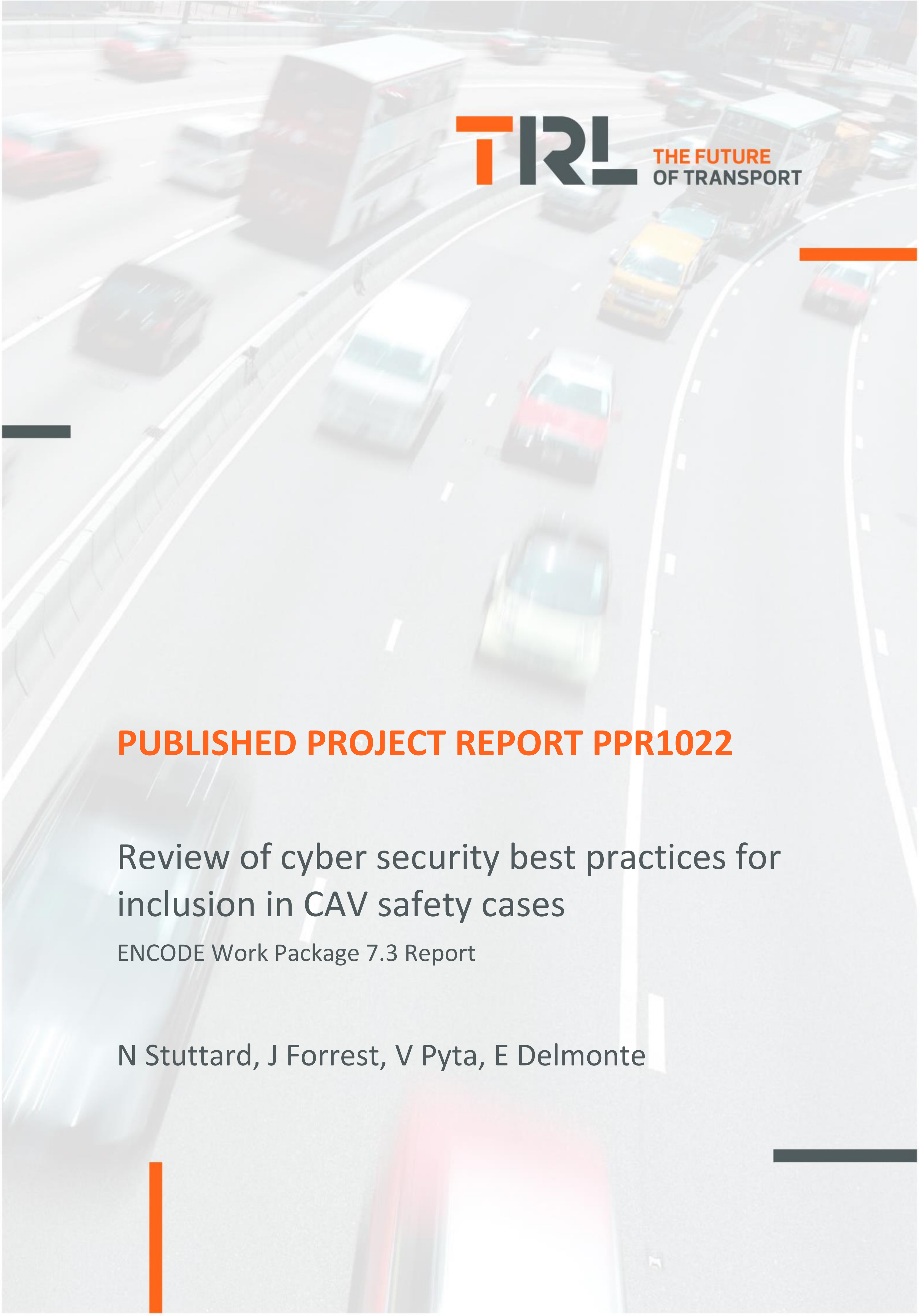

PUBLISHED PROJECT REPORT PPR1022

Review of cyber security best practices for inclusion in CAV safety cases

ENCODE Work Package 7.3 Report

N Stuttard, J Forrest, V Pyta, E Delmonte

Report details

Report prepared for:	CCAV
Project/customer reference:	11226169
Copyright:	© TRL Limited
Report date:	31.03.2022
Report status/version:	Issued
Quality approval:	

S Abisa (Project Manager)		C Fowler (Technical Reviewer)	

Disclaimer

This report has been produced by TRL Limited (TRL) under a contract with CCAV. Any views expressed in this report are not necessarily those of CCAV.

The information contained herein is the property of TRL Limited and does not necessarily reflect the views or policies of the customer for whom this report was prepared. Whilst every effort has been made to ensure that the matter presented in this report is relevant, accurate and up to date, TRL Limited cannot accept any liability for any error or omission, or reliance on part or all the content in another context.

When purchased in hard copy, this publication is printed on paper that is FSC (Forest Stewardship Council) and TCF (Totally Chlorine Free) registered.

Executive summary

The introduction of remote operation has the potential to accelerate the development of driverless vehicles and make their safe deployment more viable. However, the wireless connections between vehicles and operators present new cyber security hazards that could be exploited by attackers.

This study identified best practices in cyber security so that they can be incorporated into safety cases for the future trials and deployments of Connected and Automated Vehicles (CAVs). Potential mitigations for cyber-attacks were drawn first from a review of the existing cyber literature, and subsequently from interviews with expert stakeholders.

The literature review suggested that the best cyber mitigations were intrusion detection, encryption of data, verifying the identity of all users and the use of minimum risk manoeuvres. The stakeholder engagement suggested that ensuring that any cyber-systems were secure by design and resilient to any attacks were the most important factors.

To ensure cyber security of remote operation of CAVs, this study highlighted several actions that should be considered. Though many cyber security techniques exist, it is best practice to implement cyber security mitigations on a case-by-case basis and, where possible, these systems (e.g. authentication methods) should be secure from their conception. Furthermore, minimum risk manoeuvres should be developed, to ensure the safety of both vehicle occupants and other road users.

Table of Contents

Executive summary i

1 Introduction 1

1.1 About Encode 1

1.2 About this task (WP 7.3) 1

1.3 A note on good practice 2

1.4 Structure of the report 2

1.5 Cyber security and remote operation of CAVs 3

1.6 Guidance and standards 4

1.7 Safety Cases 5

2 Literature review method 7

2.1 Approach 7

2.2 Search terms 7

2.3 Assessment of quality and relevance 7

2.4 In-depth review of full text literature 8

3 Literature review results 9

3.1 Brief overview of findings 9

3.2 Threats to the internal functions, local software, and network security of the remote vehicle 10

3.3 Security of communications to and from the vehicle 14

3.4 Implications of safety driver vs no safety driver 16

3.5 Implications of different types of remote operation (line of sight, relying on vehicle sensors, relying on infrastructure sensors) 17

3.6 Summary of literature review findings 18

4 Stakeholder engagement method 20

4.1 Approach 20

4.2 Stakeholder recruitment 21

4.3 Interview method 21

4.4 Analysis 22

5 Stakeholder engagement results 23

5.1 Trial operators (group 1) 23

5.2 Expert stakeholders (group 2) 28

5.3 Overall themes 30

6 Discussion and safety case considerations 32

7 References 33

Appendix A Search terms used for the literature search 36

Appendix B List of mitigations found in the literature search 37

1 Introduction

1.1 About Encode

Encode “Ensuring cyber secure deployments of driverless teleoperated vehicles” is an Innovate UK project which aims to:

- Accelerate the adoption of Connected and Automated Vehicles (CAVs) in first- and last-mile goods, by ensuring cyber secure deployments of driverless remotely operated vehicles.
- Extend StreetDrone cyber security analyses and implement mitigations, focused on a **"multi-driver" system**, contributing research and evidence to industry standards and good practices.
- Work with CAV key stakeholders including regulators and end-customers to fully understand the impacts of multi-driver systems, their inherent liabilities and enable overarching visibility via a proof-of-concept fleet monitoring system.

Multi-driver vehicles can be operated **manually** (by an operator within the vehicle), **autonomously** (by an automated driving system with an operator in the vehicle who can take over control of the driving task) and **remotely** (remotely operated by an operator who can service multiple vehicles).

The Inland Transport Committee of the Economic Commission for Europe recognises that the ability to reliably and safely conduct remote driving of vehicles has the potential to enable mobility services, provide flexibility in safety-critical situations, or support further development of automated driving systems[1].

Subject to the safety case being accepted by the relevant stakeholders, the Encode project will conclude with a simultaneous live trial of "multi-driver" vehicles across two locations, on public roads, demonstrating the potential of remote driving. Tasks conducted as part of the project will contribute to a greater understanding of safety and security requirements to enable remote driving.

The project is being delivered by a consortium led by StreetDrone and supported by TRL, Coventry University, Oxfordshire County Council, and Angoka.

1.2 About this task (WP 7.3)

Cyber security is an important issue for CAVs. This has been largely managed by limiting or eliminating safety critical inputs to the vehicle from external sources. However, external input is essential for remote operation and reliability of this input is critical for safety critical

[1] https://unece.org/sites/default/files/2021-09/ECE-TRANS-WP1-2021-Informal document-1e_2.pdf

tasks, including remote driving. There has been significant focus on cyber requirements for CAVs but there is minimal published guidance available specifically for remotely operated CAVs. Work package 7 will produce safety case considerations for driverless trials includes options for demonstrating cyber security and providing assurance to stakeholders. In aid of this, task 7.3 aims to:

1. review the current and emerging good practices for the cyber security of remote operations of CAVs; and
2. identify options regarding the type of evidence that could be used to demonstrate secure operations to include in the safety case.

