IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D5.4.2
Identity, Security and Safety in Product Lifecycle Data Management

The IoT4CPS Consortium:
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

For more information on this document or the IoT4CPS project, please contact:
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Document Control

Title: Identity, Security and Safety in Product Lifecycle Data Management
Type: public
Editor(s): Violeta Damjanovic-Behrendt
E-mail: violeta.damjanovic@salzburgresearch.at
Author(s): Violeta Damjanovic-Behrendt, Leo Happ Bottler, Konrad Diwold, Kay Uwe Römer
Doc ID: D5.4.2

Amendment History

Version	Date	Author	Description/Comments
V0.1	10.04.2020	Violeta Damjanovic-Behrendt	Document organization
V0.2	30.04.2020	Violeta Damjanovic-Behrendt	The document version sent out to the partners
V0.3	20.05.2020	Leo Happ Bottler, Konrad Diwold, Kay Uwe Römer (TUG-ITI)	Added: Section on “Localization as a pillar for safety”; Section “Relation to WP3”.
V0.4	28.05.2020	Kai Nahrgang, Heribert Vallant (JR)	Added: Section on „Relevant Security and Safety Threats”
V0.5	29.05.2020	Violeta Damjanovic-Behrendt	Added: Section on “Safety and Privacy Analysis of Two Automated Mobility Use Cases”
V0.6	04.06.2020	Violeta Damjanovic-Behrendt	Added: Section on “Trust and Ethics in Connected and Automated Mobility Applications”
V0.7	10.06.2020	Violeta Damjanovic-Behrendt	The report sent out for QA
V0.8	14.07.2020	Philipe Reinisch, Heinz Weiskirchner	QA comments received
V0.9	06.08.2020	Mario Drobics	QA comments received
V1.0	06.09.2020	Violeta Damjanovic-Behrendt	Final version of the report

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

FFG
Forschung wirkt.

Content

Abbreviations

ABS	Anti-lock Braking System
ADAS	Advanced Driver Assistance System
ADS	Automated Driving Systems
AI	Artificial Intelligence
AoA	Angle of Arrival
BLE	Bluetooth Low Energy
CAD	Computer Aided Design
CAM	Connected and Automotive Mobility
CAN	Controller Area Network
CC	Cyclomatic Complexity
CIM	Computer Integrated Manufacturing
CITS	Cooperative Intelligent Transport System
CPS	Cyber Physical System
CSRF	Cross-Site Request Forgery
CTI	Cybersecurity Threat Intelligence
CySiVuS	Cybersecurity for Transport Infrastructure and Road Operators
DDoS	Distributed Denial of Service
DIF	Decentralized Identity Foundation
DPIA	Data Privacy Impact Assessment
ECU	Engine Control Unit
FP	First Path
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite Systems
HIDS	Host-based Intrusion Detection System
IDM	Identity Management
IDP	Identity Provider
IoT	Internet of Things
IoV	Internet of Vehicle
ITS	Intelligent Transport Systems
LOC	Lines of Code
LOS	Line-Of-Sight
ML	Machine Learning
NASAMDP	NASA Metric Data Program
NIST	National Institute for Standards and Technology
NLOS	Non-Line-Of-Sight
NREN	National Research and Education Networks
OBD	OnBoard Diagnostics
PAT	Pangea Arbitration Token
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PLCDM	Product LifeCycle Data Management
RX	Receive
SAML	Security Assertion Markup Language
SFC	Software Fault Prediction
SP	Service Provider

SPI	Sensitive Personal Information
SSO	Single Sign-On
SVM	Support Vector Machine
ToF	Time of Flight
TX	Transmit
UWB	Ultra WideBand
V2C	Vehicle-to-Cloud
V2E	Vehicle-to-Everything
V2H	Vehicle-to-Home
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
XML	eXtensible Markup Language
XSRF	Cross-Site Request Forgery

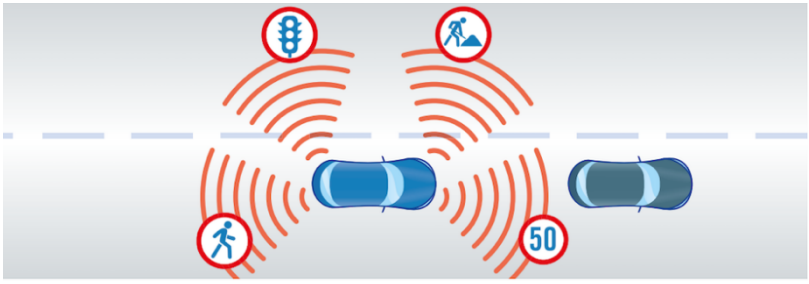
Executive Summary

This report is the successor of the D5.4.1 report that is published in M18 of the project duration. D5.4.1 captures identity and security aspects of two automotive driving scenarios and extends the model created in **D5.2 "Product Lifecycle Data Management (PLCDM) Stakeholder Perspectives"** by adding a set of security threats defined in Work Package WP4 "Security Verification and Analysis" of IoT4CPS. The extended model ensures the inclusion of both multi-stakeholder and IoT-/ CPS-based assets (and their services) along lifecycle phases of connected car scenarios and adds the cybersecurity perspective to it. In this report, D5.4.2, an additional safety and privacy analysis of Connected and Automotive Mobility (CAM) use cases (defined in D5.4.1) is provided. In addition, D5.4.2 includes the localisation techniques for safety and also addresses trust and ethics in CAM applications.

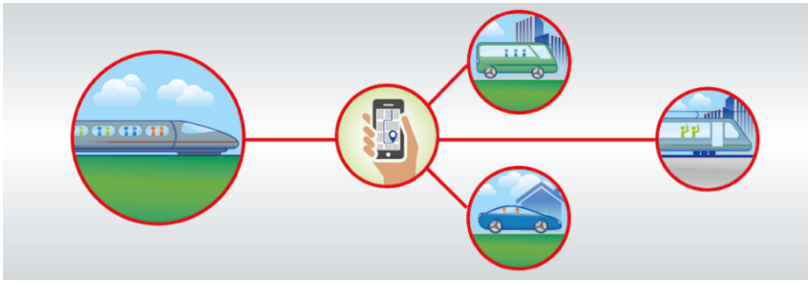
1. Introduction

The focus of the predecessor report **D5.4.1 "Identity, Security and Safety in Product Lifecycle Data Management"** is on identity and security aspects of the two Connected and Automotive Mobility (CAM) scenarios combining the Device.CONNECT™ business case (defined by AVL) and the CAM use cases presented in "Austrian Action Programme on Automated Mobility" (BMVIT, 2019):

- **"Safety+ through an all-round view"**: This use case (figure below) is about driver assistance systems using sensors to intervene in traffic situations whenever danger is imminent. The information collected from other road users and from the infrastructure itself benefits to this use case, by enhancing road safety in the immediate environment of the vehicle.



- **"New flexibility"**: This use case (figure below) describes automated vehicles offering new, on-demand services that can increase the flexibility of mobility users (e.g. route optimization, driving times tailored to personal preferences, secure and convenient connection mobility with intermodal transfer points, booking services, etc.) and ease the burden on the environment (e.g. by decreasing the environmental impact of CO2 emissions in the atmosphere).



In D5.4.1, the two above-mentioned use cases, initially presented in (BMVIT, 2019), are further extended to address the specific requirements of the IoT4CPS project. These two use cases are defined in D5.2 as "Safety & Cybersecurity+ through the Lifecycle Stages" and "Assistive Intelligence+ through the Lifecycle Stages". D5.4.1 gives an overview of both user identity and device identity in the cloud and discusses Identity Management (IDM) systems, including blockchain-based IDMs. In addition, D5.4.1 provides the cybersecurity analysis for the above-mentioned CAM use cases by looking at their Product Lifecycle Data Management (PLCDM). Such analysis includes identification of the involved IoT-/ CPS-based assets (and their services) and stakeholders, which are further linked to the relevant identity and security risks. The D5.4.1 report highlights the importance of periodical checks and cybersecurity validations for verifying the integrity of the system (at a software level) as a way of ensuring that desired security and safety postures of the system remain in place. For example, the identity of sensors could be established correctly, even if they do not operate at their intended location, which may be caused by mechanical collisions, vibrations, or sabotages or even malicious conduct. The promising solution in such cases is to implement wireless localization system for assets used along lifecycle phases.

In Section 4 of this report, an example of a wireless localization system is described and its accuracy, precision and resilience are validated for CAM use cases. In addition, we look at trust and ethics in relation to the CAM applications. The results of the analysis provided in D5.4.1 and D5.4.2 serve as a basis for the data acquisition and for the implementation of the Digital Twin prototype in task T5.5.

Document organisation: The rest of Section 1 shows the relation to other tasks and reports in the project, e.g. D2.2, D3.3, D3.4, and more. Section 2 provides an analysis of safety and privacy indicators for smart vehicles, which are linked in Table 1 – Table 4 to the users (stakeholders) and devices (assets) for the two use cases. Note that similar analysis is provided for identity and security issues in the predecessor report, D5.4.1. Section 3 discusses relevant safety and privacy threats in IoT4CPS that are based on the threat model developed in IoT4CPS and described in D4.1 **"Automotive Ethernet Protection Profile"**. Section 4 describes the use of localisation methods to address safety issues in the project by estimating the direction (rather than a range) of incoming signals from smart vehicle's sensors. The current experimentation with localisation methods is used in realistic indoors environments, and placed in the context of above-mentioned scenarios. Section 5 discusses current standards, regulations and frameworks for security, privacy, trust and ethics in CAM applications. Section 6 concludes this report.

1.1 Relation to IoT4CPS Business Case on Security Verification Along the Lifecycle (D2.2)

The **D2.2 "Business needs consolidation – competitive intelligence"**, Section 3.2 "AVL: Security Verification Along the Full Life Cycle of IoT-based Industrial Instrumentation Systems" describes the role of the Device.CONNECT™ system that enables communication links with the external systems, e.g. through smart/ predictive maintenance services in the cloud. It provides connectivity to a multitude of cloud-based commercial products, such as emission analysers, particle samplers, instrumentation systems, etc. At the same time, the cloud-based nature of the Device.CONNECT™ puts this device into a category of highly vulnerable assets that need to be continuously monitored and checked against common threat intelligence indicators, regulations and stakeholders' governance rules. In this report, we extend the two selected use cases from (BMVIT, 2019) by adding the AVL's business case (the Device.CONNECT™ system).

1.2 Relation to IoT4CPS Resilient System Architecture (D3.3) and Solutions for Safe & Secure IoT (D3.4)

In Work Package WP3, several state-of-the-art technologies applied to indoor localization and autonomous driving are discussed (see **D3.3 "Guidelines and recommendations for resilient system architecture pattern and concepts and HW-based solutions for safe & secure IoT"** (IoT4CPS D3.3, 2019)). In addition, WP3 investigates how localization systems can enable multi-stakeholder trust provisioning during production and maintenance. This is done by analysing different approaches in the context of indoor localization and identifying attacks which could be used to compromise such localization approaches (the results of this investigation are outlined in the **D3.4 "System architecture patterns for enabling multi-stakeholder trust provisioning during production and maintenance"**). Given that localization provides mechanisms for contextualization, it can be also used to establish additional information regarding entities in a cyber-physical system, e.g. to verify and ensure that all components of a specific setup are in place thus allowing to test the physical integrity of a system (which is not possible via sole identity management). This requires reliable and energy efficient indoor localization mechanisms to be exploit. The need for energy efficiency results from the fact that such setups should be able to operate over long time-periods with minimal engineering efforts. In the course of the work in this project, two technologies suitable for indoor localization, namely Ultra-wideband and Bluetooth Low Energy have been considered. In this report, we evaluate performances of those technologies and discuss their applicability to verify the physical integrity of a system and support safety in identity management systems, e.g. in vehicle localization inside tunnels and localization of objects (e.g., pedestrians) that are equipped with compatible devices.

1.3 Relation to Other WP5-Tasks on Product Lifecycle Data Management (D5.2 and D5.4.1)

This report strongly relates to the work presented in **D5.2 "Product Lifecycle Data Management (PLCDM) Stakeholder Perspectives"** that captures multi-tenancy aspects related to smart vehicles, actual legislations and emerging standards for data and information exchange in the Automotive Mobility sector, along the product lifecycle. This report is also linked to its predecessor **D5.4.1 "Identity, Security and Safety in Product Lifecycle Data Management"** that further extends the data model from D5.2 by adding identity and security aspects.

1.4 Relation to Other Work Packages in IoT4CPS: WP3, WP4 and WP7

Figure 1 illustrates the major concepts in IoT4CPS, e.g. product lifecycle (PLCDM, in green), security aspects (in blue); trustworthy connectivity (in orange), and Digital Twin demonstrator (in pink). These concepts are related to other tasks and WPs in the following way:

1. Cybersecurity Lifecycle (joint work through WP3, WP4, WP5) that is based on data models created in tasks T5.2 and T5.4;
2. Digital Twin modelling (WP5) with the initial concepts and building blocks presented in D5.5.1 "Lifecycle Data Management Prototype I";
3. Trustworthy connectivity (WP7);
4. Traceability through lifecycle phases (WP7), related to task T7.2;
5. Security by isolation (WP7), related to task T7.3;
6. Smart production use case (Device.CONNECT™) (WP2, WP7) as described in section 3.1;
7. Autonomous vehicles (WP6), related to task T6.1 on secure and safe platform for Automated Driving applications.

Figure 1 also illustrates the Cybersecurity Data Lifecycle that adds identity, security and safety features to the main PLCDM observations, which are implemented in the IoT4CPS Digital Twin prototype (T5.5).

