Project BeARCAT

Bas**e**lining, **A**utomation and **R**esponse for **CA**V **T**estbed Cyber Security

Work Package 1 Deliverable Report

Connected Vehicle & Infrastructure Security Assessment

Version 1.03

31st March 2020

Grant-funded by Innovate UK and CCAV

Project No. 133897 - © 2020 BeARCAT Project Partners

Page left intentional blank.

Executive Summary

Connected, software-based systems are a driver in advancing the technology of transportation systems. Advanced automated and autonomous vehicles, together with electrification, will help reduce congestion, accidents and emissions. Meanwhile, vehicle manufacturers see advanced technology as enhancing their products in a competitive market. However, as many decades of using home and enterprise computer systems have shown, connectivity allows a system to become a target for criminal intentions. Cyber-based threats to any system are a problem; in transportation, there is the added safety implication of dealing with moving vehicles and the passengers within.

For this report, the main BeARCAT (**B**as**e**lining, **A**utomation and **R**esponse for **CA**V **T**estbed Cyber Security) project partners are WMG at the University of Warwick, Cisco, and Telefonica, with support from Millbrook. In this report, subject matter experts have addressed connected vehicle and infrastructure security assessments. It is one of three work packages responding to an Innovate UK Connected and Autonomous Vehicle (CAV) cyber-security feasibility study. Each work package covers one of the three requirements of the study. This report addresses the measurement and maintenance of cyber resilience and identification of vulnerabilities, the second work package addresses the specifications of a physical test facility, while the third work package explores the business case.

This report discusses the technologies underpinning connected vehicular systems and cyber security threats to those technologies. It is a baseline for understanding the security implications of CAVs, and those of the communication systems that enable or enhance their operation. Cyber security is not a problem that is fully solvable because of the fundamental nature of computers, communications and software. Instead, the threat from attack is a problem to be reduced to an acceptable level of risk. The testing techniques to assess cyber threats and achieve risk reduction, thus enabling and improving cyber resilience, are discussed.

The connected transportation ecosystem is a large and complex super-system which must be assimilated by numerous stakeholders. Understanding and testing complex technologies can be aided by technology itself. Software tools, supporting systems and physical test facilities will be required to perform the threat assessment and cyber security testing of CAVs, and the roadside infrastructure, communications systems and cloud services with which the CAVs interact. Automation of testing will be essential as the testing task is substantial and CAVs will operate within a multiagent environment.

This report provides:

1. A discussion of the techniques required to systematically address cyber threats and reduce risks to improve the CAV ecosystem's resilience. This is framed within a CAV testing Security Framework, which can be used as the basis of a certification process.
2. It summarises the technologies used within the CAV ecosystem, with emphasis on the communication technologies used between CAV and cloud services, an important area of the ecosystem.

Cyber security incidents are inevitable. Real-world incidents have occurred, and researchers continue to find security issues with vehicular systems with regularity. A systematic response to

incidents and a meaningful security testing framework will be required throughout the lifecycle of CAVs and the supporting ecosystem.

Recommendations

- Future investment in a CAV security testbed would be beneficial to the UK's emerging CAV industry and ecosystem, and to the communications and cyber security domains. The investment would provide a foundation for world-leading research in CAV and communications security assessments, risk reduction and cyber resilience techniques.
- Communications infrastructure and cloud services are areas of the CAV industry that are identified as requiring focus for cyber security investment. There has been and continues to be, substantial interest in the cyber security issues related to in-vehicle and sensor systems. This continues to be important, however, the CAV communications and cloud services technologies would benefit from equal attention as they become increasingly part of the marketplace.
- Investment in the design and development of a CAV cyber testing Security Framework to benefit the UK's transport and communications CNIs.
- It is important to realise that C-V2X may yet become the global automotive connectivity standard and we need to prepare for that, with testing, evaluation and development of the standards.
- It is not certain how C-V2X will interact with DSRC, if at all, but further research is required in this area to establish the best way forward for the UK.
- A special focus should be given to the communication system required to support real-time V2V, which is unlikely to be C-V2X or DSRC in the near term.
- Certification of the cyber security testing process is required. Procedures based around ISO SAE 21434, which can be regarded as a superset of the UNECE CSMS, are likely to be embraced by vehicle manufacturers.

The several areas that would benefit from research investment to accelerate the adoption of a CAV and communications testing Security Framework are:

- Investment to research and develop the Security Framework for the CAV ecosystem.
- Investment in new software tooling to support, disseminate and keep relevant the framework.
- Investment to research and develop a CAV ecosystem security testing knowledge base as part of the framework.
- Investment to encourage stakeholders to engage and network to exchange information and resources on cyber security threats to the CAV ecosystem.

The UK is a leader in cyber, vehicle and communications technology and can provide, and does provide, centres of excellence in understanding, testing and countering threats. That skill base can be used to protect the CAV ecosystem, and aid the development of the UK CAV industry, and contribute to the overall UK cyber security expertise. This report provides the relevant stakeholders with the baseline information to fully develop an industry-relevant Security Framework. The overall goal of the Security Framework is to keep the cyber security risks in the CAV ecosystem to a residual level, maintaining CAV cyber resilience.

Table of Contents

Figures

Tables

1. Introduction

Communications and transport are two of the UK's 13 Critical National Infrastructures (CNIs). Vehicle connectivity, the connected car, is now common, with most manufacturers highlighting connectivity and the value-added services that it brings as a selling point. Communications methods including mobile, satellite, radio and Wi-Fi enabled vehicle connectivity. Mobile networks provide "Carrier Grade" security and include 3G, 4G and Long Term Evolution (LTE), plus 5G technology. Vehicles and vehicle users can now connect to remote services, however, as the decades of using traditional Information Technology (IT) systems have demonstrated, any connected system is a target for malicious intent via a cyber attack. This has already been proven to be true with real-world vehicle hacking incidents having taken place, and researchers have demonstrated the ability to compromise connected vehicles. This is a concern, not only from the security of the communications systems but also the safety of all road users and the general public.

Another area of technological growth within the transportation sector is the development of highly automated in-vehicle systems including Advanced Driver Assistance Systems (ADAS). Such systems can detect drivers drifting out of marked lanes on the roadway, provide cruise control that can steer a vehicle within a lane, or provide collision detection and avoidance. In the future, 'self-driving' vehicles should eventually allow journeys to be taken without human intervention. These *Connected Automated Vehicles* and *Connected and Autonomous Vehicles* (CAVs) are highly reliant on digital systems. This includes systems being used to aid vehicle control, whose internal operation rely upon increasingly complex algorithms and decision-making processes. A CAV is a Cyber-Physical System (CPS) and their kinetic nature has safety implications.

Knowing such systems may be subject to a cyber attack requires stakeholders to invest in techniques that can mitigate such a threat. This report examines the cyber security threats to the CAV ecosystem and how a CAV Cyber Test Facility (CTF) could be used to assess and mitigate those threats.

1.1. Report Objectives

This report presents the argument for a holistic *Security Framework* to address the long-term mitigation of the cyber security risks to the CAV ecosystem. The framework provides a model, or architecture, for cyber security and cyber resilience testing processes. The operation of the framework will be supported by a specialised testing facility and proving ground, the CTF, that can provide the support infrastructure and services necessary for the CAV ecosystem stakeholders to achieve the goal of minimising risk from potential cyber attack incidents.

This report does not present a final framework design; indeed, the rate of technological change means that any security framework or process evolves as technology changes. However, it does provide a strong foundation for a CAV security framework that can be built upon by the CAV industry to become a national working practice for CAV security testing.

This report was produced in response to the Innovate UK funding competition[1] to address feasibility studies in CAV cyber security. It addresses the requirement to "find ways to measure and maintain cyber-physical resilience and identify vulnerabilities" within the CAV ecosystem.

[1] https://apply-for-innovation-funding.service.gov.uk/competition/430/overview

1.2. Associated Reports

This report is one of three providing recommendations for addressing cyber security and cyber resilience in the CAV ecosystem. It has been written by the consortium on the BeARCAT Project (in alphabetical order) Cisco, Millbrook, Telefonica and WMG (University of Warwick). The two companion reports address the physical infrastructure requirements for the CTF, and the business case for CAV ecosystem security testing within the UK, see Figure 1.

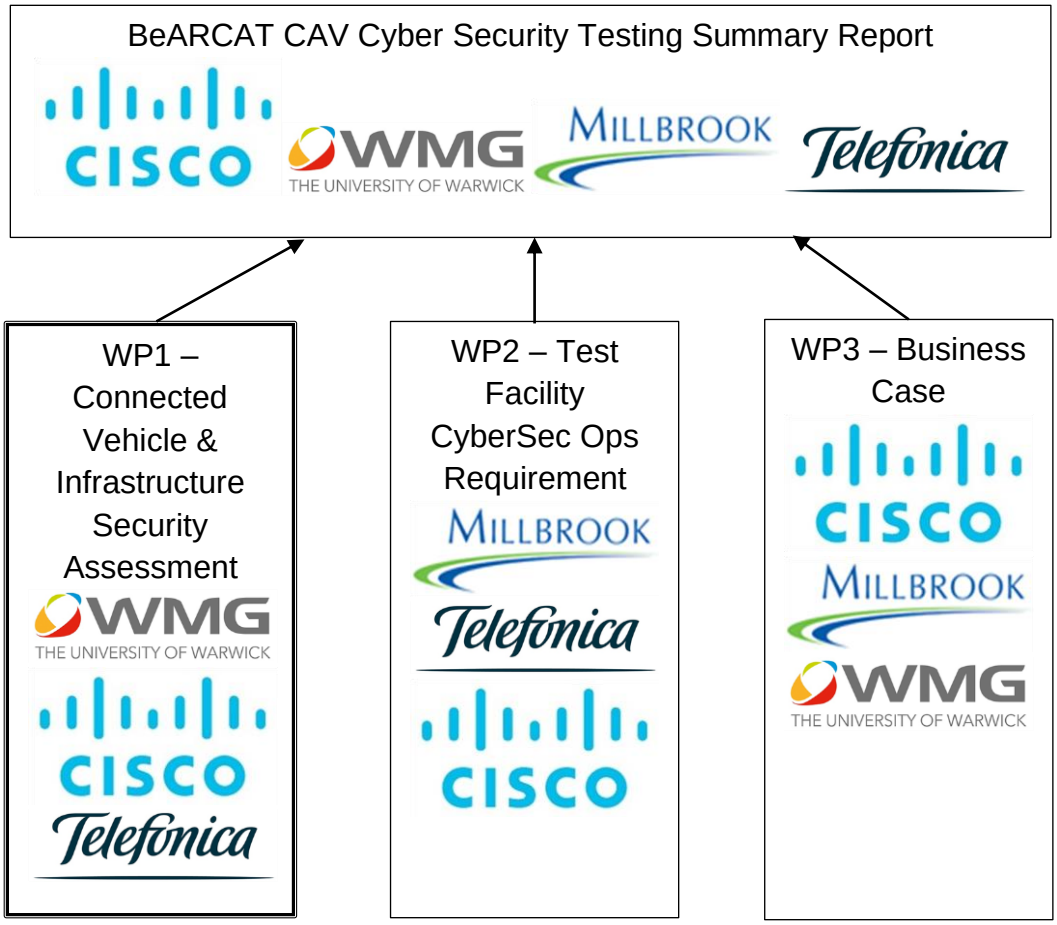


Figure 1. Work Package 1 (WP1) in relation to Project BeARCAT outputs

1.3. Stakeholders

The stakeholders are numerous as the CAV ecosystem crosses engineering and social domain boundaries:

- Vehicle original equipment manufacturers (OEMs)
- Vehicle retailers and service centres
- Mobile Network Operators (MNO)
- Mobile Virtual Network Operators (MVNO)
- Telecommunications service providers (business-to-business and business-to-consumer) and equipment manufacturers
- Information technology and cloud providers
- Roadway infrastructure providers and highway authorities
- Trade bodies and organisations
- Standards bodies

- Consumer device manufacturers and digital assistant operators
- Automotive component and tier suppliers

The CAV cyber security concerns for these organisational entities will vary, however, our connected society means that security issues have the potential to impact different points within the ecosystem. Cyber security concerns include:

- Mass or localised disruption to transportation and communications systems.
- Tracking and accessing vehicles.
- Tracking and endangering individuals.
- Covert surveillance and theft of data, audio, and video information.
- Cyber crime for financial gain, for example, using ransomware.
- Cyber vandalism by disaffected individuals.
- Protection of manufacturers' digital intellectual property (IP), including insider threats.

Specific challenges are facing the development and deployment of connected and automated vehicle systems. The design process for such systems typically takes multiple years, with the physical components of a vehicle being determined two to three years before the vehicle is 'in production'. Although there has been significant progress concerning the ability to update firmware and software within a vehicle, not all vehicle systems have this capability. Also, there are regulatory issues to such updates that, at the time of writing, are still be addressed. For example, a software update changing the operation of a vehicle to an extent that it may impact the vehicle's type approval, or insurance risk.

Vehicle system manufacturers are faced with an environment where cyber security threats and attacks continue to evolve, long after the components for a vehicle system have been finalised. Furthermore, the vehicle system manufacturer may be responsible for the cyber security of the vehicle for up to the lifetime of the vehicle (typically 10-15 years). This creates a situation whereby the effectiveness of the cyber security solutions that are deployed within a vehicle system degrade before the vehicle has started production and will continue throughout the vehicle's life.

For the above reasons, CNIs and CPSs must be designed and tested for cyber resilience, able to withstand, deflect and nullify cyber attacks and continue to operate securely and safely throughout the lifetime of the system. To achieve this, the various stakeholders within the communications and transportation ecosystem need to cooperate to ensure that they not only reduce the cyber security risks in their products, but they do not increase the risks to the products with which they interconnect. A vehicular cyber security test facility that provides a centre of excellence for combining physical testing capabilities with expert knowledge in vehicles, automotive systems, communications technology, cyber security and systems engineering will be a world-class and world-leading asset for the UK transport industry.

1.4. Report Contents

The report describes the technology that currently exists within the CAV ecosystem and how it can be impacted by cyber security incidents. It discusses many of the cyber security concepts within the current cyber security domain, and how they apply to CAVs, mobile networks, communications systems and infrastructure. The proposed security framework is described, beginning with the need to define an industry reference architecture that allows stakeholders to

understand the scope of the CAV ecosystem. The reference architecture enables different stakeholders to view any aspect of the CAV ecosystem, and from that view perform a cyber security threat analysis.

The threat analysis begins with threat modelling to determine the risks to systems, from end-to-end. There are many threat modelling techniques, with a few of the most used techniques being discussed within this report. Threat modelling allows for risks to be evaluated and ranked; again, different risk assessment techniques exist, and the most popular methods are reviewed. Once risks have been identified, they need to be mitigated within the designs of the system and its sub-assemblies. The systems then need to be subjected to testing, to ensure that the applied mitigation is enough to reduce the risk to a residual level.

The principle aim of this report is to address the need within the UK transportation ecosystem (and the wider global community) to develop a Security Framework, see section 2, for performing cyber security testing and assessment of CAVS and the supporting infrastructure. It specifically focuses on the communications subsystems within the vehicle and, importantly, the onward connectivity, via mobile networks, to infrastructure and cloud servers and services. Whilst the internal vehicular systems are equally important, there is already extensive research in that area, which is ongoing. However, extra-vehicular communication requires equal investment in security research and development (R&D) effort. This is due to the rapid growth in the use of cloud-based services for the CAV ecosystem and the development and adoption of future services such as Automated Vehicle fleet management. Mobile networks provide so-called “Carrier Grade security” and as such are of great interest for the V2X & V2I communication. To this end, recommendations are provided on developing a UK CAV Security Framework, including a discussion on certification requirements and the lifetime management of any constructed facility and the framework's maintenance, an important point due to the ever-changing technological landscape.

1.5. Report Challenges and Notes

The BeARCAT project feasibility study was run over a short time span, during the first three months of 2020. This period coincided with a worldwide coronavirus pandemic. The short project duration, and the impact of the pandemic, has not prevented the completion of the report. However, there may be areas that could benefit from further study, review and proof-reading.

The report studies the domain of cyber security. This term may be written as *cybersecurity*, which is common in the Americas and international standards and publications. In the text, the term cyber security is used which is common in UK documents, unless it is quoted from elsewhere, for example, the title of a referenced publication. Similarly, the phrase cyber attack is often hyphenated, but in this report, it follows cyber security and is not hyphenated.

The project partners acknowledge grant-funding by Innovate UK and CCAV, and for the opportunity to produce this report.

2. Overview of the Security Framework

Testing of any vehicle is a complex process, testing CAVs and their interactions will add to the complexity. On top of that, cyber security testing is challenging due to the need to look beyond the functional specifications of systems. To aid with the security testing challenge a framework is provided to help the stakeholders understand the various interactions within the security testing process. The high-level view of the framework is provided in Figure 2.

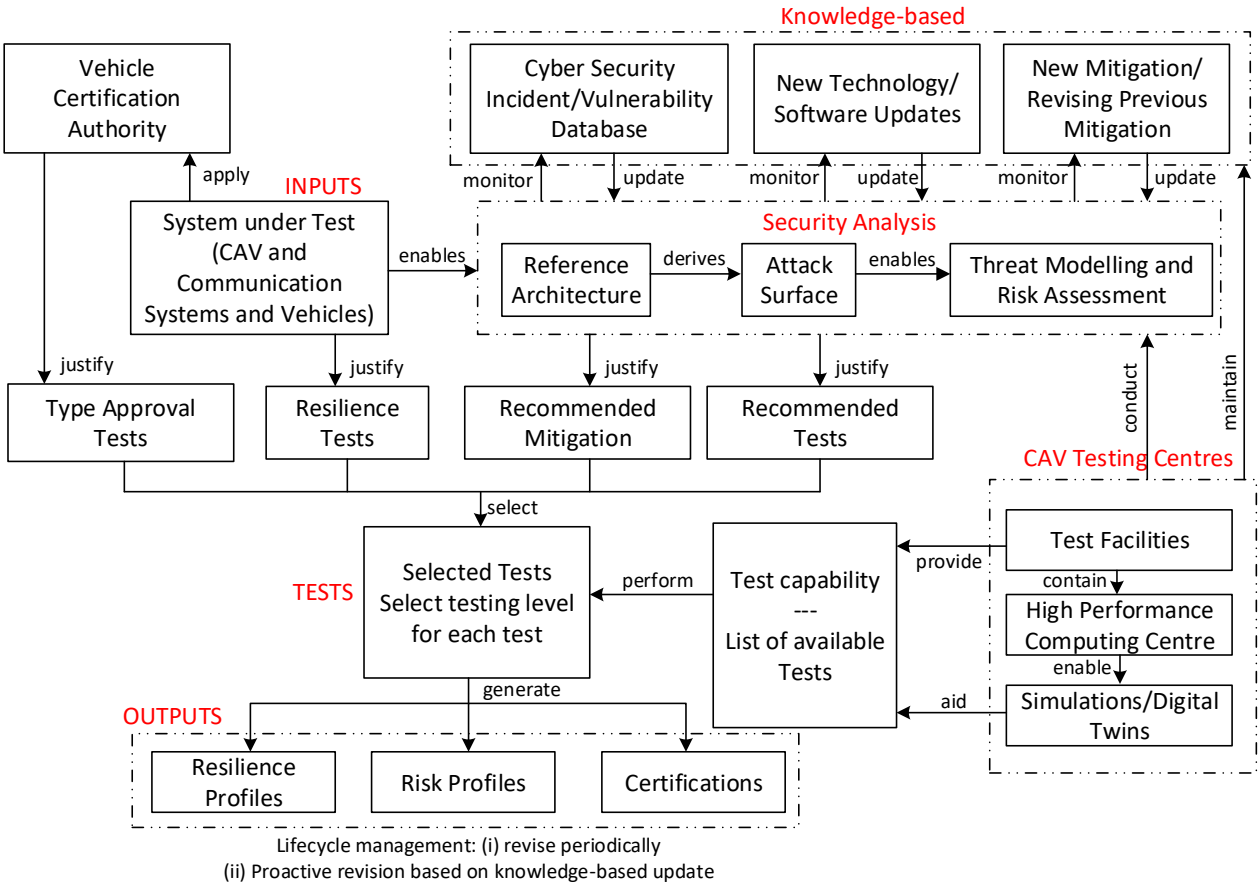


Figure 2. Holistic cyber security framework for CAV cyber test facility

The major sections of the framework are:

- ***Inputs****:* System Under Test (SUT) or Devices Under Test (DUT), CAVs and communication systems, even sub-systems and devices.
- ***Security Analysis****:* A systematic way of modelling the threats to a system and assessing the security risks, threat modelling and risk assessment, conducted by the testing centre is covered in this report.
- ***Knowledge****:* Technology and the threat landscape changes; the framework needs to account for changes. Testing centres should maintain knowledge of attacks, mitigation, and new technology, working nationally and internationally with other security professionals.
- ***Tests****:* The security tests to mitigate risks and determine system resilience, an overview of security testing is provided in this report. There will be many tests that are recommended from security analysis, mitigation analysis, certification guidance, resilience analysis;

however, the selection of tests will also be based on the capability of the testing centre, as well as the available time and resource.

- ***Test Centre****:* The testing happens at a physical location, the physical requirements and operation of a CTF are addressed in the Work Package 2 companion report. Testing centres will need to work with a national Vehicle Certification Authority, which already exists to coordinate and apply the current Type Approval process.
- ***Outputs****:* Certification against the tests (pass/fail) and profiles of risk and resilience. These feed into a systems *Lifecycle Management*, especially when a real-world incident requires a re-test and system update. For security, outputs are not one-time assessments but should be revised proactively and periodically upon updates to the knowledge record. There is an assumption of evolving threats (proactively testing) and normal system operational changes (periodically testing) when doing the assessments. Incident management must be handled through a CAV or systems lifecycle.

Using the above Security Framework overview, it is possible to see where the different sections of this report fit into the security testing map. This helps assimilate the amount of information provided on the various technical aspects of the CAV ecosystem, the communications infrastructure, and security testing methods provided in this report.

3. Definition of V2V, V2I, V2C and Similar

The CAV ecosystem has many interactions amongst entities. In this section, some of the terminology used for those interactions is discussed for those unfamiliar with the terms.

V2X communication connects vehicles to ‘everything’, which includes Vehicle-to-vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Cloud (V2C) and Vehicle-to-Pedestrian (V2P). Connectivity may be achieved using several different communications technologies and solutions, including by Dedicated Short Range Communications (DSRC) with the Intelligent Transport System 5 GHz Access Layer (ITS-G5), Cellular V2X (C-V2X), 3G/4G/5G mobile systems, and Wi-Fi technologies.

DSRC is an 802.11p-based vehicle wireless communication technology that enables highly secure, high-speed direct communication between vehicles and the surrounding infrastructure, without involving the mobile network infrastructure. It is the Institute of Electrical and Electronics Engineers (IEEE) specified standard for V2V and other forms of V2X communications.

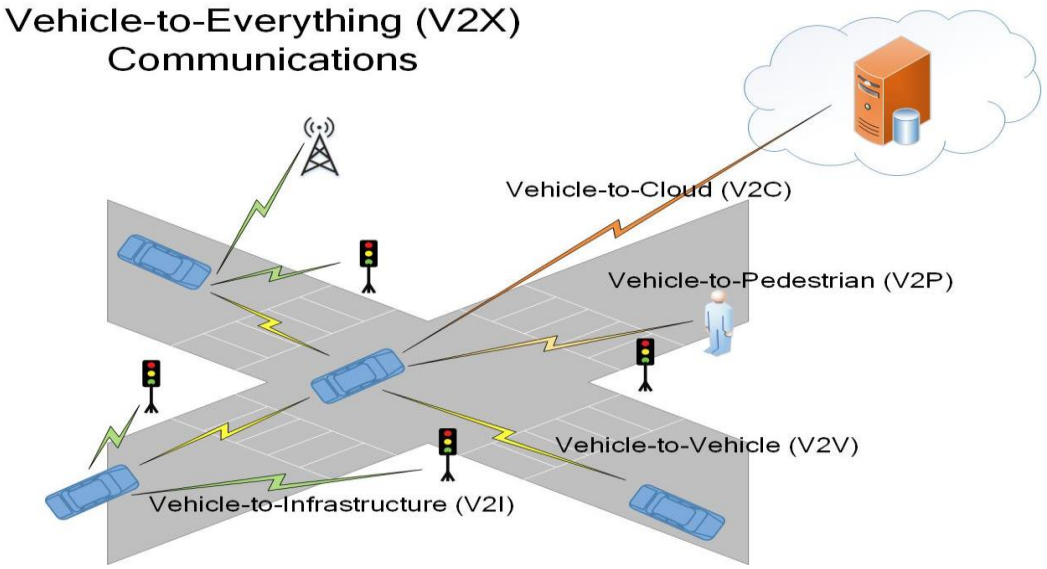


Figure 3. An architecture of V2X communications

3.1. V2V Communication

Direct communication between a vehicle and other vehicles to support safety-critical and latency-sensitive applications, exchanging information such as trajectory, speed, brake status and others sharing the road information. V2V communication uses DSRC/ITS-G5 or C-V2X (LTE direct) technology.

3.2. V2I Communication

Communication between a vehicle and an infrastructure/roadside unit (RSU) to support applications such as traffic management, transmitting messages for upcoming changes in road/traffic signs, traffic signal violations and congestion information. V2I communication typically uses DSRC/ITS-G5 or C-V2X technology.

3.3. V2C Communication

Communication between a vehicle and a cloud to support remotely hosted applications. Analysis based on the cloud can provide vehicle diagnostics, anomaly detection, firmware updates and security authentication as well as consumer-facing connected car services, such as connected infotainment and navigation, firmware updates and security authentication. V2C communication typically uses mobile communications technologies such as 3G, 4G/LTE and will include 5G in the future, more commonly known as C-V2X.

3.4. V2P Communication

Direct communication between a vehicle and a pedestrian to support pedestrian safety applications, enabling collision prediction, providing collision alert to driver, a pedestrian (though connected handheld devices) or both. The 'pedestrian' 'encompasses various vulnerable road users' including pedestrians, cyclists, wheelchair users and passengers embarking and disembarking buses and trains.

3.5. C-V2X Communication

The Mobile C-V2X is a 3rd Generation Partnership Project (3GPP) standard describing a technology to achieve the V2X requirements. C-V2X is an alternative to 802.11p. Pre-commercial C-V2X deployments have recently gained momentum with support from multiple automakers.

3.6. Examples of Use Cases for V2C

Vehicle telemetry can offer the manufacturer significant insights into the operational behaviour and performance of the vehicle, as well as the ability to understand their customer base in greater detail. The data may also open other business relationships such as vehicle insurance (own or partnered) and shared mobility services. Telemetry can reveal if the windscreen wipers are used, and if so, how often. It can reveal if functions within the vehicle are being used or not – which may then help the manufacturer to determine if they should continue to develop a feature or potentially withdraw it. In addition, to for some vehicle manufacturers, the collection of telemetry information combined with data from sensors such as cameras, is extremely valuable in providing 'training data' for Advanced Driver Assistance Services (ADAS) and systems that may offer forms of automated driving (SAE J3016 Levels 3, 4 & 5[2]) in the future.

While vehicle telemetry monitoring may appear to be a valuable service to the owner/user of the vehicle, the greatest value is perhaps to the vehicle manufacturer themselves in the ability to gather information from the vehicle fleet. This information has applications in vehicle manufacture and supply chain. This can be vital in helping manage the number of vehicles impacted by recall notices and the associated warranty costs. As the importance of electronics and software has grown, so has complexity, with some vehicles now having well over 100 million lines of code. Detecting and mitigating issues that may impact the vehicle fleet is vital to vehicle manufacturers.

[2] SAE (2018) Society of Automotive Engineers (SAE), 'SAE J3016-201806: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles'

In 2016, the United States had ~11.5 million trucks registered, with a growth rate of ~400,000 new trucks being added each year[3]. The total vehicle fleet accrued over 285,000 million miles travelled in one year. For industries such as freight haulage, vehicle telemetry is an increasingly valuable, an asset[4], helping to improve operating efficiency of vehicles and the safety of their drivers. Analysis of data including individual driving patterns and behaviour, traffic on routes and weather conditions can yield actionable insights that reduce time in transit and avoidable idle times.

More directly, a 2013 report identified that fuel represents 39 percent of the annual operating costs of the average truck in the United States with an average running cost of $180,000[5]. Reducing fuel usage and the across an entire vehicle fleet by as little as 2-3 percent can have significant financial benefits, as well as reducing environmental impact.

Vehicle fleet operators often gather their own telemetry, independent of vehicle manufacturers by incorporating their own sensors and communications equipment into their fleet of vehicles. Fleet operators' use of telemetry is a direct input into business operations, which can help drive efficiency improvements and profitability. For freight haulers, their vehicle fleet must spend most of their time in motion moving goods. Their areas of focus include:

- **Idle time**. Any time a vehicle isn't moving, such as when it's being unloaded, it costs money. If a vehicle misses its slot at a distribution centre and has to wait, time is lost along with profits. Even processes such as presenting identification and providing manifest information is an area for optimization. Data transmitted between the vehicle and the distribution centre can ensure that slots aren't missed, which leads to efficiency improvements on all sides.
- **Fuel costs**. Fuel is one of the primary costs for haulers. Saving even a small percentage can make a difference in profitability. Tracking issues such as headwinds and other weather events can lead to fuel savings. Using telemetry from their fleet, companies can make routing decisions to avoid bad weather, but it requires access to near-real-time information and processing capability.

It is useful to understand what information may be contained within the data collected from Connected Vehicles. There is of course a wide range of data that can be collected, and one must bear in mind that the breadth of data may also reflect the price-point of the vehicle (budget, mid-range, luxury).

The following example is taken from a luxury vehicle maker: vehicle telemetry includes information relating to the vehicle being involved in an accident such as the fact that the airbags have been deployed or the sensors have been activated. Further data includes the fuel amount, the distance to empty status, the odometer value, the distance to service status, the coolant level, the washer fluid level, the brake fluid status, the brake pad wear, the tyre pressure, tyre pressure sensor failure, engine malfunction, the oil level, the door and window status, if seatbelts are buckled or not, and information from any sensors, for example, in the

[3] https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/docs/safety/data-and-statistics/413361/fmcsa-pocket-guide-2018-final-508-compliant-1.pdf
[4] https://www.mckinsey.com/business-functions/operations/our-insights/ask-an-expert-capturing-fleet-impact-from-telematics
[5] https://www.thetruckersreport.com/infographics/cost-of-trucking/

car, on the steering wheel, or from camera information, including if the cab is open, boot open, bonnet open status, battery information including voltage, emissions information and whether the alarm is armed or sounding.

As more sensors are added to vehicles, not only will vehicle manufacturers gather information about the performance and operation of the vehicle itself but may also gather data generated from the sensors themselves. This does not mean that such data is gathered continuously but rather that vehicle systems may transmit a form of the sensor data in cases of 'interest' such as an accident or an unexpected set of telemetry data being recorded. Such information is of interest to not only the vehicle makers but potentially to organisations such as insurance companies.

As one can see from the information collection details, the manufacturers are collecting far more information than just fault conditions. The position and movement information can include details such as braking and acceleration styles. Traction-control indications can help determine road conditions at a location. Some vehicle makers and mapping service providers are starting to use such information to identify roadway hazards such as potholes.

When considering consumer-centric V2C applications, the most well-known are those providing in-car entertainment, or what is known as In-Vehicle Infotainment (IVI). As with other forms of consumer entertainment, the methods by which consumers access their entertainment has changed and will continue to change. Not that long ago, many cars were fitted with a CD player as part of the integrated car audio system. That is now relatively rare with that media being replaced by a USB port or a Bluetooth interface to enable the use of media streamed from a paired device. The IVI system unit continues to evolve, running a full operating system. Many include high-resolution touch-screen capabilities and an automotive navigation system. Some offer broadcast television receiving functions, more advanced solutions including the ability to run smartphone-like applications and connected to additional entertainment services, examples include Spotify and Netflix. These applications require communications connectivity to the infotainment service provider, which will mean, Internet access over a mobile network connection.

In the Automotive industry, a debate about the vehicle manufacturer's role in the infotainment value-chain is underway. One camp offers the position that the vehicle manufacturer has no real role to play anymore, 'disintermediation'. The car can be viewed as an advanced paired Bluetooth accessory, enabling the user to play media from a connected personal communications device with some infotainment systems offering connection solutions such as Apple Carplay and Android Auto. Further, that navigation services will be delivered to the connected personal device, doing away with the need to offer an integrated navigation service within the vehicle.

The alternative position suggests that the vehicle manufacturer can participate in the infotainment value-chain, offering a variety of integrated and connected experiences, with infotainment systems that include versions of applications such as Spotify and Google Maps. If the media is delivered via an integrated infotainment system, the dataflow is often from the infotainment service provider (such as Spotify) via the vehicle manufacturer's digital real estate, through the mobile service provider and on to the vehicle. In some cases, the data stream may be from the infotainment service provider through the mobile service provider and on to the vehicle.

When considering navigation services, one must consider that many integrated solutions retain map information on local storage within the vehicle (such as a flash drive). Periodic map updates may be provided to the vehicle over a mobile connection. ‘Layer information’ such as live traffic congestion updates and road construction notifications are received by the vehicle over the mobile communications network.

4. Threat Analysis, from Reference Architecture to Risk Mitigation

4.1. Introduction

With the continuously increasing use of software in vehicles, network connectivity to the outside world, and the variety of applications and services from the vehicle manufacturer and third-parties, security must be of primary concern. The attack surface is growing both inside and outside the vehicle, where it now extends to the end-to-end connectivity path, from the vehicle, through the various communications networks and on to the cloud and computing providers. Attacks against application servers now constitute the largest exploit, with recorded incidents at 25%, according to Upstream Security’s 2020 Global Automotive Cybersecurity Report[6], up from 21% in 2018. Attacks may not be against the vehicle manufacturer itself but instead targeting providers (telematics, navigation, infotainment) providing services on behalf of the vehicle manufacturer to the vehicle. A successful attack represents a highly impactful incident with the potential for considerable damage to the vehicle manufacturer’s reputation, magnified by the fact that the impact of the attack is not against one vehicle but rather the vehicle manufacturer’s vehicle fleet.

The emerging transport ecosystem sees vehicle connectivity, powertrain electrification and autonomous operation as the new paradigms. The CPSs that these emerging vehicles represent are enabled by two key technologies, software in embedded computers and communications. Vehicles have been increasingly reliant on computer technology for the last three decades, with various subsystems controlled by ECUs and increasing amounts of on-board computational capacity. With CAVs, those previously isolated computers now have wireless connections to the outside world. A connected computer becomes a target for various threat actors with malicious intent, from lone hackers, to criminals, to nation-state actors. Threats to connected systems are well established in the modern world, and the kinetic nature of transportation adds a further dimension, since it impacts upon the safety of the vehicle occupants, other road users and infrastructure. To maintain safety requires the consideration of cyber security in this new transportation era. This requires a new framework under which all the stakeholders in the industry can develop the processes needed to minimise risks.

The complexity of the emerging CAV ecosystem necessitates a common understanding amongst all the various stakeholders. This can be provided by a reference architecture (RA), an agreed description of the CAV ecosystem, summarising its various entities, subs-systems and inter-communication links. The RA is then used to map out the various attack surfaces within this system-of-systems. These aid a threat modelling process to determine the potential

[6] https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2020/

risks to the systems, and the mitigations that are required to reduce the risks to an acceptable level.

This section introduces the RA and its use as a starting point for threat modelling. Threat modelling approaches are then described. The outcome of threat modelling will provide risk mitigation measures, and a method to assess risks is given. Mitigation is addressed by implementing security measures, re-engineering systems (if required or possible), or making design changes. The mitigation will require various testing methods to be applied to ensure it has been correctly deployed.

4.2. A Reference Architecture as a Security Framework Foundation

An architectural diagram is useful for understanding the operation of any complex system. CAVs will operate within a transportation ecosystem, with different functions being provided by the various entities and actors. The ecosystem includes the road infrastructure, the vehicles travelling on the roads, traffic control systems, communication networks and operation management centres. The resulting complexity of CAVs, and the systems to which they connect, makes vehicular transportation a complex multi-agent system-of-systems, essentially a collective. The goal of the RA is to convey the complexity of this collective in an efficient manner to allow for assessment of cyber security issues.

4.2.1. Introduction to Reference Architectures

Architecture has moved beyond its original meaning to convey the design of a building. A complex system uses architecture to provide:

"The fundamental organisation of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution."[7]

The developers of the Unified Modelling Language (UML), Booch, Jacobson, and Rumbaugh, understood the importance of architectural diagrams for complex software projects. They made architecture a key aspect of their Rational Unified Process (RUP)[8]. When the Systems Modelling Language (SysML) extended UML to handle model-based systems engineering (MBSE), architecture was maintained as a fundamentally important concept and an essential part of systems engineering[9], going so far as defining an Architectural Framework to aid constructing architectures.

The military uses architecture as an aid to operational effectiveness and uses the Architecture Framework concept seen in SysML for architecture design. The United Kingdom's (UK) Ministry of Defence Architecture Framework (MODAF)[10] was developed

[7] ISO and IEC (2007) ISO/IEC 42010 IEEE Std 1471-2000 Systems and software engineering - Recommended practice for architectural description of software-intensive systems. New York
[8] Philippe Kruchten (2004) The Rational Unified Process: An Introduction. 3rd ed. Addison-Wesley, ISBN 0321197704
[9] Simon Perry (2013) SysML for Systems Engineering: A Model-Based Approach. 2nd ed. Computing. Institution of Engineering and Technology, ISBN 9781849196512
[10] https://www.gov.uk/guidance/mod-architecture-framework

from the US Department of Defense Architecture Framework (DoDAF) and aided the development of the NATO Architecture Framework (NAF).

SysML stresses the importance of conveying understanding. Architecture is a complete, but abstracted, representation of a system. It is a high-level model and a starting point for further detail. However, the stakeholders of a system, and the architects, must understand the model. The process of building the architectural model includes agreement on inherent concepts and terminology. The ontology of the architecture (the categories, properties and relationships of concepts and entities) reduces the risk of misunderstanding of system functionality.

Whilst architecture is often used during the design, construction and deployment of a system, it is also important for the ongoing evolution and future use of the system. It ensures the interoperability of new components and the management of system change. These factors are what makes an architecture a *reference architecture*[11], as such it needs to track system changes and reflect system operation, a process that can be covered in SysML by Life Cycles. The need for an architecture to reflect the ongoing use and design of the system is important when using it for cyber security threat modelling.

4.2.2. Reference Architecture to Identify a Target of Evaluation

The elicitation of cyber security risks, via attack surface analysis, is a goal when using a RA for cyber security testing of systems. CAVs, the systems with which they communicate and interact, and any other environmental considerations, are a system-of-systems transportation collective that will require adequate coverage from any threat modelling process. Ensuring adequate coverage is challenging due to the finite time and cost limits that exist for any system building and testing process. However, RAs can aid the systematic application of threat modelling, and thus, aids efficiency.

Early work at WMG, part of the University of Warwick, has defined a first iteration of a RA for the collective[12]. The high-level architecture schematic is shown in Figure 4 below. The RA must be designed to provide adequate information to quickly convey the overall operation of the collective. However, it does not provide the detail necessary to describe how the individual subsystems operate internally. That would be the domain of the subject matter experts. What it does provide is the ability to extract operational viewpoints on different aspects of the ecosystem.