This was achieved through the completion of two subtasks; a literature review and stakeholder engagement. The literature review provided documentation of published literature on good practice in cyber security of remote operations of CAVs and the stakeholder engagement supplemented and validated this information with insights from both their operational and research experience.

This report represents a synthesis of these two subtasks and acknowledges the cyber security risks and mitigations that are relevant to all CAVs but focuses on the risks that are especially important or unique to a remote operation scenario.

1.3 A note on good practice

This report identifies cyber security considerations for a remote driving safety case based on current and emerging good practice. Fast paced developments in technology and methods of interference mean any recommendations on good practice should incorporate ongoing monitoring of emerging threats and mitigations. Methods of control need to be able to detect problems that might indicate interference and methodically analyse and isolate risks without necessarily being pre-cognisant of the specific source or form of attack. Given the novelty and pace of change in this field, we are qualifying our use of the term ‘good practice’ to mean methods that are well-tested and noting that what is currently considered good practice is unlikely to remain static but will need to be reviewed regularly and updated.

1.4 Structure of the report

The report is split into six sections. Section 1 provides an overview of the task and introduces key concepts such as remote driving and safety cases. Section 0 summarises the approach taken for the literature review, the findings of which are presented in Section 0 Section 0 then summarises the approach used for the stakeholder engagement, and Section 0 presents its findings. The report is concluded in Section 0 with a discussion of the results which highlights the key safety case considerations.

1.5 Cyber security and remote operation of CAVs

Remote driving has been defined as the "real-time performance of the dynamic driving task (DDT) and/or DDT fallback (including, real-time braking, steering, acceleration, and transmission shifting), by a remote driver[2]". However, in a multi-driver scenario, there are different levels of remote operation including driving, monitoring or assistance that can be provided remotely. Remote operation systems may require safety driver intervention if a failure is detected or may conduct a minimum risk manoeuvre to bring the vehicle to stop prior to requiring human intervention. All levels of remote operation including driving, monitoring and assistance are considered within scope for this report because their vulnerability to cyberattack (and the related mitigations) are likely to align, although the consequence severity of the attack will vary.

Cyber security risks refer to risks to vehicles, passengers and other road users, testbed infrastructure and data arising from electronic and telecommunications means. There are a range of cyber security risks that are relevant to all CAVs (including CAVs that can be remotely operated). Examples of cyber security threats include:

- Tampering with a vehicle's wired or wireless connections
- Equipment jamming
- Tampering with equipment testbed infrastructure
- Information disclosure from testbed IT infrastructure

Table 1 outlines the STRIDE method of threat analysis, which categorises the types of threats that CAVs are vulnerable to and gives a brief description of each. These terms will be used throughout this report to refer to cyber security threats.

Table 1: STRIDE: method for threat analysis

THREAT CATEGORY	DESCRIPTION
Spoofing	A person or entity masquerades as another
Tampering	Insertion, modification or deletion of data
Repudiation	An entity denies responsibility for an action
Information disclosure	Provision or leak of information to an unauthorised entity
Denial of service	Making a resource unavailable to authorised entities
Elevation of privilege	An entity gains greater authorisation than permitted

[2] https://unece.org/sites/default/files/2021-09/ECE-TRANS-WP1-2021-Informal%20document-1e_2.pdf

These threats could all be relevant to a remotely operated CAV. However, for the purpose of this report, we have focused on the unique or additional cyber security risks related to remote driving:

- Threats to the internal functions, local software and network security of the remote vehicle
- Security of communications to and from the vehicle
- Implications of a remote vehicle operating without a safety driver in the vehicle
- Implications of different types of remote operation (line of sight, relying on vehicle sensors, relying on infrastructure sensors)

1.6 Guidance and standards

There is currently limited guidance available specifically covering remote operation of on-road vehicles. However, there are several substantial documents that set guidelines and recommendations for the cyber security of CAVs in general, which form a good base from which to work. These include:

- BSI Publicly Available Specification (PAS) 1885 (BSI, 2018): This document elaborates on the Department for Transport (DfT) key principles of vehicle cyber security for connected and automated vehicles (DfT, 2017), providing guidance for the implementation of the principles (principles are summarised in the box below).
- BSI PAS 11281 (BSI, 2018). This document focuses on the safety implications of security and the interaction between security and safety.
- European C-ITS standards developed by ETSI (2010;2012;2017) for the security of V2X vehicles.
- *UNECE Regulation 155 – UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management systems* (United Nations, 2021). This regulation outlines requirements to which vehicle manufacturers must adhere to, to obtain and maintain a certificate of compliance for their cyber security management systems. It includes the technical requirements for the management systems required to effectively manage the cyber security of a vehicle over its lifecycle and to ensure software updates will be sufficiently appraised and protected before they are sent to a vehicle.

Principles of cyber security for connected and automated vehicles (DfT, 2017)

1. Organisational security is owned, governed and promoted at board level
2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain
3. Organisations need product aftercare and incident response to ensure systems are secure over their lifetime
4. All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system
5. Systems are designed using a defence-in-depth approach
6. The security of all software is managed throughout its lifetime
7. The storage and transmission of data is secure and can be controlled
8. The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail

1.7 Safety Cases

The aim of this report is to provide recommendations on the cyber risks and associated mitigations that may need to be included in a safety case for remote operation. Initially it is important to understand the purpose of a safety case is, and how cyber security fits within it.

The **safety case** is a document compiled to demonstrate how safety and security has been assessed and will be effectively managed during operation. *The Code of Practice for Automated Vehicle Trialling* states that all trialling organisations should develop a detailed safety case for any trialling they wish to undertake in the UK (DfT, 2019). The document *Safety Case Framework: The Guidance Edition for Creators* brings together the key learnings from several standards and good practice documents to provide concise guidance on the development of safety cases (Zenzic, 2021).

The Zenzic safety case framework describes three major components of a **safety case**:

1. **System safety case**: The system that is referred to here is the interconnected physical, electromechanical, electronic and data elements of the vehicle, including the automated driving system (ADS) and any offboard subsystems that directly facilitate automated driving. The system safety case outlines how the safety of this collective system has been assessed, including its 'functional safety' (managing risks pertaining to potential system faults) and 'safety of the intended function' (managing inherent risks due to design limitations). A system safety case may be reused for trials where the same system is in place.

2. **Operational safety case**: This considers the ways the trial vehicles will interact with the operating environment, including the route, operator or safety driver, passengers, and other road users. It provides evidence to demonstrate operational safety and includes mitigations or controls proportionate to the risk posed. It is time and location dependent, and therefore needs to be tailored for each trial.

3. **Security safety case**: This considers the risks of interference with trial equipment, including the ADS. It includes physical access risks and **cyber security** risks (risks coming from electronic and telecommunications means). This is the primary concern of this report.

Cyber security relates to all computer-based, electronic and telecommunications systems involved in the trial, including systems associated with the testbed and trial operator, the electronic systems of the vehicle, systems enabling communications, control and monitoring and any remote systems (Zenzic, 2021).

2 Literature review method

2.1 Approach

This literature review comprised a review of the current good practice standards and guidelines regarding the cyber security of CAVs. The literature review also explored the different ways in which a vehicle could be tele-operated and examined the types of security measures to prevent it being attacked.

The literature review had the following aims:

1. To review the current and new good practice for the cyber security of remote operations of CAVs
2. Make recommendations regarding the evidence to include in the final security case

The literature review took a systematic approach consisting of three tasks:

1. Definition of search terms to be used
2. Assessment of the quality and relevance of identified literature
3. In-depth review of full text literature

2.2 Search terms

A list of search terms relevant to the research aims was generated to run the literature review (Appendix A). These search terms were tested and applied in several research databases (e.g., Google Scholar, ScienceDirect, TRID) as Boolean search expressions.

Other research databases were tested (e.g., Journal of Safety Research, Transport Policy) and found to not be useful sources for this review as they failed to produce sufficient literature relevant to the current investigation. Multiple searches were conducted within each database through an iterative process, wherein search terms were tested individually and in combination with each other to identify which terms generated relevant results. This ensured that the review was as in-depth as possible.

Once the terms had been tested, those that generated relevant results were merged into a Boolean search expression. This allowed the output to be refined to the most manageable number of relevant texts. All additional filters were kept as ‘open’ to provide access to a broad range of results. A more general search for grey literature was also conducted, to ensure that sources such as press releases, especially in other countries, were not missed.

2.3 Assessment of quality and relevance

Once the final papers had been obtained, an assessment of quality, relevance and timeliness was carried out. Specific inclusion criteria were applied to assess the suitability of the literature. This was done to ensure that only the highest quality and most relevant literature was identified. Each document was reviewed using the following criteria:

- Relevance – how useful was the paper in fulfilling the research aims

- Timeliness – how recent was the paper; more recent literature (e.g. from 2016 onwards) was deemed more useful
- Quality – whether the paper detailed a robust scientific study

Using these criteria ensured that a manageable, yet high quality set of papers were reviewed. In total, 90 titles and abstracts were screened.

2.4 In-depth review of full text literature

The literature was reviewed in full and findings recorded systematically. Eighteen articles were reviewed in-depth. Each individual text was examined, and the relevance to remote operations of CAVs and mitigations for cyber security risks were summarised. Conclusions relating to the research aims of the project were drawn, where possible, from each reference and summary. After the in-depth review, a total of twelve papers were included in the report. Once these twelve papers had been identified, they were collectively examined to identify the most prevalent mitigations for cyber security risks to remote operations of CAVs. The mitigations were also assessed on the effort required to implement them.

