Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOmated driving Progressed by Internet Of Things

D. 5.4

IoT Policy Framework for autonomous vehicles applications

Due delivery date: 31/12/2018

Actual delivery date: 26/12/2018

Organization name of lead participant for this deliverable: SINTEF

Project co-funded by the European Commission within Horizon 2020 and managed by the European GNSS Agency (GSA)		
Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential, only for members of the consortium (including the GSA)	

Project funded by the European Union's Horizon 2020 Research and Innovation Programme (2014 – 2020)

Document Control Sheet

Deliverable number:	D5.4
Deliverable responsible:	SINTEF
Work package:	5
Editor:	Ovidiu Vermesan

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Ovidiu Vermesan	SINTEF	Ovidiu.Vermesan@sintef.no
Roy Bahr	SINTEF	Roy.Bahr@sintef.no
Antoine Lapeyre	CONTI	antoine.lapeyre@continental-corporation.com
Jean-Francois Simeon	CONTI	jean-francois.simeon@continental-corporation.com
Daniele Brevi	ISMB	brevi@ismb.it
Ilaria Bosi	ISMB	bosi@ismb.it
Carlotta Firmani	THA	carlotta.firmani@thalesgroup.com
Vincenzo Di Massa	THA	vincenzo.dimassa@thalesgroup.com
Georgios Karagiannis	HUA	georgios.karagiannis@huawei.com
Abbas Ahmad	EGM	abbas.ahmad@eglobalmark.com
Marine Février	EGM	marine.fevrier@eglobalmark.com
Philippe Cousin	EGM	philippe.cousin@eglobalmark.com
Yvonne Barnard	UNL	Y.Barnard@leeds.ac.uk
Haibo Chen	UNL	h.chen@its.leeds.ac.uk
Kaushali Dave	UNL	K.G.Dave@leeds.ac.uk
Gillian Harrison	UNL	G.Harrison@leeds.ac.uk
Johan Scholliers	VTT	Johan.Scholliers@vtt.fi
Marcos Cabeza Irisarri	CTAG	marcos.cabeza@ctag.com
Louis Touko Tcheumadjeu	DLR	louis.toukotcheumadjeu@dlr.de
Robert Kaul	DLR	robert.kaul@dlr.de

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.01	29/03/2017	Template integration and initial version.	SINTEF
V0.02	23/05/2018	Document structure refined.	SINTEF

V0.03	28/11/2018	Prefinal version ready.	SINTEF, CONTI ISMB, THA, HUA, EGM, UNL, VTT, CTAG, DLR
V0.04	11/12/2018	Pre-review and comments addressed.	CNIT, TI, SINTEF
V0.05	19/12/2018	Final review and comments addressed.	VTT, AKKA, SINTEF
V1.00	21/12/2018	Final version released.	SINTEF

Abstract

This document presents a comprehensive autonomous vehicles and IoT policy framework including trust, security, privacy and stakeholders engagement that includes a set of principles that form the basis of making rules and guidelines, and give an overall direction to planning, development and deployment of technologies and solutions for autonomous vehicles, IoT and AI systems.

The autonomous vehicles and IoT policy framework takes into consideration the specific requirements from the two fields, and the trust, security, privacy and data protection policies, the access to information policy, and the autonomous vehicles security and safety policies.

The autonomous vehicle and IoT policy framework offers a starting point for understanding policy's impact on autonomous vehicles applications integrated with IoT services and is intended to guide the stakeholders involved in such complex ecosystems in developing, implementing, and maintaining a coherent policy that addresses trust, security, privacy and engagement elements.

The proposed policies are presented at high-level are technology neutral, and concern risks being a prerequisite for the implementation-specific information, which is part of the security standards, procedures and guidelines.

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. © 2017 by AUTOPILOT Consortium.

Abbreviations and Acronyms

Acronym	Definition
ACEA	European Automobile manufacturers Association
ADAS	Advanced driver assistance system
ADS	Automated Driving Systems
AI	Artificial Intelligence
ANSI	American National Standards Institute
AOSSL	Always On SSL
API	Application programming interface
AR	Augmented reality
ASIL	Automotive Safety Integrity Level
AV	Automated vehicle; Autonomous vehicle
AVA	Autonomous Vehicle for All
BSM	Basic Safety Message
CA	Co-operative awareness
CAD	Connected Automated Driving
CAM	Co-operative Awareness Message
CARTS	Committee for Autonomous Road Transport for Singapore
CAV	Connected and Autonomous vehicles
CC	Critical communication
CCAV	Centre for Connected and Automated Vehicles, (U.K.)
ComS	Communities services
C-ITS	Cooperative Intelligent Transport Systems
CoNa	Co-operative navigation
CP	Certificate policy
CSM	Co-operative speed management
C-V2X	Cellular vehicle-to-everything, (communication)
DCC	Decentralized Congestion Control
DDoS	Distributed Denial of Service
DENM	Decentralised Environmental Notification Messages
DGT	Dirección General de Tráfico, (Spanish Traffic Authority)
DL	Down-link
DLR	German Aerospace Centre
DLT	Distributed Ledger Technology
DoS	Denial of Service
DOT	Department of Transportation, (U.S. DOT)
DSRC	Dedicated short range communication
EC	European Commission
EC-GSM	Enhanced coverage GSM
ECU	Electronic control unit; Engine control unit
eMBB	Enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
ENISA	European Union Agency for Network and Information Security
FHWA	Federal Highway Administration, (U.S.)
FMCSA	Federal Motor Carrier Safety Administration, (U.S.)
FMVSS	Federal Motor Vehicle Safety Standard, (U.S.)
FU	The Freie Universität of Berlin

GA	Grant Agreement
GBA	Generic Bootstrapping Architecture
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GRRF	UNECE Working Party on Brake and Running Gear.
GRVA	UNECE Working Party on Automated/Autonomous and Connected Vehicles
GSM	Global System for Mobile communications
HAV	Highly autonomous vehicles
HMI	Human Machine Interface
HSPA	High Speed Packet Access
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
IACS	Industrial Automation Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IMU	Inertial measurement unit, (acceleration and rotation)
IoT	Internet of Things
IoV	internet of Vehicles
ISO	International Organisation for Standardisation
IT	Information technology
ITS	Intelligent transportation system
IVIM	Infrastructure to Vehicle Information Message
LBS	Location based services
LCM	Life cycle management
LTE	Long-Term Evolution, (communication standard)
LTE-M	LTE for Machine type communication
M2M	Machine-to-Machine, (communication)
MaaS	Mobility as a Service
MAPEM	MAP (topology) Extended Message
MIIT	Ministry of Industry and Information Technology, (China)
mIoT	Massive Internet of Things
MISRA	Motor Industry Software Reliability Association
MIT	Ministry of Infrastructure and Transportation, (Italy)
ML	Machine Learning
MNO	mobile network operator
MOLIT	Ministry of Land, Infrastructure and Transport, (South Korea)
MOT	Ministry of Transport, (China)
MPS	Ministry of Public Security, (China)
NB-IoT	Narrowband IoT
NCSL	National Conference of State Legislatures, (U.S.)
NHTSA	National Highway traffic Safety Association, (U.S.)
NN	Neural network
NR	Narrowband
OBD	Onboard diagnostic
OBU	Onboard unit
OEM	original equipment manufacturer
OT	Operational technology

PIA	Privacy impact assessment
PKI	Private Key Infrastructure
PO	Project officer
PS	Pilot Site
PSK	Pre-Shared Key
QoE	Quality of Experience
QoI	Quality of Information
QoS	Quality of Service
R&D	Research and development
RHW	Road Hazard Warning
RMB	Renminbi, (official Chinese currency)
RSU	Road-side unit
RTK	Real-time kinematic (enhanced precision satellite navigation technique)
SAE	Society of Automotive Engineers
SCMS	Security Credentials Management System
SLL	Security Socket Layer
SPATEM	Signal Phase And Timing Extended Message
StVG	Straßenverkehrsgesetz, (Road Traffic Act in Germany)
TCB	Trusted Computing Base
TC ITS	Technical Committee Intelligent Transport Systems, (ETSI)
TEN-T	Trans-European Transport Network
TLS	Transport Layer Security, (LTE)
Trafi	The Finnish Transport Safety Agency
UMTS	Universal Mobile Telecommunications System
UN	United Nations
UNECE	United Nations Economic Commission for Europe
UL	Up-link
URLLC	Ultra-Reliable and Low Latency Communications
Uu interface	The radio/air interface between the mobile and the radio access network
V2C	Vehicle-to-Cloud, (communication)
V2D	Vehicle-to-Device, (communication)
V2E	Vehicle-to-Edge; Vehicle-to-Environment, (communication)
V2G	Vehicle-to-Grid, (communication)
V2I	Vehicle-to-Infrastructure, (communication)
V2M	Vehicle-to-Maintenance, (communication)
V2N	Vehicle-to-Network, (communication)
V2O	Vehicle-to-Owner, (communication)
V2P	Vehicle-to-Pedestrian, (communication)
V2V	Vehicle-to-Vehicle, (communication)
V2X	Vehicle-to-Everything, (communication)
VR	Virtual reality
VRU	Vulnerable road user
VVLC	Vehicular Visible Light Communication
WP	Work Package

