International Review of Law, Computers & Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Tempting the Fate of the furious: cyber security and autonomous cars

Scott McLachlan, Burkhard Schafer, Kudakwashe Dube, Evangelia Kyrimi & Norman Fenton

To cite this article: Scott McLachlan, Burkhard Schafer, Kudakwashe Dube, Evangelia Kyrimi & Norman Fenton (2022): Tempting the Fate of the furious: cyber security and autonomous cars, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2022.2060466

To link to this article: https://doi.org/10.1080/13600869.2022.2060466

Published online: 25 May 2022.

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
https://doi.org/10.1080/13600869.2022.2060466

Tempting the Fate of the furious: cyber security and autonomous cars

Scott McLachlan[a]*, Burkhard Schafer[a], Kudakwashe Dube[b], Evangelia Kyrimi[c] and Norman Fenton[d]

[a]Edinburgh Law School, University of Edinburgh, Edinburgh, UK; [b]School of Fundamental Sciences, Massey University, Palmerston North, New Zealand; [c]Risk and Information Management, Queen Mary University of London, London, UK; [d]Health Informatics and Knowledge Engineering Research (HiKER) Group

ABSTRACT

The United Nations Economic Commission for Europe (UN ECE) has developed new aspects of its WP.29 *agreement for harmonising vehicle regulations*, focusing on the regulation of vehicle manufacturers' approaches to ensuring vehicle cyber security by requiring implementation of an approved *cyber security management system* (CSMS). This paper investigates the background, framework and content of WP.29's cyber security regulation. We provide an overall description of the processes required to become certified, discuss key gaps, issues and the impacts of implementation on stakeholders, and provide recommendations for manufacturers and the authorities who will oversee the operation. Putting the discussion into a broader theoretical framework on risk certification, we explore to the role of non-academic sources to shape public risk perception and to drive, for better or worse, legislative responses.

KEYWORDS

Automotive; cyber security; vehicle regulation

The major difference between a thing that might go wrong and a thing that cannot possibly go wrong is that when a thing that cannot possibly go wrong goes wrong it usually turns out to be impossible to get at and repair.

Douglas Adams

Guess we have some improvements to make before production haha.[1]

Elon Musk

(Tesla CEO)

CONTACT Scott McLachlan s.mclachlan@qmul.ac.uk Edinburgh Law School, University of Edinburgh, Edinburgh, UK

*Present address: Health Informatics and Knowledge Engineering Research (HiKER) Group; Edinburgh Law School, University of Edinburgh, Edinburgh, UK

1. Introduction

In 2017, *The Fate of the Furious* reflected public anxieties about automated cars, with scenes of remotely-hacked driverless *zombie* vehicles speeding dangerously through crowded streets to collide with other cars, buildings and people (Wolk 2018).

The film fed into a steady stream of news reporting the latest vulnerability discovered in autonomous vehicles. It wasn't long before national and international legislators and regulators were beginning to respond to the growing public concern. The two new sets of rules by the *United Nations Economic Commission for Europe World Forum for Harmonisation of Vehicle Regulations Working Party 29* (UN ECE WP.29) may not be the most riveting read, and, in comparison to The Fate of the Furious, suffer from a predictable plot and slow character development: but then, for its creators, 'nothing happening at all' would mean an impossible mission successfully completed.

This article investigates the content, scope and potential effect of the new UN ECE WP.29 Cyber Security and Cyber Security Management System regulation for motor vehicles (the Regulation) drafted during 2020 and first published in January 2021. It will: (a) review provisions of *the Regulation*; (b) explain the application of and process for achieving UN ECE WP.29 certification; (c) investigate and discuss *the Regulation's* stakeholders and potential impacts; and (d) put the proposal into a wider historical context to identify strengths and weaknesses.

To do this, we will put it into a wider context of public discourse on autonomous driving. We will look in particular at the question of how risk perception is shaped by a complex mix of popular culture, media reporting of scientific-technological studies and also, arguably, some self-serving claims made by various industry players. This mix could lead to the danger that the resulting initiatives respond to (mere) perceptions of risks that are not grounded in strong empirical data, skew the regulatory responses away from mundane but real dangers towards spectacular but low probability events, and ultimately create a 'security theatre' that may make technology more trusted, but not more trustworthy.

2. Driving dangerously: the emerging security landscape for autonomous cars

In 2013, vehicle security researchers Charlie Miller and Chris Valasek sat in the back seat of a 1.6 ton Ford SUV driven by journalist Andy Greenberg (Greenberg 2013). Using a MacBook computer connected via a data cable to the OBD-II data port commonly located under the dash of most modern vehicles, Miller demonstrated how easy it was to disable the imposing vehicle's brakes, causing the pedal to drop alarmingly to the floor as they drove slowly through an empty shopping centre car park. In 2015, Miller and Valasek put the same journalist in a Jeep Cherokee and from several kilometres away and demonstrated that they could remotely control safety critical systems like brakes and steering, as well as minor components like air conditioning and windscreen wipers (Greenberg 2015). As a result, Chrysler issued an unprecedented recall to update the software in 1.4 million motor vehicles (BBC 2015). Buoyed by these and other similar research-based examples (Tengler 2020), and numerous academic articles portending cyber security risks and potential motor vehicle cyberattack scenarios

(Macher et al. 2020), the media jumped on stories about the threat to safety for the general public with alarming headlines about vehicle cyber security flaws and the potential life-threatening harms of car hacking (Mortimer 2015). Some authors continue to depict scenarios that see totally unprepared vehicle manufacturers paving the way for cyberattacks on cars that during rush hour bring whole cities to a standstill, or cause significant property damage and loss of life (Ryan 2020; Lee 2019; Vivek et al. 2019).

Just how problematic this convergence of media reporting and academic futurology can become can be seen also by the way in which it can influence academic writing; in one case is a paper using fictional scenarios to elicit societal implications of autonomous vehicles (Ryan 2020). However, these scenarios claim to be grounded in reality, substantiated by a reference to an attack on London that 'used crypto malware to extort money from passengers before releasing control of the vehicle'. We did not succeed finding any external evidence of such an attack. Rather, it seems to have been based on an equally fictional scenario described in two mainstream newspaper articles of the day (Kiss 2016; Beall 2016). Their reporting also blurred the boundaries between reports of actual events and extrapolations of these into possible future threats, which makes it understandable that some may have read them as reports of actual events. Be this as it may, it points to a potentially closed loop between popular media reports on technological risks and academic study of these risks, each informing the other and, in the process, limiting the opportunity of external validation, while creating a dystopian picture for popular consumption that combines appealing plot development with academic gravitas.

In response to the various simulated cyberattacks, the ensuing headlines, and public calls for regulators to intercede, governments began developing regulations to establish standards for motor vehicle cyber security. However, regulatory responses to high-profile, but ultimately 'local' events risk the emergence of multiple potentially unaligned regulatory regimes. The cost of developing separate models of the same vehicle with seemingly minor *tweaks* to satisfy the internal regulation of different markets can be prohibitive, as much as USD$50 m for one vehicle model (Kreindler 2013). This can lead manufacturers to withdraw from, or not even develop, models for sale in some countries (Welch and Cheok 2020).[2] Organisations such as the *International Organisation for Standardization* (ISO), *SAE International*, and the *United Nations Economic Commission for Europe* (UN ECE) have sought to mitigate these market risks by developing frameworks for standards and regulation designed for consistent application across all member countries. The original UN ECE WP.29 *agreement for harmonising vehicle regulations* was formed in 1958 to establish uniform standards for vehicles and their components in relation to safety, environment, energy and anti-theft requirements for member states (UNECE 1995). Revision 2 (Rev2) of WP.29 was ratified in 1995 and encouraged membership outside of what had been mostly European countries (UNECE 2016). The addition of Japan, Australia, South Africa and others as contracting parties made WP.29 Rev2 a truly global agreement. The current list of contracting member states includes 54 countries at January 2021 when the *Cyber Security and Cyber Security Management Systems* regulation reviewed in this work was released.