[11] Robert Cloutier et al. (2010) 'The Concept of Reference Architectures', Systems Engineering 13.1, pp. 14–27. doi: 10.1002/sys.20129

[12] Maple, C., Bradbury, M., Le, A.T., and Ghirardello, K. (2019) 'A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis', Applied Sciences, 23, doi: 10.3390/app9235101

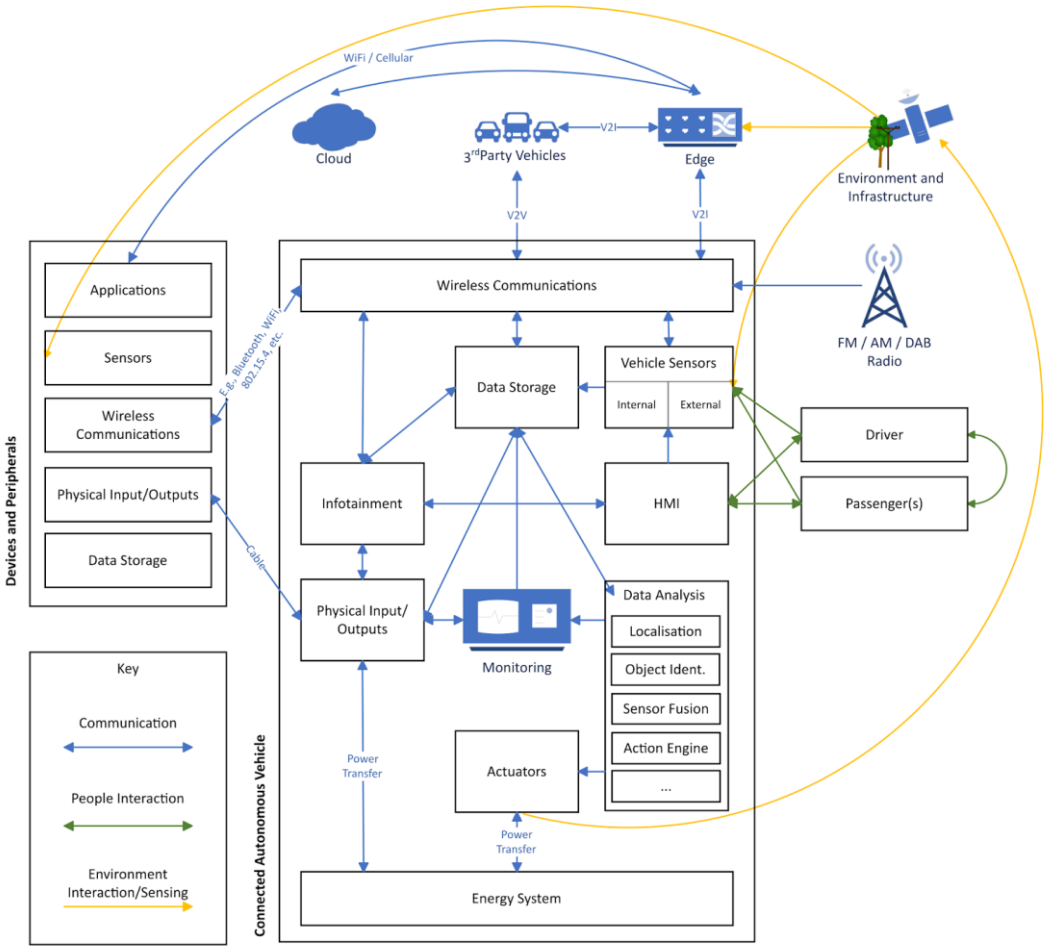


Figure 4. A reference architecture for CAV systems, their communications and environment

4.2.3. Views, Viewpoints and Perspectives

There will be multiple stakeholders in a system, each interested in a system function based upon their domain expertise. An engineer will require a different view of the architecture than a business manager. The former may use it to drill down into technical details, the latter may use it to understand costs. The two viewpoints are valid for their requirements.

A wide variety of views can be derived from a RA to meet different needs. An engineer may have more than one view of a system depending upon the area of system functionality in which they are interested. SysML uses the term Viewpoint to define the elements of the model that make up a View, with multiple views collectively forming a Perspective. Views can aid the decomposition of an architecture into its subsystems and components to allow focus on a set of functionalities. The system's architectural framework may define rules for viewpoints to ensure that views remain consistent and are complete models of extracted functionality. The use of views on the architecture in Figure 4 aid the subdividing of the system into functional and communication viewpoints, required for targeted threat modelling.

4.2.4. A CAV Ecosystem View

A security specialist performing a threat analysis on an aspect of the CAV ecosystem can develop an appropriate RA viewpoint as a starting point. The viewpoint allows a functional

use case to be extracted from the RA as a view to be used during a Threat Analysis and Risk Assessment (TARA) process when performing threat modelling (see Section 4.3). Figure 5 shows a cloud services view extracted from the RA. For the TARA process, this view allows focus on the particular use case under consideration. In this use case, the cloud services are used by vehicle occupants, or the vehicles themselves, to provide information-based services. For example, a vehicle occupant can receive details about a booked work job they are attending, or the vehicle can provide its perceived traffic information. The view provides the boundaries of the threat analysis. The communication links between the view entities, and the entities themselves, can be iterated to extract ToEs and begin the TARA process.

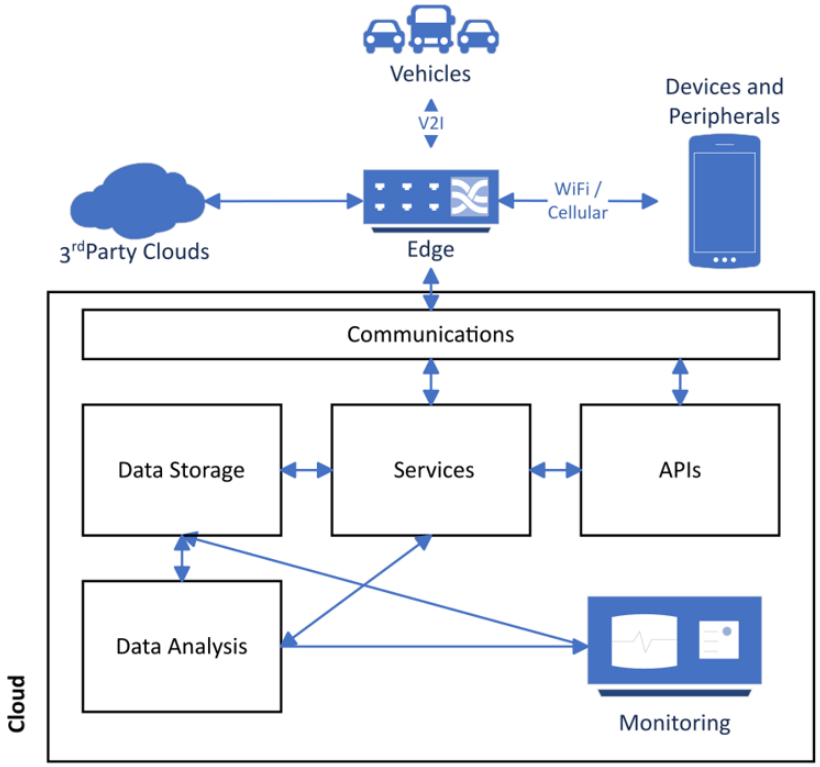


Figure 5. A cloud services view from the CAV ecosystem reference architecture

4.2.5. Tooling for Reference Architectures

The RA is not just a schematic of a system. It is a process designed to capture the key elements of a complex system. The high-level overview is supported by a documentation store to help the system's stakeholders obtain the required knowledge to understand the system operation. Tooling support is required to ensure that the RA is useful and not onerous. SysML, MBSE and other design tools can be used to aid the development, day-to-day use, and management of a RA. They should be *sharp* tools[9], they should not just be a diagramming package but contain features that aid the RA building process. For example, include rules that aid for consistency checks. A user should be able to define their own rules. For example, a Bluetooth communications path could only be established between entities that support the Bluetooth protocol. Other useful features will support the defining of viewpoints and extracting views.

4.2.6. Investing in a CAV Security Framework Reference Architecture

All connected devices need serious consideration of cyber security implications. CAVs are regarded as part of the Internet of Things (IoT) with their connectivity providing an attack point from threat agents. However, the CAV ecosystem is a complex system-of-systems with many stakeholders. It requires a systematic method to aid efficient analysis, risk management, and mitigation of cyber threats. This will be achieved by a security framework that has buy-in from all stakeholders.

The RA is the foundation of the security analysis, providing the stakeholders a common view from which the threat analysis work can be systematically derived. WMG's research into RAs is still at an early stage. The use of RAs for security analysis needs additional research to leverage the potential gains in efficiency in handling complex system-of-systems. Further investment in RA research will address several areas:

- The current RA needs further expert input to refine its design and ensure it matches the CAV ecosystem technology and communications.
- The notation used for the current schematic design should be translated into a machine compatible format. A notation such as SysML is a likely candidate. However, other notations may be desirable, though translations to other notations from SysML are possible.
- Tooling for RA defining and management, the tooling must allow for the defining of views for cyber security threat analysis. This tooling is required for CAV industry stakeholders. Investigations into the suitability of existing tooling, or the design of new tooling, is required.
- The reference architecture is not static. The technology and applications of the collective will change and evolve as society progresses. Thus, the reference architecture will need to change to maintain relevance, incorporating changes in technology and communications techniques. How this is best achieved amongst stakeholders will need consideration.

CAV ecosystem modelling can aid the development and deployment of the emerging new industry. The targeting of suitable investment provides the UK with an opportunity to be a leader in the design and application of a Security Framework within the industry.

4.3. Threat Modelling

As a part of a threat detection program, and to optimise a threat analysis and risk reduction operation for any system, it is recommended to use *threat modelling* for efficiency. This section reviews some approaches in threat modelling, in terms of both the overall threat analysis of a system to determine the possible threats, and the ranking of those threats via a risk assessment method. After looking at different TARA methods, their application to threat modelling within the automotive field is examined. It gives recommendations for selecting the most suitable techniques.

4.3.1. Introduction to Threat Modelling

Threat modelling can be used to qualitatively and quantitatively highlight the potential security risks to CAVs, the environment they operate within, the ITS systems with which

they interact, and the supporting communications infrastructure. Threat modelling defines security goals, identifies vulnerabilities, outlines defence plans and remediates security threats. It should be employed early in the system design process and development cycle to lead to proactive architectural decisions, providing the motivation and evidence to support those decisions[13].

System and vehicle development timescales place a finite limit on the time available for security testing for potential threats and existing known threats. Threat modelling can highlight where mitigation can be deployed to cover the most critical threats. Furthermore, the modelling will capture the security state of the system at a point in time, allowing comparison with a revised system once mitigation measures have been applied. This allows reports to be generated on the security improvements made.

A thorough threat modelling and risk assessment must be conducted to identify those critical threats. The modelling reduces the likelihood of threats taking advantage of potential system vulnerabilities. The CAV ecosystem has a variety of intertwined software technologies and physical infrastructures, involving a variety of stakeholders. Threat modelling can reduce the potential costs of rearchitecting, fixing and retrofitting a complex CPSs or communications system, by reducing the risk from an in-field security incident.

Threat modelling is an analysis process, which uses abstractions to categorise threats and aid in evaluating the risks[14]. The abstraction can learn from analogies and similarities to the known security issues reported from other types of systems; thereby help identify new threats which are difficult to detect by automated tools, e.g. static code analysis.

A reference architecture can aid threat modelling in eliciting and validating the attack paths required to achieve the attacker's goals[12]. The attack paths, or surface, and attack goals will be needed to assess the likelihood of a successful attack. There are several structured threat modelling techniques proposed in the literature, designed with specific objectives. The following sections provide an overview of some of the techniques.

4.3.2. STRIDE

STRIDE is a mature modelling approach to target threats in software development. Microsoft adopted this model in 2002 and has improved it to cover changes in the threat landscape. It is usable in various domains to evaluate the system design in detail by applying a set of well-known threats including **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, and **E**levation of Privilege, hence the name. These are the classifications of different techniques that threat agents can use to attack a system. STRIDE builds data-flow diagrams (DFDs) to identify system entities, events, and the boundaries of the system[13] [15]. Table 1 explains STRIDE's definitions and required security goals.

[13] Shevchenko, N. (2018) *Threat Modeling: 12 Available Methods.* Retrieved from Software Engineering Institute, Carengie Mellon University: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

[14] Shostack, A. (2014) 'Threat Modelling: Designing for Security', John Wiley & Sons

[15] Bodeau, D., McCollum, C., & Fox, D. (2018) Cyber Threat Modeling: Survey, Assessment, and Representative Framework. The MITRE Corporation, McLean, VA.

Table 1. STRIDE Threat Modelling

Threat	Property Violated (security requirement)	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be something or someone other than yourself.
Tampering	Integrity	Modifying data or code.	Modifying something on disk, memory, network, or elsewhere.
Repudiation	Non-repudiation	Claiming to have not performed an action.	Claiming that you didn't do something or were not responsible; can be honest or dishonest.
Information Disclosure	Confidentiality	Exposing information to someone not authorised to see it.	Providing information to someone not authorised to access it.
Denial of Service	Availability	Deny or degrade service to users.	Exhausting resources needed to provide service.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization.	Allowing someone to do something they are not authorised to do.

4.3.3. DREAD

DREAD is as qualitative risk assessment method once used, and created, by Microsoft. It provides an evaluation scheme to assess, score and prioritise threats that are identified by STRIDE, or other methods. DREAD enables the threat modelling to cover risk assessment[15]. The mnemonic comes from the five risk factors which are used to provide a comparative score for different threats:

DREAD Risk = (**D**amage + **R**eproducibility + **E**xploitability + **A**ffected Users + **D**iscoverability) / 5

DREAD provides a scale conversion to numerically assess the likelihood of specific threats. The sum of all the factors are normalised to represent the overall likelihood rating. Each threat will be scored on the five elements from 1 to 10, to provide a calculated risk of the severity and impact that can be used to rank threats, see Table 2.

Table 2. DREAD Risk Assessment Ratings

Damage Potential - how much damage that the threat can create	
0	Nothing
5	Information disclosure that could be used in combination with other vulnerabilities
7.5	Individual non sensitive user data is compromised
9	Administrative non sensitive data is compromised
10	Complete system or data destruction
10	Function unavailability
Reproducible - level of difficulty in reproducing the threat	
0	Very hard or impossible, even for administrators of the application
5	Complex steps are required
7.5	Easy steps are required
10	Easy with limited number of tools are required
Exploitability - level of difficulty in launching the threat	
2.5	Advanced programming and networking knowledge, with custom or advanced attack tools
5	Exploit exits in public, using available attack tools
9	An Application and Proxy tool is available
10	Very easy to exploit
Affected Users - number of users who are affected by the threat	
0	None
2.5	Individual user that is already compromised
5	Some users of individual privileges, but not all
7.5	Administrative users/systems
10	All users
Discoverability - level of difficulty in finding the vulnerability	
0	Very hard and requires source code, configuration or administrative access
5	Can figure it out by monitoring and manipulating requests and services
7.5	Details of faults like this can be easily discovered
10	The information is visible on the user or network side

As with other qualitative scores, subjectivity may be an issue and experience will improve its application. However, when applying to complex security analysis, the guidance is still vague, inconsistent, or debatable, which requires significant time and expertise to reach a reliable judgment. Common Vulnerability Scoring System (CVSS), described in see Section 4.5, is more practical than DREAD when applied to the vehicle security domain. The widespread use of CVSS has provided plenty of experience in its application to rankings of known vulnerabilities.

4.3.4. TARA from Intel

Threat Agent Risk Assessment (TARA) was published by Intel Corporation in 2009. Intel's TARA should not be confused with the common threat modelling TARA term (Threat Analysis and Risk Assessment), which applies to the whole threat modelling process and the methodology within the Security Framework.

Intel's TARA detects threat agents that may cause losses by evaluating greatest risks and likelihoods. This method is cross-referenced with existing vulnerabilities and controls to pinpoint the areas that are most exposed. The security strategy inherent in TARA then focuses on these areas to minimise efforts while maximizing effects.

Intel provided a library of threat agents to be used as the starting point to characterise threat agents. The Threat Agent Library (TAL) defines 22 archetypes, using eight key attributes or parameters: Intent, access, outcome, limits, resources, skill, objective, and visibility. Intel subsequently modified its list of key parameters to include motivation. In addition, Intel identified 10 elements of the motivation parameter (ideology, coercion, notoriety, personal satisfaction, organisational gain, personal financial gain, disgruntlement, accidental, dominance, and unpredictable), and modified its model so that each agent can have multiple motivations (defining motivation, co-motivation, subordinate motivation, binding motivation, and personal motivation)[15].

4.3.5. PASTA

Process for Attack Simulation and Threat Analysis (PASTA) developed in 2012 to combine both business objectives and technical requirements. A strategic risk-centric threat model with seven stages and multiple activities. PASTA involves operations, governance, architecture, and development security requirements. It employs an attacker-centric perspective to produce an asset-centric output in the form of threat enumeration and scoring[15].

4.3.6. VAST Modelling

Visual, Agile, and Simple Threat (VAST) modelling crates an application threat model that uses process-flow diagrams and an operational threat model, which is created from a data-flow diagram. It produces actionable and reliable results by recognising differences in operations. It is based on an automated threat modelling platform named *ThreatModeler*[16]. It is mostly used in the DevOps lifecycle[15].

[16] https://threatmodeler.com/

4.3.7. Attack Trees

Attack Trees describe attacks to a system in the form of a tree. The diagram starts from the tree root, which is the goal of the attack, followed by attack methods as the leaves. A complete system threat analysis creates several Attack Trees that demonstrate separated attack goals for each component of the system[13]. Attack Tree modelling is used for threat assessments of systems and CPSs. It can be applied in combination with other frameworks, including STRIDE and PASTA. Additional information on Attack Trees is in Section 4.6.4.

4.3.8. NIST SP 800-154 Draft

NIST has the draft the SP 800-154[17], which focuses on identifying and prioritising threats against specific types of data within systems in order to inform and assess approaches for securing the data, it is a data-centric system for threat modelling.

4.4. Threat Modelling in the Automotive Domain

Many threat modelling techniques apply to systems in general, and not specifically to the automotive domain. In SAE J3061 - *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*[2], the first widely referenced vehicle security guideline, it suggests a threat analysis and risk assessment approach using frameworks such as:

- EVITA – This came from the European **E**-safety **V**ehicle **I**ntrusion pro**T**ected **A**pplications project that ran from 2008 to 2011 and investigated protection of in-vehicle networks. It looked at security engineering, threats and security requirements[18]. The use of EVITA for risk assessment is further discussed in Section 4.6.1.
- OCTAVE – This came from Carnegie Mellon's Software Engineering Institute in 1999, **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation, used for identifying and managing information security risks. It defines an evaluation method that allows an organisation to identify the information assets that are important to the mission of the organisation, the threats to those assets, and the vulnerabilities that may expose those assets to the threats[19].
- HEAVENS – This came from the Swedish **HEA**ling **V**ulnerabilities to **EN**hance **S**oftware Security and Safety project that ran from 2013 to 2016. The goal was to identify security vulnerabilities in automotive systems. The resultant HEAVENS security model is a systematic approach (methods, processes and tool support) of deriving security requirements and to perform security testing and evaluation systems[20].

These frameworks are aimed at vehicular systems, and they contain four main functional processes:

[17] Souppaya, M., & Scarfone, K. (2016) 'Guide to data-centric system threat modeling', NIST Special Publication (SP) 800-154 (Draft). National Institute of Standards and Technology
[18] Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., … Pedroza, G. (2009) 'Security requirements for automotive on-board networks based on dark-side scenarios', EVITA deliverable 2.3
[19] Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999) 'Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0', Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA
[20] HEAVENS, Retrieved from: http://www.vinnova.se/sv/Resultat/Projekt/Effekta/HEAVENS-HEAling-Vulnerabilities-to-ENhance-Software-Security-and-Safety/

- Asset analysis
- Threat identification
- Threat classification
- Risk assessment

A mapping consideration between the processes and the core functions are provided in Figure 6.

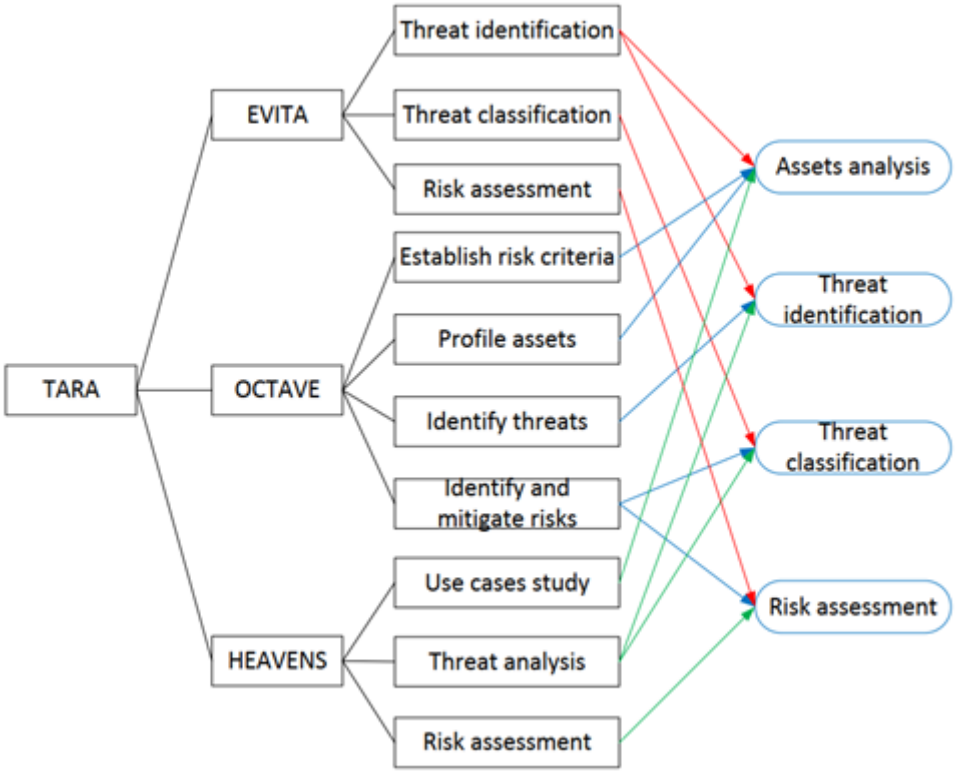


Figure 6. Main functions of common threat modelling methodology[21]

There are several attempts to improve the TARA to match the context of autonomous driving such as follows:

DAS-TARA[21]: TARA for Driving Automation System that considers the levels of automation when considering the risks and countermeasures applied in the driving functions. The method proposed to consider explicitly the Dynamic Driving Tasks, which are detailed in SAE J3016[2], rather than the general driving functions of the conventional cars.

TARA+[22]: extends the impact assessments through incorporating the attack controllability by the automated driving system or by the driver.

The practices of applying these approaches, combined with some of the methods from the previous Section 4.3, for identifying the CAV security threats are summarised in Table 3.

[21] Cui, J., and Sabaliauskaite, G. (2017) 'On the alignment of safety and security for autonomous vehicles', IARIA CYBER, Barcelona, Spain

[22] Bolovinou, A., Atmaca, U., Sheik, A.T., Ur-Rehman, O., Wallraf, G., and Amditis, A. (2019) 'TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems'

Table 3. Commonly used threat modelling methods in vehicle security projects

Model	Description	Applicable
CIA	A classical model to consider security in the aspects of confidentiality, integrity and availability	Medium
STRIDE	Microsoft threat model to categorise attacks by purposes	High (used in several vehicle security projects)
DREAD	Microsoft model to rank the risk of threats	Medium
OCTAVE	Consider threats on three aspects: security practices, technology, and operational risk.	Medium (it is too complex to apply in the context of vehicles)
EVITA	Qualitatively assesses the impact of threats and provides a ranking to risks.	High (often cited in automotive security research)
HEAVENS	A system to identify risk to automotive system.	High (coordinated by Volvo)
TVRA	ETSI threat model to analyse the emerging Intelligent Transport System architecture	High

For addressing the potential threats toward CAVs, under a proposed Security Frame (see Figure 2) within a cyber security centre, the following steps can be applied:

1. Identifying the CAV communication components and assets via a reference architecture.
2. Applying STRIDE to analyse the potential threats to the components and assets.
3. Desktop research (review the knowledge base and known literature) to find evidence of the potential threats and their relevant risks.
4. Check the vulnerability databases to see more detailed assessments of the threats.

A CAV's complex operation is controlled by interconnected computers, or Electronic Control Units (ECUs). Several in-vehicle networks (IVNs) allow ECUs to operate in functional domains to exchange data[23], see Figure 7. A gateway ECU allows data to flow between functional areas, for example when engine revolutions are displayed on an interior tachometer. The number of ECUs, IVNs and their functionality will vary between vehicles.

Different ECUs may deliver wireless communications to a connected vehicle, they include a Telematics Box (T-Box) or Telematics Control Unit (TCU), In-Vehicle Infotainment (IVI) system, separate Radio or Bluetooth receivers, systems Telematics Service Provider such as fleet management systems, mobile applications, as well as other types of ECUs, such as insurance monitoring.

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

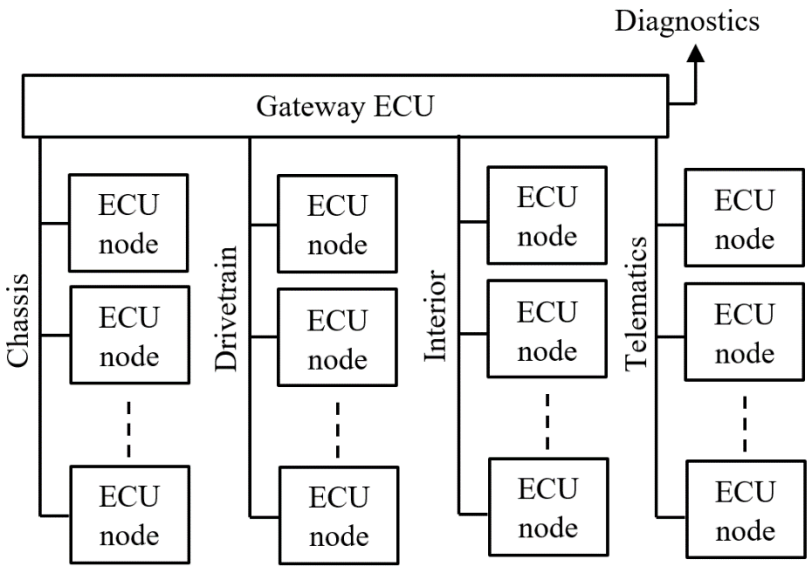


Figure 7. In-vehicle networks interconnect various vehicle ECUs

How ECUs and IVNs are design will vary by manufacturer. Some may combine different functions into one unit to reduce component cost, for example combine a gateway ECU with a T-Box and even incorporating an IVI. Once the communications components are identified (step 1) the threats towards the system can be identified and reviewed. Here providing examples under a high-level STRIDE analysis. In these examples not every STRIDE category applies.

4.4.1. Telematics Box

The T-Box is responsible for the remote communications between the vehicle and the cloud platform communications networks. T-Box devices can be electronic units which integrate communication chip functions required for access to communications networks. This includes the 3G/4G, Bluetooth, Wi-Fi wireless module, microcontroller (MCU) or System on a Chip (SoC), the GNSS receivers and other functionality. Commands from telematics service providers or smartphone apps can be transferred through T-Box devices to remote control the CAV to open the doors, stop the engine, or other physical functions[24]. Some of the T-Boxes allow the vehicle to be tracked in real-time using satellite constellations to deliver functions such as planning the optimal route or anti-theft[24].

Applying STRIDE for Telematics Box:

- ***Spoofing****:* Malicious firmware can be installed if the attacker can enter the uboot universal asynchronous receiver-transmitter (UART) debug interface in the T-Box hardware layer[28]. Attackers can also use wireless access to connect to the vehicle, as was the case in the famous Jeep attack[25].
- ***Tampering****:* Researchers[26] used a side-channel attack which tampers the embedded block random access memories (BRAMs) which store the Advanced Encryption

[24] Li, Y., Luo, Q., Liu, J., Guo, H., and Kato, N. (2019) 'TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions', IEEE Wireless Communications, 2019, 26, (3), pp. 125-131
[25] Miller, C., and Valasek, C. (2015) 'Remote exploitation of an unaltered passenger vehicle', Black Hat USA
[26] Aldaya, A.C., Sarmiento, A.J.C., and Sánchez-Solano, S. (2016) 'AES T-Box tampering attack', Journal of Cryptographic Engineering

Standard (AES) keys of the T-Boxes. Others[27] showed techniques to reverse-engineering the T-Box firmware to recover the Next Generation Telematics Patterns (NGTP) protocol and the encryption/signature algorithms. Consequently, they can send NGTP messages via SMS to trigger the Remote Service. They can then send remote code execution to provision an update and send messages onto the CAN Bus.

- ***Information disclosure****:* The attackers can eavesdrop the communication through T-BOX by using techniques such as pseudo base stations and DNS hijacking[28]. The real-time tracking function once compromised can expose users' privacy[24].
- ***Denial of Service****:* attackers can overwhelm the T-Box to disrupt remote connections which rely on it.
- ***Elevation of Privilege****:* XSS attack can be used when the users access the malicious websites which contain malicious scripts that can control their browsers. The compromised scripts can allow attackers to bypass authentications, therefore have rights to access private information or manipulate users' data[24]. Authentication maybe simplified for the high mobility and short transmission distance of the connected cars. This makes other techniques to bypass T-Box authentication possible, including brute force and authentication spoofing.

Suggestions for testing T-Box[29]:

- penetration tests to test the security services such as debugging and data output interface, start-up verification, secret key management, operating system security, OTA upgrade.
- using vulnerability scanner, source code analysis, firmware reverse scanning to scan the relevant information of security issues regarding the tested T-Box.
- using network simulations to study the potential impacts when attacks happen.

4.4.2. In-Vehicle Infotainment (IVI)

The IVI delivers the multimedia, application and navigation services to the passengers via the car's information system via different interfaces such as voice command, touchscreen input, or physical controls. Users' smartphone can also be connected to the IVI[30]. The IVI system can use communication protocols such as 3G, 4G, RF (Radio Frequency) antennas to connect to the servers, normally via the T-Box.

Threats in IVI

- ***Spoofing attack****:* Attackers can mislead the driver's destination by spoofing the surrounding GPS signals[31]. Malicious signals can be injected into the vehicle via the mobile network and lead to acquiring the control of vehicle brakes and other critical

[27] Cai, Z., Wang, A., Zhang, W., Gruffke, M., and Schweppe, H. (2019) '0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars', Black Hat USA
[28] Wang, Z., Wang, Y., Zhang, Y., Liu, Y., Ma, C., and Wang, H. (2019) 'A Brief Survey on Cyber Security Attack Entrances and Protection Strategies of Intelligent Connected Vehicle', Springer International Publishing
[29] Shao, X., Dong, C., and Dong, L. (2019) 'Research on Detection and Evaluation Technology of Cybersecurity in Intelligent and Connected Vehicle', pp. 413-416
[30] Zhang, Y., Han, S., Zhong, S., Shi, P., and Shao, X. (2019) 'Research on Information Security Test Evaluation Method Based on Intelligent Connected Vehicle', Springer International Publishing
[31] 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

systems[25]. The Tyre Pressure Monitoring System (TPMS) uses the 315 MHz or 433 MHz band frequency which are vulnerable from jamming and falsification attacks. When such attacks happen, the TPMS system can trigger false warning messages on the IVI which can disrupt the driver[31].

- ***Information Disclosure**:* Attackers can eavesdrop users' private information such as GPS; data from the in-cabin microphone which is used for hand-free calling; or other data that connected through the IRC channel[32].
- ***Denial of Service**:* Jamming attacks can be used to disrupt the IVI functions[31], for example preventing in-vehicle apps from communication to cloud services.
- ***Elevation of Privilege**:* There is a known vulnerability of the MirrorLink protocol for integrating a smartphone to an automotive infotainment system[33]. In detail, attackers can control the driver's smartphone and send malicious messages into the in-vehicle network through the IVI system. Besides that, researchers[34] show a method to compromise the IVI system via a fake WiFi connection to redirect the traffic to a malicious domain for installing compromised firmware. The compromised firmware later allows the attackers to control the vehicle remotely. Researchers[35] have demonstrated injection of malicious code into a genuine Android app to provide a backdoor, which allows the attacker to access the infotainment remotely to record sounds inside the vehicle and collect information circulating on the CAN bus.

4.4.3. Radio

The radio surface refers to the communications through radio waves, including mobile, Wi-Fi and Bluetooth communications, TPMS, or Remote Keyless Entry System (RKMS) that leverage radio communications.

- ***Spoofing**:* Attackers can send spoofing signals to the vehicle claiming that they are a serving edge node[36]. If the vehicle connects to the rogue edge node, there will be high risk of privacy leakage and other consequence attacks such as man-in-the-middle or DoS.
- ***DoS**:* Researchers[37] show that a compromised vehicle can send malicious messages, which spoof its trajectory data (speed and location), to the Intelligent Traffic Signal System to malfunction its congestion control.
- ***Elevation of Privilege**:* according to the Armis security lab[38], an attack called BlueBorne which exploits the vulnerability of Bluetooth can take complete control over

[32] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., and Kohno, T. (2011) 'Comprehensive experimental analyses of automotive attack surfaces'
[33] Mazloom, S., Rezaeirad, M., Hunter, A., and McCoy, D. (2016) 'A security analysis of an in-vehicle infotainment and app platform'
[34] Nie, S., Liu, L., and Du, Y. (2017) 'Free-fall: Hacking tesla from wireless to CAN bus', Briefing, Black Hat USA
[35] Costantino, G., Marra, A.L., Martinelli, F., and Matteucci, I.: 'CANDY: A Social Engineering Attack to Leak Information from Infotainment System', 2018
[36] Lu, X., Wan, X., Xiao, L., Tang, Y., and Zhuang, W. (2018) 'Learning-Based Rogue Edge Detection in VANETs with Ambient Radio Signals'
[37] Chen, Q.A., Yin, Y., Feng, Y., Mao, Z.M., and Liu, H.X. (2018) 'Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control'
[38] The Attack Vector 'BlueBorne' Exposes Almost Every Connected Device, https://www.armis.com/blueborne/

targeted devices without requiring the targeted device to be paired, or even to be set on discoverable mode.

4.4.4. Telematics Service Provider (TSP)

- ***Elevation of Privilege****:* Researchers[39] found that the CVE 2014-4113 vulnerability regarding the Session Example servlet, which used by TSP Cloud Platform, can be exploited by the attacker to gain the administrator right in a session.

4.4.5. Electronic Control Unit (ECU)

- ***Elevation of Privilege***: Researchers[39] showed that malicious code can be injected into Bluetooth cable devices to manipulate the in-vehicle systems.

4.4.6. Mobile Application (Mobile App)

- ***Denial of Service****:* In a car sharing app it was possible to upload an unlimited number of pictures, flooding a server[39].
- ***Elevation of Privilege***: In car sharing apps and a car manufacturer's diagnostic app researchers[39] found it was possible to modify the app code to leak user account information.

4.5. CVSS Scoring of Vulnerabilities

When, as part of a security assessment, vulnerabilities are identified, it is useful to score them. This enables the vulnerabilities to be directly compared to each other, as well as ranked for purposes such as remediation.

CVSS, the Common Vulnerability Scoring System, is a security industry de-facto standard way of quantitatively grading vulnerabilities or security issues. At a high level, each vulnerability ends up with a score between zero and ten, with ten being the most severe. This final value is calculated by assessing various attributes or properties of the vulnerability, including (in version 3):

- The attack vector (local or remote)
- The attack complexity (low to high)
- The privileges required to perform the attack
- Whether the attack requires a user to interact with the system
- Whether the attack grants the attacker additional scope for further exploitation
- How the attack affects the confidentiality of the system
- How the attack affects the integrity of the system
- How the attack affects the availability of the system

These individual metrics are then tallied to result in the final 0 to 10 score. It should be noted that CVSS does not make a provision for safety as a factor, however with CVSS v3.1 extensions framework[40] would permit safety to be added as a factor if this was deemed necessary.

[39] Yan, W. (2015) 'A two-year survey on security challenges in automotive threat landscape'
[40] FIRST, 'CVSS User Guide' https://www.first.org/cvss/user-guide

4.5.1. Worked Example

For the given use case of V2C telematics, let us consider that an attacker can unplug an exposed connector inside a vehicle, disconnecting the antenna used to transmit and receive mobile data. This means that the vehicle cannot send or receive telematics data.

This attack (whilst simple) could be useful in several real-world scenarios. For example, a car thief may disconnect this antenna in order to prevent telematics from reporting a stolen vehicle's location. This could also be a boon to privacy, allowing a legitimate end user to physically prevent their vehicle from 'phoning home' with data about the user's behaviour.

Qualitatively, the attack requires physical access to the vehicle, but no technical expertise or skill, with no privileged access to any systems. It results in a denial of service for any vehicle functionality which relies on mobile data (including telemetry).

The CVSS v3 score is obtained as:

AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

This is shown in the CVSS calculator Figure 8.

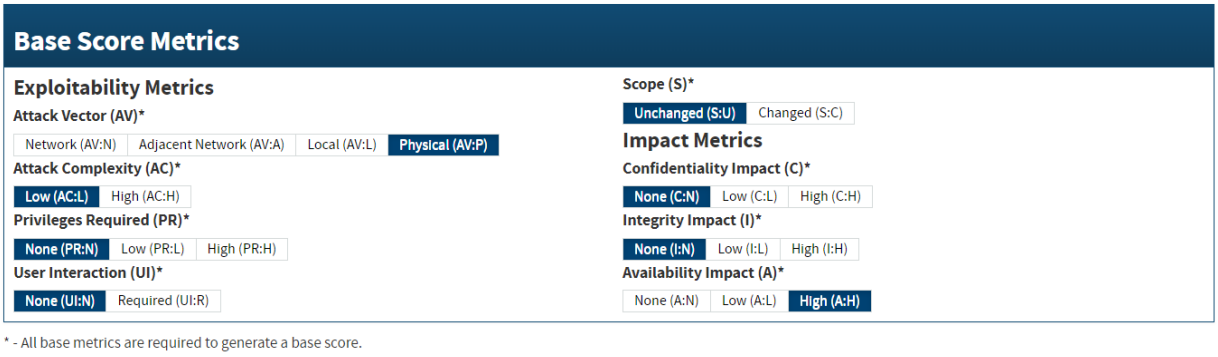


Figure 8. NVD's CVSSv3 calculator

This results in an overall CVSSv3 score of 4.6. The full workings for this final score can be tried on a CVSS calculator[41].

4.6. Assessing and Managing Cyber Security Risks

Risk assessment is the process of evaluating the risks to rank or categorise the threats. The main approaches in risk assessment include quantitative, qualitative, or hybrid (combination between quantitative and qualitative). For the vehicle security domain, the qualitative approach is suggested in several standards, best practices, and guidelines, for example J3061[12] and ISO/SAE 21434[42]. The quantitative approaches may be industry specific and difficult to implement for embedded systems, as with OCTAVE; therefore, they have been used less within the automotive field.

[41] NIST, CVSS Calculator, https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
[42] ISO and SAE (2020) Road vehicles – Cybersecurity engineering (ISO SAE DIS 21434). Geneva

Risk assessment consists of two separate parts: assessing threat likelihood and assessing threat impacts. The overall risk evaluation of a threat will be obtained only after understanding the probability that this threat will happen (likelihood) and how much damage it can create to the system. Details of these two processes are presented in the following sections.

4.6.1. Threat Likelihood

Threat likelihood assessments consider how easy it is to attack a system. Firstly, the requirements that need to be met in order to launch an attack successfully need to be considered. The threat becomes feasible only when the attackers have acquired the capability to launch it. Therefore, the requirements to launch the attack is also called 'attacker capability'. Secondly, the assessment process needs to understand the defender's capability, which is the available mitigations inside the system to defend against the attack. The final evaluation of threat likelihood will be obtained after comparing between the attacker and defender capabilities.

Common threat likelihood assessment rankings use EVITA (see Section 4.4), DREAD (see Section 4.3), CVSS (see Section 4.5), each of which decompose the attacker capability into different factors for easier evaluation.

In the EVITA framework the attacker capability can be assessed through the following five factors:

- **Elapsed Time**: the total amount of time taken by an attacker to identify that a potential vulnerability may exist, to develop an attack method and to sustain the effort required mounting the attack.
- **Specialist Expertise**: This refers to the required level of knowledge of the underlying principles, product types or attack methods.
- **Knowledge of the system under investigation**: This refers to specific expertise in relation to the system under investigation.
- **Window of opportunity**: This has a relationship to the Elapsed Time factor. Identification and exploitation of vulnerability may require considerable amounts of access to a system that may increase the likelihood of detection of the attack. Some attack methods may require considerable preparation, and only brief access to the target to exploit. Access may also need to be continuous or over a number of sessions.
- **IT hardware/software or other equipment**: This refers to the equipment required to identify and exploit the vulnerability.

A detailed evaluation for enumerating the attacker capabilities is given in Table 4. The overall numerical value is calculated by summing the values of all the five factors. The threat likelihood can be accessed by converting the attacker capabilities through a conversion table, which is given in Table 4.

