EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS

NOVEMBER 2019

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use iot-security@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

ACKNOWLEDGEMENTS

Charalambos Tsitlakidis, European Commission – DG Communications Networks, Content and Technology

Christophe Jouvray, Valeo

Markus Tschersich, Continental

Gianmarco Baldini, European Commission – DG Joint Research Center

Jasja Tijink, Kapsch Trafficcom AG

Erwan Broquaire, Cerema

Jocely Delatre, ACEA

Ba Sadio, the National Cybersecurity Agency of France (ANSSI)

Dimitri Havel, Aston Martin Lagonda

Andy Davis, NCC Group

Carsten Maple, University Of Warwick, UK

Timo Van Roermund, NXP Semiconductors

Alessandro Farsaci, CNH Industrial - Iveco Commercial Vehicle

Ian Smith, GSMA

Reda Yaich, IRT SystemX

Johan Lindqvist, Volvo Cars

Christian Wieschebrink, the Federal Office for Information Security (BSI), Germany

Jan Muenther, Here Technologies

Christian Urban-Seelmann, Wabco

Horst Klene, Volkswagen AG

Mouhannad Alattar, Alliance Renault-Nissan-Mitsubishi

Lorenzo Perrozzi, Garrett Advancing Motion

Achim Fahrner, ZF Friedrichshafen AG

Michael Feiri, ZF Friedrichshafen AG

Jan de Meer, Association for Computing Machinery

Eetu Pilli-Sihvola, the Finnish Transport and Communications Agency Traficom

Jacques Kunegel, ACTIA Group

Joachim Lueken, Nokia Bell Labs

Julien Burlet, National Gendarmerie, Ministry of the Interior, France

Thomas Born, Vodafone

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-317-9, DOI 10.2824/17802

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report defines good practices for security of smart cars, namely connected and (semi-) autonomous vehicles, providing added-value features in order to enhance car users' experience and improve car safety. Taking stock of all existing standardization, legislative and policy initiatives, this report aims to serve as a reference point to promote cybersecurity for smart cars (connected and automated cars) across Europe and raise awareness on relevant threats and risks with a focus on "cybersecurity for safety".

The automotive industry is undergoing a paradigm change towards connected and autonomous vehicles[1]. Smart cars already available today provide connected, added-value features in order to enhance car users' experience or improve car safety. With this increased connectivity (that the emergence of 5G is expected to further promote) novel cybersecurity risks and threats arise and need to be managed.

It is undeniable that there is a rapid pace when it comes to technological advancements in the area of connected and autonomous cars. With the emergence of semi-autonomous and autonomous cars, which make use of advanced machine learning and artificial intelligence techniques, the potential risks and cybersecurity challenges increase. Moreover, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interfaces needed for the deployment of intelligent transport systems and autonomous cars, further exacerbate security risks since they largely expand the potential attack surface and attack vectors.

With the increasing smart cars connectivity and the emergence of (semi)-autonomous cars, novel cybersecurity challenges, risks and threats are arising. Attacks targeting smart cars may lead to vehicle immobilization, road accidents, financial losses, disclosure of sensitive and/or personal data, and even endanger road users' safety. Thus, appropriate security measures need to be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians.

It is therefore important to analyse the relevant threats and cybersecurity risks pertaining to smart cars and put forward security measures to address these risks taking into account the particularities of this highly complex, heterogeneous and volatile environment.

Accordingly, this ENISA study provides the following information:

- High level reference model of connected and autonomous vehicles.
- Detailed asset and threat taxonomy for the connected and autonomous vehicles ecosystem.
- Concrete and actionable good practices to improve the cybersecurity posture of connected and autonomous vehicles.
- Mapping to existing legislative, standardization and policy initiatives to foster harmonization.

[1] See JRC 2019 Report 111477, Alonso Raposo M., Grosso, M., Després, J., Fernández Macías, E., Galassi, C., Krasenbrink, A., Krause, J., Levati, L., Mourtzouchou, A., Saveyn, B., Thiel, C. and Ciuffo, B. An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. Effects of automated driving on the economy, employment and skills:
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111477/kjna29226enn.pdf

1. INTRODUCTION

Over the last few years, the automotive industry has undergone a paradigm change towards increasingly connected and autonomous cars. Smart cars available today are vehicles equipped with systems providing connected and added-value features in order to enhance car users experience and/or improve car safety. Within the next few years, smart cars' connectivity is expected to expand and smart cars will become connected to other vehicles, pedestrians and their surrounding infrastructure through information exchanges via Vehicle-to-Everything (V2X) communications[2]. Semi-autonomous and autonomous cars (i.e. levels 4 and 5 of autonomy as defined in SAE J3016[3]), which make use of advanced Machine Learning (ML) and Artificial Intelligence (AI) techniques, are also emerging. Indeed, several smart cars stakeholders (including car manufacturers, system suppliers, road operators and other providers) are already carrying out trials of supervised autonomous vehicles, with a driver on board ready to take control of the car if necessary.

In recent years, there has been a growing interest in autonomous cars both from end users and manufacturers and deployment of smart cars has a growing rate in the automotive market[4][5]. According to a survey of 5,500 global city dwellers from all around the world[6], 58% of global respondents are willing to take a ride in a driverless vehicle. Acceptance rates are higher in emerging markets such as China (75%) and India (85%) than in European countries such as United Kingdom (49%) and Germany (44%). However, the European economy is expected to benefit from autonomous vehicles[7], as EU gathers 23% of global motor vehicle production. Moreover, almost 72% of inland freight is transported by road in Europe, and trust in Original Equipment Manufacturers (OEMs) is strong. While optimistic predictions mention that fully automated vehicles could be widely deployed by 2030[8], scientific experts are more cautious and underline that further research is still required to build a fully autonomous vehicle, mostly in the fields of AI and cybersecurity[9].

Cybersecurity is a crucial aspect that will affect the evolution of smart cars. There have already been several research publications on attacks targeting smart cars. One of the most known attacks is the spectacular proof-of-concept remote attack[10] where the researchers took control of a vehicle and sent it off-the-road, thus leading to the recall of over a million cars. Lately, some researchers also demonstrated that it was possible to locally or remotely take control of smart

[2] See EC Communication "On the road to automated mobility: An EU strategy for mobility of the future": https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf, May 2018
[3] See SAE J3016 "Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles": http://sae.org/standards/content/J3016_201806/
[4] See JRC 2019 Report 111477, Alonso Raposo M., Grosso, M., Després, J., Fernández Macías, E., Galassi, C., Krasenbrink, A., Krause, J., Levati, L., Mourtzouchou, A., Saveyn, B., Thiel, C. and Ciuffo, B. An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. Effects of automated driving on the economy, employment and skills:
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111477/kjna29226enn.pdf
[5] See Autonomous cars: a big opportunity for European industry: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Autonomous%20cars%20v1.pdf, January 2017
[6] See "Self-Driving Vehicles in an Urban Context": http://www3.weforum.org/docs/WEF_Press%20release.pdf
[7] See European Commission "On the road to automated mobility: An EU strategy for mobility of the future": https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf
[8] See "Rethinking Transportation 2020-2030 – The disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries":
https://static1.squarespace.com/static/585c3439be65942f022bbf9b/t/591a2e4be6f2e1c13df930c5/1494888038959/RethinkX+Report_051517.pdf
[9] See "Self-driving Ubers could still be many years away, says research head": https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head
[10] See "Hackers remotely kill a Jeep on the highway – with me in it": https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

cars infotainment system[11] by exploiting diagnostic services to manipulate smart cars functions. Moreover, security specialists succeeded to hijack cars using their smart alarm, thereby illegitimately performing actions such as enabling/disabling the immobilizer or cutting the engine[12]. Towards the objective to provide a generic development and evaluation environment for vehicle cybersecurity technologies, an open-source testing platform called PASTA[13] (Portable Automotive Security Testbed with Adaptability) was recently released; it simulates the remote operations of vehicle wheels, brakes, windows, and other features to learn more about the electronic communications features and find vulnerabilities as well as test exploits. However, such a platform may also be used by an attacker, thus facilitating their tasks.

With the increasing smart cars connectivity and the emergence of (semi)-autonomous cars, novel cybersecurity challenges, risks and threats are arising. For instance, there have been some experimental remote attacks[14,15] on autonomous cars' cameras and Light Detection and Ranging (LiDAR) systems showing effective camera blinding, making real objects appear further than their actual locations or even creating fake objects. In addition to malicious sensor manipulations, other attack vectors have been practically demonstrated such as Global Navigation Satellite Systems (GNSS) spoofing[16] and fooling AI-based functions[17] with the famous example of trapping a self-driving car by just drawing a chalk circle around the vehicle. Attacks targeting smart cars may lead to vehicle immobilization, road accidents, financial losses, disclosure of sensitive and/or personal data, and even endanger road users' safety. Thus, appropriate security measures need to be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and even the privacy of vehicle passengers and all other road users, including pedestrians.

1.1 OBJECTIVES

This ENISA study aims at addressing the security and privacy challenges related to the evolution of smart cars. The main objectives were to collect good practices to ensure the security of smart cars, while mapping the relevant security and privacy challenges, threats, risks and attack scenarios.

More specifically, the aim of this study is to identify the good practices in order to ensure smart cars security against cyber threats, while focusing on V2X communications and (semi-) autonomous cars[18]. Towards this end, the following objectives have been set:

- Analyse smart cars architecture and define a high-level reference model
- Identify smart cars sensitive assets
- Identify potential and main cyber threats, risks and attack scenarios targeting smart cars
- Map identified threats to assets
- Identify relevant security measures based on the threats and assets, and map the identified security measures to the relevant threat(s).

[11] See "Experimental security assessment of BMW cars: A summary report": https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf
[12] See "Hacking smart car alarm systems": https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/
[13] See "PASTA: Portable Automotive Security Testbed with Adaptability": https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-Toyama-PASTA-Portable-Automotive-Security-Testbed-with-Adaptability-wp.pdf
[14] See "Remote attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR": https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf
[15] See "Self-driving and connected cars: fooling sensors and tracking drivers": https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf
[16] See "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems": https://www.usenix.org/node/217477
[17] See "Meet the Artist Using Ritual Magic to Trap Self-Driving Cars": https://www.vice.com/en_us/article/ywwba5/meet-the-artist-using-ritual-magic-to-trap-self-driving-cars
[18] See SAE J3016 "Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles": http://sae.org/standards/content/J3016_201806/

This ENISA study aims to serve as a reference point to promote collaborative automotive cybersecurity across the European Union and raise awareness of the relevant threats and risks with a focus on "security for safety".

1.2 SCOPE

This ENISA study outlines good practices for the security of smart cars. It is building on the previous ENISA study on smart cars entitled "*Cyber Security and Resilience of Smart Cars*"[19] and mainly focuses on V2X communications and (semi-)autonomous cars[20] as these technologies were not previously considered.

During this study, ENISA identified available documentation and standards on smart cars cyber security, with a focus on connected and autonomous cars. ENISA also collected inputs from a number of automotive security experts through a structured questionnaire and a series of interviews. Following a thorough analysis of the identified material and the review of security experts feedbacks, ENISA identified the main assets and threats targeting smart cars. Based on these threats, a set of security measures and good practices were defined to ensure smart cars security.

The study highlights three groups of security measures to address security challenges in terms of technologies, policies and processes. A risk-based and holistic approach to security was undertaken. ENISA considered the cybersecurity of smart cars throughout their lifecycle (from conception to end-of-life) and addressed all the essential elements of automotive cybersecurity. Particular attention was paid to the overall supply chain while considering the different stakeholders involved in the smart cars manufacturing (i.e. OEM, software and hardware components providers, etc.).

1.3 EU AND INTERNATIONAL POLICY CONTEXT

The various attacks on smart cars[10,16,17,21,22,23,24] that were publicly reported over the last few years led to a relatively quick awareness of the automotive industry of the security needs and the development of several cybersecurity regulations and initiatives aiming to ensure properly secure vehicles, as presented below.

- **EU Policy**:
  - Early 2014, the Commission's Directorate-General for Mobility and Transport (DG MOVE) set up a C-ITS deployment platform. This latter was conceived as a cooperative framework including national authorities, Cooperative Intelligent Transport Systems (C-ITS) stakeholders and the European Commission with the objective to identify and agree on how to ensure interoperability of C-ITS across borders and along the whole value chain, as well as to identify the most likely and suitable deployment scenario(s).
  - In 2017, the Directorate-General for Internal Market, Industry, Entrepreneurship and Small and Medium-sized Enterprises (SMEs) (DG GROW) launched an initiative on safety regulations with the aim to contribute to a further decrease of the number of road fatalities and injuries considering amendments to the General Safety Regulation and the Pedestrian Safety Regulation.

[19] See ENISA (2016) "Cyber Security and Resilience of smart cars – Good practices and recommendations": https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[20] See SAE J3016 "Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles": http://sae.org/standards/content/J3016_201806/
[21] See "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR": https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf
[22] See "Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications": https://eprint.iacr.org/2017/613.pdf
[23] See "Fast and Vulnerable: A Story of Telematic Failures": https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf
[24] See "Robust Physical-World Attacks on Deep Learning Visual Classification": https://arxiv.org/pdf/1707.08945.pdf

- In 2018, the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) launched an initiative on Cooperative, Connected and Automated Mobility (CCAM) with the aim to:
  - provide further guidance on a governance framework for access and sharing of data generated by connected vehicles
  - clarify cybersecurity requirements for the connected car environment
  - provide guidance on the use of pioneer spectrum for 5G connectivity for large scale testing and experimentation for connected vehicles
- In 2019, the European Commission has set up an informal group of a hundred experts named "the Single Platform for open road testing and pre-deployment of cooperative, connected, automated and autonomous mobility" in order to provide advice and support regarding testing and pre-deployment activities for CCAM[25].
- The protection of road users' privacy and personal information is also addressed by the recent EU General Data Protection Regulation (GDPR)[26] which officially went into effect in May 2018.
- The Network and Information Security directive (NIS)[27] also addresses autonomous vehicles' cybersecurity issues as it intends to provide generic security measures in order to enhance cybersecurity across EU.

- **International Context**:
  - The European OEMs published a set of cybersecurity principles, through the ACEA Principles of Automobile Cybersecurity[28], which are already implemented by OEM companies.
  - The National Highway Traffic Safety Administration (NHTSA) from the U.S. government issued in late 2016 a document introducing several cybersecurity best practices for smart cars[29].
  - The US Automotive Information Sharing and Analysis Center (Auto-ISAC) has been maintaining since 2016 a series of Automotive Cybersecurity Best Practices[30] which provide guidance on the implementation of automotive cybersecurity principles.
  - Several cybersecurity standards and recommendation documents are also under development. In particular, the United Nations Economic Commission for Europe (UNECE) is currently drafting a proposal for a recommendation on Cyber Security[31] with a focus on key cyber threats and vulnerabilities against vehicles as well as measures to be considered in order to mitigate the identified threats. UNECE is also introducing a United Nations regulation on cybersecurity which defines a set of requirements that shall be fulfilled by vehicle manufacturers, suppliers and service providers, covering the entire vehicle lifecycle (i.e. from the vehicle development to its decommissioning).

[25] See "European Commission Launches CCAM Single Platform": https://connectedautomateddriving.eu/mediaroom/european-commission-launches-ccam-single-platform/
[26] See EU "General Data Protection Regulation": https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[27] See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union": https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN
[28] See ACEA "https://www.acea.be/publications/article/acea-principles-of-automobile-cybersecurity"
[29] See NHTSA "Cybesecurity best practices for modern vehicles": https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwji2PqR0cDjAhXq2eAKHcnrAnUQFjAAegQIAxAC&url=https%3A%2F%2Fwww.nhtsa.gov%2Fstaticfiles%2Fnvs%2Fpdf%2F812333_CybersecurityForModernVehicles.pdf&usg=AOvVaw33nVAk2UWXpL3tzDmpRBjl
[30] See Auto-ISAC "Automotive Cybersecurity Best Practices – Executive summary": https://www.automotiveisac.com/best-practices/
[31] See current draft of the UNECE "Proposal for Recommendation on Cyber Security": https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

- **Standards**:
  - The British Standards Institution (BSI) Group published in December 2018 two Publicly Available Specifications (PAS), namely PAS 1885[32] and PAS 11281[33]. The former, which is entitled "The fundamental principles of automotive cyber security", provides high-level guidance to provide and maintain cybersecurity. As regards to PAS 11281, entitled "Connected automotive ecosystems – Impact of security on safety – Code of practice", it provides recommendations for managing security risks in a connected automotive ecosystem.
  - The European Telecommunications Standards Institute (ETSI) has been developing a set of technical specifications, ETSI TS 102 940 to 102 943[34], which define an Intelligent Transport System (ITS) security architecture along with services specification to ensure information confidentiality and prevent unauthorized access to ITS services. They also address the trust and privacy management for ITS communications.
  - The standard of Society of Automotive Engineers SAE J3061[35], officially published in January 2016, is considered as the first standard addressing automotive cybersecurity. It provides a set of high-level cybersecurity principles and guidance for cyber-physical vehicle systems.
  - The International Organization for Standardization (ISO) and SAE collaborated to supersede the SAE J3061 recommended practice and propose the ISO/SAE 21434[36]. This standard is also under development and focuses on automotive cybersecurity engineering by specifying requirements and providing recommendations for cybersecurity risk management for cars (including their components, software and interfaces) all along their entire lifecycle. Concurrently, the SAE is working on another document, SAE J3101, which aims to define common requirements for security to be implemented in hardware for ground vehicles.

In 2016, ENISA performed a study on smart cars security issues which resulted in a document entitled "Cyber Security and Resilience of smart cars"[37]. It has also established the Cars and Roads SECurity (CaRSEC) working group which addresses smart cars cybersecurity threats, challenges and solutions so as to protect road users' safety. CaRSEC group members are car manufacturers with focus on cybersecurity, suppliers and developers of embedded hardware/software for smart cars, road authorities and academia, as well as standardisation bodies and policy makers.

1.4 TARGET AUDIENCE

This study provides a set of good practices and security measures to improve smart cars security and mitigate the potential threats and risks. Therefore, similarly to the previous ENISA smart cars study, the target audience of this study is mainly:

- **Car manufacturers**: also referred to as OEMs, they design new cars and handle the assembly of the various car components. In particular, most of the various car components are not produced by the car manufacturer itself, but rather by their suppliers according to a set of functional, safety and security requirements defined by the car manufacturers.

[32] See "PAS 1885:2018 - The fundamental principles of automotive cyber security. Specification": https://shop.bsigroup.com/ProductDetail?pid=000000000030365446
[33] See "PAS 11281:2018 - Connected automotive ecosystems. Impact of security on safety. Code of practice": https://shop.bsigroup.com/ProductDetail?pid=000000000030365540
[34] See ETSI TS 102 940 v1.3.1, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management"
ETSI TS 102 941 V1.2.1 "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
ETSI TS 102 942 V1.1.1 "Intelligent Transport Systems (ITS); Security; Access Control"
ETSI TS 102 943 V1.1.1 "Intelligent Transport Systems (ITS); Security; Confidentiality services"

[35] See SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems": https://www.sae.org/standards/content/j3061_201601/
[36] See ISO/SAE CD 21434 "Road Vehicles – Cybersecurity engineering": https://www.iso.org/standard/70918.html
[37] Relation between this study and "Cyber Security and Resilience of Smart Cars" is described in Annex A.

- **Tier 1 and Tier 2 car components suppliers**: provide the different car components required to produce the car. Tier 1 refers to the entities having direct contractual relationships with the car manufacturers, whereas Tier 2 refers to the entities having contractual relationships with Tier 1 suppliers. For instance, car seats are manufactured by Tier 1 suppliers whilst electronic components or software are usually provided by Tier 2 suppliers.
- **Aftermarket suppliers**: provide added-value aftermarket products, such as smart dongles or third-party GNSS systems, which can be bought by customers and connected to the car to provide additional features.

1.5 METHODOLOGY

ENISA has developed this study following a five-step methodological approach as depicted in **Figure 1**.