Safety engineering and assessment have long been integral to automotive engineering (Macher 2020). IEC 61508 Ed 2 was developed to provide safety standards for electrical, electronic and programmable electronic systems (E/E/PE). Published in 2010, it helped provide the first fundamental steps towards recognising that security threats *should* be

considered as part of hazard analysis and prescribed: (a) development of a *safety life cycle* to discover and eliminate design errors and omissions; and (b) use of a probabilistic failure approach to account for the impact of device failure. ISO 26262 was a 2011 adaptation of IEC 61508 for automotive E/E systems that was widely adopted by the automotive industry. However, with the release of EVs and semi-automated ADAS functions, much of the technology and connectivity in motor vehicles has moved on considerably since 2010.

As shown in the timeline in Figure 1, the first organisation to respond to Miller and Valasek's 2013 and 2015 demonstrations was the SAE who in 2016 presented the SAE J3061 guidebook for cyber-physical vehicle systems (SAE 2016). This release also marked the start of a collaboration between SAE and ISO to develop a comprehensive standard for motor vehicles, resulting in the early 2020 release of ISO/SAE 21434 *draft international standard* (DIS) to help manufacturers to (a) define a structured process for ensuring cyber-secure design; (b) reduce the potential for successful attacks and losses; and (c) provide clear and consistent approaches to react to cyber security threats (Macher 2020). ISO/SAE 21434 is intended to supersede or replace SAE J3061 (Oliver 2020).

In November 2019, the *European Union Agency for Cybersecurity* (ENISA) released the first version of a report titled *Good Practices for Security of Smart Cars* (ENISA 2019). This report presented asset and threat taxonomies that are multi-layered, but where each type of device or attack is assumed to be mutually exclusive. ENISA proposed a range of attack scenarios and provided each with a severity score. However, the standard or risk model by which these scores and their effect ratings were derived remains unclear. This is a general weakness observed in *United Nations* and *European Commission* safety standards and regulations that is being addressed in work such as that of Hunte, Fenton, and Neil 2020.

In June 2020, the UN ECE's *World Forum for Harmonization of Vehicle Regulations* publicly released its submission for a standardised framework for approval of vehicle cyber security and cyber security management systems. This submission and the draft regulation it proposed, which are informed by ISO/SAE 21434, are what became *the Regulation* investigated in this work.

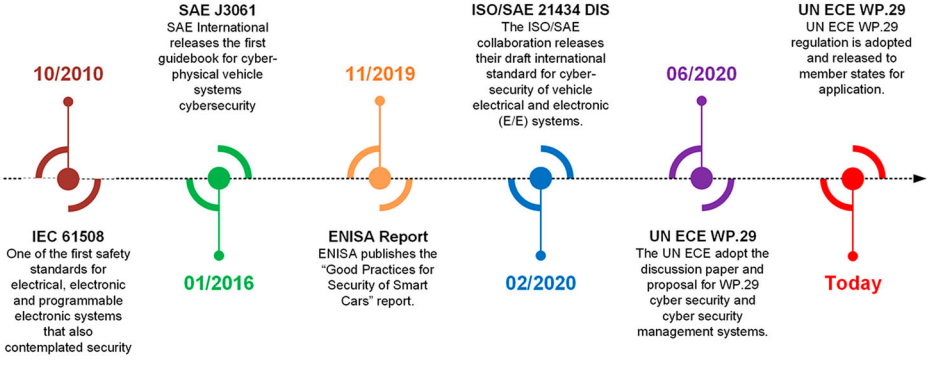

Figure 1. UN ECE WP.29 timeline.

3. Modern vehicle or mobile computer terminal?

One particular danger in the way in which we frame and analyse security risks for 'intelligent' vehicles is that we focus on a point in the near future, where highly autonomous vehicles are stipulated to be the norm. That framing creates a chasm between these 'new' machines and the risk they bring, making it more difficult to learn from the past and marshal data we already have for a more grounded risk assessment. It is therefore helpful to put the development of 'smart' cars in a historical context. In 1968, German car manufacturer Volkswagen (VW) released the first vehicles with *electronic fuel injection* (EFI) (Buttgereit, Voges, and Schilter 1968). Using sensors to monitor a variety of engine metrics and a Bosch-designed but still quite rudimentary control unit to determine engine fuel requirements, EFI would go on to replace the carburettor in all modern engines. However, it was not until General Motors (GM) released the 1977 Oldsmobile Toronado that the first microcomputer-based *electronic control units* (ECU) were integrated into a production vehicle. By 1981, all GM vehicles were equipped with computer-based control systems (Charette 2009), and every other manufacturer soon followed GM's lead. GM's ECU represented the first steps along a winding path leading to the *automated driver assist systems* (ADAS) that have become ubiquitous in present-day cars, and the self-driving or autonomous *vehicles of tomorrow*.

Modern vehicles have been described as sophisticated computers, with so much internal and external connectivity that they have become new mobile nodes of the *Internet of Things* (IoT) (Gerla et al. 2014). The cost of software, microcomputers and complex electronics is estimated to account for as much as 35–40 per cent of the total cost of every vehicle coming off the production line (Buckl et al. 2012). Today's vehicles contain more than 100 million lines of code embedded within an integrated array of 70–100 ECUs from many different suppliers (Levi, Allouche, and Kontorovich 2018; Payne 2019). Much of the complexity of modern vehicles comes because the functions enabled by all this software and computing power are highly interconnected; integrating streams of sensor data, mechanical actuators and ADAS including *anti-lock brakes*, *forward collision mitigation*, *adaptive cruise control* and *blind spot detection* with information delivered to, and inputs from, the driver (Buckl et al. 2012). The current shift toward electric (EV) and self-driving (SDV) vehicles is only increasing that complexity, which some argue makes the removal of the human driver from the loop not just a possibility or desirable, but a necessity (For a discussion, Wagner and Koopman 2015; Pelliccione et al. 2017). Crucially, not all of the integration that we observe is necessary just for driving the car. Customisable entertainment electronics is also routinely integrated into the system, to enable e.g. recommendation of radio stations from location data. These design choices that can all create cyber security risks need to be taken, but are generally accepted, and then remedied through better cyber security measures.

As noted above, while cyber security researchers *have* demonstrated illicit remote control of a subset of vehicle functions, these *simulated attacks* have tended to require both a human driver to start the vehicle or put the vehicle's transmission into gear, and some prior exploitation of the software or systems to gain knowledge of or prepare the attack on a target vehicle (Miller 2019). In their cyberattack demonstration described in Section 1, Miller and Valasek identified a vulnerability in the Harmon Kardon-supplied infotainment unit and used this to reprogram a gateway chip in the

stereo unit that had access to the vehicle's *controller area network* (CAN). This enabled them to be able to capture and view messages travelling between various *command and control* ECUs in the vehicle, and eventually to take control of several physical systems in the car, including steering and braking. They were further able to demonstrate that, where the vehicle also had cellular connectivity, it was also possible to connect with, implant the reprogrammed software they developed, and take control of the remote vehicle without ever having had physical access. The only prerequisite required for their remote attack was for the vehicle's owner to have already switched on and be operating the car. Miller himself contends these issues can be easily mitigated by applying existing technologies and enterprise security techniques. Toyota, in their response to the experiment, replied that 'Our focus, and that of the entire auto industry, is to prevent hacking from a remote wireless device outside of the vehicle', and WP.29 ostensibly shares this focus.

