Cybersecurity Engineering in Connected and Automated Mobility: Cyber Resilience in Transportation

Daniel S. Fowler
dan.fowler@warwick.ac.uk

29th September 2021

Cyber Security Summit Brazil 2021 - 28th and 29th September
Theme - Digital Economy and the Cybersecurity Scenario for the Future
Keynote E General Session
`https://www.cybersecuritysummit.com.br/`

Abstract

The mass-manufactured car and new transportation systems have become connected entities. Connected and Automated Mobility uses wireless interfaces to provide drivers and customers with information, entertainment, and new functionality. Cars are now another of our smart devices and the connected data services add value to enhance vehicle marketability. However, decades of using enterprise and Internet systems have demonstrated that connectivity provides an attack vector for threat agents.

When cars were first fitted with computers the hacking began. However, vehicle cybersecurity was not a major concern before the connected car because hacking was restricted to single vehicles. That changed when researchers demonstrated the ability to take control of a car over a cellular connection. Vehicle manufacturers and the wider automotive industry have responded by taking seriously the transportation cybersecurity threat. Cyber resilience engineering processes have emerged to reduce the cybersecurity risk to vehicles. The aim is to maintain high safety levels within the global transportation super-systems.

Discussed are the cyber threats to transportation and the new vehicular cybersecurity engineering processes (to which the UK is a major contributor). Furthermore, the UK is developing research capabilities to ensure the cyber resilience of future CAM. The UK encourages and contributes to the international development of cybersecurity testing for cars and CAM systems. How cyber resilience is being developed for transportation systems is useful for those developing processes in other domains, for example, smart factories, medical devices, and space systems.

1 Introduction

An overview of cybersecurity engineering in Connected and Automated Mobility (CAM) is provided, and a discussion on the need to bring cyber resilience into our future transportation systems. The topic of cyber resilience is one of the research areas of interest within the Secure Cyber Systems Research Group (SCSRG) at WMG [26]:

- WMG is located at the University of Warwick.
- It was founded in 1980, focusing on industrial management and manufacturing technology (hence **W**arwick **M**anufacturing **G**roup).
- It is a faculty performing applied engineering and manufacturing research, amongst other subjects.
- It is an academic department providing apprenticeships, graduate and postgraduate teaching.
- WMG's size means it occupies several buildings on the Warwick campus, near the City of Coventry, central England, the historical heart of the UK's vehicle manufacturing industry (Jaguar Land Rover, Aston Martin, Dennis Eagle, etc.)
- WMG links academic research with business and educates the next generation of engineers, industry managers, and technical leaders.

SCSRG is a large and growing research group within WMG that has projects in a variety of topics including:

- Internet of Things
- Communication systems
- Vehicles
- Space systems

- Cyber policy
- Trust, Identity, Privacy, and Security (TIPS) topics
- Digital forensics
- Blockchain technologies

SCSRG works with many Universities, companies, organisations, and the UK Government. Fundamental research is delivered through collaborative Research and Development (R&D), private and Government funded projects, and contracted research.

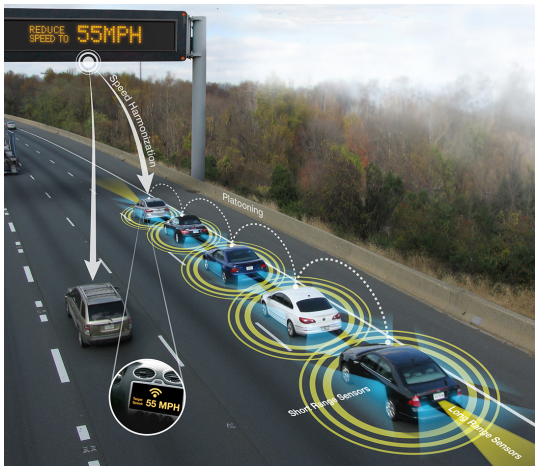
1.1 Why cybersecurity engineering in Connected and Automated Mobility

Connected and Autonomous Vehicles (CAVs) are on the roads and automated mobility is being deployed. The University of Warwick is collaborating to bring very light rail to Coventry City. The manufacturer Jaguar Land Rover, in the University's locality, produces many electric cars. Furthermore, vehicles are connected and rely on software for much of their functionality. Thus, today's vehicles are electrified, connected and software controlled, see Figure 1. However, connected and software-controlled systems can be a target for cyber attacks. How can automotive engineering reduce the risks from cyber attacks? That is the goal of cybersecurity engineering research in CAM.