Table of Contents

Executive Summary 10

1. Introduction 13

1.1 Purpose of document 13

1.2 Intended audience 13

2. Autonomous vehicles legislation overview 14

Legislation in different European countries 15

2.1 Legislation in the Netherlands 15

2.1.1 Change of the road traffic Law from 1994 16

2.1.2 Documentation related to Legislation in the Netherlands 17

2.2 Legislation in France 17

2.3 Legislation in Italy 18

2.3.1 The implementing decree 19

2.4 Legislation in Spain 21

2.5 Legislation in Finland 22

2.6 Legislation in UK 22

2.7 Legislation in Germany 26

International legislation outside Europe 28

2.8 Legislation in USA 28

2.9 Legislation in China 31

2.10 Legislation in Singapore 32

2.11 Legislation in South Korea 34

2.12 Autonomous vehicles readiness and ranking 36

3. Autonomous vehicles and IoT policy framework 37

3.1 Communication technologies 37

3.1.1 V2X communication technologies 37

3.1.2 IoT communication technologies 45

3.2 Artificial intelligence in trust, security, privacy and engagement 51

3.2.1 Requirements for complex autonomous and IoT systems that have embedded AI techniques and methods 52

3.3 V2X application and use cases 56

3.4 Autonomous vehicles IoT trust framework 58

3.4.1 AI mechanisms and trust 59

3.4.2 Trustworthiness 59

3.4.3 Dependability 60

3.4.4 Sustainability 60

3.4.5 Availability 61

3.4.6 Reliability 61

3.4.7 Resilience 61

3.4.8 Privacy 62

3.4.9 Security ... 62
3.4.10 Safety ... 63
3.4.11 Requirements and recommendations ... 64
3.5 Autonomous vehicles IoT security framework ... 64
3.5.1 Security mechanisms ... 66
3.5.2 AI mechanisms and security ... 66
3.5.3 Identification ... 67
3.5.4 Authentication ... 67
3.5.5 Authorization ... 67
3.5.6 Availability ... 68
3.5.7 Confidentiality ... 68
3.5.8 Integrity ... 68
3.5.9 Network prescribed policy ... 68
3.5.10 Secure communication ... 69
3.5.11 Secure analytics ... 71
3.5.12 Security by default ... 71
3.5.13 Security by design ... 72
3.5.14 Security practices ... 73
3.5.15 Requirements and recommendations ... 74
3.6 Autonomous vehicles IoT privacy framework ... 76
3.6.1 AI mechanisms and privacy ... 79
3.6.2 Privacy regulations ... 79
3.6.3 Data minimisation ... 80
3.6.4 Data portability ... 81
3.6.5 Transparency ... 81
3.6.6 Compliance disclosures ... 82
3.6.7 Privacy by default ... 83
3.6.8 Privacy by design ... 83
3.6.9 Privacy practices ... 85
3.6.10 Requirements and recommendations ... 86
3.7 Autonomous vehicles IoT engagement framework ... 88
3.7.1 AI mechanisms and engagement ... 88
3.7.2 Ethics ... 89
3.7.3 Guidelines and standards ... 90
3.7.4 Legislation ... 90
3.7.5 Contractual arrangements ... 93
3.7.6 Requirements and recommendations ... 94
4. Conclusions ... 96
5. References ... 97

List of Figures

Figure 1: The autonomous vehicles IoT ecosystem and architecture framework 13
Figure 2: Authorization mark on approved vehicles.. 20
Figure 3: Example page of current Highway Code that will need updating in line with Automated Vehicles... 24
Figure 4: Application standards and guidance related to cyber security for connected and automated vehicles (non-exhausted list) [22] 25
Figure 5: Progress of the UK Automated and Electric Vehicles Act 2018 25
Figure 6: States with enacted autonomous vehicle legislation, Source NCSL [1] 31
Figure 7: Autonomous vehicle testing in China [97] 32
Figure 8: AV Policy and Legislation variable scores in the KPMG Autonomous Vehicle Readiness Index [31]... 33
Figure 9: MOLIT AV Commercialisation Support Policy [99] 35
Figure 10: South Korea K-City schematic [101]... 35
Figure 11: Automated Vehicle amendment to the Motor Vehicle Management Act [104] 36
Figure 12: The four pillars of AV and IoT policy framework 37
Figure 13: Roadmap for development and deployment of V2X and C-V2X technologies.................... 40
Figure 14: AVs and IoT policy framework covering all the domains of interaction 42
Figure 15:Integration of technologies in Internet of Vehicles Autonomous Mobility Applications......... 51
Figure 16: IoT policy framework - Extending in-vehicle and AI-based functions in AVs and IoT applications 52
Figure 17: Autonomous vehicles IoT trust framework 59
Figure 18: Autonomous vehicles IoT security framework 65
Figure 19: Autonomous vehicles IoT privacy framework 77
Figure 20: Autonomous vehicles IoT engagement framework 88

List of Tables

Table 1: Participation in the Vienna Convention on Road Traffic [123] 14
Table 2: Selected paragraphs.. 27
Table 3: Federal and State regulatory roles, Source U.S. DOT/NHTSA [3] 30
Table 4: Overall Autonomous Vehicles Readiness Index Results [31]... 36
Table 5: Performance requirements of different V2X use cases [82] 38
Table 6: Quality assessment of communication technologies to support V2X use cases [78][79][80]. 38
Table 7: Target 5G performance requirements [74] 39
Table 8: Comparison of V2X communications features [110][111][112][113][114] 42
Table 9: Comparison of IEEE 802.11p and C-V2X, Source Autotalks Ltd. [57] 43
Table 10: Comparison of communication infrastructure technologies [115]... 44
Table 11: ITS service and estimated sensor data to be transmitted/received [119] 56
Table 12: Assumptions and estimates for computational requirements for training based on data collected from a fleet of 100 autonomous vehicles [118].. 57
Table 13: V2X treats and attacks [108].. 57
Table 14: ETSI ITS Basic set of applications definitions [77] 58
Table 15: Trust - Requirements (Req) and Recommendations (Rec) 64
Table 16: Security - Requirements (Req) and Recommendations (Rec) 74
Table 17: Privacy - Requirements (Req) and Recommendations (Rec) 86
Table 18: Engagement - Requirements (Req) and Recommendations (Rec)...................................... 94

Executive Summary

The Internet of Things (IoT) applications connect multiple devices through the Internet. Autonomous vehicles utilize connectivity when updating their algorithms based on user data, interact with the infrastructure to get environmental information, communicate with other vehicles, exchange information with pedestrians using mobile devices and wearables, and provide information about the traffic attributes and information collected by the vehicle sensors. These autonomous vehicles require significant quantity of data collecting and processing and through IoT applications and services the autonomous vehicles shares information about the road, the actual path, traffic, and how to navigate around any obstacles. This information can be shared between IoT connected vehicles and uploaded wirelessly to the cloud or/and edge system to be analysed and operated improving the automation and automated driving level of each individual vehicle.

Intelligent connectivity is used to describe the combination of flexible, high-speed 5G networks, the IoT and artificial intelligence (AI). Underpinned by ubiquitous, hyper connectivity, intelligent connectivity marks the beginning of a new era defined by highly contextualised and personalised experiences, delivered as and when you want them. It will have a significant and positive impact on individuals, industries, society and the economy [116].

Internet of Vehicles (IoV) solutions for autonomous vehicle applications are emerging through advancements of networking, 5G, the IoT and AI. With the IoV and increased connectivity, the development of innovative industry applications features management capabilities for data, interconnections, operations, security and safety.

Intelligent connectivity enables transformational new capabilities in transport, entertainment, industry and much more. In order for technical systems to match human actions digitally with connected environments, however, they must meet the speed of our natural reaction times. The network used must be ultra-reliable, as many critical tasks will be executed remotely, and must also rely on cost-effective edge infrastructure to enable scaling. Connectivity is therefore necessary for such services to work optimally. Intelligence can then be enabled close to the user experience through multi-access edge computing; at the application level IoT, AI, automation, robotics, telepresence, augmented reality (AR) and virtual reality (VR) will all also play a part [116].

As autonomous vehicles, IoT, and AI connected systems are deployed they increasingly rely on information that is exchanged in order to perform and conduct their safety-critical operations. Keeping such systems (and the information within) trustworthy, secure, safe, private for the required cases is a critical element for the acceptance and adoption of such autonomous systems. Challenges include legislative issues in order to identify the accountability in case of incidents and malfunction, provide technologies like software, hardware, communication, security to assure 100% reliable sytems to avoid technical mistakes, provide solutions to protect the vehicles from cyber-attacks and external interference, implement mechanisms to protect the privacy of the owners/users/pedestrians and address ethical issue such as the vehicle behaviour model in an inevitable collision (e.g., to hit a pedestrian or to drive a vehicle off the road where passengers may be in danger).

In this context, an up-to-date comprehensive policy framework for autonomous vehicles and IoT including trust, security, privacy, and engagement. The framework elements are an important step for accelerating innovation and developing the right technologies and applications for such complex autonomous systems.

The autonomous vehicles and IoT policy framework proposed in this document includes a set of principles that form the basis of making rules and guidelines. Moreover, it also gives an overall direction to plan, develop and deploy the technologies and solutions for autonomous vehicles and IoT systems.

The autonomous vehicles and IoT policy framework takes into consideration the specific requirements from three fields:

1. The trust, security, privacy and data protection policies.
2. The access to information policy.
3. The autonomous vehicles security and safety policies.

The autonomous vehicle and IoT policy framework offers a starting point for understanding policy's impact on autonomous vehicles applications integrated with IoT services and is intended to guide the stakeholders involved in such complex ecosystems in developing, implementing, and maintaining a coherent policy that addresses trust, security, privacy and engagement elements.

Considering the dynamic environment of autonomous vehicles and IoT applications, the requirements for trust, security, privacy and dynamic continuous engagement over the whole life-cycle of autonomous vehicles and IoT applications are not straightforward. The challenge is to come up with the most technically and economically feasible solutions for protecting autonomous vehicles and IoT systems, knowing that today's most secure/trusted technology will be vulnerable tomorrow.