With this we can start our discussion on whether WP.29 is sufficient for the task, or tries to solve the wrong problems with the wrong tools.

4. The long road to UN ECE cyber security certification

The main objective of WP. 29 is to create a system of certification. Ideally, vehicles and their components that pass this test are then demonstrably trustworthy with regards to the security aspect. This effort builds on a number of existing certification initiatives for IoT security more generally, for instance the European Cyber Security Organisation Working Group 1 (ECSO WG1) that develops standards, certification, and labelling,[3] the European Union Agency for Network and Information Security (ENISA) and its proposal for privacy online seals that can visualise the different dimensions of security (Tschofenig et al. 2013) or the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[4]

4.1. Cyber Security Management System (CSMS) Certification

We can now look in more detail at WP.29 There is a minimum of four primary phases required to complete the WP.29 process. These are (i) CSMS certification; (ii) RxSWIN process development; (iii) SUMS approval; and (iv) TYPE certification. This section describes each phase, the approach to realising in-country local administration and homologation, and provides a roadmap for demonstrating the interdependencies and the order in which the phases must be completed.

The first step towards attaining certification that is described in WP.29 is the development of the *Cyber Security Management System* (CSMS). The CSMS is a set of interrelated systems and processes that together enable everyone within the organisation to know what they need to do, and how and when to do it in order to achieve and maintain security (Dexter 2002). The primary purpose for requiring a CSMS is to encourage cyber security to become integral to organisational culture and governance. Relevant policies, rules and processes must be developed and implemented both within the manufacturer's organisation and right through the entire supply chain. These policies should address cyber security matters during the vehicle's design, development, production, operation, maintenance, and decommissioning. A range of requirements

for the CSMS are provided in WP.29 Section 7 that include that the CSMS should govern processes for cyber security risk management, information sharing, vulnerability identification and disclosure, lifecycle monitoring and overall incident response. However, WP.29 provides its 7 categories of threats and 23 cyber security mitigations in broad overarching terms and leaves the manufacturer to develop their own conforming processes,[5] documentation[6] and approaches for demonstrating that the CSMS will realise the necessary outcomes. Figure 2 identifies four primary processes that a manufacturer is required to develop for managing cyberattacks as components of their overall CSMS strategy.

In order to develop and establish their CSMS, manufacturers are referred[7] to standards like ISO/SAE 21434 which in accessible language describes the process of CSMS development with five primary steps:

1. Appoint a security manager who will have overall responsibility for the CSMS
2. Identify the risks within your organisation
3. Mitigate those risks with security solutions
4. Issue cyber security policies based on your risks
5. Train your staff on your risks and policies, and then test their awareness

ISO/SAE 21434 also provides some strategies for key WP.29 CSMS tasks, such as how to secure the supply chain.

When certifying a vehicle TYPE, the Approval Authority (AA) is required to verify that all of the requirements for the CSMS laid out in Section 7 have been effectively fulfilled.[8] This establishes the requirement for CSMS certification to have been successfully achieved prior to any application for vehicle TYPE certification.

4.2. RxSWIN

RxSWIN are unique *software identification numbers* assigned for each certified vehicle TYPE that identifies software (function) that is impacted by a software update. It is proposed that at some future point RxSWIN could be read from the vehicle as part of market surveillance (i.e. during annual maintenance checks)[9] to verify whether TYPE-approved updates are present in the vehicle.

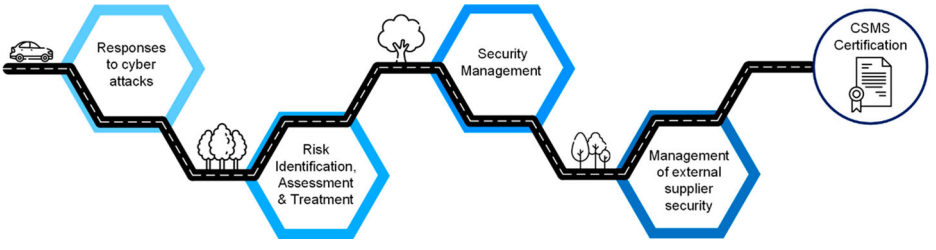

Figure 2. CSMS certification roadmap: Primary processes for managing cyberattacks.

4.3. Software Update Management System (SUMS)

WP.29 requires manufacturers to develop and implement a *software update management system* (SUMS) and demonstrate SUMS compliance prior to seeking vehicle TYPE certification. It is expected that implementation of SUMS will ensure: (a) more robust governance of software update development, approval and deployment; (b) increased awareness and visibility of the impact that software updating has, including on drivers; and (c) traceability for external authorities. Put simply, the UN ECE recommendation on software updates sets out principles to ensure updates are conducted safely and in compliance with other UN ECE regulatory requirements, whether performed wirelessly or using other means.

Figure 3 shows the four primary organisation and process requirements SUMS imposes, including (i) maintenance of software version numbers (RxSWIN); (ii) validation of software compatibilities and dependencies; (iii) ensuring safety and security of the update during development, deployment and installation; and (iv) being aware of the current circumstances of the vehicle (i.e. whether it is in transit or stationary) and informing the user about the update.

4.4. Vehicle Type Certification

In order to sell any vehicle in a particular country, the manufacturer must demonstrate that vehicle's conformity to applicable regulatory standards and specifications for that market (Martins 2010). *Type approval* and *homologation* are two terms used to describe the process by which the manufacturer demonstrates compliance with local legal requirements through witnessed testing and the provision of supporting evidence. Even though different markets may have regulatory requirements that are exactly the same, different testing and homologation processes may be required (Martins 2010). One of the goals of WP.29 is to provide a regulatory framework that promotes standardisation, such that successful validation and the receipt of certification in one WP.29 market should provide manufacturers with the ability to sell that vehicle type in other WP.29 markets.

In order to achieve vehicle TYPE certification, the manufacturer must demonstrate to the local authority through documentation: (a) rigorous application of their CSMS risk management processes for that vehicle type; (b) implementation of security controls in that vehicle type's lifecycle; (c) that potential vulnerabilities and critical areas have been identified; and (d) those vulnerabilities and critical areas and any mitigations have been tested. This roadmap to TYPE certification is shown in Figure 4.

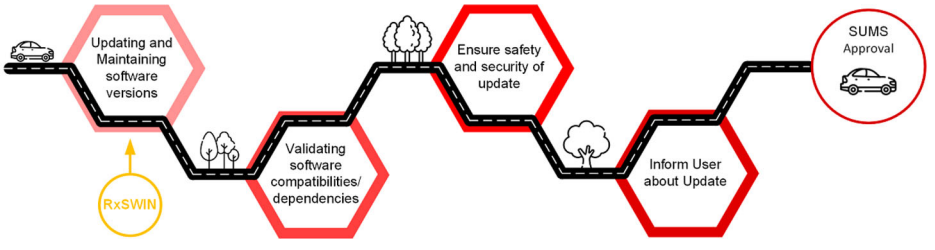

Figure 3. SUMS certification roadmap: Primary organisation and process requirements.