(a) Vehicle connectivity (author's image)

(b) Jaguar I-Pace electric car, CC BY-SA 4.0 [21]

(c) Capri [3] self-driving pod (author's image)



(d) V2X communications (Public Domain image)

Figure 1: Connected, electric and software-controlled transportation

2 Background

All mass-manufactured vehicles use interconnected computers, known as Electronic Control Units (ECUs). Multiple computers are extremely common, see Figure 2 for a typical in-vehicle network layout, up to 30 ECUs are in a typical family car. Every function within a vehicle has a computer and software element, this includes the engine and gears (powertrain), airbag and brakes (safety), infotainment system and climate control (comfort), and the cabin, seats, gauges, and doors (body). All these elements are interconnected. The networks within vehicles are complex, with connections to the outside world.

2.1 Connectivity, computers, and software allows for hacking

Connected computational systems, including vehicles, open up opportunities for hacking. Automotive hacking is aimed at vehicle systems. Hacking is a part of automotive R&D. Figure 3 shows a UK Autodrive [18] project car, a standard

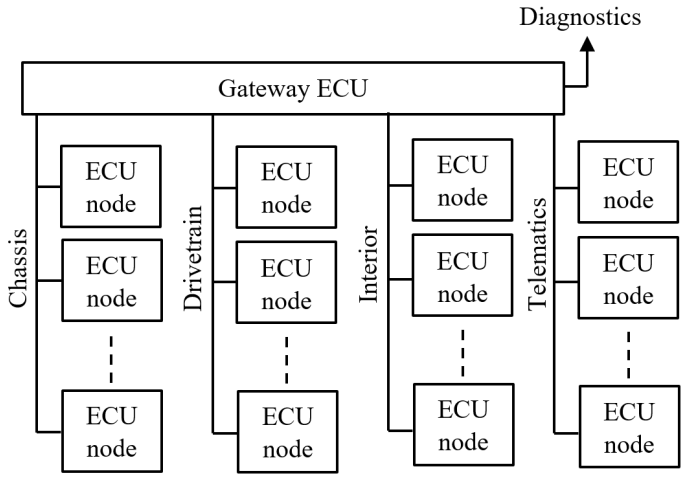


Figure 2: In-vehicle data networks group ECUs by functional areas and allow for cross-domain communication via a gateway ECU, which often provides a diagnostics connection (derived from [15])

vehicle with extra external sensors added to enable autonomous vehicle research.

Figure 3: Vehicle hacking can be part of R&D (author's image)

However, researchers have used hacking to reveal security issues with vehicles. The most famous was in 2015 when American researchers took control of a vehicle, an unmodified vehicle, from a remote location over a cellular connection [13]. They proved, in a real-world scenario, that vehicles can be compromised.

2.2 Transportation cyber threat motivations

What are the treat motivations for attacking transportation systems? The most common is financial gain. Vehicles are valuable and theft is common, the whole vehicle, the parts, and the goods they carry. In the future, if not now, vehicles will be producing personalised datasets, information has value. There is value in Intellectual Property (IP), the engineering within a vehicle is of interest for IP theft. A motivation for users of public transportation systems is to gain free rides. Then there is the passenger payment details stored within systems, the card details used to access transportation, these personal and card details are valuable. Those are examples of financial motivations for hacking. Other hacking motivations exist, including vandalism, simply proving something can be hacked by doing it. Militant activist groups may want to make a statement through hacking, i.e., *hacktivism*. There are nation-state actors and terrorists who may try to cause chaos, block roads, crash vehicles, and use vehicles as kinetic weapons. Eavesdropping on passengers within vehicles is motivation and has been performed before. Attackers can look to target very important people (VIPs) and wealthy individuals who travel in luxury transportation. There are plenty of threat motivations for attacking transportation systems, some summarised in these lists:

- Financial gains
  - Vehicle theft (including redirection and route alteration), valuable parts, goods
  - Value in extracting on-board/backend datasets
  - IP theft and reverse engineering
  - Free rides or longer rides on public transport
  - Passenger payment card details