The proposed policies are presented at high-level, they are technology neutral, and the possible described risks in the different sections need to be considered a prerequisite for the implementation-specific information, which is part of the security standards, procedures and guidelines.

The proposed autonomous vehicles and IoT policy framework can be used to define the requirements of the trust/security/privacy architecture considering the defined policy. This allows to translate the recommendations to requirements and create the trust/security/privacy infrastructure necessary for autonomous vehicles and IoT applications.

The high-level requirements can be expanded to an enough level of detail so that control selection could match the requirements from the overall technical environment. At the end the proposed solutions will tightly integrate and support the existing autonomous vehicles and IoT environment. Autonomous vehicles and IoT interoperability requirements such as systems and network support, and standards and application programming interface support are an important element of the framework.

The proposed framework allows that the defined trust/security/privacy/engagement requirements are mapped to specific risks or to specific points/recommendations in the autonomous vehicles and IoT policy framework; then those risks can be evaluated against the industry best practices. Additionally, for the case of autonomous vehicles and IoT applications they need to meet requirements specified by the continent/country or local government, or by other authoritative bodies.

The autonomous vehicles and IoT Trust Framework, according to the collective principles and underlying structure provides that the trustworthiness, dependability and privacy for autonomous vehicles and IoT solutions are exhibited into an integrated manner. The framework integrates the concepts of availability, reliability, safety, security, resilience, privacy and sustainability best practices, it embraces "privacy and security by design" as a model for an implementable autonomous vehicle and IoT code of conduct and engagement.

Considering the human-centred approach adopted, the discussion expands on the creation of an autonomous vehicles and IoT Engagement Framework, producing the need for stakeholder engagement in ethics, rules, guidelines and standards for an effective autonomous vehicles and IoT Policy Framework that would assure a sustainable and safe autonomous vehicle and IoT environment development.

Considering a user-centred approach and considering the General Data Protection Regulation (GDPR), the autonomous vehicles and IoT Privacy Framework addresses key aspects of European Data Protection law, focusing on the principles of data protection by design and data minimisation.

The autonomous vehicles and IoT Security Framework addresses the principles, security mechanisms and practices which are appropriate for the autonomous vehicles and IoT applications domain and solutions and indicates best practices and choices in design, features, implementation, testing, configuration and maintenance, as well as a dedicated methodology for facilitating compliance by design within the changing regulatory landscape. The autonomous vehicles and IoT security framework focuses on the security policy, the system architecture, combining mobile and wireless communications, while addressing authentication, authorization, and accountability.

The autonomous vehicles and IoT Policy Framework is intended to help AUTOPILOT's and other stakeholders making informed decisions through a robust methodology and evidence gathering process. The evidence gathered during the process can be used to demonstrate conformity with best practice to consumers and other autonomous vehicles and IoT stakeholders.

In this context, the document provides an overview of the current status regarding autonomous vehicles legislation in different European countries and selected countries outside Europe.

1. Introduction

1.1 Purpose of document

As the implementation of autonomous vehicles and IoT systems are deployed they increasingly rely on information that is exchanged in order to perform and conduct their safety-critical operations. Keeping such systems trustworthy, secure, safe, private for the required cases is a critical element for the acceptance and adoption of such autonomous systems. The autonomous vehicle and IoT policy framework offers a starting point for understanding policy's impact on autonomous vehicles applications integrated with IoT services and it is intended to guide the stakeholders involved in such complex ecosystems in developing, implementing, and maintaining a coherent policy that addresses trust, security, privacy and engagement elements.

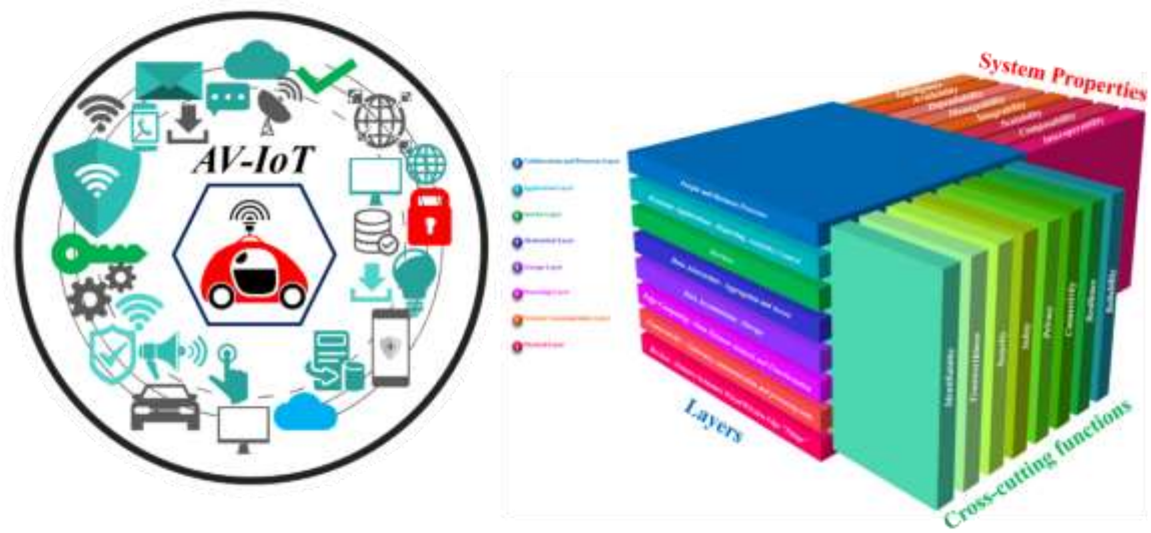


Figure 1: The autonomous vehicles IoT ecosystem and architecture framework

The proposed framework allows that the trust, security, privacy, and engagement requirements defined are mapped to specific risks or to specific recommendations in the autonomous vehicles and IoT policy framework and evaluates them against industry best practices. Additionally, for the case of autonomous vehicles and IoT applications they need to meet requirements specified by the authoritative bodies nationally or internationally. In this context, the document also provides an overview of the current status regarding autonomous vehicles legislation in different European countries and selected countries outside Europe.

1.2 Intended audience

The autonomous vehicles and IoT policy framework proposed in this document includes a set of principles that form the basis of making rules and guidelines, and gives an overall direction to planning, development and deployment of technologies and solutions for autonomous vehicles and IoT systems. The framework elements include important steps for accelerating innovation and developing the right technologies and applications for such complex autonomous systems.

The Framework is intended to help AUTOPILOT's stakeholders, as well as other stakeholders within the field of autonomous vehicles and IoT, making informed decisions through a robust methodology and evidence gathering process based on recommendations and best practices. The evidence gathered during the process can be used to demonstrate conformity with best practice to users and other autonomous vehicles and IoT stakeholders.

2. Autonomous vehicles legislation overview

At the United Nations (UN) level; the regulations have been changed over time from *the driver must always be in control of their vehicle* in 1968 (Vienna Convention) to *the driver must be ready to take over the driving functions* (2014 UNECE amendment) [84]. However, in 2018 the UN Economic Commission for Europe (UNECE) and its Global Forum for Road Traffic Safety (WP.1)[1] adopted a non-binding resolution as a guide for the countries on the safe deployment of highly and fully automated vehicles in road traffic [90]. Today, the Global Forum for Road Traffic Safety (WP.1) is a permanent body in the UN system that focuses on improving road safety, and its primary function is to serve as guardian of the UN legal instruments aimed at harmonizing traffic rules [86]. For the countries analysed later in section 2, we give a status overview of participation in the Vienna Convention on Road Traffic is given in Table 1 [123].

Table 1: Participation in the Vienna Convention on Road Traffic [123]

Country	Status
France	Signed and ratified
Italy	Signed and ratified
Spain	Abiding by treaty as a non-state-party
Finland	Signed and ratified
UK	Signed and ratified
Germany	Signed and ratified
USA	Non-signatory
China	Non-signatory
Singapore	Abiding by treaty as a non-state-party
South Korea	Abiding by treaty as a non-state-party

UNECE's Global Forum for Road Traffic Safety (WP.1) is the main coordinating body in the area of road safety, and works in conjunction with other working parties such as the world forum for the harmonization of vehicle regulations (WP.29), but also Road transport (SC.1), Transport statistics (WP.6), Transport of dangerous goods (WP.15) and Safe loading of cargo (WP.24) to offer a comprehensive platform that enables cooperation and the exchange of information and best practices among governments [88]. The world forum for the harmonization of vehicle regulations (WP.29) is dedicated to technical regulations applied to the broad automotive sector, addressing the safety and environmental performance of vehicles, their subsystems and parts [89]. They have decided to convert the working party on Brake and Running Gear (WP.29/GRFF) into Automated/Autonomous and Connected Vehicles (WP.29/GRVA) [91]. The world forum is currently working on the harmonization between UN Regulations and EU Directives, and some of the EU

[1] The intergovernmental body "Working Party on Road Traffic Safety (WP.1)" was established in 1988. The Working Party changed its name to “Global Forum for Road Traffic Safety (WP.1)” in 2017 [86].

Directives are technically equivalent to UN Regulations or only refer to the requirements of the corresponding UN Regulation [92].