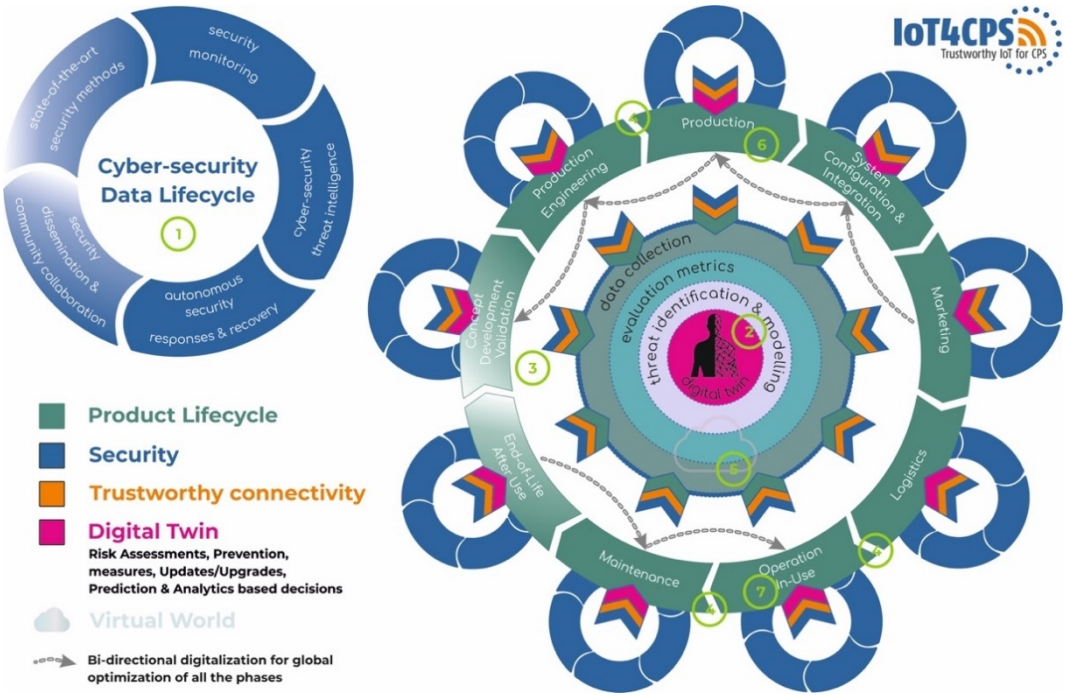


Figure 1 – The major concepts in IoT4CPS, in relation to the definition of the Digital Twin data models

2. Safety and Privacy Analysis of Connected and Automated Mobility Use Cases

The core motivation behind the design of smart cars and CAM applications for connected and (semi-) autonomous vehicles, is about the enhancement of users' experience and the improvement of both user's and vehicles' safety. Smart cars and their intelligent applications are based on Machine Learning (ML)-algorithms and many techniques from the Artificial Intelligence (AI) field that are applied to provide advanced reasoning, decision support and knowledge classification for better user experience and safety. Some of those advanced techniques provide self-learning features of algorithms and their applications, thus opening new challenges when the algorithms are used in different contexts and situations that are out of human's control.

Nowadays advanced processing algorithms run in the cloud, and coordinate large and complex service systems. On the one hand, this allows for capturing the information (near-)real time, with low-latency communication, and high data reliability and integrity that can accurately support transforming, altering and recombining the data into a new decision. On the other hand, the advancement of ML algorithms brings new cybersecurity challenges and opens further potential risks by expanding the attach surface and attack vectors. New attacks can target both roads and users of vehicles (even vehicle passengers), causing road accidents or vehicle immobilization.

The existing attacks that targeted safety aspects of smart vehicles, include the 2015' *proof-of-concept* attack where the researchers took control over a Chrysler Jeep Cherokee and sent a vehicle off the road (see: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/); the attack that remotely controlled vehicle's infotainment system (Keen Sec Lab, 2018) or hacking smart vehicle's alarm systems (see: https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/) or GNSS (Global Navigation Satellite Systems) spoofing (Zeng et al., 2018). In 2018, researchers from the KU Leuven University in Belgium demonstrated how the key fobs signals can be used to open Tesla Model S vehicle's door "in a matter of second" (https://www.zdnet.com/article/how-to-steal-a-tesla-model-s-in-seconds/).

Some of the current cybersecurity regulations and initiatives created to ensure safety conditions of smart vehicles, include the following (ENISA, 2019):

- C-ITS (Cooperative Intelligent Transport Systems) deployment platform (2014) by the Commission's Directorate-General for Mobility and Transport (DG MOVE), created with the objective to ensure interoperability of C-ITS across borders and along the whole value chain.
- The Cars and Roads SECurity (CarSEC) working group by ENISA (2016), created to protect road users' safety.
- An initiative on safety regulations (i.e. the General Safety Regulation and the Pedestrian Safety Regulation) by the Directorate-General for Internal Market, Industry, Entrepreneurship and Small and Medium-sized Enterprises (SMEs) (DG GROW) launched in 2017.
- The British Standards Institution (BSI) group published Publicly Available Specifications (PAS), namely PAS 1885 and PAS 11281. The PAS 11281 "*Connected automotive ecosystems – Impact of security on safety – Code of practice*" provides recommendations for managing security risks in a connected automotive ecosystem.
- In 2019, the European Commission set up an informal group of experts "The Single Platform for open road testing and pre-deployment of cooperative, connected, automated and autonomous mobility" in order to provide advice and support testing and pre-deployment activities for CAM.

The study in (David & Fry, 2016) lists the following safety and privacy standards in the CAM sector:

- ISO 26262: Functional safety for road vehicles;
- ISO 27018: Code of Practice – Handling PII / SPI (Privacy)
- ISO 29101: Privacy architecture framework
- J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

- E-safety Vehicle Intrusion Protected Applications (EVITA): Co-funded by the European Commission, this is an architecture for secure on-board automotive networks, with a focus on protecting components from compromise due to tampering or other faults.
- Trusted Platform Module (TPM): Written by the TCG and standardized as ISO/IEC 11889, it defines roots of trust that enable many of the key attestation activities that are mandatory on a vehicle, and more.

Recently published Upstream Security's report looks at past 10 years of security incidents associated with vehicles (Upstream, 2020). The report includes 367 incidents, out of which 155 occurred in 2019, acknowledging that there might be cases it has missed. Some of the report's headline statistics refers at a 99% growth in incidents since 2018, while more of fraud and data breach incidents are expected in the future, e.g. Toyota, Honda and Mercedes-Benz already experienced malicious database breaches that spilled the data of employees and customers (Upstream, 2020).

Figure 2 shows a variety of attacks against smart vehicles (source: (Upstream, 2020)), pointing at vehicle's network connectivity as obvious points of attack.

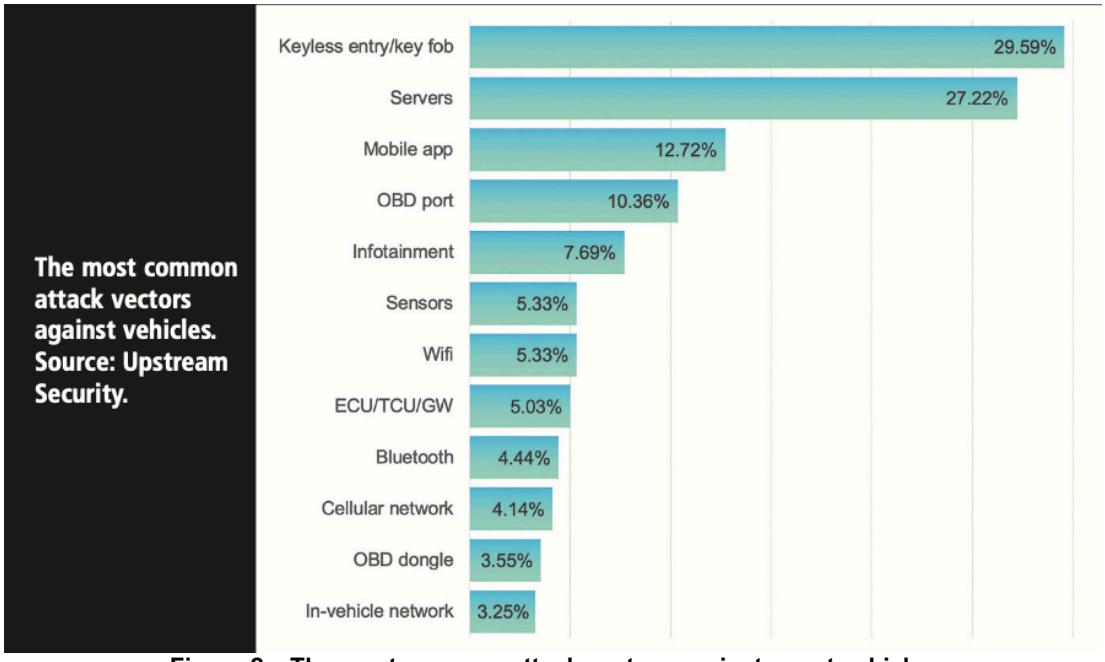


Figure 2 – The most common attack vectors against smart vehicles

There is a strong relationship between cybersecurity and automotive safety. In (SEA, 2016), system safety is described as a method concerned with protecting against harm to life, property or the environment. All safety critical systems are security critical, but there exist systems that could be only security critical, not safety critical (e.g. entertainment systems). In contrast to safety, system cybersecurity aims to prevent financial, operational, privacy, or safety losses.

The study in (David & Fry, 2016) shows that information privacy, data privacy, securing data exchange, including input and output data as well as protecting Electronic Control Units (ECUs) of smart vehicles are among the most significant security, safety and privacy issues related to smart vehicles. In the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) modes of communication (see Figure 3), the shared information can be used maliciously to track users (Safi et al., 2018). Hence, all sensitive information in and out of smart vehicles must be protected. Personally Identifiable Information (PII), i.e. location data, address books, and credit card numbers, require privacy controls and data anonymization to be put in place, in order to ensure confidentiality of personal data and prevent leaking of user data. For example, maintaining confidentiality may require data to be protected by encryption inside and outside the vehicle while it is stored, and by memory protection extensions while it is being processed (David & Fry, 2016). To prevent data leakage, some measures to improve data privacy are suggested, i.e. (1) minimizing the amount of personal data that is stored, (2) to be transparent about what data is collected, how it is used and stored, and (3) to have a clear way to securely delete any stored personal data.

Figure 3 illustrates Vehicle-to-Everything (V2E) communication model showing variety of possible communications, apart V2V and V2I; for example, Vehicle-to-Pedestrian (V2P), Vehicle-to-Cloud (V2C), Vehicle-to-Home (V2H), and Vehicle-to-Network (V2N) (source: (DIBA, 2020)).

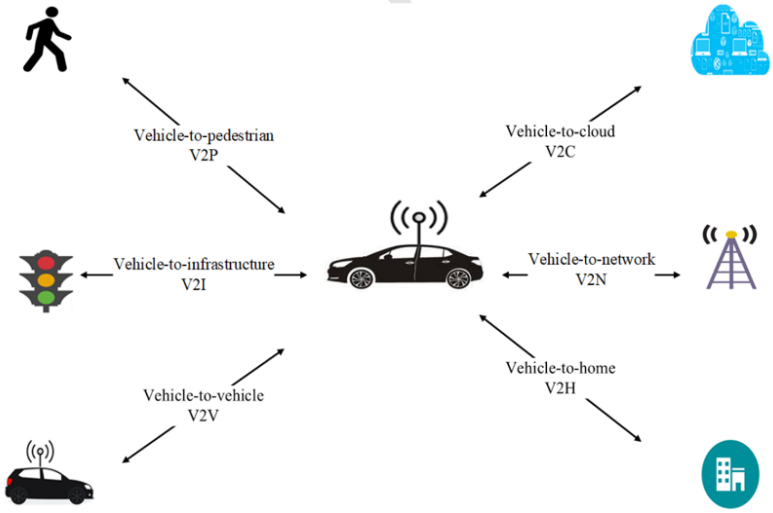


Figure 3 – V2E communication models

Figure 4 illustrates some major modern car security risks targeting both safety and privacy aspects of smart vehicles, e.g. malware and spam, hacking of OnBoard Diagnostics (OBD) adapters (e.g. OBD-II) and/or car key fobs, personal data, etc. Some other surveys on major obstacles to smart vehicle uptake identify cybersecurity and privacy as the biggest concerns for the users, too (Levine, 2019) (Hitachi Systems Security, 2019). Figure 5 illustrates the most hackable assets of smart vehicles, including **Engine and Transmission Unit (ECU)**, steering and breaking ECU, **LiDaR** (Light Detection and Ranging) that enables self-driving cars to observe the environment with a 360-degree field of view and with more than 16 laser channels, **millimeter-wave radar** that is capable of penetrating non-transparent materials, such as smoke, dust, snow, and fog, in order to handle small size, all-weather, and long detection distance; **intelligent visual sensors** (the monocular visual system and the stereo vision system) that provide semantic segmentation of the driving environment (Johnson, 2008), target detection and tracking (Song and Chandraker, 2014), ranging (Dagan et al., 2004) (Park and Hwang, 2014), driver distraction and fatigue detection (Dong and Hu, 2013), etc. Nowadays' visual sensors include integrated AI technologies to provide more accurate detection results. The AI algorithms are often targeted by attackers, leading to a false detection result (DIBA, 2020).