- Vandalism
  - Hack it because we can
  - Change on-vehicle/in-vehicle messages
  - Change the routing, falsify maps
  - Scare passengers (lock doors, increase speed, crash)
- Hacktivism, nation-state actors, terrorism
  - Cause chaos (block roads, crash vehicles, vehicles as terrorist weapons)
  - Eavesdrop/monitor data and conversations
  - Targeting VIPs and wealthy individuals (luxury cars have the most computer systems)
- Insider threats (manufacturers, supply chains, dealer networks)
- Autonomous bullying (gaining an advantage over-cautious self-driving cars)

2.3 Examples of real-world vehicle cyber issues

Vehicle cyber attacks have happened before and are happening now [5]. One of the most successful is the relay-attack against vehicle keyless entry systems [6]. This is where the vehicle's wireless key-fob is compromised to steal vehicles. A thief will use a communications system to relay the signal from a key-fob located in a building to an accomplice standing next to the vehicle. This enables them to gain access to the vehicle, start it up, and drive away.

A different type of vehicle hacking was the *Dieselgate* emissions scandal [4]. This was corporate hacking with *defeat device software*, software that enabled vehicles to beat the emissions testing regulations, Figure 4.

Figure 4: Cars had software to help evade emissions test equipment, CC BY-SA 3.0 [22]

What about the possibility of a vehicle virus. Ransomware is now very common. What if you got into your car and could not start it because of a ransomware attack on vehicles. Ransomware is for financial gain, the WannaCry ransomware attack had by June 2017 a total of 327 cryptocurrency payments totalling $130,634.77 in value [23]. A widespread attack on vehicles is a concern, as Elon Musk, founder and Chief Executive Officer of the car company Tesla said: *"One of the biggest risks for autonomous vehicles is somebody achieving a fleet-wide hack."* [14]

Ransomware has already affected transportation systems. The San Francisco municipal transit payment system was taken offline by a ransomware attack [10]. All the flights for Alaska Airlines had to be cancelled when a maintenance system was taken down. That attack impacted other American air carriers [7].

3 How to hack transportation systems

How is it possible to hack transportation systems? The methods used are similar to hacking other systems. Methods that compromise the confidentiality, integrity, and availability (CIA) of systems, software, and data. Compromising the CIA triad enables the breaking of information systems security. Traditional hacking methods, penetration testing techniques, vulnerability assessment, and fuzzing techniques are used. Malicious code (malware) can be embedded into systems. The signals and data used within the systems (e.g., for control) can be spoofed. Denial of service attacks can be performed. These methods are very familiar to attackers of any type of computer-based system. Here is a list of some of the types of attacks that can be used against vehicle systems:

- Traditional hacking
  - Pen testing
  - Vulnerability assessment
  - Fuzzing
- Malicious code

  - Malware (phishing/virus/worm)
  - Compromised/fake apps
- Spoof data and signals
  - Replay
  - Falsification
  - Modification
  - Side channel
- Denial of service
  - Flooding/blinding/saturating
  - Jamming
  - Cloaking

3.1 The transportation attack surface and engineering fallibility

Vehicles present a huge attack surface for the threat actors that may want to attack transportation systems. Internet and cloud-based communications services are increasingly engineered into vehicles. These are via cellular or WiFi connections and are used for services provided by vehicle manufacturers. Increasingly manufacturers' provide additional features that include remote diagnostics and location-based services. There are local wireless vehicle communications interfaces, for example, Bluetooth. Electric and hybrid vehicles have charging and battery management systems. The people that use transportation, the passengers, bring their own devices and connect them to vehicles. There are the vehicle's internal systems, the in-vehicle control networks present an attack surface, the control computers (ECUs), and all the sensors that are present. Telematic units are added to vehicles for services that include fleet management and insurance monitoring. Increasingly, vehicles communicate with roadside infrastructure for warning information. Here is a summary of the large number of transportation attack points to consider when designing and engineering transportation services and vehicles.

- Internet, cloud and data communications
  - Wi-Fi hotspots and connections
  - 3G/4G/5G cellular connections
  - Manufacturers' services
- Local vehicle communications
  - Bluetooth connections
  - Vehicle-to-vehicle (V2V) communication
  - Vehicle-to-infrastructure (V2I) communications (IEEE 802.11p or 3GPP standards)
  - Near-Field Communication (NFC)
- Charging and Battery Management Systems (BMS)
- Motors and actuators
- Passenger/pedestrian smartphones, tablets, and laptops
- Aftermarket devices
- In-vehicle data networks
- Computers (ECUs) and their software
- Access ports, e.g., Universal Serial Bus (USB), On-Board Diagnostics (OBD)
- Multiple sensors
  - Lidar, radar
  - Cameras
  - Ultrasonic and laser range finders
  - Global Navigation Satellite System (GNSS)/Global Positioning System (GPS)
  - Accelerometers
  - Transducers/microphones
  - Tire-Pressure Monitoring System (TPMS)