3 Literature review results

3.1 Brief overview of findings

Ensuring the safe remote operation of CAVs with regards to cyber security is a significant challenge. In particular, the presence of a remotely controlled vehicle necessitates a secure wireless network over which the signals from the remote operator can be sent. It is foreseeable that hackers could gain control of the network and therefore, direct control of the vehicle, through the remote operation facility. By reviewing the evidence of what cyber security risks are prevalent in the literature, and examining mitigations possible to prevent attacks, potential mitigations for defending remotely operated CAVs against cyber security attacks were identified.

3.1.1 Mitigations

An examination of the literature revealed sixty-eight different mentions of mitigations (see Appendix BList of mitigations found in the literature search). Of these, five main mitigations against cyber attacks appeared particularly prevalent (see Figure 1). These are discussed in detail in section 3.2.2. These identified mitigations were discussed most frequently within the literature and, as such, were judged to demonstrate good practice in the remote operations of CAVs. The mitigations were:

- Data Encryption
- Authentication
- Intrusion detection
- Time based mitigations
- Signal based mitigations

Some other mitigations were also mentioned, albeit only by one or two papers meaning that these mitigations are not likely to be as commonly used to control the level of risk posed. See Appendix BList of mitigations found in the literature search for a full breakdown of these additional mitigations.

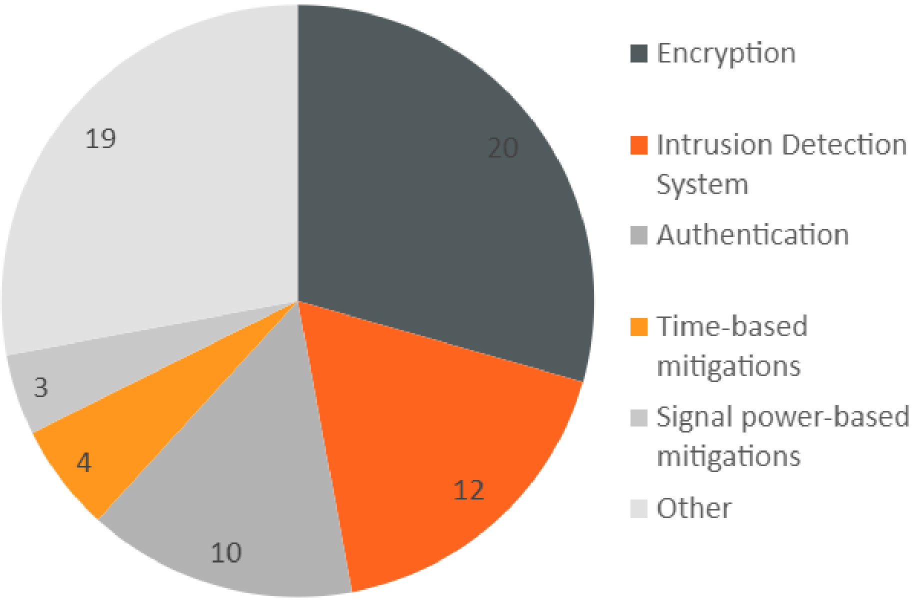

Figure 1: Key cyber security mitigations identified (N=68)

3.1.2 Threats

We have organised the potential threats to CAV remote operation identified under the following categories:

- Threats to the internal functions, local software, and network security of the remote vehicle
- Security of communications to and from the vehicle
- Implications of a remote vehicle operating without a safety driver in the vehicle
- Implications of different types of remote operation (line of sight, relying on vehicle sensors, relying on infrastructure sensors)

These findings are detailed in the remainder of this section. The findings are broken down into two parts: potential attack vectors and their respective mitigations.

3.2 Threats to the internal functions, local software, and network security of the remote vehicle

3.2.1 Attack vectors

Local software

A key attack vector which can be used to target the software of a CAV is malware. Malware refers to malicious software programs used to disrupt computer operations or gain authorised access to information (Antunes, 2014). In the context of CAV operations, malware can infect vehicles through internet connections, Wi-Fi, and file exchange (Antunes, 2014, p.10). Malware may be transferred using disguised communications, which may appear to come from a trusted source, but in fact originate from a hacker. This communication may contain hostile or intrusive software, such as spyware. Research has shown that malware poses a significant threat to the cyber security of CAVs (Parkinson *et al.*, 2017). The threat from malware may occur through weaknesses within the local software of the vehicle but also through the physical and network security. Malware attacks may also be caused by hackers physically inserting malware into the CAV, for example by USB connection (Bharati *et al.*, 2020) or inserting an infected CD (Khan *et al.*, 2020).

Threats to the internal functions of the vehicle

Two internal functions of CAVs may be targeted in a cyber security attack; these are the Electronic Control Units (ECUs) and the On-Board Diagnostics (OBD).

ECUs are computing devices in a vehicle that are responsible for controlling specific functions. Individual ECUs are often interconnected using Controller Area Network (CAN) buses or similar. OBD is a standardized system that allows external electronics to interface with a car's computer system(s). The primary purpose of an OBD is diagnostics; when a car sensor identifies an issue, the data is stored and can be read via the OBD at a later date. The driver may also be informed through the dashboard, but not always. Figure 2 highlights how the individual ECU units form the CAN Bus.

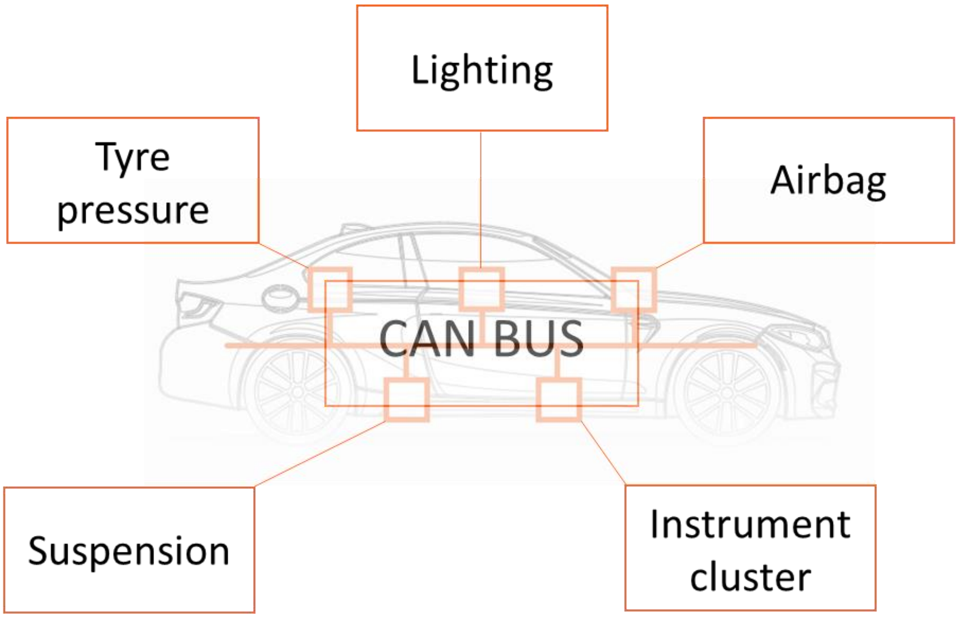

Figure 2: Example of the connections on a CAN-BUS

By gaining access to the ECU, a hacker can attack the software system of the CAV. Due to the close proximity and connectivity of the CAN bus (see Figure 2) and connected ECUs, attacking the ECU could have deleterious consequences for safe operation of the CAV (Studnia *et al.*, 2013). For example, the tyre pressure monitoring system could be manipulated or even the driving of the vehicle itself. A real-life example of this is described by Jafarnejad et al (Jafarnedjad *et al.*, 2015). In this study, a 'brute force method' was used to detect the correct password for a Renault Twizy. The researchers were then able to change the gear, apply the brake and remotely move the car both forwards and backwards.

Network security

Alongside cellular communications, Wi-Fi is used for vehicle to vehicle and vehicle to infrastructure communications (Bharati *et al.*, 2020); in the case of safe remote operations of CAVs, this creates a potential attack vector. Wi-Fi is a non-dedicated channel and is therefore insecure. 5G, as described below, is a better option to use for communications.

One potential threat to Wi-Fi communications is an Evil Twin Attack (ETA). An ETA involves a rogue Wi-Fi access point being created. Whilst this point may appear legitimate, it is designed to eavesdrop on wireless communications (Nakhila *et al.*, 2015). In the event of an ETA attack, personal or sensitive data may be stolen.

The exploitation of Fifth Generation (5G) networks also presents a potential threat to network security. 5G uses cellular networks, for which the service area is divided into small geographical cells. Potential cyber attacks on 5G connection include injection, eavesdropping and denial of service attacks (Bharati *et al.*, 2020).

- *Eavesdropping attacks* occur when unauthorized individuals gain access to vehicular messages (El-Rewini *et al.*, 2020). In the context of 5G device to device (DtD) communications, the relaying node can be thought of as an eavesdropper from whom data must be hidden, even though it is essential to the transmission (Zhang *et al.*, 2010).
- In an *injection attack*, attackers inject fake messages into an automotive bus system (El-Rewini *et al.*, 2020). Attackers can gain entry to the in-vehicle infotainment & telematics systems.
- *Denial of Service (DoS)* attacks occur when attackers continually send high priority messages that block legitimate low priority messages. DoS attacks are used an avenue to override vehicle controls, which allow attackers to take control of the vehicle.