The European Connected Automated Driving (CAD) initiative captures the expectations and concerns of users, public authorities and providers of technology, infrastructure or mobility services, and supports the development of clearer and more consistent policies on connected and automated driving in EU Member States [83]. Regarding future regulatory needs, five main challenges in the area of policy, regulatory and harmonization have been defined through the following questions [84]:

1. Today's work of industry and the discussions with national and EU stakeholders concentrate on research, testing and type approval. First activities which are focussing on the development of traffic rules have started in some countries. What is the total scope of affected policy and regulation?
2. How to bundle and coordinate EU research activities to speed up and not loose in the world-wide competition in research and testing?
3. The SAE International provides a taxonomy with definitions of six levels (from 0 to 5) of driving automation, where regulation for level 2 is still under strong discussion, level 3 has not really started yet, for level 4 and 5 there is no clear view on how to proceed. How can the type approval approach evolve? How to establish the regulation before the technology will be ready? How to develop regulation and technology in parallel without creating a "chicken-and-egg" dilemma? and How to deal with software updates?
4. How and to which extent adapt and harmonize traffic rules for fast introduction of higher automation levels?
5. What liability framework needs to be in place to facilitate market penetration from a legal and liability perspective?

However, according to CAD there are additionally aspects that need to be addressed. In a 2020 short term perspective the needs are [84]: (i) Common European understanding on necessary digital infrastructure quality and coverage for level 3, (ii) Joint approach between telecom and vehicle industries to support connected automated driving, (iii) Need for cross border pilot projects for quick level 3 rollout, (iv) Common European understanding on safety and security validation, (v) European push in setting up the framework for a safe level 4 series development (new UN Regulation), (vi) Coordinated European programs to support global competitiveness, and (vii) Adaption of road traffic rules in Member states. In a 2040 long term perspective the visions are [84]: (i) Pan European approach on overall mobility solutions for cities including electric autonomous shared mobility, (ii) Political framework for the rollout of electric autonomous shared mobility into rural areas, (iii) Clear common approach for cities to coordinate both private and public transport, (iv) Role of traffic management, and (v) Safe coexistence of automated vehicles and vulnerable road users (VRUs).

Below we give an overview of the current status regarding autonomous vehicles legislation in different European countries. International legislation outside Europe is covered in sections after.

Legislation in different European countries

2.1 Legislation in the Netherlands

The road traffic legislation in the Netherlands has been published in 1994 and is documented in [19]. The legislation related to autonomous vehicles is ongoing, and is specified and documented in several presentations, press releases and amendments to the existing road traffic legislation, see [10], [11], [12], [13], [14], [15], [16], [17], [18].

2.1.1 Change of the road traffic Law from 1994

The following changes are described in [10] and relate to section 1 of [19]. Note that these changes are documented in the Dutch language. The below text does not represent an official translation of these Road Traffic Act changes.

Article I - Changes to the Road Traffic Act 1994 (ARTIKEL I (WIJZIGING WEGENVERKEERSWET 1994)
The Road Traffic Act 1994 is modified as follows:

A: The title of Section VII becomes Section VII Exceptions, Exemptions and Permit (HOOFDSTUK VII. VRIJSTELLING, ONTHEFFING EN VERGUNNING)
B: In article 149a, first topic (lid), the "article 149b" is replaced by: the articles 149aa and 149b.
C: After article 149a, two articles have been added:

New article 149aa, based on [10]:

1. Concerns a road experiment where a vehicle is involved without having a seating driver; A permit is required from the minister of Infrastructure after he/she reviewed the topic together with the minister of Justice and Safety.
2. Article 149a, topic/bullet two, is not valid anymore.
3. For the permit and for some cases an exemption can be provided for one or more situations:
   a. this law, with exception of articles 5 and 6
   b. other laws as long as the they are covering the tasks related to the driver or the owner of the vehicle
   c. laws, mentioned in topics/bullets ***a*** and ***b***, and their associated regulations.
4. A permit with an exemption is provided by the Minister.
5. Permit can be refused in case the experiment: (1) does not satisfy requirements, based on article 2, topic (lid) 1, (2) does not contribute to innovation and (3) if the exception described in topic (lid) 3 of this clause does to satisfy the legislation rules related to this exemption
6. The permit is provided and sent to: (1) Road traffic authority (Dienst Wegverkeer), (2) Controllers of the road traffic (Toezichthouders), as mentioned in article 159, under topic/bullet ***a***, and (3) the responsible road controllers (Wegbeheerders).
7. When the permit is handled at ministry level then it should be handled by the appropriate management offices of the ministry, following the time constraints specified in the topic 6 of this article.

Article/clause 149ab, based on [10]:

1. The permit, as specified in article 149aa, can be provided for a duration of max. 3 years.
2. The permit includes:
   a. description of the experiment
   b. on which roads (or parts of the road) will the experiment take place
   c. during which time period will the experiment take place
   d. under which working environment circumstances and during which time slots of the day may the experiment be realized
   e. under which rules, specified in article 149aa, third topic (lid), is the exemption provided and if relevant under which constraints is this exemption valid
   f. which safety measures are valid for the implementation of this experiment related to the benefits described in clause 2, sub-clause 1
   g. Explain how the minister can monitor and evaluate the experiment;
   h. guidance for law enforcement and prosecution, including in any case who the driver of the vehicle is and where the driver is located,
   i. how many vehicles can the driver control (in case of semi-autonomous driving vehicle)

3. The minister using article 149b, topic (lid) 5, can dismiss the permit whenever the permit owner does not follow the agreed rules.
4. The minister evaluates the experiment and documents it.

D: Article 149b is changed such that the above described articles become valid.
E: Article 150 is modified as follows: In the first topic (lid) "exception and exemption (vrijstelling en een ontheffing)" is replaced by "exception, exemption and permit (vergunning, een vrijstelling en een ontheffing).
F: In article 151 after "exemption (ontheffing)" is added or "permit (vergunning)".

Article II Evaluation related rule (ARTIKEL II (EVALUATIEBEPALING))
The Minister sends (to the "Staten-Generaal") within 5 years after this Law is ratified a report describing the outcome and effectiveness of this Law.

Article III – Ratification of the Law (ARTIKEL III (INWERKINGTREDING))

This Law is ratified on a time slot decided by the kingdom of the Netherlands.

2.1.2 Documentation related to Legislation in the Netherlands

In addition to the listed changes on the Road Traffic Act 1994, specified in [10], several press releases and other type of documentation has been found. These documents, among others emphasize that in order to realize large scale testing with autonomous driving possible, the Dutch minister of Infrastructure and Water management (Mrs. Cora van Nieuwenhuizen) is working on a legal framework that includes requirements for reliability and safety. In particular, in order to make infrastructure ready for this uptake, the Minister is planning to meet with road authorities, and the automotive and telecom sector. The objectives of these discussions with the stakeholder are to: (1) identify the requirements to connect cars and infrastructure, (2) identify what needs to be adjusted, (3) stimulate the arrival of 5G.

The following press releases, and other such documents provide additional insights related to the Legislation in the Netherlands are included in the reference list [10], [11], [12], [13], [14], [15], [16], [17], [18] and [19].

2.2 Legislation in France

The first law to consider in French legislation is the Vienna convention on road traffic [7]. This convention states that "Every driver shall at all-time be able to control his vehicle", which is not compatible with autonomous driving vehicles. In 2014, the convention evolved [8] to allow autonomous driving in specific cases: "automated driving technologies transferring driving tasks to the vehicle will be explicitly allowed in traffic, provided that these technologies are in conformity with the United Nations vehicle regulations or can be overridden or switched off by the driver".

The French legislation is based on the Vienna convention, but an order stated in 2016 [9] that "the traffic of partial or total driving delegation vehicle on open public roads is subject to the issue of an authorization to ensure security during the experimentation". Experimentations are thus completely allowed. The authorization is given by the ministry of transport and the prime minister, along with all the concerned parties.

A future law plans to allow level 5 autonomous driving on all open roads in France for 2020, without the delivery of a special authorization. The goal is to make France one of the leaders in autonomous driving. The details of this law should be published in the next months.

A partnership between France and Germany led to an experimentation zone on the Highway between Metz and Merzig. The goal is to test autonomous driving features in multiple countries to ensure interoperability between the developed systems.

PSA, one of the largest French car manufacturers, started its experimentations on autonomous driving vehicle in July 2015 with the “Autonomous Vehicle for All” (AVA) program. They have an authorization to drive on the highway between Paris and Bordeaux, in the middle of the traffic. The experimentations with “non-experts” drivers started in March 2017 on the same highway. They use Citröen C4 Picasso and Peugeot 3008 to test these functions and plan to sell fully autonomous vehicles by 2020.

Renault, another French car manufacturer, uses a demo car, the Renault Symbioz, to demonstrate its autonomous driving features. They have an authorization to drive on the highway between Paris and Caen, also in the middle of the traffic. The demo car can drive on the highway and cross toll gates. They also work closely with Tomtom to update their map and make it more precise. They plan to sell level 4 autonomous vehicles by 2023.

Vedecom is a public-private institute that aims to develop autonomous driving features by 2020 at an affordable cost. They currently have a demo car based on Renault Zoe capable of driving in the city of Versailles. The institute gathers multiple companies such as Renault, PSA, Continental, Valeo and different French universities.

Easymile is a start-up that develops an electric autonomous shuttle with a capacity of 15 passengers. Their goal is to resolve the “last kilometre issue”, for example how to travel from public transport to the destination. They are testing their shuttle in different cities of the world. In France, they are authorized to transport people on dedicated roads.

Navya is also building an autonomous shuttle and an autonomous cab. They have the authorization to drive in Paris airport and cross open roads, but not yet to drive on open roads. The AUTONOM SHUTTLE was specifically designed to meet the needs of an autonomous, driverless vehicle while also optimizing navigation and safety features. With neither a steering wheel nor pedals, AUTONOM SHUTTLE uses effective guidance and detection systems that combine various types of advanced technology. Data from Lidar sensors, cameras, GPS RTK, IMU and odometry is merged together and interpreted by deep learning programs.