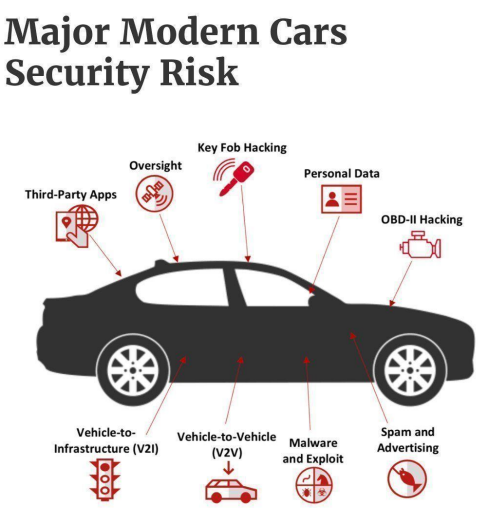


Figure 4 – The major modern cars security risks

Photo source: https://www.itlab365.com/major-modern-cars-security-risk/

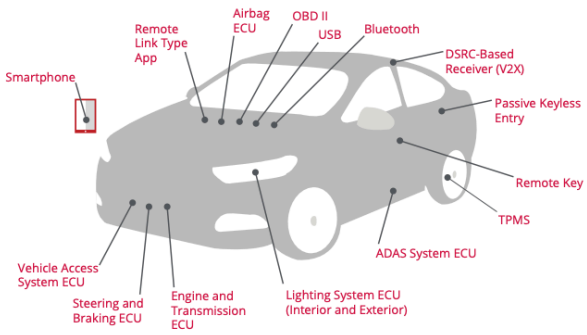


Figure 5 – The most hackable assets of smart vehicles

Photo source: (David & Fry, 2016); Available online: https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf

Examples of the data retention policies for smart vehicles are discussed in (CAR2CAR, 2018) including the following:

- A received safety related CAM (Common Awareness Messages) message shall not be forwarded/ multi-broadcast (ETSI EN 302 637-2. § 5.3.4.1);
- A received safety related DENM (Decentralized Environmental Notification Messages) may be forwarded/ broadcast only within a limited predefined geographical area (ETSI TS 101 539-1/2/3 and ETSI EN 302 637-3 § 6.1.3.3);
- Driving conditions data are kept in memory from a few seconds to a few minutes, depending on the need of the service. They are erased as soon as their emission conditions are over, and at each start of the engine (ETSI EN 302 637-3 § 6.1.2);
- No CAM is relayed to a vehicle manufacturer backend.

The study in (DIBA, 2020) classifies and compares the existing defences against the attacks in vehicular networks, e.g.:

- **Cryptography-based algorithms used to enhance security for smart vehicles.** Here, encryption is an essential key to ensure safety and can be based either on symmetric key encryption, asymmetric key encryption, or attribute-based encryption;
- **Network security for enabling communication between vehicle's sensors and other devices,** e.g. the CAN and ECUs which are often targets for adversaries. This category includes signature-based detection methods, and anomaly-based detection methods;
  - Signature-based detection method first stores existing signatures of known attacks in a database for retrieving them and making a comparison. The intrusion attack is detected by comparing oncoming cases from the Internet of Vehicle (IoV) with existing signatures of known attacks in store;
  - Anomaly-based detection method predefines the baseline of normal cases. The new types of attack can be identified once they are observed to have abnormal information beyond the baseline (Sedjelmaci et al., 2014);
- **Software vulnerability detection** is crucial to prevent any potential threat, data theft and accidents (e.g. software-controlled vehicle's infotainment system or alarm system) (Amoozadeh et al., 2015) (Kumar et al., 2018). The most popular techniques for software vulnerability discovery include:
  - Static analysis methods that do not execute the code and can be performed using some common techniques: lexical analysis (McGraw, 2004), control-flow analysis (Abadi et al., 2005) (Tice et al., 2014) (Ding et al., 2017) and data flow analysis (Wögerer, 2005) (Castro et al., 2006);
  - Dynamic analysis methods that depend on running the program to examine whether it has errors and vulnerabilities. The two important dynamic analysis techniques are fuzzing (Takanen et al., 2008) (Godefroid et al., 2008) and dynamic taint analysis (Newsome and Song, 2005) (Schwartz et al., 2010) (Clause et al., 2007);
  - Software testing techniques include symbolic execution (Khurshid et al., 2003) and mutation testing (Deng et al., 2017);
  - Machine Learning (ML) and especially deep learning has been employed to automatically detect software vulnerabilities in (Lin et al., 2018) (Li et al., 2018) (Shin et al., 2011) (Perl et al., 2015) (Zhou and Sharma, 2017) (Shar et al., 2015) (Grieco et al., 2016);
- **Malware detection methods** are used to prevent incidents that can cause millions of dollars loss related to smart vehicles (Luo and Liu, 2018). Malware attacks on smart vehicles can be of various types, e.g. spyware, ransomware, worms, viruses, trojans, adware, spam, bots. Some of well-known intelligent malware detection approaches include the following:
  - Malicious Sequential Pattern mining for automatic Malware Detection (MSPMD) uses a modified version of the K-nearest neighbour algorithm for malware detection (Fan et al., 2016);

- Hybrid of Maximum Relevance–Minimum Redundancy and Support Vector Machine Score (MRMR–SVMS) uses the combination of SVM wrapper with MRMR filter (Huda et al., 2016) to extract API statistics as features that can be used to identify malware. The goal of this hybrid approach is to exploit the strengths of each of these two basic approaches and to achieve the highest accuracy with detection;
- The authors in (Huda et al., 2017) propose a novel semi-supervised malware detection system for CPS that uses supervised learning, clustering, and available unlabelled data for dynamic feature extraction. The proposed approach provides protection against new malware without manually labelling or updating the database;
- CloudIntell proposes computational offloading using SVM (Support Vector Machine), decision tree and boosting on decision tree (Mirza et al., 2017). This approach offers a high detection rate and is energy efficient, but requires continuous connectivity.

The following two subsections provide an analysis of safety and privacy issues along the product lifecycle of connected vehicles, for two use cases and for both users (stakeholders) and devices (assets) involved in these use cases (see Table 1 – Table 4). Note a similar analysis is provided for identity and security issues in D5.4.1. The identification of stakeholders and assets, and their assignment to relevant threat indicators through lifecycle phases are based on literature review related to connected car security, safety and privacy features and recent incidents, e.g. (ENISA, 2016), (FPF, 2018) (Hitachi Systems Security, 2019) (Levine, 2019) (ENISA, 2019). In addition, the definition of relevant safety and privacy issues for both use cases is informed by the threat model described in **D4.1 "Automotive Ethernet Protection Profile"**.

2.1 Use Case 1 "Safety & Cybersecurity+": Analysis of Safety and Privacy Aspects

Figure 6 illustrates an extension of the BMVIT's "Safety+ through an all-round view" use case by including the AVL's Device.CONNECT™ system that collects data related to the road and environmental conditions, e.g. air pollution, temperature near the surface of the road, humidity. This data can be combined with the data from the car's powertrain controls (e.g. sensor information from electrical engines, transmission, wheels) and chasses controls (e.g. sensor information coming from the steering and brakes, airbags, embedded cameras, real-view mirrors, windshield wipers). Figure 6 captures both cybersecurity and multi-stakeholder perspectives along the vehicle's lifecycle. Sensor data collected through the assets in this use case (e.g. Device.CONNECT™, electrical engines, wheels or chasses controls, etc.) can be targeted by adversaries and manipulated in a way that can affect safety and privacy of stakeholders. Hence, we proceed with the identification of the common assets of smart vehicles used in this use case (see Table 1) and various stakeholder (see Table 2). The most common safety and privacy issues related to both assets and stakeholders are presented in Table 1 and Table 2.

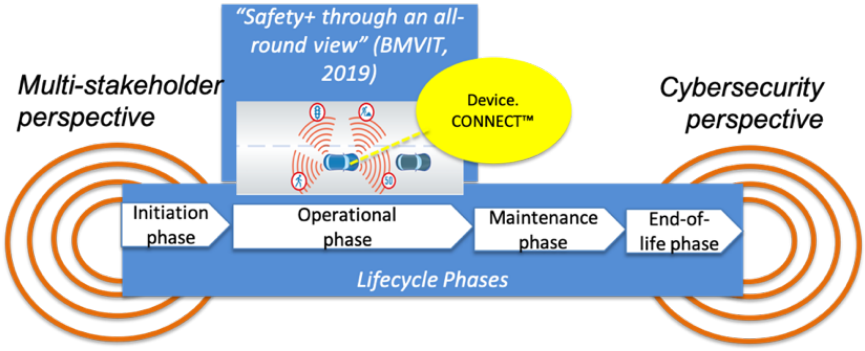


Figure 6 – Extension of the use case 1 to capture safety & privacy indicators related to vehicle's PLCDM

Identification of assets. Note both assets and stakeholders captured in Table 1-Table 4 in this report correspond to assets and stakeholders presented in Table 1-Table 4 in D5.4.1. The difference is that in D5.4.1, the focus is on identity and security aspects, while in D5.4.2, the focus is on safety and privacy indicators.

Table 1: Use case 1: Assets, and relevant safety and privacy indicators

Smart vehicle's devices/ sensors	Type of sensor data	Possible relevant safety and privacy issues
Initiation phase		
CAD uploader	Computer Aided Design (CAD). It assures that the design of the CPS-based product is analysed, optimized and sent to manufacturing.	**Safety:** Physical harm of electrical or mechanical manufacturing processes caused by vulnerable behaviour of the system.
		Privacy: Sensitive data; systematic monitoring of the manufacturing process; innovative use or applying new technological solutions; device identity theft.
Collaborative analysis checker	It enables collaborative design and further improvements of CPS-based products to be manufactured.	**Safety:** Provision of false design information leading to destruction of assets and safety issues.
		Privacy: Device identity theft; identity fraud; sensitive data breach.
CAM/CIM initiator	Computer Aided Manufacturing (CAM) / Computer Integrated Manufacturing (CIM). It enables the manufacturing flow from raw materials to finished products, with quality assurance and automated assembly.	**Safety:** Provision of false information as a basis for CAM/CIM processes. Safety issues related to automated assembly and quality assurance.
		Privacy: Device identity theft; identity fraud; sensitive data breach. Damaging effect on manufacturer reputation.
Robotic assembly checker	It checks the production of completed assemblies, part size, part defects.	**Safety:** Long term damage of manufacturing processes and assemblies.
		Privacy: Device identity theft; identity fraud; sensitive data breach; systematic monitoring.
Supply chain status control	It checks for the delivery terms in order to meet the demand.	**Safety:** Provision of fake delivery details through malware injection, compromised digital signatures, etc.
		Privacy: Access to sensitive corporate data and spying through backdoors installed on factory machines. Device identity theft; identity fraud.
Operational phase		
Device.CONNECT™	Air pollution, temperature near the surface of the road, humidity data.	**Safety:** Planting backdoors on corporate devices. Provision of fake delivery details through malware injection, compromised digital signatures, etc.
		Privacy: Device identity theft. Access to sensitive corporate data.
Powertrain control	Data from electrical engines, transmission data, wheels data.	**Safety:** Remote control through hijacked sensors.
		Privacy: Device identity theft. Access to sensitive corporate data.
Chasses control and OBD-II	Data about the steering and brakes conditions, airbags, embedded cameras, real-view mirrors, windshield wipers. OBD-II collects driver behavioural information (how fast he/she drives the vehicle, how aggressively he/she apply the brakes, etc.) as well as geolocation data.	**Safety:** Wirelessly controlled radio stations, windshield wipers, air conditioning system, vehicle steering, etc. Compromised brakes, speed and gear controls leading to destruction of assets and safety issues.

		Privacy: Retrieving information about the vehicle, such as vehicle ID number, make, model, IP address, GPS coordinates. Scanning multiple mobile apps and connected devices to find out the owner of the vehicle in order to track a person.
Maintenance phase		
CIM Remote Monitoring Service	It monitors for unauthorized access and changes to the files and smart vehicle's devices.	**Safety:** Provision of false information leading to safety issues.
		Privacy: Device identity theft.
Integrity Monitoring Service	It detects and reports changes made in files or detects manipulations.	**Safety:** Provision of false information leading to safety issues.
		Privacy: Device identity theft.
End-of-life phase		
Privacy Data Monitoring Service	It ensures that retained privacy data are removed from the connected cars (FPF, 2018), e.g. mobile apps that are used, mobile apps log-in data, location, the driver's daily route, phone contacts and address books, garage door codes, various digital content, subscription services, WIFI hotspots, data services, etc.	**Privacy:** Exploring privacy data stored in the connected car or in the cloud databases. Inventory of PII that may be difficult to identify and track by the users due to limited data reporting, and notice of data collection. Personal data sold or leaked to the public. Unauthorized access to privacy information.
Other Data Monitoring Services	It enables other data to be removed from the connected cars, e.g. OBD information.	**Safety:** Exploring other data in the connected car or in the cloud databases, e.g. electronic data recorders (black boxes), data collected from the vehicle monitoring devices, etc. leading to safety issues.
		Privacy: Exploring other data in the connected car or in the cloud databases, for privacy breaches. Sharing PII with external parties.

Identification of stakeholders. Table 2 lists potential stakeholders (directly or indirectly) involved in the use case 1. This list is partly based on (ENISA, 2016).

Table 2: Use case 1: Stakeholders identification and relevant safety and privacy issues

Stakeholder	Description of the stakeholder's role in the use case	Potential relevant safety and privacy issues
Initiation phase:	Manufacturers & Suppliers	
Manufacturer	Provides the production and assembly of the car components.	Threatening safety and privacy of manufacturers. Reputational damage. Intellectual property theft.
Aftermarket Supplier	Provides components with additional features, e.g. media player.	Spying on corporate secrets. Reputational damage. Conflicting security and safety features.
Operational phase:	Car Users & Internal Services	
Driver	Drives and uses the connected car's gadgets and apps/services. Connects via smartphone. Uses external cloud applications.	Privacy and safety risks to the drivers. Personal data sold or leaked to the public. Data integrity that affects accuracy of data with the potential to create safety and privacy problems for users.