DoS attacks pose a particular threat to the cyber security of CAVs. A DoS attack has the potential to drain a CAV of all its resources, to cause a collision involving the CAV and another vehicle. This may be accomplished by targeting the battery in a CAV. Alternatively, a DoS attack may be used to block the communication channels with other vehicles.

Jamming attacks also pose a threat to the remote operations of CAVs. Jamming is when radio noise interrupts the communications between the CAV and the cloud (Khan *et al.*, 2020). Jamming can be conducted on any wireless network (e.g., Zigbee, WiFi, cellular etc.), including GPS, which makes this attack a significant threat. For example, Zigbee jamming has been shown to drain the CAV battery in the correct conditions (Bharati *et al.*, 2020).

5G and Wi-Fi also pose a risk in terms of information disclosure. Information disclosure is used to describe any consequence or technical impact, for any vulnerability, which results in a loss of confidentiality. Research has shown that information disclosure is a key issue in the cyber security of remote operations of CAVs (Patsakis *et al.*, n.d.). Information disclosure is usually initiated by a passive man in the middle attack (MiMA). A MiMA is when a hacker interrupts the messages between both the CAV and the sender and redirects them to eavesdrop / manipulate the communication.

A discussion paper by Guevara and Cheein (2020) examined the challenges of using 5G technology on smart cities, intelligent transportation systems and vehicular communications. As the authors highlight, by its nature, 5G carries a significant amount of personal privacy information, including identity and position. The threat from privacy protection and information disclosure is particularly prevalent in CAVs, where leaked privacy information may reveal the location of a vehicle. As highlighted by Collingwood (2017), the data obtained from a CAV could be used to convey sensitive information about where a user is and what they are doing, as well as their past and future locations. This could potentially be used to build a profile of the individual, if for instance, they regularly park in a wealthy neighbourhood.

3.2.2 Mitigations

Several mitigations for network security attacks are evident from the literature. These are data encryption, using software updates and moving target defence. Data encryption is a well-documented method for enhancing the privacy protection of CAVs (Raiyn, 2018; La Manna *et al.*, 2021).

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission. An individual's vehicle data, if encrypted, would therefore be unusable for any attacker who obtains it, therefore mitigating against any such attacks. Encryption has been shown to be effective against attacks on the ECU / CAN bus, as makes it difficult to decrypt any encrypted messages. Encryption is also effective when used against jamming attacks (Khan *et al.*, 2020).

Moving target defence and intrusion detection are both other mitigations against eavesdropping (Gudla *et al.*, 2018). Moving target defence works by changing the system characteristics from static to dynamic, thus making it more complex to attack. By implementing randomness into the system configuration, to make it less static and predictable, the attacker is forced to spend longer carrying out a more resource intensive attack. Intrusion detection systems can be used to protect a CAV against potential jamming attacks and replay attacks. Intrusion detection automatically inform the remote driver that an intruder had gained access to the system (Bharati *et al.*, 2020).

Software updates including updating firmware and messaging software as well as an updated master key are also ways to mitigate against eavesdropping (Chowdhury *et al.*, 2020).

Mitigations for Wi-Fi jamming attacks are software related and include confidentiality and integrity protection, authentication, authorisation, and software patches (Bharati *et al.*, 2020). Data leaks in Wi-Fi networks can be prevented through using randomised or momentary identifiers (i.e., MAC and IP speeches) to detach the data from the CAVs.

A DoS attack may be prevented by continuously checking the system for these types of attacks (Gudla *et al.*, 2018); this is referred to as intrusion detection and is discussed in detail in section 3.3.3. The use of firewalls is another method to protect against DoS (He *et al.*, 2017), as well as cryptographic techniques such as the use of a Message Authentication

Code (MAC) (see section 3.3.2 for a detailed description of MAC). The potential impact of a DoS attack may be mitigated by having a contingency plan in place. For example, He, Meng and Qu (Anon., 2017) suggest that, should a CAV be hijacked, the CAV should enter a safe state by pulling up to the side of the road to a safe location when a sudden battery loss is detected. This would reduce the likelihood that the CAV would run out of power and collide with another vehicle.

Attacks on a CAV's ECU(s) may be prevented by cryptographic solutions through ECU-authentication. Although this is hard to establish for all components of a CAN-bus, dedicated hardware security modules can be created to ensure messages are encrypted. Further cyber mitigations include anomaly detection (if the delay between two frames is too short) or only allowing signals to go to certain nodes of the CAN-bus so any cyber attacks do not attack the whole system (Studnia *et al.*, 2013).

Jamming attacks, while difficult to prevent, may be mitigated in two ways. These are:

1. Assigning IPs to specific vehicles and dropping duplicate IPs during message transfer.
2. Verifying packet delay using timing attack prevention protocol (Chowdhury *et al.*, 2020).

Certain mitigations have been suggested including only allowing USBs that are certified with a registered website and blocking any further movement from non-critical to critical areas. Antivirus software can be mitigated via firewalls, antivirus, and intrusion detection systems (Altawy and Youssef, 2016).

3.3 Security of communications to and from the vehicle

3.3.1 Attack vectors

Spoofing

Spoofing is the act of disguising a communication to make it appear to be from a known, trusted source, when in fact it originates from an unknown source.

He, Meng and Qu (2020) describe how a spoofing attack works, within the context of CAV operations.

- A vehicle uses Global Navigation Satellite System (GNSS) to locate itself and navigate.
- In a spoofing attack, similar GNSS signals are sent to the CAV, to mislead the operators.
- These fake signals may mislead the driver of the vehicle into driving to an incorrect location or into potentially dangerous objects.
- These fake signals may also falsely suggest that a vehicle is in the immediate vicinity of the CAV, leading to potentially dangerous manoeuvres as it tries to evade the fictional object (He *et al.*, 2017).

A spoofing attack is potentially more threatening than a GNSS jamming attack, in that while a jamming attack may disable a vehicle, a spoofing attack may change the route or destination altogether. This may lead to damage or injuries, should the vehicle be deliberately led astray by an attacker.

3.3.2 Mitigations

Several mitigations exist for countering spoofing attacks. These centre around ensuring that all communications come from a legitimate source. Using Message Authentication Code (MAC) is one such way to achieve this.

A *Message Authentication Code (MAC)* is a tag attached to a message to ensure the integrity and authenticity of the message (Liu, 2009). A MAC is created by a MAC algorithm using a secret cryptographic key and attached to a message. The purpose of a MAC is to validate the source of a message and its integrity. As Figure 3 highlights, the MAC code used in the message provided by the sender is checked against that of the receiver. If it matches, the message is judged to be authentic.

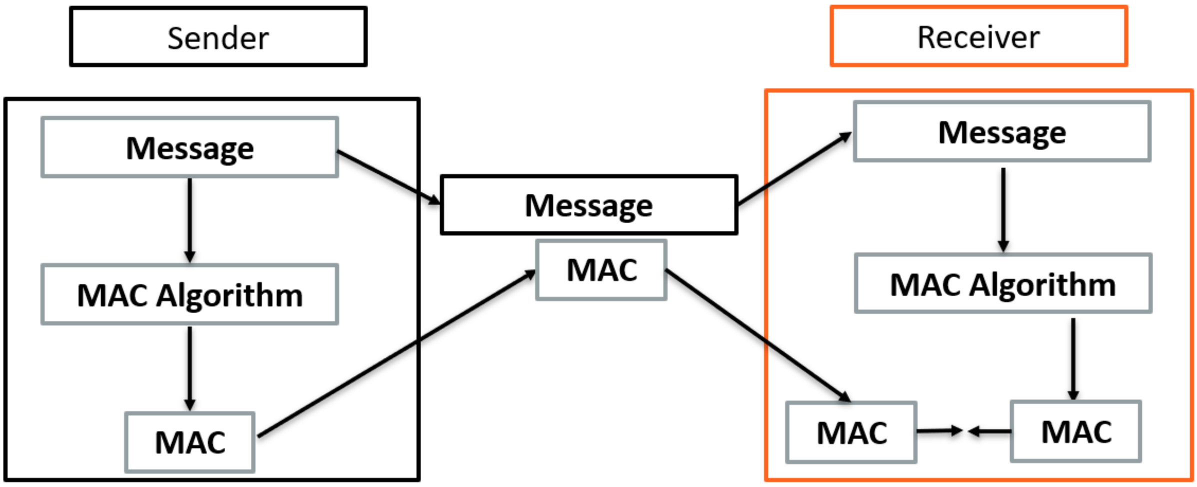

Figure 3: Message Authentication Code (MAC) process

Examining the authenticity of messages by examining if other CAVs can corroborate the information provided (i.e., if other CAVs also detect the presence of the fake car) is another way to reduce the threat from spoofing (He *et al.*, 2017). Examining the signal characteristics of a message is also a tested solution. The travelling time of a signal may be used to indicate how far away the spoofing signal was, which can then be used to deduce whether the sender is legitimate (Altawy and Youssef, 2016).

Another way to identify the presence of a spoofing attack is to use time and signal-based mitigations.

A time-based mitigation to detect spoofing involves checking the GPS observables that denote the signals' travelling time, as a proxy to indicate how far away the sources are (Altawy and Youssef, 2016).

A signal-based mitigation involves examining the sudden changes in signal power or observables within a tolerable range, as a sudden increase in power may be an indicator of the start of a spoofing attack (Chowdhury *et al.*, 2020).

Replay attack

A replay attack occurs when an attacker gains control of the vehicle sensors, to replace the existing measurements with fake signals. While the system is in normal operation, the attacker observes and records the sensor readings for a certain amount of time and then feeds the control system with the recorded measurements while carrying out their attack (Merco *et al.*, 2018). For instance, if a CAV received communication that a collision or incident had occurred further down its intended route, an attacker could replay this message, to cause the CAV to again deviate from its path.

