Connected and Autonomous Vehicle Innovation: Approaches to Navigating the Hazards

Juliet Flavell

Technical Report

RHUL–ISG–2020–3

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student name: Juliet Flavell

Student number: 100887542

Supervisor: Professor Paul Dorey

Connected and autonomous vehicle innovation:

approaches to navigating the hazards

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:

Acknowledgements

I would like to extend my thanks and appreciation to the experts who agreed to be interviewed to share their valuable expertise and opinions:

Peter Davies, Thales

Conrad Downes, FIS

Professor Luciano Floridi, Oxford Internet Institute

Durgesh Gaitonde, Balfour Beatty

Ben Gardner, Pinsent Masons

Stephen Gibson, SLG Economics

Philip Pfeffer, Herbert Smith Freehills

Charlotte Walker-Osborn, Eversheds Sutherland

Peter Wood, Barnes Wood Consulting LLP

I would like to thank those who shared their expertise via email correspondence:

Andy Moattari, BCS IRMA

Professor Stephen Wolthusen, Royal Holloway, University of London

I would like to thank my supervisor, Professor Paul Dorey, for his engagement and availability throughout.

Finally, I would like to express my biggest love and thanks to my partner Derek and our children, Beth, Dan, Rob and Becca, for their constant support throughout my MSc studies.

Contents

List of figures

List of acronyms

Acronym	Organisation
ADAS	Automatic driver assistance systems
ASIL	Automotive Safety Integrity Level
Auto-ISAC	Information Sharing and Analysis Center (US)
BIS	Department for Business, Innovation and Skills
CAN	Controller Area Network
CAV	Connected and autonomous vehicle
CCAV	Centre for Connected and Autonomous Vehicles
CiSP	Cyber Security Information Sharing Partnership
CPNI	Centre for the Protection of National Infrastructure
DARPA	Defense Advanced Research Projects Agency (US)
DfT	Department for Transport
ECU	Engine Control Unit
ENISA	The European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
HARA	Hazard and risk analysis
LiDAR	Light Detection and Ranging
IoE/IoX	Internet of Everything (communications)
IoV	Internet of Vehicles (communications)
ITS	Intelligent transport systems
MaaS	Mobility as a Service
NCSC	National Cyber Security Centre
NHTSA	National Highway Traffic Safety Administration (US)
NIC	National Infrastructure Commission
OBD	On board diagnostics
OEM	Original equipment manufacturer
OICA	International Organization of Motor Vehicle Manufacturers
SAE	Society of Automotive Engineers (US)
SAL	Security Assurance Level

SMMT	**The Society of Motor Manufacturers and Traders**
SoS	Systems of systems
SRA	Security Reference Architecture
STPA-Sec	System-Theoretic Process Analysis for Security
TRL	Transport Research Laboratory
NIC	National Infrastructure Commission
NIS Directive	Network Information Security Directive
UNECE	United Nations Economic Commission for Europe
VANET	Vehicle Ad-hoc Network
V2IoT	Vehicle to IoT (communications)
V2V	Vehicle to vehicle (communications)

Executive summary

The government has set 2021 as its target date for fully autonomous vehicles to be in use on roads in the UK. This project investigates whether the approaches being adopted to security and risk assessment are effective and whether there can therefore be assurance of security. A unique set of cyber security vulnerabilities and requirements arises due to the impact of the unprecedented scale and complexity of CAV systems both in isolation and as nodes in the intelligent transport networks they rely on. Existing security techniques may not suffice but the need for advanced techniques may not yet be fully understood and budgets may not be available. Although broad initiatives are now in place at government level, the pace of change may not be fast or broad enough to address the risks and opportunities of CAVs. The expertise needed to address all the challenges spans many different disciplines. Safety will rely on security and the two disciplines should work together but there may be a culture clash due to their differing approaches. Although a start has been made to update legislation, the existing legislation and standards framework do not yet accommodate CAV implementation adequately. This uncertainty may stifle innovation. Due to the challenges of solving the above unique set of problems associated with the CAV domain, the target of 2021 may not be achieved.

Introduction to the project topic and method

My motivation for choosing this project topic stems from reading about the government's ambition to have fully autonomous vehicles driving on UK roads by 2021. This led to a curiosity about a future with driverless cars and smart cities where cutting-edge technology will provide new models of on-demand transport and mobility services fuelled by data. As this report is being written, OEMs are launching cars with new features including mobile phone connectivity and autonomous driver assist features like remote control parking. Development towards autonomy seems to be in the fast lane, but how will the hazards be navigated?

This is the problem I would like to investigate: connected and autonomous vehicles (CAVs) are expected to be operating on UK roads within a few years. As they are computer systems, CAVs will rely on being secure to be safe. How will this security be assured?

I begin by investigating plans, motivations, entities involved, progress to date and the predicted benefits and risks. Next I examine how CAVs work both as autonomous machines and as connected devices, exploring some of the connections and infrastructure they will depend on and the challenges these will give rise to. I then look briefly at their vulnerabilities in order to understand possible approaches to securing them. I look at the professional disciplines which will be responsible for this and how their approaches differ. I then move on to investigate which laws, regulations and standards might influence CAV development and operation and ultimately their safety and security. Finally I investigate approaches to assessing the risks of highly complex and interconnected systems to assesses differences and similarities.

My method of investigation was firstly to research facts, plans and analysis by reading publications from the government, automotive industry, the legal profession and official bodies including those responsible for transport, infrastructure and cyber security. I then read academic papers and research investigating the vulnerabilities and risk methods.

I secondly conducted semi-structured interviews to seek the opinions of experts. These were conducted with professionals specialising in different fields of security (automotive, business continuity, information assurance and penetration testing), law (commercial law with expertise in autonomous vehicle technology, product liability and technology law and automotive technology) and other disciplines (economics and philosophy and ethics of information) for wider perspectives. The diversity of experts reflects the cross-disciplinary nature of the CAV domain.

Section 1: Progress and motivations

Introduction

In this section I examine the plans for the development and introduction of CAVs in the UK by the target date of 2021. I ascertain the motivations, identify the main entities involved and examine the predicted benefits to safety, security and the economy as well as considering the risks and challenges and briefly look at some of the associated ethical questions which arise.

Internet research was used to develop my understanding of the background to CAV development including identifying the industries, entities and expertise involved by researching government and industry strategies and publications. It was clear the CAV domain extends well beyond the automotive industry, with lawyers and insurers heavily involved. I also read analysis of and predictions about the future of CAVs by consulting and law firms. This enabled identification of some of the entities, existing and newly-formed, which have been given a remit for cyber security and enabled an examination of their output for frameworks, guidance and timelines. I searched for security and automotive industry opinions on the most relevant security issues. I also used data from semi-structured interviews conducted with experts in law, security, economics and ethics to ascertain their overall views of CAVs, particularly the benefits and what might prevent them being implemented by 2021.

Industrial Strategy 2017

In its 2017 *Industrial Strategy* the government announced long-term plans to build "a Britain fit for the future" and announced the *Future of Mobility Grand Challenge* [1]. The Strategy sets out to create economic growth after the UK's exit from the European Union, helping UK businesses create employment. It also emphasises the positive impact of strategic state intervention and encourages collaboration between government and the private sector, supported by a Challenge Fund matched by commercial investment.

The *Mobility Challenge* declares the desire to position the UK as a world leader in shaping the future of mobility along with the ambition to put fully self-driving cars on the UK roads by 2021 [2]. The target date of 2021 was affirmed by Chancellor Philip Hammond in the Autumn Budget 2017 [3] [4]. It has subsequently been reaffirmed in July 2018 [5].

Turning to who might partner with the government to help deliver this vision, the Strategy describes how new disciplines and collaborations are expected to emerge to ensure goals like vehicle safety and security.

Research into adopting cutting-edge technologies for use in cars started in the 1950s in the US when technologies developed in the Second World War were used [6]. The Defense Advanced Research Projects Agency (DARPA) launched a 150km autonomous vehicle Grand Challenge in 2002 with the aim of adapting the technologies developed for use by the military. By 2007 there had been many entrants with winning vehicle entries from Stanford University and Carnegie Mellon.

In 2009 Google employed researchers from the winning DARPA teams and entered the market. An announcement by the head of Google X, its secret project division, read: "We have developed technology for cars that can drive themselves" [7]. Google's competitors including Tesla, Apple and Uber are also very active in this space, partnering with automotive players among others to leverage their technology advantage by aiming for higher levels of autonomy from the start.

Evidence from interview: some of the most successful technology companies are relatively new entrants operating for under 10 years old eg. Uber, and if this continues there could be an early winner in the CAV domain too.

Official entities

Research into the overall plans for CAV development identified the following entities of relevance and here their roles are briefly introduced.

Department for Transport (DfT)

DfT is the overarching government department with responsibility for steering transport policy and guidance and funding local authorities to operate roads. Their primary priority is to boost economic growth and opportunity. They also identify new major transport schemes. One of their CAV actions was to determine the need to review insurance and the Highway Code [8].

InnovateUK

Formerly the Technology Strategy Board, InnovateUK manages investment of millions of pounds in collaborative R&D projects, working with DfT and Department for Business, Innovation and Skills (BIS) [9]. They also chose the winners for investment in CAV testing: the GATEway Project in Greenwich, UKAutodrive in Milton Keynes/Coventry and VENTURER in Bristol [10].

Centre for Connected and Autonomous Vehicles (CCAV)

CCAV is part of the DfT and BIS and was established in 2015. It works with industry, academia and regulators to try to make the UK one of the top global seats of CAV development. One of its four objectives is cybersecurity [11].

National Infrastructure Commission (NIC)

NIC's remit is to provide independent, strategic analysis and advice and as such it is active in determining the strategy for the infrastructure needed by CAVs and intelligent transport systems (ITS) [12].

Centre for the Protection of Critical National Infrastructure (CPNI)

CPNI provides security advice relating to protecting national infrastructure including transport and communications, both of crucial importance in the CAV domain [13].

National Cyber Security Centre (NCSC)

NCSC, part of GCHQ, helps to protect critical services from cyber attacks as well as managing major incidents and improving security generally across the UK. They have co-authored some of the only official advice on securing CAVs to date [14].

House of Lords

The House of Lords publishes records of activity and the evidence of witnesses in its consultations and so this is a good source of information. The Science and Technology Committee was involved in a general review in 2013 which concluded that verifying safety and reliability of CAVs was a main policy challenge [15]. In 2017 a subsequent investigation resulted in key recommendations relating to cyber security [16]: funding should be allocated through the Cyber Science and Technology Strategy; cyber security should be an integral part of the review of the regulatory framework; efforts should be coordinated by CCAV and involve NCSC; and progress should be made on the international stage to put cyber security on the agenda and establish global standards [11]. As will be demonstrated in Section 3, it is not clear that the second of these recommendations has been met.

As shown in Section 2, CAVs are highly dependent on internet connections which are part of critical information infrastructure. Review of the *National Cyber Security Strategy 2016-2021* highlights threats to the interconnected systems that are fundamental to society, health and welfare [17]. Its approach to defend, deter, develop and build international allegiances approach could be a useful way of analysing techniques for CAV security. It was unclear exactly which government departments had contributed to this strategy and consequently which departments might be good

sources of further information about the alignment of the *National Cyber Security Strategy* and CAVs.

Testing

CAVs on public roads in the UK are still at the testing stage. Heathrow has for some time been running autonomous pods on its private land on a dedicated track from a car park to Terminal 5, connecting them wirelessly to a central server control room [18]. Testing of truck platooning is underway but is beyond the scope of this project [19].

In the US testing has progressed further. For this reason I have included some of the approaches to safety, security and risk assessment adopted in the US to see what lessons have been learned there which could be applied in the UK.

In the UK trials undertaken by consortia part-funded by government innovation investment are addressing amongst many other challenges those surrounding security. Consortia members are from various industries and professions including automotive, technology, communications, insurance, legal, academia and local authorities. I found no direct evidence of commercial or government security involvement.

In terms of their security findings, the security challenges the DRIVEN project sets out to address for example have been reported [20][21]. These include communication and data sharing between connected vehicles, risk profiling and the new cyber security challenges this level of data sharing will bring. DRIVEN will also define common security and privacy policies related to connected and autonomous vehicles. Set to finish in 2019, details of the security findings are not being made public while it is underway and so could not be used for this MSc project.

Other trials are now complete. While underway the GATEway consortium for example published an article about cyber security [22]. This highlighted the dual nature of CAVs which due to their high levels of connectivity in a "massive and distributed network of things including other cars, buildings, IoT devices, knowledge repositories and databases" could potentially eliminate accidents but could also amplify the potential negative impacts of accidents. The article warns that which outcome is more likely depends on the design of the whole car as a system and whether security is embedded in CAVs from the start of the development lifecycle. It also argues that there is a risk of security being played down because security is not the primary purpose of the car or because security incidents are rare. This was an insightful article but attempts to uncover further output on the security outcomes of the GATEway trial were unsuccessful. This could be concluded to be deliberate, to avoid giving away intelligence to competitors or adversaries.

Opportunities

The government predicts major potential benefits which could profoundly change our lives for the better, by making road transport safer, smoother and smarter [8].

Analysis by expert law firms was reviewed [23], [24]. This concludes population growth is causing us to reach capacity limits in urban areas which will have a negative impact on congestion, safety and welfare. In addition the need to support societal trends such as the move to shared ownership and the increase in "as a service" offerings like Mobility as a Service (MaaS) are stressed.

Evidence from interview: personal ownership of CAVs may decline. Instead commercial fleets of CAVs for hire may be deployed, maybe with enterprises owning their own fleets. In this model high fixed costs would be accompanied by low marginal costs. New business models may emerge and personalised advertising to passengers is likely to be lucrative along with attractive SLAs tailored to different groups of customers.

The opinion expressed by the interviewee above appears to be borne out by the most recent DfT consultation seeking opinions on new models of delivery vehicles for cities, aiming to transform last-mile deliveries [25]. This could be also construed to show that the government is refining the scope of its mobility aspirations to focus on more specific problems rather than aiming for widespread adoption. The benefits of CAVs described in this consultation include the ability to remove parking spaces from city centres to reuse for housing. A blurring of public and on-demand transport is anticipated along with shared mobility, and new business models like MaaS. Cyber security is mentioned briefly as a challenge along with safety and privacy.

Based on research into other transport and infrastructure sources on the internet, the main predicted benefits can be summarised as follows [12], [26], [27], [28]:

For society

- Towns and cities could be redesigned if there are fewer vehicles to park;
- Better use of road space could lead to less congestion and fuel use;
- CAVs could increase existing network capacity and improve accessibility for groups such as the young, the elderly and disabled;

For the economy

- Time spent behind the wheel could be put to better or more productive use leading to overall productivity gains;
- By 2020 the UK will be producing 2 million vehicles a year;

For safety

- 90% of UK road casualties in 2015 (1,732 fatalities and 22,137 serious injuries) are believed to have been caused by driver error;
- CAVs could significantly reduce road casualties caused by driver error.

Evidence from interview: the significant reduction in accidents is a compelling motivation for the authorities to introduce CAVs. Even though they may still cause some accidents because of security vulnerabilities, what will matter more is the level of reduction. Asking manufacturers to eliminate all accidents is too unrealistic.