Figure 1: Methodology

1. **Project scope definition:** the first step consisted in establishing the scope of the project and identifying the main topics to be considered during the study.
2. **Desktop research and experts' identification:** extensive research of relevant documents to gather as much information as possible about (semi-)autonomous cars and V2X communication technologies. The identified documents and standards were used as references for the development of this report. During this step, subject matter experts were also invited to validate scope and provide feedback. Experts from car manufacturers, tier-1 and tier-2 suppliers as well as other organisations, such as Government Authorities and ITS system suppliers were invited. Additionally, experts from ENISA's CaRSEC[38] informal expert group were also invited to contribute.
3. **Questionnaire and interviews with identified experts:** ENISA got in touch with the identified experts in order to get their point of view. To this end, a structured

[38] See https://resilience.enisa.europa.eu/carsec-expert-group for more information on the terms of reference and scope of the ENISA CarSEC Informal Expert Group.

questionnaire covering various security aspects, such as critical assets, key threats targeting smart cars and awareness with respect to smart cars standards and guidelines, was developed. The questionnaire was completed by some of the identified experts, and interviews were conducted to collect additional valuable inputs to prepare the report.

4. **Analysis of collected material and report development:** all the collected information, either through desktop research or directly from the identified experts, was thoroughly analysed. This led to the development of the first draft of this report.
5. **Review and report validation:** ENISA shared the draft of the report with its relevant stakeholder communities and reference groups for review. Taking into account the stakeholders feedbacks, the proposed final version of the report was issued and a validation face-to-face workshop was organized to present the results of the study.

1.6 STRUCTURE OF THE DOCUMENT

The study is structured as follows:

- **Chapter 1 – Introduction:** provides introductory information on the objectives, scope, relevant EU and international policies, target audience, followed methodology and the structure of this study.
- **Chapter 2 – Smart cars: Connected and (semi-)autonomous cars:** first defines V2X communications, semi-autonomous and autonomous cars. Then, it provides a high-level reference architecture of smart cars and lists the sensitive assets to be protected.
- **Chapter 3 – Threats and risk analysis:** identifies the main threats against smart cars and indicates the affected assets. Some examples of significant smart cars attack scenarios are also detailed.
- **Chapter 4 – Security measures and good practices:** describes the security measures and good practices to mitigate the aforementioned attacks.

Further details are provided in the appendix:

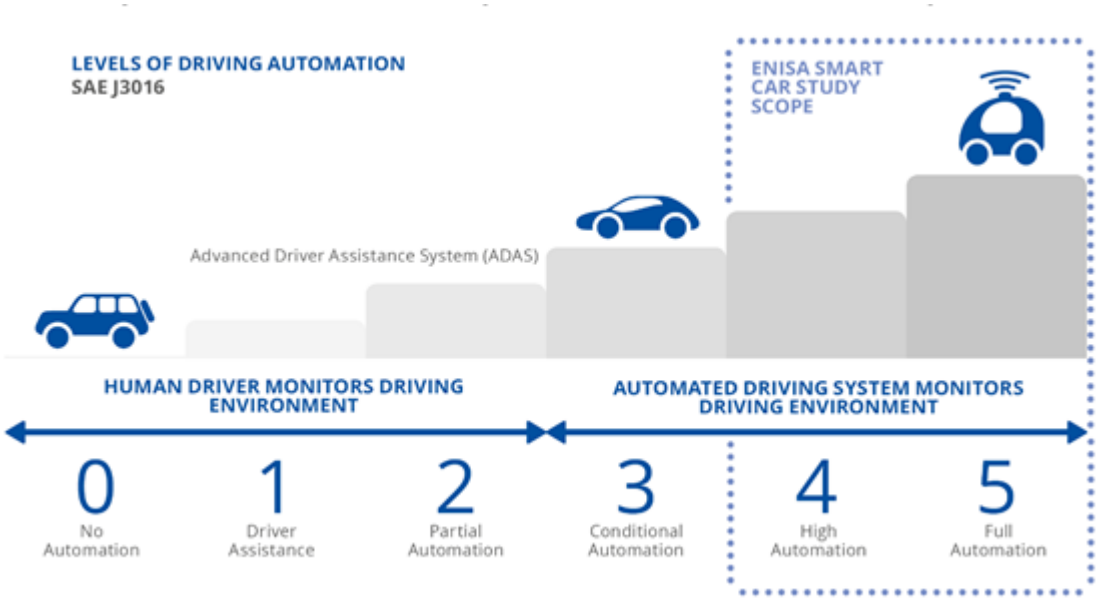
- **Annex A – Asset Taxonomy:** presents the different assets and provides a brief description of them
- **Annex B – Threat Taxonomy:** provides a brief description of the different threats and maps each threat to the asset(s) that may potentially be affected
- **Annex C – Mapping of security measures to threats, standard and good practices:** details the security measures mentioned in chapter 4 and maps them to the corresponding threats.

2. SMART CARS: CONNECTED AND (SEMI-) AUTONOMOUS CARS

2.1 DEFINITIONS

The SAE J3016[39] standard defines six levels of driving automation for on-road vehicles, ranging from level 0 with no driving automation at all to level 5 with full driving automation and no need for a driver, as shown in Figure 2.

Figure 2: SAE vehicles automation levels as defined in SAE J3016



Even though the provided recommendations and good practices can apply to all vehicles (i.e. no matter their automation level), this study focuses on **semi-autonomous** and **autonomous cars**, which are also referred to as Automated Driving System-Dedicated Vehicle (ADS-DS) in SAE J3016 standard, as well as on **V2X communications**, defined as follows:

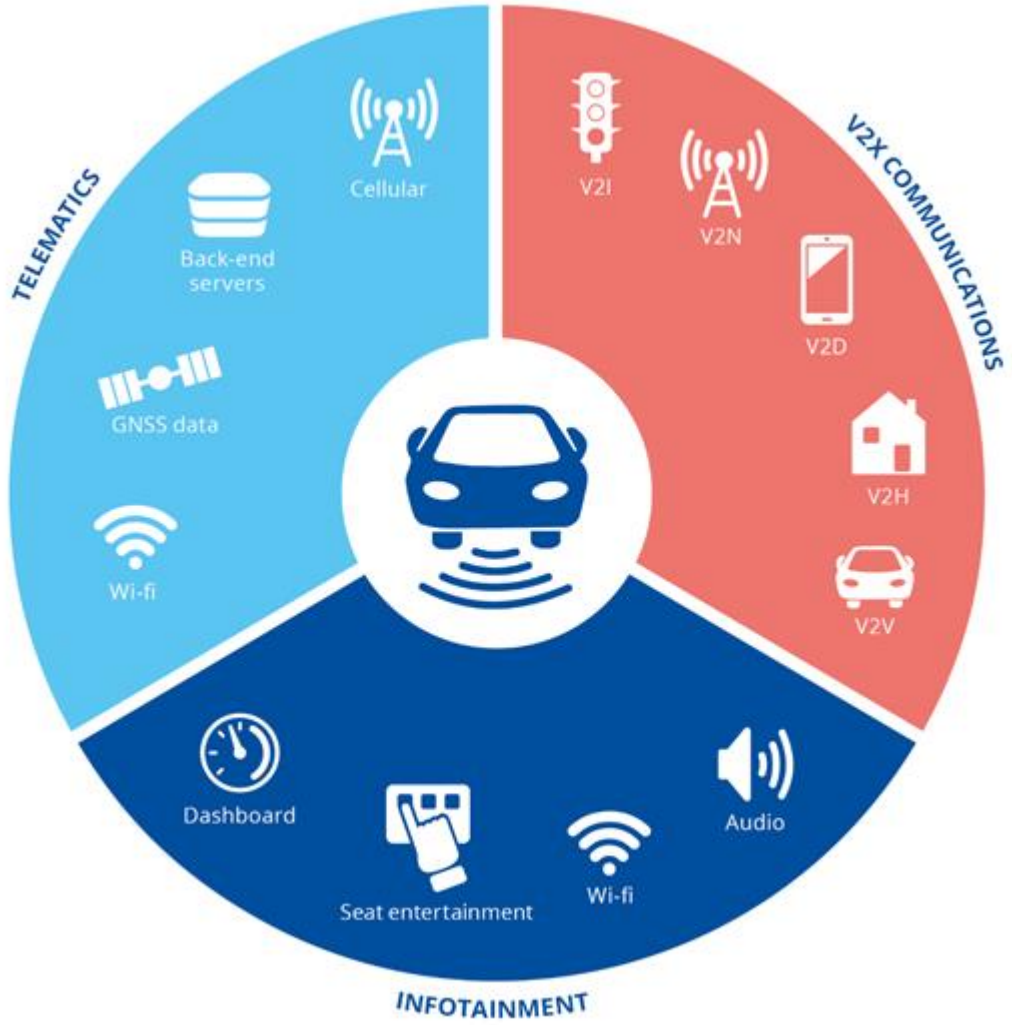
- **Semi-autonomous cars (level 4 of automation):** refers to highly automated cars that are equipped with a multitude of sensors in order to be able to autonomously (i.e. without any human driver intervention) perform **all** driving functions **under certain conditions** (e.g. on a given type of roads).
- **Autonomous cars (level 5 of automation):** refers to fully automated cars that are equipped with a multitude of sensors in order to be able to autonomously perform **all** driving functions **under all conditions** (i.e. at any time and on any road). Those cars may not even include a steering wheel or accelerator/brake pedals.
- **V2X communications:** refers to data exchanges between a vehicle and any other entity (e.g. a road infrastructure, another vehicle, a pedestrian, etc.). It covers the notions of V2V (Vehicle-to-Vehicle) communications and V2I (Vehicle-to-Infrastructure) communications. In this study, the term V2I refers to all communications between the vehicle and its

[39] See SAE J3016 "Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles": http://sae.org/standards/content/J3016_201806/

surrounding, aside from V2V communications. Thus, V2I includes V2P (Vehicle-to-Pedestrian) and V2N (Vehicle-to-Network) communications. To enable V2X communications, vehicles are equipped with different wireless communication systems such as Dedicated Short Range Communications (DSRC[40]), Visible Light Communication (VLC), Image Sensor Communication (ISC), Wi-Fi or mobile communication technologies, such as 3G, 4G and 5G. This study is meant to be agnostic about the communication technologies actually used.

Figure 3 gives an overview of the smart car ecosystem depicting systems and application both *in-vehicle [41] and outside the car.*

Figure 3: Smart cars ecosystem



In this study, we focus on smart cars that, as connected systems, have the necessary capabilities to autonomously perform all driving functions under certain (or all) conditions, and are able to communicate with their surroundings including other vehicles, pedestrians and Road-Side Units (RSU).

Good practices discussed in this report do not only concern passenger cars but also commercial vehicles (e.g. buses, coaches, etc.), including self-driving ride-sharing vehicles which can be

[40] In this document, DSRC refers to the standards from the European Committee for Standardization EN 12253:2004 and EN 12795:2002
[41] In-vehicle refers to assets inside the vehicle

shared with other users. This study does not focus on specific use cases such as connected infotainment and specific intra-vehicular communications.

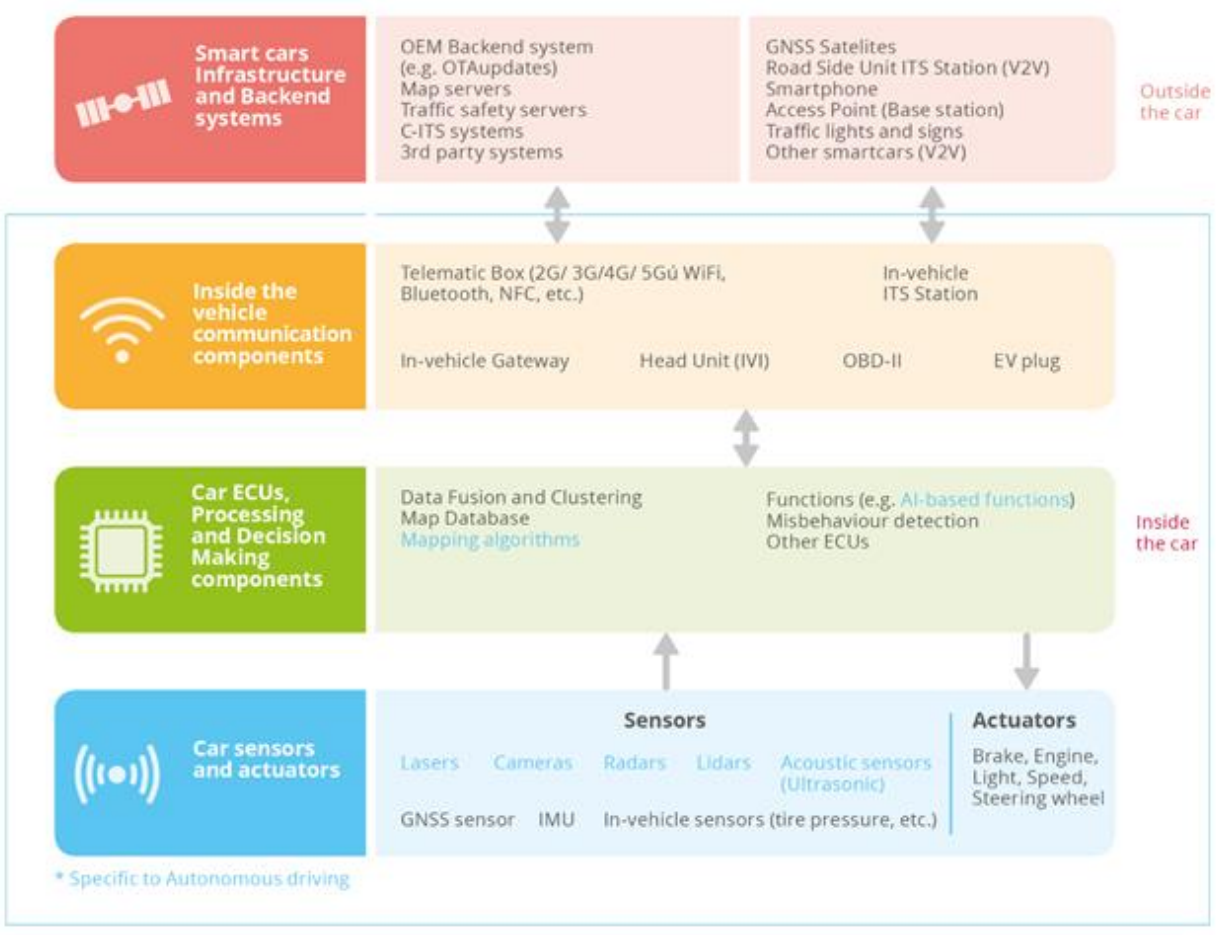
To achieve enhanced autonomous driving capabilities, smart cars rely on various technologies including:

- **Sensors and Actuators:** devices that have various capabilities, such as sensing and detecting objects, actuating, etc.
- **Artificial Intelligence:** algorithms that enable ECUs and computers to perform tasks typically associated with intelligent human beings.
- **Machine Learning:** algorithms that enable computers to act and enhance their ability to predict events or situations.
- **Cloud Computing:** solutions enabling access to shared sets of resources such as servers and applications with minimal requirements concerning managerial effort and service provider interaction.
- **Communications and/or Networks:** radio technologies and communication protocols that allow data exchange between different entities.

2.2 HIGH-LEVEL REFERENCE MODEL

Smart cars and especially (semi-)autonomous cars, which include several ECUs and components, may seem unduly complicated at first glance. Although smart cars functions (e.g. braking, steering, door locking, etc.) are the same throughout vehicles, nevertheless each OEM has its own in-vehicle architecture and there is no common and unique architecture that can be used as a reference model. **Figure 4** presents the high-level functional model that ENISA

Figure 4: High-Level Smart Cars Reference Model



defined for the study based on an extensive review of relevant efforts and having validated it with the experts. The model's aim is to provide a generic overview of the smart cars technologies and their interplay. It needs to be noted that the model is only indicative and does not reflect the complexity of the various automotive architectures; it aims at encapsulating the main elements of the latter in a high-level view. This model provides a general overview of the different functionalities, used technologies and most important components providing smart cars major features.

The high-level reference model consists of four layers arranged in order, with the three lowest layers being part of the smart car, whereas the upper layer represents components that are outside the actual containment of the car, but which are part of its environment such as RSUs and map servers for instance. In addition to the components and technologies depicted in **Figure 4**, smart cars also include critical functions (e.g. acceleration, braking, object detection, navigation, etc.) that ought to be protected against cyberattacks. Indeed, altering the operations of those functions may lead to unexpected situations (e.g. vehicle collision or crash) that could endanger road users' safety.

Hereinafter, we provide a brief description of the different layers:

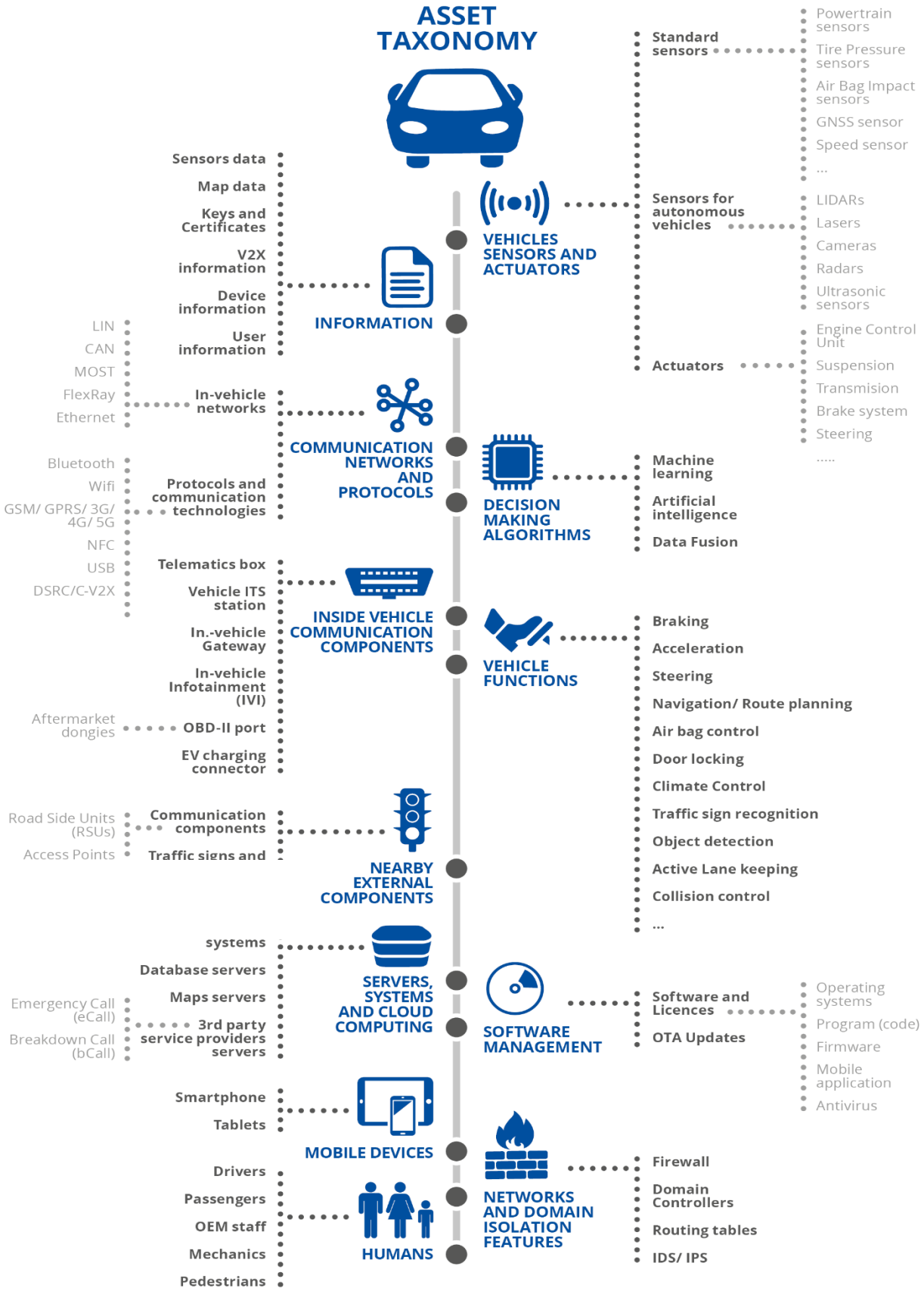
- **Car sensors and actuators:** the lowest layer of the architecture comprises the various smart cars sensors used to monitor the driving environment by collecting data on the vehicle surroundings, such as road conditions, distance to other objects and vehicles, Global Navigation Satellite Systems (GNSS) positions, as well as the different actuators that execute the necessary actions.
- **Car ECUs, processing and decision making components:** this layer comprises all the hardware and software components, including AI, that are used for the processing of the data received from layer Car sensors and actuators (i.e. data collected by the smart cars sensors) and In-vehicle communication components (e.g. data received from other C-ITS stations), as well taking the appropriate decision and transmitting it to the relevant actuator.
- **In-vehicle communication components:** this layer includes the different in-vehicle communication components used for both in-vehicle communications (e.g. Head-Unit which is also referred to as In-Vehicle Infotainment (IVI), or in-vehicle gateway) as well as communications with external components such as other vehicles or RSUs.