Table 4. EVITA enumeration of attacker capabilities

Factor	Level	Comments	Value
Elapsed time	< 1 day		0
	1 day – 1 week		1
	1 week – 1 month		4
	1 month – 3 months		10
	3 – 6 months		19
	Unidentified	The attack is not exploitable within a timescale that would be useful for the attackers	∞
Expertise	Layman	No special security knowledge	0
	Proficiency	Familiar with security	3
	Expert	Mastering security in one or a few relevant fields	6
	Many experts	Collaboration of experts from multidisciplinary	8
Knowledge	Public	Easy to access	0
	Restricted	Confident within a company	3
	Sensitive	Known between a developing team	7
	Critical	Known between few individuals	11
Opportunities	Unnecessary	Do not need windows of opportunities	0
	Easy	(<1 day) & (number of assets < 10)	1
	Moderate	(1 day to 1 month) or (number of assets is between 10 and 100)	4
	Difficult	(More than 1 month) or (number of assets > 100)	10
	None	Window of opportunities is negligible	∞
Equipment	Standard	Already available for the attackers	0
	Specialised	Not available but easy to get	4
	Bespoke	Expensive and not available	7
	Multi-bespoke	Different types of bespoke are needed	9

4.6.2. Threat Impacts

The impacts of a threat represent the harm that this threat can create to the targeted system. Threat impacts can be considered in the four following EVITA perspectives:

- **Safety:** the safety harm (e.g. injuries) that a threat causes to the human involved in the transportation system.
- **Privacy:** the attack can cause leakage of sensitive information, which can be information about the operations of a vehicle, information from the passengers' data, or the data from accessing (online) services.
- **Financial:** the attack can cause financial losses to the vehicle itself and to other relevant on-road properties.
- **Operational:** the attack can cause interference to the vehicle operations or downgrade its performance.

Table 5 presents a numerical assessment of threat impacts regarding these four perspectives. This table has been cited heavily in vehicle cyber security risk assessment work, for example when assessing OBD security issues[43]. The impacts are related not only on the threats, but also to the operational scenarios. Therefore, when assessing the impacts of threats towards a targeted vehicle or component, it is important to clarify the working scenarios for these entities (which may include how the entities work, what are the relevant assets, what is in the surrounding environment, and other factors).

[43] Klinedinst, D., & King, C. (2016) On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=453871

Table 5. EVITA severity classification

Impact Level	Safety	Privacy	Financial	Operational
0	No injuries	Undisclosed or non-linkable data	No loss	No impact on vehicle performance
1	Single light to moderate injury	One identified vehicle	Low-level loss (< £10)	One small impact on a vehicle
2	Single severe injury or multiple moderate injuries	One vehicle tracking or identification of multiple vehicles	Moderate loss for a single vehicle (between £10 and £100; or Low losses for multiple vehicles	One big impact or many small impacts
3	A single life-threatening injury or multiple severe injuries	Multiple vehicle tracking	Heavy loss (≈ £1000); or moderate losses for multiple vehicles	Big impact on many vehicles
4	Life threatening or fatal injuries for multiple vehicles	Driver or vehicle tracking for multiple vehicles	Heavy losses for multiple vehicles	Significant impact for multiple vehicles

4.6.3. Risk Assessment Rating

The risk rating can be considered as a function of the threat likelihood and its impact. For qualitative approaches, the risk rating can be obtained through a lookup table. This allows a statement of the subjectivity of the impact to be turned into a numerical value. Furthermore, when assessing the impact of a threat, it could adversely affect the safe use of a CPS. The CAV security literature differentiates the impacts of safety from the privacy, operational and financial factors (see Table 5) because safety may endanger human life. Therefore, safety is of higher criticality in comparison with other factors. As a result, the impact of safety is often considered to be more severe than those of the other perspectives. Table 6 and Table 7 give examples of a lookup that can be used to derive the risk assessment ranking from the threat likelihood (ranked 1 to 5), and the safety or non-safety impact (ranked 1 to 4).

Table 6. Conversion to risk rating given the non-safety threat impact and likelihood

Non-safety impact level	Threat likelihood				
	1	**2**	**3**	**4**	**5**
1	0	0	1	2	3
2	0	1	2	3	4
3	1	2	3	4	5
4	2	3	4	5	6

Table 7. Conversion to risk rating given the safety threat impact and likelihood

Safety impact level	Threat likelihood				
	1	**2**	**3**	**4**	**5**
1	2	3	4	5	6
2	3	4	5	6	7
3	4	5	6	7	7+
4	5	6	7	7+	7+

4.6.4. Risk Management

Analysis of the threats to a system, vehicle or communication channel may identify many feasible attacks. Testing on all the *known* threats does not necessarily reveal the complete security posture of the tested system. For example, out of 100 test cases, system A passes 90, while system B only passes 80 threats. If A fails on some of the threat tests that B passes, it is difficult to conclude that system A is more secure than B. Therefore, what is more important is to understand the risks behind the threats. It is also important to emphasise that rather than show that the system is free from certain threats, the purpose of testing is to justify:

- the risks that have been eliminated (via a re-engineering);
- the risks that have been mitigated (reducing the risk's rating);
- the risks that are remaining.

An effective method to manage the relations between threats and risks is via the use of Attack Trees[13], see Section 4.3.7. They aim to address all possible elements that an attack needs in order to be launched successfully. The analysis focuses on drawing a logical 'tree' for each attack. Each tree has a root node which represents the final goal of the attack. The leaves of the tree are the logical steps that attackers need to achieve before reaching the root. The parent node and child node of a tree can relate to each other by either 'OR' or 'AND' conditions. In an 'OR' relationship, the parent node is true if any of the child nodes is true. On the other hand, in an 'AND' relationship, all the child nodes need to be achieved in order for the parent to be successful. Other system fault analysis such as ETA (event tree analysis), FTA (fault tree analysis), and FMEA (Failure Mode Effect Analysis) have similar structure and can be easily converted to Attack Trees. Both quantitative and qualitative risk assessment techniques can be applied in Attack Tree analysis. Much research has applied Attack Tree methodologies to assessing vehicle security risk, for example in the EVITA project[18].

The key idea of using an Attack Tree to manage the threats is to structure the attack surface by the potential threat agents and their goals to compromise the system. Based on the attackers' goals, the defenders will need to investigate the attack surface to find all the possibilities of manipulations to achieve the goal. The attack surface is restructured as multiple Attack Trees, each tree includes one goal as the tree root and multiple tree leaves, which are sub-goal and activities that are essential to reach the main goal. Instead of a bottom-up strategy which tries to test every possible threat to assess the security posture, the defenders now use a top-down approach which focuses on the most relevant risks (justified from the threat agent analysis) to derive the tests which are necessary. The top-down approach can create a list of tests which are more relevant and more understandable in terms of justifying the risks.

Another advantage of Attack Tree as a method is the capability of reusing the analysis work. For example, when considering a new risk, the defenders can break it into multiple sub-goals, some of which may already be analysed in other Attack Trees. In such cases, the tree can be built more quickly by retaking the previous analysis for the known branches.

Attack Trees can be employed to synthesise, manage, and control the attack surface. The process to perform the Attack Tree analysis is illustrated in Figure 9. The tree starts with the attack goals, which can be derived from attackers' motivations and stakeholders' security requirements. It then goes to the child nodes which represent the attacked functions or sub-goals that need to satisfy the attack goal. The attack surfaces and detailed knowledge of the attacks (i.e. STRIDE modelling) will be structured based on the attacked functions.

Evaluation of threat agents appears on both ends of the Attack Tree. In one end, threat agents influence the attack goals. It is assumed that threat agents will consider only goals that suit their needs. For example, a thief will be motivated by stealing the physical assets more than creating damage, while a hacktivist is more likely to find ways to manipulate the system rather than to inflict harm to it. On the other hand, each threat will require a certain

technique, skills, knowledge, equipment etc. to be implemented. Therefore, at the other end of the tree, the capability of threat agents needs to be evaluated to see whether the goal is feasible.

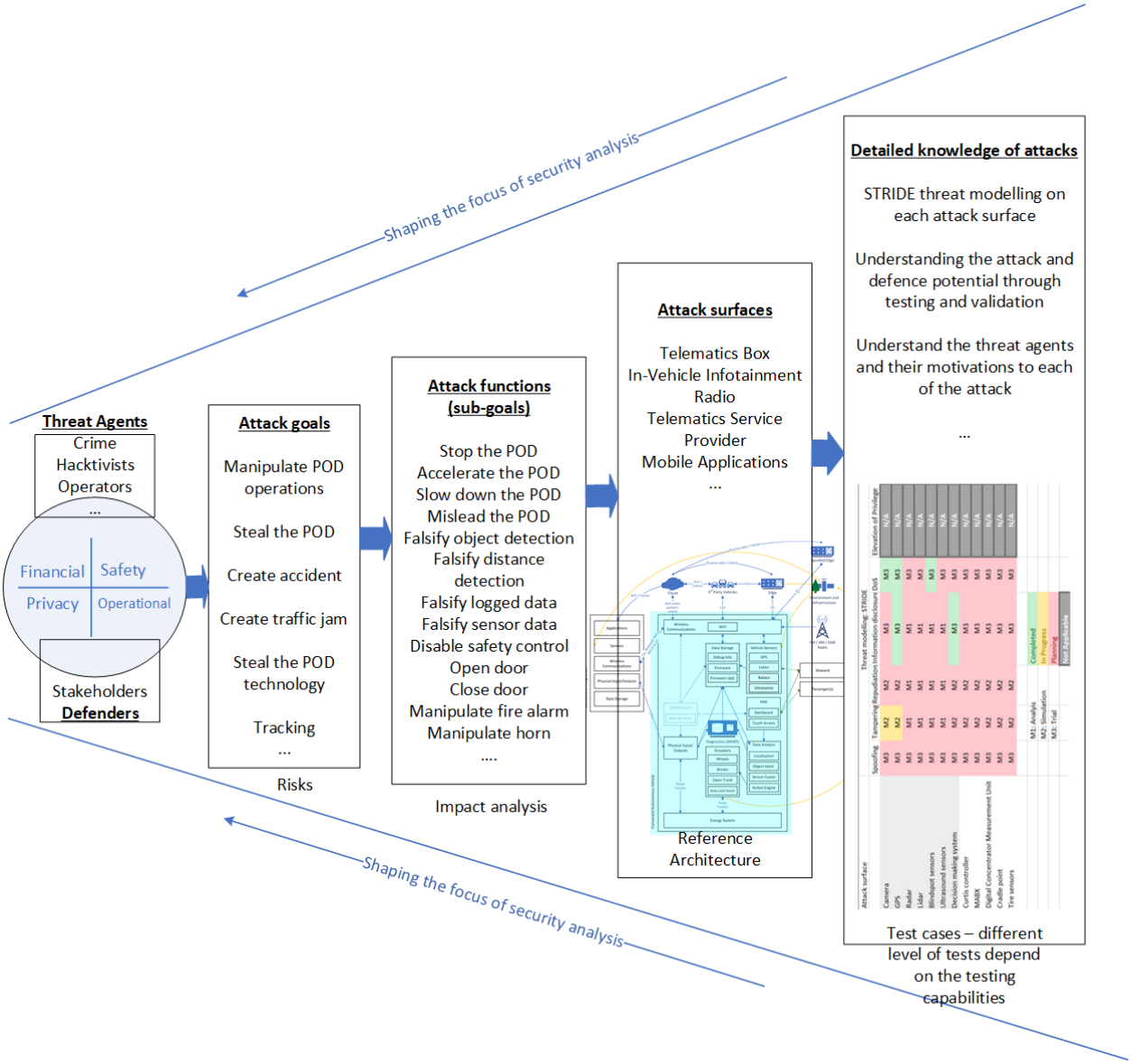


Figure 9. A threat management strategy based on Attack Trees

4.7. Mitigation

Mitigation for cyber attacks can be categorised under two main types, authentication across boundary domains (including encryption of data) as the first line of defence to prevent unauthorised access, and secondly intrusion detection as the second line of defence to monitor abnormal behaviours once the attackers get in the system. However, mitigation applying for each attack and risk can be varied as they can affect the operation of the assets which need to be protected. For example, encryption algorithms applied in the CAN network should be light weight with low delay given the limited memory and computing power of the ECUs; while encryptions in other networks could be more sophisticated to strengthen the defence. As a result, it is important to keep up to date with the reported mitigation towards specific attacks and risks. There are also attacks which aim at breaking certain mitigation, for example, the side-channel attacks such as power analysis aiming at exposing the encryption key. If this kind

of attack is successful, the targeted mitigation can become invalid. Therefore, it is essential to update the strength and weakness of each mitigation when applying to the security system.

Table 8 synthesises the common security controls for mitigating the attacks in the vehicle's communication[44] [45] [46]. These controls are categorised based on the targeted components, while the 'x' marks their effectiveness to STRIDE threats. This table can be used to find suitable mitigation for threats or risks targeting components.

Table 8. Countermeasures applied in vehicle communication, derived from multiple sources

Components	Countermeasures	S	T	R	I	D	E
Telematics gateway, a.k.a. T-Box	Detection of fake mobile networks	x	x	x	x	x	
	Secure boot process		x				
	Debug port authentication	x	x				
	Over the air software updates		x		x	x	
	Memory randomisation to protect buffer overflow		x				x
	IDS and IPS	x	x	x	x	x	x
	Data encryption to secure client-server communications from the T-Box to the cloud services				x		
	Trust anchor for external communications	x	x	x	x		
	SMS authentication	x					
	Hardening hardware security	x	x	x	x	x	x
Mobile network operator	SMS firewall		x		x	x	x
	Secure SIM data	x	x	x	x		
Telematics service provider	Encrypted communication		x		x		
	Adherence to security standards (ISO 27001)	x	x	x	x	x	x
	Mutual authentication for all client communications	x					
ECUs/CAN bus/OBD	OBD hardware covering	x					x
	CAN bus firewall	x	x			x	x

[44] Oyler, A., and Saiedian, H. (2016) 'Security in automotive telematics: a survey of threats and risk mitigation strategies to counter the existing and emerging attack vectors', Security and Communication Networks, 9, (17), pp. 4330-4340
[45] Graubart, R.D., McQuaid, R., and Woodill, J. (2019) 'Cyber Resiliency Metrics and Scoring in Practice'
[46] ENISA (2019) 'ENISA good practices for security of Smart Cars'

	Message authentication codes	x	x				
	ECU key management	x	x	x	x	x	x
	CAN bus anomaly detection network monitor	x	x	x	x	x	x
	Validate source of messages and suppress invalid messages	x		x		x	x
	Attestation functions for ECUs	x	x	x	x	x	x
	Digital signing for ECU updates: require OEM digital signature for updating ECU firmware	x	x	x	x	x	x
	OBD lock either physical or logical to prevent unauthenticated CAN bus access via OBD	x	x	x	x		x
	Centralised authentication	x	x				
In-vehicle infotainment/ Radio	Digital signatures for applications	x	x	x			
	Embedded virtualization	x	x		x	x	x
	Wi-Fi password policy	x	x		x		
	Wi-Fi security compliance with NIST guidelines	x	x		x	x	x
	Bluetooth security compliance with NIST guidelines	x	x		x	x	x
	USB security compliance with best practices		x				x
	Recovery by design						x
	Bug bounties	x	x	x	x	x	x
	Periodic refresh of the Infotainment system			x	x		x
	Validate infotainment system	x	x	x	x		x
	Multi-Factor Authentication to strengthen the authentication of door lock, e.g. PIN entry on the IVI to counter key fob relay attacks		x				x

It is important to consider how much security of the system is improved after applying mitigation, and how to choose the mitigation effectively given the limited security resource that a system has. Attack Trees can be used to tackle these issues. The main idea is to build an Attack Tree for each of the potential risks and assess whether the root of the tree can still be reached with the available mitigation. For example, mitigation which can prevent any leaf of an ‘AND’ Attack Tree is enough to eliminate the risk corresponds to this tree, while the ’OR’ Attack Tree will require mitigation for all the leaves in the tree. The effectiveness of a mitigation should be

considered given all the Attack Trees within the security scope of the system rather than for just a single threat. There are also automation tools (e.g. isograph[47]) for Attack Trees which can speed up the analysis for selecting the effective mitigation.

Besides specific mitigation, there are other general mitigation strategies which employ system design to reduce the impacts of the attacks. The testing procedure also needs to revise the design of the target systems following these strategies for recommendations. The potential strategies include (but not limited to):

- Applying the principle of least privilege: the principle is about limiting the (access) rights of every program or application programming interface to only what is needed to complete the work or action[48]. This strategy is to prevent attackers from exploiting the vulnerability of one attack surface to escalate the access right to other components. This principle can be applied to many assets and services in vehicle communication. For example, messages from the telematics gateway should not be able to invoke access to the CAN bus; or SMS service provider should be whitelisting to prevent unauthorised remote operation services.
- Separating the safety-critical network segments from the external interfaces: if there exists any interface that connects a safety-critical network an external path, attackers can exploit an interface to manipulate the safety related functions, which can lead to safety issues.
- Planning different operation modes to react when the system is under attack: attacks can be unavoidable in some circumstances despite all the defence efforts (e.g. due to unknown attack, zero-day vulnerability). Therefore, it is important to prepare for several scenarios such as “Safe Mode”[49] in which all the non-essential communication functions of the vehicle are turn-off; or “Go Dark”[49] mode where all the wireless interfaces are disabled to eliminate the remote attacks.

4.8. Reviewing Security Testing Techniques

For vehicle manufacturers and their suppliers, guidelines and standards, and proposed standards, require the implementation of practical security testing. This is the next stage in the security assessment of a system once the TARA process has progressed. Security testing is an additional overhead in the development process for new vehicle models. Such testing must include the links beyond the boundary of the vehicle because vehicle connectivity has made it part of a wider cyber ecosystem. This means security testing extends to the communications infrastructure and ITS. Fortunately for manufacturers, their existing investments and expertise in functional testing can be leveraged for the challenges of cyber security testing, and, as the J3061 guidelines indicate, testing processes should not need to change a great deal. Furthermore, if cyber security testing is performed early enough it can allow for feedback into designs prior to production, as it should do to ensure security is baked into systems.

When engineers design a system, they can specify functional security mechanisms, for example, authentication of a user via a logging-in facility, e.g. entering a Personal Identification Number (PIN) when syncing a smartphone to a vehicle. Any designed-in security mechanisms are to protect the security (CIA) properties of the system. The functional security mechanisms

[47] https://www.isograph.com/software/attacktree/mitigating-against-attacks/

[48] Oyler, A., and Saiedian, H. (2016) ‘Security in automotive telematics: a survey of threats and risk mitigation strategies to counter the existing and emerging attack vectors’, Security and Communication Networks

[49] Graubart, R.D., McQuaid, R., and Woodill, J. (2018) ‘Cyber Resiliency Metrics and Scoring in Practice’

will be defined in the system specifications. The test plans for the system will check that such defined security mechanisms function as intended[50].

What is often exploited by malicious agents is hidden, and unwanted, functionality[51], caused by engineering issues. In a system that uses software for much of its functionality, it is **bugs** that cause engineering issues. These bugs can take the form of:

- Logical errors in code (or models used to generate code) resulting in run-time bugs.
- Weaknesses in system design, for example, if no consideration has been given to data encryption or a lack of strong checks to ensure that input can only be received in the expected manner (or format).
- Functional bugs due to a mismatch between what the system specification states and how the system has been implemented, and these not being caught by the functional testing.
- Additional and undocumented features provided by third party components and software libraries. Examples include test functions or features that were developed for another use case (e.g. another customer) that remain present within the system.

Not all bugs can be exploited to reveal weaknesses, however, for exploitable bugs, three types of testing can be performed to reveal them[10] [11]. Indeed, Section 8.4.7 of J3061 describes them as "critical tools in evaluating the Cybersecurity performance of a system":

- **vulnerability testing** - performing tests for security weaknesses and exploits using scanning tools and a corpus of known attacks;
- **fuzz testing** - dynamically sending the system large amounts of random and malformed data to see how it responds, in an effort to reveal a vulnerability;
- **penetration testing** - using intelligence and tools to attack a system based on how adversaries would attempt to overcome security mechanisms.

As researchers[11] point out, these three classes of security tests are relatively new to automotive software and test engineers, and mobile network and communications engineers. Furthermore, they add to the existing systems functional testing workload. Integrating security tests systematically and rigorously into the systems testing regimes will take some effort, particularly considering the complexity and number of interfaces that can now be found with the ecosystem. The proliferation of advanced features, supported through cloud-based services which can be probed for weaknesses at the client (vehicle or device) or server (service provider) ends, adds to the attack surface. Whilst mobile networks carry out extensive cyber security checks on a regularly basis, the incorporation of mobile communications into the CAV ecosystem extends the attack footprint.
The work required to implement the three types of security tests into CAV testing regimes has begun[52], and researchers at Chalmers University of Technology have used the three security tests as part of a proposed *Start - Predict - Mitigate - Test* (SPMT) process to systematically

[50] S. Bayer, T. Enderle, D.-K. Oka, and M. Wolf (2016) 'Automotive Security Testing-The Digital Crash Test', in Energy Consumption and Autonomous Driving Proceedings of the 3rd CESA Automotive Electronics Congress, Paris, 2014, J. Langheim, Ed., Paris: Springer
[51] H. H. Thompson (2003) 'Why security testing is hard', IEEE Security and Privacy, vol. 1, no. 4, pp. 83–86, ISSN: 15407993. doi: 10.1109/MSECP.2003.1219078
[52] P. Wooderson and D. Ward (2017) 'Cybersecurity Testing and Validation' in SAE Technical Paper, SAE International, doi: 10.4271/2017-01-1655

analyse vehicular cyber security[53]. The SPMT process, which has the high-level steps illustrated in Figure 4, is complicated by vehicle complexity and the nature of the possible threats, however, here is a brief summary of the four phases:

- **Start** - Perform an analysis of the vehicle systems to determine what needs protecting. This is the TARA in the Security Framework.
- **Predict** - Perform a threat assessment to quantify and rank risks. This would be the application of attack tracks from the Security Framework.
- **Mitigate** - Apply countermeasures to the ranked risks. Economic considerations influence the application of countermeasures. Mitigation is based upon the outputs of the previous two phases.
- **Test** - Apply the three security testing regimes (vulnerability, fuzz, penetration) to ensure that designs are resilient to attack, and that applied countermeasures are effective. Use test automation, where possible, for efficiency. Any revealed security issues must be reviewed.

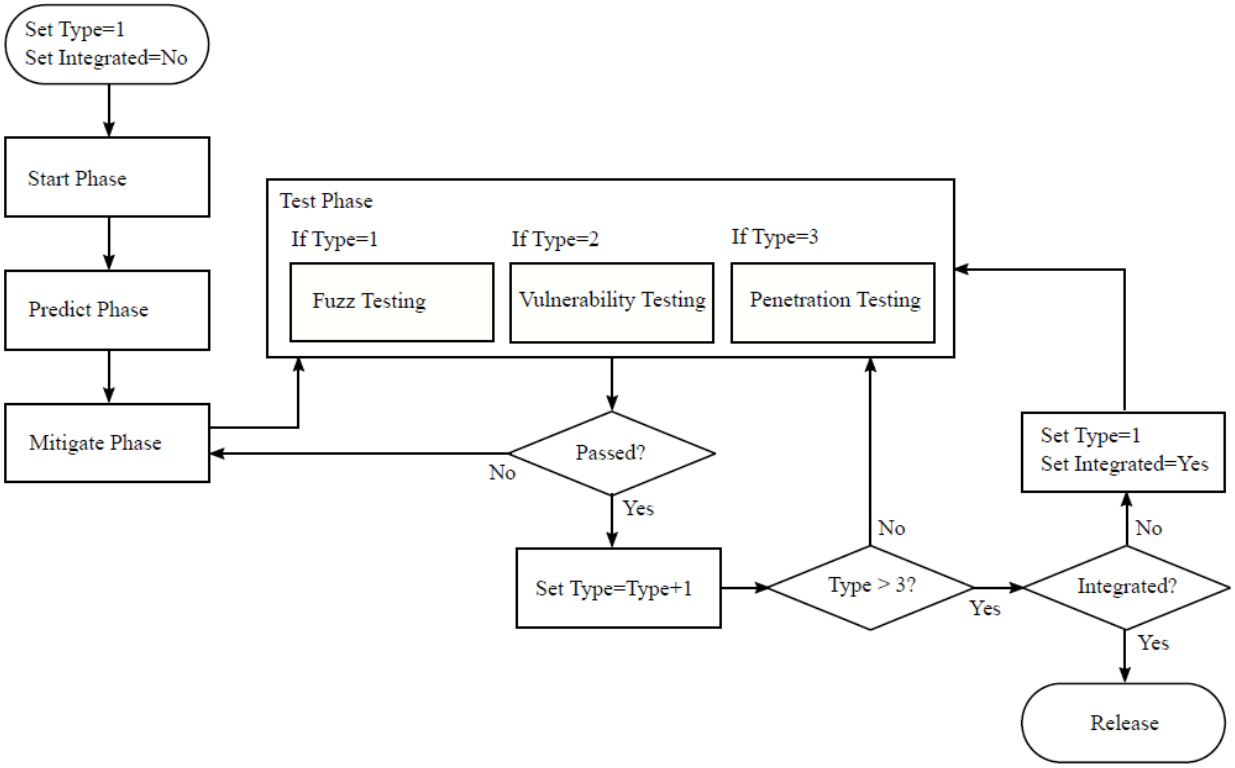


Figure 10. The SPMT process for security testing proposed by Chalmers University

J3061 suggests that vulnerability and penetration testing is performed by parties independent of the systems engineering development. Indeed, BMW proved the benefit of having vehicles tested by independent automotive security specialists[54]. Having an unbiased and independent analysis of a system by security experts can reveal unconsidered exploitation paths and system weaknesses.

[53] Strandberg, K., Olovsson, T., & Jonsson, E. (2018) 'Securing the Connected Car: A Security-Enhancement Methodology', IEEE Vehicular Technology Magazine, 13(1), 56–65, doi: 10.1109/MVT.2017.2758179

[54] Tencent Keen Security Lab (2018) 'Experimental Security Assessment of BMW Cars: A Summary Report' Tech. rep. Keen Security Lab

Vulnerability and penetration testing can be performed by manufacturers, but there may be a bias in the results. Fuzz testing is a beneficial security test for manufacturers to perform themselves. However, a lack of available fuzz testing resources, and information to implement fuzz testing, is likely to restrict adoption. This is one area which would benefit from additional investment into research.

In this section, the major types of security testing have been discussed. Security tests are the practical engineering that occurs to ensure that a level of security, as specified in requirements and designed into a system, is present, and that any mitigation designs have been addressed. The tests form part of the Security Framework, following on from the derivation of the attack surfaces from a reference architecture, the TARA process, and the Attack Tree rankings.

5. Possible Cyber Security Vulnerabilities in Telecommunications C-V2X

The following Sections, 5 to 11 inclusive, will focus on technology and the potential cyber security vulnerabilities within the telecommunications system of the CAV ecosystem. This part of the report focuses primarily on the mobile network architecture, the built-in security features within mobile networks, and the associated and known vulnerabilities within the system. The CAV network architecture will be introduced, the security vulnerabilities specific to CAV will be addressed. Threat Modelling see Section 4.3, within communications is covered, including risk ratings.

Some case studies relevant to mobile network security in general, as well as specific CAV examples, are discussed. These case studies demonstrate the importance and urgency of having effective cyber security controls and the risk mitigation frameworks that are explored in subsequent sections.

5.1. Introductory Overview to Mobile Networks

Mobile networks (also called cellular networks), primarily consist of a distribution of radio communication nodes that are organized in a cellular structure, with each node responsible for providing radio coverage in a specific geographic area through a radio transceiver known as a radio base station. Each radio base station provides radio coverage through a dedicated set of radio channels or frequencies carefully planned to propagate only a given coverage area. When grouped together, these cells form a network infrastructure that provides radio coverage and ensures connectivity and continuity of communication as users move through a larger geographic area.

Connectivity to the network infrastructure can be achieved with portable or handheld User Equipment (UE) such as mobile phones, personal computers and vehicular communications systems. Continuity of communication is achieved through a process called ‘handover’, in which an ongoing voice or data call is transferred from one radio base station to another as the UE moves about the coverage area.

Mobile networks have evolved since the introduction of the analogue First Generation (1G) networks, the development of the voice centric Second-Generation (2G) Global System for Mobile (GSM) networks and the upgrade to the higher data rate Third Generation (3G) Universal Mobile Telecommunications System (UMTS) networks about 19 years ago. However, 3G came of age 10 years ago when High Speed Packet Access was launched. Current Fourth Generation LTE (4G) mobile networks were designed as packet networks, allowing them to support higher data rates than 3G networks. The Fifth Generation NR (5G) mobile networks are currently being developed, standardised and deployed with the expectation that they will provide much higher capacity and data rates, through additional spectrum, larger channels and ability to aggregate more carrier, faster network response times and provide new service capabilities for a wide range of industry verticals enabled by; MEC, Private Networks and Network of networks. To be clear, to realise the full potential of 5G significant amounts of new spectrum will be required.

5.2. General Mobile Network Architecture

Mobile networks have a structure that typically starts at the Base Transceiver Station (BTS), assuming a 2G mobile network as an example. The BTS provides radio coverage through its antenna systems and enables direct connectivity and communications with mobile devices. All base stations are connected back to one or more base station Controllers (BSC) by copper, microwave, fibre and even satellite backhaul links.

The BSC (or RNC in 3G) has overall control functions of the base stations such as radio channel setup and handovers, ensures effective utilisation of the Radio Resources and serve as the interface between the BTS (in 2G), NodeB (in 3G) or eNodeB (in 4G) and the core network. This is referred to as Evolved Packet Core (EPC) in a multi-radio access technology system.

The MSC is the gateway responsible for interfacing with other network operators and external networks such as the Public Switched Telephone Network (PSTN). The MSC also handles user authentication and the handover process to other BSCs. The MSC contains the VLR (Visitor Location Register) and HLR (Home Location Register) which holds the information of the mobile network subscribers.

Figure 11 provides a high-level system architecture of a 2G, 3G and 4G mobile data network with the associated functional elements and interfaces. This architecture is derived from the 3GPP reference architecture for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access[55].

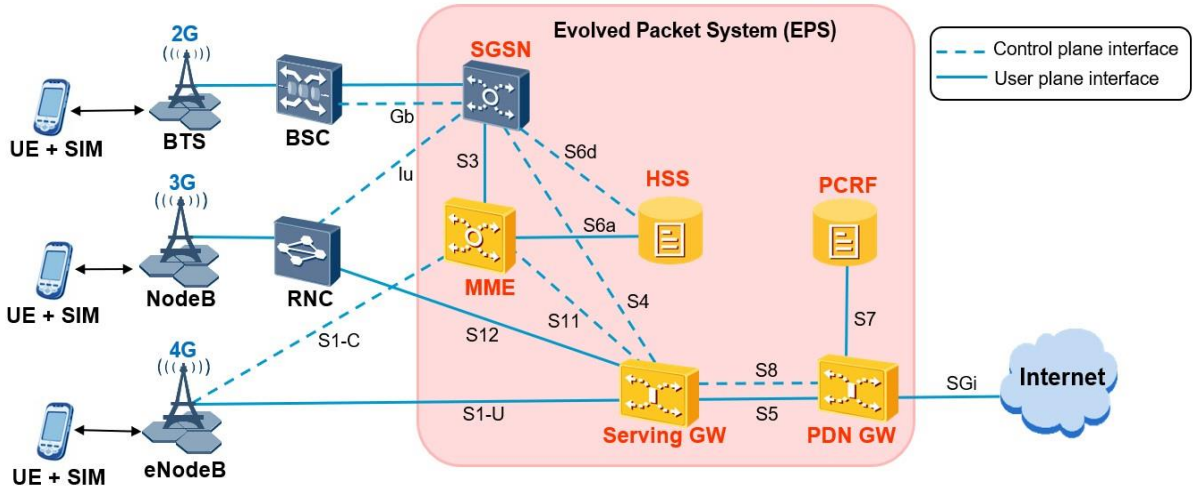


Figure 11: General mobile data network architecture

5.3. Functional Elements of a Mobile Network

Mobile networks consist of several functional elements or sub-networks that connect and interface with each other to form the overall network architecture. Each of these functional

[55] 3GPP TS 23.401, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=849

elements or sub-networks have certain logical or physical interfaces that allows the various interactions between them to occur.

The interactions between these functional elements, however, means that there are certain security implications that must be considered in order to provide guaranteed end-to-end security for the network.

The radio access, core, and backhaul networks are the key functional elements considered in this work. The key security vulnerabilities that have been identified in each sub-network or network interface are provided. The security threats and attacks that have been demonstrated in each sub-network are highlighted. As a way of mitigating against the highlighted threats, the built-in security features and capabilities in each of these sub-networks are also discussed in the subsequent sections of this report.

5.3.1. Radio Access Network (RAN)

The Radio Access Network (RAN), in most cases, forms the largest component of the overall mobile network. It typically comprises of the Base Transceiver Station and the associated BSCs. The RAN is used to implement the radio access technology, using radio signals to connect subscribers (i.e., the mobile devices) to the Core Network.

UEs, the mobile devices, primarily connect to the RAN through the BTS, which means that the interface between the RAN and the BTS, starting from the Subscriber Identity Module (SIM) card that is embedded in the mobile devices, forms part of the RAN from a mobile security perspective.

RAN technology has evolved over the years since the first generations of mobile networks from GSM. RAN uses a mixture of General Packet Radio Service (GPRS) and Enhanced Data rates for Global Evolution (EDGE), and data networks as well as circuit-switched voice. 3G improved data speeds with UMTS, with Circuit Switched Voice and High-Speed Downlink Packet Access (HSPDA) technology. 4G/LTE and recently upgraded to LTE-A (LTE Advanced) which is truly packet based and offers high data rates and low latency, as well as voice service though Voice Over LTE (VOLTE), supported by an Internet Protocol (IP) Multimedia Subsystem (IMS) platform in the core, this allows us to support Wi-Fi calling for an authenticated device.

Each generation has also brought in better security measures and capabilities to mitigate the known security vulnerabilities of the preceding generation. For example, in earlier 1G mobile networks, it was possible to capture the radio signals using a transceiver, due to the lack of security against eavesdropping between the mobile devices and base station. It was also possible to use ‘cloning', either of the mobile subscriber to use services without paying, or of the base stations, in order to deceive the UE into connecting to a false base station and gain unauthorised access to user information. These security threats have been reduced in second generation networks onwards; for example, with the introduction of better security features and capabilities such as encryption and mutual authentication techniques.

5.3.2. Core Network (CN), the EPC

The core network (CN), i.e. the EPC, forms the central part of the mobile network, providing access to the required services for users connected through the RAN. It comprises of entities such as the Mobile Switching Centre (MSC), the Home and Visitor Location Registers (HLR and VLR), known collectively as the HSS, the Equipment Identity Register (EIR), the Authentication Centre (AuC), the Serving Gateway (SGW) and the Packet Gateway (PGW) that interfaces with external data networks and the internet.

The core network provides the circuit-switched and packet-switched functionalities required for mobile users to access mobile voice, SMS and data services as well as directing calls over the PSTN. To ensure that only the mobile users entitled to a service can have access and are accurately billed for it, the core network provides the authentication and charging capabilities of the network. It is also responsible for mobility management functions such as providing handover assistance between the mobile devices and BTS as well as managing paging, access, handover, and the location update process.

Earlier generations of mobile networks such as 2G and 3G, used a set of protocols, namely the Signalling System number 7 (SS7), which were designed many years ago for the communication between networks and the coordination of activities such as authentication, voice and data switching and location updates. SS7 has an identified possible design flaw that, if not correctly managed, might introduce security threats by allowing messages to be altered, deleted or injected into the networks, leading to possible compromising data integrity and security of the network. This was mostly mitigated by the introduction and use of a newer and improved signalling system called ‘Diameter’ in 4G mobile technology.

5.3.3. Transport Network (Backhaul)

The backhaul of a mobile network connects the core network with the other subnetworks. It is typically used to transport data from the base station to the central elements of the core network such as the Serving Gateway (S-GW) and Mobility Management Entity (MME) in an LTE network for example.

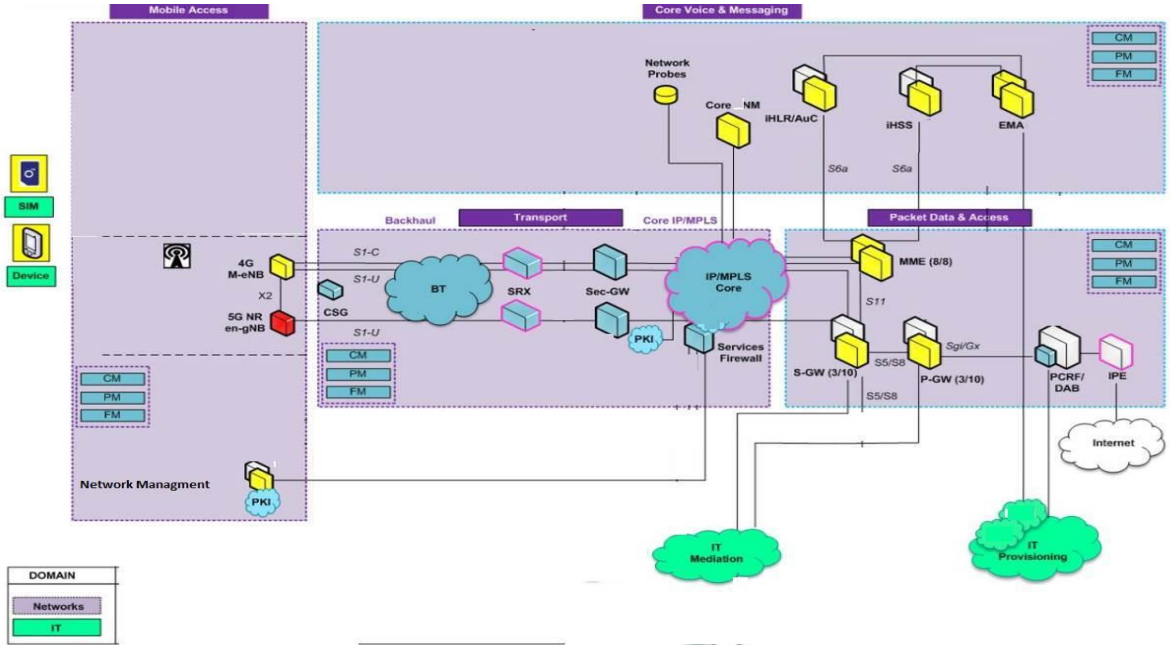


Figure 12: 4G Network Architecture showing backhaul subnetwork elements

The backhaul network usually comprises of three nodes: Access or last mile, preaggregation and aggregation nodes. The access and preaggregation networks can both be implemented through wireless media such as microwave technology or wired networking with the use of copper or fibre optic cables. The aggregation network requires a very high capacity and is therefore usually implemented using fibre technology. The access network links the edge of the mobile network (i.e. base station) to the preaggregation nodes. The aggregation node groups the data from all preaggregation nodes and is then responsible for aggregating all traffic and forwarding it to the core network.

Earlier generations of mobile networks implemented backhaul technologies using standards such as Asynchronous Transfer Mode (ATM) and Time-Division Multiplexing (TDM). These protocols were less understood by hackers and were therefore less attacked. However, current 4G backhaul technology is based on a flat All-Internet Protocol (All-IP) architecture that is well understood by many and therefore presents a larger surface area for attacks including traditional Internet security threats such as malware-based trojan attacks, jamming-based Denial-of-Service (DoS) attacks, IP Spoofing attacks (masquerading), eavesdropping and Man in the Middle (MitM) attacks.

Some of the security threats and vulnerabilities in the backhaul network can be mitigated by using security gateways, Layer 3 IPsec tunnels and implementation of certificate authorities. The threats, vulnerabilities and capabilities of all the mobile network components introduced in this section are discussed in detail in the subsequent sections of this report, particularly as relate to CAV security.

While the Internet is not a security issue per se for the mobile network, its connection to the mobile network may introduce large scale security threats, with a lot of Internet-based attacks occurring from this entry point. It should be noted that the modelling of any security threat outside the mobile network, such as external networks like the Internet or PSTN is outside the scope of this report.

5.4. Connectivity Infrastructure for CAV

Connectivity is a key enabler upon which the benefits of CAV technology will be realized. It refers to the communication infrastructure that allows data to be transferred from and between the different elements that make up the CAV ecosystem. In CAV, V2X is the umbrella term that denotes the communication framework in which data from a variety of sources including vehicle sensors, vehicle telematic systems, roadside infrastructure, pedestrians and communication networks are transferred across the system.