Risks

KPMG casts some doubt on the UK being able to achieve its goal of attracting global CAV development [29]. Its Readiness Index compares the progress of the countries which are developing CAVs. The UK is positioned fifth out of twenty, scoring highly for technology and innovation partnerships, R&D, policy and regulation. Infrastructure and 4G coverage reduce its readiness score.

As will be seen in Section 2, CAVs will rely on roadside infrastructure and network coverage which is not yet fully in place.

Evidence from interview: specific "hotspot" cities will be early adopters as happened with wifi, to position themselves as ahead. While there are risks to being early adopters, at the same time cities could subsequently gain from helping to coordinate others.

My research into analysis of risks relates to negative impacts on congestion and health more than safety or security concerns [12], [30], [31].

The Parliamentary Office of Science and Technology (POST) review identified network coverage and standards as key barriers to adoption along with system incompatibility [15]. As early as 2013 this stressed that systems will need to fail safely and have multiple backup systems in the event of communication systems not being available. Risks arising from the reliance on data generated by

other vehicles were identified as well as privacy questions about access to the data and its use. The establishment of new standards was recommended for verifying the reliability of software.

There are also risks due to the dependence of CAVs on critical information infrastructure. NCSC released a joint statement with the FBI recently stating the Russian Government has been attacking critical network infrastructure devices worldwide [32]. The attacks succeeded because of the use of legacy unencrypted protocols, insufficiently hardened devices and end-of-life devices no longer supported by manufacturers. Sophisticated techniques such as zero days and malware are not needed. This raises an interesting point for CAV risk assessment: CAVs will depend on networks which are known not to be safe and which are arguably too distributed to be secured and are not auditable.

Focus on cyber security

CCAV is working with the CPNI and NCSC in a cyber security capacity to engage with industry and raise awareness [33]. This includes promoting best practice such as automotive Information Exchanges and intelligence sharing via the Cyber Security Information Sharing Partnership (CiSP). The high-level approach to CAV security proposed is to:

- Understand the cyber threat and the vulnerabilities for the transport sector
- Mitigate cyber risks and take appropriate action to protect key assets
- Respond to cyber incidents effectively and ensure that lessons are learned
- Promote cultural change, raise awareness and build cyber capability

Further research into progress on these aims found a lack of published output from the authorities beyond the *Key Principles of Cyber Security for Connected and Autonomous Vehicles*, which will be examined in Section 3.

Some references to and concerns about cyber security were found in the early plans for CAVs.

Evidence was given to the *Connected and Autonomous Vehicles: The Future?* consultation in which concerns were raised about a number of cyber security issues [34], [35]. 2030 was suggested by one witness as the target date rather than 2021 with one of the challenges being lack of trust with regard to cyber security, and specifically what CAVs will do in specific situations. Another warning given was that security is an on-going challenge which it is not possible to fix permanently.

The *Connected and Autonomous Vehicles: The Future?* report states that the Transport Select Committee was given evidence that CAVs could be used for criminal or terrorist purposes including as car bombs and driving into crowds of people. Witnesses stressed that the government should take a strong coordinating role in CAV cyber security, with input from industry experts and stakeholders. In particular, security should not be left to industry. This view was reiterated by an interviewee.

Evidence from interview: risk methods should not be left to industry to develop themselves. When a minimum cyber security standard is eventually imposed on manufacturers, self-certification should be avoided.

A note on ethics

While researching questions of risk and opportunities it was hard to avoid questions of ethics in implementation, in view of the fact that security is so hard to get right, as the data about data breaches proves [36]. Thorny questions also arose about how and when to really be able to declare CAVs safe, apart from by conducting a risk assessment and reducing risk to acceptable residual levels.

The Royal Academy of Engineering have considered who will decide to adopt CAVs, how and when [37]. They consider who will be responsible for systems with no clear owners and suggest that autonomous systems are often seen to need to be perfect compared to the systems they are replacing. But they ask if this is really achievable, not least because they are implemented incrementally. They argue that the market should not be the dominant force and contrast this with the road infrastructure which does have a top-down system of control. But the way it happens in practice is that new technologies are adopted and then questions of interoperability and harmonisation have to be hammered out later. Their conclusion is that it is difficult to know how best to achieve this.

An academic paper argues that a new discipline of data ethics has emerged [38]. This has arisen because of moral questions around the use of data, algorithms and the practices accompanying them. This differs from the existing field of information and computer ethics insofar as it introduces new moral dimensions of data, and significantly, data that never becomes information but which nevertheless supports actions or generates behaviours.

Evidence from interview: the right conversations are not yet being had. CAVs will bring many benefits but at this point there is a lack of dialogue about realistic ways of slowly introducing them in a constrained way and a focus instead on feasibility. There is also a risk of having a hybrid situation

with both CAVs and conventional cars and this raises ethical questions about isolating certain groups of people.

Evidence from interview: the trolley problem is often used as an example of a CAV ethical dilemma but in practice manufacturers would never build a system which would make that choice. Instead it would just be programmed to avoid an accident. In machine learning systems in any case it will be impossible to trace back why a particular rule has been created because these types of systems are not programmed with outcomes.

Progress and motivations: conclusions

Ambitious plans have been drawn up to introduce new modes of transport to reflect society's changing needs and expected future challenges while strengthening the economy. There are many predicted benefits although these are not guaranteed. Investment and collaboration are underway. New partnerships and consortia are being formed.

New official bodies have been formed to coordinate activities. A variety of cyber security questions were raised early on in a consultation exercise and recommendations made by witnesses. There is evidence from debates and publications that cyber security was expected to be an important element of CAV safety and the broad principles have been established upon which to build future guidance. Although CAV trials have been investigating cyber security and safety, their findings are still under wraps. There are some complex ethical issues surrounding CAVs.

Section 2: Operation, safety and security

Introduction

This section provides an introduction to how CAVs work. I examine the nature of the infrastructure they rely on to achieve autonomy and their dependencies on interconnected networks. I give an overview of their architecture in order to illustrate some vulnerabilities which might affect their safety. I also investigate additional characteristics of the CAV ecosystem which give rise to a unique set of significant challenges in their own right. I then examine the different methods of automotive engineers and security professionals in light of the need for cross-disciplinary

collaboration between automotive safety and computer security experts and investigate approaches to securing CAVs so that safety is assured.

Sources of evidence for this section were internet research for background information, reviews of academic literature for technical insight into vulnerabilities and attacks and in depth analysis by consulting firms and law firms. I also interviewed cyber experts specialising in a variety of fields of security (automotive security, information assurance, business continuity and penetration testing) who contributed insight and perspectives based on their expertise.

Definitions

For clarity the distinction between connected and autonomous vehicles is provided, as defined by Catapult Transport Systems [27]:

Connected vehicles: cars with increasing levels of connectivity, enabling communication between cars and their environment, such as infrastructure and other vehicles, about the road, traffic or weather conditions or providing a connection to wider connectivity services.

Autonomous vehicles: cars with increasing levels of automation, taking information from built-in sensors and other systems to understand their geographical position and local environment, enabling operation with little or no human input for some or all of the journey. They are also known as automated, self-driving or driverless cars.

How CAVs work: as autonomous systems

Context

Autonomous and connected features will complement and reinforce each other. The ability to send and receive data is already used by cars to operate their autonomous functions. Vehicles with limited autonomous features need not be connected, but convergence of the technologies is likely to lead to intelligent vehicles which are both connected and autonomous.

In 2014 the US Society of Automotive Engineers (SAE) published the first taxonomy of CAVs, J3016, defining six levels of vehicle automation ranging from 0 (no automation) to 5 (full automation) [39].

Cars at Levels 1 and 2 are already used on public roads and sold to the public. At these levels it is still the human who monitors the driving environment. They are increasingly augmented with advanced driver assistance systems (ADAS) [40]. These are autonomous, usually unconnected systems which provide safety enhancements using on-board technologies such as radar, cameras and infrared sensors. Currently these react in predetermined ways, to ensure the goals of safe

operation and to allow the automated control of acceleration, braking and steering for periods of time [41] [30]. In the UK this is referred to by DfT as driver assistance.

At Level 3, conditional automation, an automated driving system monitors the driving environment although the driver is still "in the loop" and must pay attention and respond quickly to alerts from the vehicle to do something or take back control.

Level 4, high automation, comes much closer to removing the human from the loop. The driver is no longer needed during specific driving tasks or use cases which the car will perform by itself. At Level 5, full autonomy, vehicles are able to drive themselves without human intervention, performing an end-to-end driving task wholly independently [26]. The key distinction between Levels 4 and 5 is that at Level 5 the driver can fully disengage from vehicle operation.

The J3016 Levels are still widely used but have been further refined as CAV development has progressed. Figure 1 illustrates the human or autonomous driver's role more clearly. Specific driving tasks or use cases are set out eg. Urban Automated Driving. Other use cases include entertainment and information (infotainment) systems and intra-vehicular communication [42]. Use cases are also a useful tool for security and risk management frameworks [43].

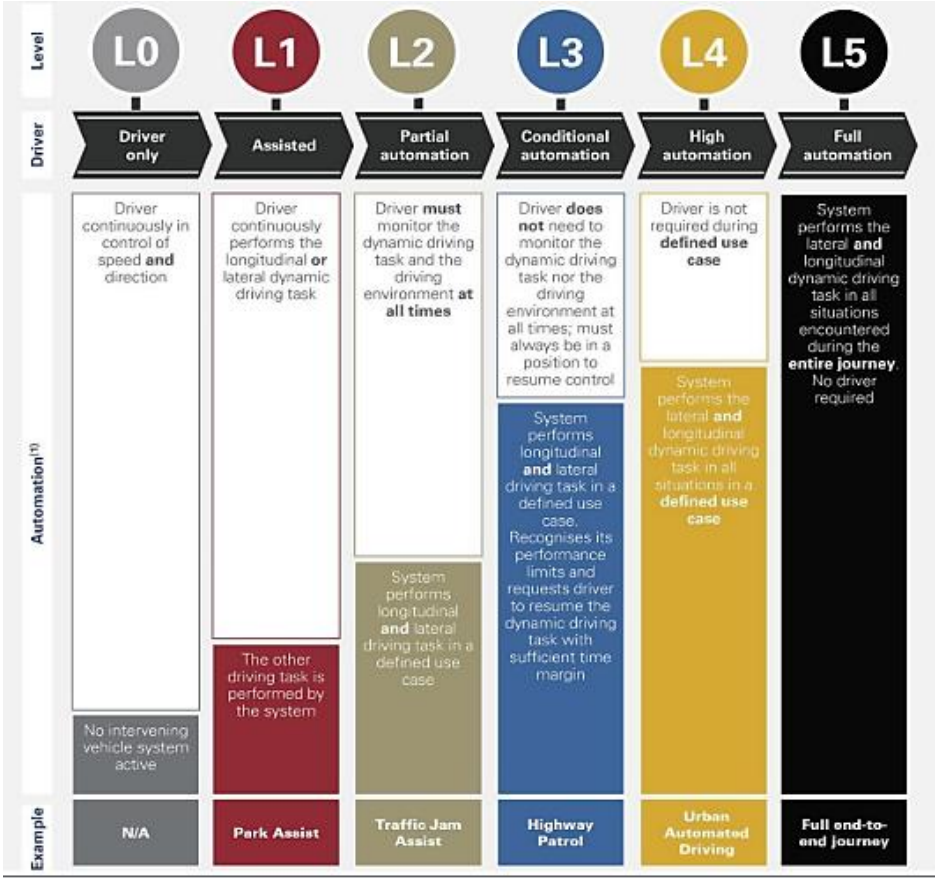


Figure 1: OICA's Levels of Automated Driving, based on SAE J3016 (SMMT) [26]

CAV technologies

CAVs are highly complex cyber physical systems which use a variety of technologies to perform driving tasks. Figure 2 shows the different technologies and components which are combined in CAV architecture and highlights the complexity of the systems to be secured in terms of their variety and different physical interfaces. A paper from the 2015 IEEE Transactions on Intelligent Transportation Systems journal provides an overview of the types of components and control systems involved: [44]

External sensors: examples are radar, engine control sensors, tyre-pressure monitor systems and LiDAR (Light Detection and Ranging) [7];

Internal sensors: examples are breath analysis to detect alcohol and interpret tone of voice;

GPS: providing absolute position data for location and navigation information and timing references for communications;

Inertial measurement units: examples are accelerometers and gyroscopes which monitor the environment and detect gradient for example, adjusting speed accordingly.

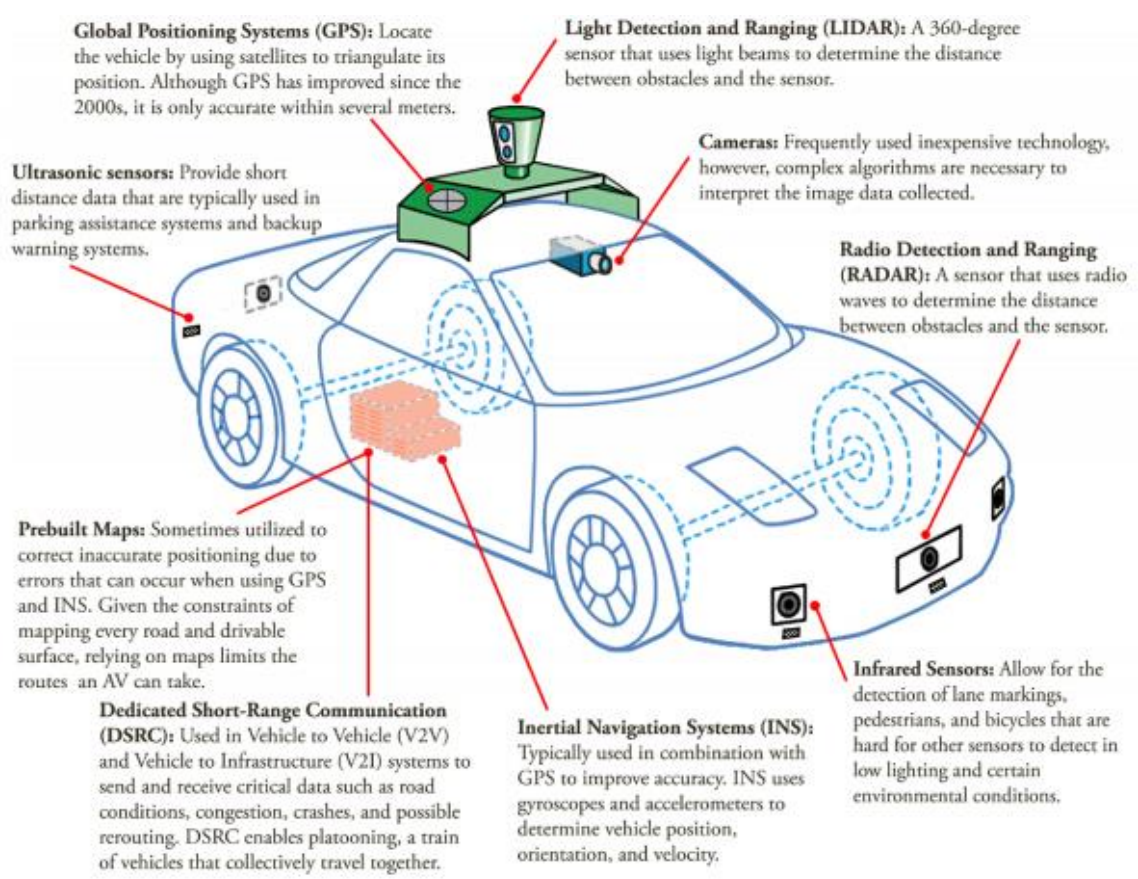


Figure 2: Autonomous vehicle technologies (University of Michigan) [45]

Vehicle control modules: embedded systems which are Engine Control Units (ECU), for example the electronic brake control module, engine control module, heating and ventilation modules.