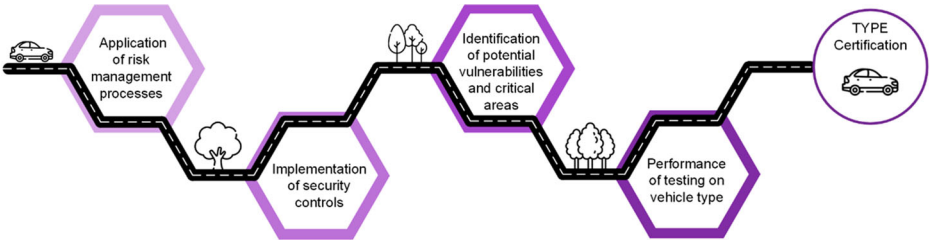

Figure 4. TYPE certification roadmap: Manufacturer demonstrable processes.

4.5. Overall Certification Process

There are dependencies and an interrelationship between each of the processes necessary to WP.29 Cyber Security certification, as shown in Figure 5. CSMS certification is required before a TYPE application can commence. SUMS approval incorporating an RxSWIN software versioning protocol is established as components supporting the TYPE certification process. Any TYPE certification application will fail absent of prior certification of CSMS and SUMS.

4.6 Approval Authority

Each contracting member state is required to establish an office to oversee the operation of WP.29 within its borders. This office is described as the *Approval Authority* (AA) and, along with the *Technical Service* (TS) the AA will employ, they will oversee local approval of manufacturer CSMS, SUMS and TYPE certification applications. The AA is called to verify each manufacturer's application for certification initially *by means of document checks*.[10] Where the AA or its TS are called to verify by testing, the scope is limited to ensuring the manufacturer has implemented the cyber security measures they have documented.[11] While further testing is encouraged, the regulation describes testing by means of

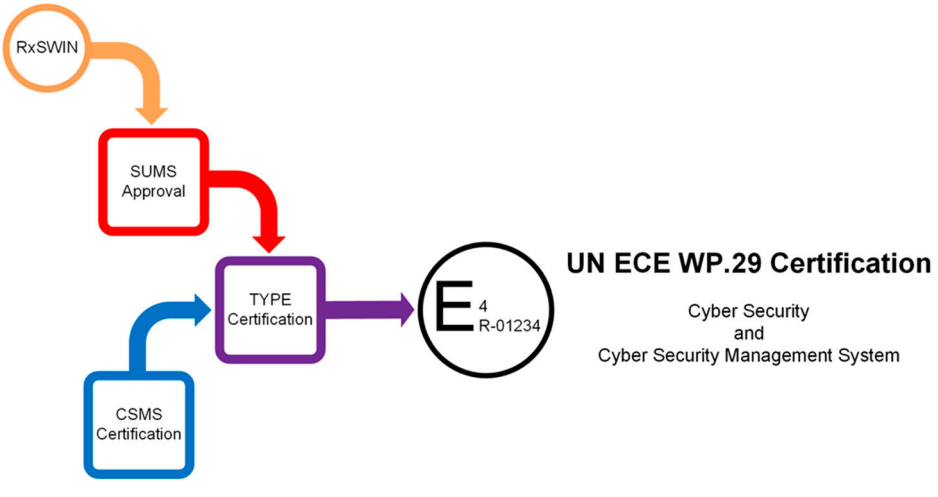

Figure 5. The UN ECE WP.29 certification pathway.

a sampling process primarily focused on but not formally limited to manufacturer-identified high-risk items.[12]

5. WP.29: the good, the bad and the ugly

Our analysis of the intention, content and application of this new cyber security regulation drew attention to five topics requiring further attention. These topics and their impact on key stakeholders are now considered.

WP.29 and ISO/SAE 21434: We can identify four key areas of alignment between WP.29 and ISO/SAE 21434. Both require: (a) development of an effective Cyber Security Management System (CSMS); (b) conduct of thorough Threat Analysis and Risk Assessment (TARA); (c) the manufacturer to manage supply chain security; and (d) securing of the vehicle throughout its complete lifecycle – from development, through production, and during its post-market serviceable years.

A number of important differences can also be identified. The regulation is intended to become legally binding within UN member states which are contracting parties to the original 1958 agreement, or either of the two more recent revisions. While the ISO/SAE standard may be widely accepted in industry, it is not legally binding on any manufacturer or country.

Potentially problematic conflicts could arise in this context with the proposed EU AI Act, which in Art 15(3) mandates cyber security measures. Autonomous vehicles are covered by the Act as High Risk systems under Title III of the Act, as 'AI systems that are products or safety components (broadly construed) of products already covered by certain Union health and safety harmonisation legislation'. The relevant harmonisation legislation is listed in Annex 2, which includes Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.

The AI Act controversially gives quasi-legal status to a closed list of standard setting bodies, specifically the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) as the only European standardisation organisations that the Commission can authorise to develop harmonised standards.[13] While it does not mandate compliance with these standards, it creates very strong incentives for manufacturers to do so in the form of a 'presumption of compliance'. That is, as long as manufacturers comply with the relevant CEN and CENELEC standards, they need not be concerned any longer with their compliance with the substantial duties of the ACT, or whether they chose the right procedures and standards. This has also the effect of potentially devaluing the role of ISO standards, creating a normative conflict if these in turn become the standards adopted by international initiatives such as WP29. Either approach though suffers from the problem that it delegates legislative competence to private sector organisations (and indeed in the case of ISOs 'legislation behind paywalls') which gives voices from outside industry, such as consumer protection groups or civil society, increasingly diminishing scope to shape these rules (On this topic see for the AI Act, Veale and Borgesius 2021).

Additionally, while the WP.29 regulation is prescriptive in a number of areas, including that there will be a centrally maintained broad baseline list of threats for manufacturers to

investigate when assessing whether a vehicle and its connected systems are secure, it does not generally advise on how to undertake such testing. By contrast, the ISO/SAE standard more thoroughly describes approaches such as TARA processes; cyber security management within the manufacturer organisation; and cyber security management of the supply chain.

We have shown that UN ECE WP.29 and ISO/SAE 21434 are complementary without being contradictory; meaning the effort undertaken by a manufacturer to meet the one translates efficiently to meeting many of the certification tasks required of the other. This gives manufacturers a strong and almost singular path to follow for achieving a cyber security standard recognised both within their industry, and the international regulatory community.

Cost to implement: Industry groups have estimated that by 2023, cyberattacks could cost manufacturers as much as USD$24bn in annual losses (Upstream 2019). This claim seems incredible given that the annual global cost of cybercrime for the automotive industry in 2018 was just 0.06% of that amount, (USD$15.78 m) (Statista 2020). Also, while the average cost of a data breach in 2020 was USD$3.86m, only one of the many examples provided on one cyber security analysis website was against an organisation in the automotive industry; a website database attack against UBER's ridesharing app in 2016 (Sobers 2021). Most of the identified cyber security risks faced by vehicle manufacturers remain potential attacks – and an additional concern is that some of these claims come from firms selling cyber security consultancy services (Fraser-King 2020). This alone does not mean the risk is not real – as with anti-virus software, it is maybe inevitable that those who make it their job to build technical countermeasures also know the threat environment best, but it still means to treat these figures with caution. The Australian Government report, mentioned in the introduction to part 5 of this paper, painted a rosy picture of future harmonisation as a zero-cost effort for manufacturers, with minimal administrative costs to be borne by the Australian taxpayer. In contrast, the Center for Automotive Research (CAR) estimated UN ECE harmonisation regulatory compliance costs would be USD$648–873 per vehicle (CAR 2016).