- Displays
- Telematics units (fleet management, insurance monitoring)
- Intelligent Transport Systems (ITS), i.e. infrastructure

Attackers are looking for weaknesses in engineering when targeting the above. Thus, when designing systems there is a need to understand the fallibility of humans when they perform engineering. The attackers look for engineering design complacency. Fallibility in engineering is well known, the following happens, and has happened in other systems over several decades:

- Bugs in software
- Backdoors
- User errors
- Bad configurations
- Vulnerabilities
- Poor engineering
- Phishing
- Espionage
- Complacency
- Insufficient security testing

How do we deal with these issues within transportation cybersecurity? Transportation systems engineers are fighting back. They are using cybersecurity researchers, and vehicle manufacturers have implemented bug bounty programs. Cars are subjected to penetration testing to reveal potential vulnerabilities that are then fixed [17]. Engineers need to make a best effort to improve security, after all, as security expert Richard Bejtich said, *"determined intruders will always find a way to compromise their targets"* [1].

4 Automotive cyber attack countermeasures

Engineers can design and apply countermeasures against cyber attacks. Cryptography can be used in the systems built into transportation, by adding authentication processes and data encryption to harden the internal communications protocols. Secure-by-design methods and secure coding practices can be used in the systems development and engineering processes. Security sensors, i.e., Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), can be placed within vehicles. A vehicle's sensors can be hardened and strengthened to increase attack difficulty. Here is a summary of some of the methods that can be considered as cyber attack countermeasures for transportation systems:

- Secure-by-design and secure coding techniques
- Perform Threat Assessment and Risk Analysis (TARA)
- Common sense, i.e. plausibility of signals and data
- Cryptography and authentication
- Hardening protocols
- Higher speed processing and improved algorithms, out-perform the bad actors
- Good enough security, make it uneconomical for the attacker
- Anomaly/misbehaviour detection
  - Detect anomalous real-world signals
  - IDSs and IPSs on networks and communications
  - Provide situational awareness
- Sensor redundancy
- Sensor and systems data fusion
- Fail-safe sensors
- New types of sensors

5 Working together to engineer cyber resilience into transportation

Achieving cyber resilience in any domain requires stakeholders to work together. Within the UK the Zenzic organisation is driving forward the CAM industry. There are goals for UK CAM:

- Safety and security - reducing road and pedestrian injuries
- Improving productivity - reducing congestion
- Access to transport - improved transportation for the disadvantaged
- Economic growth - CAM and CAV market growth with new transportation systems and technology

Zenzic coordinates over 100+ UK organisations (industry, government and academia) in the drive to implement the next-generation technology in the transportation sector, WMG is a member of Zenzic. *"Zenzic was created by government and industry to focus on key areas of UK capability in the global connected and self-driving sector"* [27].

Zenzic overseas CAM Testbed UK, a multi-location facility covering all forms of CAV testing and vehicular scenarios, including simulation, physical environments, junctions, highways, urban, parking, connectivity, and infrastructure interfacing. The University of Warwick campus, the location of WMG, is in the Midlands Future Mobility (MFM) testbed. MFM is one of the CAM Testbed UK's six locations and is located in the heart of the UK's automotive engineering and motor production industry. MFM is over 200 miles (320 kilometres) of central UK public roads, with varying traffic, available for trials of CAM and CAV solutions. It provides a real-world environment to support transportation testing.

5.1 Cyber resilience in transportation is a UK priority

Zenzic maintains the UK CAM Roadmap to maintain a focus on the steps required for the future visions of transportation. The roadmap has several *golden threads* as key themes for driving UK transportation market innovation:

1. Legislation and Regulation
2. Safety
3. CAM Services
4. Public Acceptability
5. Infrastructure
6. Cyber Resilience

The cyber resilience golden thread is required to ensure that future transportation systems are safe from cyber issues. How is that achieved? One way is to establish guidelines and standards for the transportation industry to follow and use as guidance when demonstrating cybersecurity assurance.