The internal architecture which the ECUs share is particularly significant from a security point of view as it is a vulnerability [41], [46]. The ECUs typically use a multi-master serial Controller Area Network (CAN) bus to allow micro-controllers to be connected by a twisted pair cable and to communicate by exchanging short messages. Messages are broadcast to every device on the bus with no identification of source or destination of messages. Both the high-speed and low-speed layers are connected with a gateway bridge to route selected data between them. Malicious packets which enter the low-speed CAN layer with lower security requirements (eg. infotainment systems) can be transferred into the high-speed CAN layer so this can be an effective attack vector in order to penetrate further into critical systems. This demonstrates that although the ECU system is complex, the connection providing entry to it is not therefore every communication pathway should be properly protected and authenticated [47] [44].

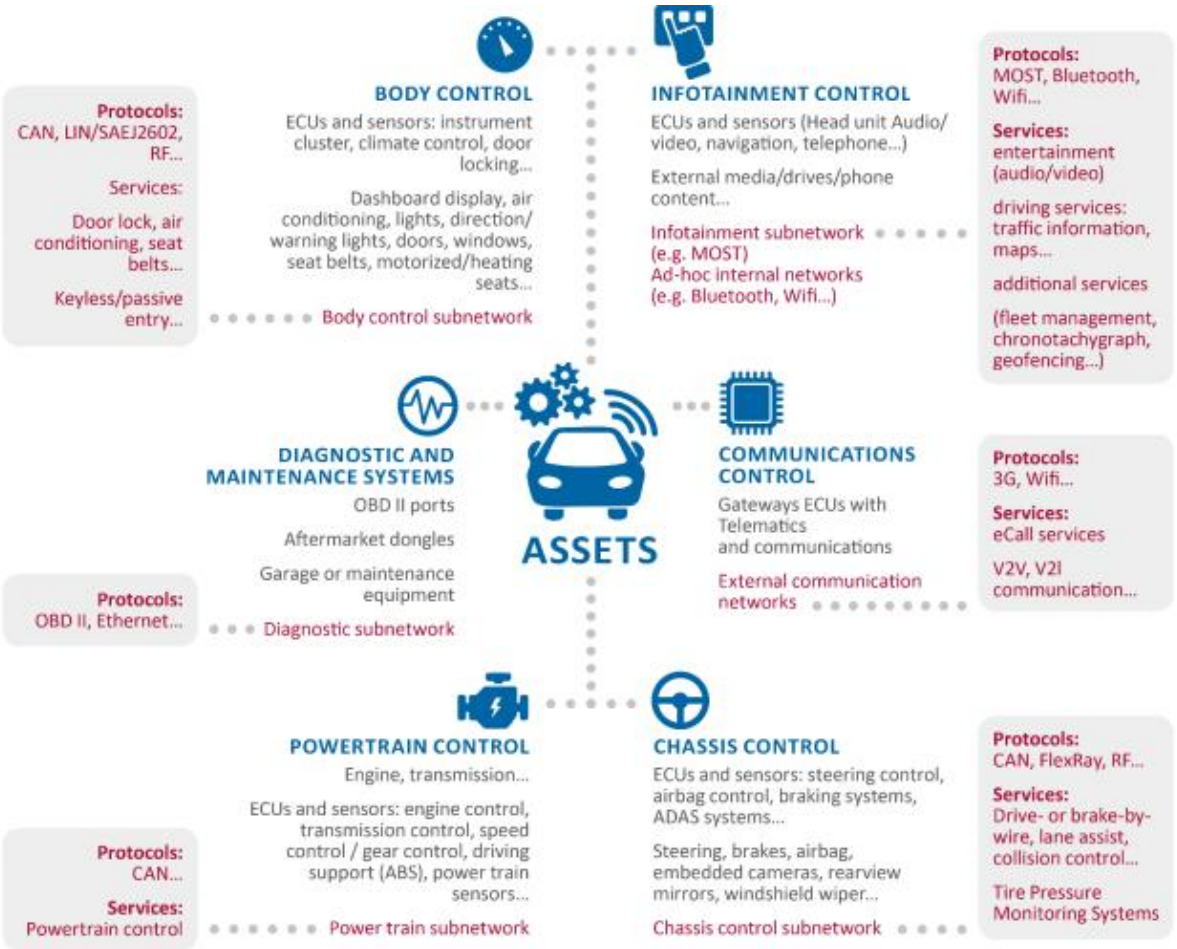


Figure 3: Smart cars assets (ENISA) [42]

Figure 3 shows an abstraction of the architecture of a CAV, its sub-networks and the variety of protocols and services in use. The complexity is clear. The entry point for wired connections is the on-board diagnostics (OBD) port which allows a cable to be connected to it for maintenance. The single gateway ECU which all traffic passes through is shown as communications control.

The IET explain in simple terms the communications architecture of a CAV beyond the CAN bus which connects ECUs, sensors and actuators [48]. The other sets of communication systems are internet access and internal. The types of external access using the internet are complex: vehicle-to-vehicle (V2V) for wireless communications between cars; and vehicles exchanging information as part of the IoT (V2IoT). Other newly-emerging communication types include vehicular ad hoc networks (VANETs), internet of vehicles (IoV) and internet of everything (IoE or IoX). From my research it appears that there is no convention for defining connections and that defining different communications is an end in itself for researchers [39], [49]. This has led to a situation where CAVs are using communications which cannot adhere to any standards because these do not yet exist. As many CAVs will be exported it is important that there is interoperability with international infrastructure, which could be partially achieved through the international agreement and standards the government is seeking to participate in and accelerate.

Also on the theme of interoperability, its importance was made clear in the investigation of the fatality caused by a Tesla when using its autopilot. Although a “black box” was being used for data recording, Tesla’s proprietary software slowed the investigation [50].

How CAVs work: as connected systems

Review of the literature on how CAVs work revealed that they will increasingly communicate and exchange information wirelessly beyond their physical boundaries with other entities such as vehicles, infrastructure, external devices and networks. This connectivity as seen will be needed for automation. Vehicles will make decisions based on data from the on-board sensors which are surveying the surroundings plus data received wirelessly from road infrastructure and other vehicles [26], [41], [51]. A constant reliable exchange of information is therefore needed to make decisions to protect passengers as well as other road users.

Disabling the internet connection while not in use will not be an option because as of 2018 all new cars already have to have wireless connectivity to use the EU eCall service which helps emergency services locate the scene of an incident quickly [48].

The nature of the CAV network and its interdependencies

As seen, CAVs operate in networks which are defined in different ways. An academic paper showed that these in combination form the IoV which is defined as a set of large-scale concurrent and distributed systems whose components are complex systems themselves, or Systems of Systems (SoS) [52]. They differ from conventional computer systems in that they have a collaborative nature and collectively have a shared purpose. The fact that some elements of transport SoS are mobile also distinguishes them from other systems and introduces vulnerabilities partly because of the harm they could potentially do to their surrounding environment and partly because they are more physically accessible to attackers. Also noteworthy is that the dynamic location and surroundings hugely complicates the risk assessment process.

An example of a transport SoS is a traffic control system consisting of vehicles, traffic lights and weather reporting systems where collective outputs could be used to predict road congestion which cars would then use as input to determine their route.

Researchers have identified some key future challenges for CAV security based on their connectivity [41], [46], [53], [54]:

- The number of connections on the IoV will continue to increase as more distributed road-side and centralised infrastructure is added. The complexity of systems will necessitate increased computational functionality. This, combined with increased connectivity, will increase the attack surfaces - therefore arguably also the likelihood of attacks;

- When operating at speed, say on a motorway where CAVs and conventional vehicles might co-exist, there is a need for reliable, real-time information about the surroundings. CAVs depend on data for safe operation. The CAN bus does not use data origin authentication. The vulnerability of wireless communications to cyber attack has also been well-documented. The radio spectrum they use is restricted to specific frequencies for specific functions, making the task of the attacker simpler.

Evidence from interview: SoS have caused a significant new paradigm to emerge: safety-critical systems exist where no single entity is able to have control over - or even full knowledge of - what the whole interconnected system is doing. This hugely complicates the task of securing individual systems and makes securing the entire system impossible.

Evidence from interview: getting infrastructure in place is very slow in the UK due in part to all the regulations. In other countries - our CAV competitors - where the infrastructure is being built for

the first time, and where there is less regulatory burden, such as China, the necessary infrastructure can be implemented more quickly.

The significance of data

Based on my research, the role and implications of data cannot be stressed enough. For example IBM now consider cars to be data centres on wheels [55].

Broadly speaking there are two types of data:

- Diagnostic: this is the data CAVs will rely on to operate safely and will be used for real-time decision making. This must be secured to ensure integrity in order to assure safety.
- Personal: this is the data CAVs will generate which will reveal information about the passengers and must be protected to ensure privacy.

Evidence from interview: the scale and quantity of data is unprecedented and it will be the real currency of CAVs. This will lead firstly to very practical difficulties in acquiring and storing the data. Secondly the data will be where OEMs will create value although there is some uncertainty over who will own it with some taking the view that if it is not protected or encrypted, it is deemed to have been given away.

Additional characteristics

Below some other factors are outlined which contribute to the unique cross-disciplinary nature of CAVs and which support the view that the task of securing them is highly complex both in terms of validating the software and keeping them updated.

Complexity

The components and architecture of CAVs are complex systems in their own right and this complexity is amplified when they become components of wider networks which are increasingly part of global information and management networks. Figure 4 shows the number of lines of code in a typical car (at least 100 million) compared with other cyber physical systems.

Evidence from interview: this number of lines of code make software difficult to validate. Even if verified in isolation, this is of limited use when it is combined with other code, leading to unknown vulnerabilities. Vehicles will not only contain many terabytes of data and many million lines of code, but also due to the number of components will have a security baseline which will need to be updated on an almost continuous basis; an unprecedented requirement. Recognising the complexity of interconnected systems is crucial in designing security and resilience.

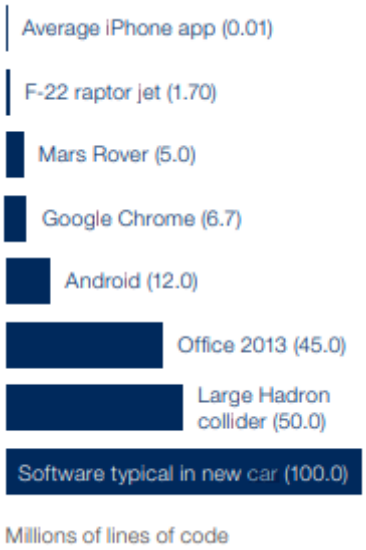


Figure 4: Size of codebase for popular software (WEF/BCG) [56]

Evidence from interview: vehicle control systems are full of interdependencies with nested levels and cascading failures so an attacker can be quite far removed. They are difficult to troubleshoot because of lack of linearity and a loop nature

Outsourcing and distributed supply chains

OEMs use tier suppliers, who are themselves part of wider supply chains. Third party manufacturers often only deliver exactly what has been specified in their contract, without adding extra security features [41][44]. Also, as lawyers point out, large amounts of data must often be shared with suppliers presenting privacy challenges requiring security measures to be adopted [24]. If liability remains with car manufacturers, as will be examined later, they will be required to ensure that the whole supply chain adopts best practice which would be difficult [23].

Machine learning

As automation increases, decision-making will need to mimic human intelligence to interpret movements of pedestrians or actions of other road users [57]. Machine learning is proposed to fulfil this function. It works by coding a framework algorithm into a computer and this being modified by the computer itself based on learning. The large amount of data provided by CAVs is a significant factor in increased use of machine learning. A key challenge will be verifying the integrity of machine learning algorithms, which will depend on the integrity of the data they use which will be input from their immediate surroundings and communications received from elsewhere which as shown is vulnerable to compromise.

Evidence from expert: developers have the right intentions but do not apply a criminal mindset early enough. The standard approach to security is to try to make a system work instead of trying to break it at every stage which is a better approach.

Patching

Given the complexity of SoS, vulnerabilities are likely to be discovered almost continuously so updates will be needed continuously. It remains to be seen how patches will be distributed. The government's recent review concluded that the new single insurer model means drivers will be liable if they make unauthorised modifications or fail to update software. While this puts the onus on the user it does also mean manufacturers must make updating easy [24]. The current method of monitoring safety, the MOT, will need to change [23].

Evidence from interview: testing of patches is unviable because of the need to distribute them immediately before they too become redundant. An alternative is highly accelerated testing using simulators followed by monitoring once the update is live. In practice, it may be that a manufacturer has every reason to believe a fix will be error-free based on their expert judgement and that this, combined with an obligation to test throughout its lifecycle, will have to suffice for practical reasons.

Evidence from interview: for practical reasons there will need to be an option to install a patch at a later time but in any case patching should be performed as part of regular safety checks eg. the MOT. Remotely connecting to the vehicle to check its patching level should be a feature.

The two differing views above show the variety of opinions among professionals, and lead to the conclusion that the unprecedented complexity of CAVs is not widely appreciated even within the security profession and that commonly-used best practice security techniques and approaches may not apply in the same way within the CAV domain.

Security challenges

My conclusion from reviewing academic papers is that there are many theoretical attacks and a very broad scope for novel attacks which cannot be predicted. The literature sets out many vulnerabilities and different methods of categorising them [39], [42], [47], [47], [51], [59], [60]. The two features most susceptible to attack are the wireless communications and GPS [46].

Evidence from interview: attacks are at the implementation of standards therefore using standards to counter them is not a good approach. Different people can implement them correctly so both are doing the right thing but getting the wrong answer.

Evidence from interview: security professionals generally work from best practice and checklists but there is too much focus on checklists. These should be used as a baseline only but there will still be gaps and these should be addressed using threat-based tests.

Analysis by McKinsey suggests six areas of automotive cyber security to be considered [61]. Three relate to the lifecycle element (design, development and maintenance) and three to the ecosystem (OEM-supplier alliances, end users and government agencies). Figure 5 shows the security services they recommend for the design of CAVs. These align with some of the *Key Principles* which will be examined in Section 3; namely not relying on single points of failure (redundancy), segmenting critical systems (air gaps), building systems which can respond of non-safety critical functions fail (analog backup) and applying defence in depth techniques (cryptography).