2.3 Legislation in Italy

The Italian legislation for Automated Driving is quite new. The decree has been published on 28th of February 2018, by the Ministry of Infrastructure and Transportation (MIT). Before this law the experimentation of Autonomous vehicles in Italy was foreseen only on private tracks.

The decree lists the practical rules to make experiments with automated vehicles on Italian roads. It is worth mentioning that this set of rules is strongly linked with the “Smart road” initiative. The “Smart road” project started some years ago in Italy and has its focus on the implementation of 5.9 GHz network technology solution in Italian highways and main roads. Indeed, for Italy, autonomous and connected cars are strongly related. Italy is also very active in many European initiatives like C-ROADS.

In the framework of “Smart roads” several call for tenders are already issued. The first one was for the Mediterranean A2 Highway (in the south of Italy). Other calls were for the mountain road toward Cortina D’ampezzo (North of Italy for the Word Sky Championship of 2021) and for the Rome orbital road.

2.3.1 The implementing decree

First of all, it is worth mentioning that the decree, is strongly linked with a series of similar European initiatives like:

- The declaration of cooperation for autonomous driving (Amsterdam – April 2016) signed among the European transportation ministries;
- The European strategy towards smart and connected system (November 2016);
- The C-ITS European Platform;
- The Gear 2030 initiative.

A particular attention will be devoted to the highways that are part of the Trans-European Transport Network[2] (TEN-T).

The decree defines an **autonomous vehicle** as a vehicle that implements driving behaviours without the intervention of the driver, in certain roads and conditions. Currently, homologated cars with driver-assistance system that needs a continuous driver's attention are not considered autonomous systems. The decree does not directly refer to SAE levels but gives only the above definition.

Another important definition is the **Supervisor** or a person that must be always on-board, ready to take the full control of the vehicle in any moment and in any case of necessity, independently from the automation level in use. His/Her intervention must automatically disable all the autonomous functions, so he/she can take the complete control of the vehicle.

Finally, the decree also gives its definition of **smart road** that is basically a street where the road operator has initiated the process of digital transformation for the introduction of traffic monitoring platforms, data management systems, advanced digital services, the implementation of C-ITS "Day-1" services, etc.

The main objective of the decree is not only the definition of the rules for testing autonomous driving solutions but also the enhancement of the road infrastructure (thanks to technological solutions) and the improvement of road safety. The decree is a big step towards innovation in the field of transport technology, including better infrastructure to provide real-time information on issues like weather and traffic conditions.

From the operational point of view, the authorization is granted by the Italian Ministry of Infrastructure and Transportation. The authorization can be asked by two subjects: 1) an OEM and 2) a public or private research body. The authorization can be granted only for already homologated vehicles (in the non-autonomous version) or for pre-production series (following the corresponding rules). After the grant, the vehicles will be registered to a dedicated ledger and will obtain an authorization mark that must be clearly shown during the experimentation phase. In Figure 2 you can find an example of this mark.

Moreover, the tested vehicle must have a testing plate following the general rules of the Italian laws. The permission is related to a specific road (or set of roads) and the applicant needs the allowance of the road holder (owner and dealer).

[2] The Trans-European Transport Network (TEN-T) is a European Commission policy directed towards the implementation and development of a Europe-wide network of roads, railway lines, inland waterways, maritime shipping routes, ports, airports and rail-road terminals [109].

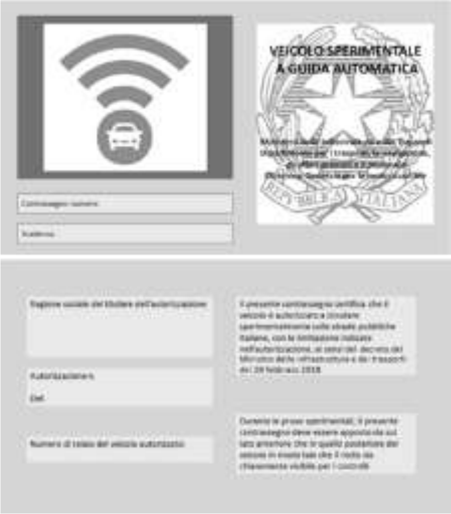
The supervisor must respect the following characteristics:

- Own a driving license for 5 years;
- Own a safe driving certification or a specific certification for AD;
- Having 1000 km of AD on private or public roads.

He/She has the responsibility of the vehicle in both manually and automated operative modes.

The applicants must provide several proofs about the vehicle characteristics and features especially for its AD and e-security related capabilities. The vehicle must have a liability insurance and all the tests must be carried out "in conditions of absolute safety".

Another important prerequisite is to have at least 3000 km of experimentation (also on different vehicle models) by the testing company. This amount of km can be real or simulated and even be done outside Italy.



VEICOLO SPERIMENTALE
A GUIDA AUTOMATICA

[illegible]

REPUBBLICA ITALIANA

Contrassegno numero

Scadenza

Ragione sociale del titolare dell'autorizzazione

Il presente contrassegno certifica che il veicolo è autorizzato a circolare sperimentalmente sulle strade pubbliche italiane, con le limitazioni indicate nell'autorizzazione, ai sensi del decreto del Ministro delle infrastrutture e dei trasporti del 28 febbraio 2018

Autorizzazione n.

Del

Numero di telaio del veicolo autorizzato

Durante le prove sperimentali, il presente contrassegno deve essere apposto sul lato anteriore che in quello posteriore del veicolo in modo tale che il risulti chiaramente visibile per i controlli

Figure 2: Authorization mark on approved vehicles

Moreover, the vehicle must log a series of data like:

- General data;
- Data about vehicle dynamic;
- Operative modes (manually/automated);
- Date, time and position;
- V2X messages sent and received.

The logging should be performed almost at 10 MHz. The data must be stored for a period of 24 months and a detailed report must be sent within 15 days from each test. It can contain not only logs but also video, etc.

Finally, it is worth mentioning that if the applicant is not an OEM, the OEM authorization for the selected model is mandatory.

The license will last 1 year and can be renewed. A final annual report must be sent at the end of the authorization period. The MIT will also create a Smart Road Observatory that will monitor: 1) the results of the experimentations 2) all the activities related to Connected and Autonomous vehicles (CAV), etc. Currently in addition to the AUTOPILOT Livorno Pilot Site (PS), two more urban testbed are expected to obtain the Authorization; they are located in Turin and Modena. Basically, the mobility offices in these Municipalities are aggregating several actors (companies and research centres) interested in CAV to start with several different experimentations under a unique umbrella.

2.4 Legislation in Spain

As in other countries autonomous vehicles must be able to drive themselves, deciding on routes and actions related to driving, with optimal levels of safety.

The vulnerabilities associated with autonomous vehicles driving, are associated with: a) the vehicle itself, b) the environment in which it moves and c) the communication networks required for its operation.

The large-scale deployment of this type of vehicle will require the introduction of numerous changes in terms of the signalling of streets, sections, crossings, traffic lights, etc. Intelligent vehicles are also dependent of smart streets to be able to drive on them. This transition is going to be complicated and the change necessarily progressive, since it is foreseeably possible that at a given moment vehicles with different levels of autonomy will be able to circulate at the same time (given the possible different versions of the software used), which can lead to situations of risk that should be prevented.

Spanish legislation:
In Spain, the definition of "autonomous vehicle" can be found in Instruction 15 / V-113, dated November 13, 2015:

a) Autonomous vehicle: "Any vehicle with motor capacity equipped with technology that allows its operation or driving without specifying the active form of control or supervision of a driver, whether that autonomous technology was activated or deactivated, permanently or temporarily."

b) Autonomous mode: "Driving mode consisting of driving or driving the autonomous vehicle without active control of the driver when its autonomous technology is activated", while in the conventional mode that autonomous technology is deactivated, and its driving or management requires control active vehicle by a driver.

In general, Spanish legislation says that only manufacturers, institutions or companies can test vehicles without a driver and only in certain roads.

The Report of the State Attorney General's Office published in 2016, says that "the implementation of autonomous vehicles should be preceded by an administrative regulation." The question is: What laws should be changed to legalize the autonomous car?

1. The first is the one that affects civil liability. The current norm speaks of the responsibility of the driver in an accident but, what happens when there is no human being at the wheel? In this regard, the State Attorney General's Office says that some responsibility may have to be transferred to the manufacturer. It is also said that some of the fault could be extended to those who collect the cartographic data and ultimately to the Public Administration when they are autonomous vehicles that provide a public service.
2. The second aspect is about criminal responsibility. Who has to be charged as responsible in case of an accident?

The current status in Spain:
In the case of Spain, the current legislation (Law on Civil Liability and Motor Vehicle Insurance) considers that the driver of the vehicle is responsible, by virtue of the "risk created by driving", for the damage caused to people or the goods on the occasion of driving.

Obviously, this regulation does not specifically provide for the case of an accident caused by an autonomous vehicle, where the driver has no active intervention or obligation to supervise driving.

Although, it is evident that the owner of the vehicle will have to answer for the damages caused (possibility already provided by our legislation regarding the non-autonomous car), in addition to the possible responsibility of the manufacturer for faults in the design of the driving systems.

Spain has an advantage considering that it will have more facilities when it comes to regulating the presence of autonomous vehicles on the roads, and has not signed the Vienna Convention on Road Traffic, which stipulates in one of the articles (e.g. 8.1) that: "Every vehicle in motion or any set of vehicles in motion must have a driver".

By not signing this agreement, it is simpler to regulate activities related to the autonomous vehicle applications since it is not necessary to amend a document signed by so many countries.