3.3.3 Mitigations

There are two main ways to mitigate against relay attacks.

Intrusion detection is one way to protect against replay attacks. Intrusion detection automatically inform the remote driver that an intruder had gained access to the system (Bharati *et al.*, 2020).

A *challenge response method* is another mitigation. This is used to ensure that the message received by the CAV originates from a legitimate source. The sender of the message is required, by the vehicle, to provide a challenge value which only the sender knows (He *et al.*, 2017).

Time-based mitigations are other ways to reduce the threat from replay attacks. For example, adding a time stamp (Chowdhury *et al.*, 2020), or tagging an encrypting component with a session ID and component number (Khan *et al.*, 2020) have both been suggested as mitigations to replay attacks. By adding a time stamp to each packet, it may be possible to identify which packets have only just been sent, and which ones have been sent previously. Therefore, any packets that are identified as being sent outside of a given time window can be ignored, as this may indicate a replay attack.

3.4 Implications of safety driver vs no safety driver

According to BSI Vocabulary Flex (2020), a Safety Driver has been described as a person who:

- Is situated within a CAV with access to its controls.
- Pays attention to the CAV's operating environment.
- Ensures the rules of the testing area are followed.
- Identifies risks.

A *Remote Operator* is a generic term for a human who supervises the operation of a CAV from a remote location. Supervision can comprise monitoring the CAV, intervening in the CAVs' operation, assisting passengers, or managing part of the CAV service. The supervision of operations may need to be real-time, such as for remote driving, and the Remote Operator may or may not have final authority for control of the CAV.

A *safety driver* is responsible for identifying deviations from expected behaviours and can take full control of the Dynamic Driving Task (DDT) of an CAV when necessary. If an CAV encounters an anomaly, a safety driver will be able to slow the vehicle down and may be able to carry on. If no safety driver is in the vehicle, this may not be possible

3.5 Implications of different types of remote operation (line of sight, relying on vehicle sensors, relying on infrastructure sensors)

3.5.1 Attack vectors

A clear attack vector which falls under denial of service comes in the form of LiDAR and Radar attacks. Light detection and ranging (LiDAR) use light point cloud to detect the distance and boundaries of surrounding obstacles and environments. This assists the vehicle in localisation and parking. The potential issue of LiDAR use is compounded by a reliance on sensors to guide the vehicle, as is the case in remote operations. Attacks on LiDAR and radar present a threat in terms of damage to the vehicle, its passengers and other road users, rather than the theft or manipulation of data.

He et al (2020) describe several ways in which a CAV vehicle might be attacked via its LiDAR and radar.

- *Jamming attacks* jam the LiDAR by using strong lights to reflect the original light. This attack may not result in information theft; rather, vehicle damage may occur as a result.
- *Hidden object attacks* interfere with LiDAR's reliance on light reflections to orient the vehicle. Through using light absorbing materials to camouflage objects in the vehicle's path, the vehicle itself may crash, potentially injuring the driver/ passengers.

Radar attacks also pose a significant threat to CAVs. Radar is like LiDAR, except that it uses radio waves rather than light to detect surroundings. CAVs use two types of radar.

- Millimetre Radar –used for object detection.
- Ultrasonic Sound Waves – this is slow and is used for short distance scenarios such as parking assistance system.

The potential attacks which can be leveraged against radar are like lidar; these are detailed below.

- *Jamming attacks* target the radar sensors and use the noise to degrade the signal of the radar. This makes the vehicle vulnerable, as it may not be able to detect an object in its surroundings.
- *Fake object attacks***.** Attacks create fake radar signals. These are then detected by other vehicles, and in the process of attempting to take evasive action to avoid these objects, collisions between one vehicle and another may occur.

3.5.2 Mitigations

Mitigations to radar and LiDAR attacks are documented in He et al. (2020) These are categorised into five main ways in which all attacks may be mitigated. For LiDAR and radar, the main mitigation is reduction. Reduction aims to reduce the possibility of an attack down to a minimum, rather than eliminate it altogether. In the context of LiDAR and radar sensors, this involves using both sensors, rather than only relying on one for direction. For example, should one sensor be eliminated through a blind vision attack, for instance, another sensor could still be used to guide the vehicle safely.

Khan et al (2020) suggest that encryption and cryptography techniques can also be apt mitigations against sensors failing. Sensor tampering indicators are also important to detect a cyber attack. Attacks on ultrasonic can be mitigated with pop-noise-based general defence strategy, audio turbulence and audio squeezing. Central gateway-based architecture in the automotive bus system can also help with sensor impersonation (Chowdhury *et al.*, 2020).

3.6 Summary of literature review findings

The literature review findings will be supported by the outcomes of the stakeholder interviews, described in section 0These interviews supplement and validate the outcomes of the literature review, and the good practice options may change to account for this additional information.

The aim of the literature review was to review the current good practices for the cyber security of remote operations of CAVs and to provide options regarding effective mitigations and therefore the evidence to include in the safety case. The remote operation of a CAV requires a reliable link to a command centre meaning that the safe operation of the vehicle could be compromised by cyber attack. There may also be a lack of line of sight of the vehicle, for the remote operator, making reliable methods of monitoring for attacks without requiring sight of the vehicle critical. The options provided in this report are based on the findings regarding the additional or unique requirements that arise from remote operation (over and above the cyber security measures for CAV operation when there is a driver or operator in the vehicle).

The literature review revealed five main mitigations for countering cyber security threats directed at CAVs. Of these five groups of mitigations, the following options are the most relevant for the remote operation of CAVs.

- **Encryption** of the data which is shared between the CAV and the remote command centre.
- **Use of authentication methods,** including MAC, to further ensure that the communications between the command centre and remote CAV are authentic.
- **Intrusion detection systems** are used to safeguard the vehicle against attacks and to notify the remote operator of potential cyber attacks.

Particular attention should be paid to protecting those aspects of remote operation that create the greatest vulnerability and risk. This can be determined through a threat analysis of the specific systems, but it is likely to include (i) protecting the integrity of the connection between the remote operation base and the vehicle and (ii) implementing methods to detect attacks and ensure safe operation without needing the vehicle to be within line of sight.

In addition to identifying cyber threats and implementing cyber security controls, the Zenzic (2021) *Safety Case Framework: The Guidance Edition for Creators* recommends that (1) security controls are tested to confirm whether they effectively mitigate cyber risks and (2) the risk assessment is updated with results from these tests. They mention three cyber security testing methods: vulnerability scanning, fuzz testing and penetration testing. These are outlined in the box below. It would be advisable to apply cyber security testing methods to those aspects of the remote operation that pose the greatest risk if compromised. Finally, the Zenzic document also recommends ongoing process for managing security risks to ensure that new or changed risks are identified and that controls are updated accordingly.

Summary of typical cyber security testing methods (from Zenzic 2021, p.75)

Vulnerability scanning: Testing, usually automated, of a system for instances of known cyber security vulnerabilities. Vulnerability scanning tools exist for many software and network technologies and are an effective way to quickly find known issues, although they are less effective for finding unknown or system-specific issues

Fuzz testing: A method for identifying weaknesses that could potentially be exploited by testing a system with intentionally invalid or malformed input data. The input data can be generated by a combination of random, systematic or adaptive methods, and the effect on the system is monitored to determine any exploitable cases.

Penetration testing: A method in which the tester tries to attack the system by adopting similar tools and techniques to a real attacker. This approach is time consuming and is not feasible to apply exhaustively, but it is an effective way of identifying previously unknown vulnerabilities and exploring how they could be exploited.

4 Stakeholder engagement method

4.1 Approach

Stakeholder engagement was conducted via semi-structured interviews, which aimed to improve understanding of the following:

- Current practice in assessing, monitoring and mitigating cyber security risks that are relevant to remote operations.
- Whether any specific cyber security provisions are required (or have been implemented) for remote operations.
- Any gaps and weaknesses that are perceived in cyber security provisions for remote operations.

To explore these issues, two stakeholder groups were identified. TRL developed a list of questions specific to each group:

- Group one (Trial operators) – those responsible for ensuring cyber security and preparing safety cases.
- Group two (Expert stakeholders) – other stakeholders who may require evidence of cyber security or who review safety cases

The questions asked during the interviews are shown in Table 2.

Table 2: Questions asked during the stakeholder engagement

Group one (trial operators)	Group two (expert stakeholders)
How do you currently assess your systems for cyber security risks? What are the biggest risks/concerns relating to ensuring vehicles can be remotely operated without being vulnerable to cyber threats? Where do these vulnerabilities lie? What controls or vehicle manoeuvres could be used to mitigate the severity or consequence of a cyber attack? How are you already evidencing management of these threats? Would any further structure/support make it easier for you to manage and demonstrate how you manage these	What are the biggest risks/concerns relating to ensuring vehicles (or telemetry/communications more generally) can be remotely operated without being vulnerable to cyber threats? What information would make you feel confident that cyber security had been addressed? Have you already encountered these standards/cyber mitigations in this industry or more widely? How are standards and regulations currently addressing cyber vulnerabilities, and are you aware of notable gaps? Where/with whom does the responsibility for the cyber security of the system lie?

threats?	

4.2 Stakeholder recruitment

Relevant stakeholders were identified from organisations which had previously taken part in related engagement activities. Thirteen stakeholders were sent information describing the project aims and objectives and were asked to complete a short survey to indicate their willingness to participate in an interview, and to provide consent. Nine stakeholders agreed to take part in the stakeholder engagement; these are described in Table 3.