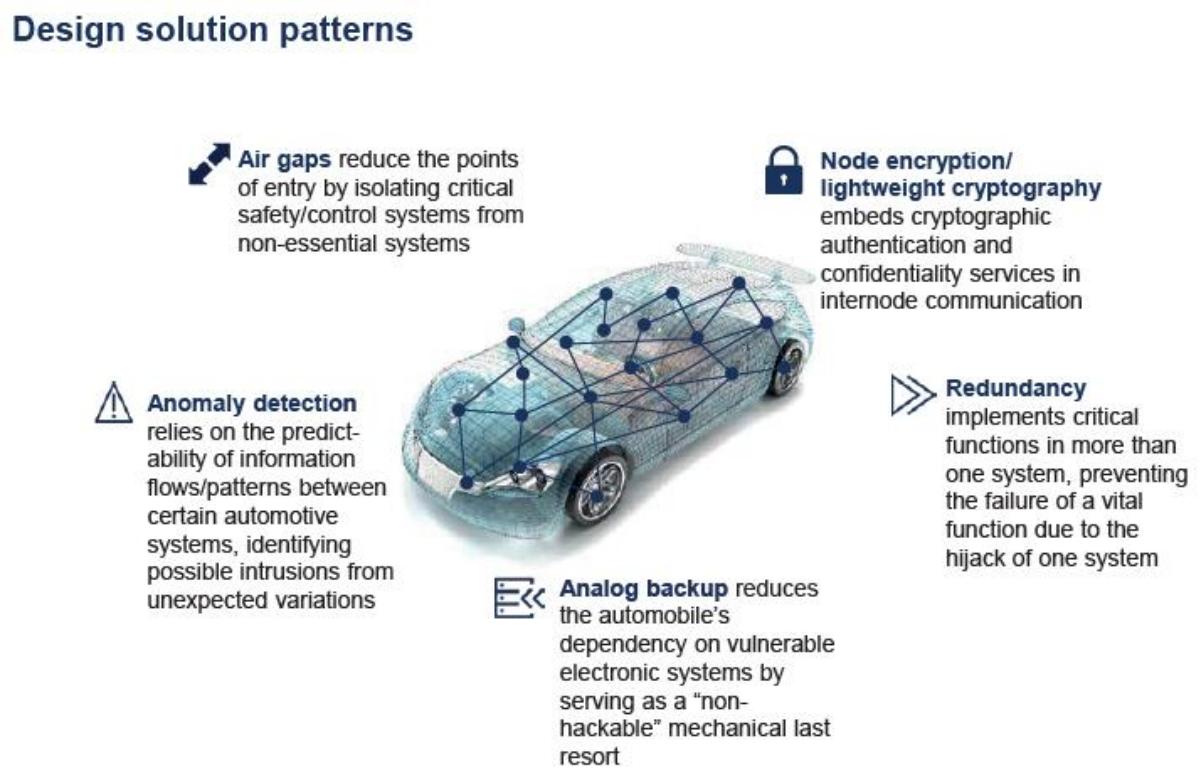


Figure 5: Design solution patterns (McKinsey) [61]

Below some attacks carried out by testers and researchers are briefly described to demonstrate what results they were able to achieve.

The Jeep attack

In the Jeep attack of 2015 researchers first connected a cable to the OBD port then later remotely exploited weaknesses in the wireless communications (no authentication or blocking of messages received by the ECUs) to take remote control of a Jeep [62] [48]. Commands from the drivers were overridden while they in the Jeep and driving it. The researchers took control of steering functions and made the fuel tank appear to be empty.

Evidence from interview: it took the highly skilled Jeep attackers six months before they were able to refine their attack sufficiently so that it would only affect a single system. Less skilled attackers accidentally affecting multiple systems would be much easier, and although unintentionally done this could have a devastating effect.

Tesla penetration testing

A team of penetration testers tested the Tesla Model S [63]. No remotely executable attacks succeeded but after physical access, they were able to gain root access to two elements of the infotainment system and use this to perform further tasks including remotely opening and closing the boot and starting and stopping the car.

RollJam

The RollJam key fob attack defeats rolling codes security used in cars by intercepting, jamming and storing signals sent by the owner's key fob while trying to unlock their vehicle. The stored codes are replayed later by the attacker to successfully unlock the car [64].

Denial of Service DoS

Interfering with low-level feedback input systems can have a significant effect on car behaviour. Research by academics has demonstrated how interfering with the inertial measurement units can make a car falsely believe it is on a slope causing it to slow down which could lead to a denial of service if the speed was very slow [41].

Evidence from interview: the complexity of CAVs means that system errors may occur. While a conventional car could pull over, an automated system can enter an unknown state or reboot, causing a DoS situation.

Merging security and safety

Automotive safety can be defined as functional safety: an electromechanical system must avoid events which will cause harm directly or indirectly to people or the physical environment nearby [65]. A system perceived to be safe is one which operates as intended in response to the inputs it receives ie. has fault tolerance [66]. A key feature of safety testing is predictability and repeatability.

Security testing via penetration testing on the other hand is about capturing the flag; crafting attacks designed to break systems and adapting and altering these until they succeed.

Evidence from interview: those who design security almost always lack the budget to test from an attacker's perspective. Within the automotive industry the cost of carrying out this exercise would affect profit but it is particularly important due to the accessibility of vehicles to attackers. Warfare techniques should be adopted because no plan survives engagement with the enemy.

A research paper from City University London sets out some of the main differences between safety and security approaches [67]:

- Use of different concepts and terminology and the lack of a shared language;
- A difference in emphasis and potential conflicts in the understanding of principles;
- Use of different underlying threat models and methodology;
- A lack of security-informed safety cases;
- The way generic and industry safety and security standards work together needs to be clarified.
- Security is a broad discipline encompassing many different approaches of value to CAV security. I asked experts from a variety of security specialisms via interviews for their thoughts on approaches to security.

Evidence from interview: within automotive manufacturing, security should not be separated from safety. There is a lack of dedicated security standards for automotives, but there is also an absence of combined safety and security practices.

Automotive Safety Integrity Level (ASIL)

ASIL is part of Hazard and Risk Analysis (HARA), used to classify risks based on the potential severity, the probability of a situation where it will arise and the controllability [52]. Vehicles must comply with the *ISO 26262 Functional Safety Standard* so manufacturers must consider specific device or system failures: the exposure, potential severity of an accident and its controllability. The output is a number representing the criticality of that part or system.

Security Assurance Levels (SAL)

There is no widely-accepted version of safety integrity levels in security [68]. This is because security applies to much wider systems with more far-reaching consequences along with a wider set of possible circumstances leading up to an event. In other words, security is vastly more complex and reducing security to a single number will not suffice.

Evidence from interview: in safety there are safety integrity levels (SIL) but not in security. "State of the art" security is based on best practice which is defined by research.

An approach has been proposed which classifies four different types of SAL: target, design, achieved and capabilities, based on different aspects of the security lifecycle. Target SALs reflect the desired level of security and are determined by a risk assessment. Design SALs reflect the planned level of security and may be revised during design as various countermeasures are tested. Eventually vendors could be required to provide them as capability SALs for their vehicles.

Security lessons learned from the trials

The Transport Research Laboratory (TRL) were responsible for safety expertise in the GATEway trials [69]. One goal was to investigate safety and cyber security to contribute to the development of codes of practice, specifications and change legislation. The project's final report outlines its findings, explaining that the tests were used to develop a comprehensive Safety Framework which can be used to assure all future AV activity. The framework is shown in Figure 6.

A copy of the framework was requested from TRL to evaluate in more detail but was not provided. The information below therefore is taken from GATEway's final project report.

The report reveals that the framework encompasses critical areas eg. site/route validation as well as delivery practices and training. It is reported to be operating as a proven and transferable model which is in use in truck platooning tests and DRIVEN.

Figure 6: TRL's safety framework [69]

Key approaches were:

- potential risks from cyber activity were assessed throughout and this extended to taking the appropriate technical and organisational measures protect the integrity of the vehicles and their systems
- This enabled vulnerabilities to be assessed and insight into how cyber security may potentially impact the future of automated mobility
- A live, iterative safety case document was kept up-to-date throughout to facilitate feeding back of lessons learned and mitigating factors into subsequent risk assessment.

Approaches were investigated which might bring about a closer alignment between safety and security. I found theoretical approaches without being able to ascertain whether these have been adopted in practice in a security context.

Safety, Security and Survivability Engineering

In 2003 Carnegie Mellon published a technical note to help engineers from separate disciplines with requirements specifications [70]. The note analysed the similarities and differences between safety, security and survivability engineering (survivability refers to the prevention or reduction of both hazards and threats). Engineers specify the levels of safety, security and survivability (referred to as quality factors) needed instead of referring to threats, vulnerabilities and hazards.

Figure 7 shows an example of the report's analysis, in this instance of defensibility, which is broken down into a set of quality subfactors (goals): asset protection, incident detection, incident reaction and system adaptation. The author suggest this type of abstractions has benefits. First, it aids understanding between disciplines and provides a method of standardisation. Second, it broadens the scope beyond asset protection. Third, asset protection could be subdivided into other goals such as protection of confidentiality, integrity and availability and fourth, it is flexible enough to be adapted and developed.

This is a useful model. It encourages different disciplines to speak the same language and refers to survivability which equates to resilience. It uses security goals rather than a threat model.

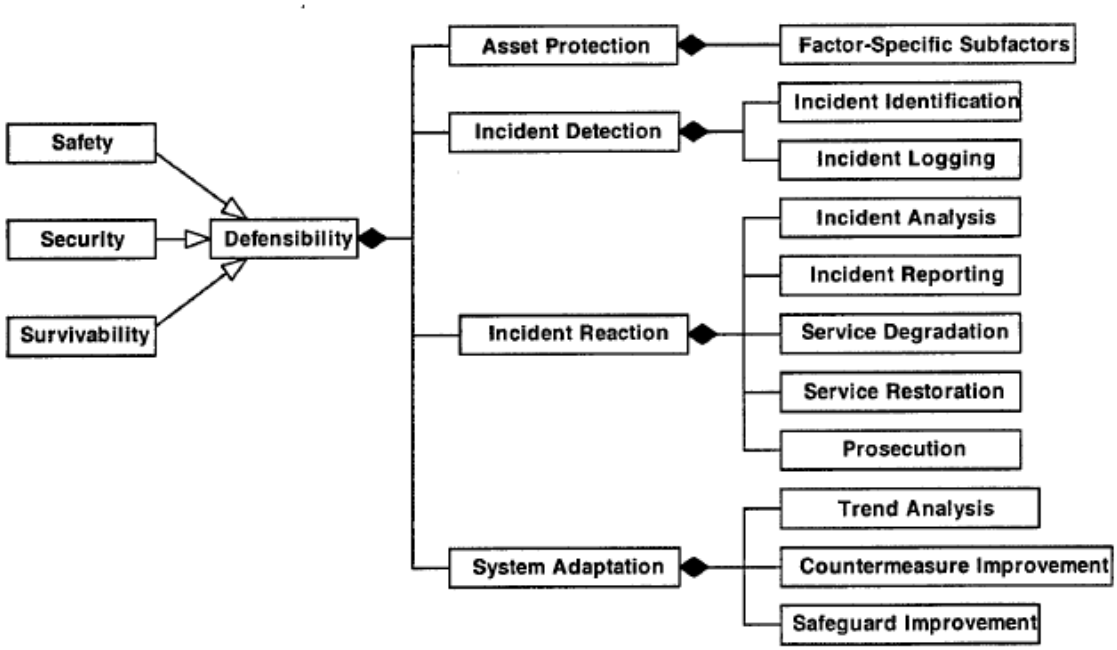


Figure 7: Standard Decomposition of Defensibility into Quality Subfactors (Carnegie Mellon) [67]

Systems theory

Engineers from Massachusetts Institute of Technology have developed systems theory [71]. This has been used in safety analysis for some time. According to this theory, defensive cyber security strategy is often based on what an adversary might do and so by definition contains unknown unknowns. Systems theory advocates thinking less about adversary intent and all possible attack types and seeing the problem instead as loss prevention. When used for both safety and security this forces whole systems to be considered, not just the technical aspects.

The overarching security goal therefore becomes maintaining the service despite disruptions, in a resilience approach. This is achieved by aiming to control component vulnerabilities instead of second-guessing adversary actions. Deciding what constitutes top level failures allows further abstraction and analysis to determine causes and identify countermeasures. The authors concede that the abstraction can never create a model of the whole system.

As taught in the MSc, resilience can be defined as the ability to tolerate faults and attacks to an extent, by degrading in a gradual, at least partially predictable manner, and the ability to recover from such incidents to either the previous operational state or a degraded but stable state.

Another key benefit of the top-down, system engineering approach is the ability for conflicts between safety and security to become apparent early in the development process. Further, it acknowledges the fact that the defender is always at a disadvantage due to the number of threats, the variety of threats and knowing how to prioritise them to allocate resources effectively.

Operation, safety and security: Conclusions

CAVs are cyber physical systems with unprecedented scope and complexity in terms of components, software, architectures, interconnectivity and perhaps above all, data. For this reason the challenges of securing them are not yet widely understood. Widely adopted and effective security practices may no longer be valid in view of this unprecedented complexity.

During research and interviews, data emerged as being of unexpected value and significance and presents a unique set of challenges.

Theoretical vulnerabilities have been discovered by some researchers while others have moved on to successfully test attacks on vehicles in operation. This is a penetration testing approach which is a technique often not used enough because of its cost and impact on profits.

Car safety on the other hand is achieved through engineers testing components and systems repeatedly to meet long-standing and widely-accepted safety standards. This approach differs from that of security, a discipline in which complying with the same standards may lead to different implementations.

Section 3: The role of legislation and standards

Introduction

In this section I set out to clarify the hierarchy of legislation, regulations and standards, encompassing those which already exist and those in the pipeline. The scope of these is both national and international. I consider whether these might have an impact on the security of CAVs.

I conducted this part of my research firstly by reading in-depth analysis by commercial law firms and management consultancies. I also reviewed publications on the Parliament website throughout the passage of the Automated and Electric Vehicles Act 2018. To further gain insight I conducted interviews with a lawyers with expertise in product liability, technology law and automotive technology and a commercial lawyer with expertise in autonomous vehicle technology for clarity and opinions on the situation. I also sought the opinion of security experts as to the role of standards which they would potentially refer to in the context of CAVs.

Context

This section begins with a description by a lawyer of the complex legal situation in the UK.

Evidence from interview: The domestic regulatory framework is highly complex with regulations derived from a variety of sources, both international and domestic, and with overlaps but not conflicts. Many laws apply, ranging from primary legislation like the Road Traffic Act 1988, and statutory instruments such as the Road Vehicles (Construction and Use) Regulations 1986, to guidance like the Highway Code. There are many different road traffic acts, some international and some domestic. Non-binding codes of practice exist beneath regulations. As new technology develops against a backdrop of no dedicated legislation, the laws become more convoluted and traverse different areas of law. The law cannot keep up and it is currently unclear how this situation will develop.

This evidence explains why since March 2018 a 3-year review into automated vehicles has been underway by the Law Commission [72]. This will consider the extensive set of applicable laws and

support the creation of a new legal framework to apply in the future if or when all vehicles are fully automated. A key area to be examined will be who is to decide whether a CAV is safe. Cyber security is out of scope of the review although it is acknowledged to be integral to delivering effective policy.

Within this context of a wide variety of existing laws combined with a lack of applicable up-to-date laws, opinions were sought from expert lawyers on the effect of this.