6 Vehicle cybersecurity regulations

The UK is active in CAV standards development. The British Standards Institute (BSI) has its CAV guidelines [2], towards which WMG researchers contributed. The BSI guidelines help build the knowledge required to keep future CAM and CAV technology safe. Furthermore, in many countries vehicles have to meet a set of legal requirements. These rules are often referred to as *Type Approval*. The Type Approval regulations protect the users of vehicles, see Figure 5.

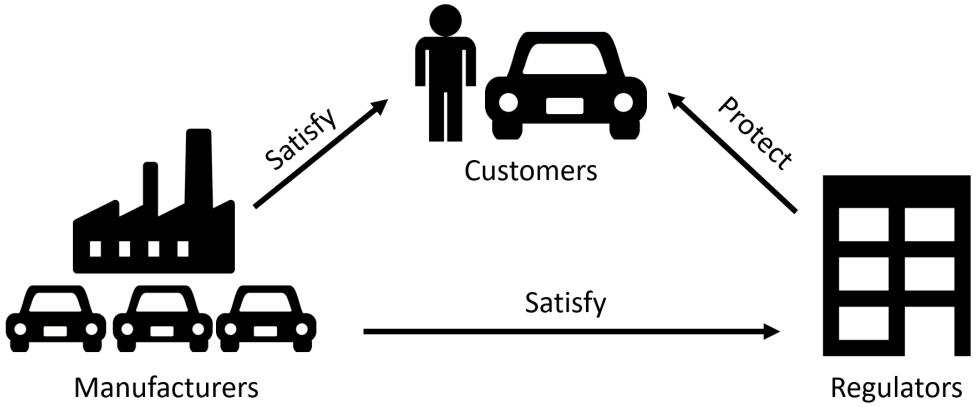


Figure 5: Vehicle Type Approval is overseen by regulators to protect vehicle users (author's image)

Rules are required to ensure that a vehicle maintains safe operational use, as it says in the BSI automotive cybersecurity guidelines: *"The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail"* [8]. Therefore, cyber attacks against vehicle systems must not affect safety integrity. This means vehicle cybersecurity engineering and testing is driven by safety concerns (which may cause damage to manufacturers reputation) and regulations.

6.1 International cybersecurity regulations for vehicles

The United Nations Economic Commission for Europe (UNECE) is home to the World Forum for Harmonization of Vehicle Regulations (WP.29), it has 64 participating countries. The WP.29 group issues regulations for vehicle safety. In June 2020 it issued vehicle regulations on a Cyber Security Management System (CSMS) [19] and vehicle software updates [20].

In addition to the new UNECE regulations, the International Organization for Standardization (ISO) and the formerly named Society of Automotive Engineers (SAE) have produced a global standard for addressing *Road vehicles Cybersecurity engineering*, namely ISO/SAE 21434 [9], a replacement for the SAE J3061 cybersecurity guidelines [16]. ISO/SAE 21434 and the UNECE regulations were multinational efforts to develop cybersecurity processes to apply to the whole of a vehicle's lifecycle. Furthermore, ISO/SAE 21434 is comprehensive and exceeds UNECE CSMS requirements and covers more topics, thus following ISO/SAE 21434 will meet UNECE regulations. Essentially, these regulations give the transportation industry a foundation upon which they can base their cybersecurity engineering processes, covering:

1. The life cycle of a vehicle - development, production, post-production
2. An organisation's cyber security management processes
3. Risk management - identification of risks to a vehicle, their assessment, categorisation and treatment
4. Security testing processes
5. The ongoing risk assessment
6. Monitoring, detecting and responding to cyber attacks, threats, and vulnerabilities
7. Management of dependencies with third parties and other organisational divisions
8. Handling of aftermarket software, services, and data
9. Modifications after being granted type-approval (e.g., updates)
10. Conformity in production

6.2 Key messages from standards and regulations

There are some key messages from the cybersecurity regulations. Cybersecurity is to be regarded as an organisation-wide task, with all management layers and engineering functions taking responsibility. The same standards on cybersecurity for the original equipment manufacturers (OEMs) of transportation systems apply to their supply chains. The tier suppliers to OEMs have a responsibility. Furthermore, there is the need to have a TARA process to identify vulnerabilities. Systems should be secure-by-design and tested for resilience, removing any vulnerabilities when found. Thus cybersecurity engineering applies to the whole vehicle lifecycle, from design, through production, servicing, to vehicle destruction. For cyber risk reduction to succeed, a cybersecurity process is required when engineering vehicles and transportation systems.