Table 3. Participating stakeholders

Organisation type	Group	Current experience with remote operations
Autonomous Vehicle (AV) Developer	1	Conducting trials of remote assistance of automated vehicles
CAV developer	1	Conducting trials of remote driving of automated vehicles
CAV developer	1	Monitoring automated vehicles with fleet management and exploring remote assistance
Academic Research Expert (Telecoms & Cyber Security)	1	Researching cyber threats and mitigations for automated and remote operation
Cyber Security Technology Expert	1	Generating technical solutions for ensuring cyber security for remote operation
Academic Research (Automation & Cyber Security)	1	Researching cyber threats and mitigations for automated and remote operation
Insurer	2	Insuring automated vehicles
Local Authority	2	Hosting trials of automated vehicles in their area or responsibility
UK Government body	2	Generating guidance for and fostering development of automated vehicles

4.3 Interview method

Interviews were conducted via Microsoft Teams during December 2021 and January 2022 and were recorded and transcribed with the consent of each participant. Either one or two interviewers were present for each interview, with one individual being present at every interview for consistency.

At the beginning of each interview, the participant was given a brief introduction to the ENCODE project before being asked the five or six questions relevant to their group. The interviewer(s) probed responses to elicit further information where necessary.

4.4 Analysis

A transcript of each interview was generated using Microsoft Teams' automated transcription service. A third researcher, independent to the interviewers, checked the transcript against the recording to correct any errors to ensure data quality. All data were fully anonymised (e.g. reference to organisation names etc. removed from transcripts) before analysis to ensure that identifying information could not be linked to participants. An internal workshop was held which was attended by the technical lead, the interviewers, and two independent researchers. During this workshop, the interviewers presented and discussed the themes identified through their interviews to achieve an overall consensus regarding the final high-level themes. Following the workshop, each participant's responses were summarised and interpreted by two researchers, and quotations from the transcripts were identified to support the high-level themes.

Due to the limited scope of the task, no in-depth analysis of the transcripts was carried out; the purpose was to make sure that high-level themes were identified to inform the recommendations for the safety case.

5 Stakeholder engagement results

This section presents the findings of the questions asked during the stakeholder engagement.

5.1 Trial operators (group 1)

5.1.1 How do you currently assess your systems for cyber security risks?

Two main, opposing themes emerged from the analysis in relation to assessing systems for cyber security risks. The CAV developers agreed that focussing on standardised ways of assessing systems (including the use of standards, e.g. PAS 1885 or ISO 21434) was beneficial.

> *"We follow the main standards, PAS 1885, but mostly it's the ISO 21434." (CAV developer)*

In contrast, the interviewees from the technology provider and Academic Research highlighted promoting system resilience involving implementing multiple layers of protection, to reduce risks to a minimum.

> *"We're very experienced in threat modelling. We'll take a threat modelling approach[…], the mitre attack framework." (Academic Research Expert)*

> *"And that's where for us our approach is more of a best practice from our side and our knowledge and cyber security and building cyber physical systems from industrial systems[…]so within [name of organisation] itself we have our own risk framework that we have developed. That allows us to do that risk assessment and that threat modelling."(Cyber Security Technology Expert)*

The findings for this question may suggest a potential disparity between the stakeholders in terms of security risk assessment. This may be because CAV developers require a specific set of guidelines, which pertain directly to CAVs. For instance, PAS 1885 relates directly to the cyber security and functional safety aspects of the entire automotive development and use life cycle. Conversely, the cyber security experts may view the issue of cyber security from a more holistic viewpoint.

5.1.2 What are the biggest risks/concerns relating to ensuring vehicles can be remotely operated without being vulnerable to cyber threats?

The interviewees' responses highlighted four main risks and concerns with regards to remote vehicle operations.

Stakeholders expressed concern that, with remote operation, potential issues may arise if the communication in remote operation becomes disengaged.

> *"You know, then we look at what could happen in this communication. So it's either we don't receive the control signal from teleoperation or it's wrong." (Academic Research Expert)*

Interviewees also expressed concerns relating to the security by design of remotely operated vehicles. Security by design, in software engineering terms, is designing software to be secure from the outset, to reduce the likelihood of flaws which might compromise information security. Interviewees expressed concern that the security of safety systems may be too focussed on mechanical safety, rather than cyber.

> *"The main concern is security by design and the security lifecycle. If those two are enforced or deployed from the get-go that will actually reduce a lot of the risks." (Cyber Security Technology Expert)*

> *"Most of the issues that we are finding in the systems that are coming out, they are being built and tested from a mechanical safety, from a physical safety. They are still getting into the sphere of testing it from a digital safety, which cyber security is an element of." (Cyber Security Technology Expert)*

Failure at scale was another overarching concern; this is where a potential flaw in the teleoperation of remote vehicles may affect a significant number of vehicles within an entire fleet. Interviewees highlighted that engineering the teleoperation correctly should reduce this risk.

> *"My biggest concern is failure at scale, That's the biggest concern in vehicles. Now, so long as you've engineered the teleoperation well, you shouldn't have failure at scale." (Academic Research Expert)*

The final concern revolved around the physical security of the vehicle. Though a remote cyber attack may be prevented, a hacker may still be able to carry out a physical attack on the vehicle, through targeting an ECU, for example.

> *"It's usually physical access from people. If someone wanted to take down our system, those are the points where they would most be able to." (CAV developer)*

5.1.3 Where do these vulnerabilities lie?

Interviewees suggested potential vulnerabilities in multiple areas. One of these areas was network connectivity, specifically the communications network between the vehicle and the teleoperations system as this may be dependent on a Long Term Evolution (LTE), a mobile network, or a cloud system.

> *"When it comes towards teleoperation, when you are passing command and control at top of messages, that ability of those messages to be intercepted, spoofed, manipulated through that process." (Cyber Security Technology Expert)*

One expert highlighted the threat of denial of service which, similarly, stems from the vulnerability of the teleoperations system and the potential to block it through jamming during the remote phases of the trial.

> *"Jamming is the easiest thing that can be either at the centre end, so they could have some denial of service. It could be at the vehicle, or in some intermediate point. The two most likely are to be at the centre or at the vehicle, and that's what I think is a big problem." (Academic Research Expert)*

CAV developers, in particular, highlighted that the physical security of the vehicle (e.g. the USB ports) presents a vulnerability. Systems which can be physically accessed are most vulnerable; the drive by wire system is one of the most safety critical systems as it is ultimately the most important measures of controlling the vehicle. Moreover, conducting trials in a public environment presents opportunities to physically target the vehicle.

> *"Our drive by wire system, I suppose, is the key bit because you need physical access to change it because it's not connected to any web-based interface and (name of organisation) system secures that. So that's the most important low hanging fruit for them to pick off." (CAV developer)*

5.1.4 What controls or vehicle manoeuvres could be used to mitigate the severity or consequence of a cyber attack?

There were three distinct themes that emerged in relation to mitigating attacks. First, controls within the system were often mentioned to make it harder for intruders to hack into the system, or hack into the entire system

> *"So the way we manage it is to limit what can be done by any one system and so if you've got systems cross checking each other, then if what one system does is out of the bounds of what the other systems will allow then you've added a level of safety in there." (CAV developer)*

> *"And that's where security by design becomes important where you make those devices aware of what is their normal behaviour, and then when suddenly they are doing abnormal behaviour [because of a hack], they themselves or the others on their network will flag that as an alert." (Cyber Security Technology Expert)*

As well as controls to ensure that the vehicle was secure by design, the value of minimum risk manoeuvres (MRMs) was noted, and a few specific examples were discussed:

> *"Yep, safety driver could take control of the vehicle and cause it to go into manual mode and then the system is in manual, it's just a normal car at that stage." (CAV developer)*

On the other hand, while performing minimum risk manoeuvres could help to mitigate many cyber attacks, some of the experts with a deeper background in cyber security highlighted that the same manoeuvre should not performed in response to every scenario of cyber attack. For example, some interviewees noted that MRMs should be used with care and be context specific, as some MRMs may be useful in one scenario but be counterproductive in another:

> *"Because I remember some of the people on the committee said, OK, when the vehicle is driving and it's under cyber attack, you stop it straight ahead. I was like well you can't stop it straight ahead. You might be in the middle of the road, you might be turning, you can't do that." (Cyber Security Technology Expert)*

> *"And you have to understand it, you know, what you're doing by introducing some countermeasure, when you're doing something else, you're moving to a different state of the vehicle, and you've got to understand what that new state, whatever it is." (Academic Research Expert)*

One respondent noted that if a vehicle was on the outer lane of a motorway and the hack was to open the windows to let rain in, a full minimum risk manoeuvre would not be practical. This is because:

- Other drivers may struggle to stop in time to avoid the vehicle, due to the nature of the road and the vehicle's position on the road.
- Whilst rain entering a vehicle may be slightly uncomfortable, this attack should not compromise the safety of the occupants or a safety driver's ability to drive a vehicle, whether or not under remote operation.

These findings suggest that whilst CAV developers are content with having set minimum risk manoeuvres within the vehicle, it is likely that hackers could use the information against the automated vehicle and their occupants, if they know that the same minimum risk manoeuvre could be used every time. This is aligned with the likely need to have minimum risk manoeuvre options to allow the automated driving system to select the safety and most appropriate option for the given environment.