2.3 SMART CARS INFRASTRUCTURE AND BACKEND SYSTEMS:

This layer comprises the different external communication components (e.g. RSU, traffic signs) or systems (e.g. other vehicles, access points, pedestrian smartphone) that communicate directly with the smart cars, as well as servers and systems that remotely provide services to smart cars. It includes, amongst others, OEM back-end systems used for over-the-air (OTA) updates, map data servers and third party service provider's systems.assets taxonomy.

To address smart cars cybersecurity issues, it is essential to identify assets of such a complex ecosystem. A taxonomy of the key assets that should be protected in order to ensure highly secure vehicles is depicted in **Figure 5**, and a brief description of the different assets is provided in Annex A. Especially, smart cars functions (e.g. obstacle detection) are of utmost importance as they directly influence smart cars behaviours and may endanger passengers' safety. These functions are at the crossroads between different technologies from sensors to AI-based algorithms by way of infrastructure components, listed in the asset taxonomy. This highlights that securing smart cars requires a multidisciplinary approach, as assets domains are quite diversified.

Figure 5: Asset taxonomy



3. THREATS AND ATTACK SCENARIOS

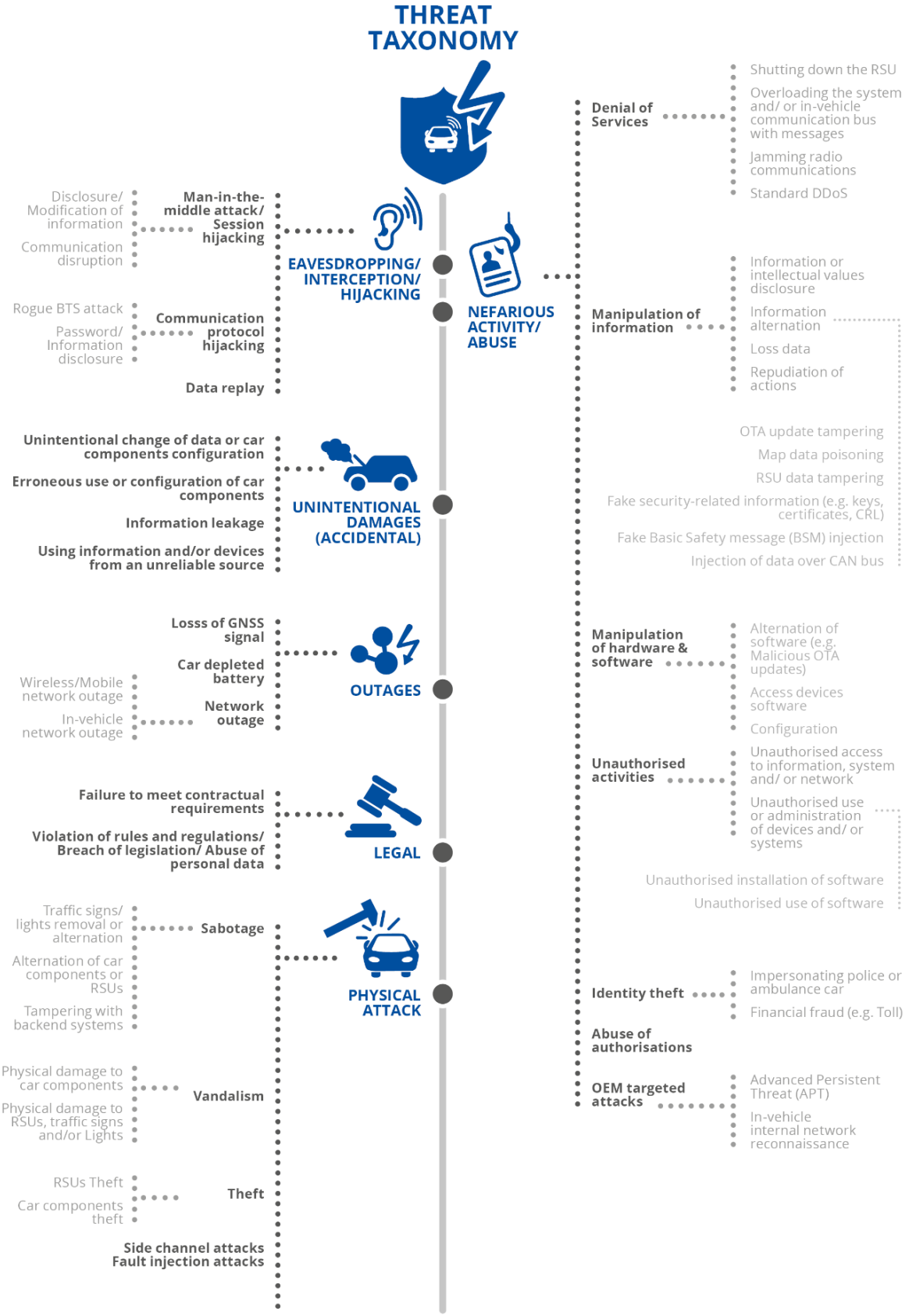
3.1 THREATS TAXONOMY

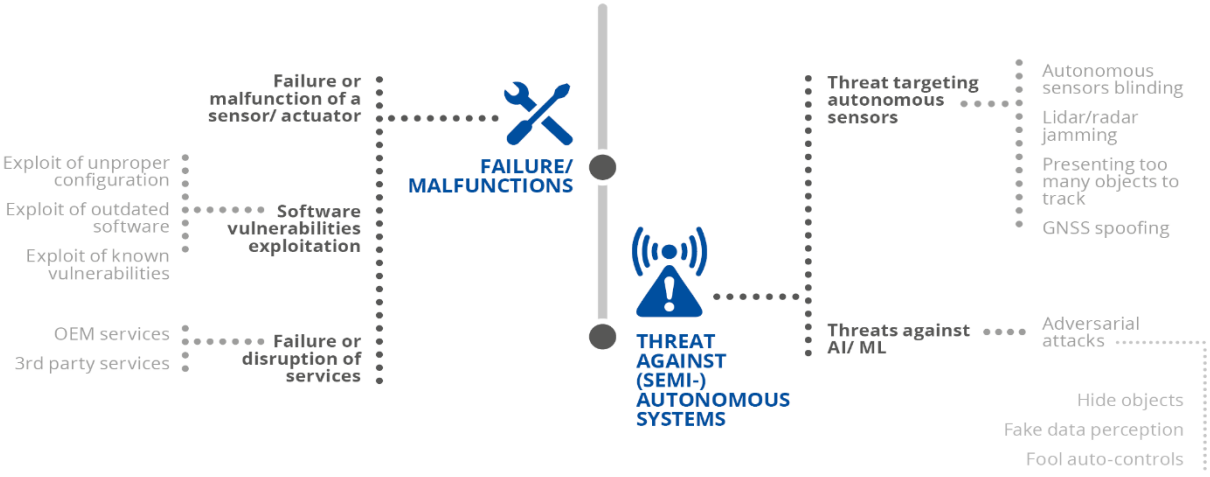
Smart cars increased connectivity and automation expose them to several crucial cyber threats. Those threats may directly target smart cars or their surroundings such as RSUs, traffic signs/lights or even remote servers of the OEM or third-party service providers.

In accordance with the ENISA Threat Taxonomy[42], we have developed a threat taxonomy[43] focused on smart cars as depicted in **Figure 6**. Annex C provides a description of the different threats and identifies the assets that may be affected by each threat.

[42] See "ENISA Threat Taxonomy" (2016): https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
[43] It is a snapshot of today's threats and may not be up-to-date in the future.

Figure 6: Threat taxonomy




Failure or malfunction of a sensor/ actuator
Exploit of unproper configuration
Exploit of outdated software
Exploit of known vulnerabilities
Software vulnerabilities exploitation
OEM services
3rd party services
Failure or disruption of services
FAILURE/ MALFUNCTIONS
THREAT AGAINST (SEMI-) AUTONOMOUS SYSTEMS
Threat targeting autonomous sensors
Autonomous sensors blinding
Lidar/radar jamming
Presenting too many objects to track
GNSS spoofing
Threats against AI/ ML
Adversarial attacks
Hide objects
Fake data perception
Fool auto-controls

3.2 EXAMPLES OF SMART CARS CYBER SECURITY ATTACK SCENARIOS

During the interviews, automotive experts assessed the criticality of several attack scenarios based on their potential impacts and the aforementioned threats, so as to enable the identification of critical attack scenarios. For each attack scenario, experts were asked to indicate whether they consider its potential impact (i.e. severity level) as high, medium or low. Table 1 depicts the different attack scenarios along with the interviewees' perceived severity level.

Table 1: Smart cars attack scenarios

ATTACK SCENARIOS	SEVERITY[44]
1. **Vulnerability exploit in a communication stack**: exploitation of a vulnerability in a communication stack of an in-vehicle network (e.g. no protection mechanism against replay attacks, lack of authentication, etc.) can lead to severe issues such as critical ECU reprogramming and taking control the vehicle over the Controller Area Network (CAN bus).	**High**
2. **Mobile car application[45] being hacked/attacked allowing access to the car**: by hacking the mobile application, an attacker could order a car to drive him somewhere although he is not allowed to do so.	**High**
3. **Attack on remote servers to influence car behaviours**: several attack scenarios exist regarding remote servers. For instance, an attacker could compromise map data with the aim to affect plausibility checks, or even alter data on traffic conditions to change the current car itinerary resulting in an inefficient service.	**High**
4. **Fake communication unit to compromise telematics unit and deploy rogue firmware:** use of malicious communication unit, such as Base Transceiver Station (BTS), Wi-Fi router, RSU, with the objective to spread a malware or just disrupting the infrastructure communications.	**High**
5. **Large scale deployment of rogue firmware after hacking OEM back-end servers:** penetration of OEM back-end servers with the aim to initiate malicious firmware updates could lead to devastating results as this kind of attacks is highly-scalable.	**High**
6. **Hacking an RSU with the aim to spread wrong traffic and safety messages:** as RSUs constitute an important part of the autonomous vehicles' ecosystem, they could be the target of hackers in order to create traffic jams or other kind of disruptions.	**High** – **Medium**
7. **Rogue vehicle sending wrong information through V2V interfaces:** vehicles unknown from the infrastructure (e.g. counterfeit cars) that are deployed to decrease the safety level by sending wrong information about traffic conditions and other functionalities (i.e. fake information with the aim to update map data).	**Medium**

[44] This severity is a global perception of the risk based on interviews. In practice, it varies strongly depending on the actual architecture of each smart car.
[45] Mobile application that provides value added services with respect to the car (e.g. mobile application that enables to unlock the car, start the engine, etc.)

8. Sensor fooling by adversarial perturbation: attack scenarios to disrupt the sensors' proper functioning by different means depending on the targeted sensor (e.g. flash the camera, relay the light waves from the LiDAR).	Medium – Low
9. Communication jamming: producing radio interferences to disrupt wireless networks so the vehicles cannot emit or receive V2X messages.	Low
10. GNSS spoofing: by replacing GNSS signals, an attacker can fool a third-party service into thinking that the vehicle is elsewhere in either time or location. This can lead to accident or vehicle theft.	Medium
11. Blocking critical messages at automation level 4: an attacker can block critical messages, such as Denial of a Service (DoS) attack, and prevent the semi-autonomous vehicle (or driver) from reacting appropriately to the situation (e.g. apply the brakes, warn the driver that he needs to take control of the vehicle, etc.).	High

Hereinafter, we detail three types of attack scenarios encompassing various use-cases. The first attack scenario (**Large scale deployment of a rogue firmware after hacking OEM back-end servers***)* is typical of the threats lying over connected cars. The second one (**Hacking/altering a V2X mobile application that allows access to the car**) is extracted from V2X use-cases. The third one (**Sensor fooling by adversarial perturbation**) is more related to (semi-)autonomous features. These three attack scenarios were selected so as to represent different families of attacks linked with connected cars and automation levels 4 & 5, which are the focus of this study. The impact is an overall estimation based on the outcome of the interviews.

Attack scenario 1: Large scale deployment of a rogue firmware after hacking OEM back-end servers

DESCRIPTION	
This attack scenario refers to deployment of malicious firmware from back-end servers. This could be initiated by OEMs employees (e.g. developers) or by external attackers capable of penetrating back-end servers. Malicious OTA updates could then be executed so that autonomous vehicles think it is a legitimate one, as it is initiated from a trusted server.	
IMPACT	
High – **Crucial**: Remote servers might communicate with numerous vehicles at the same time. Thus, compromising such a centralised server could affect the entire ecosystem, including passengers' safety.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium: Remote servers should have enough resources to implement advanced monitoring techniques. However, the deployment of many remote servers increases the attack surface to be protected.	**High**: Such attacks are highly-scalable as they can be executed remotely and affect a fleet of vehicles instantly.

ASSETS AFFECTED	STAKEHOLDERS INVOLVED
Back-end system Software and Licenses OTA Updates Vehicle functions Information (User, Device, Keys and Certificates)	OEMs

ATTACK STEPS

1. To perform this attack scenario, the attacker needs first to penetrate the targeted OEM back-end server. This may be carried out by leveraging a known vulnerability of used software, a misconfiguration on the server side or by spoofing the administrator account for instance.
2. Once the attacker gets access to the OEM back-end server, the attacker can request the execution of an OTA firmware update for a given fleet of vehicles. To this end, he follows the same steps required to perform a legitimate OTA firmware update.
3. Upon receiving the OTA update request, vehicles acknowledge and accept the request as it is initiated by a legitimate OEM server.
4. Next, the attacker uploads a rogue firmware on the OEM back-end server and launches the OTA update process to deploy this firmware.
5. Once the rogue firmware is installed on smart cars, the attacker can take remote control of a fleet of vehicles by exploiting a backdoor introduced in the rogue firmware.

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium – **High**: Depending on the nature of the deployed firmware, cancelling the update by returning back to the retro version can be challenging if the attacker was able to change update related information (e.g. certificates, policies). Use of logging can help to identify the attack origin.	Lack of awareness and knowledge Lack of a secure boot process Lack of proper product lifecycle management

COUNTERMEASURES

1. Regularly assess the security controls and patch vulnerabilities.
2. Deploy Intrusion Detection Systems (IDS) at vehicle and back-end levels.
3. Introduce a new device or software change into the vehicle only according to an established, accepted and communicated change management process.
4. Consider establishing a CSIRT.
5. Apply security controls at back-end servers.
6. Establish an incident handling process.
7. Incident report to back-end servers.
8. Conduct periodic reviews, of authorization and access control privileges for instance.
9. Software authenticity and integrity checked before installation.
10. Use of secure OTA firmware updates.

11. Protect OTA update process.
12. Use of secure boot mechanisms.
13. Application of security controls to back-end servers.
14. Apply least privileges principle and use individual accounts to access devices and systems.
15. Maintain properly protected audit logs.
16. Allow and encourage the use of strong authentication mechanisms.

Attack scenario 2: Hacking/altering a V2X mobile application that allows access to the car

DESCRIPTION	
IMPACT	
High: Such attacks can result in illegitimate access to the smart car or even its theft through the compromise or hacking of a V2X mobile application.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium: Individual should pay attention to the different applications installed on their smartphone (e.g. avoid installing suspicious applications).	**Medium**: This attack scenario target individuals and allows compromising many vehicles at once using V2X application
ASSETS AFFECTED	**STAKEHOLDERS INVOLVED**
Mobile application User information Keys and certificates Mobile devices (smartphones and Tablets)	OEMs Third-party service providers
ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)	
1. The attacker manages to retrieve user's credentials associated to a V2X application (e.g. car, traffic or platooning application) by one of the following means: by making the honest user install a fake application instead of the real one, via a phishing attack, or by leveraging an existing or a new discovered vulnerability in the V2X application. 2. Once the attacker has retrieved the user's credentials, he installs the legitimate V2X application and uses stolen credentials to login successfully; thus impersonating the honest user. 3. Finally, the attacker can use the V2X application to get access to the smart car, and potentially steal the smart car if keyless driving is allowed and the hacked application enables to start the engine.	
RECOVERY TIME / EFFORT	**GAPS AND CHALLENGES**

Medium: As soon as the flaw in the application that allow such attacks is discovered, a security patch should be applied. Depending on the vulnerability, it might take days or weeks. If V2X application user has informed OEM about credential compromise, they should revoke the disclosed credentials for that particular user.	Response to zero-day vulnerabilities Lack of awareness and knowledge Insecure design or development

COUNTERMEASURES

1. Perform vulnerability surveys.
2. Third party testing of V2X applications.
3. Regularly assess the security controls and patch vulnerabilities.
4. Information sharing between different actors.
5. Adopt a holistic approach to security training and awareness among the employees.
6. Raise users' awareness.
7. Allow and encourage the use of strong authentication (e.g. multi-factor authentication).
8. Consider establishing a Computer Security Incident Response Teams (CSIRT).
9. Mitigate vulnerabilities or limitations of software libraries.
10. Protect mobile applications against reverse engineering and tampering of their binary code.
11. Securely store sensitive data on mobile devices.

Attack scenario 3: Sensor fooling by adversarial perturbation

DESCRIPTION

IMPACT

High: The impact depends on the introduced perturbation. However, abusive detection, or lack of detection of stop signs could entail major accidents endangering road users' safety and leading to driver, passenger, or pedestrian deaths.

EASE OF DETECTION	CASCADE EFFECT RISK
Medium: Without appropriate countermeasure, the modifications brought to the signs could be undetected by human eyes before an accident occurs.	**Low**: The perturbation is local, and may affect only the cars passing by the modified or spoofed sign.
ASSETS AFFECTED	**STAKEHOLDERS INVOLVED**
Decision Making algorithms Sensors for autonomous vehicles Vehicle functions	OEMs Road infrastructure

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)	
1. The attacker first analyses the capabilities of the targeted versions of cameras and AI-based image classifier to ensure detection and classification as desired of the modified sign. This setup phase can require trying multiple perturbation patterns or display parameters. The attacker needs to perform some experimentation as well, to test the adversarial perturbation and ensure that his attack will succeed. 2. At a next step, the attacker attaches a set of black and white stickers[46] to a physical road sign to cause misclassification of the traffic sign. 3. Due to the added stickers, the cars passing by the altered traffic sign will erroneously classify it into the attacker's targeted class (e.g. interpret a stop sign as a speed limit sign) and react accordingly (e.g. reduce speed instead of stopping the vehicle).	
RECOVERY TIME / EFFORT	**GAPS AND CHALLENGES**
Medium: Sensor fooling attacks can go unnoticed. Once detected, modified traffic signs can be repaired in hours.	Traffic sign authentication would be an appropriate countermeasure but is complicated to deploy Collaboration of vehicles
COUNTERMEASURES	
1. Protect critical sensors in order to prevent attacks that may alter their perception of the environment. 2. Hardening against Adversarial Machine Learning. 3. Use of hardware redundancy mechanisms. 4. Use of data redundancy mechanisms, such as sensors information fusion. 5. Perform data validation, for instance by comparing sign information collected by sensor with information from digital maps stored in the vehicle.	

[46] "Robust Physical-World Attacks on Deep Learning Models": https://arxiv.org/pdf/1707.08945.pdf

4. SECURITY MEASURES AND GOOD PRACTICES

4.1 SECURITY MEASURES CATEGORISATION

Security measures and good practices development is one of the major objectives of this study. Indeed, a considerable effort was expended to identify all relevant security measures in order to help mitigate the potential threats and risks, thus improving smart cars security.