Approval Authority: The logical choice for AA in most countries would be existing motor vehicle registries,[14] due to their ongoing role in registering, taxing, centrally maintaining annual vehicle fitness records and issuing of driving licences. These organisations already regulate the standards necessary to register new or existing motor vehicles, and oversee the requirements and process for approved annual roadworthiness checks. As noted above, Europe is developing a separate regime of AI regulation, and there too a new regime of approval authorities will be necessary. Member states nominate appropriate national bodies, which for some issues are likely to be the information commissioner offices charged with data protection, co-ordinated by a new Europe-wide AI board. How this regime, which overlaps but is not identical to the one developed for WWP.29, will interact is at this point unclear, though it is likely that on a sectoral basis at least, countries will nominate the same institution as approval authority for both. More difficult will be the relation with the approval authorities envisaged by WP29 and the yet to be created European AI supervisory board.

WP.29 reinforces the position that an AA should refuse to grant TYPE approval in a broad range of situations, including where the manufacturer: (a) did not protect the vehicle against risks they previously identified[15]; (b) did not secure dedicated environments

within the vehicle for storage and execution of aftermarket software, services, applications or data,[16] (c) has not put in place satisfactory measures to manage the cyber security aspects covered by WP.29[17]; or (d) where the *manufacturer did not perform exhaustive risk assessment.*[18] However, while the approach and syntax of Section 5.1.3(a) provide scope such that an AA could objectively maintain pace with new technology and the risks it may introduce, it also permits the potential for subjectivity, or at least claims thereof from manufacturers, where an AA has declined an application.

Testing and certification: The approach to verification and testing by the AA is described primarily as two processes: first as *document checks* in Section 5.1.1, and second as testing of implemented cyber security measures, or *mitigations*, in Section 5.1.2. There is strong potential that this may lead to potentially expensive and standardised tokenistic box-ticking exercises (Reddy 2019),[19] with manufacturers less focused on effective cyber security and solely occupied with *being compliant*. This outcome has been observed with other similar attempts to impose regulation and governance on corporate entities (Enriques and Zetzsche 2015). Successfully selling this regulation to the public should include a requirement that the AA performs distinctly more comprehensive testing of each vehicle type as part of the certification process, rather than only testing the mitigations proposed by manufacturers for manufacturer-identified vulnerabilities. The major weakness in this approach is that leaving manufacturers to identify and expose vulnerabilities *in camera* creates potential for known vulnerabilities to remain undisclosed, at least until the manufacturer has developed a working mitigation.

While it is true that harmonised regulation in international markets may bring a myriad of potential benefits, WP.29 reads more like a box-ticking exercise, and presents as regulation for regulation's sake. When: (a) it is more likely that manufacturers will withhold known vulnerabilities from assessment until they are able to mitigate them; (b) the regulator in each country is only called to assess the mitigations of those vulnerabilities that the manufacturer has disclosed; and (c) it is possible in some countries that TYPE evaluation might only occur on entering the marketplace, the most critical or zero-day exploits, which is those requiring the most urgent attention, could remain quietly accessible to hackers well into a vehicle's post-market life, even though WP.29 does create the requirement for ongoing monitoring of cyber security for at least a decade after the vehicle has been sold.

At present, and as a result of other market pressures, many manufacturers are continuing vehicle types and models in the market for significantly longer periods than they have previously. Many new vehicle releases are simply a facelift of the previous version,[20] which means a vehicle TYPE certification could potentially run in production for a decade or more. This could extend the benefits of WP.29 certification. However, it is more likely, as discussed above, that this could lead to greater manufacturer complacency. It may be that with some adjustment to the wording of WP.29 to consider evaluation and certification of *model year releases* as well as *types*, WP.29 could provide a stronger incentive to manufacturers to increase cyber security in each *model year*, and encourage them to provide patching of newly secured vulnerabilities in a way that is backwards compatible to previous model years of the same vehicle type. With this, the main challenge that AI and machine learning technologies bring to cyber security remains unaddressed – the constant change of the underlying data models used for training. Here too potential conflicts with the regulatory regime for AI under the AI Act are likely.

Post-market vehicle surveillance: One key issue that arises from this regulation is the need for manufacturers to provide software updates to mitigate security issues during the vehicle's entire lifecycle. Many markets require regular, often annual, roadworthiness checks to ensure vehicle owners are performing necessary mandatory maintenance of safety-related components such as brakes, tyres, seatbelts, windscreen wipers, lights and any modifications that have been made. However, these checks have generally not extended to verifying the currency of software versions contained in the myriad of ECUs that operate many safety-critical functions.[21] A number of authors have proposed that safety and security-based updates should be made mandatory in law to ensure firstly the manufacturer provides post-market updates and undertakes surveillance to ensure they are applied, and secondly that owners or users of vehicles both allow and ensure these updates are applied to their vehicle (De Bruyne and Werbrouck 2018 and Pearah 2017). The most cost and resource-effective approach to enforcing such regulation would be to inspect software versions during the annual roadworthiness check. Software version details from the vehicle's core systems could be verified against the current details provided by manufacturers for that vehicle type. It should be noted that this would add an additional step to existing vehicle testing processes, which would be likely to increase the cost of annual roadworthiness checks to consumers.

Implementing international standards requiring seatbelts or ABS brakes in all motor vehicles serves to improve safety while bringing the unit cost to consumers of each component down, due to increased economies of scale. Consequently, there can be no doubt that further homologation under an environment of harmonised regulation could bring significant benefit to vehicle manufacturers, regulators and consumers. For manufacturers, it could be as simple as the ability to produce one version of each vehicle type that meets the rules of many markets. For regulators, the core benefit comes in establishing: (a) an evaluation and certification standard that all member states can apply consistently; and (b) the provision of a central repository for recording certification and reporting each vehicle type's manufacturer-reported issues and successful mitigations that regulators have verified. This database is also intended to provide a core set of potential vulnerabilities for future manufacturer and regulator vehicle testing. Finally, for consumers it could mean confidence in knowing that every vehicle they drive (irrespective of whether it was sold locally, imported, or is even a holiday rental overseas) was required to meet the same standard for engineering, security and safety.

6. Of hot steam and cold wars: the worries we should have and the worries we wished we had

The analysis of WP29 so far gave us a mixed picture: probably well intentioned, the TYPE approval system and the long lead-ins mean that the new problems created by smart vehicles are at best partially addressed. Worse, car manufacturers at least in part mark their own homework, and can simply choose not to disclose the most worrying aspects. It will create income opportunities for private sector companies such as Deloitte that will provide certification services, but without a mechanism to externally evaluate if the resulting system is really increasing security. As noted above, this is an inherent problem of 'forward looking' certification: if nothing happens, was it because of the robustness of the security certification, or because there was no appetite by adversaries

to attack the system in the first place? This problem is not new: back in 2009, Anderson showed how certification systems have often failed in to lead to real improvements of security, while sustaining a certification industry that may contribute to the trust people place in technology, but not necessarily its trustworthiness (Anderson and Fuloria 2009). It does not look as if the lessons from these approaches have been learnt, Worse, the shift in application from military security certification to civilian uses means that that the social and political advantages that were gained during the cold war through certification are unlikely to accrue here.

In this final section, we will put WP.29 in a broader historical and theoretical context, building on the short discussion in section 4 in order to evaluate some of its key aspects.