Evidence from interview: The law is lagging behind and deployment is slow because of this. The 2021 target for L4/5 is unlikely to be realised. Car sharing and leasing models are more likely to happen before full autonomy. This is for pragmatic reasons: automotive OEMs are used to being heavily regulated and do not like to operate with the type of legal uncertainty which currently exists around manufacturing requirements. It is expensive to retro-fit autonomous features. This contrasts with GDPR which is explicit, for example about when to report breaches by. Certainty is good for industry. The law will catch up in time.

Evidence from interview: as technology develops the law becomes more spread out and convoluted. The law is lagging behind technology innovation and it will eventually have to speed up.

Evidence from interview: some of the most significant conflicts of interest will arise between balancing the need to protect public safety with the need to help industry develop and profit from CAVs.

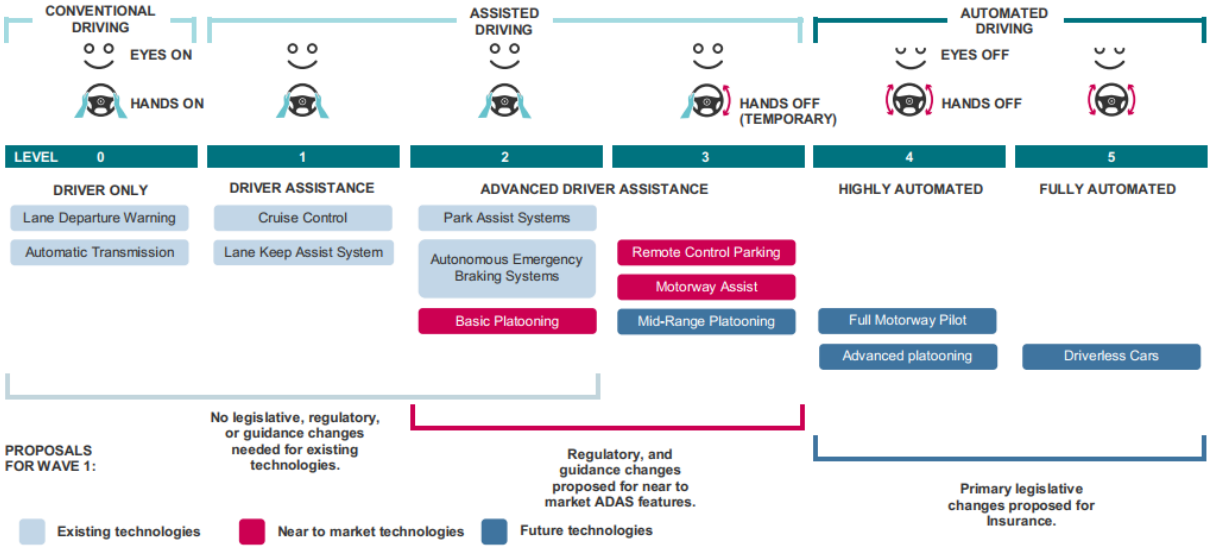


Figure 8: Levels of assistance and automation adapted by CCAV from the SAE J3016 Standard

CCAV have produced a useful diagram based on the J3016 Levels and illustrating the legislative changes needed. Figure 8 shows that primary legislative change is needed for highly and fully automated driving (hence the Law Commission's review) while in the meantime changes will be to regulations and guidance for new ADAS features. It also shows the useful eyes on/hands on (Level 0) to eyes off/hands off (Level 5) taxonomy.

The *Pathway to Driverless Cars* Review

Review of regulations to enable testing

The *Pathway to Driverless Cars Review* reviewed existing legislation and regulations to facilitate testing [30]. The review concluded that it would be lawful without being restricted to certain areas, there would be no requirement for a licence and no surety bond would be needed, as long as insurance was in place.

The review explains the approach towards testing is deliberately light-touch and non-regulatory; partly to give the UK a competitive advantage over other countries but also partly to avoid making laws which will no longer apply in a short timeframe given the rapid pace of technology development.

CCAV provides more insight into this [73]. It states that it intends to regulate in waves of reform, taking a step-by-step approach and learning important lessons from real-life experiences of driving of increasingly automated vehicles.

The Automated and Electric Vehicles Act 2018

This Act received Royal Assent on 19th July 2018 [5]. Part One relates to issues around CAVs while Part Two focuses on electric vehicle charging. Key questions of liability are addressed to allow for the insurance of CAVs operating alongside conventional cars.

A research briefing explains the background to this [74]. The Road Traffic Act 1988 assumes the presence of a human driver, who must be a competent and careful driver with a duty of care to other road users. Compulsory motor insurance must be in place in case an accident occurs. The new Automated and Electric Vehicles Act clarifies questions of liability where CAVs are considered to be the driver and the individual - formerly the driver - now becomes the passenger. Insurance

claims made by individuals after accidents will be dealt with by the motor insurance settlement framework rather than product liability laws applying to manufacturers.

Evidence from interview: the Act could have gone further to allow enactment of legislation in more agile way to be able to respond to future technology advances. Review will in future also be needed of infrastructure and telecoms regulations.

The Act refers to software updates (patching) [75]. If an individual policyholder has made unauthorised modifications to the vehicle's software or failed to install safety-critical software updates resulting in an accident, the insurer will not be liable to the policyholder, only to a third party. An implication of this is that CAV operators or owners will need to have proper records of patching and physically secure vehicles too to prevent tampering [76].

The Act states that an insurer will not be liable where an accident is the direct result of:

a) software alterations made by the insured person, or with the insured person's knowledge, that are prohibited under the policy, or
b) a failure to install safety-critical software updates that the insured person knows, or ought reasonably to know, are safety-critical.

Evidence from interview: an expert product liability lawyer explained this succinctly: failure to update a CAV will be considered a defect with the user or owner, not the product.

Examination of the written evidence submitted by outside bodies and individual MPs appointed to examine the Bill during committee stage revealed that the following concerns were raised [77]–[79]:

- Cyber security and data protection must be enshrined in both private and public data storage to ensure the safety of drivers and the public;
- Tampering with a vehicle's software should be made a serious offence;
- One MP asked for a clause to be inserted to require the government within 12 months of the Act receiving Royal Consent to consult on the risks of automated and electric vehicles being hacked and to ensure that measures are in place to address this.

These suggestions were not implemented in the final Act.

Code of Practice for Testing

In July 2015 the Code of Practice was published [80]. This cleared the way for the trials referred to in Section 1 to commence.

The Code contains one high-level security requirement "all prototype automated controllers and other vehicle systems have appropriate levels of security built into them to manage any risk of

unauthorised access". It is recommended that testing organisations consider adopting the security principles set out in *BSI PAS754 Software Trustworthiness - Governance and management - Specification* or an equivalent. Although lacking detail, this is perhaps not surprising as the trials are heavily monitored so risk of harm is low.

International legislation

Overall regulation of the car industry is at an international level [8]. Cars sold in the UK must comply with global regulations set by the UN. Cars are treated as a product under the EU Directive on Liability for Defective Products (85/374/EEC) and the Framework Directive for Whole Vehicle Type Approval (2007/46/EC) [23].

Work on amending regulations to allow for CAVs and codifying best practice for their security is underway at both UN and EU level. In 2016 the Declaration of Amsterdam was signed by all European Union Member States including the UK [81]. A white paper was published with plans to create a regulatory framework, stressing the importance of a harmonised set of rules to cover different EU states.

1968 Vienna Convention on Road Traffic

This is of interest because it stipulates that every car should have a driver in the front seat but it was amended in 2016 to allow for autonomous operations as long as there is a manual override option in the vehicle which the driver can use whenever needed [23].

GDPR and the Data Protection Act 2018

There are risks to privacy due to the type of data processed by CAVs. Researchers have shown that when combined with other data (Facebook posts, Tweets, alarms, position), data originating in the vehicle may be used to identify the car's occupants [41]. I asked for the opinions of lawyers on this in interviews.

Evidence from interview: GDPR and Data Protection are the most significant in relation to CAVs and the issues at stake should be understood at a corporate level and not left to manufacturers.

Evidence from interview: The value and ownership of data and who has the right to use it are key issues, with inconsistency between countries which affects exports. Some countries say IP address is not PII. Sensor data will effectively be PII because it can be used to identify the starting point of the journey etc. There is a GDPR requirement for the consumer to understand how their PII is being

used up front but there is ambiguity about the legal interpretation of this. Car sharing would need to collect journey information because of billing queries for example and this would need to be made quite clear in advance.

Analysis by law firms highlights some of the diverse obligations of manufacturers arising from data collection in addition to GDPR requirements [24]. For example, under the Data Retention and Investigatory Powers Act 2014 there is a need to collect and retain large amounts of communications data. There are also regulatory obligations to share safety data. Other issues around collecting and using data are highlighted. For example it will be difficult to adhere to transparency and purpose limitation requirements ie. to make sure customers understand what data is being collected and what it will be used for. Other challenging requirements of GDPR in the context of CAVs are the need to keep data processing to a minimum and not hold it for longer than necessary and complex questions of the legality of cross-border data transfers. Performing a DPIA (data privacy impact assessment) would be a complex task.

Evidence from interview: the ambiguity in laws about personal data can lead to some conflicting requirements in security services needed. PII will allow passengers to be identified therefore best practice for ensuring privacy should be followed which dictates that it should be encrypted. But if safety data is encrypted, this cannot be monitored or acted on as real-time data to support safety. Manufacturers want to avoid a situation where they are potentially facing being taken to court both for not encrypting PII and taken to court for encrypting data and making it unusable for safety purposes.

The DPA 2018 has received less media attention than GDPR. It covers areas beyond the GDPR provisions including requirements for processing personal data for criminal law enforcement purposes, and for national security. There are grey areas around CAV data being used for surveillance. The intelligence services adhere to requirements based on Council of Europe Data Protection Convention 108 [82].

UNECE World Forum for Harmonization of Vehicle Regulations (WP.29)

DfT officials are participating in the UNECE World Forum for Harmonization of Vehicle Regulations (Working Party/WP.29) standards framework which is under development [83]. These will apply to the wider ITS ecosystem and not just CAVs. The DfT describe the working party's aims in relation to security [33]. These are to investigate the development of a regulation or resolution by defining requirements for addressing cyber threats, for defining requirements for software update management with respect to safety type approval and defining guidance or measures for how to achieve this. These are high-level aims but align with the UK's aim to take action on the

international stage and it is reasonable to assume that NCSC and CCAV are playing a coordinating role as the *Autonomous Vehicles Inquiry* proposed

Principles

CCAV

The Key Principles of Cyber Security for Connected and Automated vehicles were published by CPNI along with CCAV and DfT; evidence of collaboration across different departments [14].

The eight principles are guidelines and not a statutory requirement and are designed for use throughout the automotive sector, the CAV and ITS ecosystems and their supply chains. The first three relate to system security:

1. Organisational security is owned, governed and promoted at board level;
2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain;
3. Organisations need product aftercare and incident response to ensure systems are secure over their lifetime;

The remaining four relate to system design:

4. All organisations, including sub-contractors, suppliers and potential third parties, work together to enhance the security of the system;
5. Systems are designed using a defence-in-depth approach;
6. The security of all software is managed throughout its lifetime;
7. The storage and transmission of data is secure and can be controlled;
8. The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

These reflect many of the problems of CAV security which came to light in my research and serve as a solid foundation on which to build good practice.

SMMT

SMMT considers guidelines as part of the security by design principle to be the best approach as at 2017 [26]. Their position paper reiterates their support for the WP.29 security guidelines:

- The protection of CAVs requires verifiable security measures based on existing security standards (e.g. ISO 27000 series, ISO 15408, ISO 29101);
- CAVs must be equipped with integrity protection measures (e.g. security software updates);
- Vehicle manufacturers and their suppliers must have appropriate measures in place to manage used cryptographic keys;
- The integrity of internal communications between controllers within CAVs must be protected (e.g. by authentication);
- Online services for remote access into CAVs must have strong mutual authentication and secure communication between involved entities.

SMMT acknowledge the breadth of the entities involved and suggest these should be extended to encompass board-level governance, the supply chain, product aftercare and incident response, personnel, procurement, and data storage and transmission.

Standards

Because of their cross-disciplinary nature, many standards could potentially apply to the manufacture, operation and maintenance of CAVs. As already mentioned, no formal automotive-specific cyber security standards exist yet but are under development.

The list below of some of the applicable safety standards is taken from a paper presented at the 2017 XXVI International Conference on Information, Communication and Automation Technologies [52]. It demonstrates the wide variety of applicable areas where efforts are being made to codify cybersecurity and combine it with safety:

- SAE J3061, the *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* - the closest to a joint safety and security assessment (I consider this more in Section 4);

- IEC 61508, an international standard for the functional safety of electrical, electronic and programmable electronic safety-related systems – covers software requirements and the reuse of pre-existing software elements to implement all or part of a safety function;

- ISO 13849, an international standard on safety of machinery and safety-related parts of control systems;

- ISO 26262:2011, a functional safety standard for malfunctions occurring in the electronic systems within road vehicles - introduced when safety-critical embedded systems started to be used in cars. It consists firstly of a Hazard Analysis and Risk Assessment (HARA) which as described previously uses potential component failures to determine top-level safety requirements. Secondly it provides requirements and guidance to avoid hardware and system faults;

- ISO/WD PAS 21448: Road vehicles - Safety of the intended functionality - under development;

Also many ISO standards relate to ITS communications and protocols, such as ISO 10711:2012 – Interface Protocol and Message Set Definition between Traffic Signal Controllers and Detectors – and ISO/TR 10992:2011 – use of nomadic and portable devices to support ITS service and multimedia provision in vehicles.

Evidence from interview: a "gold standard" is expected to be created – perhaps in the US or China – which will act as a precedent which developers in other countries will need to follow.

Evidence from interview: the UK will need to adhere to whatever regulations are agreed internationally because of the value to the UK of its export market.

Evidence from interview: standards from a wide variety of domains would need to be complied with including manufacturing, authentication, privacy, data protection, road standards, location services, incident management and business continuity.

Evidence from interview: it will be vital for automotive security professionals to have a deep knowledge of the automotive industry, how it operates, its regulations, governing bodies, industry dynamics and subtleties.

Challenges

Evidence from interview: drafting legislation is made harder for government because there is a fine balancing act between public safeguards like ensuring safety while promoting enterprise without stifling innovation

Evidence from interview: what matters to businesses is that they can provide evidence in court of having adopted best practice if an accident has happened which they are being held liable for. How this best practice is determined when there is a lack of industry consensus is unclear.

Evidence from interview: in the US progress has been slowed because the Senate is tied up making decisions about cyber security and privacy.

The role of legislation and standards: conclusions

The legal situation is complex due to the variety of laws traversing the CAV domain as well as the applicability of global laws but this should be simplified after the Law Commission's review is finished. The government has adopted a light-touch, non-regulatory approach to support testing and innovation but it was perceived by lawyers that a lack of certainty as to precise rules for manufacturing might conversely discourage OEMs and technology companies from developing CAVs here.

GDPR hugely complicates how data is used with the main complications arising from it being needed to be unencrypted for speed for real-time safe operation while at the same time protected for privacy reasons. How the legal requirements are interpreted in the CAV context appears highly complex and open to interpretation despite GDPR being clear about its requirements.

Although there is a lack of dedicated standards, work is being done to develop standards to guide CAV development and statements of best practice are beginning to be published. These go some way towards providing the best practice which will inevitably be needed to refer to in legal proceedings.