The list of security measures has been established by analysing relevant documents and standards identified during desktop research[47]. This analysis allowed the identification of frequently mentioned topics regarding smart cars security and their classifications into different security domains. The resulting list consists of seventeen security domains grouped into three main categories, namely Policies, Organisational practices and Technical practices as shown in **Figure 7**. The latter provides a comprehensive view of smart cars security landscape, and points out the areas to be protected.

Figure 7: Cybersecurity Good Practices Overview

[47] The data collection was performed between March and July 2019. Updates may have impacted the reference documents since the publication of this report. See Bibliography in chapter 6.

4.2 POLICIES

This first category of security measures encompasses the different policies and procedures to be established within organizations to ensure an appropriate cybersecurity level.

Policies-related security measures cover both security and privacy aspects, and have been classified into four main security domains, namely **Security by design**, **Privacy by design**, **Asset management** and **Risk and threat management**.

The security measures in this section are addressed at both OEMs and suppliers, due to the tight links between them.

4.2.1 Security by design

These security measures emphasize the need to consider security aspects from the very beginning of product development, throughout the supply chain and all over smart cars lifecycle.

- **PS-01**: Adopt a security by design approach where smart cars cybersecurity is considered from both the vehicles as well as the infrastructure perspective.
- **PS-02**: Address security in each relevant specification document to ensure that security aspects are considered from the very beginning of the concept phase, and not as an afterthought.
- **PS-03**: Promote the use of methodologies that consider security in every stage of the development phase and operations phases (e.g. DevSecOps[48], Secure Development Lifecycle (SDL)[49], etc.).
- **PS-04**: Consider including a security role within the product engineering team to lead security related tasks.

4.2.2 Privacy by design

This security domain includes a set of security measures related to the protection of private data that are collected, processed and/or stored by smart cars stakeholders.

- **PS-05**: Consider applying local and international privacy related regulations, such as the GDPR, to prevent privacy issues.
- **PS-06**: Conduct Privacy Impact Assessments (PIA), taken into account the context of use, in order to identify any privacy related risk, and define appropriate countermeasures to mitigate it.
- **PS-07**: Perform Privacy Audits during smart cars development and over back-end systems on a regular basis, e.g. at least once year, in order to ensure compliance with privacy related policies.

4.2.3 Asset Management

Hereinafter, security measures pertaining to assets discovery, monitoring, administration and maintenance are outlined.

- **PS-08**: Use tools supporting asset management that can automatically discover, identify and enumerate assets specific to the organization and smart cars ecosystem.
- **PS-09**: Ensure that the organization maintains a consistent and up-to-date asset inventory.

[48] DevSecOps is short for Development, Security and Operations. It aims to implement security decisions and actions at the same scale and speed as development and operations decisions and actions. See https://www.forcepoint.com/cyber-edu/devsecops
[49] See SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems": https://www.sae.org/standards/content/j3061_201601/

- **PS-10**: Introduce a new device or software change into the vehicle only according to an established, accepted and communicated change management process.

4.2.4 Risk and Threat Management

This security domain gathers the security measures related to the process of risk and threat management.

- **PS-11**: Adopt an approach to risk management dedicated and suitable for automotive sector, considering emerging threats and attack scenarios targeting smart cars.
- **PS-12**: Perform a cybersecurity risk analysis from the very early stages of the design process, and which should be revised at least annually and upon any major change or in case of critical security vulnerability detection or critical security incident.
- **PS-13**: Monitor security vulnerabilities with a focus on vehicles that are on the market on a regular basis, e.g. every 6 months or more frequently based on risk assessment.
- **PS-14**: Conduct security evaluations, such as penetration testing, during the development phase and then, on a regular basis following an event driven approach, e.g. in the case of new threats or vulnerabilities and after major updates.
- **PS-15**: Consider establishing a threat intelligence process in order to be informed on emerging attack types and sources as well as new relevant vulnerabilities.
- **PS-16**: Regularly assess the security controls at least once a year overall smart cars lifecycle, and deploy patches (after testing them) to mitigate vulnerabilities.
- **PS-17**: Regularly check, at least every six months over smart cars lifecycle, that the security assumptions (e.g. operational environment assumptions) are still valid. In particular, consider defining procedure for communication and handling of end-of-life/out-of-warranty status for cybersecurity.

4.3 ORGANISATIONAL PRACTICES

Organisational and governance processes are of utmost importance to ensure smart cars security. In what follows, a set of organisational rules and best practices are detailed. They cover several aspects such as relationships with suppliers, employees training, incident management, etc.

4.3.1 Relationships with Suppliers

- **OP-01**: Foster security-related information sharing between the different stakeholders while protecting intellectual property.
- **OP-02**: Define cybersecurity relevant aspects of the partnerships along the supply chain, and develop security requirements and procurement guidelines for suppliers[50].

4.3.2 Training and Awareness

- **OP-03**: Share relevant information between all organisations, including subcontractors, suppliers and third parties to enhance smart cars security, by following the examples of existing Information Sharing and Analysis Centers (ISACs) for instance.
- **OP-04**: Adopt a holistic approach to security training and awareness among the employees, including employees on all levels of the organization, as well as consider expanding it to suppliers.
- **OP-05**: Ensure that security trainings are continuous, regular and frequently updated.

[50] The current draft of the ISO/SAE 21434 standard provide a Development Interface Agreement (DIA) template example where for each work product, one can clearly mark each organisation as either responsible, approver, support, inform or consult.

- **OP-06**: Raise vehicle owners', drivers' and passengers' awareness with respect to security issues and how to prevent them, on a regular basis.

4.3.3 Security Management

- **OP-07**: Consider establishing an OEM Security Operations Center (SOC) with clearly defined roles, responsibilities and cybersecurity competences to centralize knowledge on cybersecurity, monitor and anticipate potential threats.
- **OP-08**: Designate one or several[51] dedicated security team(s) with security specialists having diversified and broad range of competencies in security related topics (e.g. risk assessment, penetration testing, secure design, etc.).
- **OP-09**: Define a dedicated Information Security Management System (ISMS)[52] that covers smart cars entire lifecycle.
- **OP-10**: Consider defining an internal task force, which involves board-level management, to guide security-related strategic decisions and facilitate accountability.

4.3.4 Incident Management

- **OP-11**: OEMs and 3rd party suppliers should establish an incident handling process that should be tested and revised at least annually and as soon as possible in the case of a major change.
- **OP-12**: OEMs and 3rd party suppliers should consider establishing a Product Security Incident Response Team (PSIRT) and Computer Security Incident Response Team (CSIRT)[53]. Each team would be dedicated to handling security incidents respectively related to Products and Infrastructure and work along with the SOC if there is one.
- **OP-13**: Report incidents to back-end servers to ensure that systems are secure over their lifetime.
- **OP-14**: Define and classify relevant cybersecurity incidents to enable the identification of the most critical incidents and their prioritization, based on their potential impacts or broader effect for instance.
- **OP-15**: Consider establishing a secure and reliable process for detecting and handling misbehaving ITS stations, e.g. revoke credentials of misbehaving ITS stations.

4.4 TECHNICAL PRACTICES

Besides to the policies and organisational practices listed above, a set of technical security measures should be implemented to protect both smart cars and the associated back-end systems. Hereinafter, we provide an overview of these technical practices which covers several aspects such as software security, cloud security, detection, access control and so on.

4.4.1 Detection

- **TM-01**: Deploy Intrusion Detection Systems (IDSs) both at vehicle and back-end levels to enable the detection of malicious activities or policy violations.
- **TM-02**: Maintain properly protected audit logs to prevent their disclosure to unauthorised entities, while clearly defining their storage location and retaining period.

[51] For large organisations, it may be considered to build several security teams to split the scope, for instance, by separating corporate security policy, back-end systems and connectivity services, cars and embedded components security.
[52] "An ISMS consists of the policies, procedures, guidelines and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets." See ISO 27000: https://www.iso.org/fr/standard/73906.html
[53] See for instance https://www.first.org/

- **TM-03**: Consider periodically reviewing network logs, access control privileges and assets configuration.
- **TM-04**: Perform data validation to check the correctness of incoming information.
- **TM-05**: Define appropriate forensics procedures to enable event reconstruction, facilitate crash investigation, prevent similar attacks and/or for accountability purposes.

4.4.2 Protection of Networks and Protocols

- **TM-06**: Protect remote monitoring and administration interfaces through mutual authentication and access control mechanisms to prevent illegitimate access to smart cars systems.
- **TM-07**: Protect the integrity and authenticity of all critical in-vehicle internal communications.
- **TM-08**: Protect the integrity and authenticity of all external communications between the smart cars and all the different entities it is interacting with.
- **TM-09**: Enforce session management policies for the different communication sessions (e.g. administration,) to avoid session hijacking.
- **TM-10**: Timestamp all exchanged messages using reliable time sources (e.g. provided by secure embedded component or coming from satellite system) to mitigate replay attacks.
- **TM-11**: Manage radio frequencies and the frequency of beaconing[54] and other repeated messages in order to prevent Distributed DoS (DDoS) attacks.
- **TM-12**: Implement frequency agility feature to prevent signals jamming, if applicable.
- **TM-13**: Perform packet filtering at the different layers (e.g. ECU and sensors, mobile network communications, etc.) to analyse incoming and outgoing packets and discard illegitimate traffic.
- **TM-14**: Provide end-to-end protection of sensitive data in terms of confidentiality and integrity using secure protocols.

4.4.3 Software Security

- **TM-15**: Secure the default configuration of devices and services and ensure that the most secure operation mode of device (or service) is used by default.
- **TM-16**: Ensure software authenticity and integrity before its installation, to ensure that only legitimate software is used.
- **TM-17**: Implement and document changes in configuration according to a change management policy developed by the organisation based on risk analysis.
- **TM-18**: Secure OTA firmware updates to avoid firmware manipulation, disclosure or rollback to vulnerable versions.[55]
- **TM-19**: Define a secure OTA update process.
- **TM-20**: Implement secure boot processes that ensure systems integrity and authenticity. A risk-based approach may be used to identify when secure boot is actually needed.
- **TM-21**: Ensure that vulnerabilities and limitations of software dependencies, especially open source libraries, are mitigated or addressed in a risk assessment.
- **TM-22**: Protect mobile applications against reverse engineering (e.g. through code obfuscation techniques) and against tampering of their binary code (e.g. by signing it).
- **TM-23**: Securely store sensitive data (e.g. passwords) on mobile devices, and protect local files created by the mobile application.

[54] Beacons are messages exchanged periodically over vehicular networks to carry information such as location, heading, and speed.
[55] An example of secure OTA firmware update guidelines can be found in the Uptane project documentation https://uptane.github.io/uptane-standard/uptane-standard.html

4.4.4 Cloud Security

- **TM-24**: Cover security and availability aspects in agreements with cloud security providers, if applicable.
- **TM-25**: In the context of cloud-based application and centralised systems, ensure that single points of failure are prevented.
- **TM-26**: Operate critical systems and applications within the private[56] or at least hybrid[57] deployment models.
- **TM-27**: Protect all data within the cloud and during transfer while ensuring that cloud services providers do not have access to the decryption keys, so as to mitigate any potential risk stemming from cloud attacks.

4.4.5 Cryptography

- **TM-28**: Encrypt all sensitive, personal and private data to prevent its disclosure to illegitimate entities. Moreover, authenticated encryption may be used to avoid the manipulation of personal data while ensuring their confidentiality.
- **TM-29**: Use well-known and standardized cryptographic schemes and protocols that are widely considered as secure, and avoid the use of proprietary schemes.
- **TM-30**: Use of storage encryption to protect both users' data as well as data needed to enforce smart cars security (e.g. used keys, security credentials, etc.).
- **TM-31**: Implement a secure key management process. The process should cover all the steps of key lifecycle: key length choice in relation with key lifetime, key generation using an appropriate level of entropy from a reliable source, secure key storage, key rotation and revocation, etc.
- **TM-32**: Consider the use of dedicated and tamper resistant hardware security modules for secure execution of cryptographic algorithms and secure key storage.

4.4.6 Access Control

- **TM-33**: Apply security controls at back-end servers; covering policies, physical and logical security aspects as well as the security of internal networks and data.
- **TM-34**: Apply least privileges principle and use individual accounts to access devices and/or systems.
- **TM-35**: Segregate remote access by developing a set of rules for the control and monitoring of remote communications.
- **TM-36**: Allow and encourage the use of strong authentication mechanisms, e.g. Multi-Factor Authentication (MFA), define an account lockout functionality, etc.

4.4.7 Self-Protection and Cyber Resilience

- **TM-37**: Implement differential monitoring on the GNSS system, to ensure accurate localisation data.
- **TM-38**: Apply a hardening approach on the different level (i.e. devices, network, back-end, etc.) to reduce the attack surface.

[56] A private cloud refers to a cloud environment that is operated exclusively for a single organization.
[57] A hybrid cloud combines both private and public cloud that are bound together for better cost-effectiveness and to provide more flexibility and control.

- **TM-39**: Reinforce interfaces robustness, e.g. to cope with buffer overflows or fuzzing.
- **TM-40**: Consider strengthening applications isolation at runtime, using trusted software technologies.
- **TM-41**: Apply system, sub-domain and network segregation using physical and logical isolation techniques where appropriate (based on risk assessment).

4.4.8 (Semi-) Autonomous Systems Self Protection and Cyber Resilience

- **TM-42**: Consider using inboard Inertial Navigation System (INS) or existing dead-reckoning methods to get localisation data, even in case of GNSS failure.
- **TM-43**: Protect critical autonomous sensors to prevent the different attacks aiming to alter smart cars environment perception.
- **TM-44**: Harden against Adversarial attacks, to prevent AI and ML components from being tricked.
- **TM-45**: Prevent data falsification or manipulation in regard to AI and ML.
- **TM-46**: Use of data redundancy mechanisms (e.g. sensor data fusion) that correlate data acquired from the different sensors in the vehicle and data obtained via V2X communications before making a decision.
- **TM-47**: Use of hardware redundancy mechanisms by adding extra hardware components able to carry out the required operations and perform self-driving tasks.

4.4.9 Continuity of Operations

- **TM-48**: Ensure that notifications are easy to understand, and help users find a remediation or workaround.
- **TM-49**: Create a Business Continuity Plan (BCP) and a Business Recovery Plan (BRP) that cover third-party aspects and are periodically tested, at least annually, to ensure the resilience of smart cars systems.
- **TM-50**: Define important parameters for the business continuity of the organisation, e.g. Recovery Time Objective (RTO), Maximum Tolerable Outage (MTO), etc.

5. ABBREVIATIONS

ACRONYM	DEFINITION
ADS-DV	Automated Driving System-Dedicated Vehicle
AI	Artificial Intelligence
AP	Access Point
Auto-ISAC	Automotive Information Sharing and Analysis Center
BSI	British Standards Institution
BSM	Basic Safety Message
BTS	Base Transceiver Station
CaRSEC	Cars and Roads SECurity working group
CCAM	Cooperative, Connected and Automated Mobility
CSIRT	Computer Security Incident Response Team
C-ITS	Cooperative Intelligent Transport Systems
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
DG MOVE	Directorate-General for Mobility and Transport
DSRC[58]	Dedicated Short-Range Communications
ECU	Electronic control Unit
E/E	Electrical and Electronic
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System

[58] In this document, DSRC refers to the standards from the European Committee for Standardization EN 12253:2004 and EN 12795:2002

IDS	Intrusion Detection System
ICE	In Car Entertainment
IMU	Inertial Measurement Unit
IPS	Intrusion Prevention System
ISC	Image Sensor Communication
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transportation System
IVI	In-Vehicle Infotainment
LiDAR	Light Detection and Ranging
LIN	Local Interconnect Network
MFA	Multi-Factor Authentication
MITM	Man-In-The-Middle
ML	Machine Learning
MOST	Media Oriented Systems Transport
NFC	Near-Field Communication
NHTSA	National Highway Traffic Safety Administration
NIS	Network and Information Security directive
OBD	On-Board Diagnostic
OEM	Original Equipment Manufacturer
OS	Operation System
OTA	Over-The-Air
OT	Operational Technology
PAS	Publicly Available Specifications
PIA	Privacy Impact Assessment
RSE	Road Side Equipment

RSU	Road-Side Unit
SAE	Society of Automotive Engineers
SME	Small-Medium Enterprises
SOC	Security Operation Center
TCU	Telematic Control Unit
UNECE	United Nations Economic Commission for Europe
UTC	Universal Coordinated Time
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything. Includes the notion of V2V, V2I, V2P and V2N communications
VLC	Visible Light Communication

6. BIBLIOGRAPHY/REFERENCES

SAE J3016 “Taxonomy and Definitions for Terms Related to Driving Automations Systems for On-Road Motor Vehicles”: http://sae.org/standards/content/J3016_201806/

ENISA (2016) “Cyber Security and Resilience of smart cars – Good practices and recommendations”: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

“Self-Driving Vehicles in an Urban Context”: http://www3.weforum.org/docs/WEF_Press%20release.pdf

European Commission “On the road to automated mobility: An EU strategy for mobility of the future”: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf

“Rethinking Transportation 2020-2030 – The disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries”: https://static1.squarespace.com/static/585c3439be65942f022bbf9b/t/591a2e4be6f2e1c13df930c5/1494888038959/RethinkX+Report_051517.pdf

“Self-driving Ubers could still be many years away, says research head”: https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head

“Hackers remotely kill a Jeep on the highway – with me in it”: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

“Experimental security assessment of BMW cars: A summary report”: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

“Hacking smart car alarm systems”: https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/

“PASTA: Portable Automotive Security Testbed with Adaptability”: https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-Toyama-PASTA-Portable-Automotive-Security-Testbed-with-Adaptability-wp.pdf

“PASTA 1.0 L and F Software Development Tools – Product details”: https://www.chip1stop.com/USA/en/view/dispDetail/DispDetail?partId=LANF-0000001

“Remote attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR”: https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

“Self-driving and connected cars: fooling sensors and tracking drivers”: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers.pdf

"All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems": https://www.usenix.org/node/217477

"Meet the Artist Using Ritual Magic to Trap Self-Driving Cars": https://www.vice.com/en_us/article/ywwba5/meet-the-artist-using-ritual-magic-to-trap-self-driving-cars

"Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR": https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

"Illusion and Dazzle: Adversarial Optical Channel Exploits against LiDARs for Automotive Applications": https://eprint.iacr.org/2017/613.pdf

"Fast and Vulnerable: A Story of Telematic Failures": https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf

"Robust Physical-World Attacks on Deep Learning Visual Classification": https://arxiv.org/pdf/1707.08945.pdf

"European Commission Launches CCAM Single Platform": https://connectedautomateddriving.eu/mediaroom/european-commission-launches-ccam-single-platform/

EU "General Data Protection Regulation": https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union": https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Cybersecurity Best Practices for Modern Vehicles – NHTSA : https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Auto-ISAC "Automotive Cybersecurity Best Practices – Executive summary": https://www.automotiveisac.com/best-practices/

UNECE "Proposal for Recommendation on Cyber Security": https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

"PAS 1885:2018 - The fundamental principles of automotive cyber security. Specification": https://shop.bsigroup.com/ProductDetail?pid=000000000030365446

"PAS 11281:2018 - Connected automotive ecosystems. Impact of security on safety. Code of practice": https://shop.bsigroup.com/ProductDetail?pid=000000000030365540

ETSI TS 102 940 v1.3.1, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management": https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

ETSI TS 102 941 V1.2.1 "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

ETSI TS 102 942 V1.1.1 “Intelligent Transport Systems (ITS); Security; Access Control” https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/ts_102942v010101p.pdf

ETSI TS 102 943 V1.1.1 “Intelligent Transport Systems (ITS); Security; Confidentiality services” https://www.etsi.org/deliver/etsi_ts/102900_102999/102943/01.01.01_60/ts_102943v010101p.pdf

ETSI TS 103 097 v1.3.1, “Intelligent Transport Systems (ITS); Security; Security header and certificate formats”: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

ETSI TR 102 893 “Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA) https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf

SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”: https://www.sae.org/standards/content/j3061_201601/

ITF/OECD “Safer Roads with Automated Vehicles”, https://www.itf-oecd.org/sites/default/files/docs/safer-roads-automated-vehicles.pdf

ISO/SAE CD 21434 “Road Vehicles – Cybersecurity engineering”: https://www.iso.org/standard/70918.html