As noted above, certification as a regulatory innovation was a nineteenth century response to the highly volatile and explosion-prone steam boilers, whose role in deadly accidents led to the first examples of test-and-certify schemes. In the UK, the Report from the Select Committee on Steam Boats from 1817, set up in response to the explosion on board of a ship that led to 12 fatalities and numerous injuries, recommended a system of external inspection and certification of safety valves. Parliament, however, was slow to act on the recommendations, though occasional accidents would trigger similar inquiries (Ozawa et al. 2021 and House of Commons 1817).[22]

Many of the discussion points in the debate in the nineteenth century will sound familiar to present-day readers interested in AI regulation. Illuminating for our purposes is in particular Sir John Rennie's submission to the Select Committee in 1843 (discussed in detail in Burke 1966). As one of the major boiler manufacturers, Rennie opposed any regulation that could act as an impediment to innovation and the commercial exploitation of steam power. Instead, established rules of liability and post-incident litigation were sufficient to ensure that manufacturers would minimise the risk as much as possible – not only because of the fear of damages awarded against them but also because in his view the inquests held by coroners' juries were so detailed that the reputational risk for manufacturers was significant. By contrast, a regime of constant examination of boilers would create costs and inconvenience without really contributing to public safety. If anything, the public would be lulled into a false sense of security. The range of boiler and engine designs in particular made a uniform testing and certification process unfeasible – this echoes the discussion surrounding Type certification as a contemporary but ultimately unconvincing answer to a similar problem.

In the same way as we discussed above in the present, newspaper reporting, 'popular science reporting' and public perception also shaped responses to technology in the 19th century, for better or worse. Reports about the explosion of the 'Aetna' in 1824 that killed thirteen people and seriously injured many more is a case in point (For a full account of the Aetna accident and the public response, see Burke 1966, 8). The Aetna had deployed pressure boilers made from wrought iron. Previously, the majority of steamboats in New York had used copper boilers, but at much less dangerous lower temperatures. Drawing the wrong inference from the Aetna disaster, the public began to consider copper boilers inherently safer, even at high pressures, contrary to the emerging scientific consensus. Market pressures then seem to have delayed the use of the safer technology: what the public trusted more was in reality less trustworthy.

Similarly with WP29: it responds to fears of scenarios that are novel and, as depicted in the media, also terrifying in scope (the Fast and Furious scenario) and on the impact on

the individual; what can be more frightening to lose control over a fast-moving vehicle and succumb to the will of an adversary (the Miller and Valasek scenario). However, our research, based on an extensive literature survey, found no evidence of this type of attack occurring in the wild. At least one person, however, has been prosecuted for accessing the web-based immobilisation tool of his former employer to 'brick' over 100 cars (Poulsen 2010). However, that was an aftermarket device fitted to the vehicles by an overly wary financier, and was not a manufacturer-installed production component. What we can find, however, are attacks against smart cars that follow much more established patterns, especially attempts to extract information and turn them into surveillance tools.

In Australia, a mechanic was convicted of stalking offences after he used a vehicle manufacturer-supplied software (Land Rover's InControl App)[23] to control the start/stop function and access location-based data of an ex-girlfriend's vehicle (Bevin 2019). In the UK, a man was charged with theft offences and received a five-year prison sentence for his part in removing the *Electronic Ignition Switch* from over 100 late-model Mercedes vehicles, using the manufacturer's computer software to 'code' new blank keys to the switch, and on returning the switches to the original vehicles, using the blank keys to steal them (Suffolk Police 2021). This, however, is a systemic problem, and much less likely to be solved by a simple technological fix, as here the interests of industry and those of possible criminals – to get as much information about drivers as possible, align.

Back in the 19th century, the debate on steam engine regulation remained fierce and controversial. Proponents of regulation warned that the law was not going far enough, and left too much control to the owners and operators of the ship. Opponents continued to warn against over-regulation and obstacles to innovation. For our purposes, one particularly interesting argument was mooted by some opponents of the law. If steam boilers were as dangerous as the expert reports made them out to be, so the argument went, then the debate was misconceived from the beginning.

While legislation in the UK and US was slow and often inefficient, a very different development took place in France. There, from the beginning, the problem was framed as one of 'engineering-informed law' rather than a pure engineering question, or one for the markets to settle. From the 1830s onwards, France began introducing a series of safety standards and a state-administered certification scheme, notably with criminal punishment against attempts to circumvent the technical safety measures, and criminal sanctions against corrupt certification officials backing up the law. It is difficult to quantify if this more aggressive approach to certification was more successful in protecting life, but at least contemporary commentators expressed their belief that travelling on the Seine was considerably safer than on the Mississippi. Some of the reasons for this difference in approach were political in nature. In the US, the question of whether the federal government had the appropriate competency to legislate at all was central to the discussion. For obvious reasons this was not an issue for the highly centralised Napoleonic France with its developed, and overall highly trusted, administrative bodies. There was however also a cultural difference, a topic that gets us back to the Fast and the Furious with which we started this paper.

In France, politically connected public intellectuals such as François Arago, Arthur Mangin and most of all Eugène Huzar in his 'La Fin du monde par la science' had popularised not only the new technologies and made them accessible to the general public,

they had embedded these accounts in ambitious and far-reaching visions of the future. These more often than not had dystopian overtones, Huzar's book depicting the end of the world as a result of scientific hubris. But despite this, they were not anti-science, or anti-technology the way in which in the UK, romanticists like William Blake railed against the 'Satanic Mills'. In Huzar's own words, 'I wage war on neither science nor progress, but I am the implacable enemy of an ignorant science, of a blind progress that walks with no guide and no compass' (Huzar 1855). Fiction then becomes one of the ways a 'guide and compass' can be provided, by opening up a wider debate on what type of future society wants. Depiction of catastrophic risks is an integral part of this endeavour, because it equips us with the tools to determine which paths to pursue, which goals to seek, and what type of government intervention may be needed to reach them (Fressoz 2007).

We can now bring past and present together to explain why 'tick box approaches', that are at least partly what WP.29 delivers, are, despite their shortcomings, so difficult to avoid and so ubiquitous. As we have seen, popular accounts of technology and its risks have always played, and continue to play, an important role in shaping legal responses to innovation, for better or worse. Huzar's book contains stories of disasters on a significant scale, but crucially, they happen within societies that are also reaping the benefits of innovation. Huzar saw himself as an advocate, not a detractor, of technological progress. By providing a positive vision of the future, a common stake in the success of the enterprise is generated, allowing us to see regulation as a way to prevent incidents that ultimately harm all parties.

There is a symmetry here with the Fast and Furious film we mentioned above. There too, for the disaster to unfold, it is assumed that autonomous driving is already a success, and so widely adopted that any successful attack against the system has consequences far beyond an individual compromised car. We call these types of worries 'wishful worries', borrowing the term from technology historian David Brock (Brock 2019). He defines wishful worries as 'problems that it would be nice to have', but which 'function as pleasant distractions from what one might call our actual agonies'. Often, says Brock, they are set in some vaguely defined near-future where what is now an experimental technology has already been fully accepted and integrated into everyday life. These popular accounts inevitably exaggerate the technical feasibility of these technologies, and assume as resolved issues that in the present are still hard problems. Yes, it would be nice to live in the world of Fast and Furious, where we can all relax on the morning commute as our car drives us to our destination. Only against this background of already-resolved technological issues can the catastrophic failure of the system take place. The danger then becomes that the dystopian element takes centre stage in the discussion on regulation – something has to be done about it now – losing sight of all the very real issues that cause harm in the now: for instance, as we noted above, the privacy hazards of even relatively 'dumb' cars that are on our roads today.