DSRC is based on the IEEE 802.11p-based wireless standard and supports secure communication between vehicles and the surrounding infrastructure without the involvement of the mobile communications infrastructure.

As introduced in Section 3, C-V2X is a 3GPP standard, for vehicle wireless communication technology that is implemented using the mobile 4G or 5G technology. The early specifications and service requirements were defined and implemented in 3GPP Release 14 and significant enhancements, especially higher demands on security and reliability, provided in 3GPP Releases 15 and 16.

As an example of C-V2X, this report primarily focuses on vehicle to mobile network technology (C-V2N). This uses the mobile network to provide services such as fleet management, logistics and infotainment as well as enabling improved driving safety and road traffic efficiency through Cooperative Intelligent Transport Systems (C-ITS) and Advanced Driver Assistance Systems (ADAS). DSRC is an alternative V2X technology.

For example, C-V2N connectivity enables the distribution of real-time road traffic signals and traffic situations to drivers in the form of GeoCasted messages (messages that are disseminated with information regarding a target geographic area) from the LTE network to the SIM card placed in the modem of the vehicle's communications system.

Connected and autonomous vehicle technology enable a range of services and societal benefits as highlighted earlier. However, with these benefits come significant risks that must be mitigated against. For example, despite the elimination of driver error as a positive outcome, risks may exist from a myriad of factors, such as system errors, cyber attacks on safety systems, and the behavioural improprieties of both passengers and pedestrians.

In addition, sophisticated data processing and storage abilities of CAV systems also raise data privacy concerns, examples include tracking of user location from location data stored in vehicles, and unauthorised use of personal data synced from personal devices. Connection to external networks such as the mobile network and cloud infrastructures, which may be necessary for vehicle cooperation on the roads, increases privacy risks as data can be accessed by attackers and retrieved if network vulnerabilities are successfully exploited[56].

The privacy and cyber security risks introduced by utilizing LTE C-V2N as a connectivity technology in CAV technology is also introduced. The cyber security threat modelling and risk analysis, scoring and mitigation frameworks beginning with the dataflows from the SIM card

[56] Hazel Si Min Lim, A. T. (2018) 'Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications' Retrieved from MDPI: https://www.mdpi.com/1996-1073/11/5/1062

interface inside the connected vehicle to the mobile LTE RAN and Core networks are discussed in the subsequent sections.

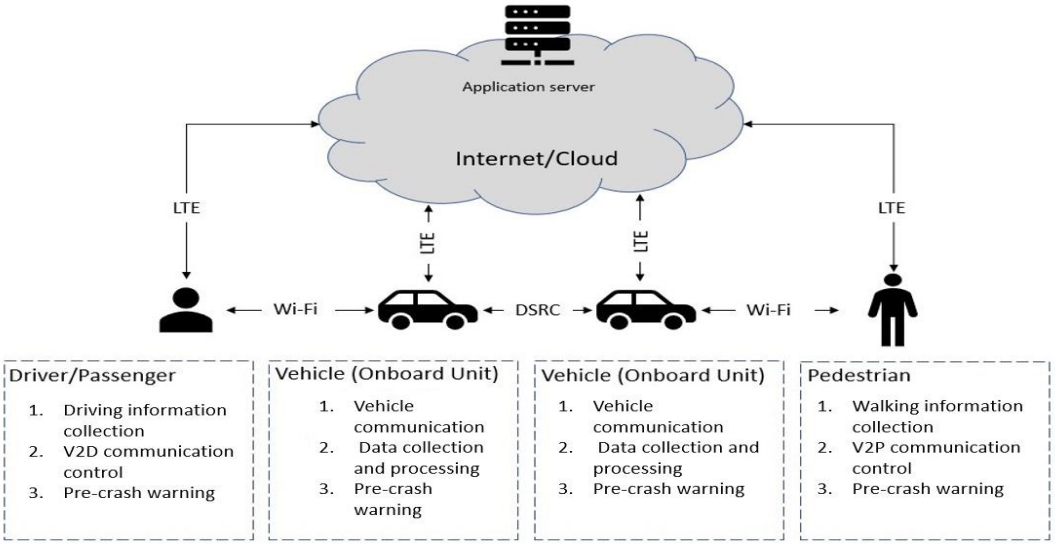


Figure 13: V2X communication systems architecture[57]

In Figure 13 above, the general architecture of a heterogenous V2X system uses DSRC, C-V2X and Wi-Fi technologies to enable communications between devices with a wide range of motion patterns including Vehicle-to-Vehicle, Vehicle-to-Pedestrian and Vehicle-to-Cloud. In this architecture, the LTE network provides vital connectivity to the cloud Application Server.

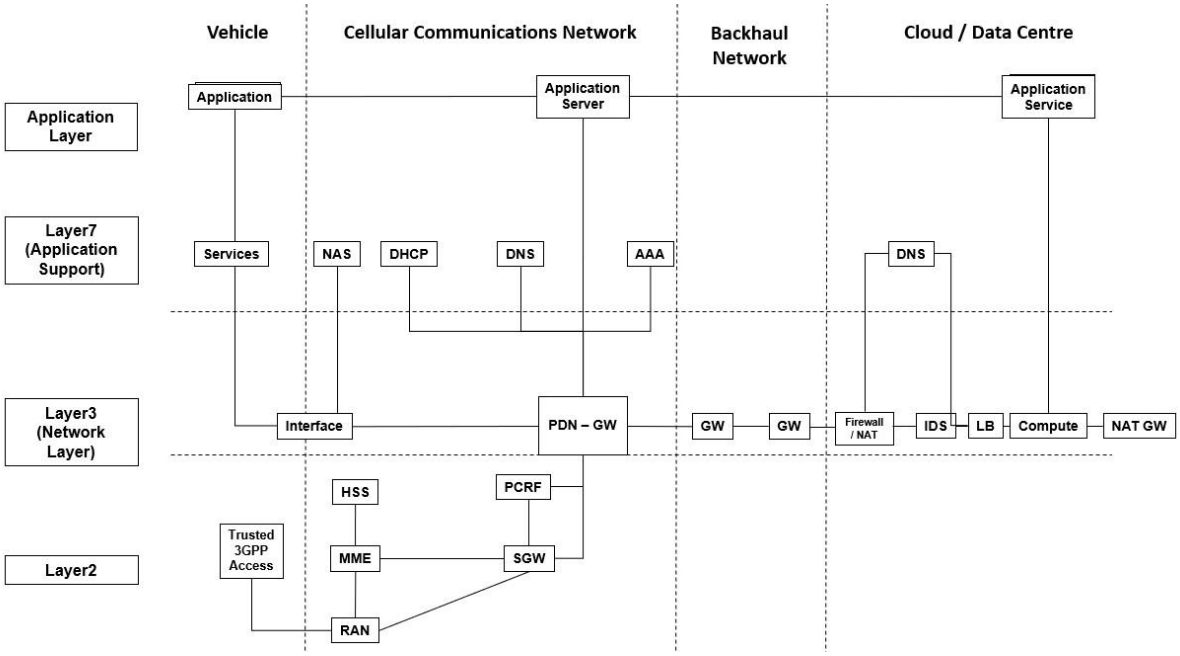


Figure 14: End-to-end reference architecture of LTE V2C communications (Cisco)

Figure 14 provides an end-to-end high-level reference architecture of a Vehicle to Cloud communications systems enabled by the LTE mobile infrastructure. The high-level system components, from the vehicle to the cloud, their connectivity interfaces and the interaction layers are shown.

[57] Marojevic, V. (2018) C-V2X Security Requirements and Procedures: Survey and Research Directions

Figure 15 then describes the high-level framework for data and message transfers from a C-V2X Application Client, which may be resident in a vehicle, roadside infrastructure unit or personal communications device, to a cloud based V2X Application Server through an LTE mobile infrastructure[58].

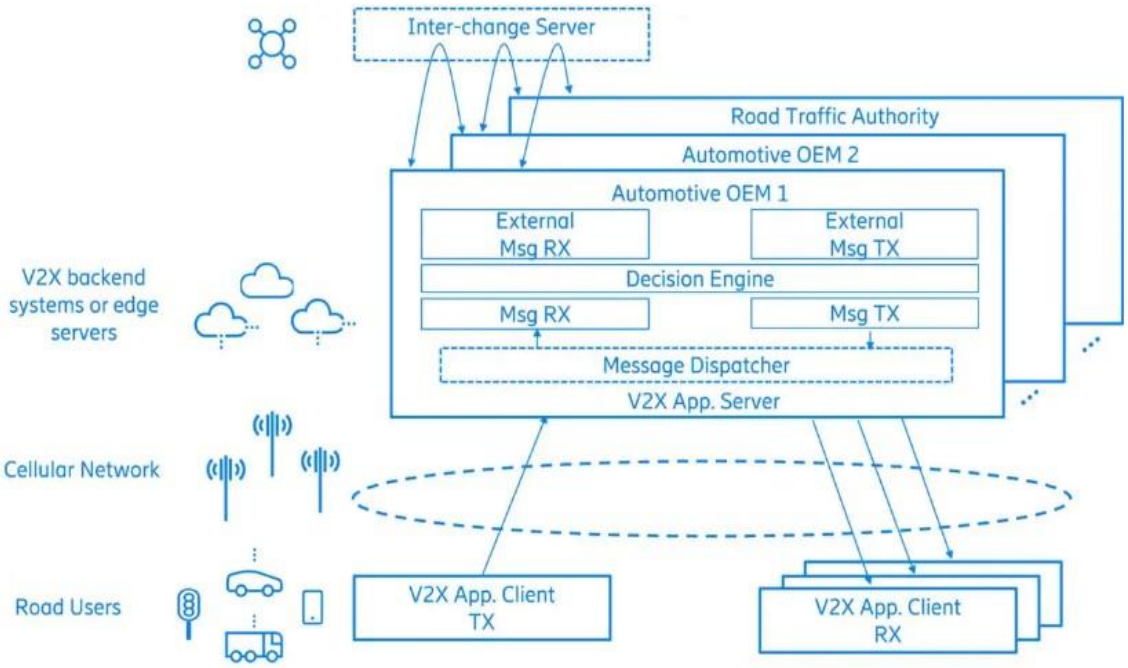


Figure 15: Architecture for delivering C-ITS messages over mobile networks

The above implementation of C-V2X primarily consists of the mobile network layer, V2X Application Server, the V2X Application Client and the Inter-change Server that ensures interoperability across different V2X Application Servers and backend systems.

The V2X Application Client has both a transmit and receive module and can be hosted inside the vehicle communications unit, on personal communication devices, or road-side units which are all provisioned with the required mobile connectivity, enabling the transmission of uplink unicast messages to the V2X Application Server.

The V2X Application Server is located at the backend or edge servers that are accessible by V2X Application Clients via mobile networks and uses downlink unicast, multicast or broadcast transmission to transfer data to the Application Clients[58].

[58] Essaili, A. E., Lomar, T., Nylander, T., & Zang, Y. (2019, October 25). Ericsson Blog. Retrieved from Ericsson Web site: https://www.ericsson.com/en/blog/2019/10/cellular-v2x-the-road-ahead-c-its-adas

6. Challenges in Vehicular Communications

6.1. Introduction

There are four groups of vulnerabilities for vehicular communication[59] [60]:

- **Limited connectivity:** It is still a challenge to perform updates of a vehicle's software and firmware to protect it against emerging cyber attacks.
- **Limited computational performance:** Vehicles are more vulnerable to security threats and a security solution implementation is restricted due to the limited computational performance.
- **Unpredictable attack scenarios and threats:** It is difficult to rearchitect a vehicle system including databases, communication system and vehicular parts to cover new cyber security challenges. An unsecure OEM element of this system might lead to a security breach.
- **Critical risk for drivers or passengers' lives:** A vehicle could be at a high risk even if only a limited number of sensors malfunction, if there is a lack of communication, or if illegitimate messages are delivered[61].

A CAV is at risk from attackers who maliciously interfere with the vehicular communication layer and might compromise confidentiality, integrity and availability. Moreover, the privacy, repudiation, flexibility and real-time constraints are targets of attacks.

Confidentiality is defined as "preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" by NIST[62]. Integrity means that the delivered message is not corrupted or altered by any intruder. It is necessary to provide the verification ability to make the receiver node sure that the message is legitimate.

NIST defines availability as "ensuring timely and reliable access to and use of information"[562]. Non-Repudiation is crucial in case of an accident. It is necessary to rightly identify all elements during an investigation and to make sure all messages are transmitted reliably. Privacy means anonymity is protected and no unauthorised user can access the vehicle's or driver's private data[63]. It is crucial to prevent outdated information by providing online and reliable data transmission. This is guaranteed by real-time constraints that avoid transmission delays.

The need for a flexible means of communication within a security architecture is significant in a dynamic environment. The dynamic nature of security attacks makes it challenging to provide flexible in vehicular communication.

[59] Onishi, H. (2013) Guidelines for vehicle cybersecurity. Retrieved from https://docplayer.net /7458872-For-vehicle-cyber-security.html
[60] Onishi, H. (2012) Paradigm change of vehicle cyber security. 4th International Conference on Cyber Conflict, pp.381–391
[61] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2019) Cybersecurity challenges in vehicular communications. Vehicular Communications, 2214-2096
[62] Guttman, B., & Roback, E. (1995). An Introduction to Computer Security: The NIST Handbook. DIANE.
[63] Zhang, L. (2010) Research on Security and Privacy in Vehicular Ad Hoc Networks. Retrieved from www.tesisenxarxa.net

A mature cyber security program has several components that improve the threat detection program and effectiveness as follows[64]:

- **Secure design:** The development process requires an appropriate solution to identify and prevent security vulnerabilities. Design analysis and security testing should be applied to stages of the development lifecycle to ensure flaws and vulnerabilities are covered. Constant penetration tests after development provide the ability to plan attack mitigations and appropriate updates to address new threats.
- **Threat intelligence:** A proper threat detection program needs an up-to-date threat and vulnerability database, including public and proprietary threat information.
- **Asset identification:** It is crucial to identify and document a list of assets including third-party assets related to the environment to conduct proper threat analysis. In the lack of appropriate asset identification, vulnerable assets might be unknown to security team inside the ecosystem.
- **Mitigation capabilities:** This refers to a security team's ability to detect and resolve attacks as they emerge. Effective security planning requires the identification of applicable mitigation capabilities and security controls to provide the security team with the ability to take proper actions against security threats using existing resources.
- **Risk Assessment:** It is important to evaluate, score and rank security risks of various components of a system by conducting a risk assessment process. The output is a list of security risks which are ordered based on their significance.
- **Mapping and modelling:** Modelling methods build visual workflows and security operations plans based on multi-angle approaches. The modelling goal is to resolve existing issues and plan for future threats. It is crucial to cover and measure all components because a lack of planning might leave assets vulnerable. A mature threat model improves the threat mitigation process by simplifying threat detection and analysis.

[64] Walker, A. (2019) What Is Threat Modeling? Retrieved from https://learn.g2.com/author/aaron-walker

6.2. Threat Detection, Monitoring and Analysis

To reduce the risk of cyber threats against CAV, it is necessary to define an organisational process to detect, monitor and analyse cyber security threats. Auto-ISAC has provided the *Threat Detection, Monitoring And Analysis, Best Practice Guide*, a framework containing five steps[65], see Figure 16.

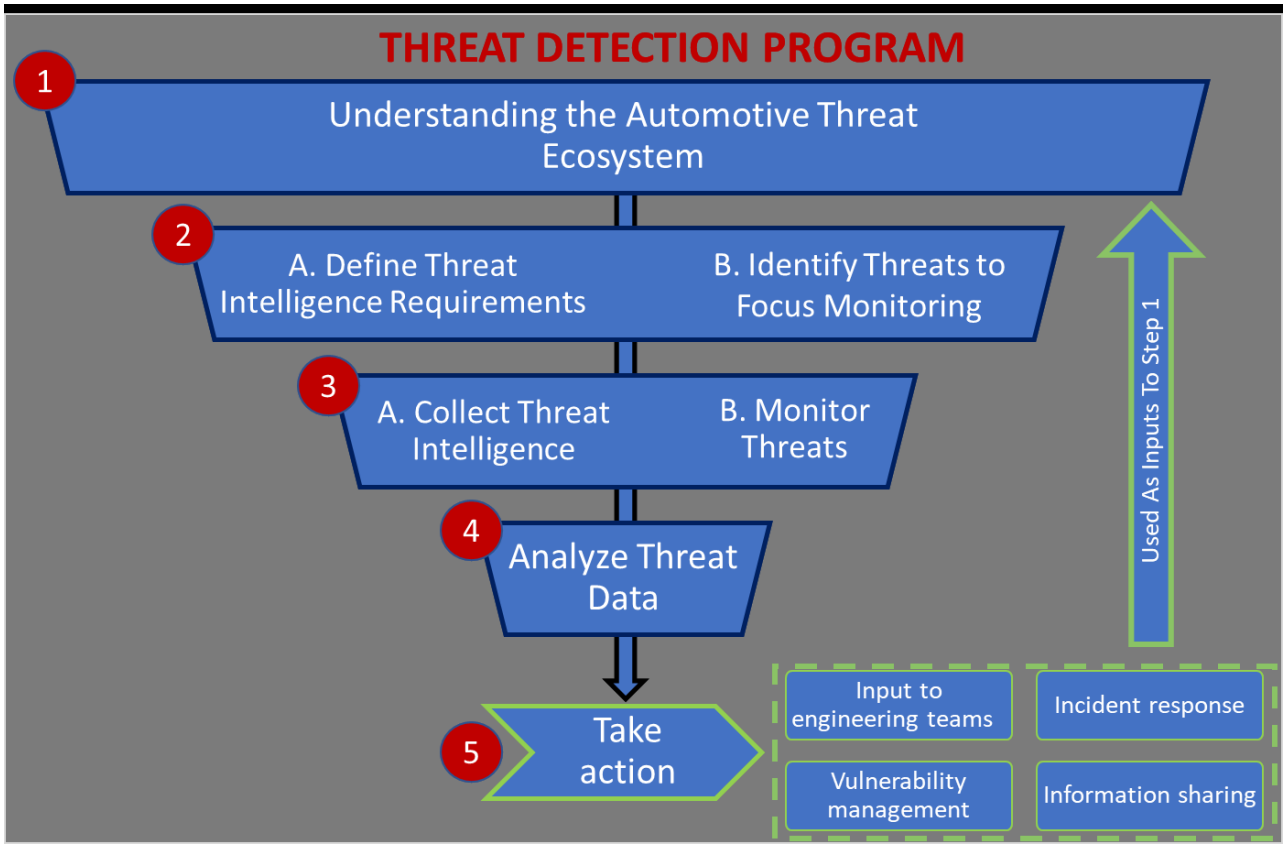


Figure 16. A threat detection program

Step 1 - Understand the CAV communication threats ecosystem to create the program basis including past research and reviews, and the history of security breaches; and how this relates to the vehicle communication components, software applications and connected services should be considered in the customer environment. Insider threats and operational technologies are included in the enterprise environment. The third-party environment also covers any devices or services which are supplied by vendors[65].

Step 2 - Threat intelligence requirements and monitoring targets should be identified to provide adequate information of interested assets and relevant threats. This helps to understand the threat landscape to define breach indicators, tactics and unusual incidents.

Step 3 - It is required to create a risk profile of threats and applicable vulnerabilities. This helps to form a knowledge base risk profile that leads to threat identification and appropriate monitoring techniques.

[65] AUTO-ISAC. (2019) Threat Detection, Monitoring and Analysis, Best Practice Guide, Version 1.3. Retrieved from https://www.automotiveisac.com/best-practices/

An effective monitoring process requires to determine crucial security risks and concentrate on monitoring the related threats. The constantly evolving vehicle technologies makes the CAV security risks a dynamic model and consequently, it is necessary to employ a flexible process to monitor the source of threats.

Step 4 - An accurate threat analysis provides adequate information to develop a risk mitigation plan and comprehensive security control design.

Threat analysis is the process of threat identification, validation and verification. It is necessary to detect threat events for each validated threat and respond appropriate strategy.

Step 5 - Information from threat analysis and impacts makes this possible to identify appropriate controls and develop security architecture. These come together to develop a risk mitigation plan which defines required actions to reduce risk. The action plans should be design to provide, engineering and security teams with corrective actions and mitigations.

Reactive approaches do not have the capacity to predict and respond to the dynamically changing nature of the risks. An effective CAV cyber security risk classification should be flexible, adaptive and evolving to cover new threats as they arise.

6.3. CAV Threat Environment

The threat environment is defined by threat actors and attack vectors. A cyber security threat will be executed by a person or entity (threat actor) that uses various methods on an attack surface (threat vectors) used to exploit a vulnerability of the ecosystem. To identify a threat in the CAV ecosystem, it is necessary to consider its impacts and consequences to the security properties. It is also required to understand threat actors' capabilities and motivations by employing risk assessment and incident response processes[65].

The following threat actors are identified by Auto-ISAC that might affect the vehicle ecosystem[66]:

- Terrorist organisations
- Malicious insiders
- Nefarious individuals
- Cyber criminals
- Organized crime groups
- State sponsored attackers and intelligence agencies
- Vandals/pranksters/hacktivists

[66] AUTO-ISAC (2019) Risk Assessment and Management, Best Practice Guide, Version 2.3. Retrieved from https://www.automotiveisac.com/best-practices/

Auto-ISAC has also identified several attack vectors that increase the security risks on the vehicular ecosystem:

- Distance from vehicle:
  - Near:
    - Bluetooth.
    - Wi-Fi.
    - Tire Pressure Monitoring Systems (TPMS).
  - Far:
    - Via back-office channels.
    - Via remote capabilities.
- Internal to vehicle:
  - Standard user interface.
  - Infotainment.
  - USB.
  - Standard programming/data interface.
  - Non-standard interface.
    - Accessing and modifying vehicle electrical systems.

According to the above attack actors and attack vectors, the following threats might be possible through compromising the vehicular communication layer:

- Theft or exposure of data:
  - Theft or exposure of personally identifiable information (PII) or other sensitive data,
  - Theft or exposure of vehicle-related data or software.
- Physical theft or compromise:
  - Unauthorised physical access to the interior or breaking door locks,
  - Theft of the entire vehicle.
- Manipulating vehicle controls:
  - Illegal manipulation of components and functions,
  - Unauthorised activation or deactivation of functionality,
  - Co-opting vehicle systems,
  - Loss of vehicle control.
- Threats to availability:
  - “Bricking” vehicle systems,
  - Denial of service attacks,
  - Ransomware attacks.

6.4. Threat Types

The CAV ecosystem follows current mobile computing and Internet communication security requirements. From this perspective, cyber security threats to CAV communication layer are divided into passive and active attacks[67].

Passive attacks eavesdrop or monitor the transmissions between nodes, where the attackers cannot modify or change the content in the transmission and would not interact with the data

[67] He, Q., Meng, X., & Qu, R. (2017) Survey on cyber security of CAV. 2017 Forum on Cooperative Positioning and Service (CPGPS), 351-354

transmitted[68]. These attacks can be hard to identify because there is no modification to messages. Passive attacks that are most likely to be faced by CAV include the following:

- **Eavesdropping and Release of the Information**: Without appropriate encryption mechanisms, an attacker could eavesdrop in on the vehicle's communication messages sent using the C-V2X communication channels.
- **Traffic Analysis:** Attackers could use traffic analysis method to obtain the length and time of messages, and with such information, could gather further information such as the time the car is used, and thus the user's working time and time of their daily activities.

Attackers are more likely to take actions to modify or damage the messages and the data transmitted in active attacks[68]. These can cause much more damage than passive attacks, especially in the CAV environment, and might result in injuries or death to drivers and passengers. In CAV, active attacks can be divided into four categories as follows:

- **Spoofing:** A spoofing attack is conducted by faking identities or data. This happens when an unauthorised attacker pretends to be an authorised user.
- **Replay Attack:** Attackers can intercept the message with authentication from sender to receiver and resend the message to the receiver to obtain the authenticated access to the service. Attackers do not need to know the content inside the message, so the encryption of data is useless in this attack.
- **Modification:** In this kind of attack, attackers can modify the message such as GPS information between the communication channels.
- **Denial of Service (DoS):** DoS attacks will block the access to the target server by making use of flaws in the system or protocol to send huge amount of data, or request to interfere with the receiver's network[69]. This attack may cause delay and breakdown of the receiver's response. In some contexts, the delays caused by this might be an inconvenience. However, in CAV safety systems, for example, C-V2X messaging, low latency is importance and timing delays might reduce capabilities.

Compared with passive attacks, active attacks are much more difficult to defend against but much easier to detect. It is crucial that CAV designers and car manufacturers always carefully consider all the possible flaws in CAV systems and protocols.

[68] Gagandeep, A., & Kumar, P. (2012) Analysis of different security attacks in MANETs on protocol stack A-review. International Journal of Engineering and Advanced Technology (IJEAT), 269-275

[69] Hasbullah, H., & Soomro, I. A. (2010) Denial of service (DOS) attack and its possible solutions in VANET. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 813-817

7. Communication resilience

Communication networks are facing a large group of challenges, especially for vehicular communication networks. It is essential to recognise, which is crucial for network design and planning. The difficulties for communication networks are large-scale disasters, Socio-Political and Economic Challenges, dependent failures, human errors, malicious attacks, unusual traffic, and environmental challenges[70] .

7.1. Introduction of Communication Resilience

7.1.1. Challenges of Communications Networks

Large-Scale Disasters are usually caused by natural disasters, including earthquakes or hurricanes, and pandemics. They significantly disrupt communication networks. Typically, they are communication hardware facilities failures. Another source of large-scale disasters is human activity.

Socio-Political and Economic Challenges include voluntary activities (also acts of terrorism) aimed at disrupting the regular network operation, e.g. as a response to political decisions or to achieve advantage on economic markets.

Dependent Failures refer to challenges that may result in a cascade of failures, for instance, after a failure of a system (or its part) offering service to another network. Examples include power grids providing power supply for the Internet.

- *Non-malicious human activities imply human Error*s. They include, e.g., misconfiguration errors being a result of incompetence. Consequently, communication networks may even encounter catastrophic failures.
- *Malicious Attacks* is another group of challenges referring to deliberate actions designed to cause as much disruption as possible, commonly by being targeted at an essential software/hardware element of the network infrastructure.
- *Unusual Traffic* can be a problem if its volume exceeds the upper design limit of the network. If such additional traffic can be inserted into the network, e.g., after the occurrence of a catastrophic event not necessarily disrupting the network infrastructure itself, but, resulting in a significant increase of several simultaneous requests to get information. This can result in significant issues for Network Service restoration.
- *Environmental Challenges* are in turn dependent on communication environment characteristics. They are related, e.g., to mobility aspects in ad-hoc wireless networks (and in particular to time-dependent characteristics of wireless links).

Based on the research[71], network challenges can be categorised based on detailed criteria including:

[70] Cetinkaya, E.K., Sterbenz, J.P.G. (2013) A taxonomy of network challenges. In: Proc. 9th International Conference on Design of Reliable Communication Networks (DRCN'13), pp. 322–330

[71] Avizienis, A., Laprie, J.-C., Randell, B. (2014) Dependability and its threats: a taxonomy. In: Jacquart, R. (ed.) Building the information society, vol. 156, IFIP International Federation for Information Processing, pp. 91–120. Springer, New York

- **cause** - natural, human-made, or challenge-dependent;
- **boundaries** - internal, or external;
- **target** - direct, or collateral;
- **objective** - non-malicious, selfish, or malicious;
- **intent** - non-deliberate, or deliberate;
- **capability** - accidental, or incompetence;
- **dimension** - hardware, software, protocols, or traffic;
- **domain** - medium, mobility, delay, or energy;
- **scope** - nodes, links, or area;
- **significance** - minor, major, or catastrophic;
- **persistence** - short-lived, long-lived, or transient;
- **repetition** - single, multiple, or adaptive.

7.1.2. Disciplines of Communications Resilience

It is difficult to identify real-time communication network challenges. A multi-stage approach is used to recognise those challenges[72], Figure 17. It includes detection of challenge symptoms (i.e., that may lead to recognition of a challenge onset), identification of the root cause of a challenge, and determination of a potential impact on the system. Challenge detection mechanisms, typically invoked in a distributed manner, should be as lightweight as possible in order not to use resources unnecessarily (which is an essential requirement for resource-limited networks), and not to disturb the system's regular operation.

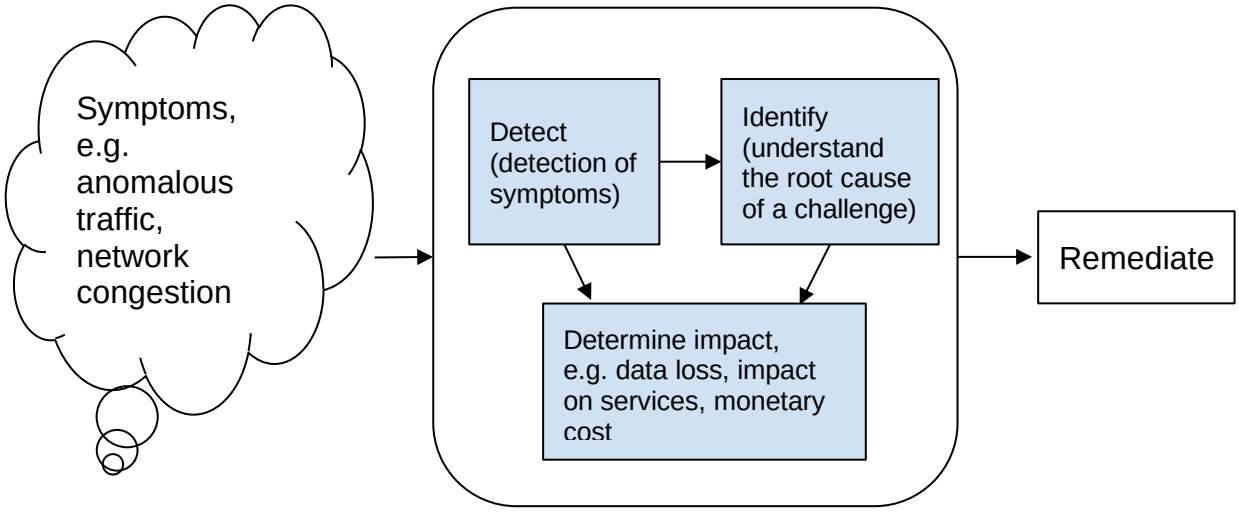


Figure 17. Aspects of challenge identification

For any challenge, apart from evaluating its impact on communication network performance, it is crucial to identify the probability of a challenge occurrence (P_c), as well as the probability of a particular challenge which results in a fault (P_f). The two measures combined with information on the challenge impact Ican be used to derive the ratio of network resources exposure E to disruptions.

$$E = (P_c \times P_f) \times I$$

[72] Fry, M., Fischer, M., Karaliopoulos, M., Smith, P., Hutchison, D. (2010) Challenge identification for network resilience. In: Proc. 6th EURO-NF Conference on Next Generation Internet (NGI'10), pp. 1–8

A fault, if not adequately dealt with, can next cause an error, defined as a deviation between the observed value/state and its specified (correct) value/state. If the error propagates, it may result in a service failure.

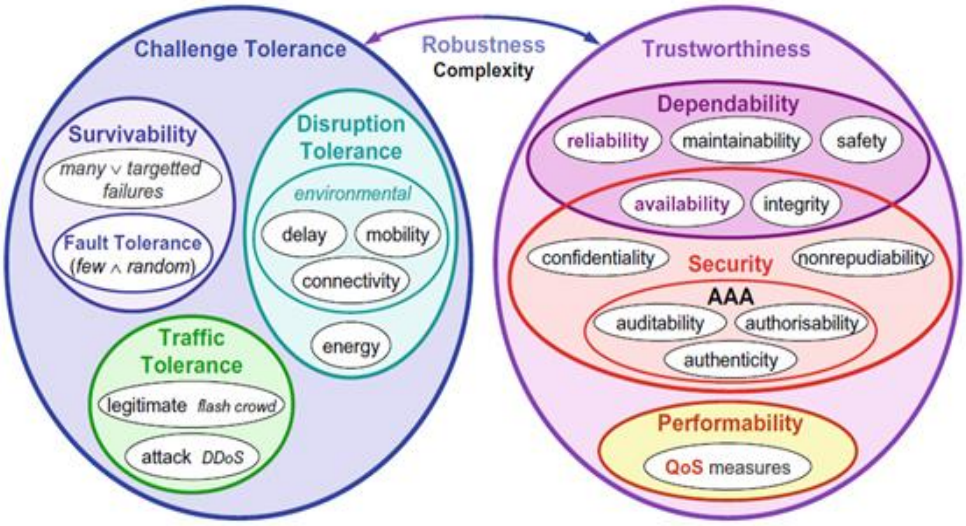


Figure 18. Resilience disciplines

Network resilience is the ability of a network to provide and maintain an acceptable level of service in the face of various faults and challenges to regular operation of the network. Since faults and challenges are inevitable, network resilience should be viewed as one of the most important characteristics of a communication networks design.

Mobile network operators typically offer a service level agreement of between 96% to 97% availability translating to around 2-hour a week of network downtime. It should be noted that these are not global network outages that affects all customers of the network but are mainly an aggregation of clusters of downtime that are localised, affecting subsets of customers. Some of the network outages are planned outages that may be communicated to customers in advanced and are required in order to conduct essential maintenance works such as software upgrades, feature integration, optimisation and fault resolution. These are usually done at times when the network usage is predicted to be at its lowest peak, for example in the early hours of the morning. The effect of these planned outages is therefore not acutely experienced by the mobile network subscribers.

A typical classification of resilience disciplines[73] is shown in Figure 18. Resilience disciplines can be classified into two main categories: *challenge tolerance* focusing on network design and approaches to provide service continuity in the presence of challenges, and *trustworthiness* describing measurable characteristics of analysed communication systems. The relation between challenge tolerance and trustworthiness is the indicator of the performance of a network under perturbative conditions.

[73] Sterbenz, J.P.G., Hutchison, D., Cetinkaya, E.K., Jabbar, A., Rohrer, J.P., Sch€oller, M., Smith, P. (2010) Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Comput. Netw. 54(8), 1245–1265

Survivability is the ability of a network to recover the affected traffic in failure environments and to provide different services continuously[74]. It refers to the ability of automatically reacting to both physical and software faults by redirecting the traffic from the affected routes to ones which are operating correctly[75] .

The scope of survivability is broader than fault tolerance and comprises issues of correlated failures for unbounded networks[76], e.g., failures due to malicious human activities (attacks) or failures of large parts of a communication network infrastructure[77].

Fault Tolerance is the ability of a network which tolerates faults but does not result in service failures[78]. It is relying on network redundancy to compensate for unexpected and uncorrelated failures of system components. However, fault tolerance is not sufficient to provide recovery after multiple correlated failures, and therefore, it is considered as a subset of survivability.

Another significant type of challenge that is unique to communication networks is to maintain stable end-to-end connections between users.

Disruption Tolerance is the ability of a system to tolerate disruptions in connectivity among its components[79] . This connectivity is measured in terms of communication channel characteristics, and may be affected due to environmental challenges including, e.g., weak and episodic channel connectivity, node mobility, unpredictably long delay, and signalling power challenges[80].

Traffic Tolerance is the ability of the network system to tolerate the unexpected communication traffic load[79]. High traffic volume is a big challenge of wireless communication because of the resource-constrained environments. If the communicating demand amount rises far beyond the network design assumptions for the normal operational state, the network services will possibly fail. Examples of this scenario include either legitimate activities such as flash crowd following natural disasters like earthquakes implying the need to get the relevant information or e.g., malicious actions like DDoS attacks[81].

[74] Haider, A., Harris, R. (2004) Recovery techniques in Next Generation Networks. IEEE Commun. Surv. Tutorials 9(3), 2–17
[75] Chołda, P., Jajszczyk, A. (2010) Recovery and its quality in multilayer networks. IEEE/OSA J. Lightwave Technol. 28(4), 372–389
[76] Mukherjee, B., Habib, M.F., Dikbiyik, F. (2014) Network adaptability from disaster disruptions and cascading failures. IEEE Commun. Mag. 52(5), 230–238
[77] Neumayer, S., Zussman, G., Cohen, R., Modiano, E. (2011) Assessing the vulnerability of the fiber infrastructure to disasters. IEEE/ACM Trans. Networking 19(6), 1610–1623
[78] T1A1.2 Working Group (2004) Reliability-related metrics and terminology for network elements in evolving communication networks. American National Standard for Telecommunications T1. R1.524-2004, Alliance for Telecommunications Industry Solutions – ATIS
[79] Sterbenz, J.P.G., Hutchison, D., Cetinkaya, E.K., Jabbar, A., Rohrer, J.P., Sch€oller, M., Smith, P. (2010) Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Comput. Netw. 54(8), 1245–1265
[80] Khabbaz, M.J., Assi, C.M., Fawaz, W.F. (2004) Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. IEEE Commun. Surv. Tutorials 14(2), 607–640 (2012)
[81] Ho, P.-H.: State of the art progress in developing survivable routing schemes in mesh WDM networks. IEEE Commun. Surv. Tutorials 6(4), 2–16

Trustworthiness is the ability of a network to assure the system will perform as the purpose of design. The trustworthiness disciplines measure the service delivery of a network, which includes (1) dependability, (2) security, and (3) performability.

Table 9 presents the selected sets of resilience characteristics defined by ITU-T and IETF for communication networks. From the client perspective, the essential resilience characteristics are related to the perceived service quality (QoS), referred to as the Quality of Resilience (QoR) features, being the QoS characteristics related to resilience observed by the end-users[82].

[82] Chołda, P., Mykkeltveit, A., Helvik, B.E., Wittner, O.J., Jajszczyk, A. (2007) A survey of resilience differentiation frameworks in communication networks. IEEE Commun. Surv. Tutorials 9(4), 32–55

Table 9. Measurable metrics for resilience quantification[83]

Recommendations of International Telecommunication Union – Telecommunication Standardisation Sector (ITU-T)		
ID	**Area**	**Metric**
E.800 E.802 E.820 E.850 E.855 E.860 E.862 E.880	General (e.g., Internet access), ISDN telephone network	• Retainability • (Mean) time between interruptions (MTBI) • Down time (MDT), up time (MUT) • Instantaneous (un)availability, steady-state/asymptotic (un)availability (U/A) • Reliability function (R(t)) • Time to failure (MTTF) • Time between failures (MTBF) • Time to recovery (MTTR) • p-fractile repair time • Failure/repair rate • Probability of fault coverage
G.911	Fibre optic systems	• Median life – a value on a lognormal probability plot of time to failure at which 50 % of the devices fail earlier and 50 % of the devices fail later • Standard deviation – a value of a standard deviation concerning the natural logarithms of the time to failure • FIT: number of failures per billion device hours
Y.1540 Y.1541 Y.1542	IP	• IPLR: “ratio of total lost IP packet outcomes to total transmitted IP packets in a population of interest” • Service availability: “classifies the total scheduled service time for an IP service into available and unavailable periods,” using the threshold on IPLR • PIU/PIA: “percentage of total scheduled IP service time categorised as (un)available using the IP service availability function”
P.10	General telephone network	• MOS is a subjective measurement of the quality. It is used in a survey-based studies when a service is tested by users • QoE: “overall acceptability of an application or service, as perceived subjectively by the end user”
3386	Multilayer networks	• Protection switch time: “time interval from the occurrence of a network fault until the completion of the protection-switching operations” • Restoration time: “time interval from the occurrence of a network fault to the instant when the affected traffic is either completely restored, or until spare resources are exhausted, or no more extra traffic exists” • Definitions show the difference in the approaches of ITU-T and IETF, where the former is more general, and the latter more focused on particular methods

[83] 12. Chołda, P., Tapolcai, J., Cinkler, T., Wajda, K., Jajszczyk, A. (2007) Quality of Resilience as a network reliability characterization tool. IEEE Netw. 23(2), 11–19 (2009)

7.1.3. Existing Approaches of Communication Resilience

To recover communication services continuity after failures, communication capacity redundancy (mostly related to link bandwidth) is a commonly reserved method in a network. It provides the possibility of an alternate communication path with the primary communication link failing[84]. In general, the higher the capacity to be protected, then the more significant the task to protect the network from failures.