Passengers	Use gadgets and apps or are exposed to apps and services running on other user's devices.	Privacy and safety risks to the passengers. Personal data sold or leaked to the public. Data integrity creating safety and privacy critical situations for passengers. Personal data include vulnerable data subjects.
Powertrain control services	Transmission controls; wheels controls; services for monitoring of the engine features, etc.	Security and safety risks, e.g. a physical hacking technique to exploit the CAN protocol of a vehicle. Compromised and unexpected behaviour of cars, e.g. heating seats.
Operational phase:	External Services	
Road services	Monitoring road and traffic conditions; Safety recommendations and contextual insights, e.g. speed limit changes, roadway conditions. eCall services.	Disturbance of surrounding vehicles and road services. Safety issues through incorrect signalisation data or incorrect navigation data.
Testing and certification services	Monitoring driving habits; Contextual insights.	Privacy and safety risks to the drivers. Driver's disruption.
Insurance services	Pay-How-You-Drive insurance plan.	Privacy risks and secrets. Fraud situations. Unauthorized copies. Continuous monitoring of user's behaviour and driving routines. User evaluation and scoring. Data processing on a large scale.
Network connectivity providers & services	Network access and services. Remote transmission of vehicle data. Remote engine start. Geo-fencing. Crash reporting and emergency warning (eCall), etc. Remote diagnostics and fleet management. The principle of least functionality should be incorporated to provide only essential device/service capabilities.	Integrity breach and disruptions. A loss of control of a car. Spoofed communication causing accidents. Increasing the possibilities for eavesdropping, data manipulations and interception.
Smart cities & services	Economical use of the road infrastructure. Smart city weather station and road speed controls. Environmental impact evaluation.	Trade secrets. Data confidentiality and privacy of citizens, drivers and passengers. Safety related vulnerabilities. Increasing the possibilities for eavesdropping, data manipulations and interception. Data processing on a large scale.
Maintenance:	External Services	
Road services	Monitoring traffic conditions; Safety recommendations.	Trade secrets. Safety risks. The likelihood of eavesdropping on network communication.
Manufacturer	Evaluation of part's functionality and safety. The principle of least functionality should be incorporated to provide only essential device/service capabilities.	Integrity breach and disruptions. Safety risks. Trade secrets.
End-of-life phase:	External Services	
Smart city services	Economical use of the city infrastructure. Environmental impact evaluation.	Security and safety vulnerabilities. The likelihood of eavesdropping.

2.2 Use Case 2 "Assistive Intelligence+": Analysis of Safety and Privacy Aspects

To support the assistive intelligence capabilities relevant to safety and privacy aspects, we "redefine" the use case on "New flexibility" (BMVIT, 2019) by adding the Device.CONNECT™ system and the Digital Twin prototype

(task T5.5) to support stakeholders along the lifecycle and to verify the system's safety and privacy conditions (see Figure 7). The smart vehicle collects data such as air pollution, temperature near the surface of the road, humidity, telematics data about braking, engine performance, collision detection and emergency calling, vehicle diagnostics, vehicle speed, GPS data and many more. The power of data lies in its combination. For example, the smart vehicle can recognize the intention of another car to change lanes, or based on light signals, it becomes aware which vehicle will turn and which will continue moving straight. This scenario shows a potential to eliminate traffic fatalities in the future and improve safety conditions related to the roads and vehicles.

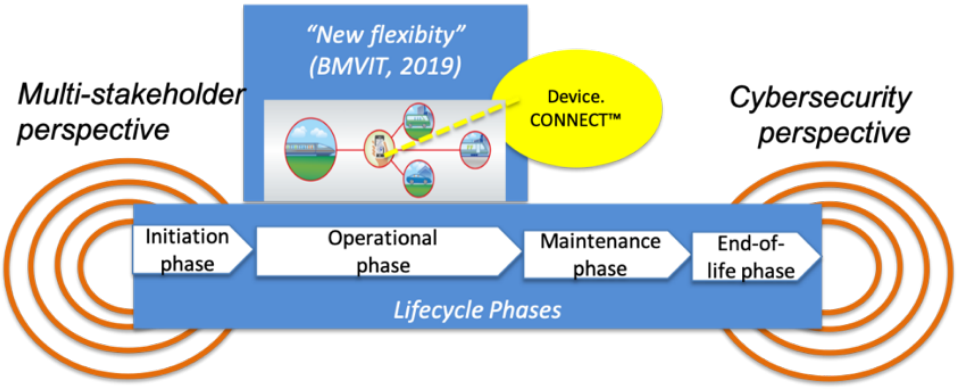


Figure 7 – Extension of the use case 1 to capture safety & privacy indicators related to vehicle's PLCDM

Identification of assets. Table 3 lists various assets involved in the use case 2. It assigns possible safety and privacy indicators related to each asset.

Table 3: Use case 2: Assets, and relevant safety and privacy issues

Smart vehicle's devices/ sensors	Type of sensor data	Possible relevant safety and privacy issues
Initiation phase		
Robotic assembly checker	It checks the production of completed assemblies, part size, part defects (e.g. based on feeder jam data)	**Safety:** Long term damage of manufacturing processes and assemblies. Provision of false assembly information that lead to safety issues.
		Privacy: Device identity theft. Access to sensitive manufacturing data and data breach.
Supply chain status control	It checks for the delivery terms in order to meet the demand	**Safety:** Provision of fake delivery details through malware injection, compromised digital signatures, etc.
		Privacy: Access to sensitive corporate data and spying through backdoors installed on factory machines. Device identity theft; identity fraud.
Operational phase		
Device.CONNECT™	Air pollution, temperature near the surface of the road, humidity	**Safety:** Planting backdoors on corporate devices. Provision of fake delivery details through malware injection, compromised digital signatures, etc.
		Privacy: Device identity theft. Access to sensitive corporate data.
Powertrain control	Data from electrical engines, transmission data, wheels data	**Safety:** Incorrect data that lead the car to unsafe situations. Remote control through hijacked sensors.
		Privacy: Device identity theft.
Chasses control and OBD-II	Data about the steering and brakes conditions, airbags, embedded cameras,	**Safety:** Wirelessly controlled radio stations, windshield wipers, air conditioning system,

	real-view mirrors, windshield wipers, Advanced Driver Assistance System (ADAS)	vehicle steering, etc. Compromised brakes, speed and gear controls leading to safety issues. Incorrect navigation and assistance data that lead to unsafe situations.
		Privacy: Device identity theft. Retrieving information about the vehicle, such as vehicle ID number, make, model, IP address, ownership, GPS coordinates. Retrieving information about the driver's driving style (speed, pressure on brakes, etc.). User recognition. Tracking eye movement to detect if the driver is falling asleep behind the wheel.
Infotainment control	Music and video streaming, Bluetooth connectivity, WIFI connectivity and WIFI hotspots, SMS texting …	**Safety:** Creating fake visualizations and fake information leading to safety issues.
		Privacy: Device identity theft. Scanning multiple mobile apps and connected devices to find out the owner of the vehicle in order to track a person. The likelihood of eavesdropping on network communication.
External media	Mobile phones, Bluetooth speakers for cars, etc.	**Safety:** Switching off the emergency information and alarms, causing safety critical situations.
		Privacy: Device identity theft. Scanning multiple mobile apps and connected devices to find out the owner of the vehicle in order to track a person.
Maintenance phase		
Integrity Monitoring Service	It detects and reports changes made in files or detects manipulations.	**Safety:** Provision of false information creating safety critical situations.
		Privacy: Device identity theft.
End-of-life phase		
Privacy Data Monitoring Service	It ensures that retained privacy data are removed from the connected cars (FPF, 2018).	**Privacy:** Exploring privacy data stored in the connected car or in the cloud databases. Personal data sold or leaked to the public.
Non-Privacy Data Monitoring Services	It enables other data to be removed from the connected cars, e.g. on-board diagnostic information.	**Safety:** Exploring other data in the connected car or in the cloud databases, e.g. electronic data recorders (black boxes), data collected from the vehicle monitoring devices, etc. leading to safety issues.

Identification of stakeholders. Table 4 lists stakeholders involved in the use case 2. This list is partly based on (ENISA, 2016).

Table 4: Use case 2: Stakeholders identification and relevant safety and privacy issues

Stakeholder	Description of the stakeholder's role in the use case	Possible relevant safety and privacy issues
Initiation phase:	Manufacturers & Suppliers	
Supplier	Provides car components and /or operating system for connecting car components. The principle of least functionality should be incorporated to provide only essential device/service capabilities.	Threatening safety and privacy of supplier. Reputational damage. Intellectual property theft.

Aftermarket Supplier	Provides components with additional features, e.g. media player. The principle of least functionality.	Spying on corporate secrets. Reputational damage. Conflicting security and safety features.
Operational phase:	Car Users & Internal Services	
Driver	Drives and uses the connected car's gadgets and apps/services. Connects via smartphone. Uses external cloud applications.	Privacy and safety risks to the drivers. Personal data sold or leaked to the public.
Passengers	Use gadgets and apps or are exposed to apps and services running on other user's devices.	Privacy and safety risks to the passengers. Personal data sold or leaked to the public. Personal data include vulnerable data subjects (e.g. kids, ill persons, elderly people, etc.).
Cross-collaborative services and data exchanged among connected cars	Data received from another connected cars, e.g. the location of a car accident that another connected car spotted on the road, or received accident information from other cars, or smart city info services.	Compromised and unexpected behaviour of cars, e.g. heating seats. Safety related vulnerabilities, e.g. based on a disturbance of warning/direction lights. Missing updates and security patches for services which can keep known vulnerabilities.
Operational phase:	External Services	
Smart cities & services	Economical use of road infrastructure.	Trade secrets. Data confidentiality and privacy of citizens, drivers and passengers. The likelihood of eavesdropping on network communication. Safety related vulnerabilities.
Road services	Monitoring road and traffic conditions; Safety recommendations and contextual insights, e.g. speed limit changes, roadway conditions.	Fraud situations. Unauthorized copies. Unauthorized access to sensitive data. Eavesdropping on network communication.
Insurance services	Pay-How-You-Drive insurance plan.	Privacy risks and secrets. Unauthorized copies. Continuous monitoring of user's behaviour and driving routines.
Energy/fuel services	Energy/fuel supply.	Trade secrets. Safety related vulnerabilities.
Marketing services	Monitoring driving habits and user's preferences to create personalized offers.	Trade secrets. Data confidentiality and privacy of citizens, drivers and passengers. Unauthorized access to sensitive data and PII. Eavesdropping on network communication. User evaluation and scoring. Data processing on a large scale.
Maintenance:	External Services	
Insurance services	Pay-How-You-Drive insurance plan.	Privacy risks and secrets. Unauthorized copies. User evaluation and scoring.
Road services	Monitoring traffic conditions; Safety recommendations.	Trade secrets. Safety risks. Unauthorized access to sensitive data and PII. Eavesdropping on network communication. User evaluation and scoring.
End-of-life phase:	External Services	
Smart city services	Environmental impact evaluation. Weather data.	Trade secrets. Data confidentiality and privacy of citizens, drivers and passengers. Data leaks. Safety related vulnerabilities. Eavesdropping on network communication.

3. Relevant Safety and Privacy Threats in IoT4CPS

This section presents 14 threats, out of 328 threats defined in **D4.1 "Automotive Ethernet Protection Profile"**. The threats are selected according to their expected security and safety implications on product lifecycle data of the two use cases, e.g. security and safety manipulations at the level of vehicle data; an unauthorized access to privacy data stored in the connected car's infotainment system; sensor flooding with invalid data to cause denial of service, etc. The threat list presented in D4.1 is extended in this report by encompassing a threat modelling template created by the NCC group (Corradini, 2016).

3.1 Cross Site Request Forgery

Category: Target of an attack on a vehicle

Cross-Site Request Forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged into a web site A using a cookie as a credential. Web site B contains a page with a hidden form that is post to web site A. Since the browser carries the user's cookie to web site A, web site B can take any action on web site A, e.g. adding an admin to an account.

The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting, etc. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS.

3.2 Manipulate Vehicle Data - Illegal/Unauthorised Changes to Vehicle's Electronic ID

Category: Target of an attack on a vehicle

The vehicle identification number is the identifying code for an automobile and serves as the car's fingerprint. A change of this ID could have far reaching implications. On the one hand, wrong software updates could harm the whole system and could introduce several safety related issues. On the other hand, wrong identifier would disguise the real identity of the vehicle in case of car theft. Also, the creation of spare keys to gain physically access to the car after sniffing the cars identity number is aligned to this threat.

3.3 Manipulate Vehicle Data - Identity Fraud

Category: Target of an attack on a vehicle

This attack is performed by using the identity of e.g. the automotive service station ID without authorization to manipulate the setup of the vehicles Engine Control Unit (ECU).

3.4 Manipulate Vehicle Data - Circumvent Monitoring Systems

Category: Target of an attack on a vehicle

The "In Vehicle Monitoring System" enables the owner of the car or a third party to track the vehicle's location by collecting time-spatial data. This feature normally can be divided into active and semi-passive tracking. When a cellular network is available the tracking device will connect and transmits data to a server. Otherwise the data will be stored internally and will be transmitted to the server later when the network becomes available again. In case of a stolen car the attacker may manipulate this data to hide the exact location of the car. Also, other attacks denying the presence of the car and the driver at a certain time and place could be the aim of such a manipulation.

In addition, the monitoring data reflects the driver's behaviour and can record sudden braking or harsh acceleration and speeding which might influence the insurance premiums. Besides that, the reduction of incidents on the road by controlling speed limits would also be influenced by such an attack.

3.5 Manipulate Vehicle Data - Manipulation of Driving Data

Category: Target of an attack on a vehicle

Driving data is generated based on operations performed by the driver of the vehicle. An attacker might change this data to get better insurance premiums, e.g. Pay-How-You-Drive. Since this data consist of geographic information, user behaviour and technical information about the car, an attacker who tries to manipulate the monitoring systems or the diagnostic data have to manipulate this dataset as well to blur their attack.

3.6 Manipulate Vehicle Data - Diagnostic Data

Category: Target of an attack on a vehicle

Valid diagnostic data is a crucial point to be able to track problems of the specific car as early as possible. It could also affect the development process if serious faults are detected which have to be eliminated during the production. The aim of an attack could be to hurt a specific person by not reporting correct diagnostic values and causing an accident, or to harm the car manufacturer.

3.7 Attack on Network - Vehicle Acting as a Botnet

Category: SmartHub used as a means to propagate an attack

A botnet is a collection of internet-connected devices. Each of these devices is running malicious software which can be triggered to run a collaborative attack (e.g. Distributed Denial of Service (DDoS)) against another internet device.