7 Examples of research projects into vehicular cybersecurity

Automotive cybersecurity standards and engineering processes are important. However, ongoing research to reveal future cybersecurity issues, and to find new ways to build resilience into systems is ongoing. At WMG, and within SCSRG, projects are looking at how cyber resilience can be embedded into products, ensuring our digitally controlled world can be used and navigated safely. Here are some of the WMG projects that addressed security issues in the transportation space.

7.1 Capri project, last-mile urban transport

The Capri project [3] successfully designed and delivered self-driving Pods on Demand (PODs) for last-mile urban transportation. The PODs, see Figure 1c, were built by Westfield (the UK sports car manufacturer). The Capri project had 19 partner organisations, with WMG providing cyber-physical system (CPS) security analysis and threat assessments of the POD's sensor system. Some of WMG's work included using simulation software to model LiDAR and GNSS sensors, seeing the effect of signal spoof attacks and the results of mitigation methods, see Figure 6. The project delivered a TARA methodology [11] and aided a reference architect [12], both helping to analyse threats to vehicular systems.

Figure 6: Faking lidar signals in a vehicle simulation (WMG image)

7.2 Positioning, Navigation and Timing (PNT) GNSS cyber resilience

WMG partnered with Spirent to perform research into Global Navigation Satellite System (GNSS) vulnerabilities [24] and security. Reliable GNSS is important for CAM and CAV. The research highlighted what OEMs need to consider as important for GNSS attacks, testing, and mitigation engineering. Figure 7 shows an MFM autonomous vehicle being tested during the PNT project at University of Warwick facilities.

Figure 7: Analysing PNT attack issues and testing mitigation (WMG image)

7.3 Secure Connected and Autonomous Vehicles (S-CAV)

A UK cybersecurity startup, Ankgoka Limited, partnered with WMG to test their new cryptography technology on WMG's High Value Manufacturing (HVM) drive-by-wire innovation platform vehicle [25], see Figure 8. The technology uses decentralised cryptography protocols and hardware. It secured in-vehicle and V2X communications in real-time. Layering encryption over the vehicle's standard control network and from the vehicle to the roadside infrastructure. The testing was performed away from public roads for health and safety considerations. The use of real-time cryptography protocols can reduce the threat of spoofing data messages.

7.4 Learning from vehicle cybersecurity research

Research into cybersecurity for transportation, and past cyber incidents, provides some learning to take forward into future systems design. Engineers need to consider *misuse cases* in designs and mitigate possible threats. Where possible, engineered designs should choose simplicity over complexity to ease the testing burden. The simpler the system the easier it is to test (and build). Security testing should begin early in the design cycle, i.e., from the project start, to achieve secure-by-design, in other words, *cyber risk reduction-by-design*, thus, reducing cybersecurity risks from early in the project.

In the cybersecurity and transportation fields, *change* is the only constant. There are always new design and testing techniques emerging. Automotive engineers should keep up-to-date with trends. Whilst modern vehicle hacking is difficult, it is not impossible, and to avoid future cybersecurity issues within our complex transportation systems

Figure 8: WMG's drive-by-wire HVM Catapult innovation platform vehicle (WMG image)

engineers cannot be complacent. The threat actors are determined and weaknesses may eventually be revealed, hence the need to consider the full lifecycle of deployed systems and vehicles.

8 In summary

Modern transportation systems provide a large attack surface. This is coupled with the existing motivations and methodologies for attacking vehicles and transportation that exist. Furthermore, future threats, motivations, and methodologies will emerge. If stakeholders understand threats to vehicles it can help improve future security and safety within transportation. Systems need to be engineered to make future attacks uneconomical. This can be done by engineering in cyber resilience.

The automotive industry needs to collaborate and share cybersecurity knowledge. Transportation stakeholders need to work as a team, similar to the UK's Zenzic organisation. Transportation and vehicle cybersecurity is a growth business area and opportunities exist for businesses to flourish in the modern transportation space. The topics discussed here apply to other complex systems and products, for example, smart factories, medical devices, space systems, etc. The stakeholders within other domains may wish to see how the automotive industry is addressing cyber issues and follow a similar path.

References

[1] Richard Bejtlich. *The Practice of Network Security Monitoring Understanding Incident Detection and Response*. San Francisco: No Starch Press, 2013.

