reference	*Threats of "Physical loss of data"*	*Ref*	*Mitigation*
30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft	M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5
30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues		
30.3	The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example)		

ZENZIC

SELF-DRIVING REVOLUTION