5.1.5 How are you already evidencing management of these threats?

Although few of the respondents mentioned ways that they had seen cyber threats being managed during trials, three main mechanisms of evidencing management of cyber threats pre-trial were described. Many respondents noted that they could evidence management of these threats by showing that they had adhered to cyber standards:

> *"We follow the main standards, PAS 1885 but mostly it's the ISO 21434, so it's mostly against the ISO standard with a bit of a cross check against [PAS] 1885." (CAV developer)*

On the other hand, the use of employing a third party to assess cyber systems was also mentioned as another way to evidence how threats had been mitigated:

> *"Put it [the cyber system], you know, on a test systems that you have and attack it - the usual attacks. For us for client space depends on 3rd party. As I said, like Horiba, Mira or others to pen test, evaluate, do the risk assessments of that*

> *system"*

Other management of cyber threats include using operational based mitigations. These include risks assessments and training.

> *"So, prior to [trial name], prior to [name of business redacted] integration, it's been, mostly operationally based mitigations checklists,..controlling access where if we're on a public Road, we are checking things like software hashes and the likes before we run for the day and safety driver training." (CAV developer)*

5.1.6 Would any further structure/support make it easier for you to manage and demonstrate how you manage these threats?

Interviewees commented that having tools to assess suitable countermeasures for ease of development would assist in managing the threats observed. It appeared that having such available data would allow possible mitigations to be identified.

> *"I would automatically extract the things they [meaning the tools] need. They can sort them. Then I have some database of possible measures, I can map them and already automatically based on effectiveness of each measure for each threat it already knows…more or less can give me some reference by how much with this can be reduced[…]of course, then our part would be just to revise it." (Academic research Expert)*

One CAV developer commented that more regulations were required to fill in the gaps in the existing standards, though other CAV developers commented that sufficient standards or regulations already existed.

> *"I think that the more recent revisions of the DfT guidelines were beginning to open up to allow some remote operation type functionality as there's not as much information and guidelines as there is with the autonomous running systems."(CAV developer)*

> *"I think at the moment we're suffering a bit from standard mania in that every week there's a new one come comes out and it does create work for us. When we review them, then they're not actually adding anything over the standards that already exist." (CAV developer)*

The integration of security and safety would also assist in managing cyber-related threats, though it was noted that too much focus on security may be detrimental to managing safety threats. This was particularly noted from the academic researchers.

> *"Security problems can be solved with safety measures and vice versa, so we can help each other. Or sometimes they can conflict each other. For example sometimes we can try to secure something. So we put a lot of protections which*

> *slows down the system and from the safety point of view it has to, you know, perform fast and then we cause some safety problem because of securing the system too much."(Academic research)*

5.2 Expert stakeholders (group 2)

5.2.1 What are the biggest risks/concerns relating to ensuring vehicles (or telemetry/communications more generally) can be remotely operated without being vulnerable to cyber threats?

The findings for this question were mixed. The representative from the UK Government body's main concern was the security of the connection between the remote operator and the vehicle. Their concerns related to the 4G and 5G connection, which, as the literature revealed, is a significant attack vector.

> *"I think one of the main kind of issues with remote driven vehicles in general is, ..the type of connection established and the tech used to do this, whether it's 4G, 5G satellite link or something obviously has a big impact on the level of cyber security encryption you can use and also the latency of the connection. I think latency is probably, outside of cyber security, the biggest safety risk for remote driving." (Government Body)*

The insurer believed that the biggest threat was a potential cyber attack, which could come in the form of a denial of service attack or data theft.

> *"The biggest risk we've got at the minute as an insurer is a malicious Cyber Act. Of one description or another.. now that can move from hacking the vehicle and. Manipulating the vehicle to do something, denial of service and theft of data. (Insurer)*

Linked to this, another potential concern was the resilience and security by design of the connection.

> *"Are you actually using a VPN? You know, a VPN, VPN type connectivity, and the resilience. I think cyber resilience and you know, a system can never be totally secure….a good hacker will always.. get in." (Government body)*

5.2.2 What information would make you feel confident that cyber security had been addressed? (Group 2)

The stakeholders reported that an analysis of the remote operations system through penetration testing would increase their confidence in its cyber security. The use of a safety case was also noted. Other stakeholders also commented that any kind of cyber security system used should have resilience.

> *"Some sort of safety case or analysis of their kind of cyber security system, which is just a kind of standard thing we might ask or would like trialling organisations to have." (Government Body)*

The use of reliable third parties was felt to be advantageous, due to the independent assurance and confidence which they can provide.

> *"So the likes of [name of business redacted] who've got a technology background in communications and things like that, well supported in that, it's much more high profile. When it's a vehicle manufacturer coming to the table, they're pulling on third parties for this, and that might be your Googles, your Apples and people like that. And we saw the consequences of some of this in America, and you know, and it's the confidence." (Insurer)*

5.2.3 Have you already encountered these standards/cyber mitigations in this industry or more widely?

This question referred to the items described in the previous question. The stakeholders interviewed had not yet encountered any cyber security mitigations.

5.2.4 How are standards and regulations currently addressing cyber vulnerabilities, and are you aware of notable gaps?

The expert stakeholders interviewed had some awareness of standards. These include the PAS and UN regulations. Nonetheless, awareness of information available concerned with remote vehicles regulations was limited.

> *"I don't know if there are any UK ones, ones that's typically referred to is UN regs 155 and 156.Which are just kind of general cyber security regulations for all vehicle types, but are often used as a kind of standard or starting point and something that we're looking at is assessing whether they're fit for use or can be fully applied to fully automated vehicles." (Government Body)*

5.2.5 Where/with whom does the responsibility lie?

The findings for this question were mixed, with the stakeholders each holding different perspectives about where the responsibility for the vehicles cyber security should lie.

The insurer believed responsibility fell with the developer of the vehicle's cyber security systems.

> *"Developer of the systems… it's [AVs cyber] system protection all come with the support and guarantees and accountabilities from whomever is applying it. I wouldn't like to buy a car from BMW where the tires made by continental do not come with a guarantee of quality and safety about them." (Insurer)*

The local authority felt the trial operator was responsible.

> *"I think it still sits with the trialling organisation or in the future it will sit with the manufacturer." (Local Authority)*

The Government body asserted that the overall responsibility should be decided on a case-by-case basis.

> *"Again, I think the answer is the same. It would be done in a case by case basis, but that's again off the top of my head. The Law Commission paper will almost certainly address that as well." (Government Body)*

5.3 Overall themes

Five significant themes emerged from examining the responses to each question, collectively. These are discussed in more detail below.

5.3.1 Theme 1: Security by design

Several of the respondents noted that in order to ensure that the vehicle was secure, any system components would have to be designed to be secure as well (for example using a system that has appropriate authentication built in). Failing to do so would mean that the system would be much easier to hack into. It was implied that many component designers were creating the individual parts of the system to be functional, but not secure, suggesting that this is a current shortcoming of remotely operated automated vehicles.

5.3.2 Theme 2: Resilience of the software

Some respondents suggested that ensuring the resilience of the system was more important than ensuring that the system was secure by design. This was because it was noted that hackers would always be able to access a digital system, given enough time and effort. Resilience therefore is the ability to ensure that any cyber attacks can be averted (for example by using redundant communication systems that can be activated in response to a cyber attack on the main communication system) to reduce the severity rather than the likelihood of such attacks.

5.3.3 Theme 3: Safety vs security of the vehicle

Another problem noted was a trade-off in determining whether to focus on making the vehicle safe or secure. This was because a system which is fast is likely to make the vehicle systems far safer overall, due to the ability to make quicker decisions and avoid any collisions. However, in order to make the system secure, the system is typically slowed down by processes like encryption and decryption, authentication and challenge response systems. Therefore, developers of automated vehicles with remote operation need to ensure that an appropriate balance is struck in order to make the vehicle both safe and secure.

5.3.4 Theme 4: Implementation on a case by case basis

Several respondents noted that security measures should be implemented on a case by case basis. For example, many participants noted that the potential mitigations for a remotely operated automated vehicle would likely be different depending on what type of road the vehicle was on, or the type of cyber attack that was going to be used.

It is important to consider the hacker's goal with regards to any minimum risk manoeuvres carried out by the vehicle. For example, an intruder may want the vehicle to come to a stop. If they know that the vehicle will always come to a steady stop once a cyber attack is commenced, they may initiate a hack of the vehicle to ensure that their goal is met. Therefore, it is imperative that the goal of any hackers is anticipated, and several potential mitigations put in place.

5.3.5 Theme 5: Discrepancy between responses relating to standards

A final theme was the discrepancy in opinions surrounding regulations for AVs. Two of the CAV developers reported that they found additional standards helpful to know what they were meant to be doing, and how to make their AVs safer. This was not the view of all CAV developers however, with one respondent noting that the use of standards and regulations was onerous, and that that they were suffering from "standard mania" with new standards being rewritten, but not having any new content, suggesting that some CAV developers would prefer fewer concise standards. This may well be because different countries were all attempting to create their own standard, and had not tried to create a consistent standard across nations. On the other hand, it was also mentioned by the academic research expert that guidance, specifically with relation to cyber security was typically not up to the best standard, and should be improved to make AVs safer.

This discrepancy suggests that a new international system may be required, to streamline the process of new standards being developed, and to supersede any previous standards to avoid there being too many for developers to keep up with. However, as cyber security is a rapidly developing area, this new standard may have to be updated at regular intervals.

6 Discussion and safety case considerations

This section describes the overall findings of the literature review and the stakeholder engagement and provides some potential actions which could be taken to mitigate against cyber security threats.

The findings from the literature review identified three main mitigations which are most relevant to the remote operations of CAVs. These are:

- **Encryption of the data** which is shared between the CAV and the remote command centre.
- **Use of authentication** methods, including MAC, to further ensure that the communications between the command centre and remote CAV are authentic.
- **Intrusion detection systems**, used to safeguard the vehicle against attacks and to notify the remote operator of potential cyber attacks.