After a failure occurs, the recovery process starts with the detection of a failure. Which is followed by fault localisation and, or, isolation (i.e. determination of the faulty node/link), which is necessary to stop further transmission of information via the affected element that should be repaired[85]. Before the recovery actions, a failure notification message is sent to network nodes. Two processes are taking place at this stage:

1. The repair process, which is related to the repair of the faulty element.
2. The recovery process is to identify the affected traffic, localize the failure, and determine the alternate path for the communication data redelivery.

Ideally, the recovery time, which is defined as the time needed to switch the traffic to backup paths, should not be longer than 50ms. Because shorter than 50ms it would be treated as a transmission error by the higher network layers. Any confusion longer than 50ms results at least in packet losses, or unavailability of service[86]. A detailed classification of time outages is given in Table 10[87].

[84] Ho, P.-H. (2004) State of the art progress in developing survivable routing schemes in mesh WDM networks. IEEE Commun. Surv. Tutorials 6(4), 2–16

[85] 10. Chołda, P., Jajszczyk, A. (2010) Recovery and its quality in multilayer networks. IEEE/OSA J. Lightwave Technol. 28(4), 372–389

[86] 60. Ramamurthy, B., Sahasrabuddhe, L., Mukherjee, B. (2003) Survivable WDM mesh networks. IEEE/ OSA J. Lightwave Technol. 21(4), 870–883

[87] 22. Grover, W.D. (2004) Mesh-based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Prentice Hall PTR, Upper Saddle River

Table 10. Impacts of outage time

Target range	Duration	Main effects
Protection switching	t≤50 ms	No outage logged; recovery of Transmission Control Protocol (TCP) after one errored frame; no TCP fallback; no impact at all for most TCP sessions.
1st type outage	50ms≤t<0.2s	<5 % voiceband disconnects; signalling system switchovers.
2nd type outage	0.2s<t<2s	Common upper bound on distributed mesh restoration time: TCP/IP protocol back-off.
3rd type outage	2<t<10s	Disconnections of all switched circuit services; disconnections of private lines; TCP sessions time-outs; Hello protocol affection; web page “not available” errors.
4th type outage	10<t<5 m	All calls and data sessions terminated; timeouts of TCP/IP application layer programs; users making attempts of mass redials; link state advertisements (LSAs) sent by routers referring to failed links; updates of topology and resynchronisation network wide.
Undesirable outage	5m<t<30m	Massive reattempts causing heavy load of switches; noticeable Internet “brownout”; minor societal/business effects.
Unacceptable outage	t>30m	Major societal impacts (societal risks: travel booking, impact on all markets); headline news; regulatory reporting often required; lawsuits; SLA clauses triggered.

Based on the structure of communication networks, the existing approaches to communication resilience can be classified as ring-based and mesh-based. The ring-based methods refer to architectures introduced, e.g. Synchronous Optical Networks Synchronous Digital Hierarchy (SONET/ SDH)[88] and the early architectures of ring Dense Wavelength Division Multiplexing (DWDM) networks[89]. Based on flow direction, ring networks may be classified as unidirectional, or bidirectional, accordingly. As shown in Figure 19, both working and backup routes in ring networks are organized in rings.

[88] Siller, C.A., Shafi, M. (1996) Synchronous Networking. IEEE Press, IEEE Communications Society, New York

[89] Mukherjee, B. (2006) Optical WDM Networks. Springer, New York

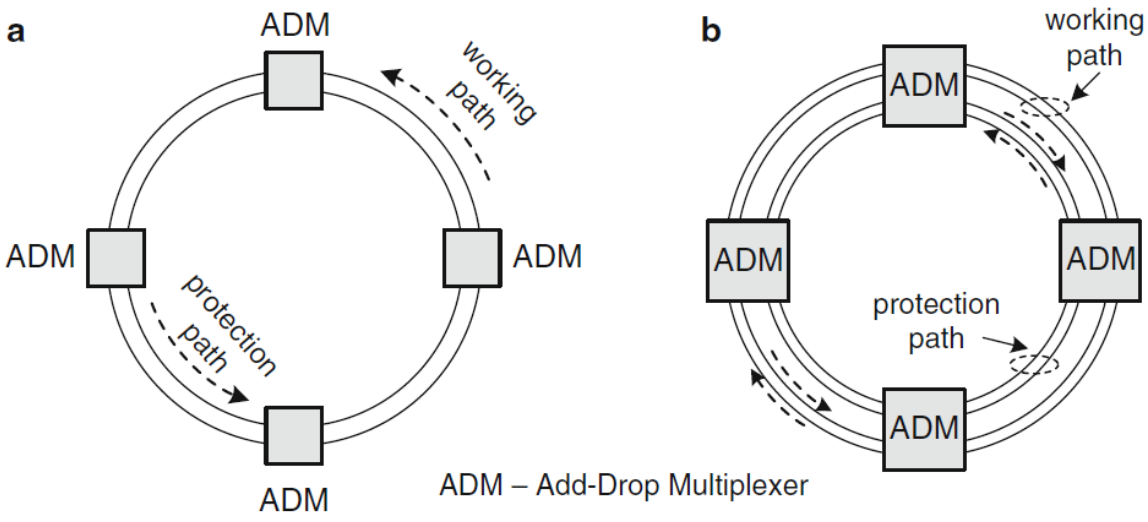


Figure 19. Example of Unidirectional Path-Switched Ring (UPSR) and Bi-directional Line Switched Ring (BLSR) with Add-Drop Multiplexers (ADMs)

7.2. Public Road Communications Resilience

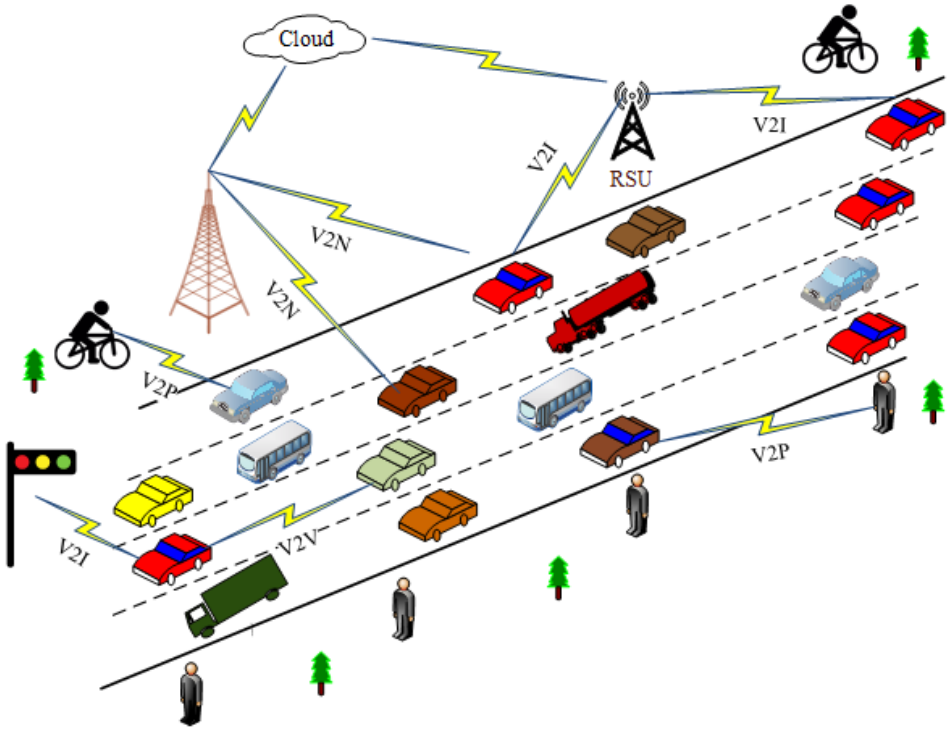


Figure 20. Vehicular communication networks with multiple paths of V2I and V2C

Vehicular communication networks provide for a wide range of applications designed to solve several problems related to:

Public Safety. Road safety can be improved by messages exchanged by vehicles, e.g., in the case of accidents/collisions, bad weather conditions (ice/water on the road) unexpected events (e.g., low bridges, oil on the road), or to assist the drivers in lane change/overtaking operations.

Traffic Information. V2X and C-V2X can be utilised to provide traffic monitoring/ shaping (including traffic light management), i.e., aimed at adjusting the scheduling of traffic lights to

help the drivers move in the green phase, thus also contributing to the reduction of environmental pollution.

Infotainment. Providing travellers with on-board information and entertainment services such as Internet access or music download.

So, vehicle communication can be divided into Public Road Safety Communications Resilience and ad-hoc vehicular communications Resilience.

Vehicular networks provide communications for a wide range of applications, as shown in Figure 20, public road communication includes V2N, V2I and C-V2X.

7.2.1. Understand Public Communications Resiliency

Communications resilience is that networks can recover from damage, accident or attack, hereby minimising the possibility of the service outage. There are three key elements of communications resilience[90]:

1. **Route Diversity**. Route diversity is defined as routing communications between two vehicles over more than one physical path (RF communication channels). As shown in Figure.6.4 vehicles can upload and download data to the cloud via V2N and V2I. Meanwhile, vehicles can act as a relay to communicate with infrastructure by V2V.
2. **Redundancy**. Redundancy means that additional or duplicate communications assets share the load or provide back-up to the primary asset. In the purpose of resilience, network redundancy means dedicated resource blocks (RB) for the recovery or emergency communication use only.
3. **Protective/Restorative Measures**. Protective measures decline the probability that a threat will affect the network, while therapeutic measures enable rapid restoration if commercial services are lost or congested.

7.2.2. Network Failure Management

Network failure management includes: Fault detection, Fault localization, and Fault notification[91].

1. **Fault Detection.** Parameters and counters can be used to detect the communication network failure at different network layers.
    - *Physical layer:* signal loss, modulation loss and synchronous clock loss.
    - *Signal strength:* the signal deterioration at the receiver side during the specified period; it can be detected from Signal-to-Interference Plus Noise Ratio (SINR), channel BER, the dispersion level, the crosstalk, or the attenuation level.
    - *Service Quality:* Package loss ratio, channel throughput or package delays, etc.
2. **Fault Localisation**. During fault localisation, where the failure occurred is determined, i.e., a faulty item is recognised.

[90]https://www.dhs.gov/safecom/blog/2018/02/07/public-safety-communications-resiliency-ten-keys-obtaining-resilient-local

[91] D. Papadimitriou and E. Mannie, Eds. (2006) 'Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based Recovery Mechanism (including Protection and Restoration)', IETF RFC 4428

3. **Fault Notification.** Fault notification is used to inform the control centre that there was a failure in the network. This triggers the appropriate procedures to resolve the fault quickly and try to prevent it happening in the future, if possible.

7.2.3. Cost of Resilience

The cost of a recovery is very important for the operator and should be taken into consideration as an important factor to determine the different resilience methods based on several parameters.

Generally, the most direct way is to base it on the network redundancy for resilience, such as the extra network resource usage for supporting the specific recovery method. Normally, it is the dedicated resource blocks (RB). There are some other elements to measure the cost of communication resilience, e.g., additional software, the increased Operational Expenditures (OPEX) related to the new staff or higher expenses on device operation[92].

7.2.4. Ad-hoc Vehicular Communications Resilience

Vehicular communications can be provided either without or with the support of a roadside infrastructure, also referred to as *vehicle-to-vehicle* (V2V) and *vehicle-to-infrastructure* (V2I) wireless networking. Based on data travel via vehicles the V2V communication can be classified as either: (1) single hop (sender to receiver directly), or (2) multi-hop V2V (between sender to receiver there are vehicles acting as relays.)

The advanced applications of intelligent transportation systems require both reliable and low-latency communication. An example is road safety warning (e.g. related to collision warning or traffic coordination issues). If the information delay is high, it may increase risk to human life or injury.

7.2.5. Reliability Requirements of V2V Communication

The V2V communication can be considered as self-organising, self-optimizing, and with a short transmission range.

- *Dynamic network topology*: with frequent topology changes resulting in common path unavailability, or even causing network disconnections/partitioning.
- *A relatively sufficient resource of energy and data storage.* Compared with other mobile communication devices (mobile phone, pads), vehicles have higher energy and data storage.
- *Geographic-based message distribution* provides fast dissemination of time-critical information to other vehicles.
- *Strict data delay requirement*, because of the safety applications.

The categories of safety applications are identified by the Vehicle Safety Communications Consortium (VSCC)[93]. Safety applications require low delay communications because the

[92] H. Lønsethagen, A. Solem, and B. Olsen (2005) 'Feasibility of Bandwidth on Demand. Case Study Approach, Models and Issues' EU FP6 IP IST-NOBEL Project internal presentation, Sept. 19–21.
[93] Delgrossi, Luca, and Tao Zhang (2012) 'Vehicle safety communications: protocols, security, and privacy', Vol. 103

validity of information (e.g., post-crash warnings) expire very fast, and any such delayed information shortly may shortly become useless for surrounding vehicles. Therefore,100ms is the maximum latency of safety message delivery, while 10 Hz is the minimum frequency of message exchange.

Safety-related notifications can be either event-driven or periodic. Event-driven messages are disseminated after identification of an event[94]. Safety applications data is normally a one-hop broadcasting communication. it should be to send out safety-related messages over 150m by one-hop broadcasting. In the case of multi-hop distribution of safety messages. The total coverage distance of safety applications is in the range between 300 m and 20 km[95]. The requirement of non-safety applications is shown in Table 6.3.

Table 11.Classification of non-safety applications

Categories	Applications	Frequency (Hz)	Latency (ms)
Traffic efficiency	Enhanced route guidance and navigation	10	<100
	Green light optimal speed advisory	10	<100
	V2V merging assistance	10	<100
Infotainment	Internet access in vehicle	1	<500
	Point of interest notification	1	<500
	Remote diagnostics	1	<500

7.2.6. Resilience of End-to-End V2V Communications

The three elements of end to end V2V communication resilience are: (1) communications path stability, (2) multipath routing.

Network Path Stability. The main factor for measuring the V2V network path stability is the path outage probability. An outage occurs if data from the source vehicle cannot reach the destination vehicle. Specifically, the transmission vehicle fails to find the destination vehicle within the vehicle's maximum communication range. The maximum communication range is defined as the range that both the receiver signal level and signal quality SINR is higher than a required Quality-of-Service (QoS) threshold.

The approach of enhancing the network capacity is to decrease the network outage probability. For example, in a single-hop network, usually one can increase the

[94] Vijayakumar, Pandi, Victor Chang, L. Jegatha Deborah, Balamurugan Balusamy, and P. G. Shynu (2018) 'Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks' Future generation computer systems 78, 943-955.
[95] ETSITR102638 (June 2019) Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Definition, ETSI Std. ETSI ITS, Specification TR 102 638

transmission power to increase the communication rang. However, this can increase the interference to other co-frequency users.

Multipath Routing. It improves the reliability of end-to-end transmission, and multipath routing can transmit information via a multiple hop relay network. Additionally, multipath routing can also improve network throughput, load balancing, and packet delivery ratio. However, multipath can cause a data delay because of the longer transmission path and relay processing. The multipath routing is suitable for the delay-tolerant service. Such as V2V store-carry-forward (SCF) network[96].

In recent years store-carry-forward (SCF) relaying has received attention for its potential to deliver extra mobile capacity for delay-tolerant data delivery. The principle idea is to transmit data close to the intended destination by physically carrying the data packets across most of the original transmission distance. It has been shown that it can lead to higher energy efficiency for transmission. What has been lacking, however, is the design of route selection algorithms that are optimised and efficient for application in large scale urban simulations, using real vehicular traffic, to examine performance trade-offs.

7.3. User Case Analysis for Communication Resilience

One of the defining trends of our century is the rapid urbanisation in both developed and developing worlds. Across the planet, more than 50% of the population is now living in cities, and this is set to rise rapidly over the next decade. Modern cities are partly defined by a high population density and high mobile devices usage (includes mobile vehicles). Therefore, there is an opportunity to achieve multi-hop communications between users. One of the critical challenges global cities face is security from terror attacks. Terrorist attacks generally target dense urban areas to deliver the greatest casualty and a high impact. In the event of such an attack, such as the 9/11 attack in New York City and the 7/7 bombing in London, the mobile networks became overloaded due to the increase phone and date usage. This is typically managed by implementing a class access bar for emergency services, meaning that critical communication can still take place.

[96] Yuan, H., Maple, C. and Ghirardello, K. (2018) August. Dynamic route selection for vehicular store-carry-forward networks and misbehaviour vehicles analysis. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)* (pp. 1-5). IEEE.

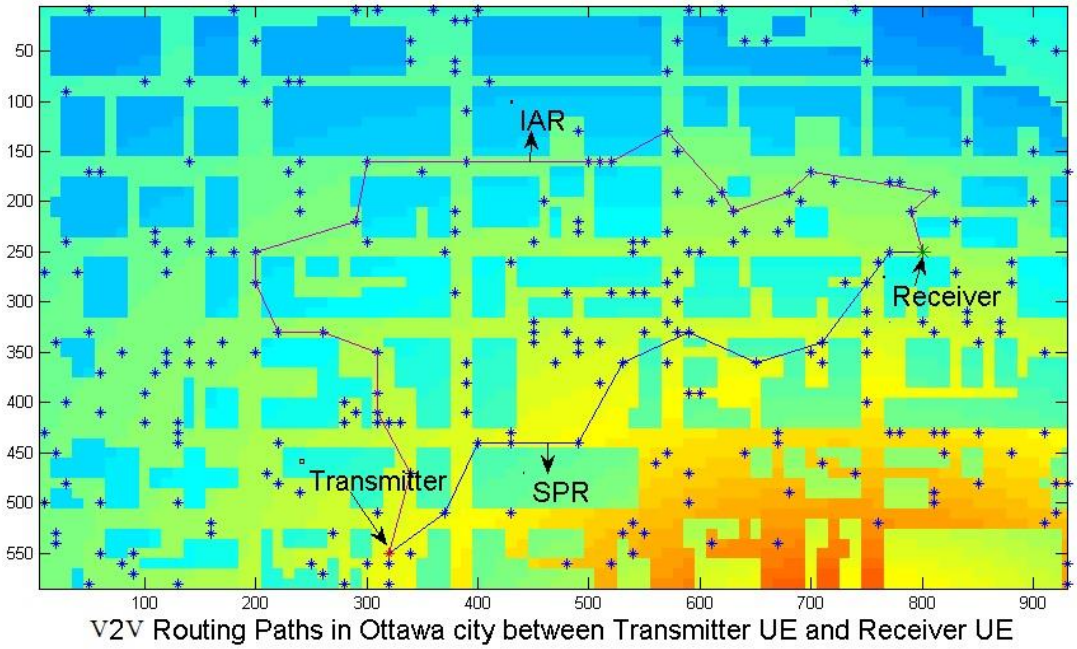


Figure 21. A simulation of V2V emergency communication under terrorist attack

7.3.1. Emergency V2V Communications Under Terrorist Attack

In this section, the use case scenario is that the public access network is under attack, and we lose some access points such as RSU or BS. It should be stated that O2's vision for C-V2X, would not provide V2V communication via RSUs, but rather directly vehicle-to-vehicle, negating the need of the RSU. In this situation, the communication network is fully loaded with data traffic, and a large set of vehicles and users are seeking alternative ways to relay vital data. Peer assistance V2V communication is a way of allowing vehicles to act as relays for each other[97]. The RSUs of the C-V2X network are then not required for data-bearing channels or to serve as a coordinator or facilitator to V2V channels.

In Figure 21, it is a use case that shows the communication resilience of V2V communication in an urban environment under terrorist attack. In this case, two V2V routing algorithms are addressed, the shortest path routing (SPR), which is a greedy path selection algorithm. SPR seeks to minimise the total multi-hop distance or the number of hops in order to improve the multi-hop V2V transmission reliability. In SPR, each V2V knows its location and that of the destination user. Each UE that holds the message will first identify the UEs to which it can reliably transmit and then transmit to the one that is closest to the destination UE.

The other routing algorithm is Interference Avoidance Routing. While algorithms such as SPR can yield reasonable performance and minimise the delay, it may not always yield the best reliability performance. This is because when cross-tier interference between conventional communication (CC) and V2V transmissions is considered, selecting the shortest path is not always the optimal strategy.

[97] Yuan, Hu, Weisi Guo, and Siyi Wang (2014) "Emergency route selection for D2D cellular communications during an urban terrorist attack." In 2014 IEEE International Conference on Communications Workshops (ICC), pp. 237-242. IEEE

Cross-tier interference is the lowest when the V2V transmissions occur at the RSU coverage boundary (cell edge). An edge routing path would reduce the V2V interference to CC transmissions in the uplink (UL) band and would reduce the CC interference to V2V transmissions using the downlink (DL) band. The interference avoidance routing (IAR) algorithm tends to migrate along the cell edge in order to trade off a longer route for reduced interference.

7.3.2. V2V Resilience Performance under CC Constraint

One of the key advantages of IAR routing over SPR routing is that it reduces the interference emitted to regular CC UEs. By picking a routing path that travels predominantly along the traditional coverage edge, it maximises the distance to the majority of CC UEs. The paper now expands the IAR routing to both consider uplink (UL) and downlink (DL) bands.

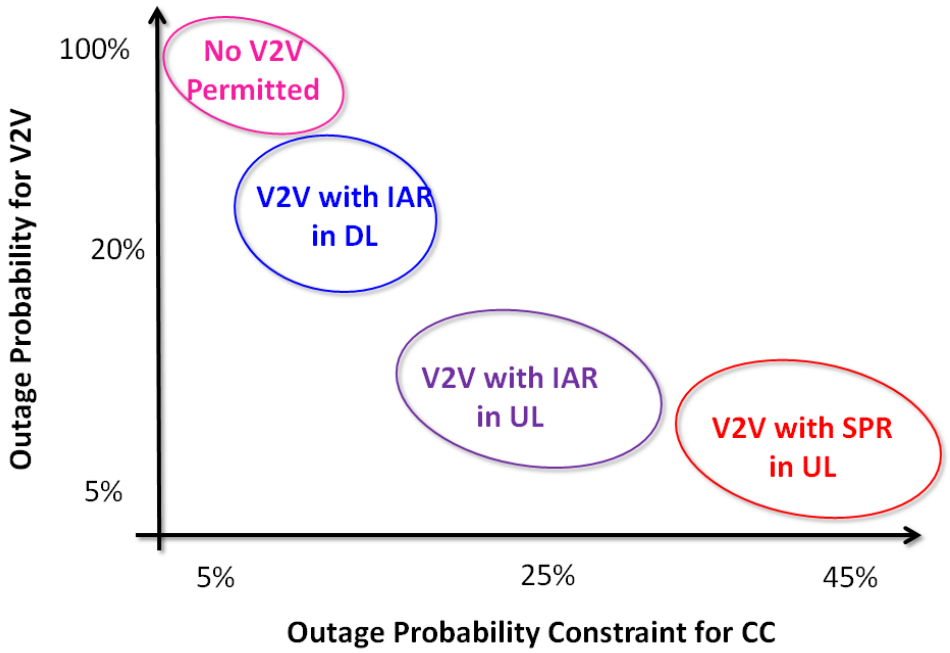


Figure 22. V2V outage probability for various CC outage constraints

Figure 22 shows the V2V outage probability for various CC outage constraints. The results show that there is an intuitive trade-off in outage probability between CC and V2V UEs. For a stringent CC outage constraint, V2V transmission is not permitted. As the CC constraint gets relaxed, the V2V routing method changes from IAR to SPR, and from the DL to the UL band. More specifically, the results show that for:

- CC outage constraint <5%: no V2V is permitted;
- CC outage constraint <12%: V2V using IAR in DL can achieve the lowest outage probability of 20%;
- CC outage constraint <15%: V2V using IAR in UL can achieve the lowest outage probability of 8%;
- CC outage constraint <40%: V2V using SPR in UL can achieve the lowest outage probability of 3%;

There is an intuitive trade-off in outage probability between CC and V2V, what has been improved is that by dynamically selecting the V2V routing method and transmission band, the V2V outage can be minimised. The V2V transmit band that causes the least interference to CC is the DL band, but the V2V outage is reasonably high. As the outage constraint is relaxed in CC, there is a shift from interference aware transmit band and routing paths, to the shortest path in UL band.

8. Introduction to Mobile Network Security

8.1. Introduction

1st and 2nd generation of mobile communications systems and their networks were not designed and implemented with security considerations as a major focus. Although today 2G, with improvements from later releases over time, is now considered to be extremely robust. This approach was mainly based on the "security through obscurity" paradigm wherein it was believed that if the algorithms used in the implementation of the mobile network technologies were kept secret, then the security of the system was assured as no one outside of the implementation group will have the requisite technical know-how to break the system. Of course, this assumption was flawed as evidenced by the recorded number of successful attacks on the TACs system.

The job to ensure that future mobile networks evolved to have better security measures, that user communications remained private, and the ability to compromise the system and disrupt services was limited, would fall to the standards body 3GPP and its members. Designing this type of security into the fabric of the network from the ground up was better known as "Carrier Grade" security.

8.2. Evolution of Mobile Network Security

The standardisation consortium responsible for implementing GSM (one of the 2G technical options) was the European Telecommunications Standards Institute (ETSI). However, the initial standards did not produce strong enough security capabilities. It became obvious that additional security measures were needed. The standardisation framework specified the following features that had to be supported by both the mobile devices and base stations, as a standard requirement in any public GSM mobile network:

- Confidentiality and authentication of the International Mobile Subscriber Identity (IMSI), i.e. the subscribers.
- Data confidentiality along physical connections (i.e. secured and encrypted).
- Data confidentiality for connectionless users.
- Data confidentiality for signalling (i.e. signal integrity)

When 3G was introduced, it provided improved security features as well as high data rates, while also providing much higher network capacities. 3G mobile networks were the first to implement "Carrier Grade security" and this differentiated them from the previous generation.

Before improvement, some of the known GSM security vulnerabilities at that time included:

- Fake base station set up by attackers for eavesdropping.
- Unsecured International Mobile Equipment Identity (IMEI).
- Lack of built-in flexibility in the system to upgrade security and functionality easily.

The new standard for 3G “Carrier Grade” security was set out with the following objectives:

- All user information must be protected against 3rd party access, misuse or theft.
- Networks and home environments must have their resources protected against misuse or theft.
- Security must be standardised and compatible worldwide, as well as allowing roaming and interoperability within these security standards.
- There should be a mechanism to allow for security to be improved in a flexible manner as new threats arise.

As mobile networks were becoming more IP oriented, a whole new group of threats to the new generations of mobile such as 4G and 5G were introduced. This was addressed by developing security from the ground up and would be known as Carrier Grade security. Figure 7 provides an overview of a generic mobile network security interactions and interfaces from the SIM inside a UE to the Mobile Core Network and beyond for current day 2G, 3G, 4G & 5G networks.

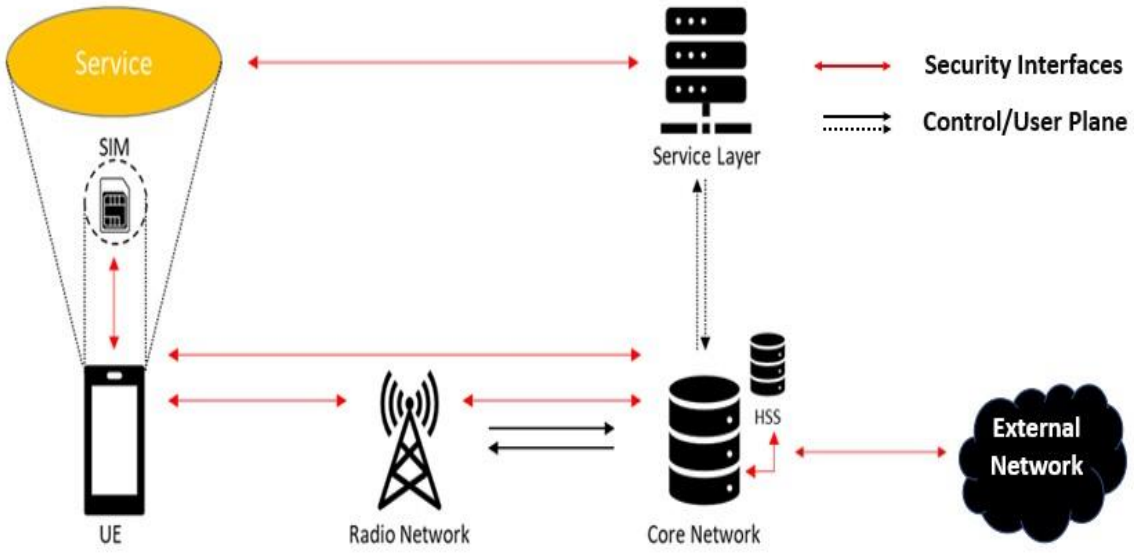


Figure 23. Generalised mobile network security interfaces

8.3. Overview of 3GPP 5G Security Features

3GPP 5G security is principally defined in 3GPP TS 33.501 and takes a very-much enhanced view of the need for security mitigation and mechanisms through its bottom-up consideration in standards. The high-level architecture for 5G security is depicted in Figure 24.

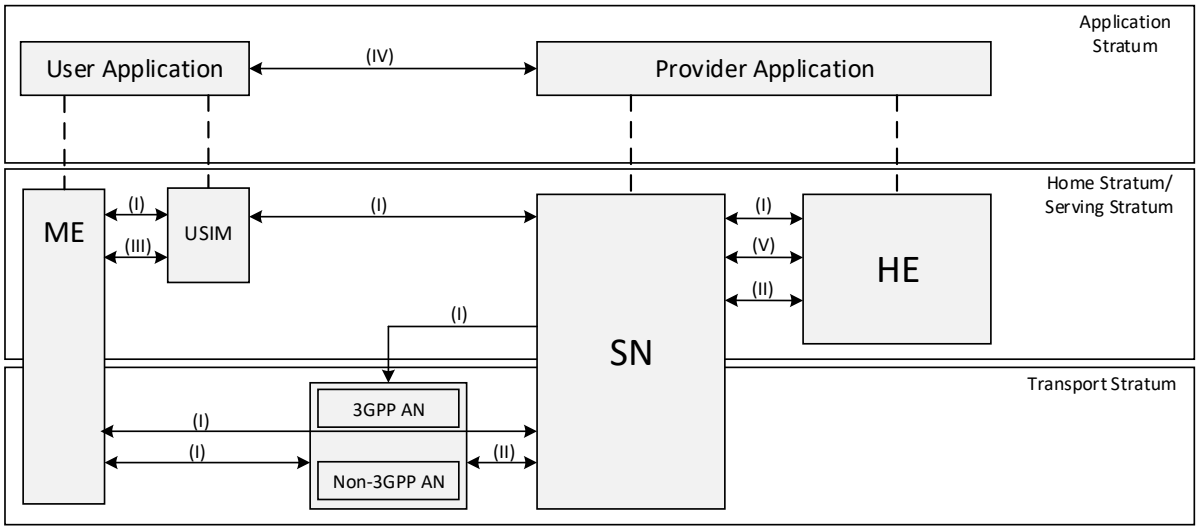


Figure 24. 3GPP security architecture, where ME=Mobile Equipment, USIM=Universal Subscriber Identity Module, AN=Access Node, SN=Serving Network

The domains and features highlighted in Figure 8, as taken from 3GPP TS 33.501, are outlined in detail below:

- **Network access security (I):** The set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from the Serving Network (SN) to the Access Network (AN) for the access security.
- **Network domain security (II):** The set of security features that enable network nodes to securely exchange signalling data and user plane data.
- **User domain security (III):** The set of security features that secure the user access to mobile equipment.
- **Application domain security (IV):** The set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.
- **Service-Based Architecture (SBA) domain security (V):** The set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorisation security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to 3GPP TS 33.401 which is the technical security specification for the preceding LTE, 3G and GSM generations standardized by 3GPP.
- **Visibility and configurability of security (VI):** The set of features that enable the user to be informed whether a security feature is in operation or not.

8.4. Security in the Context of CAVs

Cars are continually incorporating more software and becoming more connected. This opens them up to increased risks of cyber security attacks. At present, cars have more than 100 types of Engine Control Units (ECUs) and more than 100 million lines of code which provides a massive attack surface for hackers.

Hackers can exploit and gain access to any vulnerabilities in the system such as any exploitable vulnerabilities in the Bluetooth interface for example, to take control of critical core

ECUs which controls brakes or engine functionality. Attackers can then pose very serious security threats such as the ability to disable a vehicle's brakes or steering functions, shut down the vehicle's engine, or manipulate other on-board systems through DoS and other forms of attacks. However, this is may be mitigated using two data buses; one for information and connection to outside world, and another for critical control systems such as brakes and steering with no connection to the outside world without a direct cable connection. Access to this system is gained via a secure gateway or similar device.

The addition of any connected component to support vehicle infotainment systems, maintenance monitoring, and other systems increases cyber security vulnerabilities. In connected and autonomous vehicle systems, the elements or interfaces that may be exploited include:

- Sensors.
- Vehicle Communications Networks.
- Hardware components (e.g., control units).
- Software systems.

Sensors can be exploited by jamming or giving them incorrect signals. For example, with the Light Detection and Ranging System (LiDAR), a laser tuned to the correct wavelength directed at the vehicle will jam the LiDAR and cause it to stop. With Global Positioning Systems (GPS), a simple software defined radio can be used to project incorrect location information causing the vehicle to take a completely different path compared to its intended or actual path.

Vehicle communications networks can be used to enable communications between vehicles using Wi-Fi or DSRC networks, as well as other personal devices using the mobile network. This means that the vulnerabilities in the smartphone connectivity interface and data flows, such as certain elements in the LTE protocol, can be exploited to monitor the communications and information about the vehicle, or to intercept this information and inject incorrect information within the system.

The control units within connected vehicles can be exploited if accessed in a way in which the data they send for diagnostics and feedback can be tampered with. In this situation, a vehicle can then be fed incorrect information that may interfere with its control systems and decision making. This type of vulnerability includes rogue firmware updates delivered to a vehicle to then enable receipt of further compromised updates.

9. Mobile Network Vulnerabilities

9.1. Radio Access Network Security Vulnerabilities

9.1.1. Denial of Service (Registration)

One of the RAN security issues is its susceptibility to DoS attacks[98], which can be used to saturate the resources of the RAN. This is done by sending very high volumes of registration requests to the MSC, which lacks the ability to distinguish between false and

[98] Department of Homeland Security (2017) 'Study on Mobile Device Security'

legitimate requests. As a result, for each request, the MSC will attempt to get an authentication challenge from the HLR, keeping it busy, which will cause genuine requests to be lost in the presence of such a DoS attack[99]. In most modern networks this has now been mitigated.

9.1.2. Denial of Service (Attach)

Attach requests and rejects can be used to block mobile devices at the RAN[99]. This is done using a rogue eNodeB to send a false attach reject message, which tells a mobile device it cannot connect to a legitimate eNodeB, while pretending to be a legitimate eNodeB. This then convinces the mobile device that the nearby legitimate eNodeB has in fact rejected the attempt to connect to it. As a result, the mobile device will not attempt to connect to the legitimate eNodeB again and is therefore denied access to the legitimate services it desires from its mobile network service provider, at least for a certain amount of time[100], or by moving location, or doing a power-off reset.

9.1.3. Eavesdropping

This is done via the SIB (System Information Block) and MIB (Master Information Block) packets. These packets are broadcasted periodically by the base station and contain useful system information such as the mobile operator of the cell, the identity of that cell as well as the power required to trigger handover to that cell. However, these information blocks,-have no form of encryption on them, leaving them open to passive packet sniffing, where the attacker can simply listen in on the data passing through and intercept it without any real effort[101]. Using this information, it is also possible to construct a very convincing fake base station by impersonating a legitimate Mobile Network Operator and using a transmitted power value that will trigger mobile devices to initiate a handover to it. It is also possible to obtain the mapping of important control channels through this method, allowing for more accurate methods of executing a jamming attack, as the attacker now knows where the best locations to jam the mobile network are. However, this will be only a very localised attack, and does make the attacker vulnerable to detection by law enforcement.

9.1.4. IMSI Catcher

The IMSI of a mobile network user is usually kept private but must at some point be used in the communications process and data flow. It is usually transmitted before the encryption and authentication process in the Non-Access Stratum (NAS) functional layer, where the attach process occurs. The NAS is a set of protocols that are used to enable the transfer of non-radio signalling messages between a UE and the Core Network. The vulnerabilities in the protocol stack can be exploited to obtain the IMSI information during the network attach process. The IMSI catcher commonly impersonates a GSM base station so that a mobile device is forced to use low level security which can be used to monitor communications[102],

[99] RadWare. (2013) Mobile Networks Security Research Paper
[100] Altaf Shaik, R. B.-P. (2017) Practical Attacks Against Privacy and Availability in 4G/LTE Communication Systems
[101] Jover, R. P. (2016) LTE Security, protocol exploits and location tracking experimentation with low-cost software radio
[102] Timo Gendrullis, M. N. (2008) A Real-World Attack Breaking A5/1 within Hours

see Figure 25[103]. A method to mitigate this vulnerability is by minimising the transmission of IMSI, which is accomplished by using a Temporary Mobile Subscriber Identity (TMSI). This identifier is shorter than the IMSI number and hence it is more efficient to transmit. However, to be clear, the purpose of using TMSI in place of IMSI is to provide a significant improvement to security to the mobile subscriber, as IMSI does not need to be transmitted continuously.

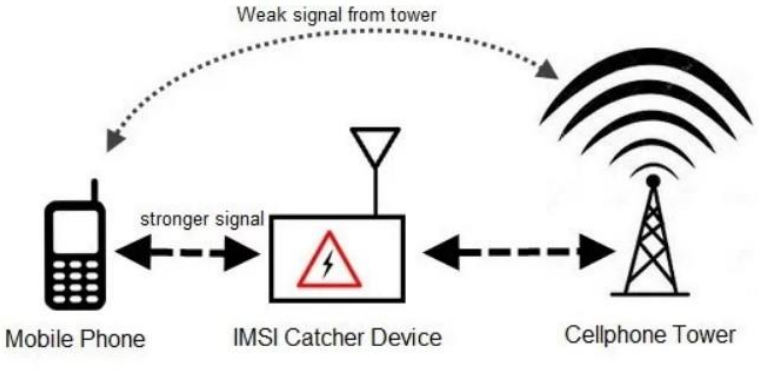


Figure 25: IMSI catcher illustration

9.1.5. Downgrade Attack

The 'Attach Reject' and TAU (Tracking Area Update) reject messages can be used in a similar way to the denial of service attacks, again with a rogue eNodeB sending the reject messages to an unsuspecting UE that will then be convinced that it is not permitted to connect to a legitimate eNodeB[100]. Instead of a simple reject message to prevent an attach or connection, the rogue eNodeB will now additionally specify that the user is not allowed to connect to 3G and 4G services, which will leave only 2G which is more vulnerable in terms of security. The UE will then exclusively attempt to connect to a 2G network layer, exposing it to eavesdropping due to the possibly weaker encryption of 2G[102].

9.1.6. Man-in-the-Middle (MitM)

Using a false base station or rogue eNodeB, it is possible to simply impersonate a legitimate provider's base station, using some of the prior vulnerabilities such as eavesdropping to obtain subscriber information and illegally intercept communications. In this scenario, mobile network users initially connect to the false base station, meaning that information will pass through the false node before being routed to its desired destination, allowing the attacker to simply monitor all communications without discovery[100].

9.1.7. Tracking

It is possible to use prior methods such as MitM attacks to obtain information allowing the location of the mobile network user to be determined, however there is a newer method which allows for this to be achieved. On the physical layer, there is a 16-bit identifier known as the Cell Random Network Temporary Identifier (C-RNTI), which is unique to each device in a cell. The C-RNTI is included in the header of the physical layer packets, meaning that this information is not encrypted. From this unique identifier, it is then possible to use the

[103] Patel, M. (2020, February) Retrieved from Paladion High Speed Cyber Defense: https://www.paladion.net/blogs/how-to-build-an-imsi-catcher-to-intercept-gsm-traffic

packets with the C-RNTI in the header to map the traffic of the user quite easily, allowing an eavesdropper to know approximately how long a user stays at a certain location. While the C-RNTI is considered temporary, it is not refreshed very often, giving a long enough period for it to be used for tracking[101], see Table 12 and Figure 26, though none of the contents of the data packets are exposed.