“ENISA Threat Taxonomy” (2016): https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

“Tesla cars can be stolen by hacking the app”: https://promon.co/security-news/hacking-tesla-app-stolen-car/

“MobilBye: Attacking ADAS with Camera Spoofing”: https://arxiv.org/pdf/1906.09765.pdf

“Robust Physical-World Attacks on Deep Learning Models”: https://arxiv.org/pdf/1707.08945.pdf

“Self-driving Ubers could still be many years away, says research head”: https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head

“Domain Controlled Architecture – A new approach for large scale software integrated automotive systems”: https://pdfs.semanticscholar.org/65ff/f1cd276736bc5cf67d0cb30db269cd08b5f5.pdf

“VCIDS: Collaborative Intrusion Detection of Sensor and Actuator Attacks on Connected Vehicles”: http://php.scripts.psu.edu/muz16/pdf/PG-ea-Comm17.pdf

“Work-in-Progress: Road Context-aware Intrusion Detection System for Autonomous Cars”: https://sudiptac.bitbucket.io/papers/raids.pdf

“Intelligent Intrusion Detection in External Communication Systems for Autonomous Vehicles”: https://www.tandfonline.com/doi/full/10.1080/21642583.2018.1440260

"Hopping on the CAN Bus – Automotive Security and the CANard Toolkit": https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf

"DEFCON – Connected Car Security": https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/defcon-connected-car-security/

"Spatially Clustered Autonomous Vehicle Malware: Producing New Urban Geographies of Inequity": https://journals.sagepub.com/doi/full/10.1177/0361198118794057

"Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars": https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

"All your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems": https://www.usenix.org/node/217477

"Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles": https://ieeexplore.ieee.org/document/8451864

"Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems": https://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-Autonomous-Vehicle-Jamming-and-Spoofing-Comment-Final.pdf

UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security : https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

Safety First for Automated Driving : https://www.aptiv.com/docs/default-source/white-papers/safety-first-for-automated-driving-aptiv-white-paper.pdf

SCOUT - Report on the state of the art of connected and automated driving in Europe : https://connectedautomateddriving.eu/publication/scout-deliverable-3-2-report-on-the-state-of-the-art-of-connected-and-automated-driving-in-europe-final/

PAS 1885:2018 The fundamental principles of automotive cyber security specification, bsi : https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview Document : https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf

Autonomous DevSecOps: Five Steps to a Self-Driving Cloud (ENT214-S) - AWS re:Invent 2018 : https://www.slideshare.net/AmazonWebServices/autonomous-devsecops-five-steps-to-a-selfdriving-cloud-ent214s-aws-reinvent-2018

Redhat DevSecOps : https://www.redhat.com/en/topics/devops/what-is-devsecops

What is DevSecOps? Developing more secure applications : https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html

Security Champions Playbook :
https://www.owasp.org/index.php/Security_Champions_Playbook

Avoid Unnecessary Pain with a Security Champion :
https://www.csoonline.com/article/3299430/avoid-unnecessary-pain-with-a-security-champion.html

IoT Alliance Australia - Internet of Things Security Guidelines v1.2 :
https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

Privacy Impact Assessment : https://gdpr-info.eu/issues/privacy-impact-assessment/

Data Protection Impact Assessment (DPIA) : https://gdpr.eu/data-protection-impact-assessment-template/

GDPR: How to Perform a Data Audit : https://www.thesslstore.com/blog/gdpr-data-audit/

GDPR checklist for data controllers : https://gdpr.eu/checklist/

Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance : https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf

Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things :
https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

IEC - IEC 62443-3-3:2013 System security requirements and security levels :
https://webstore.iec.ch/publication/7033

ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems -- Requirements : https://www.iso.org/standard/54534.html

ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls : https://www.iso.org/standard/54533.html

NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile :
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices :
https://www.sans.org/reading-room/whitepapers/threats/paper/1267

Huawei - IoT Security White Paper 2017 :
https://www.huawei.com/minisite/iot/img/hw_iot_secutity_white_paper_2017_en_v2.pdf

NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks : https://csrc.nist.gov/publications/detail/nistir/8228/final

LNS - Putting Industrial Cyber Security at the top of the CEO agenda : https://www.honeywellprocess.com/en-US/online_campaigns/lns-cyber-report/Pages/Honeywell-LNS-Study_PuttingIndustrialCyberSecurityattheTopCEOAgenda.pdf

NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Safety First for Automated Driving" (SaFAD) : https://www.daimler.com/innovation/case/autonomous/safety-first-for-automated-driving-2.html

European Commission -- Access to In-vehicle Data and Resources : https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

ENISA - Cyber Security and Resilience of Smart Cars : https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis : https://www.etsi.org/deliver/etsi_TR/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf

Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary : https://www.automotiveisac.com/best-practices/

IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use : https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf

International Telecommunications Union - Security capabilities supporting safety of the Internet of things : https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.4806-201711-I!!PDF-E&type=items

Five Star Automotive Cyber Safety Program : https://www.iamthecavalry.org/domains/automotive/5star/

Securing the Modern Vehicle : https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/securing-the-modern-vehicle.pdf

Security Development Lifecycle (SDL) : https://www.microsoft.com/en-us/securityengineering/sdl/practices

COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES : https://www.automotiveisac.com/wp-content/uploads/2018/08/2018_01_18_Best_Practice_Guide_Third_Party_Collaboration_Engagemen.pdf

ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing : https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program : https://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf

Insecurity in the Internet of Thing : https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf

IoT Security Awareness : https://resources.infosecinstitute.com/iot-security-awareness/#gref

Consumers don't care if their connected car can get hacked - here's why that's a problem : https://www.businessinsider.com/smart-car-hacking-major-problem-for-iot-internet-of-things-2016-3?IR=T

Shifting gears in cyber security for connected cars: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx

CSIRTs in Europe:https://www.enisa.europa.eu/topics/csirts-in-europe?tab=articles

ACEA Principles of Automobile Cybersecurity: https://www.acea.be/publications/article/acea-principles-of-automobile-cybersecurity

Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/securing-the-modern-vehicle.pdf

30% of Automotive Companies Lacking a Dedicated Cybersecurity Team : https://www.bleepingcomputer.com/news/security/30-percent-of-automotive-companies-lacking-a-dedicated-cybersecurity-team/

Security Champions Playbook : https://www.owasp.org/index.php/Security_Champions_Playbook

Avoid Unnecessary Pain with a Security Champion : https://www.csoonline.com/article/3299430/avoid-unnecessary-pain-with-a-security-champion.html

SAE J3061: https://www.researchgate.net/publication/307585960_Using_SAE_J3061_for_Automotive_Security_Requirement_Engineering

Security Operations Center : https://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html

MITRE :Cybersecurity Operations Center : https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

Survey and Classification of Automotive Security Attacks - MDPI : https://www.mdpi.com/2078-2489/10/4/148/pdf-vor

PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 : https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.1-Security%20Requirements%20of%20Vehicle%20Security%20Architecture.pdf

C-ITS Platform, WG5: Security & Certification - Final Report - Annex 2: Revocation of Trust in C-ITS : https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An2_v1.0.pdf

ACEA Principles of Automobile Cybersecurity : https://www.acea.be/publications/article/acea-principles-of-automobile-cybersecurity

ENISA - Baseline Security Recommendations for IoT : https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices : https://www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf

IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines : https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf

OWASP (Open Web Application Security Project) - IoT Security Guidance : https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

SANS Institute - An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity : https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf

A survey on open automotive forensics : https://forschung-sachsen-anhalt.de/publication/survey-open-automotive-forensics-1002323053

Log your car: the non-invasive vehicle forensics : https://ieeexplore.ieee.org/document/7847047

“My autonomous car is an elephant”: A Machine Learning based Detector for Implausible Dimension : https://ieeexplore.ieee.org/document/8556651

AUTOMOTIVE WORKING GROUP : https://www.w3.org/blog/auto/

OWASP: Session Management Cheat Sheet : https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

OWASP: Session fixation : https://www.owasp.org/index.php/Session_fixation

CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0 : https://www.car-2-car.org/service/privacy/

Secure Device Configuration Guideline : https://security.berkeley.edu/secure-device-configuration-guideline

ISA-95.01 MODELS & TERMINOLOGY : https://isa-95.com/isa-95-01-models-terminology/

Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor : https://www.industry.usa.siemens.com/automation/us/en/formsdocs/Documents/2016%20MIA-

%2023%20Industrial%20Security%20Applying%20IoT%20Security%20Controls%20on%20the%20Industrial%20Plant%20Floor.pdf

Gowling WLG & UK Autodrive - Connected and Autonomous Vehicles: A Hacker's Delight? : https://gowlingwlg.com/GowlingWLG/media/UK/pdf/autodrive/170907-cyber-security-white-paper.pdf

Cybersecurity Solutions for Connected Vehicles : https://www.trendmicro.com/us/iot-security/content/main/document/IoT%20Security%20for%20Auto%20Whitepaper.pdf

Securing Self-Driving Cars : http://illmatics.com/securing_self_driving_cars.pdf?_sm_au_=iqs579QRrj9HP44Q

Using Open Source for security and privacy protection : https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/10-using-oss.html

Federal Office for Information Security: Business Continuity Management : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems : https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.12-v1.0.pdf

Online Trust Alliance - IoT trust framework 2.5 : https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

SANS Institute - Building the New Network Security Architecture for the Future : https://www.sans.org/reading-room/whitepapers/internet/paper/38255

Cloud Security Alliance - Future Proofing the connected world : https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1

FAQ: CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0 : https://www.car-2-car.org/fileadmin/documents/General_Documents/C2CCC_TR_2051_Data_Protection.pdf

European Commission - Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport System (C-ITS) : https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

What is physical security? How to keep your facilities and devices safe from on-site attackers : https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html

Principle of least privilege (POLP) : https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

Improving security through least-privilege practices : http://techgenix.com/improving-security-through-least-privilege-practices/?_sm_au_=iqs579QRrj9HP44Q

GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems : https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.13-v1.0.pdf

Autonomous integrity monitoring of navigation maps on board intelligent vehicles : https://www.researchgate.net/publication/278826487_Autonomous_Integrity_Monitoring_of_Navigation_Maps_on_board_Intelligent_Vehicles

Symantec - Insecurity in the Internet of Things : https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/insecurity-in-the-internet-of-things-15-en.pdf

OWASP Internet of Things Project – OWASP : https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

OWASP Top Ten Project – OWASP : https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Secure hypervisor versus trusted execution environment : http://www.diva-portal.se/smash/get/diva2:1120483/FULLTEXT01.pdf?_sm_au_=iqs579QRrj9HP44Q

Isolated Execution in Many-core Architectures : https://eprint.iacr.org/2014/136.pdf

An Autonomous Vehicle Navigation System Based on Inertial and Visual Sensors : https://www.researchgate.net/publication/327470347_An_Autonomous_Vehicle_Navigation_System_Based_on_Inertial_and_Visual_Sensors

Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR : https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

Towards deep learning models resistant to adversarial attacks : https://openreview.net/pdf?id=rJzIBfZAb

Explaining and harnessing adversarial examples : https://arxiv.org/pdf/1412.6572.pdf

Pixeldefend: Leveraging generative models to understand and defend against adversarial examples. In International Conference on Learning Representations (ICLR),2018 : https://openreview.net/forum?id=rJUYGxbCW

The robust manifold defense: Adversarial training using generative models : https://arxiv.org/abs/1712.09196

Thermometer encoding: One hot way to resist adversarial examples. In International Conference on Learning Representations (ICLR), 2018 : https://openreview.net/pdf?id=S18Su--CW

Securing the Future of AI and ML : https://docs.microsoft.com/en-us/security/securing-artificial-intelligence-machine-learning

Groupe PSA - Attacker model for Connected and Automated Vehicles Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR : https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

Duo Security - The Internet of Fails ; Where IoT Has Gone Wrong : https://www.slideshare.net/markstanislav/the-internet-of-fails-where-iot-has-gone-wrong-and-how-were-making-it-right

A Hard Problem with No Easy Answers | Decipher - IoT Security : https://duo.com/decipher/iot-security-hard-problem-no-easy-answers

Center for Internet Security (CIS) - Critical Security Controls : https://www.cisecurity.org/controls/

oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report : http://www.onem2m.org/images/files/deliverables/Release2A/TR-0008-Security-v_2_0_1.pdf?_sm_au_=iqs579QRrj9HP44Q

OWASP – Mobile Application Security Verification Standard: https://github.com/OWASP/owasp-masvs/releases/download/1.1.4/OWASP_Mobile_AppSec_Verification_Standard_1.1.4_Document.pdf

ENISA – Smartphone Secure Development Guidelines: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

ANNEX A: ASSET TAXONOMY

Annex A lists the different assets mentioned in **Figure 5**, and provides a brief description of each asset.

Asset Group	Assets	Description
Car sensors and actuators	Standard Sensors	These devices are common sensors (e.g. tire pressure, air bag impact, GNSS, speed, powertrain, seat belt, passenger occupancy, temperature, oil, water coolant, parking and climate control sensors) usually embedded in cars to measure some parameters and/or monitor or detect some events. The collected data is transmitted to ECU for processing purposes.
	Sensors for autonomous vehicles	These devices are relatively new sensors embedded in autonomous vehicles to provide self-driving capabilities (e.g. localization, enabling the detection and identification of objects and people). This category of sensors mainly includes the following sensors: • Light Detecting and Ranging (LiDAR) • Lasers • Cameras • Radars • Ultrasonic sonars
	Actuators	These devices are an important part of vehicles. They interact with the environment by converting an electrical signals received from the ECU into an action (e.g. apply the brake when a red light or a pedestrian crossing the road is detected, speed reduction on bad weather conditions, change of direction to get around an obstacle). The engine control unit, suspension, transmission, brake system and steering system are some examples of actuators.
Decision Making Algorithms **(Car ECUs, processing and decision making components** **Smart cars Infrastructure and Backend systems)**	ML and AI algorithms	These software components provide smart cars with the capability to perform tasks that are typical for intelligent beings, such as reacting to an unanticipated and new situation based on previously collected data. ML and AI algorithms are implemented inside smart cars to enable them to react in real time whenever required, but they may be implemented outside the vehicle in remote servers as well.

Asset Group	Assets	Description
	Data fusion algorithms	These software components combine data acquired from different sensors (e.g. LiDAR and camera) and V2X communications.
Vehicle Functions **Car sensors and actuators** **Car ECUs, processing and decision making components**	Vehicle functions	This term refers to the different vehicle functions (such as braking, acceleration, operating the steering wheel, route planning, etc.) which rely on one or several sensors data as well as processing and actuating nodes to operate correctly.
Software management **Car ECUs, processing and decision making components** **In-vehicle communication components** **Smart cars Infrastructure and Backend systems**	Software and Licenses	This term refers to the different software components of the vehicle. It includes on-board operating systems (which manage the resources of a given smart car hardware device and provides common services for other computer programs to run), programs and codes (which are written to perform a given task or technological objective, such as AI-based algorithms as well as real-time monitoring algorithms, or even protocol stacks/cryptographic algorithms' software implementations), mobile applications (which correspond to programs running on mobile devices such as smartphones and tablets that are used to communicate with the smart car, to unlock the doors for instance) and antivirus (which is a particular software that monitors a device or network to detect and identify malwares, and prevent them from infecting devices) as well as on-board firmware (which is a class of software that are stored on a device read-only memory and provides instructions on how the device should operate). A smart car can include several OSes embedded on different devices. As for programs, antivirus and firmware, they can be found at every level: from ECUs to back-end servers.
	Software updates	This term refers to software updates (including Over-The-Air (OTA) updates) that are used by the OEM to remotely or locally deploy new firmware or software on smart cars.
Inside vehicle Communication Components	Telematics box	This electronic module is the vehicle main communication unit. It provides the capability to connect to the cellular communication networks and enables other short and long range communications based on several technologies, such as Near Field Communications (NFC), Bluetooth, WiFi, etc.

Asset Group	Assets	Description
In-vehicle communication components	Vehicle ITS station	This device enables wireless V2V and V2I communications.
	In-Vehicle Gateway	This device plays a crucial role in smart cars. It interconnects the various in-vehicle networks to the telematics box and ITS station. It also provides physical isolation between the different functional domains.
	In-Vehicle Infotainment (IVI)	This asset, also known as Head Unit or In-car Entertainment (ICE), refers to a vehicle system combining information exchanges (between the vehicle and the drivers/passengers through a touch screen-based tablet like device) and entertainment (i.e. audio and video). Smartphones can also be paired with such unit, allowing remote connectivity. It provides a hardware interface for the entire vehicle.
	OBD-II port	The OBD-II port, also called diagnostics plug, is an external interface that allows plugging different maintenance and diagnostic devices to smart cars.
	EV charging connector	The interface used to plug an electric or hybrid smart car to a charging station.
Communication Networks and Protocols (Car ECUs, processing and decision making components **In-vehicle communication components** **Car sensors and actuators**	In-Vehicle networks	In-vehicle communications and domain subnetworks rely on several protocols such as Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), FlexRay and Ethernet.
	Protocols and communication technologies	Telematics box and ITS station provide different wireless communication technologies including 802.11p (DSRC), Cellular-V2X (C-V2X), cellular technologies (2G, 3G, 4G, 5G), NFC, Wi-Fi, Bluetooth.
Nearby External Components **Smart cars Infrastructure and Backend systems**	Communication Components	These devices refers to nearby communication components interacting with smart cars. They include: Access Points (AP) which is a cellular networking hardware device that supports cellular communications and which directly communicates with the smart car telematics box. Road Side Unit (RSU), also known as Road Side Equipment (RSE), which is a communication device located on the roadside to provide connectivity and enable communication between the road side infrastructure and smart cars.

Asset Group	Assets	Description
	Traffic signs and lights	Traffic signs and lights provide road users and smart cars with the necessary safety instructions and are mainly used to regulate the speed and traffic flow. In particular, traffic signs give the driving practices to follow and warn about dangerous conditions while traffic lights provide vehicles and drivers with the necessary instructions to follow at intersections and along roads. This asset includes lane marking as well.
Network and Domain Isolation Features **Car ECUs, processing and decision making components,** **In-vehicle communication components** **Smart cars Infrastructure and Backend systems**	Firewall	This network security device or software monitors and controls incoming and outgoing network traffic based on a predetermined set of security rules.
	Routing table	It corresponds to a set of rules enabling to direct data packets to its destination or drop the packet if no match is found.
	Domain controllers[59]	These devices interconnect the different in-vehicle functional domains. They need to be powerful in terms of processing capabilities and real-time performance in order to support autonomous vehicles' highly interconnected architecture.
	IDS/IPS	Intrusion Detection Systems (IDS) allow automatic monitoring of the happening events, and analyses them to detect any potential sign of intrusion. Intrusion Prevention Systems (IPS) can also perform given actions whenever some specific events happen in attempt to stop the incident. Such systems can be found deployed at the vehicle level[60,61] as well as the infrastructure level[62].
Servers, Systems and Cloud Computing **Smart cars Infrastructure and Backend systems**	Back-end Systems	This term refers to the back-end systems which enable Over-The-Air updates among other services.
	Database servers	This term refers to a database back-end system which consists of both hardware and software used to run a database. These servers may for instance store and process in-vehicle data and resources to enable service providers to propose services such as software updates.
	Maps servers	This term refers to remote servers that provide longitudinal and lateral data to the smart cars, thus

[59] See "Domain Controlled Architecture – A new approach for large scale software integrated automotive systems": https://pdfs.semanticscholar.org/65ff/f1cd276736bc5cf67d0cb30db269cd08b5f5.pdf
[60] See "VCIDS: Collaborative Intrusion Detection of Sensor and Actuator Attacks on Connected Vehicles": http://php.scripts.psu.edu/muz16/pdf/PG-ea-Comm17.pdf
[61] See "Work-in-Progress: Road Context-aware Intrusion Detection System for Autonomous Cars": https://sudiptac.bitbucket.io/papers/raids.pdf
[62] See "Intelligent Intrusion Detection in External Communication Systems for Autonomous Vehicles": https://www.tandfonline.com/doi/full/10.1080/21642583.2018.1440260

Asset Group	Assets	Description
		enabling it to navigate and to decide the next trajectory to reach its destination. These servers may also provide a map database that can be locally stored on the vehicle.
	Third- party service providers servers	This term refers to remote servers used by service provider in order to propose added value services such as eToll for toll payments and breakdown call (bCall).
Information **Throughout model**	Sensors data	This asset refers to data that is gathered by the different smart car sensors and which will be transmitted to the appropriate ECU for processing.
	Keys and certificates	This asset refers to the different keys and certificates used for security purposes (such as authentication, securing the exchanges, secure boot, etc.). Keys are stored in devices embedded in the vehicle (e.g. ECU) and/or in servers depending on their use.
	Map data	This asset refers to the information about the car environment. Map data allow to increase the passenger safety by correlation its information with the sensors perception. Contrary to GNSS which gives only information about the geolocalization, map data gives information about the surrounding environment.
	V2X information	This asset refers to the different information exchanged via V2X communications (e.g. emergency vehicle approaching, roadworks/collision warning and traffic information).
	Device information	This asset refers to the different information related to a device embedded in a smart car (e.g. ECU, TCU) or connected devices (e.g. smartphones, tablet). This includes information such as type, configuration, firmware version, status, etc.
	User information	This asset refers to smart cars user (e.g. driver, passenger, etc.) information such as name, role, privileges and permissions.
Humans **Throughout model**	Drivers	This asset refers to all individuals who are entitled to drive the smart car. This asset is optional when considering SAE automation level 5 as such smart car is fully automated.
	Passengers	This asset refers to all individuals that are onboard smart cars.