Besides these wishful worries, there is a similar category of concerns that our paper indicated. We call them 'comforting worries'. Comforting worries can be very real concerns. They are however concerns for which relatively straightforward solutions are available. In all the security breaches described above, there was an easy and often inexpensive remedy: debug some code, slightly redesign some hardware, upgrade some chips. None of them calls into question the underlying design rationale, or the

desirability of autonomous vehicles. As we have seen, a significant number of successful attacks use as the point of entry parts of the system that are not essential for driving, in particular the car's entertainment system. Just as some in 1838 asked if the inherent dangers of steam boilers, as they then were, should lead to their prohibition, so we can ask if the inherent dangers of combining (often customisable) entertainment software with safety-essential components should be permitted at all. A certification scheme can then create a 'comforting worry' that reassures us that any problem can be solved, without addressing the root causes. The 1836 US law, and quite possibly WP. 29, did have the effect of directing public concerns away from the more fundamental societal discussions and decisions to those problems the industry felt capable of solving in the short term, with costs that often can be passed on to the drivers in any case.

With its cybersecure E-badge *carrot*, and ability to become a legal requirement in contracting states, WP.29 may appear at first blush as a *stick* that can be used to ensure manufacturers remain vigilant regarding the cyber security of vehicles they produce. However, it could equally be said that once the vehicle is in the market, or even three years later when that model may no longer be in production, WP.29's stick in its current form could be found to be more like wet spaghetti and not the bamboo cane the UN might promote it as.

Notes

1. A Tweet by Elon Musk. Retrieved from https://twitter.com/elonmusk/status/1198090787520598016
2. In February 2020, General Motors announced their withdrawal from the right-hand drive (RHD) markets of Australia, New Zealand and Thailand due in part to the high cost of making country-specific RHD vehicles for these small markets, and the claim that their two largest markets, the left-hand drive (LHD) markets of USA and China, were financially supporting RHD vehicle production.
3. ECSO, WG 1: Standardization certification labelling and supply chain management. Available at https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf.
4. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Technical Report (2018), 10.6028/nist.cswp.04162018.
5. WP.29, Section 7.2.2.2 requires manufacturers to demonstrate that the processes they use ensure security and risks are adequately considered both in developing and applying the CSMS, and in the way they mitigate any cyber security issues identified in their organisation, supply chain or vehicles.
6. WP.29, Section 6.3 prescribes that documentation describing the CSMS is to be submitted by manufacturers to the Approving Authority. However, it does not go on to lay out the format or granular content of that CSMS documentation.
7. A footnote to Section 5.3.1(a) provides ISO 26262-2018, ISO/PAS 21448 and ISO/SAE 21434 as examples that offer suitable standards of knowledge for CSMS.
8. WP.29, Section 5.3.
9. In many jurisdictions, annual vehicle maintenance safety checks are mandated as part of the registration process for a motor vehicle. For example, in Australia these are referred to as a *roadworthiness check*, in the UK they are known as an *MOT test*, and in New Zealand they are described as a *warrant of fitness*.
10. ECE/TRANS/WP.29/2020/79 Revised, Section 5.1.1.
11. *Ibid.,* Section 5.1.2.
12. *Ibid.*

13. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025
14. For example: the Roads and Traffic Authority (RTA) in NSW, Australia; New Zealand Transport Agency (NZTA); and Driver and Vehicle Licensing Authority (DVLA) in the United Kingdom.
15. WP.29, Section 5.1.3(b).
16. WP.29, Section 5.1.3(c).
17. WP.29, Section 5.3.
18. WP.29, Section 5.1.3(a).
19. Box ticking manifests itself firstly, by companies complying with the letter rather than the spirit of the provisions, and, second, by companies not utilising the inherent flexibility of the code to implement their optimum firm-specific governance structures by explaining rather than complying.
20. For example, Chrysler and Dodge have continued to offer model year updated versions of the 2008 Dodge Caravan/Voyager and Dodge Journey vehicles well into 2020, meaning that these vehicle TYPEs remained in production with various model year facelifts for over 12 years. Australia's General Motors brand, Holden, released the VE commodore in 2006 and through a number of facelifts and rebadging as the VF it was offered for sale until quite late in 2017; an 11-year production run. In all cases these vehicles received additional *options* and technologies during their prolonged sales periods, including several sophisticated ADAS systems.
21. Like *anti-lock brakes*, *blind-spot detectio*n, *forward collision mitigation* or *lane keeping*.
22. Report of the select committee appointed to consider of the means of preventing the mischief of explosion from happening on board steam-boats, to the danger or destruction of His Majesty's subjects on board such boats. Available at https://hdl.handle.net/2027/nyp.33433010754467
23. Land Rover's InControl App. Available at https://www.landrover.com.au/ownership/incontrol/connectivity/incontrol-remote-premium.html

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

McLachlan and Schafer were supported by grant EP/T026952/1 AISEC; McLachlan was additionally supported by a grant from the Royal Academy of Engineering (RAEng) - Safer aviation from ethical Autonomous Intelligence Regulation (SafeAIR) (ICRF2122-5-234); Schafer was additionally supported by a grant from the UKRI Strategic Priorities Fund to the UKRI Research Node on Trustworthy Autonomous Systems Governance and Regulation (EP/V026607/1, 2020-2024).

References

Anderson, R., and S. Fuloria. 2009, September 22–25. "Certification and Evaluation: A Security Economics Perspective." *IEEE Conference on Emerging Technologies and Factory Automation*, 1–7, Palma de Mallorca, Spain. IEEE.

BBC. 2015. "Fiat Chrysler recalls 1.4 million cars after Jeep hack" https://www.bbc.co.uk/news/technology-33650491.

Beall, A. 2016. "Self-driving cars to be targeted by hackers: Cyber criminals could infect vehicles and hold them to ransom until the owner pays" Daily mail. https://www.dailymail.co.uk/sciencetech/article-3491452/Self-driving-cars-targeted-hackers-Cyber-criminals-infect-vehicles-hold-ransom-owner-pays.html.

Bevin, E. 2019. "Man pleads guilty to stalking and controlling ex-girlfriend's car with his computer" https://www.abc.net.au/news/2019-11-06/ract-employee-pleads-guilty-to-using-app-to-stalk-ex-girlfriend/11678980.

Brock, D. C. 2019. "Our Censors, Ourselves: Commercial Content Moderation" Los Angeles Review of Books. https://lareviewofbooks.org/article/our-censors-ourselves-commercial-content-moderation/.

Buckl, C., A. Camek, G. Kainz, C. Simon, L. Mercep, H. Stahle, and A. Knoll. 2012. "The software car: Building ICT architectures for future electric vehicles" *IEEE International Electric Vehicle Conference*. https://mediatum.ub.tum.de/doc/1285769/591565.pdf.

Burke, J. G. 1966. "Bursting Boilers and the Federal Power." *Technology and Culture* 7 (1): 1–23.

Buttgereit, W., C. Voges, and C. Schilter. 1968. "Exhaust Emission Control by Fuel Injection: The VW 1600 with Electronically Controlled Fuel Injection System." *Society of Automotive Engineers (680192)*, 1–8. doi:10.4271/680192.

CAR. 2016. "Potential Cost Savings and Additional Benefits of Convergence of Safety Regulations between the United States and the European Union" https://www.cargroup.org/wp-content/uploads/2017/02/Potential-Cost-Savings-and-Additional-Benefits-of-Convergence-of-Safety-Regulations-between-the-United-States-and-the-European-Union.pdf.

Charette, R. 2009. "This car runs on code." IEEE Spectrum. https://spectrum.ieee.org/this-car-runs-on-code.

De Bruyne, J., and J. Werbrouck. 2018. "Merging Self-Driving Cars with the law." *Computer Law & Security Review* 34 (5): 1150–1153.

Dexter, J. 2002. "The Cyber Security Management System: A Conceptual Mapping" https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591.