3.8 Extract Data/Code - Unauthorized Access to Privacy Information

Category: Target of an attack on a vehicle

Based on the data collected a detailed driver profiling might be possible. Depending on the information collected by vehicle especially a combination of time, location and the direction of movement could comprise information about friends, co-workers and relatives. Information collected by the entertainment system and the hands-free car kit could reflect the stress level or the physical condition of the driver.

3.9 Cause Vehicle to Move Out of the Lane

Category: Spoofing

Either physically by sending raw camera data to the target sensor or via manipulation of the cameras e.g. printing out a fake image.

3.10 Prevent Vehicle from Unintended Steering

Category: Spoofing

Spoofing the Environment in order to prevent car from steering when it should - potentially causing a crash.

3.11 Manipulate Data in Transit to the Targeted Process Causing Vehicle to React Differently

Category: Tampering

The attack might occur by physically connecting directly onto the network or remotely interfering with the targeted process in order to modify data in transit, e.g. by modifying a V2X packet to introduce an imminent threat could cause the car to perform an emergency brake.

3.12 Updates Downloaded from a Web Server Resulting in Disclosure of Sensitive Information

Category: Information Disclosure

Reverse engineer the head unit firmware to find information about the update server and download software update files which may contain sensitive information.

3.13 Sensor Flooding

Category: Denial of Service

Sensors can be flooded with invalid data to cause denial of service, which might lead to a breakdown of the vehicle causing a traffic incident.

3.14 Elevation of Privilege by Flashing Custom Firmware

Category: Elevation of Privilege

Elevation of privileges in order to exploit the targeted process. Flash Custom Firmware onto the targeted process in Order to Fully Control the Module.

4. The Role of Localization Techniques for Safety

Section 2 of the report **D5.4.1 "Identity, Security and Safety in Product Lifecycle Data Management"** discusses cybersecurity features in PLCDM. It highlights the importance of periodical checks and cybersecurity validations for verifying the integrity of the as a way of ensuring that desired security and safety postures of the system remain in place. In this section, we discuss the importance of verifying the physical position of the elements within a Cyber-Physical System (CPS), alongside with their identity (note that the identity as a topic is discussed in D5.4.1). To start with an example, we consider a sensor system (as a part of a CPS) that is used to measure a physical variable in an experiment (e.g., the air flow in an exhaustion system). If the sensors are not placed correctly, the measurements obtained by the sensor system could be compromised. For example, the identity of sensors could be established correctly, even if they do not operate at their intended location, which may be caused by mechanical collisions, vibrations, or even sabotages or malicious conducts. In safety-critical systems, a wrong setup can lead to injuries or fatalities. A desirable feature in such systems would be the system's ability to perform self-checks (similarly to identity checks) in order to confirm its physical integrity, and if the physical integrity cannot be verified, certain countermeasures should take an action e.g. switching into a safe state, immediate stopping of the system or raising an alert for maintenance. The self-checks procedures may in many cases not be practical due to the use of physical contacts, especially in wireless (and dynamic) systems, or systems implemented in large areas. The promising solution could be to implement wireless localization technologies that can support certain requirements regarding accuracy, precision and resilience of systems.

A recent review of suitable technologies for real time localization systems shown that Ultra-WideBand (UWB) is the most efficient wireless localization technique (Halawa et al., 2020). The study provided by (Halawa et al., 2020) considers a Time-of-Flight (ToF) based UWB system, which calculates the position of tags based on their distance estimations to a set of anchors warehouses. UWB is shown to be useful for the identification of human poses, too (Bazo et al., 2020). This is particularly relevant for applications requiring the identification of people, enabling a double-check in existing systems, in addition to biometrical or badge-based identification. Likewise, the authors in (Arsan and Kepez, 2017) evaluate the use of WIFI, UWB and Bluetooth Low Energy (BLE), as technologies to implement Behaviour Mapping, a technique which enables to understand the interactions among humans and between humans and the environment, both based on a position of humans. These technologies are based on traditional mechanisms e.g., Received Signal Strength-based for WIFI and BLE, and ToF for UWB. The latter proved to be suitable for automated behaviour mapping due to its accuracy.

Another application scenario for the above-mentioned localization technologies is automated driving. Within such a scenario**, indoor localization technologies** can be used to estimate a position of vehicles, within tunnels (because GPS is not applicable in such scenarios), as well as to securely localize objects in the surrounding of a vehicle, while increasing road safety in the immediate environment of a vehicle. A number of studies investigate the use of UWB in this context. The authors in (Fang and Ding, 2019) evaluate a UWB-based system for supporting autonomous and safe driving in tunnels. Distance estimations between base-stations (positioned in fixed known coordinates in the environment) and tags (placed on vehicles) are used to enable the localization of the vehicles. The positioning accuracy ranged from 15cm to 18cm which, according to the authors, suffices for the presented use case. The distance between base-stations and the vehicles (tags) for this use case should range between meters to more than 100m, which is the typical range of UWB transceivers.

The problem of localization of pedestrians using a UWB-based infrastructure is investigated in (Ishizuka et al., 2013) and a positioning error of less than 15cm is achieved for pedestrians situated at most 10m apart from any of the base-stations/anchors. The authors in (Zhang et al., 2019) propose a similar system that uses two ToF anchors positioned on the top of the vehicles' rear-view mirrors to localize tags situated in front of the vehicle, at distances up to 50m. The results shown a maximum positioning error of approximately 1m when the tag was 50m away from the car.

Despite all evaluation efforts on the accuracy of localization technologies, there is still an open question on capabilities of these technologies to estimate direction (rather than ranges) of incoming signals. To our knowledge, no study has come up yet with an answer to this question. In this section, we show the results of the analysis of UWB in realistic indoors environments of aforementioned application scenarios. In particular, we focus on analysing Angle-of-AArrival (AoA) estimations (note that these have not been subject to investigation

before) using UWB technology that are affected by multipath and non-line-of-sight, as two common capabilities affecting localization systems in complex environments. Errors in angle estimations due to these phenomena imply errors in position estimations. We evaluate the magnitude of these deviations to estimate the resulting position error. Additionally, we conduct similar experiments using BLE, in order to compare the outcomes of these two technologies. A comparison with WIFI will be explored in our future work.

4.1 Multipath and Non-line-of-sight

Multipath and Non-line-of-sight constitute a challenge for RF-based localization mechanisms. Here we refer to multipath as the existence of multiple alternative paths of a signal transmitted by a specific transmitter, reaching a receiver. Other than the signal received via the direct straight line that connects the transmitter and the receiver, multipath is caused by reflections from objects in the environment. It can cause destructive interference in the received signal, which usually distorts localization estimations (both for distance and angle). For technologies using short (ns) pulses, or equivalently wide frequency bandwidths, such as UWB, the different paths, which have different absolute path lengths in comparison to the first path (FP), can introduce enough time delays in multipath signals in such a way that the FP signal and the multipath signals do not interfere with each other (Decawave, 2017). This makes UWB more robust to multipath in comparison to BLE, which is narrowband (UWB uses a 499.2 MHz bandwidth for channels 1,2,3 and 5 and over 1 GHz for channel 4 and 7, while BLE uses approximately 80 MHz in total). Therefore, for BLE, multipath and FP signals have an increased chance to overlap in time at the receiver. Since they have different phases (due to the different path lengths they had to travel), the signal sampled at the receiver will have a different amplitude and phase than its FP counterpart. Thus, it is difficult to develop accurate distance and angle estimations for narrowband technologies for complex environments.

A different situation occurs when the FP component is obstructed by an obstacle, such as humans, walls or appliances. This situation is commonly referred to as Non-line-of-sight (NLOS) as opposed to direct line-of-sight (LOS). In the case of NLOS, an attenuated version of the FP signal will reach the receiver, while the multipath components can have the same power as before. The attenuation is due to the refraction of an electromagnetic wave passing through the obstacle. For narrowband technologies, such as BLE, the multipath components are likely to dominate the received signal in case of interference (either constructive or destructive). For UWB, the different pulses can still be resolved, but the signals refracted due to obstacles are delayed, in comparison to the LOS ones (Heydariaan et al., 2018). While this is known to insert a positive bias in distance estimations, the effect on directions estimations of obstacles are, to the best of our knowledge, not yet evaluated for this technology. For this reason, we conduct a number of experiments to investigate quality of UWB's AoA estimations and evaluate UWB's potential to accurately estimate the direction of an incoming signal indoors.

4.2 Experiments and Results

We conducted a series of experiments in order to evaluate how the common issues affecting localization technologies, namely NLOS and multipath, distort AoA estimations for UWB. We limited the experiments to placing both receiver (RX) and transmitter (TX) on the same plane (altitude) as the modules used for the experiments feature linear antennas only and are not suitable for 3-dimensional angle estimation. However, it is possible to extrapolate 3-dimensional performance from performance evaluations performed in a 2-dimensional space (Li and Yang, 2015). To extend systems capable of providing 2-dimensional angle estimations to 3-dimensional angle estimations, directional antennas and 2D or 3D antennas can be used (Zhang et al., 2018). Assuming that we have an error-free distance estimation, errors in angle measurements can be translated into errors in position estimations as illustrated in Figure 8.

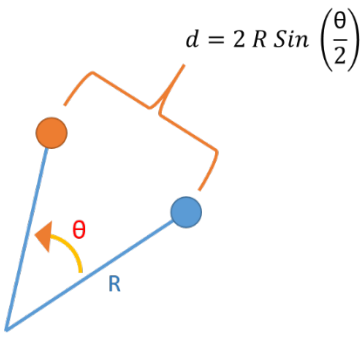


Figure 8 – Effect of an angular error estimation equals theta onto error in position estimation.

A detailed description of the experimental setup is available in the IoT4CPS's D3.7. Here we only briefly introduce the technology and the performed experiments, and analyse the experimental results.

The multipath resilience of UWB was tested in two environments: 1) a classroom and 2) a long hallway. To give the reader an idea on the performed experiment, the classroom setup is depicted in Figure 9, where a transmitter and a receiver were placed in front of one another, without any obstacles in between.

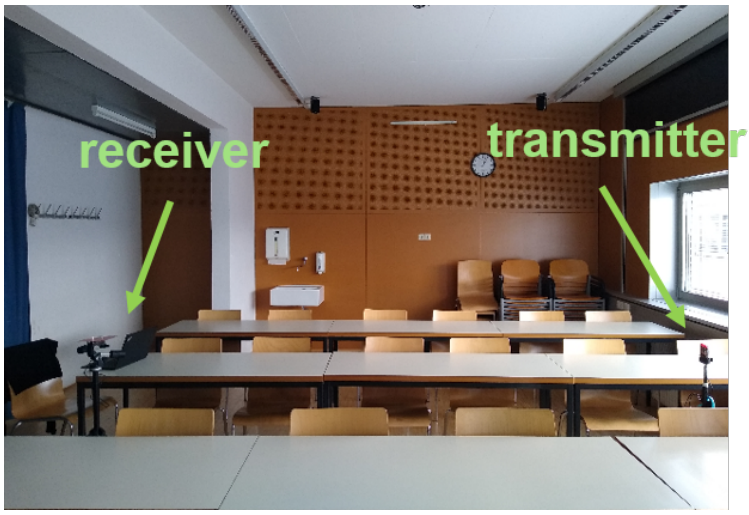


Figure 9 – Experiment setup for measuring angles with UWB in a classroom.

Both a transmitter and a receiver are placed on top of tripods, at a height of 1m from the floor, approximately in the mid of the room and at 3 different distances: 2m, 3m and 4m. A total of 1000 angle estimations is acquired per angle (-90, -60, -30, 0, 30, 60, 90) and distance (2m, 3m and 4m). A constant angle offset is added to all measurements to align the measurement at zero degree with the true zero degree (calibration[1]) using the criteria of least squared errors for the three distances altogether. The results of the experiment are depicted in Figure 10 and show that a distinction between the different angles (depicted in different colours) can be achieved, which corroborates UWB's potential for indoor localization based on AoA estimations. The angles in Figure 10 are shown from -90 degrees up to 90 degrees, in steps of 30 degrees. It can be also seen that the angles closer to 0 degrees are estimated with higher accuracy than the ones near the fire ends (the axis of the antenna array). These results agree with initial experiments of the manufacturer (Decawave, 2018).

[1] Evidently, if this calibration is performed per distance (which is usually the main purpose of using UWB devices) the results can potentially be improved. This constitutes a topic for future investigation.

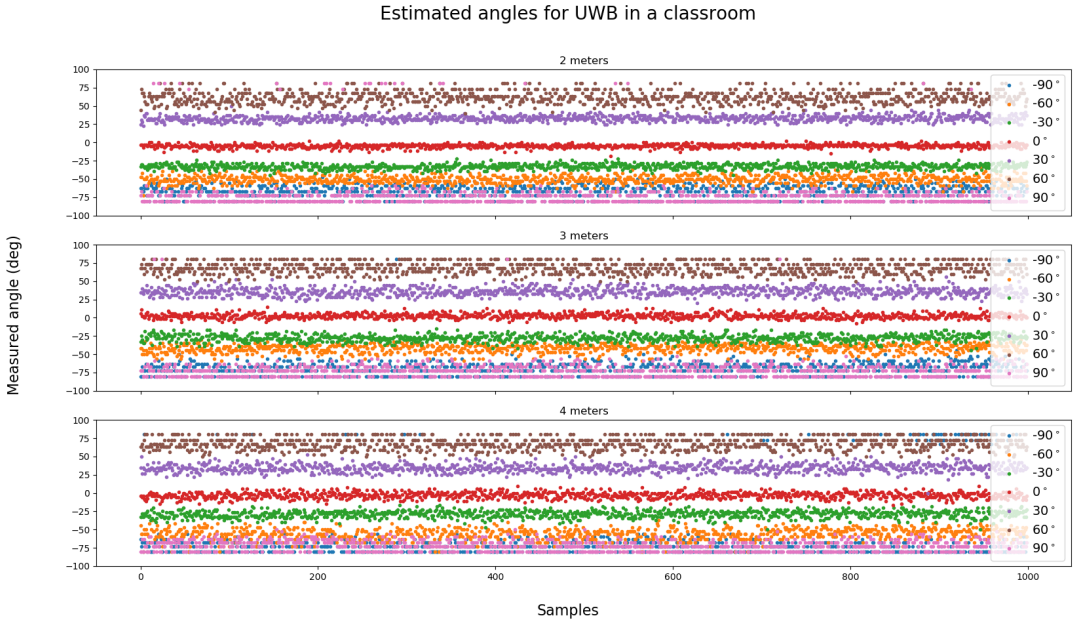


Figure 10 – Angles estimation in a classroom at 3 different distances for UWB with a clear LOS

Each resulting time series (for each distance and angle) is tested for normality by means of the D'Agostino and Pearson's tests, after mapping using a Yeo-Johnson transformation. The normality was additionally checked via boxplots. To put it into numbers, the standard deviation for 0 degree at 2m, 3m and 4m distances is equal to 2.42 degrees, 3.34 degrees and 4.09 degrees, respectively. These errors convert into a position error of 8.4cm, 17.5cm and 28.5cm, respectively. Figure 9 shows this dependence for all the angles measured between -60 degrees and 60 degrees. The remaining angles are affected by the jump over at -90 degrees and 90 degrees occurring to the angles near the fire ends. In this case, the measurement at 90 degrees is estimated at approximately -90 degrees (note the pink dots in the bottom of each of the subplots in Figure 10). At lower angles, the estimations look accurate as we can clearly distinguish angles that are 30 degrees apart.