Asset Group	Assets	Description
	OEM staff	This asset refers to OEM individuals who have physical or remote privileged access to the smart car for several purposes (such as maintenance, adding features and performing updates).
	Mechanics	This asset refers to non-OEM individuals who have physical access to smart cars for maintenance purposes.
Mobile Devices **(Smart cars Infrastructure and Backend systems)**	Smartphones and Tablets	This term refers to portable devices that run mobile applications providing added value services to the vehicle user.

ANNEX B: THREAT TAXONOMY

Annex B provides a brief description of the different threats subcategories mentioned in **Figure 6**, and maps each threat to the asset(s) that may potentially be affected.

Threat Category	Threat	Description	Impacted Assets
Nefarious activity/Abuse	Denial of Service	Smart cars and their infrastructure, may be subject to Distributed Denial of Service (DDoS) attacks, or even used to launch such attacks. DoS attacks may target (or originate from) RSUs or the IT systems. An attacker may for instance shut down the RSU (via physical access or remotely), overload the system with messages to process or even jam radio communications, etc. In-vehicle components can also be the target of DoS attacks. For instance, overloading the CAN bus with malicious messages will alter the vehicle behaviour[63].	All assets
	Malware	These malicious software aim at performing unwanted and illegitimate actions such as disabling smart cars functions (e.g. prevent car unlocking or immobilize the engine). Malware can cause unexpected behaviours of the smart car and even endanger passengers' safety. Common examples or malwares are Ransomware[64], viruses, Trojan horses, Spyware[65] and exploit kits.	All assets
	Manipulation of hardware and software	This threat consists of unauthorized and illegitimate alteration of a component firmware, operations or configuration data by an attacker (e.g. malicious OTA updates). An attack might also access the binary file, compromising the intellectual property. The risk is emphasized when there are no security measures (e.g. secure boot) to protect the authenticity of critical hardware and software components. An attacker may also perform Man-in-the-middle attacks by	All assets

[63] See "Hopping on the CAN Bus – Automotive Security and the CANard Toolkit": https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf
[64] See "DEFCON – Connected Car Security": https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/defcon-connected-car-security/
[65] See "Spatially Clustered Autonomous Vehicle Malware: Producing New Urban Geographies of Inequity": https://journals.sagepub.com/doi/full/10.1177/0361198118794057

Threat Category	Threat	Description	Impacted Assets
		manipulating the hardware. Potential consequences of this kind of threats may include inappropriate smart cars behaviours.	
	Manipulation of information	This threat consists of illegitimate and unwanted data alteration by an attacker. To this end, the attacker may use various technical means such injecting fake Basic Safety Message (BSM)[66], performing map data poisoning, faking security-related information (e.g. keys, certificates, Certificate Revocation List), tampering with RSU data or OTA update exchanges, injection of packet over CAN bus[67], repudiation of actions (e.g. deny eToll), loss of data (e.g. erase of vehicle history), etc. Information manipulation threats may result in inappropriate decisions that are based on the altered/falsified data, and may also lead to information or intellectual values disclosure.	- Vehicle sensors and actuators - Decision making algorithms - Vehicle Functions - Network and Domain Isolation Features - Information - In-vehicle Communication Networks - In-vehicle Communication Components - External Communication Components - Servers, Systems and Cloud Computing - Mobile Devices - Humans
	OEM Targeted attacks	Cyberattacks targeting smart cars manufactured by a specific OEM or its backend systems during which the attackers typically use several attack methods and entry points to achieve their goals. Such attacks are usually scalable and may lead to reputational damage and/or information or intellectual property disclosure (such as the knowledge of in-vehicle internal architecture).	All assets
	Unauthorised activities	A legitimate user may try to access unauthorized functions for various reasons: they might want to circumvent DRMs on applications or media, or get an unauthorized	All assets

[66] A specific message format aimed to convey critical vehicle state information in support of V2V safety applications, as defined in SAE J2735 https://www.sae.org/standards/content/j2735_201603/
[67] See "Hopping on the CAN Bus – Automotive Security and the CANard Toolkit": https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf

Threat Category	Threat	Description	Impacted Assets
		access to features (geo-fencing, digital tachograph…), or they might simply want to tune the vehicle for comfort or performance purposes. Outside vehicles, manufacturers may also be confronted with garages using unauthorized or unlicensed professional tools and software. Unauthorised software may also be installed by an attacker. This threat also includes the notion of cloning, for example when an attacker copies the firmware of an existing device, in order to commercialize it without authorization.	
	Identity theft	Impersonation attacks in which an adversary successfully assumes the identity of one of the legitimate parties in the system or in a communication protocol. A common example is to impersonate a key fob[68] to steal the associated car. This may, however, be completed for other purposes, such as fraud, for example if a user wants their car to display another identity when communicating with: - road infrastructures such as toll systems, thus leading to financial fraud; - manufacturer backend[46] (to get access to paid services without subscription). An attacker may also impersonate a police car or ambulance in order to make other vehicles slow down or pull over. Thus, the attacker can reach his destination more quickly.	All assets
	Abuse of authorizations	A disgruntled employee (backend services, garage) may use their authorizations to perform malicious actions (e.g. create illegitimate user accounts, or add malicious software into the system). A slightly different scenario would be for an infotainment application to abuse its authorizations (for example, to mine private data or perform surveillance activities).	All assets

[68] See "Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars": https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passive-keyless-entry-and-start-in-modern-supercars/

Threat Category	Threat	Description	Impacted Assets
Threats against (semi-) autonomous systems	Threats targeting autonomous sensors	Smart cars autonomous sensors (like cameras, LiDARs and Radar sensors) may be subject to DoS attacks using several means such as presenting too many objects to track, blinding camera[69] and LIDAR/radar jamming[70]. GNSS spoofing[71] attacks may also be performed in an attempt to deceive a GNSS receiver through the broadcast of incorrect GNSS signals.	- Sensors for autonomous vehicles - Vehicle Functions - Information
	Threats against AI and ML	Attacks may be carried out against AI and ML features. For instance, the attacker may perform adversarial perturbation[72] in an intent to hide objects, fool auto-controls (e.g. radar/LIDAR confusion) and/or perceive fake data (e.g. fake crash sound or ultrasonic reflection[73], magnetic attacks targeting odometric sensors). An attacker may also provide malicious inputs during the model training phase in order to alter the classification.	- Sensors for autonomous vehicles - Decision Making algorithms - Vehicle Functions - Information
Physical attack	Sabotage	Intentional tampering of a device by an attacker with the aim to alter the proper functioning of the vehicle, thus endangering the safety of smart cars passengers and roads users. The attacker may directly target smart cars components (e.g. by compromising decision making algorithms or brake system, replacing a car component with a malicious one), or alter/remove RSUs, traffic signs and/or lights. The attacker may even compromise backend systems (e.g. eCall platform, database servers) in an attempt to execute unauthorized operations.	All assets
	Vandalism	Intentional physical degradation of car components (e.g. damage cameras), RSUs, traffic signs or lights (e.g. alter or remove traffic signs on the road). Such threat would impact the operations of the vehicle and	- Vehicle sensors and actuators - Decision making algorithms - External

[69] See "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR": https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf
[70] See "Illusion and Dazzle: Adversarial Optical Channel Exploits against LiDARs for Automotive Applications": https://eprint.iacr.org/2017/613.pdf
[71] See "All your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems": https://www.usenix.org/node/217477
[72] See "Robust Physical-World Attacks on Deep Learning Visual Classification": https://arxiv.org/pdf/1707.08945.pdf
[73] See "Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles": https://ieeexplore.ieee.org/document/8451864

Threat Category	Threat	Description	Impacted Assets
		make cause accidents and dangerous situations.	communication components - Information - Humans
	Theft	Theft of devices (e.g. car components, RSUs) that may alter the vehicle proper functioning and endanger road users' safety.	- Vehicle sensors and actuators - Decision making algorithms - External communication components - Information - Humans
	Side-channel attacks	Side-channel attacks consist in exploiting physical characteristics of the computing platform (e.g. execution time, power consumption) to recover security credentials (i.e. cryptographic keys and passwords) in order to bypass security mechanisms. Such attacks generally require a physical access to the targeted device, but some of them (e.g. timing attacks) may be performed remotely. Side channel attacks could target critical ECUs or other devices that use security credentials (e.g. for V2X communications).	- Vehicle sensors and actuators - Functions - Software and licenses - Information - In-vehicle communication networks
	Fault injection	Fault injection threats consist in disrupting the computational operations of a security mechanism (e.g. skipping a password verification) to bypass security mechanisms. Such attacks generally require a physical access to the targeted device, but some of them (e.g. Rowhammer attacks) can be performed remotely. They would mainly target critical ECUs.	- Vehicle sensors and actuators - Functions - Software and licenses - Information - In-vehicle communication networks
Failures / Malfunctions (Car sensors and actuators **Car ECUs, processing**	Failure or malfunction of a sensor/actuator	This threat impacts the proper functioning of a sensor and/or actuator. It may accidentally happen (e.g. as a result of improper use or maintenance). It may also be intentional through software vulnerabilities (e.g. ability to spread a malware on ECUs).	- Vehicle sensors and actuators - Functions - Software and licenses

Threat Category	Threat	Description	Impacted Assets
and decision making components)			- Information - In-vehicle communication networks - In-vehicle communication components - Decision making algorithms - Humans
	Software vulnerabilities exploitation	Threats leveraging the use of outdated software versions, bugs, improper configurations, zero-day vulnerabilities or specific software components such as weak cryptographic algorithms or vulnerable open source libraries. Unsecure OTA updates might also be exploited in order to spread a malware or perform software downgrade to a version with known vulnerabilities.	All assets
	Failure or Disruption of service	This threat targets OEM services and/or third party services in order to limit the car features, or disrupt smart cars' operations. It could be done by different means (e.g. DDoS attack, malicious software updates).	- Decision making algorithms - Functions - Software and licenses - External communication components - Servers, systems and cloud computing - Information - Humans - Mobile devices
Eavesdropping /Interception /Hijacking	Communication protocol hijacking	Cyberattacks that exploit flaws in communication protocols so as to perform impersonation attacks (e.g. rogue BTS attack due to a lack of authentication), replay attacks (e.g. performing an ECU software downgrade), or more generally the injection of malicious packets, the interception of information or the disruption of communications. Such threats may lead to	All assets

Threat Category	Threat	Description	Impacted Assets
		the disclosure of sensitive and/or private information, including passwords.	
	Data replay	Cyberattack that exploits data replay techniques. Such attack can occur at the protocol level (e.g. lack of timestamp and/or authentication) but also at the sensor level (e.g. use a repeater to create a ghost vehicle).	-Decision making algorithms -Functions -External communication components -In-vehicle communication networks -In-vehicle communication components - Servers, systems and cloud computing -Information -Humans
	Man-in-the-middle attack / Session hijacking	Man-In-The-Middle (MITM) attacks exploit the lack of authentication to disrupt the communications between legitimate entities or to disclose/modify exchanged information (e.g. provide fake information to RSUs to affect traffic conditions). They apply to both in-vehicle and V2X communications.	All assets
Unintentional Damages (accidental) (In-vehicle communication components)	Unintentional change of data or car components configuration	Unintentional modification of configuration or data by a legitimate entity leading to potential vulnerabilities. It can arise from the misconfiguration of an equipment (e.g. by mechanics or OEM staff during maintenance) or simply because defined security procedures were not followed.	All assets
	Information leakage	This may typically concern administration errors in back-end services or errors when storing data intended for diagnostic in garages, for example.	- Information - Humans
	Using information and/or devices from an unreliable source	Unintentional damages may cascade from ill-defined trust relationships: for example, trusting a third-party cloud provider with poor data protection, or failing to notify a Tier developer that the data they will store is sensitive.	All assets

Threat Category	Threat	Description	Impacted Assets
	Erroneous use or configuration of car components	Unintentional damage to car components (e.g. cameras or autonomous sensors) due to an erroneous use or misconfiguration by a smart cars' users, insufficiently trained OEM staff members (e.g. incompatibilities between components), mechanics (e.g. when using diagnostic equipment), or lack of adaptation to the changing threat landscape (the use of vulnerable cryptography is an example of this).	-Vehicle sensors and actuators - Decision making algorithms - Functions - In-vehicle communication components - In-vehicle communication networks - Information - Humans - Mobile devices
Outages (Smart cars Infrastructure and Backend systems)	Loss of GNSS signal	GNSS jamming[74] that may be either performed by the smart car legitimate user (e.g. to fraud GNSS tolls, avoid tracking mechanisms) or by an external attacker aiming to disrupt the proper functioning of the vehicle.	- Decision making algorithms - External communication components - Servers, systems and cloud computing - Information - Humans - Mobile devices
	Car depleted battery	This threat aims to partially or completely drain the smart car battery (e.g. through the use of a malware). The attacker's goal is to decrease the overall performance of a car, or immobilize it.	- Functions - Humans - Mobile devices
	Network outage	This threat aims to bring down internal (e.g. CAN bus) and/or external (e.g. C-V2X) networks so that the vehicle cannot operate normally. Such attacks can arise from improper configurations (e.g. CAN bus overload due to multiple applications accessing data at the same time) or from targeted attacks (e.g. DDoS).	All assets

[74] See "Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems": https://tlpc.colorado.edu/wp-content/uploads/2016/11/2016.11.21-Autonomous-Vehicle-Jamming-and-Spoofing-Comment-Final.pdf

Threat Category	Threat	Description	Impacted Assets
Legal	Failure to meet contractual requirements	Breach of contractual requirements by Tier 1 and/or Tier 2 car components or software suppliers. Such threat may lead to financial, safety, privacy and/or operational impacts.	All assets
	Violation of rules and regulations/Breach of legislation/ Abuse of personal data	Lack of compliance with international or European regulations and laws (e.g. GDPR and UNECE regulations). Such threat may have an impact on users' privacy (e.g. disclosure of user's personal information) or road users' safety (e.g. no eCall feature). In particular, the abuse of personal data consists in compromising sensitive and private data (e.g. authentication credentials, name and address, daily commutes) stored in the smart cars or in OEM/service providers backend servers. The attacker's main goal is to retrieve individuals' private information in order to sell it, or even use it for another attack vector (e.g. social engineering, phishing).	All assets

ANNEX C: SECURITY MEASURES MAPPING

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Security by design	**Adopt a Security by Design Approach.** Treat automotive cybersecurity as a cycle, and not as a one-off process. Take into consideration cybersecurity aspects in any activity of the development of the solution from the very beginning. Adopt security by design approach both from the vehicle as well as from the infrastructure perspective. In particular, the secure design should demonstrate how the vehicle security covers the threats identified in the risk assessment. Design should also take into account cybersecurity key principles such as defence in depth, principle of least privilege, disabling of test/debug features and ports, etc. Regarding critical services, more resilient/advanced solutions, such as hardware-supported Trusted Computing Base (TCB), may be used.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles: Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -US Department of Transportation - Cybersecurity Best Practices for Modern Vehicles -SCOUT - Report on the state of the art of connected and automated driving in Europe -PAS 1885:2018 The fundamental principles of automotive cyber security specification, bsi

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Security by design	**Address security in relevant specification documents.** In each design document, include a chapter that addresses the security of all information and control systems in the smart vehicle and the corresponding infrastructure. This ensures that security aspects are considered from the very begining of the concept phase, and not as an afterthought.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles: Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines - Overview Document -US Department of Transportation - Cybersecurity Best Practices for Modern Vehicles -SCOUT - Report on the state of the art of connected and automated driving in Europe
Security by design	**Promote the use of DevSecOps methodology.** The DevSecOps process aims at merging the security discipline within DevOps, thus considering security in every stage of the development process. By having security and development teams working together early in the development lifecycle, security naturally finds itself in the product by design.	All	-Autonomous DevSecOps: Five Steps to a Self-Driving Cloud (ENT214-S) - AWS re:Invent 2018 -Redhat DevSecOps -What is DevSecOps? Developing more secure applications -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Security by design	**Consider including a security role within the product engineering team.** Bring Information Technology (IT) / Operational Technology (OT) people, including people in charge of security topics, together in all phases. Making security an equal consideration alongside	All	-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification -Autonomous DevSecOps: Five Steps to a Self-Driving Cloud (ENT214-S) - AWS re:Invent 2018 -Security Champions Playbook -Avoid Unnecessary Pain with a Security Champion

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	development and operations is a must for any stakeholder of the supply chain.		
Privacy by design	**Consider applying privacy regulations.** OEMs and all third parties should address privacy related issues based on applicable local and international regulations such as the GDPR. To meet privacy-related regulatory requirements, several privacy-preserving rules should be followed such as defining the purpose of private data processing, only collecting a minimal amount of personal data and avoid collecting private data if they are not necessary. Privacy protection accountability aspects should be taken into account, enabling OEMs, Tier 1 and Tier 2 to demonstrate the implemented measures and their effectiveness.	• Legal	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -SCOUT - Report on the state of the art of connected and automated driving in Europe -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Privacy by design	**Conduct PIA.** Autonomous vehicles may collect private information about the owner and/or passengers of the vehicle for a variety of purposes (e.g. authorization, comfort customization, entertainment settings), thus PIA need to be conducted in line with GDPR requirements to identify any potential privacy related risk and define appropriate countermeasures to mitigate it.	• Nefarious activity/abuse • Legal	-GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview -IoT Alliance Australia - Internet of Things Security Guidelines v1.2 -Privacy Impact Assessment -Data Protection Impact Assessment (DPIA)