Table 12: Mobile network user identity mapping flow

Identity	Lifetime	Accessibility	Layer
Phone Number (MSISDN)	Lifelong	Public	Layer 8
Permanent Identity (IMSI)	Per SIM card lifecycle	Private (Core)	NAS Protocol (Layer 3)
Temporary Identity (TMSI)	Per NAS Connection (MNO policy)	Private (Core and RAN Network)	NAS Protocol (Layer 3)
Temporary Radio Identity (RNTI)	Per Radio Connection	Private (eNodeB)	MAC Protocol (Layer 2)

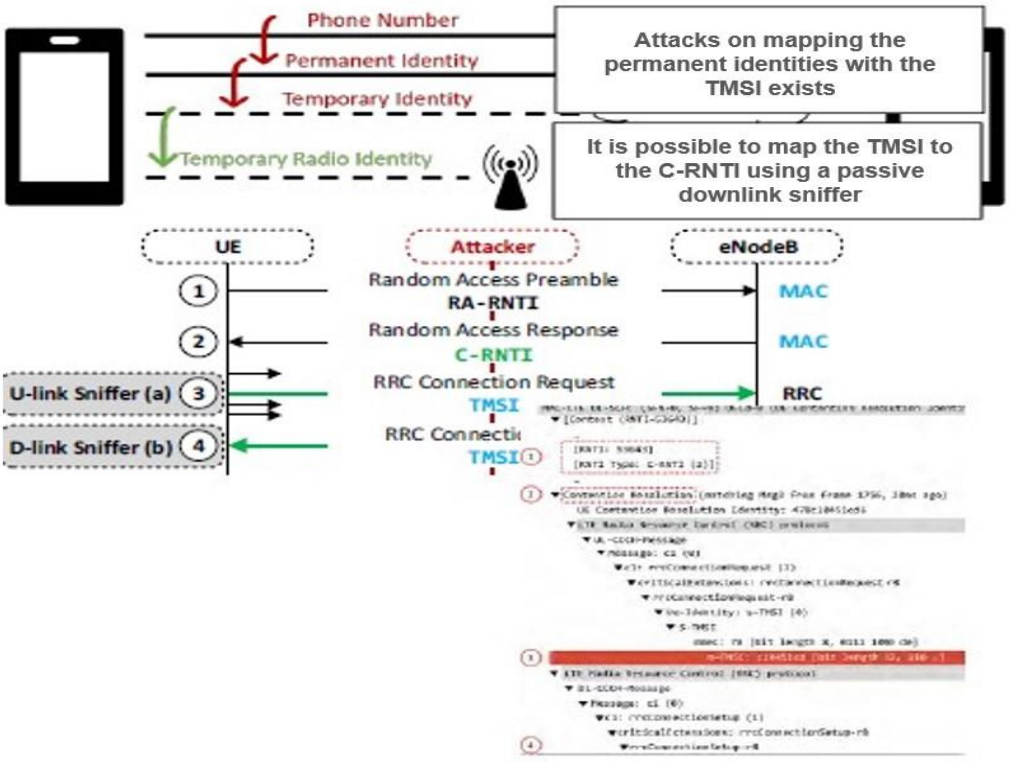


Figure 26. Mapping user identity for tracking

9.2. Core Network Security Vulnerabilities

9.2.1. Unsecured SS7

The SS7 protocol outside of the Mobile Application Part (MAP) protocol component is essentially security-free, meaning that an attack on the SS7 protocol would be met with no direct opposition[104]. As a result, the signalling protocol stack connected to the core network can potentially be exploited to access the ports of the core network, allowing for a range of attack vectors due to the number of services supported by the core network[105]. But this is

[104] GSM Association. (2019) Mobile Telecommunications Security Threat Landscape.
[105] Vacca, J. (2014) In Network and System Security - Second Edition (pp. 319-350)

generally well managed, within the mobile network core network buildings, with managed access, i.e. no access to general public or staff.

9.3. Backhaul Network Security Vulnerabilities

9.3.1. Optional Implementation of IPsec

4G transmissions have a security vulnerability as backhaul traffic from the eNodeB to the IP core network is unencrypted[98] on a VLAN. Most of the tier 1 operators have implemented IPsec to address this issue. IPsec is a real necessity for operators due to the added layer of security it provides and the fact that LTE is an all-IP mobile system. The IPsec protocols were defined by the Internet Engineering Task Force (IETF) to provide end-to-end security that can protect IP networks and protect higher-layer applications[105].

9.3.2. Unsecure CPRI protocol

CPRI (Common Radio Interface Protocol) is a digital interface standard to transport antenna samples between a radio equipment and a radio equipment control unit that performs the digital processing of these signals. In other words, it is an opensource protocol between Baseband and Radio Unit in base stations.

CPRI defines how the radio signal data is exchanged and not the data itself.
CPRI uses network security protocols such as IPsec and MACsec. However, the implementation and usage of IPsec or MACsec is vendor specific and are both optional solutions to provide transmission security in both the user plane and management plane. For the synchronisation plane, there is no defined security recommendations. If any vendor uses an unencrypted part of CPRI then all communications between baseband and radio unit are deemed to be unsecured.

9.4. Summary of Mobile Network Vulnerabilities and Defences

In Table 13, some possible defences are proposed for the current mobile network vulnerabilities. These are quite general with the aim of dealing with where the attack occurs, including the signalling protocols of mobile networks.

Table 13: Mobile network vulnerabilities and proposed defences

Vulnerability	**Proposed Defence**
DoS (Registration)	Make the Core Network capable of determining non-legitimate requests so that they can be dropped before resources are saturated.
DoS (Attach)	Develop a unique session ID or form of distinguishing different eNodeBs, as well as changing the reject system so that a phone does not stop attach requests after a single eNodeB has issued a reject.
Eavesdropping, Tracking	Improve security and encryption on data packets containing sensitive information which could lead to security breaches.

IMSI Catcher, Man-in-the-Middle	Stronger authentication methods to avoid the presence of false base stations. Partially mitigated using TMSI.
Downgrade Attack	Changes required for backward compatibility to avoid downgrades beyond a certain level of security if possible.
SS7, IPsec, CPRI	Use of higher-level encryptions with standardized requirements for more flexible protocols where encryption must be used where possible, especially when going into unsecured networks.

In Table 14, network security methods more specific to CAVs are proposed, with the aim of mostly ensuring that nodes and information in the CAV network are secured in a way to limit the effect of mobile attacks on the CAVs[57].

Table 14: Mobile network security defences

Defence	**Benefits**
Use physical layer channels to assign signatures and other features that allow legitimate UEs to be determined.	Detection of fake UE which could be used to compromise data and give false information.
Communication between layers to alert systems of threats on different levels.	More robust security awareness as a threat detected can be communicated to different system layers.
Use of cloud and edge networks to detect a false transmitter.	Detection of false transmissions leading to potential interception or modification of messages and information.
Periodic notification of users so that they are aware which UEs in the network are legitimate.	Prevents false nodes from hiding in a legitimate network by constantly indicating the legitimate nodes.
Local station is provided with the information from the sensors of CAVs to check for inconsistency.	Prevention of false information used to manipulate sensors in potentially dangerous ways.
Use machine learning to learn and become aware of normal behavior of CAVs.	Dangerous sensor manipulation much harder, as the machine learning would indicate it as unusual behavior and detect the threat.
Store prior information exchanges between UEs.	Can be used to identify anomalies in data exchange, indicating a possible attempt to exploit data transfer.
Validate messages using multiple types of sensor information.	Determines legitimacy of message as well as finding possible threats from the messages.

9.5. Categorisation of Attacks and their Aims

In this section, the mobile network vulnerabilities and attack vectors are summarised. The exploits are categorised based on the aims of an attacker. This is then mapped to which interfaces or network elements are compromised in a successful attack and the mobile network technology it can impact. Some attacks are targeted specifically at the service provider's network, while others affect the network users. Mobile network attacks can be categorised into the following four main elements that can be impacted from a successful exploit:

- Service
- Secrecy
- Privacy
- Integrity

Attackers can use either passive or active methods to target the RAN layer, but this is localised at a cell level. Furthermore, other types of attacks have wider consequences or footprints and can impact at a network-wide or global scale.

There are different types of mobile network attacks[106], see Table 15, and their causes and root causes are provided in Table 16[106].

Table 15: Attack categorisation and aims

Aim	Attack	Attacker Capabilities							Target	Technology			Range				
		Radio Passive	Radio Active	User Traffic	SS7 Interface	PSTN Interface	Internet Traffic	Nondescrictive Physical	User/Provider	2G	3G	4G	Physical	Cell	Location Area	Network	Global
Service	Signalling DoS	■	■						U,P	■	■	■		■			
	Attach Request Attack	■	■						P	■	■	■		■			
	Continuous Wideband Jamming		■						U,P	■	■	■		■			
	Protocol-Aware Selective Jamming	■	■						U,P			■		■			
	IPv4/v6 Middleboxes Misconfiguration			■			■		U,P			■				■	
	SMS Link Saturation				▒		■		U,P	■	■	■					■
	Insert/Delete Subscriber Data into the VLR/MSC				■				U	■	■	■					■
Secrecy	(U)SIM: COMP128v1 and MILENAGE Side-Channels							■	U	■	■	■	■				
	Baseband State Machine Exploits		■						U	■	■	■		■			
	Inter eNodeB User Plane Key Desynchronization Attack	■							U			■		■			
Privacy	AKA Protocol Linkability Attack	■	■						U		■	■		■			
	IMSI Paging Attack	■	■						U	■	■	■		■			
	Location Leak by SIP Message			■					U			■					■
	Location/Tracking Area not Allowed (Downgrade)	■	■						U		■	■		■			
	Measurement Report Localization	■	■						U			■		■			
	OTA SIM Card Update Key Reconstruction		■		▒				U	■	■	■					■
	Unauthenticated IMEI Request (IMSI Cather)	■	■						U	■	■	■		■			
	Cell-Level Tracking with SS7/MAP				■				U	■	■	■					■
	GPS Location with SS7/LCS				■				U	■	■	■			■		■
Integrity	ASN.1 Heap Overflow		■		▒				U,P	■	■	■		■	■	■	■
	Binary Baseband Exploit		■						U	■	■	■		■			
	SMS Parsing		■						U	■	■	■		■			■
	SIM Card Rooting		▒	▒	▒				U	■	■	■	■	■		■	■

Full capability	■
Partially capability (based on the network architecture)	▒

[106] David Rupprecht, A. D. (2018) 'On Security Research Towards Future Mobile Network Generations', https://arxiv.org/pdf/1710.08932.pdf

Table 16: Root causes of some mobile network attacks

Root Cause	Cause	Attack
Implementation Issue	Insecure Implementation	ASN.1 Heap Overflow
		Binary Baseband Exploit
		SIM Card Recording
		SMS Parsing
		Baseband State
	Leaky Implementation	(U)SIM: COMP128v1 and MILENAGE Side-Channels
Protocol Context Discrepancy	Accounting Policy Incocsistency	Misbilling: TCP Retransmission or DNS Tunneling
		Underbilling using VoLTE Hidden Channels
	Cross-Layer Information Loss	LTE IMS-based SMS spoofing
		Uplink IP header spoofing/Clock-and-dagger Misbilling
		Location Leak by SIP Message
		IPv4/v6 Middleboxes Misconfiguration
Wireless Channel	Channel Characteristics	Continuous Wideband Jamming
		Protocol-Aware Selective Jamming
Specification Issue	Insecure Inter-Network Protocol	Unblock stolen devices
		Cell-Level Tracking with SS7/MAP
		GPS Location with SS7/LCS
		Intercepting Calls with SS7/CAMEL
		Session Key Retrieval via SS7
		Insert/Delete Subscriber Data into the VLR/MSC
	Non-Existing Mutual Authentication	Fake Base Station SMS Spam
		Encryption Downgrade
		MitM IMSI Cather
	Unsecured Pre-Authentication Traffic	AKA Protocol Linkability Attack
		IMSI Paging Attack
		Location/Tracking Area not Allowed (Downgrade)
		Measurement Report Localization
		TMSI Deanonymization (Paging Attack)
		Unauthenticated IMEI Request
		Unauthenticated IMEI Request (IMSI Cather)
		GPS Receiver Denial of Service
		Paging Response Race DoS
	Resource Usage Asymmetry	Attach Request Attack
		DDoS HLR: Activate Call Forwarding Request
		Signalling DoS
		SMS Link Saturation
	Weak Cryptography	OTA SIM Card Update Key Reconstruction
		Inter eNodeB User Plane Key Desynchronization Attack
		Key Reusage Across Cipher and Network Generations
		Passive Over-the-Air Decryiption of A5/1 and A5/2
		SIM Key Extraction via COMP128v1 Cry
		Weak Key due to Inter-Technology Handover

9.6. Mobile Network Vulnerability Case Studies

It is important to understand why mobile network vulnerabilities and their possible implications may impact the CAV ecosystem. The case studies presented in this section demonstrate the importance and urgency of having effective cyber security controls and the risk mitigation frameworks that are explored further in the report.

9.6.1. ComSec – IMSI Catcher

A biotech company in San Francisco found that secrets had been exposed to the competition regarding expansion of its product line, which was unknown to anyone outside of a confidentially bound group of people within the company. Looking further into this with the help of ComSec, it was found that an IMSI catcher was acting as a rogue cell tower for mobile phones, monitoring all communications and taking a copy of all the details before forwarding them along the regular route, meaning that a man in the middle attack was being perpetrated the entire time[107].

In the case of the IMSI catcher at ComSec, it is possible to have access to a victims' communications, which could result in a wide range of data breaches well beyond production line secrets, as phones now have a wider range of uses than before. For example, this attack could be used to monitor the IP based communications on the user end as well as gain access to more sensitive data which can include passwords stored on the phone or bank details. However, this vulnerability is mostly mitigated by the use of TMSI, adopted by all modern networks, but is an example of attacker thinking.

9.6.2. Jeep Cherokee Hijacking

In 2015, serious weaknesses were shown in self driving personal light vehicles, particularly highlighted by the hijack of in a Jeep Cherokee by two scientists. The hijacking occurred while the vehicle was still in motion. Initially, the climate control system was hijacked, allowing for adjusting of the fan and temperature within the car, followed by the activation of the radio. An added result of taking control of the car was that these features could not be manually overridden by the person in the car. The digital display was taken control of to display unauthorised images, followed by a much more serious issue of cutting the transmission. This basically stopped the accelerator of the car and resulted in the car coming to a stop in the middle of the road, which meant that this self-driving car could be stopped at any time, resulting in a potential crash[108]. This exploit was due to the software, uConnect, which is used to connect to the Internet, allowing for the driver to have an Internet hotspot, navigate and make phone calls, meaning that this could be exploited to take control of the car provided that the IP address of the vehicle was known[25].

In this scenario, the stopping of the car was only one of the dangers. In fact, a full software control could allow for all types of spoofed data to be exploited such that a vehicle could be deceived regarding its surroundings, the detection of obstacles could return the wrong values, or the speed of a vehicle would not be detected. This could cause serious accidents, especially if all the other vehicles are also autonomous and therefore dependent on the same kind of systems.

9.6.3. SS7 Signalling Interception

SS7 can be used to track phones as well as intercept the messages being sent to and from them because it is a core network signalling protocol, giving rise to a range of possible

[107] ComSec (n.d.) ComSec: IMSI Catcher Case Study. Retrieved from ComSec: http://comsecllc.com/comsec-imsi-catcher-case-study/
[108] WIRED (2015) Retrieved from Hackers Remotely Kill a Jeep on the Highway: http://www.wired.com/2015/07/hackers-remotely-kill-keep-highway/

attacks. One of these attacks was when two-factor authentication messages to phones for Metro Bank UK banking in 2019 were intercepted. This meant that the attacker could obtain the verification codes needed to gain access to the online banking system showing an extremely serious issue in banking using mobile networks that use SS7 signalling protocols[109] (VICE, 2019). In a CAV scenario, this type of attack could lead to loss of privacy and integrity. Again, all modern networks protect against this form of attack. Attackers would need access to the core network, which is very unlikely, as these are secure managed access areas.

9.7. Vulnerabilities of OEM In-Vehicle Applications

Vehicle Original Equipment Manufacturer (OEM) applications such as Land-rover Jaguar's InControl Apps, FordPass Connect and Tesla App are some examples of the platforms that enable connectivity in modern connected cars.

These applications provide two broad functionalities and services in a CAV environment:

- A platform for services such as weather and live-traffic data, infotainment as well as personal and social media messaging.
- Driving-related functions that provide safety and convenience for drivers and vehicle occupants such as navigation data, information about charging points for electric vehicles, climate control and parking-related assistance.

Software applications, however, are never hundred per cent secure from possible exploits and vulnerabilities. Vulnerabilities in connected car applications exposes these vehicles to huge security threats as they become attractive targets for attackers. Vehicle manufacturers are cognizant of these critical vulnerabilities and routinely issue warnings to investors and consumers that despite their best efforts in designing and implementing security measures to protect against unauthorised access to their systems, they cannot guarantee that vulnerabilities will not be exploited before being identified or that their mitigation strategies are effective.

It is very common to find connected vehicle models with the capability to establish communication links between the in-vehicle applications and other external devices. Although, In-vehicle applications provide essential connectivity functions for drivers, they also increase the cyber security risk profiles of connected vehicles due to their connection to the internet amplifying the potential of being hacked.

One of the most important focus for in-vehicle security is the infotainment system which is designed to interact and connect to mobile networks such as 4G and 5G, as well as the capability to connect to smart home systems using technologies such as Zigbee, Bluetooth or Wi-Fi.

The main security considerations raised by researchers stem from a potential design flaw in most connected vehicles where the infotainment system is connected to external networks such as the Internet, through a mobile connection, as well as to the control unit of the vehicles that serve critical and safety-related functions such as the engine control and the braking

[109] VICE (2019) 'Criminals are Tapping into the Phone Network Backbone to Empty Accounts' https://www.vice.com/en_us/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank

systems. This therefore provides an attack surface for hackers to commandeer a vehicle from a remote location through the internet.

The most recent cyber-attacks on connected vehicles were conducted via in-vehicle application exploits. Applications that allow for remote access often use a web service hosted by the service provider or through direct connections to the devices. The web service then connects to the vehicle through the mobile network. Like any mobile application, in-vehicle applications are exposed to a multitude of cyber security threats and vulnerabilities. The list below provides a summary:

- **Non-standard testing and analysis:** Auto manufacturers have not yet defined industry-wide standards for fundamental activities during the design process. Tools like fuzz testing and static code analysis should be standardized across manufacturers.

- **Malware Attack:** Any digital application is exposed to the threat of malware attacks. In addition, poorly designed or maintained software provides an entry pathway for attackers wishing to exploit security vulnerabilities especially with applications that are designed and implemented using open source platforms. This risk is further amplified when third-party applications are allowed in the vehicle application ecosystem.

- **Front Door Attack:** Commandeering or over-riding the access mechanism of the OEM such as access to the Engine Control Unit (ECU), Engine Control Module (ECM), Transmission Control Module (TCM), BCM (Brake Control Module) etc. through bugs or security lapses in in-vehicle software systems.

- **Lack of Binary Protections:** This vulnerability is presented when the source code of an in-vehicle application is easy to decompile, read and reverse-engineer as a result of being written in clear-text.

- **Privacy risks:** Despite the inherent privacy implications, most consumers opt in to have their usage and interaction data with in-vehicle applications collected and sent to remote OEM servers. This means that consumers are susceptible to being tracked and have no control in stopping their data being sold to third parties or for what purposes their data is used. In addition, if the data that sits on these applications is not wiped when the vehicle is transferred to a new owner it may be exposed and exploited with severe consequences on privacy.

- **Data Leakage:** When the in-vehicle application shares services with other third-party applications and provides permissions to transfer or share any consumer data then data leakage may occur, leading to breaches of confidentiality and privacy.

- **Client-Side Injection Attack:** This Vulnerability targets application clients or users rather than assets or server resources. Through this attack, the application is used to execute a malicious code on the client side. Malicious code running in an application can have serious security and privacy implications for consumers and OEMs.

- **Weak Encryption:** This vulnerability can be exploited when outdated or weak algorithms are used to protect data and data transmissions.

- **Private Key Exposure:** When the attacker obtains a private key, then offline cracking is possible.

- **Over-the-Air (OTA) Software Updates:** Enabling OTA updates for in-vehicle software applications attracts serious security risks. If a vehicle's systems can be updated remotely then these systems can also be accessed remotely by an attacker, given enough time and resources to identify holes in the security systems relied on by the OEMs. It was reported in (Consumer Watchdog, 2019)[110] that in August 2015, security experts found six vulnerabilities that exposed the Tesla software to hacking. Those vulnerabilities were eventually patched OTA.

The remote unlocking of BMW, Mini, and Rolls-Royce vehicles has been widely publicised. This specific vulnerability was addressed by upgrading the communication encryption mechanisms between the vehicles and BMW's server, requiring the patching of at least 2.2 million vehicles.

The vehicle application vulnerabilities summarised above indicate a greater need for OEMs to improve their cyber security capabilities and put in place robust mitigation strategies to quickly address and fix vulnerabilities as soon as they are discovered. Software testing and patching can reduce the vulnerabilities, but more importantly security by design must be embraced by all vehicle manufacturers.

10. Mobile Network Security Capabilities

10.1. Introduction

In mobile networks, different sections of the network have different abilities to defend against attack. This includes encryption and methods of authorization to make sure that information is not read by a third party, as well as ensuring that UEs and base stations are authenticated and encrypted before beginning any communication. These capabilities can limit the effect of existing vulnerabilities to reduce the effect of an attacker on the network.

10.2. Radio Access Network Security Capabilities

10.2.1. Ciphering

As it is not desirable for others to have easy access to communications, mobile networks employ forms of encryption based on ciphering. This is where the communications, either in voice or text form, are encoded using a predetermined system such as AES which prevents them being easily intercepted, meaning only the end users may successfully read them without having to break the cipher, preventing eavesdropping between the mobile device and base station[105].

[110] Consumer Watchdog. (2019, July) Kill Switch: Why connected cars can be killing machines and how to turn them off. USA

10.2.2. Non-Repeating Random Values

Another form of protection for the RAN is non-repeating random values, which essentially generates a sequence of random numbers that will not have any repeats in them, so that a unique session ID is generated for each communication. This prevents replay attacks, which fraudulently repeat or delay valid data transmissions. This is usually done by an attacker who intercepts the data and retransmits it, essentially performing a type of MitM attack[105].

10.2.3. Signalling Integrity

This uses integrity keys to ensure that the data transmitted is not modified or deleted in any way, so that there is no interfering with communications between the base station and the mobile device. This consists of an algorithm agreement stage, where the mobile device and base station can securely negotiate the algorithm they will use, followed by integrity key agreement, which allows them to agree on a chosen integrity key, which also provides authentication between the mobile device and the base station (mutual authentication). This authentication also prevents the use of cloned mobile devices and base stations by an attacker[105].

10.2.4. Mutual Authentication

The mobile device and the base station must verify their identities to one another at the same time before agreeing on security measures. As a result, a fake base station will have much greater difficulty impersonating an existing station as it must verify itself to the mobile device in the same instant[101]. The 11 digit cell global identity (CGI) is a way of insuring a unique identifier for every cell in the network, it is made up of a country code (CC), a mobile network code (MNC), location area code (LAC) and cell identity (CI), therefore GCI = CC+MNC+LAC+CI.

10.2.5. Privacy (TMSI and GUTI)

The TMSI is assigned locally to mask the IMSI of the user as it is possible to track the mobile device based on this. Similarly, the use of the Globally Unique Temporary Identifier (GUTI) [100] is assigned to a mobile device on attachment. The GUTI, like the TMSI can be periodically changed, meaning that it is harder to follow the traffic of the phone to identify its location, as discussed earlier in this document.

10.3. Core Network Security Capabilities

10.3.1. End-to-End Encryption

In the core network, the SS7 group of protocols is used, which provide a range of services including number translation, billing and Short Message Service (SMS), but are mainly used for setup and teardown of phone calls. Security is provided for a protocol known as Mobile Application Part (MAP) which is based on SS7, in the form of a security protocol known as MAPSec. MAP provides an application layer for nodes in GSM, as well as core networks in GPRS and UMTS, so that services can be provided to users by accessing key nodes in the core network. When MAP is used with the IP protocol, it becomes IPsec. Both

MAPSec and IPsec are used to protect MAP messages between links by providing service node authentication, as well as message encryption from end to end. This prevents eavesdropping, as well as corruption or fabrication of MAP messages. It must be noted that both MAPSec and IPsec are optional, but most, if not all network operators enables them, the other providers must also enable it to ensure end-to-end security[105].

10.4. Backhaul Network Security Capabilities

10.4.1. IPsec and Certificate Handling

3GPP has introduced security by addressing the scenarios with and without IPsec, protecting the user and control traffic where possible. Packets encrypted at the backhaul use Internet Key Exchange 2 (IKEv2) which is used to set up Security Association (SA) protocol of IPsec. The IKEv2 protocol is certified with the use of Certificate Management Protocol 2 (CMPv2) which is used to authenticate links using Public Key Infrastructure (PKI). This form of IPsec was used to develop the 3GPP security standards for the LTE backhaul.

The packets between eNodeB and the core network are controlled by IPsec, which uses an Authentication Header offering integrity and authentication of the data, with the option of anti-replay to avoid a replay attack. The Encapsulating Security Payload offers the same services with confidentiality. The purpose of the S1 interface outlined by 3GPP is to provide end to end encryption and decryption. If the S1 and X1 sections of the network are trusted, IPsec is not mandatory, otherwise it must be used when traversing non trusted networks.

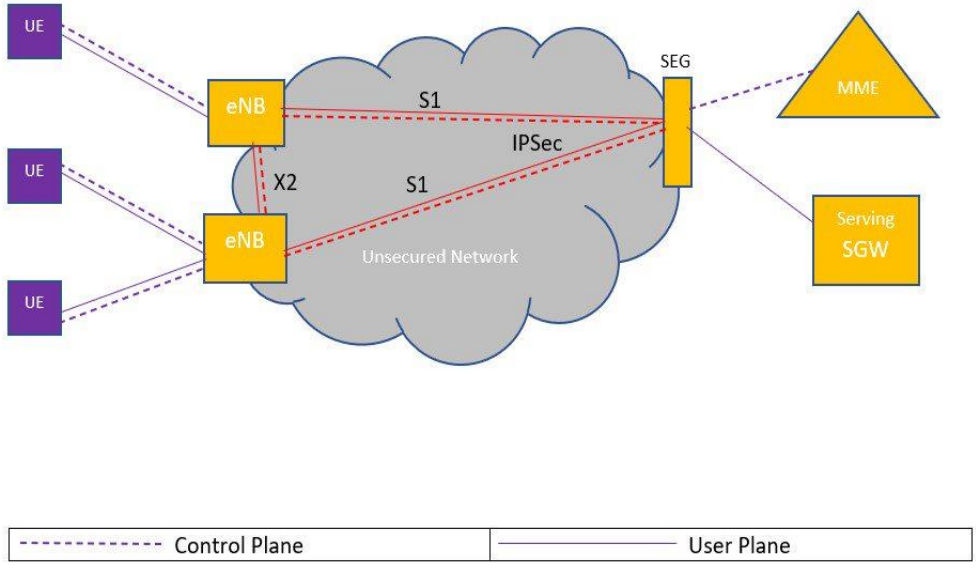


Figure 27: Backhaul security architecture[111]

[111] Backhaul Security Mechanisms. (2015) Retrieved from Long Term Evolved Security: https://longtermevolvedsecurity.wordpress.com/backhaul-security-mechanisms-in-lte/

10.4.2. CPRI (Common Public Radio Interface)

At the baseband unit of a network, signals will pass through the baseband unit which controls information and status inside the base station and will encrypt all digital information based on IPsec or MACsec according to the vendor-specific implementations. This means the data leaving the baseband unit is secured by encryption, if the optional security mechanisms are implemented.

10.5. Summary of Mobile Network Security Capabilities

A summary of the mobile network security capabilities is provided in Table 17[57], and referenced to the appropriate network element where is implemented.

Table 17. CAV security defences

Capability	**Network Location**	**Explanation**
Ciphering	RAN	Use of agreed system to encode the data to avoid others freely reading it.
Non-repeating Random Values	RAN	Sequence of random numbers used for each session to avoid attackers interfering with sessions using replay attacks.
Signalling Integrity	RAN	Integrity keys used to prevent the signal being tampered with and is used by both sides in mutual authentication.
Mutual Authentication	RAN	Both ends of the communication must identify to each other before agreeing on security.
Privacy	RAN	TMSI and GUTI used to mask the IMSI and are periodically changed to avoid using them for ID and tracking.
End-to-End Encryption	Core Network	Information encrypted before going between end users to prevent reading of information.
IPsec & Certificate Handling	Backhaul	IPsec used when transferring data along untrusted networks and certificate handling used to authenticate links before agreeing on public keys.
CPRI (Common Packet Radio Interface)	Fronthaul	Data encrypted at the baseband unit before going to next point of network to allow privacy.

11. Threat Modelling of CAV Communication

In this section an overview of the CAV communications assets and tiers is provided, see Figure 28. This is used to analyse potential threats that arise from the interactions of the various assets and asset boundaries within the Open System Interconnection (OSI) layers of the LTE protocol stack. The OSI model is a conceptual framework developed by ISO and is used in describing generic network communication data flows. In contrast to the TCP/IP model, which was developed specifically for internet and data-based communications over networks, the LTE protocol stack has similar characteristics and functionalities that can generally be mapped to the OSI model. The LTE functional assets are mapped to the OSI layers and listed in Table 18 through to Table 20. These assets are used for a high-level STRIDE analysis with mitigation using Center for Internet Security (CIS) Controls, which are described in Section 11.2.

The Data Flow Diagram created for Figure 28 is from the reference end-to-end CAV network architecture used in this report. It models the data interactions between assets and asset boundaries, starting from the SIM card located in the vehicle modem to the PGW of the mobile core network, the internet and the application servers used to provide CAV-related services.

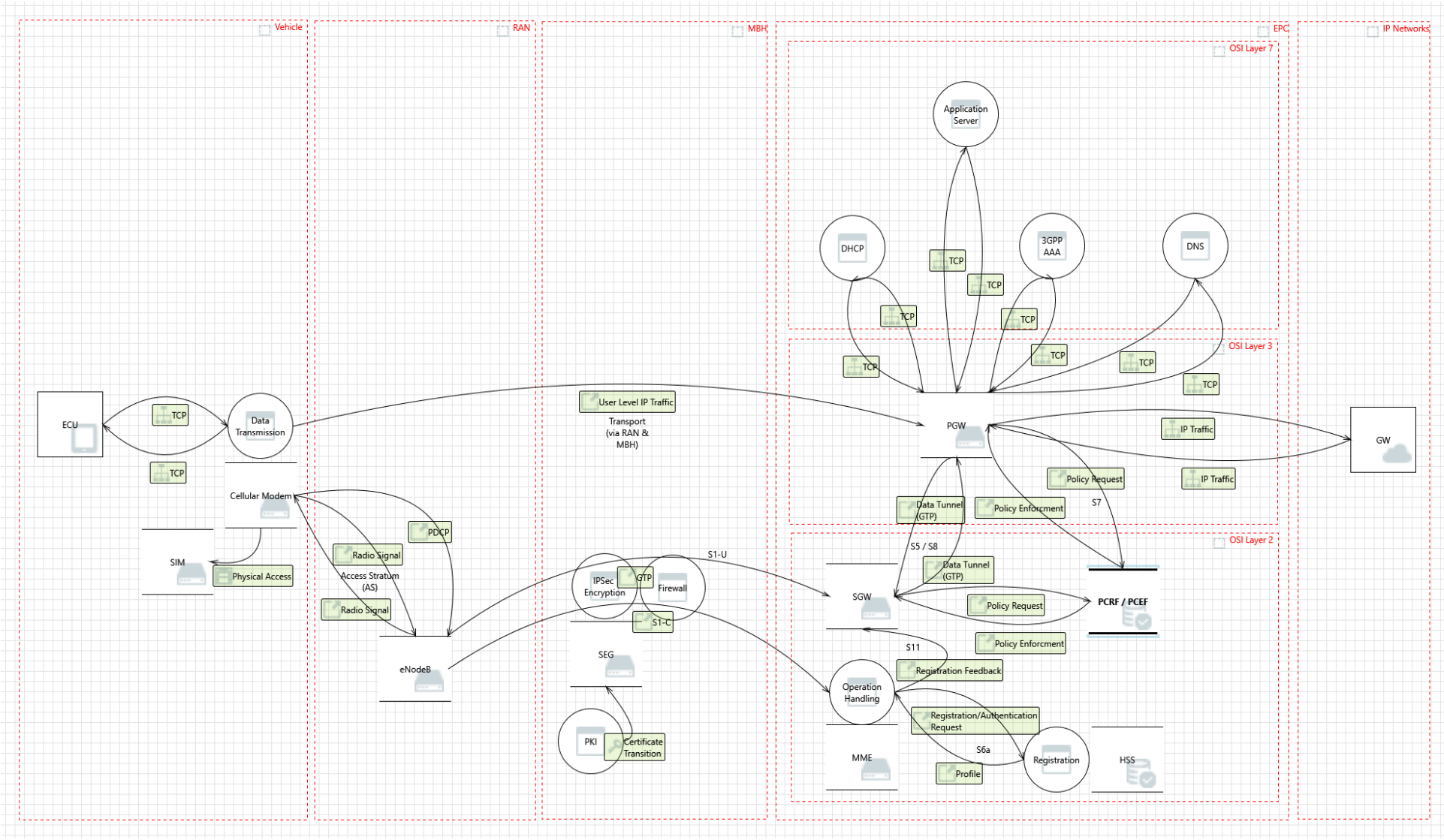


Figure 28. Data Flow Diagram for the CAV communication layer assets and their interactions

11.1. OSI Layer Assets

Table 18. OSI Layer 2 Assets

Asset	Description	Location	Confidentiality	Integrity	Availability
Modem	A device that adds wireless 4G (LTE) connectivity to vehicle.	Vehicle	M	H	H
SIM	Subscriber Identification Module securely store the IMSI number and its related key to identify and authenticate the subscribers on network.	Vehicle	H	H	H
eNodeB	Evolved Node B communicates directly wirelessly with user equipment and controls radio communication between US and EPC.	RAN	M	H	M
MME	Handles the high-level operation by the signalling messages and HSS.	EPS	M	H	H
HSS	Holds all the information about all the network operator's subscribers in a central database.	EPS	H	H	H
SWG	Performs mobility anchoring and forward data between PDN Gateway and Base Station.	EPS	M	M	H
PCRF	Accountable for controlling the flow-based charging operations in the Policy Control Enforcement Function (PCEF) and policy control decision-making.	EPS	H	M	H

Table 19. OSI Layer 3 Assets

Asset	Description	Location	Confidentiality	Integrity	Availability
PDN_GW	Communicates with PDN's employing interfaces. It performs operations like IP address allocation and packet filtering.	EPS	H	H	H
IP GW	Connects the IP network to PDN-GW	IP Network	H	M	M

Table 20. OSI Layer 7 Assets

Asset	Description	Location	Confidentiality	Integrity	Availability
DHCP	Automatically assigns an IP address and other information to each host on the network.	EPS	L	M	H
DNS	A hierarchical and decentralised naming system for resources connected to the Internet or the internal network.	EPS	H	H	M
3GPP AAA	Provides authentication, authorisation, policy control and routing information to packet gateways.	EPS	H	H	H
Application Server	Handles all application operations between users and the backend business applications or databases.	EPS	M	M	M

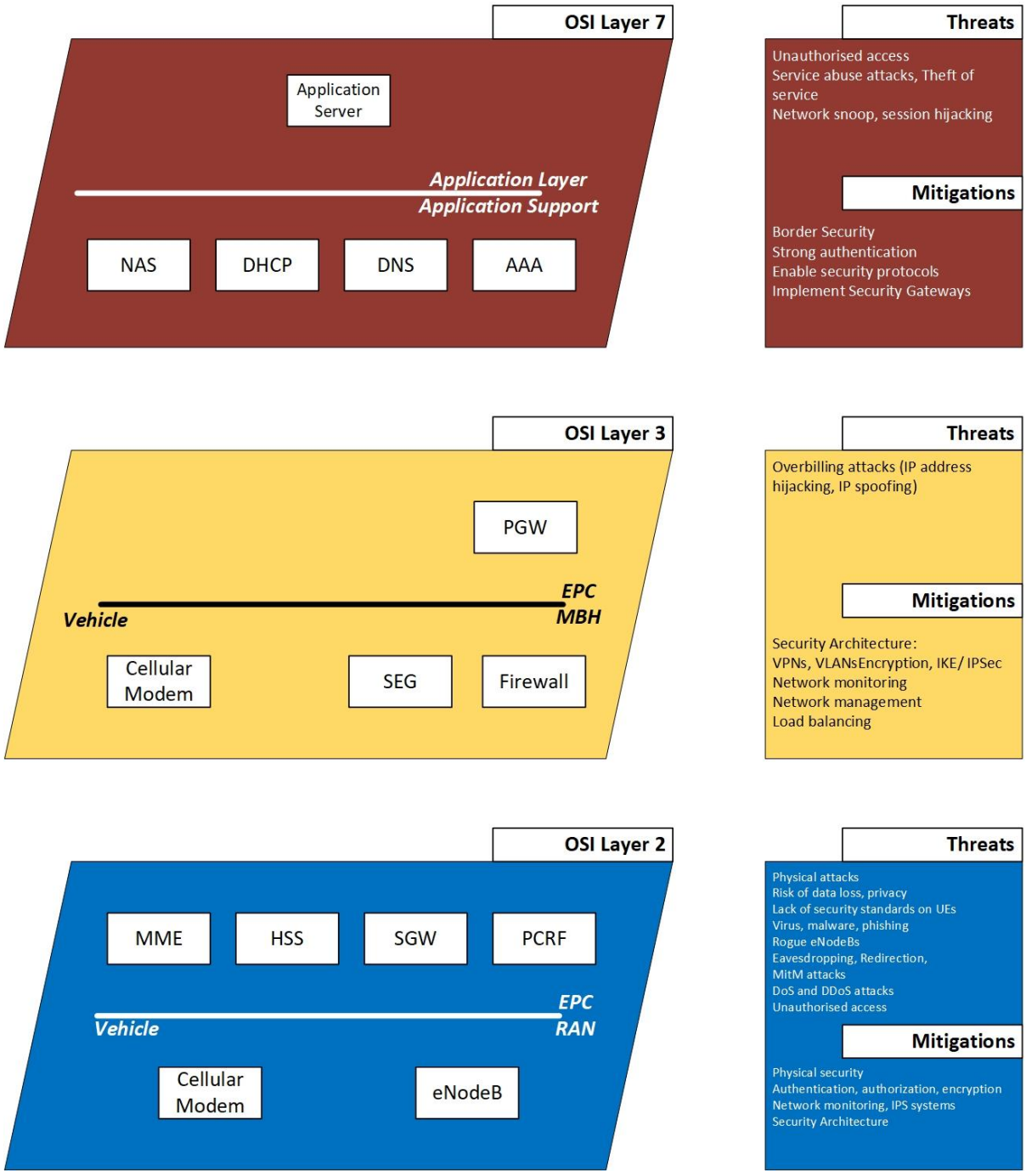


Figure 29. Simplified diagram, showing assets, threats and mitigations for each OSI layer

11.2. CIS Controls

CIS controls are developed by a global community of IT experts to provide a series of high priority security actions and mitigations that should be considered as a defence-in-depth best practice to reduce the risk of common attacks[112].

CIS controls are developed based on actual experienced attacks, which are defended effectively. The experts' extensive knowledge is gathered from various ecosystems to develop

[112] Center for Internet Security (2019) CIS Controls, Version 7.1. Retrieved from https://www.cisecurity.org/controls/cis-controls-list/

a mature collection of controls that could be employed and adopted by different industries and teams. The security improvement ideas and actions are shared by individuals and enterprises and CIS acts as a catalyst to support this community and makes sure the controls are effective and up to date.

The technical measures are specifically defined to provide the most effective controls to detect, prevent, respond to and mitigate breaches of the most common and enhanced security attacks. These might be used in combination with current formal risk management frameworks. CIS controls demonstrate critical factors of an effective defence system including:

- Offense informs defence
- Prioritisation
- Measurements and Metrics
- Continuous diagnostics and mitigation
- Automation.

All mitigation recommendations that provided in the STRIDE Threat modelling are based on CIS controls.

11.2.1. Basic Controls

CIS Control 1:
Inventory and control of hardware assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.