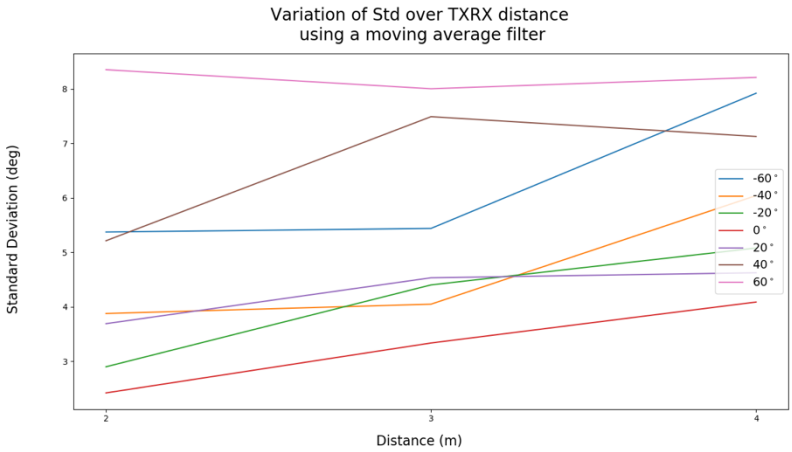


Figure 11 – Standard deviation plotted over distance between TX and RX

Angles in Figure 11, close to the fire ends, are removed as they are strongly impacted by the jump over at -90 and +90 degrees. Figure 11 shows that in most of the cases there is a positive linear relationship between distance and standard deviation. This is caused by multipath reflections from the floor, which get more accentuated as the distance between modules increases. This hypothesis will still be tested by repeating this experiment with both TX and RX at a higher altitude (distance from the floor).

It is possible to increase this accuracy by, for instance, averaging multiple samples, which can be achieved by using a moving average filter, when the distributions are Gaussian. Such increased accuracy comes with a trade-off, as each resulting sample requires more time and energy to be computed. Let's suppose that we aim to achieve an update rate of 100 measurements per second, with a maximum standard deviation that equals 2.49m, as shown in Figure 12.

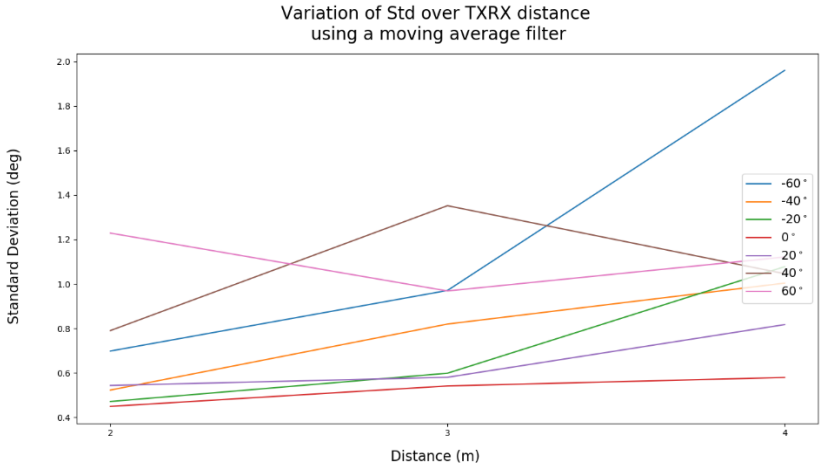


Figure 12 – Standard deviation over distance averaged over 65 samples

From the above figure, we can see the standard deviations are reduced after filtering, which results in more accurate estimations.

In the next experiment, the environment is changed to a long and narrow hallway, and the angles are estimated under LOS by the UWB receiver when rotated by -30, 0 and 30 degrees at a distance of 10m from the transmitter. The idea is to understand the influence of the environment on the direction estimation. In this experiment, the RX is not recalibrated. The results are shown in Figure 13 in which a bar chart highlights the approximately fixed bias affecting the mean, i.e., the precision of the estimations.

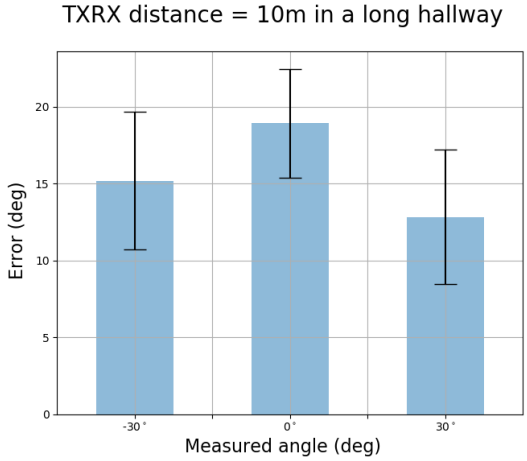


Figure 13 – Bar chart showing mean error and standard deviation of angle measurements

Although the mean errors are quite high, they are biased in the same direction (not shown in Figure 13). If this bias is removed, a precision below 5 degrees is achieved for the three angles measured. These results are more accurate for the three angles measured than the ones obtained in the classroom at 4m. Therefore, we can conclude that the geometry of the environment is critical for the accuracy of the angle estimations.

In the following, the impact of inserting obstacles in between TX and RX, has been evaluated. We set two different obstacles: a perfect absorber and an average sized human. The results of the experiment are shown in Figure 14.

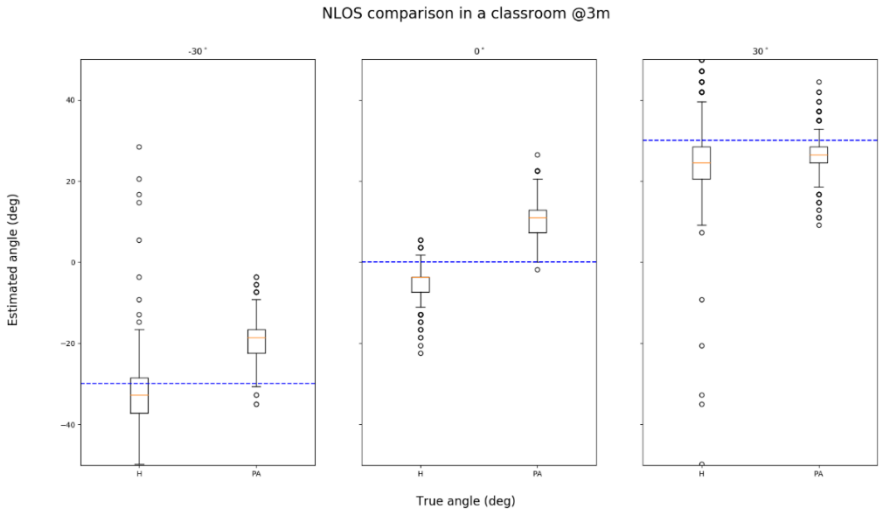


Figure 14 – Boxplots of angle estimations in a classroom with two different obstacles measured at 3 ground truth angles

In Figure 14, H states for Human (left side at each subplot) and PA states for Perfect Absorber (right side at each subplot). The obstacle is positioned exactly in between the two modules, i.e., at 1.5m of either the TX or RX. In overall, a human obstacle leads to more outliers than the perfect absorber, which is unexpected. This could be possibly caused by imperfections in the perfect absorber, meaning that the LOS is only partially blocked (Obstructed LOS). In both cases, UWB seems to be resilient to Obstructed LOS, as the mean is still close from the target mean and the standard deviation is also narrow.

The last experiment combines strong multipath reflections, expected from the long hallway, to the obstacles introduced in the former experiment. The results are shown in Figure 15.

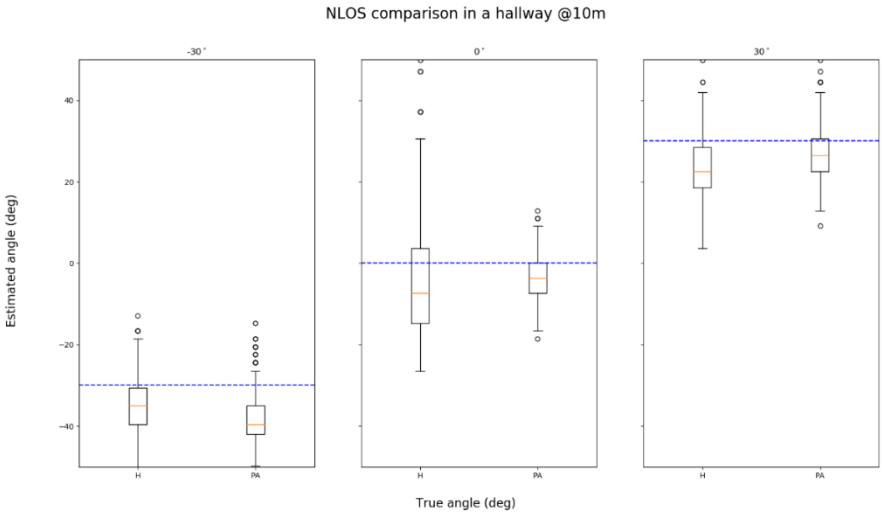


Figure 15 – Boxplots of angle estimations in a long hallway with two different obstacles measured at 3 ground truth angles

The higher quantity of outliers observed in Figure 11 is more accentuated in the latest experiment at 0 degrees. Even in this scenario, the distribution of samples stays close to the true mean and has a worst-case standard deviation that equals 13.45 degrees.

A comparison between **Error! Reference source not found.** and Figure 15 leads to the conclusion that regardless of the environment, UWB is very resilient to NLOS, at the distances and obstacles used.

4.3 Discussion of the results

To our knowledge, this is the first evaluation of the commercial UWB transceivers that support AoA estimations. The results show that a decimetre positioning accuracy at the current state of the technology is still not possible. In some situations, a standard deviation higher than 10 degrees is observed. Although this has been shown to be fixable by averaging samples, there is still an issue regarding the fixed mean offset affecting the core estimations. The drawbacks of using a moving average filter should not be relevant when dealing with the localization of main lines supplied devices. In a single-anchor localization system, in which the anchor performs distance and angle estimations to localize the tags, e.g. 10 degrees and no distance estimation error, could lead to a positioning error of 17.4cm, if the tag is positioned 1m away from the anchor, and an error of 52.3cm, if the tag is positioned 3m away from the anchor.

4.3.1 Implications of the evaluation results on the autonomous driving use cases

Due to the linear increase of positioning error over distance from the anchor, our evaluation shows that the AoA method is currently not suitable to be used in tunnels, due to the positioning error greater than the one obtained in (Fang and Ding, 2019).

Regarding the applicability for localization of pedestrians, the positioning errors are shown to be greater than those achieved in (Ishizuka et al., 2013). A more efficient approach could be to eliminate the infrastructure and localize the pedestrians by using an anchor placed in (or on the top of) the vehicles. Considering an average-sized car with length that equals 4.5m and a base-station positioned in the middle of it, the system can be helpful in avoiding collisions with pedestrians located 3m apart from the vehicle's center even with a positioning errors in the range of 50cm.

Finally, through the comparison of our results with those obtained in (Zhang et al., 2019), although we haven't evaluated the angular error at the same distances, and by considering the standard deviation observed in our experiments and measured at 0 degrees with LOS to be less than 0.6 degree, our obtained positioning error is approximately 52cm, which can be considered as an improvement of the proposed localization technology.

5. Standards, Regulation and Frameworks for Security, Privacy, Trust and Ethics for CAM Applications

The recent advancements of smart vehicles are largely based on the advanced hardware and software technologies, while many of them are still awaiting to be regulated with regard to their trustworthiness, responsible design and ethical decisions. Smart vehicles operate side by side with a variety of stakeholders (drivers, passengers, pedestrians on the roads) and within complex environments of smart cities, smart homes, smart factories, etc. thus requiring for their operational services to be fully synchronized to avoid harmful and fatal situations and ensure secure and safety conditions, privacy controls and trust.

The latest WP.29 UN cybersecurity regulation, published in June 2020 on the United Nations Economic Commission for Europe (UNECE)/WP.29' website (http://www.unece.org/?id=54667), becomes the first international regulation that mandates cybersecurity in connected and autonomous vehicles. The WP.29 regulation outlines new processes and technology that manufacturers must adopt to achieve vehicle type approval with regards to cybersecurity, safety, and environmental protection. For example, the vehicles must be able to perform 3 key functions to achieve cybersecurity type approval: (i) to detect and prevent attacks, (ii) support the monitoring capability of the vehicle manufacturer with regard to detecting threats, vulnerabilities and attacks, and (iii) support forensic analysis and audit.