Other points of enormous interest and importance that must be regulated and established refer to compulsory insurance and the road safety law. In the case of insurance, it will not be the driver but "the driving", or the elements and systems that make this possible, who will receive coverage.

These laws will have to go through parliamentary approval, so the process will be slow. The objective is that there is a regulation in place that can cover all the legal aspects associated with autonomous driving and giving an adequate legal coverage to the passengers of these vehicles, and to the buyers.

What is Spanish Traffic Authority opinion?
The Spanish Traffic Authority (Dirección General de Tráfico, DGT) works on a Strategic Vehicle Plan that includes the connected car and the autonomous car in order to establish the key definitions, requirements and levels of automation of vehicles to be able to have legal support. Mainly, work is being done to jointly modify the law on compulsory insurance and road safety with the aim of having them ready for 2017 and for the time being there are no news about it.

2.5 Legislation in Finland

The Finnish law supports at this moment already automated vehicle trials, and no amendments are required. An automated vehicle always has to have a driver, who serves as backup. The driver does not necessarily have to be inside the vehicle but can control the vehicle remotely. Permits for testing of automated are granted by Trafi, the Finnish Transport Safety Agency. Focus in the application is on the responsible behaviour of the testing organisation. The application consists of [42]:

- Trade register extract from the company’s country of incorporation
- Trial plan, including
    - A general description of the trials
    - Technical specification of the test vehicles
    - Information on the road area where the trials are intended
    - Proof of insurance cover for third party liability
    - Description of how road safety will be ensured.

Permits are granted for one year but can be renewed on request. The test plate certificate holder must submit a report to Trafi on the trial results, describing how the trial plan was implemented, and which kind of deviations from the plan were encountered [42].

2.6 Legislation in UK

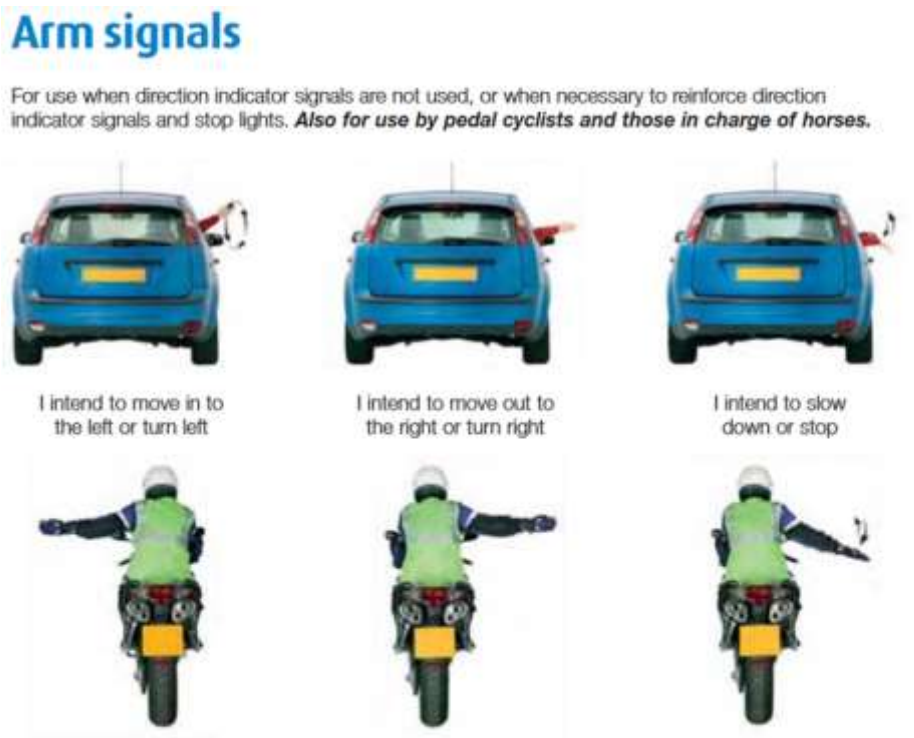
Established in 2015, The Centre for Connected and Automated Vehicles (CCAV) [25] is a government unit working across departments to support the CAV market. Automated Vehicles (AV) can currently be tested legally on UK roads under existing laws [21] and a rolling programme of regulatory reform has been ongoing since summer 2016 [24], though legislation and regulatory frameworks are currently being reviewed and revised by the Law Commission to allow for the widespread introduction [26]. This three-year review commenced in April 2018 and will examine how existing laws need to be amended to account for differences between conventional cars and AVs. This excludes data protection and privacy, theft and cyber security, and land use policy, but focuses on legal requirement relevant to drivers, such as:

- Definition of a 'driver';
- Assignment of responsibilities and liabilities;
- Possibility of new criminal offences related to the new technologies, and;
- Requirements to protect other road users.

As part of this, the Law and Scottish Law Commission jointly launched their first consultation paper in November 2018, to close in February 2019. This explores safety assurance (both prior and post deployment), criminal and civil liability and the adaptation of road rules through comprehensive descriptions of the current and proposed issues through 46 consultation questions (see [93]).

However, the government have announced that it is not the current intention to set definitive legislation in place until such a time that the technology has matured and can be covered under a standard Type Approval process [27]. In the meantime, industry and international standards will be followed. Currently ISO 26262 on functional safety can be widely applied, though adaptations or new standards will be required to address communications, traffic management, cyber-security and supply chain security [20][28].

The UK has signed (though not ratified) the Vienna Convention on Road Traffic. Current UK Legislation governing driving and motor vehicles currently includes the Road Traffic Act 1988, Motor Vehicles (Driving Licences) Regulations 1999 as well as being subject to EU Legislation and UN Regulations. Set out in these legislations are the conditions that are required for a vehicle to be 'roadworthy' and for a driver to hold a licence. In addition, the 'Highway Code' [29] sets out guidelines for road users. Some obligation set out here may be amended by the introduction of automated vehicles – for instance current prohibitions related to safe driving, such as a driver being able to see a television screen, or a holding a mobile phone.



Arm signals

For use when direction indicator signals are not used, or when necessary to reinforce direction indicator signals and stop lights. ***Also for use by pedal cyclists and those in charge of horses.***

I intend to move in to the left or turn left

I intend to move out to the right or turn right

I intend to slow down or stop

Figure 3: Example page of current Highway Code that will need updating in line with Automated Vehicles

Some key areas of legislation being considered in the UK are set out below. Additional areas not discussed here are addressed more fully in ‘The Pathway to Driverless Cars’ [21], and include:

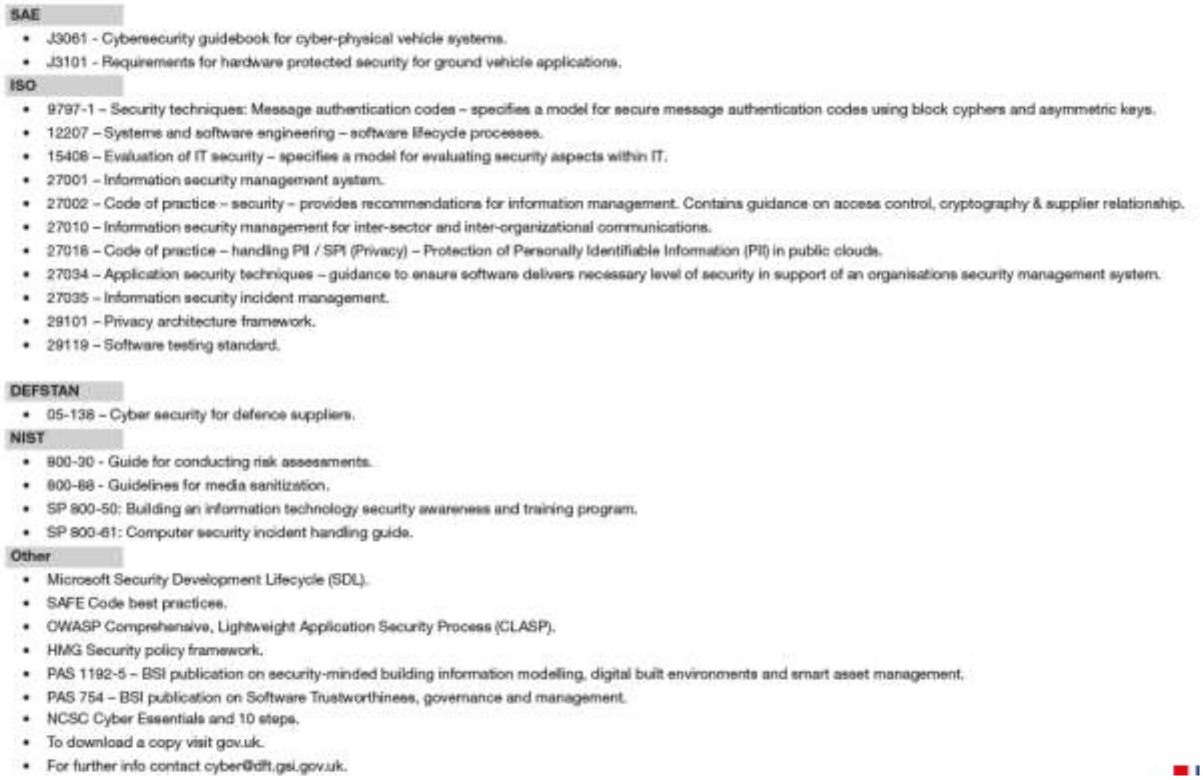
- Driver Behaviour, Testing & Licencing
- Vehicle tax, registration and licensing
- Vehicle roadworthiness and maintenance
- Safe use of vehicles
- Other Road Users
- Road infrastructure
- Standards
- Insurance
- Data protection and privacy

Advanced Driver Assistance Technology Regulation:

From June 2018, both the Road Vehicles (Construction and Use) Regulation 110 and the Highway Code were updated to allow for the use of advanced driver assistance technology, such as automated parking and lane changing [30].