Sub-Controls

1.1	Utilise an Active Discovery Tool
1.2	Use a Passive Asset Discovery Tool
1.3	Use DHCP Logging to Update Asset Inventory
1.4	Maintain Detailed Asset Inventory
1.5	Maintain Asset Inventory Information
1.6	Address Unauthorised Assets
1.7	Deploy Port Level Access Control
1.8	Utilise Client Certificates to Authenticate Hardware Assets

CIS Control 2:
Inventory and control of software assets

Actively manage (inventory, track, and correct) all software on the network so that only authorised software is installed and can execute, and that all unauthorised and unmanaged software is found and prevented from installation or execution.

Sub-Controls

2.1	Maintain Inventory of Authorised Software

2.2	Ensure Software is Supported by Vendor
2.3	Utilise Software Inventory Tools
2.4	Track Software Inventory Information
2.5	Integrate Software and Hardware Asset Inventories
2.6	Address unapproved software
2.7	Utilise Application Whitelisting
2.8	Implement Application Whitelisting of Libraries
2.9	Implement Application Whitelisting of Scripts
2.10	Physically or Logically Segregate High-Risk Applications

CIS Control 3:
Continuous vulnerability management

Continuously acquire, assess, and act on new information in order to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers.

Sub-Controls

3.1	Run Automated Vulnerability Scanning Tools
3.2	Perform Authenticated Vulnerability Scanning
3.3	Protect Dedicated Assessment Accounts
3.4	Deploy Automated Operating System Patch Management Tools
3.5	Deploy Automated Software Patch Management Tools
3.6	Compare Back-to-Back Vulnerability Scans
3.7	Utilise a Risk-Rating Process

CIS Control 4:
Controlled use of administrative privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Sub-Controls

4.1	Maintain Inventory of Administrative Accounts
4.2	Change Default Passwords
4.3	Ensure the Use of Dedicated Administrative Accounts
4.4	Use Unique Passwords
4.5	Use Multi-Factor Authentication for All Administrative Access
4.6	Use Dedicated Workstations for All Administrative Tasks
4.7	Limit Access to Script Tools
4.8	Log and Alert on Changes to Administrative Group Membership
4.9	Log and Alert on Unsuccessful Administrative Account Login

CIS Control 5:
Secure configuration for hardware and software on mobile devices, laptops, workstations and servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Sub-Controls

5.1	Establish Secure Configurations
5.2	Maintain Secure Images
5.3	Securely Store Master Images
5.4	Deploy System Configuration Management Tools
5.5	Implement Automated Configuration Monitoring Systems

CIS Control 6:
Maintenance, monitoring and analysis of audit logs

Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.

Sub-Controls

6.1	Utilise Three Synchronized Time Sources
6.2	Activate Audit Logging
6.3	Enable Detailed Logging
6.4	Ensure Adequate Storage for Logs
6.5	Central Log Management
6.6	Deploy SIEM or Log Analytic Tools
6.7	Regularly Review Logs
6.8	Regularly Tune SIEM

11.2.2. Foundational Controls

CIS Control 7:
Email and web browser protections

Minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems.

Sub-Controls

7.1	Ensure Use of Only Fully Supported Browsers and Email Clients
7.2	Disable Unnecessary or Unauthorised Browser or Email Client Plugins
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients
7.4	Maintain and Enforce Network-Based URL Filters
7.5	Subscribe to URL-Categorisation Service

7.6	Log All URL requester
7.7	Use of DNS Filtering Services
7.8	Implement DMARC and Enable Receiver-Side Verification
7.9	Block Unnecessary File Types
7.10	Sandbox All Email Attachments

CIS Control 8:
Malware defences

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defence, data gathering, and corrective action.

Sub-Controls

8.1	Utilise Centrally Managed Anti-Malware Software
8.2	Ensure Anti-Malware Software and Signatures Are Updated
8.3	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies
8.4	Configure Anti-Malware Scanning of Removable Devices
8.5	Configure Devices to Not Auto-Run Content
8.6	Centralize Anti-Malware Logging
8.7	Enable DNS Query Logging
8.8	Enable Command-Line Audit Logging

CIS Control 9:
Limitation and control of network ports, protocols, and services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimise windows of vulnerability available to attackers.

Sub-Controls

9.1	Associate Active Ports, Services, and Protocols to Asset Inventory
9.2	Ensure Only Approved Ports, Protocols, and Services Are Running
9.3	Perform Regular Automated Port Scans
9.4	Apply Host-Based Firewalls or Port-Filtering
9.5	Implement Application Firewalls

CIS Control 10:
Data recovery capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Sub-Controls

10.1	Ensure Regular Automated Backups

10.2	Perform Complete System Backups
10.3	Test Data on Backup Media
10.4	Protect Backups
10.5	Ensure All Backups Have at Least One Offline Backup Destination

CIS Control 11:
Secure configuration for network devices, such as firewalls, routers, and switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Sub-Controls

11.1	Maintain Standard Security Configurations for Network Devices
11.2	Document Traffic Configuration Rules
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes
11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices
11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
11.6	Use Dedicated Machines for All Network Administrative Tasks
11.7	Manage Network Infrastructure Through a Dedicated Network

CIS Control 12:
Boundary defence

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Sub-Controls

12.1	Maintain an Inventory of Network Boundaries
12.2	Scan for Unauthorised Connections Across Trusted Network Boundaries
12.3	Deny Communications with Known Malicious IP Addresses
12.4	Deny Communication Over Unauthorised Ports
12.5	Configure Monitoring Systems to Record Network Packets
12.6	Deploy Network-Based IDS Sensors
12.7	Deploy Network-Based Intrusion Prevention Systems
12.8	Deploy NetFlow Collection on Networking Boundary Devices
12.9	Deploy Application Layer Filtering Proxy Server
12.10	Decrypt Network Traffic at Proxy
12.11	Require All Remote Login to Use Multi-Factor Authentication
12.12	Manage All Devices Remotely Logging into Internal Network

CIS Control 13:
Data protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Sub-Controls

13.1	Maintain an Inventory of Sensitive Information
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organisation
13.3	Monitor and Block Unauthorised Network Traffic
13.4	Only Allow Access to Authorised Cloud Storage or Email Providers
13.5	Monitor and Detect Any Unauthorised Use of Encryption
13.6	Encrypt Mobile Device Data
13.7	Manage USB Devices
13.8	Manage System's External Removable Media's Read/Write Configurations
13.9	Encrypt Data on USB Storage Devices

CIS Control 14:
Controlled access based on the need to know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Sub-Controls

14.1	Segment the Network Based on Sensitivity
14.2	Enable Firewall Filtering Between VLANs
14.3	Disable Workstation to Workstation Communication
14.4	Encrypt All Sensitive Information in Transit
14.5	Utilise an Active Discovery Tool to Identify Sensitive Data
14.6	Protect Information Through Access Control Lists
14.7	Enforce Access Control to Data Through Automated Tools
14.8	Encrypt Sensitive Information at Rest
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data

CIS Control 15:
Wireless access control

The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Sub-Controls

15.1	Maintain an Inventory of Authorised Wireless Access Points
15.2	Detect Wireless Access Points Connected to the Wired Network
15.3	Use a Wireless Intrusion Detection System

15.4	Disable Wireless Access on Devices if Not Required
15.5	Limit Wireless Access on Client Devices
15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
15.8	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication
15.9	Disable Wireless Peripheral Access of Devices
15.10	Create Separate Wireless Network for Personal and Untrusted Devices

CIS Control 16:
Account monitoring and control

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimise opportunities for attackers to leverage them

Sub-Controls

16.1	Maintain an Inventory of Authentication Systems
16.2	Configure Centralized Point of Authentication
16.3	Require Multi-Factor Authentication
16.4	Encrypt or Hash all Authentication Credentials
16.5	Encrypt Transmittal of Username and Authentication Credentials
16.6	Maintain an Inventory of Accounts
16.7	Establish Process for Revoking Access
16.8	Disable Any Unassociated Accounts
16.9	Disable Dormant Accounts
16.10	Ensure All Accounts Have An Expiration Date
16.11	Lock Workstation Sessions After Inactivity
16.12	Monitor Attempts to Access Deactivated Accounts
16.13	Alert on Account Login Behaviour Deviation

11.2.3. Organisational Controls

CIS Control 17:
Implement a security awareness and training program

For all functional roles in the organisation (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programs.

Sub-Controls

17.1	Perform a Skills Gap Analysis
17.2	Deliver Training to Fill the Skills Gap
17.3	Implement a Security Awareness Program
17.4	Update Awareness Content Frequently

17.5	Train Workforce on Secure Authentication
17.6	Train Workforce on Identifying Social Engineering Attacks
17.7	Train Workforce on Sensitive Data Handling
17.8	Train Workforce on Causes of Unintentional Data Exposure
17.9	Train Workforce Members on Identifying and Reporting Incidents

CIS Control 18:
Application software security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Sub-Controls

18.1	Establish Secure Coding Practices
18.2	Ensure That Explicit Error Checking is Performed for All In-House Developed Software
18.3	Verify That Acquired Software is Still Supported
18.4	Only Use Up-to-Date and Trusted Third-Party Components
18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms
18.6	Ensure Software Development Personnel are Trained in Secure Coding
18.7	Apply Static and Dynamic Code Analysis Tools
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities
18.9	Separate Production and Non-Production Systems
18.10	Deploy Web Application Firewalls
18.11	Use Standard Hardening Configuration Templates for Databases

CIS Control 19:
Incident response and management

Protect the organisation’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.

Sub-Controls

19.1	Document Incident Response Procedures
19.2	Assign Job Titles and Duties for Incident Response
19.3	Designate Management Personnel to Support Incident Handling
19.4	Devise Organisation-wide Standards for Reporting Incidents
19.5	Maintain Contact Information for Reporting Security Incidents
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents
19.7	Conduct Periodic Incident Scenario Sessions for Personnel
19.8	Create Incident Scoring and Prioritization Schema

CIS Control 20:
Penetration tests and red team exercises

Test the overall strength of an organisation's defence (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

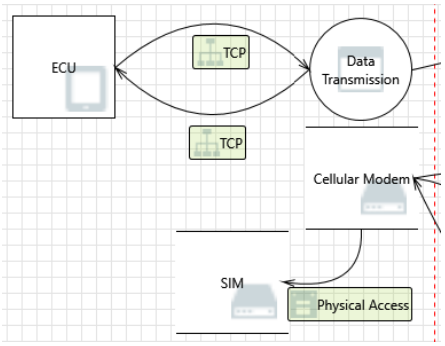
Sub-Controls

20.1	Establish a Penetration Testing Program
20.2	Conduct Regular External and Internal Penetration Tests
20.3	Perform Periodic Red Team Exercises
20.4	Include Tests for Presence of Unprotected System Information and Artefacts
20.5	Create Test Bed for Elements Not Typically Tested in Production
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards
20.8	Control and Monitor Accounts Associated with Penetration Testing

11.3. STRIDE Threat Modelling

This section identifies cyber security threats and vulnerabilities that increase the cyber security risks against assets. Appropriate security controls recommended for mitigation are provided based on the CIS Controls, see Section 11.2, to reduce the security risks. Reference is made to Figure 28, the CAV communications Data Flow Diagram.

11.3.1. Vehicle Side (UE)



Threat	Physical Tampering
Category	**T**ampering
Description	Mobile connectivity interfaces such as SIM cards and modems can be physically accessed, tampered with and used as an entry point to stage a subsequent remote attack. Cloning of SIM cards is a possible threat in this scenario. Misuse of hardware components such as jailbreaking smart devices (hardware or firmware) compromises the manufacturer's security settings, elevates the security risks, and makes it easier to gain unauthorised access to a CAV network infrastructure[113]. Tampering of hardware and software elements is a real risk, especially when conducted at the source during the manufacturing process. This includes the introduction of backdoor elements within the hardware or code that can be used as an access mechanism to spy or attack the CAV network infrastructure.
Mitigation	Using CIS controls and principles, it is recommended that Inventory and Control of Hardware assets be implemented to minimise the risk of tampering. Hardware tamper resistant, detection and security certification techniques should be implemented as major security precautions. A security awareness and training program is required to educate subscribers and provide adequate information on how to properly use these assets and keep them safe and secure. A tight control of the asset manufacturers' employees should be instituted with careful vetting and risk assessments conducted prior to any OEM or component manufacturer being allowed in the supply chain.
	CIS 1 & 17

[113] Bhasker, D. (2013). 4G LTE security for mobile network operators. Cyber Secur. Inf. Sys. Inf. Anal. Cent.(CSIAC), pp.20-29.

Related Interactions/Assets	Modem, SIM card, connectivity interfaces such as Bluetooth, Wi-Fi and GPS.
Mitigation Status	Partially Mitigated

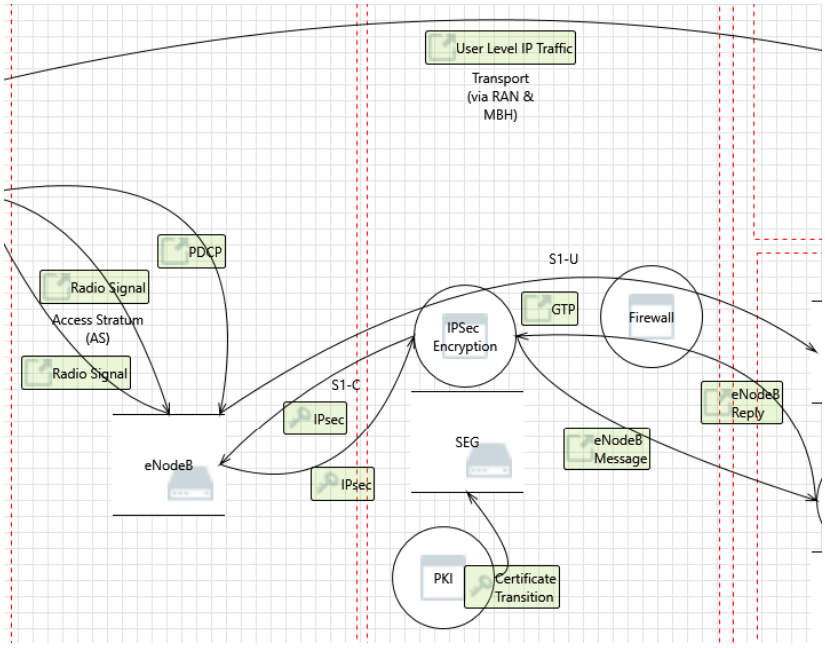
Threat	Risk of Data Loss and Unauthorised Data Access
Category	**I**nformation Disclosure
Description	With an ever-increasing storage capacity, electronic devices used in the today's vehicle wireless architecture have larger memory and storage capacities than ever before, making them attractive targets for attackers. Confidential user data on these connectivity devices are vulnerable to hacking and attackers can gain unauthorised access to files and data leading to personal information being compromised, data loss or leakage and a violation of victims' privacy[113].
Mitigation	Data protection security controls such as data encryption at rest and password protected solutions to limit access to sensitive information on connected devices is highly recommended. Access control and data input and output procedures should be implemented for vehicle files and data. It may also be required to implement Malware defence and data recovery controls to reduce the risk of data disclosure and data loss.
	CIS 13, 8 & 10
Related Interactions/Assets	Modem, UE
Mitigation Status	Partially Mitigated

Threat	Side-Channel Attack
Category	Tampering/ Information Disclosure
Description	These are attack actions undertaken on the Automotive Security Controllers (ASC). ASCs are micro-controllers used in security critical applications such as vehicle access, mobile communications (eSIM) and black box data logging. They provide security functions to protect against illegal access to data and security credentials including passwords, keys. Side-channel attacks are usually non-invasive and are carried out by monitoring the electromagnetic field emissions while a device is performing cryptographic operations. The measured patterns are then used to reverse engineer the process and retrieve the cryptographic keys. This vulnerability then exposes the security and authentication credentials and thereby threatening the confidentiality and integrity of the CAV system[114].
Mitigation	ASCs such as the Integrated Controllers in eSIM cards should be hardened with additional hardware protection to protect against side-channel attacks. It is highly recommended to use session keys to limit vulnerability and exposure if cryptographic keys are compromised.

[114] Machold, M., Brunner, M., & Steurich, B. (2019) Future requirements for automotive hardware security. Post EVITA Semiconductor Security Quo Vadis?

	Only ASCs with high levels of protection that can initiate an active counter-reaction in the event of an attack, such as an application termination or deletion of critical memory contents should be used in the CAV ecosystem[114].
	CIS 1 & 5
Related Interactions/Assets	Modems, SIM cards, Wireless connectivity interfaces
Mitigation Status	Partially Mitigated

11.3.2. RAN



Threat	Physical Attacks
Category	**E**levation of Privilege / **T**ampering
Description	eNodeB's installation in public location are vulnerable to physical tampering[113]. External attackers may be presented with opportunities to gain access to critical functions of the mobile network through physical tampering of easily accessible devices in poorly secured eNodeB site locations and microcell base stations.
Mitigation	Inventory and control of hardware assets and strong incident response and management processes are recommended by CIS to reduce the risk of this threat. It is recommended to adopt strict control of the operational functions of the network and implement strong physical security mechanism to protect against any illegal and unauthorised access to any network node or interface that can be used to launch an attack.
	CIS 1 & 17
Related Interactions/Assets	eNodeB UE access to RAN
Mitigation Status	Mitigated

Threat	Rogue eNodeB Attack
Category	**I**nformation Disclosure / **D**enial of Service
Description	In this type of attack, an attempt is made to introduce a rogue eNodeB element into the LTE network. Rogue eNodeB attacks allow for the duplication of the functionality of the base station by exploiting vulnerabilities in the protocol stack such as IP and SS7. The rogue base station is then used to impersonate the operator's node and enable interception of voice and data transmission across the network. The attacker can therefore passively eavesdrop, redirect user traffic to a different network and conduct packet modification or injection[113].
Mitigation	Implementation of strong end-to-end security protocols including authentication and traffic protection mechanisms between the UE and core networks is strongly recommended. Use of strong encryption during the UE attach procedures as well as implementation of mutual authentication between eNodeB, MME and HSS will minimise rogue element attacks. Wireless Intrusion prevention and wireless intrusion detection system can also be used rogue eNodeB for detection and minimise such attacks. From an operations point of view, it is recommended that MNO's continually monitor their access networks in real time for rogue access points and wireless attack tools to enable quick identification and elimination.
	CIS 11 & 6
Related Interactions/Assets	eNodeB UE access to RAN
Mitigation Status	Partially Mitigated

Threat	Eavesdropping, Identity tracking, Man in the Middle Attack (MitM)
Category	**I**nformation Disclosure
Description	Attackers can take advantage of a known weakness in the LTE protocol stack wherein the user identity transference occurs unencrypted, in clear text between the UE and the eNodeB, during the initial attach procedure. A MitM attack can be staged by capturing the IMSI which can then be used to impersonate and track a user. This allows a malicious node to create an independent connection between the UE and the network. It is then able to eavesdrop the communication, hijack ongoing sessions and inject or fabricate data thereby compromising the integrity and confidentiality of the CAV infrastructure[113].
Mitigation	Use of public key infrastructure (PKI) with the public key of the MNO stored in the USIM enables encryption of privacy-related information such as the transmission of the IMSI to the eNodeB. It is also recommended to use robust authentication mechanisms and digital signature to prevent MitM attacks. CIS recommends to continually run and assess vulnerability management programs in order to identify new and zero-day attacks.

	CIS 9, 3 & 15
Related Interactions/Assets	eNodeB UE access to RAN
Mitigation Status	Partially Mitigated

Threat	Paging Attack / Loss of Privacy
Category	**I**nformation Disclosure
Description	Attackers can take advantage of vulnerabilities in the LTE paging protocol to locate UEs by injecting paging requests multiple times and correlating the gathered TMSI of the phone with the paged permanent identity IMSI[113]. Unencrypted transmission of paging messages over the wireless channel is a vulnerability that can compromise a subscriber's identity. Paging attacks can result in drastic consequences for victims, enabling an attacker to conduct targeted location tracking, obtain a victim's IMSI, inject fabricated emergency alerts and perform paging channel hijacking. This can lead to a complete loss of confidentiality, privacy and integrity of the CAV system.
Mitigation	It is also strongly recommended to implement strong encryption mechanisms between the UE and the eNodeB to guard against attackers using IMSI paging and location tracking vulnerabilities and protect the privacy of subscribers and the confidentiality of the CAV infrastructure. CIS recommends the implementation, maintenance, monitoring and analysis of audit logs to monitor network traffic and ensure signalling integrity.
	CIS 6, 9 & 15
Related Interactions/Assets	eNodeB UE access to RAN
Mitigation Status	Partially Mitigated

Threat	Replay Attack / Loss of Privacy
Category	**I**nformation Disclosure / **T**ampering
Description	In replay attacks, an intruder can capture the authentication parameters sent by the MME and replay the intercepted authentication request to an unsuspecting UE. When the UE receives a replay of an intercepted authentication request it will send a synchronisation failure message, thus allowing the intruder to verify the presence of the subscriber through the received error message response. This attack has the potential to enable location tracking thus compromising privacy and security[113].
Mitigation	It is strongly recommended to implement techniques for protecting against replay attacks, such as EPS-AKA mechanism, timestamping and use of a freshness value. CIS recommends the implementation, maintenance, monitoring and analysis of audit logs to monitor network traffic and ensure signalling integrity.
	CIS 6, 9 & 15

Related Interactions/Assets	eNodeB UE access to RAN
Mitigation Status	Not Mitigated

Threat	eNodeB/Femtocell/Microcell Compromise
Category	**T**ampering / **D**enial of Service
Description	eNodeB may use a virtualized Linux operating system instead of a custom OS that has been explicitly hardened and made secure during development. If a virtualized eNodeB is successfully attacked by exploiting a security flaw in the commercial hypervisor or operating system, it may fail or be used as a launch pad for attacks against the overall network infrastructure causing service disruptions. If an attacker can get into a trusted device like an eNodeB, the attacker can navigate to many other internal devices[115].
Mitigation	CIS recommends basic controls including configuring the software and hardware securely and implementing continues vulnerability management programs.
	CIS 5 & 3
Related Interactions/Assets	eNodeB eNodeB access to EPC
Mitigation Status	Mitigated

Threat	Botnet-Launched DDOS Attacks
Category	**D**enial of Service
Description	A botnet of infected UE could be used by attackers to synchronize the behaviours of a group of malicious users Botnet in 4G mobile networks can be used as platforms to launch DDoS attacks against the air interface. The core idea of this proposed attack scenario is botmasters activate all botnet nodes at the same time and let them start downloading a large file or send dummy data to create congestion on the downlink or the uplink[116].
Mitigation	CIS recommends to security control the software assets and use appropriate security configurations. It is also necessary to monitor and analyse transmission channels to identify this kind of attacks.
	CIS 2, 5 & 6
Related Interactions/Assets	UE, eNodeB
Mitigation Status	Not Mitigated

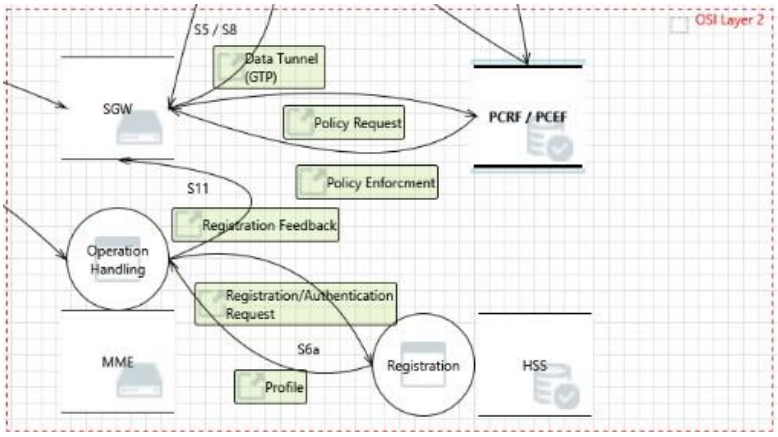
Threat	Radio Frequency Jamming
Category	**D**enial of Service
Description	These are attack actions on the communications medium between the UE and the network. RF jamming attacks are therefore

[115] Macaulay, T. (2013) The 7 Deadly Threats to 4G. 4G LTE Security Roadmap and Reference Design, McAfee: Santa Clara, CA, USA

[116] Bassil, R., Chehab, A., Elhajj, I., & Kayssi, A. (2012) Signaling oriented denial of service on LTE networks. in Proc. ACM Int. Symp. Mobility Manage. Wireless Access, 153158.

	interference attacks involving deliberate transmission of radio signals with the aim of disrupting communications by decreasing the Signal-to-Noise Ratio (SNR) of the received signal to a point where there is a complete loss of service. In LTE, jamming attacks on the synchronisation signals containing Primary Synchronisation Signal (PSS) and the Secondary Synchronisation Signal (SSS) prevents the UE from selecting the cell leading to a DoS situation.
Mitigation	Jamming attacks on the control channels in LTE can be mitigated by transmitting the vulnerable control data in unused parts of the data channels. Other mitigation solutions include monitoring of abnormally high-power levels in control channels, ensuring that control channels are randomised in time and frequency as well the use of shared keys to transmit location information to a UE.
	CIS 15, 9 & 6
Related Interactions/Assets	UE, eNodeB UE connection to eNodeB
Mitigation Status	Partially Mitigated

11.3.3. EPC – OSI Layer 2



Threat	Remote De-Registration Attack
Category	**D**enial of Service
Description	In this scenario, an attacker can exploit implementation flaws in MMEs that causes them to de-register a legitimate UE attached to the network without notification, resulting in a DoS for the victim UE. The attacker establishes an RRC connection spoofed as the victim using the legitimate UE's S-TMSI and then proceeds to send a NAS message such as an invalid security protected message or an initial plain request message to the MME serving the victim. The MME will then process the received NAS message from the attacker inappropriately and will consequently de-register the connection of the victim UE without any notification

	This attack was demonstrated by researchers[117] against a live operational LTE network and should be considered a major security threat for CAVs using LTE as a connectivity platform.
Mitigation	CIS controls recommend the implementation, management and correction of the configuration of network elements using rigorous configuration management and change management processes. De-registration attacks are mainly possible due to incorrect implementation of the MME and its functionalities in the EPC. Therefore, this attack is mitigated by implementing an MME that adheres fully with the 3GPP standards and requirements.
	CIS 12 & 11
Related Interactions/Assets	UE, eNodeB , MME
Mitigation Status	Mitigated

Threat	Authentication & Key Agreement (AKA) Bypass Attack
Category	**I**nformation Disclosure / **T**ampering
Description	The connection between the UE and MME is mutually authenticated after the initiation and completion of the Authentication and Key Agreement procedure. The procedure is completed when the UE sends the NAS authentication response to the MME. At this stage, all control plane messages that should be protected are encrypted and integrity protected using the agreed security algorithms. However, researchers[117] demonstrated that an AKA bypass attack can be employed to bypass the existing encryption of user data between the UE and MME. An AKA bypass attack can be launched by using a rogue eNodeB and actively exploiting a known weakness to skip the key agreement procedure in the RRC layer. This then nullifies the security context of RRC and user data allowing for an attacker to spoof the RRC messages and intercept private information and communication of the victim's UE.
Mitigation	Since the AKA bypass attack stems from lack adherence to the mandatory security procedures, it can be mitigated by making sure that the MME and UE do not continue with any control plane procedures prior to the successful completion of the mandatory security procedures. CIS recommends assessing and taking continuous action on new information in order to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers.
	CIS 3, 15, 9
Related Interactions/Assets	UE, eNodeB, EPC, HSS, AuC
Mitigation Status	Partially Mitigated

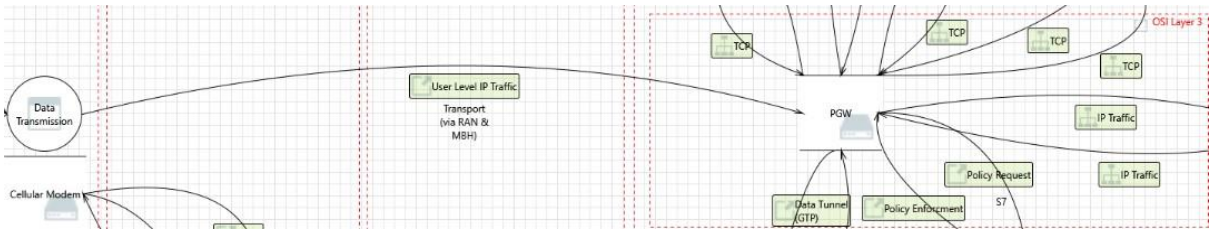
[117] Kim, H., Lee, J., Lee, E., & Kim, Y. (2019). Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane.

Threat	Signalling Storm Attack
Category	**D**enial of Service
Description	Signalling traffic can be maliciously generated by an attacker through repeated and simultaneous sending of multiple dedicated bearer or NAS requests with the expressed intention of disrupting the services provided by the EPC. If the maliciously generated signalling load exceeds the actual capacity of the MME, then services may be impacted. This is because the resources available at the core network is being diverted away from serving genuine and legitimate subscribers effectively leading to a DoS.
Mitigation	CIS recommends the continuous maintenance, monitoring and analysis of network audit logs. It is also recommended to control network traffic between network nodes by employing boundary defence solutions. Despite intrusion prevention systems and network and traffic monitoring mechanisms, signalling storm attacks cannot be entirely prevented.
	CIS 6 & 12
Related Interactions/Assets	UE, EPC, MME, HSS/AuC
Mitigation Status	Not Mitigated

Threat	Single Key Dependency
Category	**I**nformation Disclosure / **T**ampering
Description	Safeguarding the key used in the cryptographic algorithm such as EPS-AKA is a major security concern in LTE networks. If the source key (K) that is shared between the UE and the HSS and used to derive all the future keys is compromised, then the network becomes vulnerable and attackers can exploit this vulnerability and be easily authenticated by the LTE network, jeopardising the integrity and confidentiality of the network. The EPS-AKA protocol used currently in LTE is therefore rooted on the secrecy of the permanent key K. If K is compromised, especially given advances in quantum computing, then the security of the network cannot be guaranteed[118].
Mitigation	CIS recommends management of the ongoing operational use of protocols, and services on networked devices in order to minimise windows of vulnerability available to attackers It is also recommended to implement robust key management mechanisms that provide a balance between computational complexity and the secure storage and use of cryptographic keys.
	CIS 9 & 16
Related Interactions/Assets	UE, EPC, MME, HSS/AuC
Mitigation Status	Not Mitigated

[118] Rajakumar , A., Raja, G., Almagrabi, A. O., Alkatheiri, M. S., Hussain, C. S., & Bashir, A. K. (2019) A Quantum-safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario

11.3.4. EPC – OSI Layer 3



Threat	Billing Attacks
Category	**S**poofing
Description	Overbilling and billing-escape attacks generally result in revenue losses for service providers but also are an indication of compromised systems or networks. This needs to be mitigated and addressed to protect the integrity and security of the network infrastructure and the confidentiality of the network subscribers. In these exploits, an attacker hijacks the IP address of a legitimate subscriber when the IP address in being returned to the IP pool and takes control of it. The attacker then utilises the services at the expense of the legitimate subscriber's account[119].
Mitigation	Limitation and control of network protocols and services is recommended by CIS. It is also necessary to monitor and control accounts. A proper continuous vulnerability management program is also useful. Deployment of security gateways, firewalls, IDS and IPS are recommended by many infrastructure vendors. The use of VLANs for network and traffic segregation as a security measure is suggested.
	CIS 9,16 & 3
Related Interactions/Assets	UE, PGW
Mitigation Status	Partially Mitigated

Threat	Interface Attacks Through External Networks
Category	**I**nformation Disclosure / **T**ampering
Description	LTE has an All-IP architecture that exposes it to attacks that are originated at the interfaces that connect the LTE core network to external networks such as roaming networks and external IP networks such as the internet. The SGi interface of the PGW interconnects multiple IP networks containing many untrusted devices. An attacker can employ these untrusted devices to launch an attack on the core network through various IP-based attack mechanisms that includes use of Malware, port scanning, Botnets etc. Similarly, the S5/S8 interface is used to interconnect the LTE core network to external operator network to support roaming customers.

[119] Mobarhan, M. A., Mobsrhsn, M. A., & Shahbahrami, A. (2012) Evaluation of Security Attacks on Different Mobile Communication Systems. Canadian Journal on Network and Information Security, vol. 3, no. 1

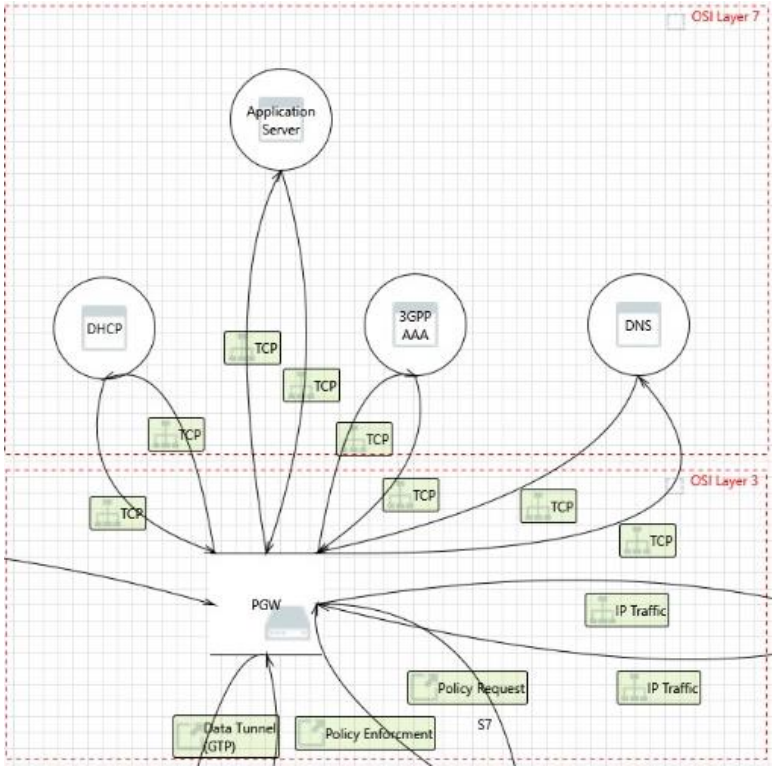
	Attackers can use a device in the untrusted external network to launch attacks on the core network through the S8 interface[120].
Mitigation	A security gateway (SEG) should be implemented as a firewall at the edge of the core network interfacing with external IP networks. The security gateway must be implemented with the capability to filter and drop malicious traffic at the entry point to the core network as well as DPI and IPS and internet noise filtering capabilities. It is recommended by CIS controls to securely configure servers and control access to network elements. Network protocols and services should be limited and controlled.
	CIS 4,9 & 14
Related Interactions/Assets	PGW, Application Servers
Mitigation Status	Partially Mitigated

Threat	Network Snooping
Category	**I**nformation Disclosure / **T**ampering
Description	Breach of confidentiality can occur when an attacker intercepts an information flow between two nodes in a SIP session. Without adequate security mechanisms, attackers can use tools like Wireshark to capture SIP signalling data[121]. Session hijacking involves the attacker inserting malicious packets, substituting traffic and breaching integrity. Packet tampering, information leakage, network scanning, SIP flooding and resource exhaustion are all attack vectors that are rooted in LTE's flat All-IP architecture.
Mitigation	It is recommended to implement encryption of SIP and other signalling data. CIS recommends securely configuring servers and implementing tight controls on access to network elements. Network protocols and services should be limited and controlled.
	CIS 4,9 & 14
Related Interactions/Assets	UE, PGW, Application Servers
Mitigation Status	Partially Mitigated

[120] Liyanage, M., Ylianttila, M., & Gurtov, A. (2013) A Case Study on Security Issues in LTE Backhaul and Core Networks. ResearchGate

[121] Slezak, D., & Gelogo, Y. (2011) Securing IP Multimedia Subsystem with the appropriate Security gateway and IPSec Tunnelling. *Journal of security engineering*

11.3.5. EPC – OSI Layers 4-7



Threat	GPRS Tunnelling Protocol (GTP) snooping attacks
Category	**S**poofing / **D**enial of Service
Description	GTP is a Signalling and tunnelling protocol used to transfer user and control data between the UE, SGW and PGW. Compromised network elements can enable an attacker to snoop into GTP traffic and extract sensitive subscriber data such as APN credentials. In addition to eavesdropping, an attacker can generate malicious requests to cause DoS, gain unauthorised access to an APN or redirect an existing GTP tunnel to another PGW.
Mitigation	It is recommended to implement a GTP firewall that has the functionality to inspect GTP traffic. IPS and DoS prevention capabilities are also suggested. It is suggested to control network boundary and control access to network devices and services. Application software security implementation is also recommended by CIS.
	CIS 12, 9 & 18
Related Interactions/Assets	UE, SGW, PGW, Application Servers
Mitigation Status	Partially Mitigated

Threat	Service Abuse Attacks, Theft of Service
Category	**E**levation of Privilege / **S**poofing
Description	The IMS can be accessed by an attacker through a compromised UE. Theft of service is achieved by the UE not releasing the established media stream between a UE and IMS core after a “Bye request” message has been sent to the call session control function

	(CSCF). This causes the CSCF to stop accounting for the session while the attacker continues to gain access to the services[122].
Mitigation	Strong authentication functionality between the UE and IMS networks, as well as the implementation of security gateways (SEG) to ensure confidentiality of data between client and IMS network CIS recommends use of application software security controls and to implement necessary limitation on network protocol and services. Secure configuration of servers is also required.
	CIS 18, 9 & 5
Related Interactions/Assets	UE, Application Servers, PGW
Mitigation Status	Partially Mitigated

[122] Belmekki, E., Bouaouda, N., Raouyane, B., & Bellafkih, M. (2013) IP Multimedia Subsystem: Security Evaluation. Journal of Theoretical and Applied Information Technology, vol. 51, no. 1

12. Security Testing

A primary outcome from investment in a CAV Security Framework, within a cyber security testing centre of excellence, is the ability to perform real cyber security tests against vehicles, products, systems and services. This section examines cyber security testing within the CAV ecosystem at the practical testing level.

12.1. Introduction to Testing

Prior to the advent of connectivity, testing a vehicle, or any system, many have been time consuming, but was essentially straightforward. It involved comparing the operation of a system function to its design specification. For complex systems this may mean many thousands, or tens of thousands, of individual tests. For each test, if the result differs from what the specification states, then that piece of system functionality is incorrect.

Manufacturers and suppliers devote considerable resources to such functional testing. Test teams develop repeatable test sets and test *oracles*, which can be used against the products or systems being constructed. However, as the previous section discussed, communications and software-based technologies have made the testing process challenging, due to the need to discover vulnerabilities that may be present and pose a potential cyber risk. It causes a paradox, in that you need to test for vulnerabilities, but you do not know the technical details, i.e. the specification, of those vulnerabilities until they have been found. This requires some of the techniques described earlier in the report, i.e. running a TARA, quantifying risks and performing security testing techniques.

Any testing process needs to be systematic, results orientated, and with reported outputs that are measurable. To achieve this a variety of metrics need to be established. Metrics allow test results to be meaningful. If results are meaningful, they can be compared with test results from other products or previous testing sessions. Unfortunately, establishment of meaningful metrics within cyber security testing has proven problematic in the past. The nature of computerised systems is part of the problem. Once a system receives a software update it is no longer the same system that was previously tested. However, useful metrics can be established, and it is the requirement of the framework to build up a bank of skills, experience, techniques, tools and practical tests. That bank of knowledge that can be called upon by the CAV industry stakeholders to perform the necessary cyber security testing of all the elements within the CAV ecosystem.

12.2. Black Box to White Box Testing

One aspect to consider with regards to performing testing at the cyber security testing centre, is how far along the black box to white box spectrum should be supported. At the outset the items to be tested will be considered a black box. Aside from operational information provided for the DUT or SUT, testing occurs with no knowledge of the detailed operation of the internals of an item under test. This is a natural state for two reasons. Firstly, the protection of IP. Manufacturers and tier component suppliers will protect their IP and not reveal details that may compromise IP. This means enough information is provided to use an item, but not reveal how the item operates internally. Secondly, this is the view that attackers have of a system, i.e. cyber security testing can proceed as if the tester is viewing the system as an attacker.

However, grey box testing and white box testing is not discounted. Grey box testing may be required when additional technical information is required in order to carry out or complete a specific test, or when a component, sub-assembly or individual part is being tested.

White box testing, where full access to detailed technical design documents, including full access to software source code, is required, is likely to be done by the manufacturers and tier one suppliers themselves. This does not preclude the CAV cyber security test centre from performing white box testing, but there is unlikely to be a large demand.