Section 4: Risk analysis

Introduction

In this section I investigate which approaches and tools are being used for risk analysis. I consider whether techniques used in cyber security can be used in the CAV domain and whether safety approaches are still valid when security enters the equation. I look for methods which could be adopted and adapted and consider the influence of the wider ecosystem and how this might be incorporated into the risk assessment process.

I conducted this research by reviewing publications by standards organisations, security framework and risk organisations, the automotive industry and those responsible for critical infrastructure protection. I include some data from interviews conducted with cyber security professionals.

Component-driven vs system-driven risk analysis

NCSC identify two different approaches to risk [84]. Component-driven (bottom-up) risk analysis considers specific threats to each component along with its vulnerabilities and likelihood of it being compromised and takes into account their importance ie. the impact of the threat being realised. This allows risks to be prioritised based on the potential impact or the ease of realising the threat.

System-driven (top-down) risk analysis considers the goals of the whole system instead of its components. It focuses on understanding how parts of the system interact. There is a focus on losses ie. unwanted events with a negative outcome. This approach, as seen in Section 2, is used in systems engineering.

Examples of both of these are examined.

Introduction to risk in the context of CAVs

The Industrial Strategy declares that a strategy that avoids risks is no strategy at all and concludes that previous industrial strategies have failed because of a lack of collaboration and a failure to listen and consult. This explains the 2017 Strategy's strong emphasis on partnerships, backed up by the funding of consortia to carry out research and testing. It also aims not to let a fear of failure make it unimaginative or risk averse.

An internet search of government publications led to the Cabinet Office's interim cyber security strategy for science and technology which has a section dedicated to CAVs [85]. It highlights how important consumer trust will be in realising CAV benefits; trust in CAVs being safe and keeping PII private. The strategy makes it clear that the full ecosystem will need to be protected and able to detect, respond and recover from cyber security incidents. Long-term plans are set out to develop a maturity assessment framework to allow insurers to perform cyber risk assessments on CAV systems.

Evidence from interviews: a perennial problem for information security professionals who perform risk assessments is that they are protecting against events which may never happen, or about which

they will not know whether their preventive measures were effective. The nature of threats is that they are often invisible. This makes justification of budgets challenging.

Below are the opinions of expert cyber security professionals on approaches to risk which could be applied to CAVs and these align with the type of risk assessment taught on the MSc and which is widely adopted.

Evidence from interview: risk assessment should be end-to-end and holistic, across the whole product lifecycle from the design stage to destruction, with an emphasis on data security at end of life. It should include manufacturers, resellers, owners, processes, technology, suppliers and other third parties. Residual risk should be carefully considered. Risks should be owned at enterprise level and include governance activities.

Evidence from interview: it will not be possible to guarantee a car's security. Any risk assessment should consider the risks caused by the driver too. Network and vehicle monitoring should be implemented and a SOC in place for incident management and monitoring. A backup data centre should be available but having one with the same capacity is difficult. Threats are very diverse and include battery failure/power loss, manual override of critical controls, unauthorised remote access, physical break-in, social engineering, insecure local authentication management, natural disaster, integration errors, power surges, poor road surfaces, GPS solar interference and even how a carrier bag on the road will be interpreted by an autonomous system.

Existing risk assessment approaches

NCSC summarise risk methods and frameworks [86]. Four are aimed at information risk management, which is partially suitable for application in CAV enterprises but not manufacturing, with the NIST approach having a US focus:

- ISO/IEC 27005:2011
- Information Security Forum (ISF) IRAM 2
- CESG Information Assurance Standard 1 & 2, a legacy technique for organisations especially government departments
- US National Institute of Standards and Technology (NIST) SP 800-30, preferred by the US government and tailored to US laws

The other three methods are:

- OCTAVE Allegro, intended as a qualitative assessment, and asset-focussed. This is differentiated from the other methods in that it is performed in small workshops conducted with those involved in an enterprise's operations and IT.

- ISACA COBIT 5 for Risk, aimed at enterprise risk governance.
- IEC 62443-2-1:2010, aimed at implementing risk management programmes for industrial automation and control systems.

None of these relate to cyber physical systems. However NCSC have promised new guidance soon in the form of a toolbox of techniques, borrowing from established risk methods from other domains like industrial safety engineering. This suggests that they believe the above methods have shortcomings and may no longer meet the risk assessment requirements of modern technology which is about more than information risk and also includes cyber physical risk. The toolbox will be part of NCSC's sociotechnical security offering, an area which relates to security that accounts for the interaction of technology with people, processes and organisations. This looks to be a promising approach which could be adopted to CAV security because it consists of a multi-disciplinary team with different approaches and one of its specialisms is engineering processes and assurance.

Enterprise Risk Management Maintaining an understanding of existing ERM techniques and developing new ones.

Reductive Risk Assessment Methods Understanding strengths and weaknesses of current-practice risk management processes in order to guide practitioner application and identify gaps in our research direction.

Systems Theory of Risk and Design Understanding systems theoretic approaches to assessing risk during system design and analysis.

Standardisation Exploring organisational and field-level implications of standardising approaches to risk management.

Data-Driven Security Developing data analysis techniques applicable to commonly-available cyber security datasets.

Security Metrics Designing and implementing appropriate metrics to measure security problems and assess interventions.

Complex Systems Investigating the application of complex systems theory to cyber security.

Figure 9: Approach of NCSC's Sociotechnical Security Group to risk [87]

There is also acknowledgement of the complexity of modern systems, not just in isolation but as part of wider systems. This is a useful summing up of the difficulties of assessing risk in CAVs: they are both complex systems in themselves but are also part of and depend on wider complex systems which are not in the control of CAV makers. This equates to a very difficult problem to solve.

Figure 9 shows the multi-pronged approach being adopted by NCSC's Sociotechnical Security Group (StSG) to risk which introduces the concept of complex systems theory.

High-level guidance from principles

UK

CCAV's *Key Principles of Cyber Security for Connected and Autonomous Vehicles* is aimed at those involved at all levels, from designers all the way through to senior executives. The first principle is that security should be owned at Board level. The second principle is about risk: security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain. Below is its detail:

- Principle 2.1: Organisations must require knowledge and understanding of current and relevant threats and the engineering practices to mitigate them in their engineering roles;
- Principle 2.2: Organisations collaborate and engage with appropriate third parties to enhance threat awareness and appropriate response planning;
- Principle 2.3: Security risk assessment and management procedures are in place within the organisation. Appropriate processes for identification, categorisation, prioritisation, and treatment of security risks, including those from cyber, are developed;
- Principle 2.4: Security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices.

These are high-level architectural principles which is a useful security foundation although there is no implementation detail.

Evidence from interview: these are a good starting point although they will not prove safety and could not be relied upon in court. They are not sufficient for enterprises to work from.

The unsuitability of high-level guidance for enterprises supports the view heard from expert lawyers that uncertainty about specifications is not good for OEMs.

US

For comparison the US NHTSA's voluntary best-practice guidelines are examined, *Cybersecurity Best Practices for Modern Vehicles*, which advocates a layered research approach to cyber security [88]. The guidelines recommend that the product development process should follow a systems-engineering approach aiming to design systems without unreasonable safety risks.

NHTSA stress the importance throughout the vehicle's lifecycle of performing risk assessments and penetration tests and documenting details of these along with any organisational decisions of significance. It is recommended that the minimum level of risk assessment should look at cyber security risks to safety-critical vehicle control functions and PII.

The holistic approach is extended beyond the manufacturing process to sharing information about lessons learned among the whole industry, considering security throughout the product development lifecycle, considering the whole supply chain, after-market suppliers, practices across the organisation and promoting education and awareness – themes echoed in the *Key Principles*.

Automotive risk methodology

Evidence from interview: Safety risks equate to numbers which equate to money, whereas cyber risks are less tangible and measurable. It is hard to accurately attach numbers to countermeasures and likelihood of occurrence and come up with an impact, so it is hard for automotive manufacturers to make decisions in the way they usually would.

Hazard and Risk Analysis (HARA)

HARA is used to classify risks in vehicles based on the potential severity, the probability of a situation where it will arise and the controllability. Manufacturers must consider specific device or system failures: the exposure, potential severity of an accident and its controllability. HARA does not consider security risks however although these could be built on to design safety strategies. Fault tree analysis and failure mode and effects analysis are also used [89]. Although top-down approaches, the shortcomings of these were taught on the MSc:

- They are static so do not capture any attacker/defender interaction
- They cannot capture novel attacks

Other possible techniques were taught on the MSc including more dynamic attack and adversary models such as attack-defence trees and attack-countermeasure trees. These begin with a top level event representing an attack and introduce the idea of uncertainty, adding detection and mitigation measures with probabilities and costs.

Including mitigating measures as well as defensive measures allows both qualitative and quantitative study of attacks including the cost-effectiveness of detection and mitigation strategies where quantitative.

Game theory is also of value in relation to adversary motivation. Take into account the interaction between adversary and defender. Constraints or payoff for specific actions are considered so the cost to each player of pursuing a particular strategy and its consequences are considered.

Evidence from interview: at a national scale we should collected adversarial techniques to use for CAV testing eg. algorithms are being built to attack random number generators. Having a set of offensive techniques will help in defence. Game theory is useful for considering sequences of moves by adversaries.

Risk methodologies for securing safety-critical systems

System-Theoretic Process Analysis for Security (STPA-Sec)

STPA-Sec is based on STPA – a hazard analysis technique [90] and Systems Theoretic Accident Model and Process (STAMP). STPA analysis enables the identification of potentially unsafe control actions arising from inconsistencies between a controller's assessment of system state and the actual process state. The loss of state can arise because of wear and tear, incorrect calibration or malicious activities but the result is always an unwanted control action to try to maintain the correct set point. In this approach a multi-disciplinary team looks at the wider structure of the whole system which allowed the system to enter a vulnerable state which the threat was then able to exploit. It is argued that cyber security analysis should change from guarding against attacks to identifying vulnerabilities which allow disruptions (intentional or unintentional) to emerge, although threat analysis is nevertheless a necessary activity. STPA-Sec is a useful technique because it brings together multi-disciplinary teams to consider problems together. However it is not sufficient for complex SoS with rapidly evolving adversaries.

NIST's Cybersecurity Risk Management Framework Applied to Modern Vehicles

NIST have adapted their Risk Management Framework (RMF) which proposes a lifecycle process [43]. This approach encompasses risk assessment, security planning and implementation as well as on-going monitoring, and integrates these into the system development lifecycle.

This differs from the original NIST RMF in that a threat model/use case step has been added and the Authorize step removed as it relates to Federal IT systems.

Figure 10 shows an overview of this risk analysis method adapted for vehicles.

Figure 11 shows an example of the subsequent analysis using FIPS 199 with use cases in the left-hand column. The impact of specific events on confidentiality, integrity and availability is shown in green, amber and red, reflecting whether the risk is low, medium or high at different phases of vehicle use eg. parked, at rest, under maintenance, on a motorway or driving slowly.

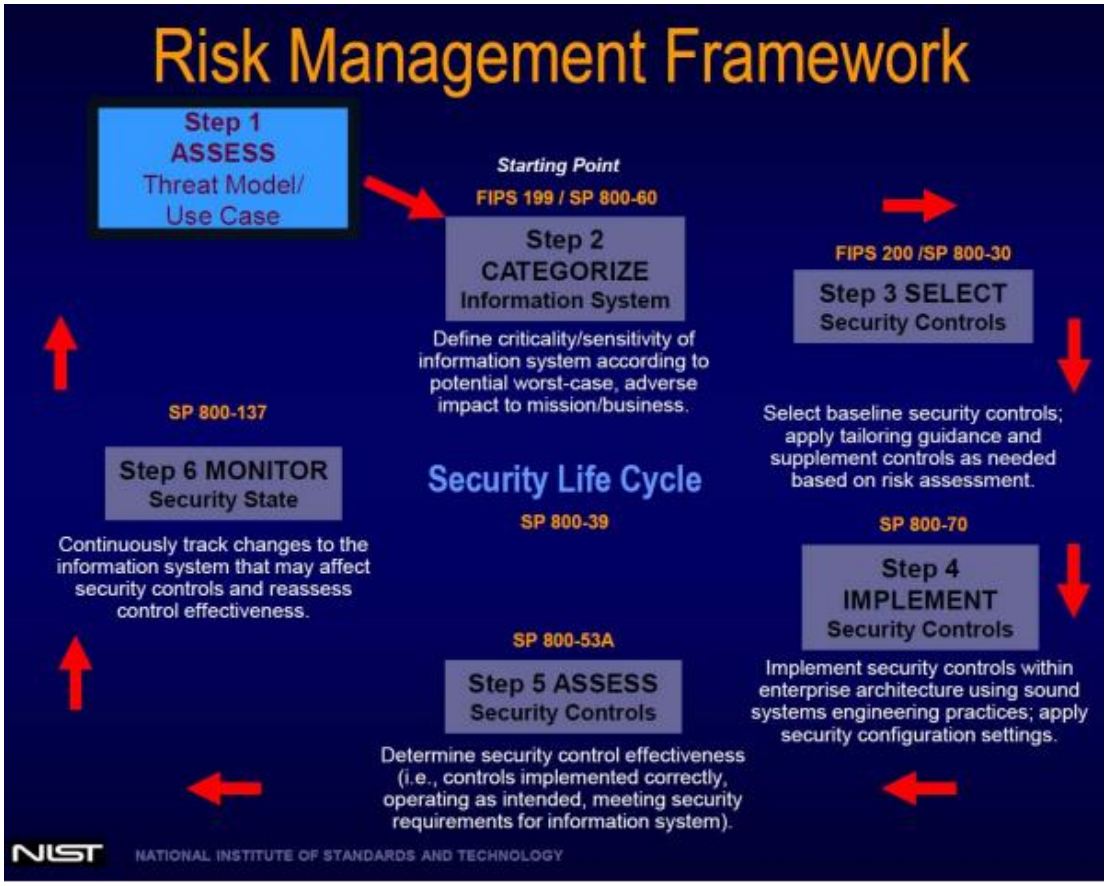
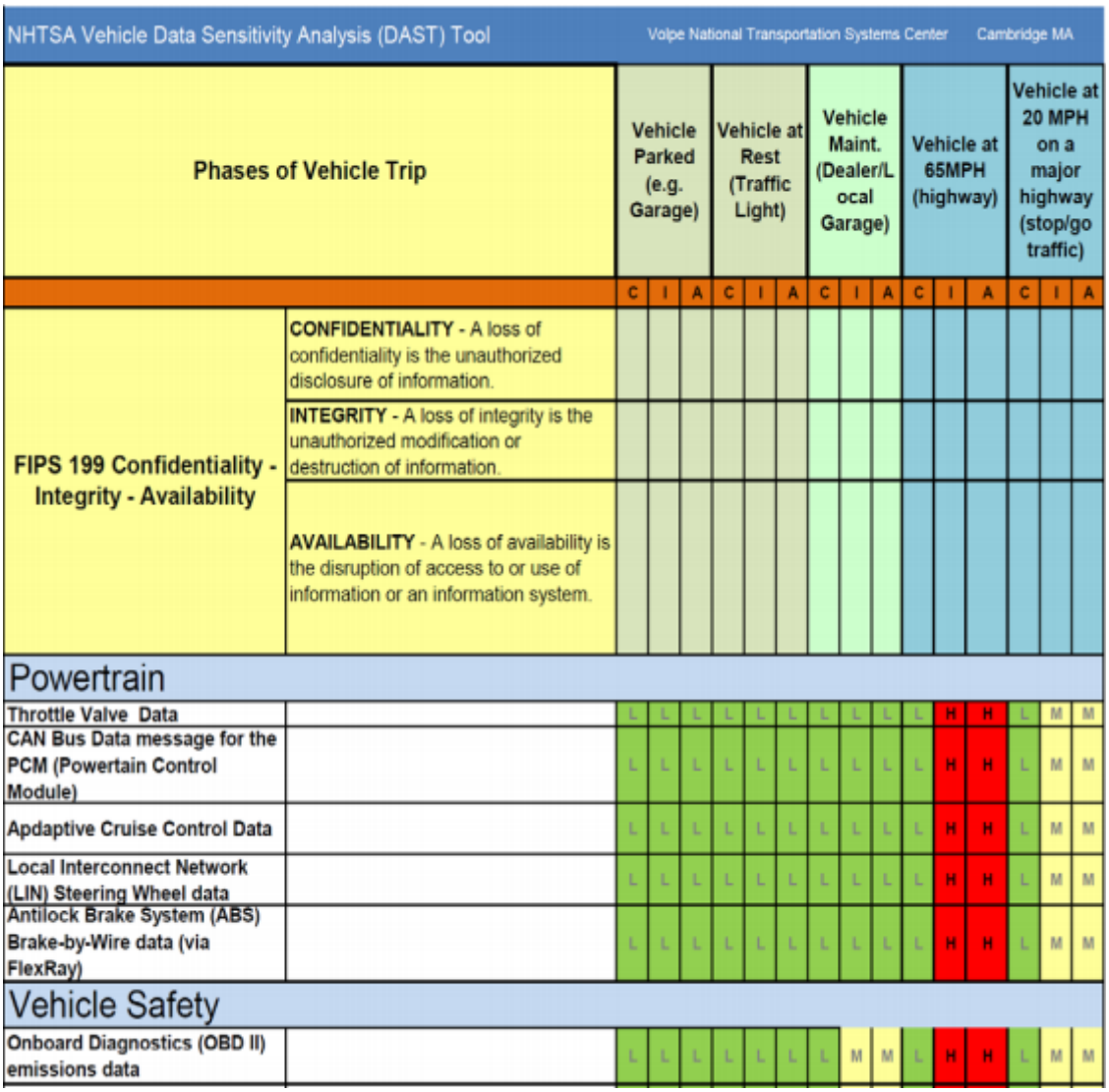