The cybersecurity measures related to the privacy issues for smart vehicles includes the following steps:

- Firstly, to prevent privacy issues, privacy related regulations need to be applied, e.g. the recent EU General Data Protection Regulation (GDPR) that officially went into effect in May 2018;
- Secondly, to identify privacy related risks and define appropriate countermeasures to mitigate risks, Privacy Impact Assessment (PIA) (or Data Privacy Impact Assessment (DPIA)) need to be conducted (see: https://gdpr-info.eu/issues/privacy-impact-assessment/);
- Thirdly, to ensure compliance with privacy policies, Privacy Audits need to be performed along the smart vehicle's lifecycle (from the design and development of the car to its operation and maintenance phase).

The Article 29 Working party in GDPR (see: https://gdpr-info.eu/art-29-gdpr/) created a catalogue of criteria which indicate that the data processing bears a high risk to the rights and freedoms of a natural person, thus requiring DPIA to be performed periodically in case of:

- evaluation or scoring the data about the users' activities,
- automated decision which lead to legal consequences for those impacted,
- systematic monitoring/ tracking,
- processing of special personal data (sensitive data), e.g. medical data,
- data processing on a large scale,
- matching or combining datasets,
- data concerning vulnerable data subjects, e.g. ill persons, elderly, etc.

Apart GDPR, the European Telecommunications Standards Institute (ETSI) developed a set of technical specifications, ETSI TS 102 940 to ETSI TS 102 943 Intelligent Transport System (ITS) security architecture along with services specification to ensure information confidentiality and prevent unauthorized access to ITS services. ETSI TS 102 941 V1.2.1 also addresses the trust and privacy management for ITS communications (ETSI-102-941, 2018). For example, the ISO/IEC 15408-2: *"Information technology - Security techniques - Evaluation criteria for IT security; Part 2: Security functional components"* identifies 4 key attributes that relate to privacy:

- **Anonymity** – this is alone insufficient for protection of a user's privacy and unsuitable as a solution to provide improved safety;
- **Pseudonymity** – this ensures that an ITS may use a resource or service without disclosing its identity but can still be accountable for that use. It can be provided by using temporary identifiers in ITS safety messages;

- **Unlinkability** – it ensures that an ITS may make multiple uses of resources or services without others being able to link them together. It can be achieved by limiting the amount of detailed immutable (or slowly changing) information carried in the ITS safety message;
- **Unobservability** – this is about undetectable actions of either sender or recipient.

ITS privacy includes two dimensions: (i) privacy of registration and authorization tickets provisioning, and (ii) privacy of communication between ITSs.

With regards to trust in IoT and CPS applications, there is a large body of trust algorithms proposed for the sensor networks and distributed applications that can be used to calculate trust of IoT systems. There is also a large body of trust management protocols for IoT systems, e.g. the study in (Chen et al., 2011) shows a trust management model called TRM-IoT, that is based on fuzzy reputation for IoT systems; the study in (Saied et al., 2013) proposes a context-aware and multiservice approach for trust management in IoT systems against malicious attacks. The authors in (Bao and Chen, 2012) present a trust management protocol that uses both direct observations and indirect recommendations to update trust in IoT systems. The authors in (Nitti et al., 2014) consider social relationships of owners of IoT devices for trust management in social IoT systems. In addition, the Online Trust Alliance (OTA) designed the IoT Trust Framework® with a set of strategic principles that are necessary to secure IoT devices and their data when shipped and throughout their entire lifecycle (OTA, 2018). The Framework is available at https://otalliance.org/IoT and includes four key areas:

- **Security Principles** – these principles should be applicable to any device or sensor and all applications and back-end cloud services, including the applications for supply chain management, penetration testing and vulnerability reporting programs;
- **User Access & Credentials** – Requirement for encryption of all passwords and user names, shipment of devices with unique passwords, implementation of generally accepted password reset processes and integration of mechanisms to help prevent "brute force" login attempts;
- **Privacy, Disclosures & Transparency** – Requirements consistent with generally accepted privacy principles, including prominent disclosures on packaging, point of sale and/or posted online, capability for users to have the ability to reset devices to factory settings, etc.;
- **Notifications & Related Best Practices** – Requirements for email authentication for security notifications, accessibility requirements, etc.

Ethics is not in the core focus of the IoT4CPS project, although it can be seen as a trust enabler of automated cars, and vice versa. (Lin, 2014) presents a simple scenario of the self-driving car's ethical dilemma: "*to either swerve left and strike an eight-year old girl, or swerve right and strike an 80-year old grandmother*." According to IEEE code of ethics, making decision based on age of a girl or a grandmother is considered to be an act of discrimination: "*to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression"* (IEEE Ethics, 2014). In 2016, the authors in (Lin, 2016) present several other examples of ethical dilemmas involving sacrifice of animals on the road, self-sacrifice, and more. In March 2018, the first incident happened when a person is killed by a self-driving car operated by Uber, in Arizona (Cameron & Martinez, 2019).

The authors in (Lin, 2016) conclude that in smart vehicles' scenarios, an accident may be unavoidable due to many factors: technology errors, misaligned sensors, malicious actors, bad weather, bad luck. According to various traffic safety administrations (e.g. the National Highway Traffic Safety Administration as discussed in (Cameron & Martinez, 2019)), the top three causes of car accidents are still: (1) distracted driving, (2) speeding, and (3) drunk driving, all caused by human errors.

Smart vehicles reduce accidents caused by human errors, although when it comes to safety-critical decisions, a certain level of risk related to making the right decision (will) remain open. The authors in (Birnbacher & Birnbacher, 2017) stress that in no case should the ethical algorithms be put in practice as non-transparent black boxes. The built-in norms should, as far as possible, be understood and commonly shared. With this, crash-

optimization strategies with a view on ethics need to become an integral part of automated cars and their controlling algorithms. For example, researchers from the University of Sao Paulo, Brazil propose a module, the Autonomous Vehicle Control (AVC) module that is independent from the vehicle's manufactured system (Molina et al., 2017). The AVC module should be tested for industry safety standards across the board, no matter how the car is designed by a manufacturer. (Whalen et al., 2016) presents the results of the High-Assurance Cyber Military Systems (HACMS) project funded by DARPA, the Air Force Research Laboratory and NASA, on constructing complex networked-vehicle software to secure all manner of military vehicles. The authors present an automatically generated assurance case tree for an unmanned air vehicle (UAV) that executes only unmodified commands from the ground station. The authors in (Lin et al., 2017) discuss a vehicle detector that creates a grid around a vehicle, called a "bounding box". Within that grid, the vehicle can detect all vehicles, whether hidden or in plain view, based on a library of vehicle training images. This work, when compared to other classical object detectors, achieves competitive results with 85.32 average precision (AP). With such a high precision, many current technology advancements around smart vehicles can be seen as mechanisms contributing to future ethics enforcement.

Finally, the current and emerging standards related to AI and robotics require building a stronger link with the CAM technical requirements and ethics. In June 2018, the European High Level Expert Group (HLEG) on AI created the "Ethics Guidelines on Artificial Intelligence" putting forward a human-centric approach on AI and emphasizing 7 key requirements that AI system should meet in order to be trustworthy (see: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top). These requirements are recently implemented as an online tool "Assessment List for Trustworthy AI" (ALTAI) (see: https://altai.insight-centre.org/) that is designed to help organizations to self-assess the trustworthiness of their AI systems under development (published in August 2020).

6. Conclusion

Standardized and regulated approaches to security, safety, privacy and trust are seen as the greatest obstacles to further growth of the IoT and CPS systems, affecting the evolution of smart vehicles and future CAM applications. The current security mechanisms in smart vehicles perform continuous tracking of vehicles for road safety purposes, thus requiring privacy and security features to be adequately addressed, e.g. through pseudonymization of messages for long and short term (authorization ticket) certificates, and more. The public is empowered by the current privacy regulations to know what sensitive data is collected, about who, and where it is stored and for how long, and how the data is used and shared. Hence, transparency laws and guidelines on the use of advanced technologies are necessary and emerging, e.g. the "Ethics Guidelines for Trustworthy Artificial Intelligence" (HLEG, 2019). At the same time, a set of obstacles can be identified in relation to the transparency paradox of hardware and software technologies in CAM applications; for example, CAM applications may include patented technology and protected algorithms that prevent the transparency of methods and open the door for privacy risks, fairness and bias in decision making.

Many European countries have already laws in place for the testing of autonomous vehicles on roads. Many automotive companies, including vehicle renting services, offer privacy checklists when selling or renting smart vehicles to customers. These lists strongly suggest removing private and sensitive data, e.g. phone and address book, navigational data to favourite locations, home, friend's home, work, mobile applications with the data exchanged during the drive, garage door programming, dongles that may share data with third parties, etc. Other approaches to protecting privacy follow Privacy by Design (PbD), GDPR, Privacy Impact Assessment (PIA), or design "notice and choice" systems that can guide users through privacy settings wizards, or send warnings to the users as a flashing light or flashing icons to show different levels of risk, or offer other automated ways for the users to check their privacy data status.

The aim of this report is to explore the security and safety implications related to both multi-stakeholder and IoT-/ CPS-based assets (and their services) along lifecycle phases of CAM applications. The predecessor D5.4.1 report highlights the importance of periodical checks and cybersecurity validations for verifying the integrity of the system and ensuring that desired security and safety postures of the system remain in place. This report explores the role of wireless localization systems for stakeholders and assets along lifecycle phases, with the aim to provide additional conformity assessment of sensor locations. For example, wireless malicious conduct over CAM applications could be proven through the use of localization systems, even in situations when the identity of sensors is shown to be established correctly. Thus, D5.4.2 explores the methods to address safety issues in the project by estimating the direction (rather than a range) of incoming signals from smart vehicle's sensors. The presented experimentation with localisation methods is performed in realistic indoors environments, and placed in the context of CAM scenarios.

Apart from digital identity, privacy, security and safety in the Automotive Industry, trust and ethics are considered as additional concerns for authorities, governance bodies, manufacturers and the public alike. Although trust and ethics are not at the core of IoT4CPS, this report touches upon certain risks related to making the right decisions and emphasizes the need for optimization strategies that should become a part of automated cars and their advanced controlling algorithms. The results of the analysis provided in D5.4.1 and D5.4.2 (as outcomes of task T5.4) serve as a basis for the design and implementation of the Digital Twin prototype in task T5.5. The design of such a prototype requires not only an effective data strategy and methods to be put in place; it also requires balancing regulatory issues at national and international levels and building a strong data governance framework that can provide the traceability of the events along the entire lifecycle and supply chain involved in CAM applications. Although CAM technologies are still developing, including connected cars, traffic signals, road infrastructure with the ability to recognize risks and respond to them accordingly, understanding certain risks related to trust, ethics and legal issues are key to ensure greater safety. This is also reflected through the recent trends towards **assisting intelligence**, placing "humans in the loop" for the final decisions while requiring constant human input and intervention (Russell, 2020).

7. References

(Abadi et al., 2005) M. Abadi, M. Budiu, U. Erlingsson, and J. Ligatti, “Control- flow integrity,” in Proceedings of the 12th ACM conference on Computer and communications security. ACM, 2005, pp. 340–353.

(Amoozadeh et al., 2015) M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” IEEE Communications Magazine, vol. 53, no. 6, pp. 126–132, 2015.

(Arsan and Kepez, 2017) Arsan, T.; Kepez, O. Early Steps in Automated Behaviour Mapping via Indoor Sensors. Sensors 2017, 17, 2925.

(Bao and Chen, 2012) F. Bao, and I. R. Chen, “Dynamic Trust Management for Internet of Things Applications,” 2012 International Workshop on Self-Aware Internet of Things, San Jose, California, USA, September 2012.

(Bazo et al., 2020) Rodrigo Bazo, Eduardo Reis, Lucas Adams Seewald, Vinicius Facco Rodrigues, Cristiano André da Costa, Luiz Gonzaga, Rodolfo Stoffel Antunes, Rodrigo da Rosa Righi, Andreas Maier, Björn Eskofier, Rebecca Fahrig, Tim Horz, Baptizo: A sensor fusion based model for tracking the identity of human poses, Information Fusion, Volume 62, 2020, Pages 1-13, ISSN 1566-2535,

(Birnbacher & Birnbacher, 2017) D. Birnbacher and W. Birnbacher, "Fully Autonomous Driving: Where Technology and Ethics Meet" in IEEE Intelligent Systems, vol. 32, no. 05, pp. 3-4, 2017. doi: 10.1109/MIS.2017.3711644

(BMVIT, 2019) BMVIT (2019). “Austrian Action Programme on Automated Mobility”. Online available from: https://www.bmvit.gv.at/en/service/publications/downloads/action_automated_mobility_2019-2022_ua.pdf

(Cameron & Martinez, 2019) L. Cameron and M. Martinez, 2019. "Ethics, Safety, And Software Behind Self-Driving Cars In The Aftermath Of First Pedestrian Killed". Online: https://www.computer.org/publications/tech-news/trends/ethics-safety-and-software-behind-self-driving-cars-in-the-aftermath-of-first-pedestrian-killed

(CAR2CAR, 2018) CAR 2 CAR Communication Consortium - FAQ regarding Data Protection in C-ITS v1,0,0 : https://www.car-2-car.org/service/privacy/

(Castro et al., 2006) M. Castro, M. Costa, and T. Harris, “Securing software by enforcing data-flow integrity,” in Proceedings of the 7th symposium on Operating systems design and implementation. USENIX Association, 2006, pp. 147–160.

(Chen et al., 2011) D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things,” Computer Science and Information Systems, vol. 8, no. 4, Oct. 2011, pp. 1207-1228.

(Clause et al., 2007) J. Clause, W. Li, and A. Orso, “Dytan: a generic dynamic taint analysis framework,” in Proceedings of the 2007 international symposium on Software testing and analysis. ACM, 2007, pp. 196–206.

(Cognilytica, 2020) Worldwide AI Laws and Regulations [CGR-REG20], Feb 2020. Online: https://www.cognilytica.com/download/worldwide-ai-laws-and-regulations-cgr-reg20/

(Corradini, 2016) Corradini C., The automotive threat modeling template. URL https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/july/the-automotive-threat-modeling-template/

(Dagan et al., 2004) E. Dagan, O. Mano, G. P. Stein, and A. Shashua, “Forward collision warning with a single camera,” in IEEE Intelligent Vehicles Symposium, 2004, pp. 37–42.