Based on the findings from the stakeholder engagement, we have identified several key areas to address for the cyber security of the proposed trial.

The mitigations identified from the stakeholder engagement included the following.

- **Using controls within the system** to make it harder for intruders to hack into the system / all the elements of the system by adding levels of safety.
- **Care needs to be taken when using set minimum risk manoeuvres** to allow the safety driver to take over control of the vehicle and reduce potential vulnerability to cyber attacks.

The analysis of the stakeholder engagement revealed five main themes, which spanned across all the interviewees.

- **Security by design**
- **Resilience of the software**
- **Balancing safety and security of the vehicle**
- **Implementation of mitigations on a case-by-case basis**
- **Discrepancy between responses relating to standards**

On this basis, the following actions should be considered in ensuring the cyber security for the remote operation of CAVs.

1. Mitigations should be used on a case-by-case basis and should be tailored towards the specific road environments of the trial and anticipated cyber attack vectors.
2. Minimum risk manoeuvres should be developed, to ensure the safety of both vehicle occupants and other road users and to ensure cyber security vulnerability is minimised.
3. Authentication methods and intrusion detection systems should be used, but such systems should be resilient and be designed to be secure from their conception.

7 References

Altawy R and Youssef AM (2016). Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Transactions on Cyber-Physical Systems, 1*(2), 1-25.

Antunes H (2014). Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. *IEEE Internet of Things Journal, Dartmouth.* Institute of Electrical and Electronics Engineers.

Bharati S, Podder P, Mondal R and Robel R (2020). Threats and Countermeasures of Cyber Security in Direct and Remote Vehicle Communication Systems. *arXiv*.

BSI (2018). *PAS 11281: 2018 Connected automotive ecosystems – Impact of Security on Safety – Code of practice.*, BSI Standards Institution, London, viewed 2021 Available from: https://shop.bsigroup.com/products/connected-automotive-ecosystems-impact-of-security-on-safety-code-of-practice/standard.

BSI (2018). *PAS 1885:2018, The fundamental principles of automotive cyber security – Specification.*, London, viewed 2021 Available from: https://shop.bsigroup.com/products/the-fundamental-principles-of-automotive-cyber-security-specification/standard.

BSI (2020). *BSI Connected and automated vehicles - Vocabulary BSI Flex 1890 v3.0:2020-10*. BSI Standards Limited: London.

Chowdhury A, Karmakar G, Kamruzzzaman J and Jolfraei A (2020). Attacks on Self-Driving Cars and their countermeasures: A survey. *IEEE Access*, 207308-207342.

Collingwood L (2017). Privacy implications and liability issues of autonomous vehicles. *Information & Communications Technology Law*, 32-45.

DfT (2017). *The key principles of vehicle cyber security for connected and automated vehicles.*, London, viewed 13 December 2021 Available from: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles.

DfT (2019). *Code of Practice: Automated vehicle trialling.*, London Available from: https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling.

El-Rewini Z, Sadatsharan K, Selvaraj D, Plathottam S and Ranganathan P (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications, 23*.

ETSI (2010). *TS 102 731 Technical Specification Intelligent Transport Systems (ITS); Security; Security Services and Architecture, V.1.1.1.*, viewed 2021 Available from: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf.

ETSI (2012). *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, V1.1.1.*, viewed 2021 Available from: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.01.01_60/ts_102940v010101p.pdf.

ETSI (2017). *Intelligent Transport Systems (ITS); Security; Security header and certificate formats.*, viewed 2021 Available from: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf.

Gudla C, Rana S and Sung A (2018). Defense Techniques Against Cyber Attacks. *Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications, Mississippi.* WorldComp.

Guevara L and Cheein F (2020). The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. *Sustainability*.

He Q, Meng X and Qu R (2017). Survey on cyber security of CAV. *2017 Forum on Cooperative Positioning and Service (CPGPS).*

He Q, Meng X and Qu R (2020). Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicle. *Journal of Advanced Transportation*.

Jafarnedjad S, Codeca L, Bronzi W, Frank R and Engel T (2015). A Car Hacking Experiment: When Connectivity meets Vulnerability. *IEEE globecom workshops.* IEEE.

Jafarnejad S, Codeca L, Bronzi W, Frank R and Engel T (2015). A car hacking experiment: When connectivity meet vulnerability. *2015 IEEE globecom workshops (GC Wkshps).*

Khan SK, Shiwakoti N, Stasinopoulos P and Chen Y (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention, 105837*, 148.

La Manna M, Trecozzi L, Perazzo P, Saponara S and Dini G (2021). Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update. *Sensors, 21*(2), 515.

Liu D (2009). *Next Generation SSH2 Implementation - Securing Data in Motion.*, Syngress.

Merco R, Pisu P and Biron Z (2018). Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control. *Annual American Control Conference (ACC).* IEEE.

Nakhila O, Dondyk E, Amjad M and Zou C (2015). User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols. *IEEE*.

Parkinson S, Ward P, Wilson K and Miller J (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE transactions on intelligent transportation systems, 18*(11), 2898-2915.

Patsakis C, Kleanthis D, Du Fuentes J, Casino F and Solanas A. External Monitoring Changes in Vehicle Hardware Profiles: Enhancing Automotive Cyber-Security. *ET Intelligent Transport Systems, 12*(9), 1103-1109.

Raiyn J (2018). data and cyber security in autonomous vehicle networks. *Transport and Telecommunication, 19*(4), 325-334.

Studnia I, Nicomette V, Alata E, Deswarte Y, Kaâniche M and Laarouchi Y (2013). Survey on security threats and protection mechanisms in embedded automotive networks. *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W).*

United Nations (2021). *UNECE Regulation 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.*, viewed 2021 Available from: https://unece.org/sites/default/files/2021-03/R155e.pdf.

Zenzic (2021). *Safety Case Framework: The Guidance edition*.

Zhang R, Song L, Han Z, Jiao B and Debbah M (2010). Physical layer security for two way relay communications with friendly jammers. *Global Telecommunications Conference (GLOBECOM 2010).* IEEE.

Appendix A Search terms used for the literature search

1st Level Search Terms		2ndlevel Search Terms		3rdlevel Search Terms
Connectivity, Autonomous, Driverless, Connected vehicles, Autono*, Remote, Controlled vehicle, Drones, Fleet management, Fleet monitoring	AND	Cyber-security, Cyber Human factors, Driver, Hack, Hacking	AND	Teleoperation, Remote operation, Hazards, Risks, Issues, Tele, Malicious, Security, Safety, Attack, Vehicle

Appendix B List of mitigations found in the literature search

Mitigation	Threats that the mitigation can avert
Acceptance range thresholds	Spoofing
Assigning IPs to vehicles and dropping duplicate IPs	Jamming
Audio Squeezing	Audio system attack
Central gateway-based architecture	Sensor attack
Configuration of system	Network attack
Correlating messages from neighbours	Spoofing
CV Guard	Denial of Service
Distance bounding protocols	Spoofing
Firewall	Physical attack, denial of service
Jamming defence	Jamming attack
Monitoring ID codes	Spoofing
Moving target defence	Eavesdropping, denial of service
Patch management	Network attack
Relying on more than one sensor type	Sensor attack
Update protocols regularly	Sensor attack, denial of service, physical attack
Using Multiple antennas with verification	Spoofing
Pop noise based general defence strategy	Audio system attack
Data management	Physical attack
Use of VPNs	Sensor attack
Encryption	Network attack, Eavesdropping attack, modification, Denial of Service, Spoofing, Jamming, Audio system attack, Physical attack, Sensor Attack
Authentication	Network attack, Eavesdropping attack, modification, Denial of Service, Spoofing, Jamming, Physical attack
Intrusion detection	Network attack, Eavesdropping attack, modification, Denial of Service, Spoofing, Jamming, Replay attack, Audio system attack, Sensor attack
Time based mitigations	Spoofing, Replay attack, Physical attack
Signal power-based mitigations	Spoofing, Physical attack

Review of cyber security best practices for inclusion in CAV safety cases

The introduction of remote operation has the potential to accelerate the development of driverless vehicles and make their safe deployment more viable. However, the wireless connections between vehicles and operators present new cyber security hazards that could be exploited by attackers.

This study identified best practices in cyber security so that they can be incorporated into safety cases for the future trials and deployments of Connected and Automated Vehicles (CAVs). Potential mitigations for cyber-attacks were drawn first from a review of the existing cyber literature, and subsequently from interviews with expert stakeholders.

The literature review suggested that the best cyber mitigations were intrusion detection, encryption of data, verifying the identity of all users and the use of minimum risk manoeuvres. The stakeholder engagement suggested that ensuring that any cyber-systems were secure by design and resilient to any attacks were the most important factors.

To ensure cyber security of remote operation of CAVs, this study highlighted several actions that should be considered. Though many cyber security techniques exist, it is best practice to implement cyber security mitigations on a case-by-case basis and, where possible, these systems (e.g. authentication methods) should be secure from their conception. Furthermore, minimum risk manoeuvres should be developed, to ensure the safety of both vehicle occupants and other road users.

TRL
Crowthorne House, Nine Mile Ride,
Wokingham, Berkshire, RG40 3GA,
United Kingdom
T: +44 (0) 1344 773131
F: +44 (0) 1344 770356
E: enquiries@trl.co.uk
W: www.trl.co.uk

ISSN 978-1-915227-06-5

ISBN 2514-9652

PPR1022