Figure 10: Modified NIST Risk Management Framework for the Vehicle Sector [43]

Appropriate security controls are selected after carrying out vulnerability identification, taking into account organisational factors as well as adversary capabilities. Likelihood is then determined. This activity involves deciding whether events, if initiated, will lead to adverse impacts. The overall risk can then be assessed. The output of this exercise is a Security Reference Architecture (SRA) which acts as an authoritative source of information to support recommendations for specific architectures.



NHTSA Vehicle Data Sensitivity Analysis (DAST) Tool — Volpe National Transportation Systems Center — Cambridge MA																
Phases of Vehicle Trip		Vehicle Parked (e.g. Garage)			Vehicle at Rest (Traffic Light)			Vehicle Maint. (Dealer/Local Garage)			Vehicle at 65MPH (highway)			Vehicle at 20 MPH on a major highway (stop/go traffic)		
		C	I	A	C	I	A	C	I	A	C	I	A	C	I	A
FIPS 199 Confidentiality - Integrity - Availability	**CONFIDENTIALITY** - A loss of confidentiality is the unauthorized disclosure of information.															
	INTEGRITY - A loss of integrity is the unauthorized modification or destruction of information.															
	AVAILABILITY - A loss of availability is the disruption of access to or use of information or an information system.															
Powertrain																
Throttle Valve Data		L	L	L	L	L	L	L	L	L	H	H		L	M	M
CAN Bus Data message for the PCM (Powertain Control Module)		L	L	L	L	L	L	L	L	L	H	H		L	M	M
Apdaptive Cruise Control Data		L	L	L	L	L	L	L	L	L	H	H		L	M	M
Local Interconnect Network (LIN) Steering Wheel data		L	L	L	L	L	L	L	L	L	H	H		L	M	M
Antilock Brake System (ABS) Brake-by-Wire data (via FlexRay)		L	L	L	L	L	L	L	L	L	H	H		L	M	M
Vehicle Safety																
Onboard Diagnostics (OBD II) emissions data		L	L	L	L	L	L	L	M	M	L	H	H	L	M	M

Figure 11: Modern Vehicle Security Categorisation (NIST) [43]

This approach has merit because unlike other risk analysis techniques examined so far, it explicitly includes vehicle-related examples of threat sources, use cases and impacts. Another advantage is that the SRA provides a common security language for those involved in CAV development even if from different disciplines and therefore are a useful technique for framing the problem. The technique provides a way of mapping of information systems and their criticality.

NIST acknowledge that using FIPS 199 (designed for single-purpose information systems) to assess risks is unlikely to be extensive enough for vehicles, characterising them not as information systems but as a collection of complex interactions of many control systems at various degrees of criticality.

NIST also stress that risk analysis should be performed at component level but their framework cannot accommodate this. They recommend instead of security categorisation levels the notion of Security Assurance Levels, as outlined in Section 2.

Security-Informed Safety Cases

Safety approaches which have been adapted by academics to include security were investigated. An approach with potential application for CAVs has been proposed by researchers at City University London which uses existing safety cases and risk assessments and augments to make them what is termed "security-informed" [67]. This highlights the difference between safety cases and security cases. A safety case shows how requirements defined for a system are met, by making claims about the system's properties and using a systematic approach to support arguments with evidence (a claims-arguments-evidence method).

The evidence relates to one or a combination of the following: claims about the systems' safety behaviour (positive properties); adherence to accepted standards and guidelines or through analysis of potential vulnerabilities (negative properties). This serves to illustrate the difference between a top-down (claims about behaviour) and bottom-up approach (vulnerability analysis) which relates back to the component-driven bottom-up approach.

The researchers go on to set out a method for incorporating security into the claims-arguments-evidence method). This entails reviewing whether the claim might be impacted by security and looking for security controls to provide the argument and evidence, then reviewing the effects of these controls on architecture and implementation and repeating and refining the process.

An 8-step risk assessment process can then be conducted in tandem with a security-informed safety case:

1. Establish the context – describe the system, its relationship with other systems and its environment; identify the services provided
2. Identify potential threats
3. Refine and focus system models
4. Perform preliminary risk analysis
5. Identify specific attack scenarios
6. Perform focused risk analysis

7. Finalise risk assessment
8. Report results

The researchers recommend that the security risk case is developed alongside the eight steps in order to synthesise risk claims, arguments and evidence. This would be a subjective exercise. One of the benefits it claims is the ability to be pitched at different audiences with its detail level adapted accordingly.

Other researchers have reviewed this technique [91]. They conclude that it lacks guidance as to how the risk assessment should be performed despite it being a requirement.

The researchers usefully distinguish between two types of resilience to be achieved. The first is resilience to threats arising from the design. The second is resilience to other threats which may be unimaginable and therefore ignored or are simply unknown.

This is a helpful distinction and could be used to assess other risk analysis techniques.

Safety-Aware Hazard Analysis and Risk Assessment (SAHARA)

At the 2015 Design, Automation & Test in Europe Conference & Exhibition a new, threat model-based approach was presented [89]. It works by analysing each component in turn and then once each is deemed secure, the whole system is deemed to be secure too.

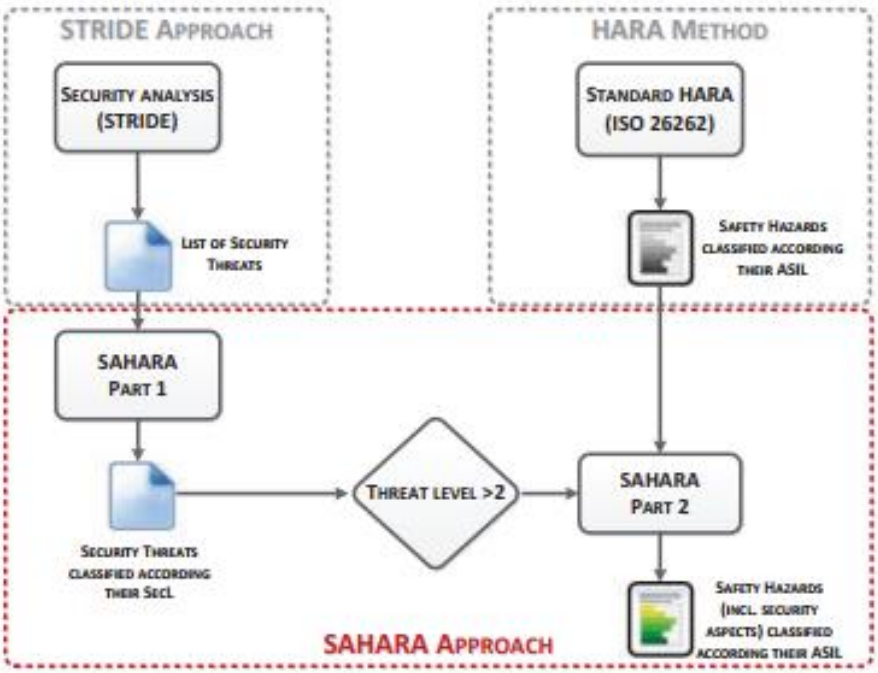


Figure 12: Conceptual overview of the SAHARA method [89]

The component-driven HARA approach is combined with Microsoft's STRIDE approach which relates to the impact of security issues on safety concepts and is a system-driven approach.

Figure 12 shows a conceptual overview of SAHARA, with the safety analysis performed according to ISO 26262 shown at the top right and the security analysis based on STRIDE at the top left. The STRIDE output is then analysed and threats are quantified as they are in the ASIL method, which consists of quantifying the resources and know-how needed to execute the threat, and the threat's criticality. Security threats that might lead to a violation of safety goals can be handed over to HARA for further analysis of the threats' effect on safety.

A disadvantage is that this analysis is aimed at the very early stages of the development of a single car but nevertheless at any stage of development if cyber security threats can be classified, this can be used as a basis for choosing countermeasures, and these can be quantified and a cost associated with them [91].

An advantage of this method is that the whole exercise is carried out by security and safety engineers collaboratively and may therefore facilitate increased understanding of each other's methods, challenges and language.

SAE-J3061 Threat Analysis and Risk Assessment approach

A research paper describes the experiences of a research project to apply J3061 in the concept phase of the secure development of an ECU [92]. The aim of the J3061 method is to identify threats and assess associated risks and use these to obtain security requirements. J3061 draws on the safety lifecycle defined in ISO 26262 to produce a security lifecycle. J3061 identifies interaction points between the security and safety process in order to coordinate the two engineering processes.

The system lifecycle consists of a number of phases: concept phase, product development (system, hardware and software), production , operation and service. These are augmented with processes including requirement, change and quality management.

The main activity of the concept phase in the threat analysis and risk assessment (TARA). J3061 does not require any specific method to be used but the overarching goal is to use the output of TARA as input for the definition of cyber security goals. Examples of methods and techniques proposed by J3061 in Appendix A include STRIDE, HAZOP, TVRA, OCTAVE and HEAVENS.

The researchers found that the method was flawed because the outcome of the TARA is based on incomplete information, because the ECU was only at the design stage and therefore lacking detail. They opted instead to base their TARA on the effect of various threats on the CIA of the ECU's data.

Other initiatives

5*StarS is a consortium developing an *Automotive Cyber Security through Assurance* project [93]. This project sets out to address the threats facing CAVs and develop an assurance methodology. Its goal will be rigorous design and testing techniques for both components and whole systems, resulting in a 5-star-type consumer rating system similar to the EuroNCAP system. This government-backed scheme is part of the efforts to put the UK at the front of global testing. The rating will help to inform car users and insurers about the risks of specific software and connectivity features.

Risk analysis: Conclusions

Risk analysis techniques can be both component-driven and system-driven. Both approaches have merits and drawbacks. Sociotechnical perspectives are a useful approach.

Risk analysis should be end-to-end, spanning the lifecycle of a vehicle. Security threats differ from safety threats in that they are unseen, making the risks difficult to quantify, and this reflects a difference in risk culture between automotive and security. Existing frameworks used in security do not account for cyber physical systems but progress is being made on this.

There are a number of approaches proposed by researchers which aim to incorporate security into safety risk assessment and some existing security techniques have been adapted. It may be that a combination of techniques will be of use but in any case increasing awareness that different approaches exist is a starting point.

Project conclusions

I set out to determine how the security of CAV computer systems will be assured in order to ensure they are safe. I have found some answers to this question but also realised that there are other questions to be asked. My scope broadened from physical safety to privacy. I became aware of the huge significance of the use of data. Although I identified risk analysis methods which could be used, it is unclear which may actually be used. The project process was helped enormously by the interviews I conducted with experts which contributed to my understanding of some of the

subtleties and conflicts at the heart of the topic, which lack black and white answers. Below are my main conclusions.

The complexity and lack of understanding of the entirety of the factors which must be right for safe implementation suggests that full autonomy by 2021 is unlikely to be achieved.

CAVs will potentially deliver benefits to society through new modes of transport resulting from society's changing needs and advances in technology. Broad initiatives are now in place at government level although the pace may not be fast enough for industry and does not reflect the pace of technology change.

Details of approaches to implementing security are difficult to find although broad principles have been established by with government coordination. The benefits of CAVs are largely societal although the task of securing them may be left to industry – this is currently unclear but a distinct possibility.

CAVs are cyber physical systems with unprecedented scope and complexity in terms of components, software, architectures, interconnectivity and above all, data. Securing CAVs means securing the entire system but the challenges of securing them are not yet fully or widely understood.

The significance of data was much greater than I anticipated. For OEMs the value and profit in future will come from data but currently there are complex legal questions around ownership of data and how to secure it while complying with GDPR. In its nature security is somewhat intangible which contrasts with the certainty OEMs usually work with in safety. The approaches to security adopted across other industries may not be sufficient in the CAV domain. Standards can be implemented in different ways leading potentially to inconsistency in levels of security achieved.

The government has a hard job to strike an acceptable balance between keeping the public safe while not stifling enterprise innovation. The areas of law that apply to automotives are wide-ranging and complex and but review has begun which will simplify them.

Existing standards are being adapted and new standards developed which are expected to provide a basis for best practice but their overall effectiveness for security is unclear.

I build on these conclusions to make some predictions about how the situation may progress.

Although technologies exist which will theoretically enable CAVs to be deployed to realise the predicted benefits, much work needs to be done to make them safe and feasible.

High level principles on the one hand and the reality of existing security practices on the other hand must somehow meet in the middle and this may be a slower process than anticipated. The types of

security approaches recommended for CAVs are not employed extensively in enterprise security while critical information infrastructure is known to have been compromised too. There are currently knowledge gaps to be filled. Bridging the gap between the certainty of safety testing and the nuances and hidden nature of security threats and countermeasures may be difficult but nevertheless techniques will have to be developed to support the new cyber physical risk paradigm.