(David & Fry, 2016) C. David and S. Fry. (2016) Automotive security best practices. Recommendations for security and privacy in the era of the next-generation car. Online available: https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf

(Decawave, 2017) I. Dotlic, A. Connell, H. Ma, J. Clancy and M. McLaughlin, "Angle of arrival estimation using decawave DW1000 integrated circuits," 2017 14th Workshop on Positioning, Navigation and Communications (WPNC), Bremen, 2017, pp. 1-6, doi: 10.1109/WPNC.2017.8250079.

(Decawave, 2018) Beta pdoa kit user manual v1.0.” Decawave, 2018.

(Deng et al., 2017) L. Deng, J. Offutt, P. Ammann, and N. Mirzaei, “Mutation operators for testing android apps,” Information and Software Technology, vol. 81, pp. 154–168, 2017.

(DIBA, 2020) M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, S. Yu, “Attacks and defences on intelligent connected vehicles: A survey”, Digital Communications and Networks(2020), doi: https://doi.org/10.1016/j.dcan.2020.04.007.

(Ding et al., 2017) R. Ding, C. Qian, C. Song, B. Harris, T. Kim, and W. Lee, “Efficient protection of path-sensitive control security,” in 26th USENIX Security Symposium (USENIX Security 17). Vancouver, BC: USENIX Association, 2017, pp. 131–148.

(Dong and Hu, 2013) Y. Dong and Z. Hu, “Driver inattention monitoring system for intelligent vehicles,” in Transportation Technologies for Sustainability. Springer, 2013, pp. 395–421.

(ECAI, 2020) “White Paper on Artificial Intelligence – A European Approach to Excellence and Trust”. Online: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

(ENISA, 2016) ENISA (2016). Cyber Security and Resilience of Smart Cars: Good Practices and Recommendations.

(ENISA, 2019) ENISA Good Practices for Security of Smart Cars. Nov. 2019. Online available: https://www.enisa.europa.eu/publications/smart-cars

(ETSI-102-941, 2018) ETSI TS 102 941 V1.2.1 “Intelligent Transport Systems, Security, Trust & Privacy Management”. https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

(Fan et al., 2016) Y. Fan, Y. Ye, and L. Chen, “Malicious sequential pattern mining for automatic malware detection,” Expert Systems with Applications, vol. 52, pp. 16–25, 2016.

(Fang and Ding, 2019) F. Fang and Z. Ding, "High Precision Positioning and Accident Detection System for Vehicles in Traffic Tunnel," 2019 IEEE 2nd International Conference on Electronic Information and Communication Technology (ICEICT), Harbin, China, 2019, pp. 419-425, doi: 10.1109/ICEICT.2019.8846435.

(FPF, 2018) FPF (2018). Personal Data in Your Car. National Automobile Dealers Association and the Future of Privacy Forum. Online available: https://www.nada.org/personaldatainyourcar/

(Godefroid et al., 2008) P. Godefroid, M. Y. Levin, D. A. Molnar et al., “Automated white box fuzz testing.” in NDSS, vol. 8, 2008, pp. 151–166.

(Grieco et al., 2016) G. Grieco, G. L. Grinblat, L. Uzal, S. Rawat, J. Feist, and L. Mounier, “Toward large-scale vulnerability discovery using machine learning,” in Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. ACM, 2016, pp. 85–96.

(Halawa et al., 2020) Farouq Halawa, Husam Dauod, In Gyu Lee, Yinglei Li, Sang Won Yoon, Sung Hoon Chung, Introduction of a real time location system to enhance the warehouse safety and operational efficiency, International Journal of Production Economics, Volume 224, 2020, 107541, ISSN 0925-5273

(Heydariaan et al., 2018) M. Heydariaan, H. Mohammadmoradi and O. Gnawali, "Toward Standard Non-Line-of-Sight Benchmarking of Ultra-Wideband Radio-Based Localization," 2018 IEEE Workshop on Benchmarking Cyber-Physical Networks and Systems (CPSBench), Porto, 2018, pp. 19-24, doi: 10.1109/CPSBench.2018.00010

(Hitachi Systems Security, 2019) Hitachi Systems Security (2019). “Smart Car Security Threats: Is the Connected Car a Good Idea?”. Online available: https://www.hitachi-systems-security.com/blog/smart-car-security-threats-is-the-connected-car-a-good-idea/

(HLEG, 2019) High Level Expert Group (HLEG) on AI presented in April 2019, “Ethics Guidelines for Trustworthy Artificial Intelligence”. Online available from: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

(Huda et al., 2016) S. Huda, J. Abawajy, M. Alazab, M. Abdollalihian, R. Islam, and J. Yearwood, “Hybrids of support vector machine wrapper and filter-based framework for malware detection,” Future Generation Computer Systems, vol. 55, pp. 376–390, 2016.

(Huda et al., 2017) Huda, S., Miah, S., Mehedi Hassan, M., Islam, R., Yearwood, J., Alrubaian, M., & Almogren, A. “Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabelled data,” Information Sciences, 379, 211-228. https://doi.org/10.1016/j.ins.2016.09.041

(IEEE Ethics, 2014) IEEE: IEEE code of ethics. http://www.ieee.org/about/corporate/governance/p7-8.html (2014).

(IoT4CPS D3.3, 2019) IoT4CPS D3.3 “Guidelines and recommendations for resilient system architecture pattern and concepts and HW-based solutions for safe & secure IoT”; see: https://iot4cps.at/wp-content/uploads/2019/07/IoT4CPS_D3.3_1.0.pdf

(Ishizuka et al., 2013) K. Ishizuka, K. Ohno and M. Itami, "A study on UWB positioning system for the safety of pedestrians," 16th International IEEE Conference on Intelligent Transportation Systems (ITSC 2013), The Hague, 2013, pp. 2445-2450, doi: 10.1109/ITSC.2013.6728593.

(Johnson, 2008) D. G. Johnson, “Development of a high resolution MMW radar employing an antenna with combined frequency and mechanical scanning,” in IEEE Radar Conference (RADAR’08), 2008, pp. 1–5.

(Keen Sec Lab, 2018) Keen Security Lab, 2018. “Experimental Security Assessment of BMW Cars: A Summary Report” https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

(Khurshid et al., 2003) S. Khurshid, C. S. Pasareanu, and W. Visser, “Generalized symbolic execution for model checking and testing,” in International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Springer, 2003, pp. 553– 568.

(Kumar et al., 2018) A. D. Kumar, K. N. R. Chebrolu, S. KP et al., “A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities,” arXiv preprint arXiv:1810.04144, 2018.

(Levine, 2019) S.Levine, Satellite Finance, (2019).“Rising Worries about Connected Car Security Shifts M&A into Higher Gear”. Online available: https://www.satellitefinance.com/insights/rising-worries-about-connected-car-security-shifts-ma-higher-gear

(Li and Yang, 2015) X. Li and S. Yang, "The indoor real-time 3D localization algorithm using UWB," *2015 International Conference on Advanced Mechatronic Systems (ICAMechS)*, Beijing, 2015, pp. 337-342, doi: 10.1109/ICAMechS.2015.7287085.

(Li et al., 2018) Z. Li, D. Zou, S. Xu, X. Ou, H. Jin, S. Wang, Z. Deng, and Y. Zhong, “Vuldeepecker: A deep learning-based system for vulnerability detection,” arXiv preprint arXiv:1801.01681, 2018

(Lin et al., 2017) C. Lin, P. S. Santoso, S. Chen, H. Lin and S. Lai, "Fast Vehicle Detector for Autonomous Driving," 2017 IEEE International Conference on Computer Vision Workshops (ICCVW), Venice, 2017, pp. 222-229, doi: 10.1109/ICCVW.2017.35.

(Lin et al., 2018) D. Lin, J. Zhang, W. Luo, L. Pan, A. Xiang, O. De Vel, and P. Mont, “Cross-project transfer representation learning for vulnerable function discovery,” IEEE Transactions on Indus- trial Informatics, 2018.

(Lin, 2014) Lin, P.: Ethics and autonomous cars: why ethics matters, and how to think about it. Lecture presented at Daimler and Benz Foundation’s Villa Ladenburg Project, Monterey, California, 21 February 2014

(Lin, 2016) P. Lin, 2016. Why Ethics Matters for Autonomous Cars. In M. Maurer et al. (eds.), Autonomous Driving, DOI 10.1007/978-3-662-48847-8_4

(Luo and Liu, 2018) Q. Luo and J. Liu, “Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions,” IEEE Wireless Communications, no. 99, pp. 1–7, 2018.

(McGraw, 2004) G. McGraw, “Software security,” IEEE Security & Privacy, vol. 2, no. 2, pp. 80–83, 2004.

(Mirza et al., 2017) Q. K. A. Mirza, I. Awan, and M. Younas, “Cloudintell: An intelligent malware detection system,” Future Generation Computer Systems, 2017.

(Molina et ., 2017) “C. B. S. T. Molina, J. R. d. Almeida, L. F. Vismari, R. I. R. González, J. K. Naufal and J. Camargo, "Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Denver, CO, 2017, pp. 16-21, doi: 10.1109/DSN-W.2017.14.

(Newsome and Song, 2005) J. Newsome and D. X. Song, “Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software.” in NDSS, vol. 5. Citeseer, 2005, pp. 3–4.

(Nitti et al., 2014) M. Nitti, R. Girau, and L. Atzori, “Trustworthiness Management in the Social Internet of Things,” IEEE Transactions on Knowledge and Data Management, vol. 26, no. 5, 2014, pp. 1-11.

(OTA, 2018) Internet of Things (IoT) Trust Framework v2.5. Online available: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

(Park and Hwang, 2014) K.-Y. Park and S.-Y. Hwang, “Robust range estimation with a monocular camera for vision-based forward collision warning system,” The Scientific World Journal, 2014.

(Perl et al., 2015) H. Perl, S. Dechand, M. Smith, D. Arp, F. Yamaguchi, K. Rieck, S. Fahl, and Y. Acar, “Vccfinder: Finding potential vulnerabilities in open-source projects to assist code audits,” in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 426–437.

(Russell, S., 2020). Russel Stuart, “How Not to Destroy the World with AI”. ECAI 2020 keynote: https://digital.ecai2020.eu/keynote-speakers/

(Safi et al., 2018) Q. G. K. Safi, S. Luo, C. Wei, L. Pan, G. Yan, “Cloud- based security and privacy-aware information dissemination over ubiquitous vanets,” Computer Standards & Interfaces, vol. 56, pp. 107–115, 2018.

(Saied et al., 2013) Y.B. Saied, A. Olivereau, D. Zeghlache and M. Laurent, “Trust Management System Design for the Internet of Things: A Context-aware and Multi-service Approach,” Computers and Security, vol. 39, part B, Nov. 2013, pp. 351–365.

(Schwartz et al., 2010) E. J. Schwartz, T. Avgerinos, and D. Brumley, “All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask),” 2010 IEEE symposium on Security and privacy (SP), 2010, pp. 317–331.

(SEA, 2016) SAE International. 2016. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Online available: http://standards.sae.org/j3061_201601/.

(Sedjelmaci et al., 2014) H. Sedjelmaci, S. M. Senouci, and M. A. Abu-Rgheff, “An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks,” IEEE Internet of things journal, vol. 1, no. 6, pp. 570–577, 2014.

(Shar et al., 2015) L. K. Shar, L. C. Briand, and H. B. K. Tan, “Web application vulnerability prediction using hybrid program analysis and machine learning,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6, pp. 688–707, 2015.

(Shin et al., 2011) Y. Shin, A. Meneely, L. Williams, and J. A. Osborne, “Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities,” IEEE Transactions on Software Engineering, vol. 37, no. 6, pp. 772–787, 2011.

(Song and Chandraker, 2014) S. Song and M. Chandraker, “Robust scale estimation in real- time monocular SFM for autonomous driving,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 1566–1573.

(Takanen et al., 2008) A. Takanen, J. D. Demott, and C. Miller, Fuzzing for soft- ware security testing and quality assurance. Artech House, 2008.

(Tice et al., 2014) C. Tice, T. Roeder, P. Collingbourne, S. Checkoway, U. Erlingsson, L. Lozano, and G. Pike, “Enforcing forward-edge control-flow integrity in gcc & llvm.” in USENIX Security Symposium, 2014, pp. 941–955.

(Upstream, 2020) Upstream Security: 2020 Global Automotive Cybersecurity Reprot. Online available: www.upstream.auto/upstream-security-global- automotive-cyber security-report-2020/

(Whalen et al., 2016) M. W. Whalen, D. Cofer and A. Gacek, "Requirements and Architectures for Secure Vehicles," in IEEE Software, vol. 33, no. 4, pp. 22-25, July-Aug. 2016, doi: 10.1109/MS.2016.94.

(Wögerer, 2005) W. Wögerer, “A survey of static program analysis techniques,” Citeseer, Tech. Rep., 2005.

(Zeng et al., 2018) Kexiong Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, Yaling Yang, 2018. "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems". In Proceedings of the 27th USENIX Security Symposium, pp. 1527--1544. Online: https://www.usenix.org/conference/usenixsecurity18/presentation/zeng

(Zhang et al., 2018) Zhang R, Liu J, Du X, Li B, Guizani M. AOA-Based Three-Dimensional Multi-Target Localization in Industrial WSNs for LOS Conditions. Sensors (Basel). 2018;18(8):2727. doi:10.3390/s18082727

(Zhang et al., 2019) R. Zhang et al., "Using Ultra-Wideband Technology in Vehicles for Infrastructure-free Localization," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 122-127, doi: 10.1109/WF-IoT.2019.8767347.

(Zhou and Sharma, 2017) Y. Zhou and A. Sharma, “Automated identification of secu- rity issues from commit messages and bug reports,” in Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering. ACM, 2017, pp. 914–919.