ECSO. "WG 1: Standardization certification labelling and supply chain management" https://www.ecs-org.eu/documents/publications/5a3112ec2c891.pdf.

ENISA. 2019. "GOOD PRACTICES FOR SECURITY OF SMART CARS" https://www.enisa.europa.eu/publications/smart-cars

Enriques, L., and D. Zetzsche. 2015. "Quack Corporate Governance, Round III? Bank Board Regulation Under the new European Capital Requirement Directive." *Theoretical Inquiries in law* 16 (1): 211–244.

Framework for Improving. Critical Infrastructure Cybersecurity, Version 1.1 Technical Report. 2018. 10.6028/nist.cswp.04162018.

Fraser-King, G. 2020. "Cyber Threats to the European Automotive Industry Part Two: Cyber Espionage Campaigns" https://www.fireeye.com/blog/products-and-services/2020/01/cyber-threats-to-the-european-automotive-industry-part-two.html.

Fressoz, J. 2007. "Beck Back in the 19th Century: Towards a Genealogy of Risk Society." *History and Technology* 23 (4): 333–350.

Gerla, M., E. Lee, G. Pau, and U. Lee. 2014. "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds" 2014 *IEEE world forum on internet of things (WF-IoT)* 241–246.

Greenberg, A. 2013. "Hackers Reveal Nasty New Car Attacks – With Me Behind The Wheel" Forbes. https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

Greenberg, A. 2015. "Hackers Remotely Kill a Jeep on the Highway – With Me in It". Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

House of Commons. 1817. Select Committee on Steam Boats https://hdl.handle.net/2027/nyp.33433010754467.

Hunte, J., N. E. Fenton, and M. Neil. 2020. "Product risk assessment: a Bayesian network approach" https://arxiv.org/abs/2010.06698.

Huzar, E. 1855. *La fin du Monde par la Science*. Paris: Dentu. 40

Kiss, J. 2016. "Your next car will be hacked. Will autonomous vehicles be worth it?" The Guardian. https://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw.

Kreindler, D. 2013. "How Much Does Homologation Really Cost?" https://www.thetruthaboutcars.com/2013/12/how-much-does-homologation-really-cost/.
Lee, S. 2019. "Hackers on the Highway: Are We Prepared?" *Chicago Policy Review*. https://chicagopolicyreview.org/2019/01/11/hackers-on-the-highway-are-we-prepared/.
Levi, M., Y. Allouche, and A. Kontorovich. 2018. "Advanced analytics for connected car cybersecurity" 2018 *IEEE 87th Vehicular Technology Conference (VTC Spring)* 1–7.
Macher, G., C. Schmittner, O. Veledar and E. Brenner. 2020, September. "ISO/SAE DIS 21434 Automotive Cybersecurity Standard – In a Nutshell" In *International Conference on Computer Safety, Reliability, and Security*, 123–135. Cham: Springer.
Martins, H. 2010. "Type approval homologation and self-certification" https://www.researchgate.net/publication/311949142_Overview_of_Type_Approval_Homologation_and_Self-Certification/link/58641d5308aebf17d3974310/download.
Miller, C. 2019. "Lessons Learned from Hacking a car." *IEEE Design & Test* 36 (6): 7–9.
Mortimer, C. 2015. "Hackers now able to take control of cars to cause deliberate accidents, scientists warn" https://www.independent.co.uk/life-style/gadgets-and-tech/news/computer-hackers-control-car-deliberate-accidents-national-security-issue-a8066466.html.
Oliver, T. 2020. "LDRA to Support New ISO/SAE 21434 Automotive Cybersecurity Standard" https://www.embeddedcomputing.com/technology/security/iec-iso-other-standards/ldra-to-support-new-iso-sae-21434-automotive-cybersecurity-standard.
Ozawa, M., M. Urata, and M. Honda. 2021. "Boiler Explosion and Inspection." *Advances in Power Boilers*, 427–460. Elsevier.
Payne, B. 2019. "Car Hacking: Accessing and Exploiting the Can Bus Protocol." *Journal of Cybersecurity Education, Research and Practice* 2019 (1): 5.
Pearah, P. J 2017. "Opening the Door to Self-Driving Cars: How Will This Change the Rules of the Road." *Journal of High Technology Law* 18: 38.
Pelliccione, P., E. Knauss, R. Heldal, S. Agren, P. Mallozzi, A. Alminger, and D. Borgentun. 2017. "Automotive Architecture Framework: The Experience of Volvo Cars." *Journal of Systems Architecture* 77: 83–100.
Poulsen, K. 2010. "Hacker Disables More Than 100 Cars Remotely" https://www.wired.com/2010/03/hacker-bricks-cars/.
Reddy, B. 2019. "Thinking Outside the box – Eliminating the Perniciousness of box-Ticking in the new Corporate Governance Code." *Modern Law Review* 82 (4): 692–726.
Regulation (EU). 2012. No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardisation. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025
Ryan, M. 2020. "The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self-Driving Vehicles in the Year 2025." *Science and Engineering Ethics* 26: 1185–1208.
SAE. 2016. "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" https://www.sae.org/standards/content/j3061/.
Sobers, R. 2021. "Cybersecurity Statistics and Trends for 2021" https://www.varonis.com/blog/cybersecurity-statistics/.
Statista. 2020. "Average annual costs caused by global cyber crime in 2018, by industry sector" https://www.statista.com/statistics/474928/average-annual-costs-caused-by-cyber-crime-worldwide/.
Suffolk Police. 2021. "Man jailed for more than five years after conspiracy to steal over 100 vehicles" https://www.suffolk.police.uk/news/latest-news/man-jailed-more-five-years-after-conspiracy-steal-over-100-vehicles.
Tengler, S. 2020. "Top 25 Auto Cybersecurity Hacks: Too Many Glass Houses To Be Throwing Stones" https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/.
Tschofenig, H., M. Volkamer, N. Jentzsch, S. Fischer-Hübner, S. Schiffner, and R. Tirtea. 2013. "On the security, privacy and usability of online seals: An overview" https://www.enisa.europa.eu/publications/on-the-security-privacy-and-usability-of-online-seals.
UNECE. 1995. "UNECE Transport Vehicle Regulations" https://unece.org/faq.

UNECE. 2016. "The Revision 3 of the 1958 Agreement – Questions and Answers" https://unece.org/DAM/trans/doc/2016/wp29/WP29-170-21e.pdf.

Upstream. 2019. "Upstream Security Global Automotive Cybersecurity Report 2019" https://upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/.

Veale, M., and F. Z. Borgesius. 2021. "Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the bad, and the Unclear Elements of the Proposed Approach." *Computer Law Review International* 22 (4): 97–112.

Vivek, S., D. Yanni, P. Yunker, and J. Silverberg. 2019. "Cyberphysical Risks of Hacked Internet-Connected Vehicles." *Physical Review E* 100 (1), 012316.

Wagner, M., and P. Koopman. 2015. "A Philosophy for Developing Trust in Self-Driving Cars." In *Road Vehicle Automation 2*, 163–171. Cham: Springer.

Welch, D., and M. Cheok. 2020. "GM to Exit Australia, Retire Holden Brand in $1.1 Billion Overhaul" Bloomberg. https://www.bloomberg.com/news/articles/2020-02-17/gm-to-record-1-1b-charges-restructuring-international-ops.

Wolk, J. 2018. "The fast and the fictional" Automotive News. https://www.autonews.com/article/20181001/SHIFT/181009996/the-fast-and-the-fictional.

Tempting the Fate of the furious: cyber security and autonomous cars

McLachlan S

2022-05-27