Cyber Security:

Cyber-security is subject to EU Data Protection Directive 95/46/EC, Directive 2002/58/EC on Privacy and Electronic Communications and the General Data Protection Regulation 2016/6794. Although no specific legislation has been developed in the UK, the UK government has set out key principles for cyber security and listed relevant standards and guidance, as in Figure 4 [22]. The principles cover level of governance, risk assessment and management, aftercare, co-operation, defence design, lifetime management, data security, and system resilience.



SAE

- J3061 - Cybersecurity guidebook for cyber-physical vehicle systems.
- J3101 - Requirements for hardware protected security for ground vehicle applications.

ISO

- 9797-1 – Security techniques: Message authentication codes – specifies a model for secure message authentication codes using block cyphers and asymmetric keys.
- 12207 – Systems and software engineering – software lifecycle processes.
- 15408 – Evaluation of IT security – specifies a model for evaluating security aspects within IT.
- 27001 – Information security management system.
- 27002 – Code of practice – security – provides recommendations for information management. Contains guidance on access control, cryptography & supplier relationship.
- 27010 – Information security management for inter-sector and inter-organizational communications.
- 27018 – Code of practice – handling PII / SPI (Privacy) – Protection of Personally Identifiable Information (PII) in public clouds.
- 27034 – Application security techniques – guidance to ensure software delivers necessary level of security in support of an organisations security management system.
- 27035 – Information security incident management.
- 29101 – Privacy architecture framework.
- 29119 – Software testing standard.

DEFSTAN

- 05-138 – Cyber security for defence suppliers.

NIST

- 800-30 - Guide for conducting risk assessments.
- 800-88 - Guidelines for media sanitization.
- SP 800-50: Building an information technology security awareness and training program.
- SP 800-61: Computer security incident handling guide.

Other

- Microsoft Security Development Lifecycle (SDL).
- SAFE Code best practices.
- OWASP Comprehensive, Lightweight Application Security Process (CLASP).
- HMG Security policy framework.
- PAS 1192-5 – BSI publication on security-minded building information modelling, digital built environments and smart asset management.
- PAS 754 – BSI publication on Software Trustworthiness, governance and management.
- NCSC Cyber Essentials and 10 steps.
- To download a copy visit gov.uk.
- For further info contact cyber@dft.gsi.gov.uk.

Figure 4: Application standards and guidance related to cyber security for connected and automated vehicles (non-exhausted list) [22]

Liability Legislation:

Product liability is covered under the Consumer Protection Act 1987, which provides injured parties with a legal course of action against manufacturers (and importers) for compensation in the event of death, injury or property damage resulting from a defective product [21]. This implemented the European Product Liability Directive 1985. However, in the case of automated vehicles it was not clear in law who might be held responsible in the event of the collision under the Road Traffic Act 1988. The first piece of UK legislation introduced to address this, the Automated and Electric Vehicles Act 2018, was passed into UK law by Royal Assent in July 2018 [23], having had its first reading in October 2017.

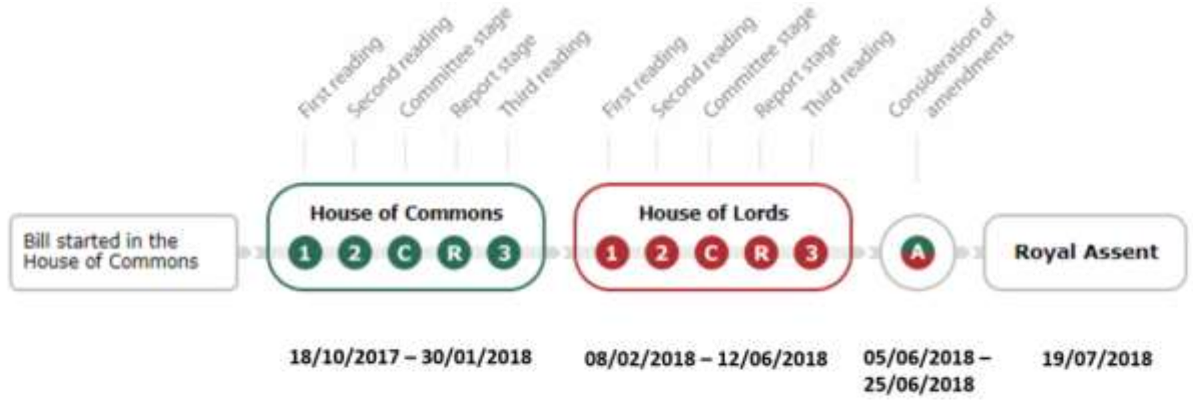


Figure 5: Progress of the UK Automated and Electric Vehicles Act 2018

The focus of the Bill in regard to Automated Vehicles (AV) was related to the liability of insurers. As part of this, it is required that the Secretary of State maintains a list of motor vehicles capable of, and may be lawfully used for, automated driving. Vehicles on this list are thus recognised 'automated vehicles' and subject to this legislation. Within two years of the publication of this list they must also prepare a report assessing the impact and effectiveness of the Act provisions. The Act defines that if an AV is insured, then then insurer would be liable for damage arising through an accident caused by an AV. 'Damage' here relates to death or personal injury to a person and damage to property other than the AV or related to certain goods carried therein). If the AV is not insured (unless exempt under certain provisions of the Road Traffic Act 1988), the owner of the vehicle is liable. Furthermore, the Act states that insurance policy compulsory terms may not limit liability beyond the specifications of the Road Traffic Act 1988. However, it does allow that insurance policies may limit liability when the accident is a result of prohibited software alterations or failure to update critical software[3]. Exceptions to sole liability apply if the accident or damage may have been partly caused by the injured party and/or if the driver of the AV allowed the vehicle to drive itself when it was "not appropriate to do so"[4]. The right of the insurer to claim against responsible persons is also defined within the Act, as is the conditions for settlement, and the application of enactments of previous legislations (Fatal Accidents Act 1976, Congenital Disabilities (Civil Liability) Act 1976, Law Reform (Contributory Negligence) Act 1945, Civil Liability (Contribution) Act 1978 and Law Reform (Miscellaneous Provisions) (Scotland) Act 1940).

2.7 Legislation in Germany

In Germany, every road user is required to comply with certain regulations and laws in road traffic. The entire fundamentals of road traffic law in Germany are described in the Road Traffic Act (Straßenverkehrsgesetz), abbreviated StVG [105]. A look at the content of the StVG can help to find regulations. The history of the Road Traffic Act StVG goes back to the year 1909. The Road Traffic Act is divided into seven sections and consists of about 60 paragraphs. The following overview shows the individual sections of the StVG:

- StVG I: Traffic regulations (Verkehrsvorschriften)
- StVG II: Liability: (Haftpflicht)
- StVG III: Penalty and fine regulations (Straf- und Bußgeldvorschriften)
- StVG IV: Driving ability register (Fahreignungsregiste)
- StVG V: Vehicle register (Fahrzeugregister)
- StVG VI: Driving licence register (Fahrerlaubnisregister)
- StVG VII: Common rules, transitional regulations (Gemeinsame Vorschriften, Übergangsbestimmungen)

The road traffic law from 1909 does not provided legal framework for autonomous driving, since the autonomous system was not developed at that time. Several research and development projects of autonomous vehicles are conducted by different German automobile manufacturers like Mercedes-Benz, Volkswagen, Audi, BMW and research organizations like the German Aerospace Center (DLR), Fraunhofer Institute, Freie Universität of Berlin (FU). To support these innovative projects, German government has taken some important initiatives in term of the regulation of the autonomous driving within the legal framework. Two significant measures have been taken by the German government for the regulation of highly and fully automated driving: the amendment of the current road traffic law (StVG) and the adoption of ethical principles for autonomous driving. Other important measures of the German government are the investment in AV infrastructure and pilots. The digital motorway test bed established on the A9 motorway by the transport ministry, the state of Bavaria and automotive and technology industry bodies are examples of such investment.

The two selected measures mentioned above are described in detail in the following sections:

[3] Software required for safe operation of the vehicle.

[4] Though the act does not guide nor define when it is or is not appropriate. However, 'self-driving' is defined as 'operating in a mode in which it is not being controlled, and does not need to be monitored, by an individual'.

Amendment of the traffic law (StVG) for autonomous driving:
The adaptation and amendment of the current traffic law StVG from 1909 has been done by adding new and adapted existing paragraphs to allow the self-driving car on the German roads and give also the path to showrooms and pilot test sites. The decree of the amendment of the traffic law StVG to support highly and fully autonomous driving has been published in the official law journal of the federal republic (Bundesgesetzblatt) Part I Nr.28 on June 20th, 2017 with the title "Achtes Gesetz zur Änderung des Straßenverkehrsgesetzes" [106]. On June 21st, 2017, one day after the publication the new regulations for automated driving came into force. The new law regulates the autonomous driving within a legal framework and creates the prerequisites for the development and testing of partially highly and fully automated vehicles in Germany. Some selected relevant new paragraphs §1a, §1b, §1c of the StVG for highly and fully automated driving are summarized in Table 2.