[2] British Standards Institute. *Connected and automated vehicles*. 2017. URL: https://www.bsigroup.com/en-GB/CAV/.

[3] Capri Consortium. *Connected and automated vehicles*. 2020. URL: https://caprimobility.exhibition.app/.

[4] M Contag et al. "How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles". In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, pp. 231–250. DOI: 10.1109/SP.2017.66.

[5] Daniel S. Fowler. *Automotive Cyber Security Timeline*. 2021. URL: https://tekeye.uk/automotive/cyber-security/timeline.

[6] Aurélien Francillon, Boris Danev, and Srdjan Capkun. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars". In: *Network and Distributed System Security Symposium (NDSS)*. 2011. DOI: 10.3929/ethz-a-006708714.

[7] Charles Harry and Skanda Vivek. "Strategic Cyber Effects in Complex Systems: Understanding the US Air Transportation Sector". In: *2021 13th International Conference on Cyber Conflict (CyCon)*. 2021, pp. 111–131. DOI: 10.23919/CyCon51939.2021.9468293.

[8] British Standards Institute. *PAS 1885:2018 The fundamental principles of automotive cyber security - Specification*. 2018.

[9] ISO and SAE International. *Road vehicles – Cybersecurity engineering (ISO/SAE 21434)*. Geneva, 2021.

[10] Usman Javed Butt et al. "Ransomware Threat and its Impact on SCADA". In: *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. 2019, pp. 205–212. DOI: 10.1109/ICGS3.2019.8688327.

[11] Anh Tuan Le and Carsten Maple. "A simplified approach for dynamic security risk management in connected and autonomous vehicles". In: *Living in the Internet of Things (IoT 2019)*. London: Institution of Engineering and Technology, 2019. DOI: 10.1049/cp.2019.0140.

[12] Carsten Maple et al. “A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis”. In: *Applied Sciences* 9.23 (2019). ISSN: 2076-3417. DOI: 10.3390/app9235101.

[13] Charlie Miller and Chris Valasek. “Remote Exploitation of an Unaltered Passenger Vehicle”. In: *Black Hat USA*. 2015, pp. 1–91.

[14] National Governors Association. *NGA 2017 Summer Meeting*. 2017. URL: https://youtu.be/2C-A797y8dA.

[15] Robert Bosch Gmbh, ed. *Bosch Automotive Electrics and Automotive Electronics - Systems and Components, Networking and Hybrid Drive*. 5th ed. Plochingen: Springer Vieweg, 2014. DOI: 10.1007/978-3-658-01784-2.

[16] SAE International. *J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. 2016.

[17] Tencent Keen Security Lab. *Experimental Security Assessment of BMW Cars: A Summary Report*. Tech. rep. Keen Security Lab, 2018, p. 26.

[18] UK Autodrive consortium. *The UK Autodrive project*. 2015. URL: http://www.ukautodrive.com/.

[19] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29). *Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. Tech. rep. Geneva: United Nations Economic Commission for Europe, 2020, p. 27.

[20] UNECE World Forum for Harmonization of Vehicle Regulations (WP.29). *Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system*. Tech. rep. Geneva: United Nations Economic Commission for Europe, 2020, p. 15.

[21] Wikimedia Commons. *2018 Jaguar I-Pace EV400 AWD*. 2018. URL: https://commons.wikimedia.org/wiki/File:2018_Jaguar_I-Pace_EV400_AWD_Front.jpg.

[22] Wikimedia Commons. *VW Golf TDI Clean Diesel*. 2010. URL: https://commons.wikimedia.org/wiki/File:VW_Golf_TDI_Clean_Diesel_WAS_2010_8983.JPG.

[23] Wikipedia. *WannaCry ransomware attack*. 2021. URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

[24] WMG Marketing. *Spirent partners with WMG to develop cyber-security services across Connected and Automated Mobility markets*. 2020. URL: https://warwick.ac.uk/fac/sci/wmg/business/success-stories/cyber-resilience/.

[25] WMG Marketing. *WMG helps rising automotive security company prove its technology*. 2020. URL: https://warwick.ac.uk/fac/sci/wmg/business/success-stories/scav/.

[26] WMG Marketing. *WMG, The University of Warwick*. 2021. URL: https://warwick.ac.uk/fac/sci/wmg.

[27] Zenzic-UK Ltd. *Zenzic*. 2021. URL: https://zenzic.io/.