12.3. Effective Testing and Testing Metrics

Measuring the results from the security testing is important in assessing the effectiveness of the testing process. For a cyber security testing centre the reporting of metrics demonstrates to the customers the work performed. However, it must be made clear that security testing metrics are difficult to use as a measure of cyber security improvement. As previously stated, comparing systems or iterations of systems is difficult due to the inherent differences between systems and system versions. However, what can be used to compare systems and iterations of systems is the reduction, or even increase, in the perceived cyber security risk to a system. Furthermore, completing security testing does not mean that a system is secure; there may still be unknown vulnerabilities waiting to be found. What systematic testing does achieve, when executed via a repeatable and reporting process, is demonstrate a best effort in security risk reduction. The testing ensures that:

- Designed mitigation has been applied.
- Assessed risks have reduced.
- If any anticipated risks remain, then planned mitigation has not occurred.
- Possible new vulnerabilities are discovered, in which case the risks will be noted as having increased.

There are metrics that can be used in relation to the management (project and personnel) and economics of security testing, for example Return on Investment (ROI) (was the spending on security testing less than the potential loss from fixing an undiscovered vulnerability in the field). These are useful for the manufacturer's finances; however, metrics must be considered that are concerned with quantitative technical aspects of the testing, and not whether the cost of finding a defect outweighs the cost of a security breach. The technical aspects of the system security are the prime concern for a security testing centre, and therefore, the metrics that relate directly to security performance (risk reduction) must be considered.

Measuring the effectiveness of security testing is an area of ongoing of research. The science is attempting to move it further from subjective results towards quantitative data. However, specific data points are highly dependent upon the DUT or SUT being tested and the types of testing being executed. For example, a penetration test on an in-vehicle network is different to a jamming test on a 4G signal. Furthermore, as implied above, results between two different iterations of systems may not be comparable. For example, a software update will change a system to a new state, i.e. the updated system is not identical to the previous version.

This report is not going to list specific security metrics that could recorded within the Security Framework, as they are highly dependent upon the SUT and specific test being executed. Furthermore, security testing that is approached as a black box exercise is inherently less

precise than white box testing, where, for example, percentage of code coverage could be easily recorded.

Once the test results have been obtained then various types of analytical reports and charts can be generated using the recorded metrics. The goal is to generate meaningful actionable reports. Reports have two major aims. Firstly, and most importantly, a report that addresses the ability of the DUT or SUT to reduce cyber security risk. Secondly, management reports that allow the operators of the testing centre to demonstrate execution of the testing process.

Another outcome of reporting is to view testing over an extended time period. This has two strands, customers can view any trends over different testing sessions, and the testing centre can view any operational trends over an extended timeline.

It will be a function of the Security Framework development to establish a list of technical metrics relevant to a test, and the metrics that can be recorded during testing. It will be important for the tooling used to support the framework (and the tooling within the testing centre) to enable measurements to be recorded as easily as possible, preferably automatically, for efficiency. Specifically, the results recording process must not get in the way of executing the security tests.

12.4. Testing Phases within Product Development

The forthcoming ISO/SAE 21434[42] standard, *Road vehicles - Cybersecurity engineering*, addresses cyber security via different phases of a product's development. These phases are covered by the different clauses of the proposed standard:

- Overall cyber security management (governance and culture)
- Project dependent cyber security management
- Continuous cyber security activities (executed throughout a product's lifetime), includes:
    - Cyber security monitoring (what is happening in the ecosystem)
    - Cyber security event assessment (analysing incident impacts)
    - Vulnerability analysis (determining security issues)
    - Vulnerability management (correcting security issues)
- Risk assessment (i.e. performing TARA)
- Concept phase (new product proposal, assess cyber security goals)
- Product development (new product engineering to include security considerations)
- Cyber security validation (testing for issues)
- Production (product build)
- Operations and maintenance (incident management and updates)
- Decommissioning (end-of-life management)
- Distributed cyber security activities (suppliers and related services)

Expertise within the cyber security testing centre may well cover all the above phases. In terms of physical test execution, that is likely to occur as part of the *Continuous cyber security activities*. It is also likely to occur in support of *Cyber security validation*, in which designed in security considerations are assessed, probably with specific intention to address any known common vulnerabilities, existing CVEs, and correct application of encryption. The validation phase:

- validates cyber security goals and claims;
- determines if an item satisfies cyber security goals;
- determines if residual risks are acceptable.

To help with the validation the requirements are:

- a validation specification;
- penetration testing, with the extent controlled by risk considerations;
- the resultant outputs being handled by the *Vulnerability management* process.

As with all cyber security considerations, validation phase, and the testing overall, is not trying to eliminate risk, which is not possible, it allows for acceptable risks.

12.5. Security Testing Considerations

The ability to compromise communication, automotive and IoT systems has seen a growth in cyber security research and testing beyond the traditional IT domain. Across the globe, researchers and security engineers have demonstrated multiple security weaknesses within non-IT systems. Alongside the search for security weaknesses, solutions to protect and enhance security are being tried and implemented. Cyber security is concerned with both cyber attack and cyber defence. The security properties within a system that cyber security address are:

- confidentiality - preventing the exposure of data, password, encryption keys, and personal information;
- integrity - ensuring data and information is not changed, corrupted or deleted, and including associated mechanisms, for example data non-repudiation;
- availability - disrupting data flows, system operation and access to systems.

The methods used to attack confidentiality, integrity and availability (CIA) on system, i.e. the types of test to perform, include:

- sniffing - covertly reading data to gain system and operational information, and to extract private data;
- replay - capturing data and then re-transmitting the data onto a communications network, allows the attacker to send data as though it originated from within the system, the attacker may also benefit from delaying replayed data;
- spoofing - generating data so that it appears to originate within the systems but is generated by the attacker;
- denial-of-service (DoS) - flooding the system network with two much data can overload components and they are no longer able to correctly perform their functions;
- man-in-the-middle (MITM) - data is diverted through the attacker, allowing the attacker to surreptitiously change data and monitor results;
- malformation (e.g. fuzzing) - manipulating data formats or values to confuse the software in a component or system;
- malware - changing the code on a component or within a system to affect the data and systems;
- social engineering - manipulating humans or the human machine interface (HMI) to influence behaviour.

The above attack methods may need to be used in combination to achieve a successful attack. The outcome of a successful attack will vary, based upon:

- the attacker's motivations and aims;
- the attacker's technical knowledge and expertise;
- how well the system is designed and engineered;
- the presence of security mechanisms to counter attacks.

The same factors above will affect the magnitude of the outcome from an attack:

- no noticeable effect - an attack is taking place, but the impact is not observed by systems users, examples include system data sniffing or exfiltration of personal data, or the attack is having negligible effect on system performance;
- minor degradation of performance - the system is functioning as intended but the performance is below normal levels of operation, for example a vehicle's braking may not be as sharp as normal, for an Intelligent Transport System (ITS), this may mean that traffic signals will be commanded to change at a reduced rate;
- major degradation of performance - the system performance is severely impacted, a vehicle may have switched into a limp mode, or some traffic signals have failed;
- complete system failure - a vehicle has stopped functioning, all the signals in an area have failed, typically a full DoS attack has been successful.

Finally, consideration of how attacks can be propagated will influence any risk mitigation actions:

- direct attack - the attacker connects directly to the system, for example via a wireless interface;
- indirect attack - a cloud-based system or third party device provides a proxy through which an attack is launched;
- automated attack - an attack is setup on external systems to be launched against targets, for example, by using a botnet;
- self-propagating attack - the attacker uses malware that is able to replicate across components, vehicles and infrastructure, for example, via a worm, trojan or virus.

12.6. Security Testing Tooling and Supporting Systems

Test execution will require supporting systems and tooling. For the entire end-to-end testing process, this will include data servers, workstations, networking, test equipment and software. Access to specialised test facilities may be required for some tests, for example testing over the air transmissions may require a vehicle sized Faraday cage. The broadcast of radio signals on most frequencies requires a valid license; therefore, it is illegal, even for testing purposes to broadcast radio signals without appropriate licenses. Thus, large Faraday cages, or other forms of isolated or remote facilities may be required.

The size and complexity of testing the CAV ecosystem and the number of expected tests to execute requires the consideration of a high level of automation and simulation. The use of automation improves test coverage, test execution speed, repeatability, reproducibility and overall testing efficiency. Simulation, including digital twins, enables the support of a wider

range of testing cases for interactive systems. It allows for the simulation of large numbers of agents in test scenarios that may be prohibitively expensive, unrealistic, or not scalable if performed in a real environment.

Much of the tooling will be in the form of software:

- operating systems for servers and workstations;
- software used to maintain the security framework and manage the cyber security testing centre;
- software tools used to manage, setup and run tests, record, store and analyse the test results and generate report on the results, including the forensic analysis of data and visualisation of data, and test equipment operating software;
- specialist software used for systems design and development can re-purposed for simulation and running digital twins, however, it is likely that high performance computing (HPC) systems for digital twins will be required for multi-agent simulations;
- tools for systems maintenance and maintenance of vehicles.

The software tools that run the security tests will vary according to the tests performed. The different classes of tools include:

- static and dynamic code analysers;
- network traffic analysers;
- vulnerability scanners;
- fuzzers;
- brute forcing software;
- hardware debuggers;
- interface scanners;
- application automation software;
- proof of concept exploit checkers.

There are many tools used by security researchers, including the same tools used by the system attackers. Many tools are sold and supported by commercial companies. A wide range of open source tools[123] exist to support security testing and research. Customised and technology specific tools will be required to supplement the readily available tools. Engineers that can write software will be a necessity when investigating the security of the wide range of technologies in use with the CAV ecosystem.

The software and systems to test different views of the CAV ecosystem will vary based on the technology being tested and the executed tests. Testing the security of a vehicular cloud service will require different tools and techniques compared to testing an in-vehicle network which interconnects ECUs. Table 21 gives an example of different tools used to test different aspects of a CAV, and Table 22 show specific tests performed on one of the units, a telematics box[30].

[123] https://sectools.org/

Table 21. Example of testing different CAV components with different tools

Test points	Test tools	Details
Telematics Box (T-Box)	Nmap	Test security of the ports and running services opened
ECU	Defensics	Fuzz testing by communication protocol
Mobile apps	JEB2	Decompile apk application
	AppScan	Discover vulnerabilities, hosts and services
	Protecode	Analyse, detect and check the known vulnerabilities of binary codes
	Burp Suite	Intercept unencrypted data
	IDA-Pro	Decompile and dynamically debug binary file
Radio/IVI	GNU Radio	Capture and record signal from the wireless key fob, GPS spoofing
	USRP	Capture and record signal from the wireless key fob, GPS spoofing
	HackRF	Capture and record signal from the wireless key fob, GPS spoofing

Table 22. Specific tests performed on a telematics unit

Test points	Test cases
Telematics Box (T-Box)	Check if uboot UART debug interface can be accessed to install firmware
	Check if any port is open and whether the opened port is secure
	Check if the memory can be tamper or expose
	Check if the firmware is secure
	Check if T-Box connects to a server using a secure mechanism

	Check the GPS privacy
	Check the XSS attack
	Verify the T-Box authentication
In-Vehicle Infotainment (IVI)	Handling of GPS spoofing
	Malicious Digital Audio Broadcasting (DAB) signal injection
	Tyre Pressure Monitoring System (TPMS)
	Microphone eavesdropping
	Other data connected through the IRC channel
	Jamming attack to disrupt the information
	MirrorLink protocol vulnerability
	Fake WiFi connection
	Android app to record sound
Electronic Control Unit (ECU)	Injected malicious code to OBD dongle
	Fuzz testing by sending random data to ECU
Mobile Application (MA)	Car sharing apps: user account leakage
	Auto diagnostic app
	XSS vulnerability - test by Burpsuite
Radio	Edge spoofing
	Spoofing trajectory data (aim at ITS)
	Bluetooth BlueBorne attacks

13. Procedures Around Testing

13.1. Cyber Security Testing Services

By taking the above discussion around the technical discovery and classification of issues, and combining with traditional professional services models, several potential service offerings arise, providing different levels of insight into the security of a system.

As discussed within this document, there are various communications technologies and networks that will be used by a connected vehicle, and testing each of these is important. The offerings outlined below primarily target the C-V2X realm of communication:

- These communications are based on IP-based networking; tooling for such testing is mature and can be automated
- Most of these communications leave the vehicle over some form of radio data network (3G/4G/LTE/5G)
- Testing facilities, such as Millbrook, are uniquely placed to offer insight into mobile network systems. Millbrook has a licence to operate a private mobile network and has the equipment. Furthermore, that equipment can be isolated from the publicly available networks, this will significantly aid the testing process.

The proposed method via which to assess the C-V2X or V2C communications of a ‘black box’ system, is to perform a passive MITM capture of traffic using a private mobile network. With the CAV deliberately connected to the private network, all communications to and from the connected vehicle can be captured and inspected. The proposal is for this information to be captured in a standard format such as a ‘.pcap’ packet capture file, that can be processed automatically, as well as manually reviewed.

The expectation is that the packet captures will be analysed to look for security issues pertaining to the protocols in use by the system, as well as its general resilience to a hostile network environment. These technical findings will be used to create a technical report.

However, a technical report in isolation is rarely the best way to offer insight to security issues. It is important to contextualise the technical report with the client, for them to gain the most insight from the findings. In Table 23 three tiers of assessment methodology are proposed:

Table 23. Levels of Cyber Security Testing Services

Cost/Time	Description	Deliverables
Base	• Automated analysis of C-V2X and V2C comms as part of a professional services or consultancy engagement	• Technical report with contextualising additions • Discussion/workshop/presentation around work conducted
Medium	• Automated analysis of C-V2X and V2C comms as part of a professional services or consultancy engagement • Comprehensive threat modelling of the system assessed	• Technical report with contextualising additions • Threat model document • Discussion/workshop/presentation around work conducted
High (variable)	• Automated analysis of C-V2X and V2C comms as part of a professional services or consultancy engagement • Comprehensive threat modelling of the system assessed • Further (manual) assessment of any facet of the system in agreement with the client	• Technical report (of automated C-V2X and V2C testing) with contextualising additions • Threat model document • Technical report of the manual assessment performed • Discussion/workshop/presentation around work conducted

The above is structured such that a client can choose the appropriate level of service, without this having an impact on the delivery of existing work.

In all cases the 'professional services engagement' is a discussion with the client prior to the testing about their black box system and its purpose. This is for the service to provide the context necessary to fully discuss the technical issues identified. Another discussion will take place after the testing has been conducted in order to discuss the results as well as to answer any questions the client may have.

It is important to note that for the high cost service offering, the cost will vary depending on the amount of manual testing required.

13.2. Handling an Identified Vulnerability (Table-top Exercise)

Whilst technical reports and contextualised security insight are useful to an organisation, without taking any action, this does nothing to improve a system's security. The way in which an organisation deals with any vulnerability, determines how much improvement to security occurs. Indeed, certification processes (see Section 14) will require evidence of audits and exercise of company procedures to ensure proficiency in addressing identified vulnerabilities, including the current management of security incidents.

It is proposed to offer a 'vulnerability workshop' exercise as a standalone/add-on to the above services. This would, at a high level, revolve around various representatives of an organisation discussing how they would respond to a proposed scenario. This allows an organisation to better understand their processes and procedures in such a situation, to build relationships with key individuals that will have to work together in difficult circumstances, as well as to identify where individual's responsibility may end, overlap, or be entirely absent.

In a ‘table-top exercise’ (conducted onsite at the testing facility), where the appropriate representatives of the client organisation are presented with a variety of cyber security incident scenarios, to which they must respond as an organisation.

Examples of such scenarios could include:

- The remediation of issues from a technical report (which could be from the previously discussed services)
- The appearance of a zero-day exploit on the system, discovered via social media
- Leaking of customer data from what appears to be an internal system
- A denial of service condition, caused by an issue with a third-party supplier

The organisation will respond to the situation (being prompted by the consultant), which will evolve as the scenario progresses. Given the nature of the scenarios that can be used, a wide range of representatives from an organisation should be present, which can include:

- System engineers
- Management
- Security
- Network Operations
- Legal
- Human Resources
- Public Relations
- Customer Support

The workshop will highlight any strengths or weaknesses in an organisation’s current policies and procedures, as well as gaps which require additional investment. It will also serve as a “fire drill” for such policies. At the end of the workshop, the organisation should have a much better idea of how well equipped it is to deal with a range of cyber security scenarios, as well as how it could improve its response in the case of any future, real, incidents.

13.3. Ongoing Testing and Diagnosis

Most of the standards, best practices and guidelines recommend the ongoing test and diagnosis, for example, PAS 1885[124] and ENISA[46] best practice. It is well-recognised that security assessment is not a one-time process as the security situations including the threat landscape and security objectives evolve.

Evaluation on the security posture of a system relies heavily on the knowledge of attack surface and threat landscape. Therefore, any updates in this knowledge can change the assessment significantly. For example, attackers can find a new method to make a low-likelihood threat more feasible. New vulnerabilities on software or hardware can also create novel surfaces for attackers to exploit the system. Given the relations between the attack surfaces, the occurrences of any new low-risk threats may lead to significant security attacks. Consequently, it is important to understand the security knowledge that the risk assessment is based on. This can be done firstly by maintaining a database of threats as well as their relations through Attack Trees. The database should provide essential information regarding

[124] BSI (2018) PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

the potential techniques to launch a threat or a set of threats (via Attack Trees); which impacts they can create on the system; and the relevant mitigations. Secondly, any changes with the research literature should be reflected in the database. For example, any new threats on system assets; any new combination between the threats to create a significantly increased attack impact; any new techniques that lower the barriers to launch threats; or any new method that makes a mitigation invalid or less efficient. Ideally version management, or version control, of any knowledge base or database is maintained. Then, security assessment of a system can be mapped to a knowledge base version to aid analytics, testing traceability and reporting. Testing should indicate that security assessment of the system is based on a certain version of the knowledge base. Version control is important for the maintenance of other vulnerability databases such as CWE or NVD; however, the difference in the vehicular domain is that the knowledge base maintains only attacks that have significant impacts on CAV ecosystem security. Furthermore, the security assessment target vehicles will be recorded, as a cyber security risk profile, which contains all the relevant information for the risk assessment, such as the list of the critical assets, their functions, operating requirements, and the relevant threats.

When there are updates in the knowledge database, the risk profiles need to be scanned to see whether the previous risk assessment assumptions are still hold. The overall attack surfaces should be reassessed to identify any new risks. Meanwhile, the impacts of relevant threats, assets, functions, and mitigation also need to be reconsidered. If there are significant changes in the risk assessment results, the testing centre needs to inform the relevant entities (manufactures, vehicle owner, service providers, application developer, etc.) that the previous risk assessment is not valid anymore. The testing centre can suggest an update of the new risk assessment if a theoretical analysis is reliable; or it can schedule a reassessment if needed.

When maintaining the vulnerability databases and risk profiles, the number of test cases will grow, possibly exponentially. Automated software can be used to manage the proactive threat monitoring procedure. It is also essential to represent the system architecture, threat and risk assessment by a standard modelling language (see Section 4.2.5) so that it can be useful for the software.

14. Certification

There are different ways to define rules. For example, they can be laid down in laws, trade bodies regulations, standards or specifications. Rules are important in many aspects of modern economies. They are primarily present to ensure human safety and fair treatment for all, but also exist to ensure the interoperability of systems and smooth running of processes. Certification is the common mechanism to ensure, or attempt to ensure, the repeatable application of rules. Certifications provide benchmarks to indicate that correct processes, specifications, or competencies are present in organisations, products, or professionals.

14.1. Summary of Current Vehicle Certification

The use of certification is well established throughout the lifecycle of a vehicle. In the UK the Vehicle Certification Authority (VCA) is responsible for type approval for new vehicles. Type approval, which may be referred to as homologation, ensures that a vehicle meets correct regulations and standards with regards to their construction for environmental and safety reasons. However, type approval cannot guarantee that a vehicle is free of design defects.

Design defects may emerge once vehicles enter the marketplace. When a design defect has an impact on safety, a vehicle manufacturer will issue a recall notice to get the defect rectified.

Without the recall process, manufacturers would be open to many more liability issues. Vehicle manufacturers, and their component suppliers, may be liable if a product is defective and causes death, injury, loss or damage. This is the reason that a new vehicle will undergo an extensive pre-production testing program, to ensure the vehicle is safe, thereby reducing liability.

There are thousands of tests performed during the pre-production testing program of a new vehicle. A large proportion of the tests will relate to the electronic and computerised functions of the vehicle systems. All the vehicles currently manufactured rely upon the use of computerised systems, and these systems are now connected to external networks and the devices that vehicle occupants carry. How these vehicle systems function can impact vehicle safety, and thus manufacturer liability.

To address the testing of vehicle systems, manufacturers use the internationally agreed standard ISO 26262, Functional Safety for Road Vehicles. It is used by manufacturers and their suppliers for functional safety testing and risk reduction in their complex electrical and electronic systems. However, this was originally implemented before the age of the connected car. The primary impact of vehicle connectivity on safety is the cyber security threat. Researchers have demonstrated proof-of-concept cyber attacks on vehicular systems and infrastructure, and real-world examples of attacks have occurred. This raises the consideration of whether some form of cyber security certification in the automotive, communication and related industries can help maintain low cyber security risks.

14.2. The Pros and Cons for Vehicular Cyber Security Certification

Certification is not an unknown quantity for an organisation. Many organisations achieve ISO 9001 certification to demonstrate to customers a commitment to quality control[125], often required in supplier contracts. Conformance to standards related to the security of traditional enterprise Information Technology (IT) systems also exist, for example, the ISO/IEC 27000 family of standards for Information Security Management, another example of cyber security certification, for the UK, is the Cyber Essentials scheme from the National Cyber Security Centre[126]. However, certification in no way guarantees security, as the regular reports of security breaches demonstrate[127]. What cyber security certification does achieve is to raise awareness of security issues and systematically apply a best practice process, especially when it comes to a management process when needing to handle a cyber attack. Thus, the real aim for certification is to reduce the risk of a cyber attack occurring and to reduce the consequences of a cyber attack when it does occur.

One downside of certification is the addition of a business cost. The certification uses resources that could otherwise be used within the core day-to-day business function. However,

[125] ISO. ISO 9001:2015 Quality management systems — Requirements. 2015. url: https://www.iso.org/standard/62085.html
[126] National Cyber Security Centre. Cyber Essentials. 2014. url: https://www.cyberessentials.ncsc.gov. uk/
[127] Paolo Passeri. Hackmageddon. 2020. url: https://www.hackmageddon.com/

the economic consequences for an organisation in not having good cyber security practices in place may be a lot higher. The same argument applies to the automotive domain, where proof-of-concept and real-world cyber attacks have been deployed, therefore, there is the need to address the cyber security of vehicular systems and the communications links to infrastructure.

Another issue with certification is the possibility of becoming complacent with regards to security. Once certification against a standard has been obtained, an organisation needs to be proactive in maintaining the procedures and adapting designs and processes. This is to cater for changes in technology, business operations, suppliers, standards, and regulations that affect an organisation's products and services. Certification is not a line the sand but a moving target that should always be in sight, otherwise security risk can increase. The point to be made is that cyber security is not a fixable problem, instead, it is an ongoing process of risk reduction and incident handling. This raises a discussion on the type of certification that would be applicable for handling the cyber security testing of vehicular systems and communication infrastructure.

14.3. Automotive Domain Cyber Security Testing Processes Certification

The ultimate objective of a TARA process is to enable a reduction in a system's attack footprint. For a complex system-of-systems, such as the CAV ecosystem, this need to be done efficiently to maximise the benefit from the limited costs (time and resources). Our proposed Security Framework can provide the systematic guidance required for efficient use of resources. As discussed in the previous section, the nature of cyber security means that certification is unable to be prescriptive with regards to technology. Indeed, the technical organisations that issue standards for interoperability will have their test regimes for equipment compatibility. In the CAV ecosystem, such organisations include:

- ITU - International Telecommunication Union
- ETSI - European Telecommunications Standards Institute
- IEEE - Institute for Electrical and Electronics Engineers
- SAE - SAE International (previously Society of Automotive Engineers)

In 2017 the UK Government issued the report *The Key Principles of Cyber Security for Connected and Automated Vehicles*[128]. It listed eight high-level principles that organisations should follow to reduce security issues. This was soon followed by the British Standards Institute's (BSI) PAS 1885:2018[124], *The fundamental principles of automotive cyber security - Specification*, in 2018. The latter references some of the eight principles listed in the former. These publications are not standards in themselves and involve no certification, they do provide guidelines on the process of managing the security of a CAV throughout its lifetime, highlighting the need to take a proactive approach to security throughout an organisation, from the board to the product designers, where the security considerations are embedded into a CAV's design from the outset of its life cycle. The forthcoming international standard ISO SAE 21434[42], *Road vehicles – Cybersecurity engineering*, currently in draft status, is security process focused. This new joint ISO/SAE standard supersedes the previous SAE J3061,

[128] HM Government (2017) The Key Principles of Cyber Security for Connected and Automated Vehicles. Tech. rep.

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems[2] which covered security practices from concept design to decommissioning.

It is not surprising that ISO is developing a standard for cyber security in road vehicles. The ISO standard ISO 26262, *Road vehicles - Functional safety*[129] is the international standard used by vehicle manufacturers and their supplies to analyse and reduce risks in the functional operation of cars and their components. It is widely used within the automotive industry and has matured through different versions. ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems that are installed in series production road vehicles. The latest 2018 version of ISO 26262 acknowledges the intersection with cyber security and is aware of the need to separately address the topic, it references the forthcoming ISO SAE 21434. This new joint ISO/SAE *cyber security engineering* standard considers the required cyber security management processes within an organisation:

- overall cyber security management - covering governance, culture, risk management, audits, information sharing and security, and managing tools;
- product cyber security management - covering requirements, recommendations, responsibilities, planning, reuse, components, and assessments;
- continuous cyber security activities - covering monitoring, requirements, recommendations and assessment of events

ISO SAE 21434, thoroughly developed over some years, is likely to become the go-to standard for vehicle manufacturers needing to implement cyber security practices within their organisation and product development processes, just as ISO 26262 became the go-to standard for functional safety. However, adherence to the ISO standard is not intended to be measured through a certification process. As for ISO 26262, organisations will have personnel trained on the provisions of the standard, who can apply it to the organisations' processes. An industry exists around ISO 26262 for training to provide personnel with the relevant capabilities to apply the standard. Some of the companies that provide ISO 26262 training do offer exams as a form of competency assessment, it is a form of self-certification. A similar industry is likely to emerge for the ISO SAE 21434 standard. However, the United Nations Economic Commission for Europe (UNECE) is incorporating certification in its proposed assessment of a manufacturer's Cyber Security Management System (CSMS).

UNECE hosts the World Forum for Harmonization of Vehicle Regulations, the forum is coded as, and commonly known as, WP.29. The forum is used for provisioning global regulations on vehicle safety and environmental issues. A WP.29 document is "proposing provisions for the approval of cyber security management systems as well as of vehicles with regard to cyber security"[130]. The UNECE proposals will require vehicle manufacturers to obtain a *Certificate of Compliance for Cyber Security Management System*. This will be achieved through the existing vehicle Type Approval processes, in the UK that would be through the VCA. However, it is worth noting that UNECE provisions do not override national regulations and laws.

[129] ISO (2018) ISO 26262-2:2018 Road vehicles - Functional safety - Part 2: Management of functional safety. Geneva

[130] Task Force on Cyber Security Issues and Over-The-Air Software (2020) 'New UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems'

The CSMS proposed by UNECE will require a manufacturer to document their cyber security management processes, and the processes used to assess the cyber security of the vehicle which is seeking cyber security type approval. Manufacturers will need to apply for a Certificate of Compliance for CSMS, with the application assessed by the appropriate Approval Authority (AA) (the VCA in the UK). The AA will verify that the CSMS complies with the proposed UNECE regulations, and if approved it will be valid for three years. The CSMS must cover several areas of the organisation's processes and vehicle cyber security testing, including:

- the life cycle of a vehicle - development, production, post-production;
- the organisation's cyber security management process;
- risk management identification of risks to a vehicle, their assessment, categorisation and treatment;
- security testing processes;
- ongoing risk assessment;
- monitoring, detecting and responding to cyber attacks, threats, and vulnerabilities;
- management of dependencies with third parties and other organisational divisions;
- handling of aftermarket software, services, and data;
- modifications after being granted type-approval;
- conformity in production.

As for ISO 23232 and ISO SAE 21434, the UNECE CSMS is not prescriptive on tools and techniques that need to be used. The UNECE proposal does have an annexe that lists threats, and possible mitigation techniques, but these are at a high descriptive level. This makes sense as they need to allow for changes in technology and testing techniques.

The UNECE proposal on cyber security is still changing and can be viewed on the UNECE W.29 website[131], though it can be easier to find the latest version on the website GlobalAutoRegs.com[132].

14.4. Certification Conclusion and Recommendation

The point was made that vehicle certification, commonly called type approval, exists to ensure that vehicles are safe to use, and safe for other road users. Increased connectivity and computerisation have introduced new threats to safety due to the possible interruption of operation from the risk of a cyber attack. The industry has responded to the threat with the new ISO SAE 21434 standard and the UNECE CMS proposal. They both recognise that unlike a technical specification, for example, an implementation of a particular version of communications protocol, cyber security is not a fixed target. Therefore, they look at the process of risk mitigation, to ensure that cyber security risk assessment and mitigation best practice is deployed. The nature of cyber security does not allow for a completely protected device; however, a ‘best effort’ must be undertaken by manufacturers, and this is what ISO with SAE and UNECE are trying to achieve.

[131] UNECE (2020) ‘World Forum for the Harmonization of Vehicle Regulations (WP.29)’ url: https://www.unece.org/trans/main/welcwp29.html
[132] GlobalAutoRegs (GAR) (2020) ‘WP.29 Rulemaking Project Draft Recommendation/UN Regulation on Cyber Security’, url: https://globalautoregs.com/documents?rule_id=226

The development of the ISO/SAE standard and the UNECE CSMS is complementary. The processes in ISO SAE 21434 are covered by the requirements of the CSMS, though differences may be present as they are both still in development. It can be envisaged that, as for ISO 23232, ISO SAE standard will become the benchmark for vehicle manufacturers assessing the cyber security of their new models. Then the CSMS certification for type approval will be issued based on manufacturers demonstrating their competence with ISO SAE 21434, not only in applying it to the management of the cyber security engineering process but to the cyber security engineering of new vehicle models.

Use of ISO SAE 21434 and the UNECE CSMS in the UK should happen as part of the normal UK type-approval process through the VCA, or at least the UK Government should ensure it happens. However, to aid the strengthening of cyber security within the UK CAV ecosystem, stakeholder organisations should also implement general cyber security schemes, these include the UK's Cyber Essentials programme[133], and the VCA may want to include such schemes within the requirements for the UNECE CSMS certification. The UK VCA should also encourage CAV stakeholders to engage with the various cyber security committees and proposing organisations to ensure that any standard, proposal or scheme addresses the UK's requirements. That work should also include a gap analysis to determine where differences exist and how those differences could be reduced or handled.

[133] National Cyber Security Centre (2014) ‘Cyber Essentials’, url: https://www.cyberessentials.ncsc. gov.uk/

15. Summary and Recommendations

Connected computational systems see an ever-increasing role within society, this includes CAVs. There are benefits to be gained from a fully mature CAV ecosystem, however, it crosses two of the thirteen designated CNIs, communications and transport, and cyber attacks are a threat to CNIs. Whilst successfully executed cyber attacks may impact operational infrastructure and organisations, they may also impact all of us as individuals. Access to online services, privacy issues, travel disruption, online fraud, identity theft and data loss are all possible. Such issues are well established cyber crimes and the CAV ecosystem is another platform on which criminals may perform them. Whenever and wherever networked systems operate the need for cyber security vigilance is required.

CAV ecosystems are complex super-systems with vehicles, communication and roadside infrastructure, cloud-based services, legislative and certification concerns, and associated services and management. Cyber threat risk reduction could be seen to be overwhelming. However, by approaching it systematically, through the application of a Security Framework (see Figure 2 for the high-level overview), it can be addressed. The information and arguments presented in this report provide a foundation for the full development and implementation of the Security Framework, with input from relevant stakeholders (see Section 1.3), and it can, and should, evolve as technology and threats change.

Security considerations must be taken into account when a new engineering endeavour begins, threat modelling can take place early in the design cycle. The whole process can begin with excellent engineering from the beginning of the initial concept for a new vehicle or associated system, together with systematic cyber security testing and risk assessment from the outset. The stakeholders in the UK's emerging CAV ecosystem can achieve that with the aid of cyber security centres, virtual and physical proving grounds and other physical CTFs. Within these facilities, the engineers and consultants can apply the Security Framework for the efficient execution of TARAs, practical security tests and results reporting. The framework enables efficient use of the technology and communications infrastructure within a cyber security centre. The framework can facilitate the dissemination of security and testing knowledge and encourage best practice. Systematic application of the framework, covering the topics presented in this report, can reduce the cyber threats to the CAV ecosystem.

15.1. Specific Recommendations

The BeARCAT project partners have identified several recommendations to make from this report (repeated in the Executive Summary):

- Future investment in a CAV security testbed would be beneficial to the UK's emerging CAV industry and ecosystem, and to the communications and cyber security domains. The investment would provide a foundation for world-leading research in CAV and communications security assessments, risk reduction and cyber resilience techniques.
- Communications infrastructure and cloud services are areas of the CAV industry that are identified as requiring focus for cyber security investment. There has been and continues to be, substantial interest in the cyber security issues related to in-vehicle and sensor systems. This continues to be important, however, the CAV communications and cloud services technologies would benefit from equal attention as they become increasingly part of the marketplace.

- Investment in the design and development of a CAV cyber testing Security Framework to benefit the UK's transport and communications CNIs.
- It is important to realise that C-V2X may yet become the global automotive connectivity standard and we need to prepare for that, with testing, evaluation and development of the standards.
- It is not certain how C-V2X will interact with DSRC, if at all, but further research is required in this area to establish the best way forward for the UK.
- A special focus should be given to the communication system required to support real-time V2V, which is unlikely to be C-V2X or DSRC in the near term.
- Certification of the cyber security testing process is required. Procedures based around ISO SAE 21434, which can be regarded as a superset of the UNECE CSMS, are likely to be embraced by vehicle manufacturers.

The several areas that would benefit from research investment to accelerate the adoption of a CAV and communications testing Security Framework are:

- Investment to research and develop the Security Framework for the CAV ecosystem.
- Investment in new software tooling to support, disseminate and keep relevant the framework.
- Investment to research and develop a CAV ecosystem security testing knowledge base as part of the framework.
- Investment to encourage stakeholders to engage and network to exchange information and resources on cyber security threats to the CAV ecosystem.

The UK is a leader in cyber, vehicle and communications technology and can provide, and does provide, centres of excellence in understanding, testing and countering threats. That skill base can be used to protect the CAV ecosystem, and aid the development of the UK CAV industry, and contribute to the overall UK cyber security expertise. This report provides the relevant stakeholders with the baseline information to fully develop an industry-relevant Security Framework. The overall goal of the Security Framework is to keep the cyber security risks in the CAV ecosystem to a residual level, maintaining CAV cyber resilience.

Glossary of Abbreviations

This glossary can be used to lookup the meaning of an abbreviation within the report text. When an abbreviated term is first used it will be written in full immediately followed by the bracketed abbreviation. Subsequent use of the term will be the abbreviated version.

1G	First Generation
2G	Second Generation
3G	Third Generation
3GPP	Third Generation Public Partnership
3GPP AAA	3GPP Authentication, Authorization, Accounting
3GPP TS	3GPP Technical Specification
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
AES	Advanced Encryption Standard
AN	Access Node
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
BSC	Base Station Controller
BRAM	Block Random Access Memory
BSI	British Standards Institute
BTS	Base Transceiver Station
CAM	Connected and Automated Mobility
CAN	Controller Area Network
CAV	Connected and Autonomous Vehicle or Connected Automated Vehicle
CC	Conventional Communications
CC	Country Code
CGI	Cell Global Identity
CI	Cell Identity
CIA	Confidentiality, Integrity, Availability
C-ITS	Cellular Intelligent Transport Systems
CMPv2	Certification Management Protocol v2
CN	Core Network
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure
CPRI	Common Public Radio Interface
CPS	Cyber-Physical System
CSMS	Cyber Security Management System
CTF	Cyber Test Facility
C-RNTI	Cell Random Network Temporary Identifier
C-V2N	Cellular Vehicle-to-Network
C-V2X	Cellular Vehicle-to-Everything
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service

DHCP	Dynamic Host Configuration Protocol
Diameter	4G protocol, replaces the RADIUS signalling protocol
DNS	Domain Name System
DoDAF	Department of Defense Architecture Framework
DoS	Denial of Service
DoS	Denial of Service
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability
DSRC	Dedicated Short-Range Communications
DUT	Device Under Test
ECU	Engine Control Unit
ECU	Electronic Control Unit (a vehicle computer)
EDGE	Enhanced Data rates for Global Evolution
EIR	Equipment Identity Register
eNodeB	Evolved NodeB
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EVITA	E-safety Vehicle Intrusion proTected Applications
GERAN	GSM EDGE Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GUTI	Globally Unique Temporary Identifier
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HSS	Home Subscriber Server
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange v2
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
IPsec	IP Security Protocol
ISO	International Standards Organisation
ITS	Intelligent Transportation Systems
ITS-G5	ITS 5 GHz Access Layer
ITU	International Telecommunication Union
IVI	In-vehicle Infotainment
IVN	In-vehicle Network
LAC	Location Area Code
LSP	Label Switched Paths
LTE	Long Term Evolution
LTE-A	LTE Advanced
MAP	Mobile Application Part
MAPSec	MAP Security Protocol
MBSE	Model Based Systems Engineering

ME	Mobile Equipment
MIB	Master Information Block
MitM	Man-in-the-Middle
MME	Mobility Management Entity
MNC	Mobile Network Code
MODAF	Ministry of Defence Architecture Framework
MPLS	Multiprotocol Label Switching
MSC	Mobile Switching Centre
NAF	NATO Architecture Framework
NAS	Non-Access Stratum
NodeB	3G base station
NGTP	Next Generation Telematics Patterns
OSI	Open Systems Interconnection
PASTA	Process for Attack Simulation and Threat Analysis
PDN GW	Packet Data Network Gateway
PGW	Packet Gateway
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RA	Reference Architecture
RAN	Radio Access Network
RUP	Rational Unified Process
S1	The interface between eNodeB and MME/SGW
SAE	SAE International (previously Society of Automotive Engineers)
SBA	Service-Based Architecture
SEG	Security Gateway
SGW	Serving Gateway
SIB	System Information Block
SIM	Subscriber Identity Module
SMS	Short Message Service
SN	Serving Network
SS7	Signalling System No.7
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, DoS, Elevation of Privilege
SUT	System Under Test
SysML	Systems Modelling Language
TAL	Threat Agent Library
TARA	Threat Analysis and Risk Assessment
TARA	Threat Agent Risk Assessment (Intel)
TAU	Tracking Area Update
TDM	Time Division Multiplexing
TMSI	Temporary Mobile Subscriber Identity
ToE	Target of Evaluation
UART	Universal asynchronous receiver-transmitter
Uconnect	Connectivity platform used by some connected vehicle OEMs
UE	User Equipment
UK	United Kingdom
UML	Unified Modelling Language

UMTS	Universal Mobile Telecommunications System
UNECE	United Nations Economic Commission for Europe
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
V2C	Vehicle-to-Cloud
V2D	Vehicle-to-Device
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VAST	Visual, Agile, and Simple Threat
VLR	Visitor Location Register
VOLTE	Voice Over LTE
X1	The interface between eNodeBs
XSS	Cross Site Scripting

Thanks go to the BeARCAT Project Contributors

Alphabetical order by company and last name:

Cisco

Maria Christopher
Mike Emery
John Kucernak
Joel Obstfeld
William Wu

Millbrook

David Kernohan
Peter Stoker

Telefonica

Mahmoud Al-Ghreify
James Bonner
Farhad Foroughi (AWTG)
Bryony Grimes
Sering Harding (AWTG)
David Owens
Jose Ramirez (AWTG)

WMG at the University of Warwick

Omar Al-Jarrah
Jo Bailey
Daniel S. Fowler
Anh Tuan Le
Sunyoung Lee
Carsten Maple
Alisdair Ritchie
Hu Yuan

Page left intentional blank.

END