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Privacy by design	**Perform Privacy Audits.** Perform privacy audits during smart car development and over back-end systems that focus on how individuals' private data are handled, collected, stored and processed, to ensure compliance with privacy-related policies. Privacy audits should be performed on a regular basis, at least once a year or even more frequently depending on PIA.	• Nefarious activity/abuse • Legal	-GSMA (Global System for Mobile Communications) - GSMA CLP.11 IoT Security Guidelines Overview -IoT Alliance Australia - Internet of Things Security Guidelines v1.2 -GDPR: How to Perform a Data Audit -GDPR checklist for data controllers
Asset management	**Use tools supporting asset management.** Asset management systems should be robust. Used asset management tools should be able to dynamically discover, identify and enumerate assets specific to the organization and smart cars ecosystem.	• Nefarious activity/abuse • Hijacking • Failures/Malfunctions	-Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance Cloud Security Alliance - Security Guidance for Early Adopters of the - Internet of Things -IEC - IEC 62443-3-3:2013 System security requirements and security levels -ISO - ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems -- Requirements -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Asset management	**Ensure that there exists a consistent and up-to-date asset inventory.** This inventory should include, among others, current firmware/operation system (OS) version, used hardware, supported communication protocols, etc. Asset inventory should also include gathered known vulnerabilities related to particular assets. The responsibility for maintaining an up-to-date asset inventory should be clearly defined and assigned to the system owner.	• Nefarious activity/abuse • Hijacking • Failures/Malfunctions • Physical attacks	-Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -Huawei - IoT Security White Paper 2017 -IEC - IEC 62443-3-3:2013 System security requirements and security levels -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Asset management	**Introduce a new device or software change into the vehicle only according to an established, accepted and communicated change management process.** Do not allow any changes or introduction of a new device or software unless designated approvals are received. Approved changes should be documented and the relevant documentation updated. Emergency changes may be carried out based on a verbal approval from the Change Management Committee Head and the system owner. However, post emergency, the standard procedure for documenting the change and risk analysis is to be applied.	• Nefarious activity/abuse • Hijacking • Unintentional damages • Physical attacks	-IEC - IEC 62443-3-3:2013 System security requirements and security levels -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -LNS - Putting Industrial Cyber Security at the top of the CEO agenda -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Risk and Threat management	**Adopt an approach to risk management dedicated to the automotive sector.** The approach to risk management should consider new parameters, threats and attack scenarios targeting smart cars ecosystem, and cover all interdependencies between cyber-physical scenarios, cyber-physical environmental and safety during the assessment phase.	All	-ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -PAS 1885:2018 The fundamental principles of automotive cyber security – Specification
Risk and Threat management	**Risk and threat analysis.** Perform risk and threat analysis involving cybersecurity experts from the very early stages of the design process of the vehicle to identify critical assets as well as security risks and associated mitigations. Cybersecurity risks targeting smart cars should be assessed and prioritized to establish efficient security measures. Risk and threat analysis should be revisited at least annually, and upon any major change or in case of critical security vulnerabilities detection or critical security incidents.	All	-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources -US Department of Transportation - Cybersecurity Best Practices for Modern Vehicles - ETSI TR 102 893: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Risk and Threat management	**Monitor security vulnerabilities.** Once a vehicle is on the market, the OEM should consider the monitoring of security vulnerabilities and fix security flaws accordingly. The vulnerabilities monitoring could include developer findings, on-line researches, CSIRTs advisories, as well as input from customers and security researchers. Vulnerabilities monitoring should be regularly performed, for instance every 6 months or even more frequently based on risk assessment.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Safety First for Automated Driving -SCOUT - Report on the state of the art of connected and automated driving in Europe -ENISA - Cyber Security and Resilience of Smart Cars -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Risk and Threat management	**Penetration testing.** Conduct security evaluations (e.g. penetrations tests) during the development phase and then on a regular basis following an event driven approach, e.g. after major updates or in the case of new threats or vulnerability. Such testing should cover all layers of the smart cars. To facilitate evaluations, frameworks for validation and verification from external laboratories should be provided.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -Safety First for Automated Driving -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Risk and Threat management	**Consider defining a threat intelligence process.** Consider incorporating a threat intelligence process within the threat management approach of automotive organisations in order to be informed on emerging attack types and sources, as well as new relevant vulnerabilities.	All	-Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary -Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -GSMA (Global System for Mobile Communications) - GSMA CLP.14 IoT Security Guidelines for Network Operators -Huawei - IoT Security White Paper 2017

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	Organizations should rely on various sources of information (e.g. other OEMs, specilized entities, CWE and CVE common sources, etc.) and share information with trusted industry partners, ISACs and CSIRTs. Determine the impact of threats detected through the threat intelligence process by performing a risk analysis.		-IIC (Industrial Internet Consortium) - IoT Security Maturity Model: Description and Intended Use -International Telecommunications Union - Security capabilities supporting safety of the Internet of things -NIST - NIST SP 800 30r1 - Guide for Conducting Risk Assessments -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Risk and Threat management	**Regularly assess the security controls and patch vulnerabilities.** Smart cars actors should define appropriate assessment procedures to regularly check, at least once a year or more frequently based on risk assessment or patch deployment, the effectiveness of their security measures, and patch them whenever needed. Patches should be tested before deployment.	All	-ENISA - Cyber Security and Resilience of smart cars -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Five Star Automotive Cyber Safety Program -Securing the Modern Vehicle -Security Development Lifecycle (SDL) -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Risk and Threat management	**Regularly check the security assumptions over smart cars lifecycle.** Assumptions are made to ensure that the security requirements are sufficient based on risk and threat analysis. These assumptions include, but are not limited to, operational environment assumptions, limitations in the usage of the vehicle, assumed properties of cryptographic schemes, etc. Vendors and users should be encouraged to regularly check, for	All	-ENISA - Cyber Security and Resilience of smart cars -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Five Star Automotive Cyber Safety Program -Securing the Modern Vehicle

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	instance every 6 months or even more frequently based on risk assessment, that these assumptions are still valid over smart cars lifecycle. Security assumptions need to be updated according to significant systems changes/updates, support of new technologies and/or communication mechanisms/technologies, etc. In particular, a procedure for communication and handling of end of life/out of warranty status for cybersecurity may be defined.		
Relationships with suppliers	**Foster security-related information sharing between the different stakeholders while protecting intellectual property.** Suppliers and service providers should provide evidences about the implementation of their cybersecurity management system to a vehicle manufacturer, as stated in UNECE regulation. For transparency purposes, OEMs should consider providing similar evidences to their suppliers and service providers as well.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -COLLABORATION AND ENGAGEMENT WITH APPROPRIATE THIRD PARTIES -Auto ISAC - Automotive Cybersecurity Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Relationships with suppliers	**Define cybersecurity relevant aspects of the partnerships along the supply chain, and develop security requirements and procurement guidelines for suppliers.**	• Nefarious activity/abuse • Failures/Malfunction • Unintentional damages	-Auto ISAC - Automotive Cybersecurity Best Practices -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -European Commission -- Access to In-vehicle Data and Resources

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	To prevent security risks and threats that may stem from outsourced services or components/systems provided by third party suppliers, organisations should define procurement guidelines as well as security requirements to be applied to their third parties suppliers. A security SLA may also be established between the organisation and its supplier to define the security level that the the supplier should meet.		-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Training and awareness	**Information sharing between different actors.** All organisations, including sub-contractors, suppliers and third parties should work together to enhance the security of smart cars. Organisations should consider communicating with other companies on a sector level including the supply chain and participate in international security events and working groups formed to enable discussion, cooperation and intelligence sharing across organisations to improve security awareness.	All	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -European Commission -- Access to In-vehicle Data and Resources - Auto ISAC - Automotive Cybersecurity Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Training and awareness	**Adopt a holistic approach to security training and awareness among the employees, including employees on all levels of the organization.** Security training should cover smart cars relevant threats and be tailored to the employees' roles and responsibilities and the different	• Nefarious activity / Abuse • Unintentional damages	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	level of knowledge of the participants. For instance, all newly hired employees and employees that change responsibilities should be provided with an appropriate cybersecurity training when starting their new job.		Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -World Economic Forum - Industrial Internet of Things: Unleashing the Potential of Connected Products and Services -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Training and awareness	**Ensure that security trainings are continuous, regular and frequently updated.** Training programs should be updated after new important threats disclosure and adjusted according to the lessons learned from ongoing incident handling and recovery activities.	• Nefarious activity / Abuse • Unintentional damages	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Training and awareness	**Raise vehicle users' awareness.** Vendors and public authorities should explain to vehicle owners, drivers and passengers which actions can contribute to mitigate potential threats, such as how to securely use interfaced systems such as smartphones and onboard tablets,	• Nefarious activity / Abuse • Unintentional damages	-ENISA - Cybersecurity and resilience of smart cars -Insecurity in the Internet of Thing -IoT Security Awareness -Consumers don't care if their connected car can get hacked - here's why that's a problem

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	basic security best practices, etc. This should be done on a regular basis, especially when significant changes/patches occur or when new threats emerge.		-Shifting gears in cyber security for connected cars
Security management	**Consider establishing a Security Operation Center (SOC).** Consider the creation of a SOC consisting of OT and IT cybersecurity specialists with clearly defined roles, responsibilities and cybersecurity competences to centralize knowledge on cybersecurity, monitor and anticipate potential threats by ensuring that potential security incidents are correctly identified, investigated and reported. Managing and acting upon the growing number of security alerts can become very complex, especially for large fleets. Therefore, a robust SOC is needed to ensure all alerts are analyzed and handled properly.	All	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -Security Operations Center -MITRE :Cybersecurity Operations Center
Security management	**Designate one or several dedicated security team(s).** As dealing with cybersecurity issues requires a very narrow set of skills, actors of the smart car industry should rely on specialists to perform several kinds of activities, notably risk management, secure design, training and awareness, penetration testing and corporate security. Whether this security team(s) should be in-house or a third-	All	-ENISA - Cybersecurity and resilience of smart cars -Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices -30% of Automotive Companies Lacking a Dedicated Cybersecurity Team

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	party company is not indifferent in some cases; in particular, risk management and corporate security require a very good knowledge of the company to be easily outsourced.		
Security management	**Define a dedicated Information Security Management System (ISMS).** Vehicles in the wild cannot be completely protected if the company itself is not able to properly protect critical assets. For example, if vehicles or components have keys injected during production, the risk of leaking these keys may be more important on the company site than on the vehicles side. For this reason, an effective ISMS is of utmost importance. The SAE J3061 describes such an ISMS, and provides references to standards often used for this purpose (ISO 27001 and NIST 800-53).	All	-ENISA - Cybersecurity and resilience of smart cars -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -SAE J3061
Security management	**Consider defining an internal task force involving board-level management to guide security-related strategic decisions.** OEM should consider the definition of an internal task force which should gather on a regular basis, e.g. once every 3 months or more frequently when necessary, to discuss security-related strategic decisions. Board-level management shall be involved in this task force so as to discuss	All	-Avoid Unnecessary Pain with a Security Champion -Security Champions Playbook

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	the different topics and make appropriate decisions. Such approach would help with accountability in case of security incidents.		
Incident management	**Establish an incident handling process**. Establish a process for incidents handling that enables the identification of affected assets, identification and classification of vulnerabilities, escalation and notification. Make a revision of the process at least annually and as soon as possible in case of a major change, e.g. change in organizational hierarchy, contracts, etc. Update the process with lessons learned from analysing and resolving security incidents. Test the process at least annually and consider different possible incidents.	All	-Auto ISAC - Automotive Cybersecurity Best Practices - Executive Summary -Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile -SANS Institute - Vulnerability Management: Tools, Challenges and Best Practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Incident management	**Consider establishing a CSIRT and a PSIRT.** OEMs and third-party suppliers/providers (i.e. Tier 1and Tier 2) should consider building a CSIRT and PSIRT. Working closely with the SOC, the CSIRT and PSIRT ultimate goal is to minimize and control the damage resulting from an incident. They do not only consist in addressing the threat itself,	All	-Cybersecurity Best Practices for Modern Vehicles – NHTSA -CSIRTs in Europe -Cybersecurity Best Practices for Modern Vehicles

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	but also communicate to customers, the organisation board, and public relevant information about the incident.		
Incident management	**Incident Report to back-end servers.** OEMs and third party providers should implement cybersecurity monitoring and reporting to back-end servers to ensure systems are secure over their lifetime. Incident reporting enables the correction of the situation, and through incident analysis and corrective action, similar incidents are avoided.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security
Incident management	**Relevant cyber incidents definition and classification.** Consider defining cybersecurity incidents relevant for your organisation based on the company's area and range of operation and classify them according to applicable standards. By ensuring the distinction between specific attack vectors and methods, the effects such incident may produce on the targeted networks, the financial impacts or their broader effects on society, it will be easier to identify the most critical incidents, prioritise and respond to them in an efficient way.	All	-ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing -Survey and Classification of Automotive Security Attacks – MDPI -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Incident management	**Consider the establishment of a secure and reliable process for detecting and handling misbehaving ITS stations.**	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -PRESERVE - Security Requirements ofVehicle Security Architecture v1.1

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	ITS-S (e.g. vehicle) can misbehave, either unintentionally due a system failure or intentionally as a result of malicious actions, and thus disrupt other vehicles and/or infrastructure. To prevent this, consider the establishment of a process enabling to collect information provided by ITS Stations (e.g. through cooperation between the infrastructure and other vehicles), detect and handle any misbehavior. For instance, the credentials of misbehaving ITS-S may be revoked.		-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -C-ITS Platform, WG5: Security & Certification - Final Report - Annex 2: Revocation of Trust in C-ITS (https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An2_v1.0.pdf)
Detection	**Deploy Intrusion Detection Systems (IDS) at vehicle and back-end levels.** An IDS is a device or software application designed to automatically detect malicious activities or policy violations. An IDS should be able to detect various types of cyber-attacks (e.g. DDoS). To do so, the IDS requires the ability to capture and do a thorough examination of every packet which has been received or transferred between vehicles and infrastructures, as well as packets exchanged over in-vehicle buses. Such systems can rely on artificial neural networks to classify malicious vehicles and sensors and exclude them from communicating with the system.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-PRESERVE - Security Requirements ofVehicle Security Architecture v1.1 -Safety First for Automated Driving -SCOUT - Report on the state of the art of connected and automated driving in Europe
Detection	**Maintain properly protected audit logs.** Security events must be logged, and	• Nefarious activity / Abuse	-ENISA - cybersecurity resilience of smart cars -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	access to the logs must be documented and protected from disclosure to unauthorized users. Logs are also needed for device integration. Typically, Tier-2 suppliers must provide Tier-1 suppliers with the opportunity to understand security events happening in their products. However, logs may also provide valuable information to an attacker, which is a serious security drawback. For this reason, the audit trail must be protected. Since logs can be very resource-intensive and require a large storage space, OEMs should define where to store them (i.e. in the car or on a back-end server) and how long the stored data should be retained.	• Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages • Outages	and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ACEA Principles of Automobile Cybersecurity -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Detection	**Conduct periodic reviews.** Consider periodically reviewing network logs, access control privileges and asset configurations to detect any event that may represent a potential security threat to smart cars ecosystem.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages • Outages	-Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -ENISA - Baseline Security Recommendations for IoT -IEC - IEC 62443-3-3:2013 System security requirements and security levels -IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices -IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -OWASP (Open Web Application Security Project) - IoT Security Guidance

Security Domain	Security Measures/ Good Practices	Threat Groups	References
			-SANS Institute - An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity
Detection	**Perform data validation.** Data validation techniques, such as plausibility checks are non-cryptographic measures which use rules and other mechanisms to determine the correctness likelihood of received data. For instance, AI-based techniques can be used to measure the likelihood of incoming information (e.g. node misbehaviour detection using machine learning based detector, "object existence" metrics) to counter spoofing attacks on V2X communications or malicious alteration of the physical world (e.g. fake speed limit sign).	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-“My autonomous car is an elephant”: A Machine Learning based Detector for Implausible Dimension -Safety First for Automated Driving -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Detection	**Define forensic procedures.** OEMs should define forensics procedures for incident investigation so as to enable events reconstruction, facilitate crash investigation, identify the leveraged weakness and prevent similar attacks, as well as for accountability purposes. Such procedure should follow proven principles to ensure that reconstructed traces are authentic, have not been altered and can be analysed.	• Nefarious activity / Abuse • Failures/Malfunctions • Threats against (semi-) autonomous systems • Unintentional damages • Outages • Legal • Physical attacks	-A survey on open automotive forensics -ENISA - Cyber Security and Resilience of Smart Cars -Log your car: the non-invasive vehicle forensics

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Protection of networks and protocols	**Protect remote monitoring and administration interfaces.** The protection of remote monitoring and administration interfaces is crucial since they often provide a highly-privileged entry point into a device. Thus, monitoring and administration interfaces must not only be protected by whitelisting, but also through mutual authentication and access control mechanisms. This protection includes access control for both the gateway and ECU level and authentication mechanisms.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -AUTOMOTIVE WORKING GROUP
Protection of networks and protocols	**Protect in authenticity and integrity all critical internal communications.** Authentication is essential to prevent spoofing or replay attacks. At the sensor level, authentication mechanims can be used to allow ECUs/TCUs to authenticate each other over the CAN bus before reacting on their commands or sensor data.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources -SCOUT - Report on the state of the art of connected and automated driving in Europe
Protection of networks and protocols	**Protect in authenticity and integrity all external communications.** Authentication is essential to prevent spoofing or replay attacks. Regarding V2V and V2X communications, authentication is crucial to ensure the trustworthiness of incoming/outgoing information.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 -European Commission -- Access to In-vehicle Data and Resources -SCOUT - Report on the state of the art of connected and automated driving in Europe

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Protection of networks and protocols	**Enforce session management policies to avoid session hijacking.** Session management contributes to making sure that the authorized user is the one using a given session. This covers the different communication sessions such as administration sessions. Typically, the following rules should be followed: • Sensitive functions such as administration via web services should require re-authentication. • No data should be transmitted before authorization. • Strong (random) session handlers should be used to avoid replay. • The user must know at any time if, and why, they are logged on a particular service, meaning that no passive sign-up for third party services should be performed.	• Nefarious activity / Abuse • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -OWASP: Session Management Cheat Sheet Session fixation
Protection of networks and protocols	**Timestamp all messages.** Including a timestamp in all messages makes it easier for a receiving ITS-S to judge whether a message is recent, and thus valid (or not). It also prevents replay attacks. If the time is derived from an external source such as Universal Coordinated Time (UTC) or GNSS, it should be	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-PRESERVE - Security Requirements of Vehicle Security Architecture v1.1 -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	ensured that each ITS-S uses the same time source as every other ITS-S. Consequently, it is quite simple for the plausibility of the timestamp in a message to be validated. The use of a precision timing source (e.g. hardware clock source, NTP) to provide accurate time may be considered as well.		
Protection of networks and protocols	**Manage radio spectrum frequencies as well as the frequency of beaconing and other repeated messages.** The use of beaconing messages in V2V/V2X communications and the repetition of some non-beacon messages generates considerable background radio traffic in high-density road-traffic environments. In order to prevent DDoS attacks, consider reducing the frequency of the beacon and other safety-of-life messages in order to reduce congestion. Adaptive frequency control, where messages would be sent at different frequencies depending upon the nature of the message and potentially other local conditions, may be a good alternative as well.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -PRESERVE - Security Requirements of Vehicle Security Architecture v1.1
Protection of networks and protocols	**Implement frequency agility.** A radio transmission broadcast at the same frequency at all times can be easily overwhelmed by a higher-power signal at	• Nefarious activity / Abuse • Hijacking	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	the same frequency. However, it is much more difficult to jam a transmission in which the radio frequency changes frequently within its defined band. If the changes in frequency and the intervals between changes are both determined on pseudo-random basis, it becomes even more difficult to jam the signal. There needs to be synchronization between the legitimate transmitter and the receiver, and both need to use the same algorithms for determining frequency steps and the intervals between changes in frequency.		-CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0
Protection of networks and protocols	**Packet filtering.** Filter communications at each network layer: ECU and sensor networks, VANET, 2-5G communications. During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -SCOUT - Report on the state of the art of connected and automated driving in Europe
Protection of networks and protocols	**Provide end-to-end protection in confidentiality and integrity using secure protocols.** Favor methods providing forward secrecy whenever possible. This should be true even for the communication of already encrypted data; encryption must cover not only external communications (e.g. V2X), but also in-vehicle networks.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -European Commission -- Access to In-vehicle Data and Resources

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Software security	**The default configuration of devices and services should be secured.** The operation mode of the device (or service) should be the most secure one by default. A user might arguably want to disable a given security function, but this should be the consequence of a deliberate action from the user, and the user should be warned that this change reduces the security of the solution. Default passwords and usernames be changed on first use (of the vehicle, service, etc).	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-ENISA - Cyber Security and Resilience of Smart Cars -Secure Device Configuration Guideline -Cybersecurity Best Practices for Modern Vehicles -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Software security	**Software authenticity and integrity checked before installation.** By validating the authenticity and integrity of software it is possible to ensure that only authorized updates and extensions can be downloaded and installed. Mechanisms for restricting the applications that can be installed should be in place. In general, a signature is included over the application package together with a certificate of the signing trusted third party.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Software security	**Implement and document changes in configuration according to a change management policy developed by the organisation based on risk analysis.** This policy should include responsibility (i.e. system owner, approvers, etc.) and	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-IEC - IEC 62443-3-3:2013 System security requirements and security levels -ISA - ANSI/ISA-95 Part 1: Models and Terminology -ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	security aspects. The business owners of assets should approve all changes.		Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile Siemens - Industrial Security: Applying IoT Security Controls on the Industrial Plant Floor
Software security	**Use of secure OTA firmware updates.** OTA updates are essential to patch vulnerabilities identified once vehicles are in the field. They should rely on strong authentication mechanisms (e.g. digital signature) to ensure the authenticity and integrity of the firmware to prevent the installation of rogue firmware and the spread of malwares. Rollback to vulnerable versions should be prevented as well. Encryption is also a good practice to prevent binaries analysis in order to protect the IP and the discovery of zero-day vulnerabilities.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices -Gowling WLG & UK Autodrive - Connected and Autonomous Vehicles: A Hacker's Delight? -SCOUT - Report on the state of the art of connected and automated driving in Europe -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources
Software security	**Protect OTA update process.** Because poorly executed OTA updates can result in malfunctioning vehicles and significant inconvenience to consumers, as well as reputational damage to the OEM, dedicated security measures should be implemented to ensure a secure OTA update process. Access controls to OEM back-end servers as well as recovery measures in case of errors (e.g. reversion	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintenational damages	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices -Gowling WLG & UK Autodrive - Connected and Autonomous Vehicles: A Hacker's Delight? -SCOUT - Report on the state of the art of connected and automated driving in Europe