Even if CAVs are not deployed by 2021, the technologies developed during the process by those inspired by the innovation and benefiting from government funding may be applied to other innovations which society could still benefit from. In retrospect adoption of innovation can appear predictable. However technology innovation from start-ups in the 21st century such as Facebook, Google and Uber has taken society in directions which would have been hard to predict and this trend should not be underestimated. Attracting the right range of disciplines, working in partnership across industries and starting to have the right conversations are the foundations of future success. Technology will be used for innovation which will deliver other benefits, if not these, creating employment and strengthen the economy in the future as is the government's aim.

Bibliography

[1] "Industrial Strategy White Paper," 2017.

[2] "Industrial Strategy: the Grand Challenges - GOV.UK." [Online]. Available: https://www.gov.uk/government/publications/industrial-strategy-the-grand-challenges/industrial-strategy-the-grand-challenges. [Accessed: 17-Feb-2018].

[3] BBC News, "Hammond: Driverless cars will be on UK roads by 2021," *BBC News*, 2018. [Online]. Available: https://www.bbc.co.uk/news/business-42040856. [Accessed: 15-Jun-2018].

[4] HM Treasury, "Autumn Budget 2017," 2017.

[5] Department for Transport, "Future of Mobility Call for Evidence," 2018.

[6] B. Clark, G. Parkhurst, and M. Ricci, "VENTURER: Introducing Driverless Cars to UK Roads," 2016.

[7] K. R. Lakhani, J. Weber, and C. Snively, "Google Car," 2015.

[8] Department for Transport, "Pathway to Driverless Cars : Proposals to support advanced driver assistance systems and automated vehicle technologies," 2016.

[9] InnovateUK, "Introducing Driverless Cars to UK Roads." [Online]. Available: https://interact.innovateuk.org/competition-display-page/-/asset_publisher/RqEt2AKmEBhi/content/introducing-driverless-cars-to-uk-roads?p_p_auth=CjGJE10t. [Accessed: 20-Jun-2018].

[10] Innovate UK, "Driverless cars: 4 cities get green light for everyday trials," 2014. [Online]. Available: https://www.gov.uk/government/news/driverless-cars-4-cities-get-green-light-for-everyday-trials. [Accessed: 15-Jun-2018].

[11] House of Lords Science and Technology Select Committee, "Connected and Autonomous Vehicles: The future?," 2017.

[12] National Infrastructure Commission, "Preparing for driverless cars," 2018.

[13] Website, "Centre for the Protection of National Infrastructure," 2014. [Online]. Available: https://www.cpni.gov.uk/. [Accessed: 15-Jan-2018].

[14] HM Government, "The Key Principles of Cyber Security for Connected and Automated Vehicles," 2017.

[15] Parliamentary Office of Science and Technology, “Autonomous Road Vehicles,” 2013.

[16] “Autonomous vehicles publications - UK Parliament.” [Online]. Available: https://www.parliament.uk/business/committees/committees-a-z/lords-select/science-and-technology-committee/inquiries/parliament-2015/autonomous-vehicles/autonomous-vehicles-publications/. [Accessed: 20-Jun-2018].

[17] HM Government, “National Cyber Security Strategy 2016-2021,” 2016.

[18] UKCITE, “UK Connected Intelligent Transport Environment,” 2016. [Online]. Available: https://www.ukcite.co.uk/. [Accessed: 10-Dec-2017].

[19] Ricardo, TRL, and TTR, “HEAVY VEHICLE PLATOONS ON UK ROADS FEASIBILITY STUDY EXECUTIVE SUMMARY,” 2014.

[20] “DRIVEN.” [Online]. Available: http://drivenby.ai/. [Accessed: 09-Feb-2018].

[21] X L Catlin Insurers, “Fleet of driverless vehicles using UK built software to be trialled between Oxford and London in 2019 | XL.” [Online]. Available: http://xlcatlin.com/insurance/news/fleet-of-driverless-vehicles-using-uk-built-software-to-be-trialled-between-oxford-and-london-in-2019. [Accessed: 15-Feb-2018].

[22] D. D. Chana and Imperial College, “The Security of Driverless Cars – GATEway Project.” [Online]. Available: https://gateway-project.org.uk/the-security-of-driverless-cars/. [Accessed: 15-Feb-2018].

[23] Pinsent Masons, “See the road ahead,” 2018.

[24] Allen & Overy, “Autonomous and connected vehicles : navigating the legal issues.,” 2017.

[25] Gov.UK, “Government kick-starts work on Future of Mobility Grand Challenge.” [Online]. Available: https://www.gov.uk/government/news/government-kick-starts-work-on-future-of-mobility-grand-challenge. [Accessed: 31-Jul-2018].

[26] K. Scharring, S. Nash, and D. Wong, “SMMT: Connected and Autonomous Vehicles: Position Paper,” 2017.

[27] Catapult Transport Systems, “Market Forecast for connected and autonomous vehicles,” 2017.

[28] Department for Transport, “Reported road casualties in Great Britain, main results: 2015 infographic,” 2016.

[29] KPMG, “Autonomous Vehicles Readiness Index,” 2018.

[30] Department for Transport, “The Pathway to Driverless Cars: summary and action plan,” 2015.

[31] “The GATEway Project: This is just the beginning. - YouTube.” [Online]. Available: https://www.youtube.com/watch?time_continue=223&v=86uZ66JaALA. [Accessed: 15-Jun-2018].

[32] NCSC, “Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices,” 2018. [Online]. Available: https://www.ncsc.gov.uk/alerts/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices. [Accessed: 09-Aug-2018].

[33] Department for Transport, “Cyber security for automotive,” 2017.

[34] C. Depré, H. Meyer, and M. Hawes, “Examination of witnesses.”

[35] I. Yarnold and I. Forbes, “Select Committee on Science and Technology Corrected oral evidence: Autonomous Vehicles,” 2017.

[36] Symantec, “Internet Security Threat Report (ISTR) 2018,” 2018. [Online]. Available: https://www.symantec.com/security-center/threat-report. [Accessed: 21-Aug-2018].

[37] The Royal Academy of Engineering, “Autonomous Systems: Social, Legal and Ethical Issues,” *R. Acad. Eng.*, pp. 1–19, 2009.

[38] L. Floridi and M. Taddeo, “What is data ethics?,” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 374, no. 2083. 2016.

[39] SAE International, “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles,” 2016.

[40] “Primary safety advanced driver assistance systems | AA.” [Online]. Available: https://www.theaa.com/driving-advice/safety/primary-safety-advanced-driver-assistance-systems. [Accessed: 30-Jun-2018].

[41] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, and T. Engel, “A car hacking experiment: When connectivity meets vulnerability,” in *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*, 2015.

[42] ENISA, “Good practices on the security and resilience of smart cars,” 2016.

[43] National Institute of Standards and Technology, “Risk Management Framework Applied to Modern Vehicles,” 2016.

[44] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges,” *IEEE Transactions on Intelligent Transportation*

Systems, vol. 18, no. 11. pp. 2898–2915, 2017.

[45] Rand, "Road Map of Autonomous Vehicle Service Deployment Priorities in Ann Arbor. CSS16-XX 20. Mersky, A. and C. Samaras (2016) Fuel economy testing of autonomous vehicles," Springer International Publishing, 2016.

[46] M. Hartong, R. Goel, and D. Wijesekera, "Transportation," in *Lopez J., Setola R., Wolthusen S.D. (eds) Critical Infrastructure Protection. Lecture Notes in Computer Science, vol 7130. Springer, Berlin, Heidelberg*, 2012.

[47] C. W. Axelrod, "Managing the risks of cyber-physical systems," in *2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2013, pp. 1–6.

[48] IET, "Automotive Cyber Security : An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles," *Whitepaper*, pp. 1–16, 2014.

[49] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, 2017, pp. 164–170.

[50] D. Shepardson, "Tesla driver in fatal 'Autopilot' crash got numerous warnings: U.S. government," *Reuters*, 2017. [Online]. Available: https://www.reuters.com/article/us-tesla-crash/tesla-driver-in-fatal-autopilot-crash-got-numerous-warnings-u-s-government-idUSKBN19A2XC. [Accessed: 21-Feb-2018].

[51] "Connected and Autonomous Vehicles: Navigating the Future | Herbert Smith Freehills | Global law firm." [Online]. Available: https://www.herbertsmithfreehills.com/latest-thinking/connected-and-autonomous-vehicles-navigating-the-future. [Accessed: 22-Jun-2018].

[52] A. Causevic, "A risk and threat assessment approaches overview in autonomous systems of systems," *2017 XXVI International Conference on Information, Communication and Automation Technologies (ICAT)*. IEEE, pp. 1–6, Oct-2017.

[53] J. Joy and M. Gerla, "Internet of vehicles and autonomous connected car - Privacy and security issues," in *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*, 2017.

[54] M. Christen and K. Weber, "A review of value-conflicts in cybersecurity : an assessment based on quantitative and qualitative literature analysis," *ORBIT J.*, vol. 1, no. January, Sep. 2017.

[55] K. Gyimesi, “Are there acceptable levels of cyber-security protection in connected cars?,” *IBM Blogs*, 2017. [Online]. Available: https://www.ibm.com/blogs/internet-of-things/iot-connected-cars-cyber-security/. [Accessed: 27-Jul-2018].

[56] World Economic Forum and Boston Consulting Group, “Cyber Resilience Playbook for Public-Private Collaboration,” 2018.

[57] A. Martin, “How risk-driven systems engineering will keep car control systems safe and secure,” *The Engineer*. 2017.

[58] K. M. A. Alheeti, S. Ehsan, and K. D. McDonald-Maier, “An assessment of recent attacks on specific embedded systems,” in *Proceedings - 2014 International Conference on Emerging Security Technologies, EST 2014*, 2014, pp. 88–93.

[59] Q. He, X. Meng, and R. Qu, “Survey on cyber security of CAV,” *2017 Forum on Cooperative Positioning and Service, CPGPS 2017*. pp. 351–354, 2017.

[60] Koscher K et al., “Experimental Security Analysis of a Modern Automobile,” in *2010 IEEE Symposium on Security and Privacy*, 2010.

[61] C. Bordonali, S. Ferraresi, and W. Richter, “McKinsey: Shifting gears in cyber security for connected cars,” 2017.

[62] C. Valasek and C. Miller, “Adventures in Automotive Networks and Control Units,” *Tech. White Pap.*, p. 99, 2013.

[63] K. Mahaffey, “Hacking a Tesla Model S: What we found and what we learned,” *Lookout Blog*, 2015. [Online]. Available: https://blog.lookout.com/hacking-a-tesla. [Accessed: 10-Aug-2018].

[64] A. Greenberg, “This Hacker’s Tiny Device Unlocks Cars And Opens Garages,” *WIRED*. 2015.

[65] B. Glas *et al.*, “Automotive safety and security integration challenges,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. P-240, pp. 13–28, 2015.

[66] SAE International, “ADAS: functional safety and freedom from unacceptable risk,” 2017. [Online]. Available: http://articles.sae.org/15703/. [Accessed: 15-Nov-2017].

[67] R. Bloomfield, K. Netkachova, and R. Stroud, “Security-Informed Safety: If It’s Not Secure, It’s Not Safe,” Springer, Berlin, Heidelberg, 2013, pp. 17–32.

[68] J. D. Gilsinn and R. Schierholz, “Security Assurance Levels : A Vector Approach to Describing Security Requirements,” pp. 1–13, 2010.

[69] GATEway: Greenwich Automated Transport Environment, “This is Just the Beginning:

Positioning the UK at the forefront of automated mobility."

[70] D. G. Firesmith, "Common Concepts Underlying Safety, Security, and Survivability Engineering." 2003.

[71] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Commun. ACM*, vol. 57, no. 2, pp. 31–35, 2014.

[72] Law Commission, "Automated Vehicles," 2018.

[73] Department for Transport, "UK Testing Ecosystem for Connected and Autonomous Vehicles Government response to the call for evidence," 2016.

[74] L. Butcher and T. Edmonds, "Automated and Electric Vehicles Bill 2017-19 — UK Parliament." [Online]. Available: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-8118#fullreport. [Accessed: 14-Feb-2018].

[75] L. McCormick, "Back to the future - the Automated and Electric Vehicles Bill 2017," *20/10/17*. [Online]. Available: http://3yf6pp3bqg8c3rycgf1gbn9w-wpengine.netdna-ssl.com/wp-content/uploads/2017/12/Back-to-the-futurethe-Automated-and-Electric-Vehicles-Bill-2017.pdf.

[76] RPC, "Automated and Electric Vehicles Act 2018," 2018. [Online]. Available: https://www.rpc.co.uk/perspectives/retail-therapy/update-automated-and-electric-vehicles-act-2018/. [Accessed: 13-Aug-2018].

[77] "NOTICES OF AMENDMENTS given up to and including PUBLIC BILL COMMITTEE AUTOMATED AND ELECTRIC VEHICLES BILL," 2017.

[78] "Written evidence submitted by Cycling UK (AEVB 20) Electric and Automated Vehicles Bill: a legal vacuum on criminal and civil liability."

[79] "Automated and Electric Vehicles Bill," vol. 19, no. 1, p. 20, 2017.

[80] Department for Transport, "The pathway to driverless cars: A code of practice for testing," p. 14, 2015.

[81] European Commission, "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility," *COM(2016) 766*, vol. 30, no. 11. p. 12, 2016.

[82] ICO, "Data Protection Act 2018." [Online]. Available: https://ico.org.uk/for-organisations/data-protection-act-2018/.

[83] Economic Commission for Europe, “UNECE Intelligent Transport Systems (ITS) for sustainable mobility.” .

[84] NCSC, “Risk Management.” [Online]. Available: https://www.ncsc.gov.uk/guidance/risk-management-collection. [Accessed: 01-Jul-2018].

[85] Cabinet Office, “Interim Cyber Security Science & Technology Strategy: Future-Proofing Cyber Security,” p. 20, 2017.

[86] NCSC, “Summary of risk methods and frameworks.” [Online]. Available: https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks. [Accessed: 19-Aug-2018].

[87] “NCSC Sociotechnical blog.” [Online]. Available: https://www.ncsc.gov.uk/blog/sociotechnical-security. [Accessed: 18-Aug-2018].

[88] NHTSA, “Cybersecurity Best Practices for Modern Vehicles,” 2016.

[89] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, “SAHARA: A Security-Aware Hazard and Risk Analysis Method,” *2015 Des. Autom. Test Eur. Conf. Exhib.*, pp. 621–624, 2015.

[90] W. Young and N. Leveson, “Systems thinking for safety and security,” in *Proceedings of the 29th Annual Computer Security Applications Conference on - ACSAC ’13*, 2013, pp. 1–8.

[91] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, “Threat and Risk Assessment Methodologies in the Automotive Domain,” *Procedia Comput. Sci.*, vol. 83, pp. 1288–1294, Jan. 2016.

[92] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, “Using SAE J3061 for automotive security requirement engineering,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 9923 LNCS, pp. 157–170.

[93] Roke, “UK 5*STARS CONSORTIUM TO FOCUS ON AUTOMOTIVE CYBER SECURITY,” 2017. [Online]. Available: https://www.roke.co.uk/media/news/news-2017/ccav. [Accessed: 01-Aug-2018].