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	if the OTA image fails to boot successfully) should be considered.		-Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources
Software security	**Use of secure boot mechanisms.** Secure boot is essential to ensure the trustworthiness (i.e. authenticity and integrity) of the executed software. Secure boot mechanisms essentially consist in signing the software with a private key owned by the manufacturer. The signature is verified during the secure boot procedure with the help of the corresponding certificate. If verification fails because the software has been altered, the boot process should react accordingly (e.g. run emergency program to guarantee the functional safety of the vehicle).	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Unintentional damages	-Cybersecurity Solutions for Connected Vehicles -Securing Self-Driving Cars -Safety First for Automated Driving -European Commission -- Access to In-vehicle Data and Resources
Software security	**Mitigate vulnerabilities and limitations of libraries for standard protocols, or address them in risk assessment.** Using an open source security library (e.g. OpenSSL) or proprietary software does not mean that the product will automatically be secure. Developers must be aware of the vulnerabilities (e.g. due to a flawed implementation) and limitations (e.g. vulnerability of the protocol itself) of the used software. They should mitigate	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-ENISA - Cyber Security and Resilience of Smart Cars -Using Open Source for security and privacy protection

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	them whenever possible by performing patching and by securing the configuration of the communication stacks.		
Software security	**Protect mobile applications against reverse engineering and tampering of their binary code.** Code obfuscation techniques may be used to prevent the reverse engineering of smart cars mobile applications. To enable the detection of the tampering of mobile application binary code, mobile applications should be signed. Root detection mechanisms may be implemented as well to check if the device was rooted.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	- OWASP – Mobile Application Security Verification Standard - ENISA – Smartphone Secure Development Guidelines
Software security	**Securely store sensitive data on mobile devices, and protect local files created by the mobile application.** No sensitive data (e.g. passwords, credentials, cryptographic keys etc.) should be stored outside the application container or mobile operating system credential storage facility (e.g. Keystore, Keychain). In particular, no sensitive data should be written in application logs. Access to data stored in the credential storage facility should be limited to authorized users. Local files created by the mobile application should also be protected and deleted when no longer needed.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	- OWASP – Mobile Application Security Verification Standard - ENISA – Smartphone Secure Development Guidelines

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Cloud security	**Include security and availability aspects in agreements with cloud security providers.** Responsibilities for cloud security aspects shall be clearly defined and allocated to particular parties or persons. Availability of service shall be measurable and defined through specified parameters.	• Nefarious activity / Abuse • Outage • Legal	-Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -Online Trust Alliance - IoT trust framework 2.5 -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Cloud security	**Avoid single points of failure.** In the context of cloud-based application and centralised systems, single points of failure should be avoided. Redundancy techniques (e.g. several clusters) and data replication may be used to avoid single points of failure.	• Failures/Malfunctions • Outages	-NIST - NIST SP 800-146 Cloud Computing Synopsis and Recommendations -Online Trust Alliance - IoT trust framework 2.5 -SANS Institute - Building the New Network Security Architecture for the Future -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Cloud security	**Operate critical systems and applications within the private or at least hybrid deployment models.** Privilege the use of a private cloud, or at least a hybrid cloud which combines both private and public cloud. When considering the use of a public cloud, a risk analysis should be performed beforehand.	• Nefarious activity / Abuse • Hijacking • Failure/Malfunctions	-Cloud Security Alliance - Future Proofing the connected world -Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT -Online Trust Alliance - IoT trust framework 2.5 -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Cloud security	**To mitigate the risk related to cloud attacks, adopt a zero-knowledge**	• Nefarious activity / Abuse • Hijacking	-Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	security approach. Cloud services providers should store and manage data without access to the decryption keys. All the data should be protected during transfer as well as when at rest (i.e. stored within the cloud). Ideally, all data should be encrypted to ensure its confidentiality. Application and interfaces should be secured as well.		-IoT Alliance Australia - Internet of Things Security Guidelines v1.2 -ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Cryptography	**Encrypt sensitive data as well as personal and private data.** Sensitive data include, amongst other, data needed to enforce security such as the configuration, different keys and certificates used for several purposes (e.g. encrypt/sign communications), as well as IP-related data. The disclosure of keys and know-how for instance may be prevented through their encryption. Moreover, authenticated encryption may be used to additionally ensure data integrity. Personal and private data covers all pieces of information that can be used to positively identify a vehicle, an ITS user, the location and behavior of a particular vehicle or its route. By encrypting personal and private data it is possible to ensure that traffic analysis and eavesdropping alone cannot reveal	• Nefarious activity/abuse •Eavesdropping/Interception /Hijacking • Legal	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	sufficient information to directly extract or indirectly deduce private information.		
Cryptography	**Do not use proprietary cryptographic schemes and protocols, but rather state-of-the-art standards instead.** Even a home-brewed implementation of a standard is not a good practice when standard implementations are available. If needed, consider getting advice from security experts or your national cybersecurity agency. This applies also to random number generation which is a critical part of the cryptographic support. A possible recommendation would be the use of cryptographically secure pseudorandom number generators.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages	-ENISA - Cyber Security and Resilience of smart cars -European Commission -- Access to In-vehicle Data and Resources
Cryptography	**Use storage encryption.** Encrypted storage is not only useful to protect user data, but also to protect data that is needed to enforce smart cars security. Internal data may be just as sensitive as user data, but are often not protected enough, leading for example, to situations where hardcoded root credentials, API keys, URLs never meant to be known to end-users, and manufacturing network configurations are found in cleartext and may be disclosed to unauthorised entities. As a general rule, configuration data should be encrypted at rest and in transit.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Legal	-ENISA - Cyber Security and Resilience of smart cars Safety First for Automated Driving -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Cryptography	**Implement a secure key management process.** Cryptographic keys should be securely generated, provisioned, used, stored, and deleted/revoked. Badly implemented key management can introduce vulnerabilities that may easily be exploited. Devices without direct user interfaces are particularly vulnerable to PKI compromising. While users can easily delete or install certificates on a PC, embedded devices (e.g. ECUs) rely mostly on remote administration, and do not even allow end-users to perform such administration tasks. For this reason, OEMs as well as Tier-1/Tier-2 should pay careful attention to the key management system, especially when the key provisioning and management are performed over-the-air. If needed, consider getting advice from security experts or your national cybersecurity agency.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintentional damages	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -European Commission -- Access to In-vehicle Data and Resources -SCOUT - Report on the state of the art of connected and automated driving in Europe European Commission - Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport System (C-ITS)
Cryptography	**Consider using dedicated and tamper resistant hardware security modules.** HW-based cryptographic solutions may help avoid the incorrect implementation of cryptographic algorithms by software vendors, as well as the coexistence of multiple implementations of the same algorithms. They eventually provide implementations that are more resource-	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-Safety First for Automated Driving -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -European Commission -- Access to In-vehicle Data and Resources

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	efficient. Choosing HW accelerated cryptography means that a reasonable assurance must be obtained on the quality of the HW implementation, since “bad cryptography” on HW will be leveraged on all the SW using these functions. Devices vendors should be aware of tamper evident or tamper-resistant mechanisms. While they are not mandated in any case, vendors should consider using them depending on the level of sensitivity of the assets stored on the device. In particular, even constrained devices could be able to implement some kind of tamper evidence, even if they are not able to implement resistance and response.		-SCOUT - Report on the state of the art of connected and automated driving in Europe
Access Control	**Application of security controls to back-end servers.** Such controls have to be at different levels: • physical (e.g. physical and environmental security) • logical (e.g. secure configuration using system hardening, firewalls) • people (e.g. security training for OEMs staff)	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks	-UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -Secure Device Configuration Guideline -IoT Security Awareness -Consumers don't care if their connected car can get hacked - here's why that's a problem -Shifting gears in cyber security for connected cars -What is physical security? How to keep your facilities and devices safe from on-site attackers

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Access Control	**Apply least privileges principle and use individual accounts to access devices and systems.** Ensure that roles (e.g. user, administrator, etc.) are clearly defined and that access rights are provided following a need-to-know/access and least-privilege principles. A distinct account should be created for each user for accountability reasons (i.e. track performed actions).	• Nefarious activity / Abuse • Eavesdropping/ Interception/ Hijacking • Unintenational damages • Physical attack	-Principle of least privilege (POLP) -Improving security through least-privilege practices -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Access Control	**Segregate remote access.** Develop a set of rules for control of remote communication. Remote access should be only limited to the required systems, and must be monitored.	• Nefarious activity / Abuse • Eavesdropping/ Interception/ Hijacking • Unintentional damages • Failures/Malfunctions	-GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - Draft NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks -OWASP (Open Web Application Security Project) - IoT Security Guidance -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Access Control	**Allow and encourage the use of strong authentication mechanisms.** Rely on Multi-factor authentication (MFA) mechanisms which require users to provide at least two different proofs of the claimed identity (e.g. password and security token) so as to be authenticated	• Nefarious activity / Abuse • Eavesdropping/ Interception/ Hijacking • Physical attacks	-Cloud Security Alliance - Identity and Access Management for the Internet of Things - Summary Guidance -ENISA - Baseline Security Recommendations for IoT -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	and granted access to the resource or service (e.g. authentication to cloud services or mobile interfaces, local/remote administration sessions). This mitigates the risks associated with passwords-only authentication. An account lockout functionality should be implemented to automatically lockout an account for a given time period after a number of successive authentication failures.		-IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -OWASP (Open Web Application Security Project) - IoT Security Guidance
Self protection and resilience	**Implement differential monitoring on the GNSS system.** Differential GNSS is a way of correcting various inaccuracies in a GNSS system and, thus, providing more accurate position information. The benefit of differential GNSS is that it is capable of positioning things very precisely and this feature can be used to detect even small anomalies in position errors.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis - Autonomous integrity monitoring of navigation maps on board intelligent vehicles

Security Domain	Security Measures/ Good Practices	Threat Groups	References
Self protection and resilience	**Perform hardening to reduce the attack surface.** Remove unused services or interfaces, integrate dedicated security software, activate memory or control flow protections. For devices that have a complete operating system, several measures can be considered to harden the device, such as ASLR, non-executable memory, process segregation or sandboxing. Another measure is removing unused tools, services and libraries. Unnecessary services should not be present on the device (typically telnet must always be deactivated, but even SSH or FTP can be deactivated in many cases). This type of measures is also applicable at a network level: the device should not leave open ports, especially ports that could be exposed via plug-n-play protocols. The default configuration of the device should be based upon the most secure parameters, and users should be warned if they have the possibility to roll back to less secure parameters.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Physical attacks • Unintenational damages	-Cloud Security Alliance - Identity and Access Management for the I+E68nternet of Things - Summary Guidance -ENISA - Baseline Security Recommendations for IoT -GSMA (Global System for Mobile Communications) - GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystems -GSMA (Global System for Mobile Communications) - GSMA CLP.13 IoT Security Guidelines for Endpoint Ecosystems -IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -OWASP (Open Web Application Security Project) - IoT Security Guidance
Self protection and resilience	**Reinforce interfaces robustness.** Software can contribute to self-protection measures, such as for robustness of interfaces against bad inputs. Secure implementation, thoroughly tested, will protect against common attack	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -Symantec - Insecurity in the Internet of Things -OWASP Internet of Things Project – OWASP- -OWASP Top Ten Project – OWASP

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	vectors such as buffer/heap overflows or OWASP's Top Ten Web Vulnerabilities. This typically includes robustness of network interfaces against buffer overflows or fuzzing.		-PAS 1885:2018 The fundamental principles of automotive cyber security - Specification
Self protection and resilience	**Consider strengthening applications isolation at runtime.** Trusted software technologies, such as Trusted Execution Environments (TEEs), hypervisors and virtualisation, may be used to ensure secure execution of applications in a segregated and trusted environment.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-ENISA - Cyber Security and Resilience of smart cars -Symantec - Insecurity in the Internet of Things -Secure hypervisor versus trusted execution environment -Isolated Execution in Many-core Architectures
Self protection and resilience	**System, sub-domain and network segregation.** Use of logical and physical isolation techniques to separate processors (e.g. OS virtualization techniques, hypervisors), vehicle domains and networks (e.g. use of an in-vehicle gateway for physical separation between safety and non-safety related domains), and external connections (e.g. firewall to filter all the incomming traffic received from outside the vehicle). These techniques should be used where appropriate (based on risk assessment) to limit and control pathways from external threat vectors to cyber-physical features of vehicles, as well as ensure suitable separation of in-vehicle systems.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking	-U.S. Department of Transportation - Cybersecurity Best Practices for Modern Vehicles -UNECE- ECE/TRANS/WP.29/GRVA/2019/2 -- Automated/autonomous and connected vehicles:Cyber security and data protection -- Proposal for a Recommendation on Cyber Security -European Commission -- Access to In-vehicle Data and Resources -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
(semi-) Autonomous systems self protection and cyber resilience	**Consider using INS or existing dead-reckoning methods to provide positional data.** In order to have other source of location information in the case of GNSS failure, consider the use of an onboard Inertial Navigation System (INS) or dead-reckoning derived from simple accelerometers such as those found in modern mobile phones. Thus, it would be possible for the ITS-S to determine its position from purely internal sources with only brief and infrequent references to GNSS for waypoint corrections. Such security measure would prevent GNSS jamming and other related attacks.	• Nefarious activity / Abuse • Failures/Malfunctions • Hijacking • Outages • Threats against (semi-) autonomous systems	-ETSI - ETSI TR 102 893 V1.2.1 -- Intelligent Transport Systems: Security, Threat, Vulnerability and Risk Analysis -An Autonomous Vehicle Navigation System Based on Inertial and Visual Sensors
(semi-) Autonomous systems self protection and cyber resilience	**Protect critical sensors in order to prevent attacks that may alter their perception of the environment.** The protection mechanisms are specific to each sensor type, and mainly depends on the type of threats targeting the sensor. For instance, Integration of near-infrared-cut filters or photocromic lenses on cameras could filter specific types of light to mitigate sensor blindness attacks. Regarding LiDARs, the emission of light pulse could be done in an unpredictable manner (e.g. pseudo-randomly) so that it will be harder for an attacker to inject a fake echoe in the right window.	• Physical attack • Nefarious activity/abuse • Outage • Threats against (semi-) autonomous features/components	-Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR -SCOUT - Report on the state of the art of connected and automated driving in Europe -PAS 1885:2018 The fundamental principles of automotive cyber security - Specification

Security Domain	Security Measures/ Good Practices	Threat Groups	References
(semi-) Autonomous systems self protection and cyber resilience	**Hardening against Adversarial Machine Learning.** Protect Artificial Intelligence (AI) and Machine Learning (ML) components in order to prevent them from being tricked by adversarial attacks. The model need to be hardened by using, for instance, adversarial data as part of algorithm training, to make the model more robust with regard to adversarial attacks. Pre-processing techniques may also be used as a protection mechanism.	• Threats against (semi-) autonomous systems	-Towards deep learning models resistant to adversarial attacks (https://openreview.net/pdf?id=rJzIBfZAb) -Explaining and harnessing adversarial examples (http://arxiv.org/abs/1412.6572). -Pixeldefend: Leveraging generative models to understand and defend against adversarial examples. In International Conference on Learning Representations (ICLR),2018 (https://openreview.net/forum?id=rJUYGxbCW) -The robust manifold defense: Adversarial training using generative models. (https://arxiv.org/abs/1712.09196). -Thermometer encoding: One hot way to resist adversarial examples. In International Conference on Learning Representations (ICLR), 2018
(semi-) Autonomous systems self protection and cyber resilience	**Prevent data falsification/manipulation in regard to Artificial Intelligence (AI)/Machine Learning (ML).** Ensure that data used to train the model are originating from a trusted entity. After any training cycle, the model should be tested to ensure that there are no considerable changes in classifications for instance.	• Threats against (semi-) autonomous systems	-The robust manifold defense: Adversarial training using generative models. (https://arxiv.org/abs/1712.09196). -Securing the Future of AI and ML
(semi-) Autonomous systems self protection and cyber resilience	**Use of data redundancy mechanisms.** Data redundancy mechanisms (e.g. sensor data fusion) consist in correlating data acquired from different sensors (e.g. LiDAR and camera) and V2X communications so as to allow the mitigation of the physical or DoS attacks against sensors.	• Physical attack • Nefarious activity/abuse • Outage • Threats against (semi-) autonomous systems	-Groupe PSA - Attacker model for Connected and Automated Vehicles Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR -SCOUT - Report on the state of the art of connected and automated driving in Europe -Safety First for Automated Driving

Security Domain	Security Measures/ Good Practices	Threat Groups	References
(semi-) Autonomous systems self protection and cyber resilience	**Use of hardware redundancy mechanisms.** Hardware redundancy mechanisms consist in duplicating sensors (e.g. several cameras, several sensors to collect the same data) in order to mitigate physical attacks or DoS attacks against sensors.	• Physical attack • Nefarious activity/abuse • Outage • Threats against (semi-) autonomous systems	-Groupe PSA - Attacker model for Connected and Automated Vehicles Security Innovation - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR -SCOUT - Report on the state of the art of connected and automated driving in Europe -Safety First for Automated Driving
Continuity of operations	**Notifications should be easy to understand and help users find a remediation or workaround.** HW and embedded systems should provide clear error data that can be leveraged upon by the SW vendors. The user must be notified in case of security errors, updates or compromised data in a device or service they use. In particular, users must be notified in the case of security events. Notification might vary greatly depending on the type of software considered. Mobile applications notification, messaging such as SMS or e-mail, hardware interfaces such as LEDs, dedicated error messages to a gateway, etc.	• Nefarious activity / Abuse • Failures/Malfunctions • Unintentional damages	-ENISA - Cyber Security and Resilience of smart cars -Duo Security - The Internet of Fails ; Where IoT Has Gone Wrong -A Hard Problem with No Easy Answers | Decipher - IoT Security
Continuity of operations	**Create a Business Continuity Plan (BCP) and a Business Recovery Plan to ensure the resilience of smart cars systems.** To ensure business continuity (even in the case of security crisis or disaster situations), a Business Continuity	• Failures/Malfunctions • Unintentional damages	-Center for Internet Security (CIS) - Critical Security Controls -Federal Office for Information Security (BSI) - BSI-Standards 100-4 - Business Continuity Management -IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program

Security Domain	Security Measures/ Good Practices	Threat Groups	References
	Plan (BCP) and a Business Recovery Plan that cover third party aspects should be created and periodically tested, at least annually, to ensure their effectiveness and improve them when required. Appropriate Third Party management and control over its involvement is essential to ensure the continuity of operations of the organisation.		-NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations -NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security -NIST - NISTIR 8183: Cybersecurity Framework Manufacturing Profile
Continuity of operations	**Define Business Continuity parameters.** Define important parameters for business continuity of the organization, such as the recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO).	All	-IEC - IEC 62443-3-3:2013 System security requirements and security levels -IIC (Industrial Internet Consortium) - IIC Endpoint Security Best Practices -IoT Security Foundation - Connected Consumer Products. Best Practice Guidelines -oneM2M - Standards for M2M and the Internet of Things - TR 0008 Security V2.0.0 - Security. Technical Report

TP-02-19-881-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-317-9
DOI: 10.2824/17802