Table 2: Selected paragraphs

- §1: Authorization (Zulassung)
  - § 1a Motor vehicles with highly or fully automated driving functions
    - (1) The operation of a motor vehicle by means of highly or fully automated driving function is **permitted** if the function is used as intended.
    - (2) Motor vehicles with highly or fully automated driving function within the meaning of this Act are those which have technical equipment,
      - 1. which can control the driving task - including longitudinal and transverse guidance - the respective motor vehicle after activation control (vehicle control)
      - 2. which is able to comply with the traffic regulations directed at the vehicle guidance during highly automated or fully automated vehicle control,
      - … The manufacturer of such a motor vehicle must declare in the system description that the vehicle complies with the requirements of sentence (1).
  - §1b Rights and obligations of the driver when using highly or fully automated driving functions
    - (1) ...
    - (2) The driver is obliged to take over the vehicle control immediately,
      - 1. when the highly automated or fully automated system asks him or
      - 2. if he&she recognizes or, because of obvious circumstances, one must recognize that the prerequisites for the intended use of the highly or fully automated driving functions no longer exist
  - §1c Evaluation
    - 1 The Federal Ministry of Transport and Digital Infrastructure will evaluate the application of the regulations in Article 1 of the law of 16 June 2017 (Federal Law Journal I p. 1648) after the end of the year 2019 on a scientific basis.
    - 2 The Federal Government informs the German Federal Parliament about the results of the evaluation.

§ 63a Data processing in motor vehicles with highly or fully automated driving functions

• (1) Motor vehicles according to § 1a store the position and time information determined by a satellite navigation system when a change of vehicle control between the driver and the highly or fully automated system takes place. Such storage also occurs when the driver is prompted by the system to take control of the vehicle or a technical malfunction of the system occurs. • (2) … • (3) The vehicle owner shall arrange for the transmission of the data recorded in accordance with paragraph 1 to third parties, if: o 1. if the data are necessary for asserting, satisfying or defending legal claims in connection with an event regulated in § 7 (1); and o 2.1 if the corresponding motor vehicle with automated driving function was involved in this event. 2.2 Paragraph 2 Sentence 3 applies accordingly. • (4) The data stored in accordance with paragraph 1 shall be deleted after six months, unless the vehicle was involved in an event regulated in § 7 (1); In this case, the data must be deleted after three years. • (5) In connection with a step in § 7 1 regulated event stored in accordance with paragraph 1, data can be transmitted in anonymous form for the purposes of accident research to third parties.
§ 63b Authorization Basics

Adoption of ethical principles for autonomous driving:
An ethic commission “automated and connected driving” appointed by the German Federal Ministry of Transport and Digital Infrastructure has been created with the mission to analyse and propose ethical principles in term of rules, guidelines, procedures for automation driving in general.
The ethics commission consists of five working groups that deal with the following five topics related to the self-driving use case:

- Working group 1: Situations involving unavoidable harm
- Working group 2: Data availability, data security, data-driven
- Working group 3: Conditions of human-machine interaction
- Working group 4: Consideration of the ethical context beyond road traffic
- Working group 5: Scope of responsibility for software and infrastructure

The final report [107] of the ethic commission containing detailed information about the ethical principles for autonomous driving has been published in June 2017.

The main aspects of the new regulation for self-driving car are summarized as follow:

- The new German law does not allow autonomous driving when all the occupants are merely passengers because the driver must be ready to take over again if and when required, but the car manufacturer is responsible for the accidents if the system fails.

The ethical principles in place require autonomous driving software to prioritise human lives over animals and property.

International legislation outside Europe

Below we give a status overview regarding autonomous vehicles legislation in selected countries outside Europe.

2.8 Legislation in USA

A comprehensive "introduction" to a new policy on highly autonomous vehicles (HAV) was published in 2016 by the U.S. Department of Transportation (U.S. DOT) and the National Highway Traffic Safety Administration: "Federal Automated Vehicles Policy - Accelerating the Next Revolution in Roadway Safety" [5]. Portions of the policy can apply to lower levels of automation. The main components of the policy are repeated below [5][6]:

- **Vehicle Performance Guidance for Automated Vehicles -** The guidance for manufacturers, developers and other organizations outlines a 15 point “Safety Assessment” for the safe design, development, testing and deployment of automated vehicles.
- **Model State Policy -** This section presents a clear distinction between Federal and State responsibilities for regulation of HAVs and suggests recommended policy areas for states to consider with a goal of generating a consistent national framework for the testing and deployment of highly automated vehicles.
- **Current Regulatory Tools -** This discussion outlines DOT’s current regulatory tools that can be used to accelerate the safe development of HAVs, such as interpreting current rules to allow for greater flexibility in design and providing limited exemptions to allow for testing of non-traditional vehicle designs in a timelier fashion.
- **Modern Regulatory Tools -** This discussion identifies potential new regulatory tools and statutory authorities that may aid the safe and efficient deployment of new lifesaving technologies.

The development of Automated Driving Systems (ADSs), is commonly referred to as automated or self-driving vehicles. The U.S. DOT and the NHTSA have prepared a voluntary guidance "Automated Driving Systems 2.0 - A vision for safety" published in 2017 to promote improvements in safety, mobility and efficiency through ADSs [3]. Nine out of ten serious roadway crashes occur due to human behaviour, automated vehicle technologies have the potential to save thousands of lives, and safety is the number one priority. This updated policy framework replaces the Federal Automated Vehicle Policy released in 2016, and offers a nonregulatory approach to automated vehicle technology safety, and a path forward for the safe deployment of ADSs by [3]:

- Encouraging new entrants and ideas that deliver safer vehicles.
- Making department regulatory processes nimbler to help match the pace of private sector innovation.
- Supporting industry innovation and encouraging open communication with the public and stakeholders.

The framework document is divided into two main sections: 1) Voluntary Guidance for ADSs and 2) Technical Assistance to States - best practices for legislatures regarding ADSs. The first section supports the automotive industry and other key stakeholders as they consider and design best practices for the testing and safe deployment of ADSs (SAE automation levels 3 through 5). To ensure consistency in taxonomy usage, the SAE Internationals' levels of automation and other applicable terminology are adopted [3][4]. The framework document points out twelve priority safety design elements for consideration, including System safety, Operational and event detection and response, Fallback (minimal risk condition), Validation methods, Human machine interface (HMI), Vehicle cybersecurity, Crashworthiness, Post-crash ADS behaviour, Data recording, Consumer education and training, and Federal, state and local Laws. In more of these twelve priority elements, entities are encouraged to cooperate with established and accredited standards-developing organizations, and adopt voluntary guidance, best practices, design principles, and standards developed by such as ISO (International Standards Organization), SAE International (Society of Automotive Engineers), ANSI (American National Standards Institute), etc., as well as standards and processes available from other industries (e.g. aviation, space, military). Vehicles on public roads are subjected to both Federal and State jurisdiction, and States are beginning to draft legislation to safely deploy emerging ADSs.

The second section contains best practices for legislatures regarding AMSs and support this State work [3]. The Federal and State roles in ADSs regulation are clarified and delineated. States continue to be responsible for regulating the human driver and vehicle operations, while NHTSA remains responsible for regulating the safety design and performance aspects of vehicles and vehicle equipment. Best practices for legislatures incorporate common safety-related components and significant elements regarding ADSs that States should consider incorporating in the legislation. It also provides best practices for State Highway Safety Officials, which offers a framework for States to develop procedures and conditions for ADSs' safe operation on public roadways, and considerations in such areas as applications and permissions to test, registration and titling, working with public safety officials, and liability and insurance.

It is important to have an overview of the Federal and State regulatory responsibilities for motor vehicle operation and should remain largely unchanged for ADSs. NHTSA is responsible for regulating motor vehicles and motor vehicle equipment, while States are responsible for regulating the human driver and most other aspects of motor vehicle operation (Table 3) [3]. Further U.S. DOT involvement includes safety, evaluation, planning, and maintenance of the National infrastructure through the Federal Highway Administration (FHWA) as well as regulation of the safe operation of interstate motor carriers and commercial vehicle drivers, along with registration and insurance requirements through the Federal Motor Carrier Safety Administration (FMCSA). States are strongly encouraged to allow U.S. DOT alone to regulate the safety design and performance aspects of ADS technology.

Table 3: Federal and State regulatory roles, Source U.S. DOT/NHTSA [3]

NHTSAs' responsibilities	States' responsibilities
Setting Federal Motor Vehicle Safety Standards (FMVSSs) for new motor vehicles and motor vehicle equipment (with which manufacturers must certify compliance before they sell their vehicles).	Licensing human drivers and registering motor vehicles in their jurisdictions.
Enforcing compliance with FMVSSs.	Enacting and enforcing traffic laws and regulations.
Investigating and managing the recall and remedy of non-compliances and safety related motor vehicle defects nationwide.	Conducting safety inspections, where States choose to do so.
Communicating with and educating the public about motor vehicle safety issues.	Regulating motor vehicle insurance and liability.

Regarding best practices for legislatures, NHTSA recommends the following when crafting legislation for ADSs [3]:

- Provide a "technology-neutral" environment.
- Provide licensing and registration procedures.
- Provide reporting and communications methods for Public Safety Officials.
- Review traffic laws and regulations that may serve as barriers to operation of ADSs.

The number of states considering legislation related to autonomous vehicles are gradually increasing in the USA [1]. The National Conference of State Legislatures (NCSL) inform that 22 states have enacted legislation related to autonomous vehicles in 2017. The current states are illustrated in Figure 6. NCSL has also an autonomous vehicles legislative searchable database, providing information about state autonomous vehicle legislation that has been introduced [2]. This is an up to date, "real-time" database, which illustrates the importance of these issues. The searchable topics are divided into: Commercial, (including platooning); Cybersecurity of vehicle; Definitions;

Infrastructure and connected vehicles; Insurance and liability; Licensing and registration; Operation on public roads; Operator requirements; Privacy of collected vehicle data; Request for study; Vehicle inspection requirements; Vehicle testing; and other.

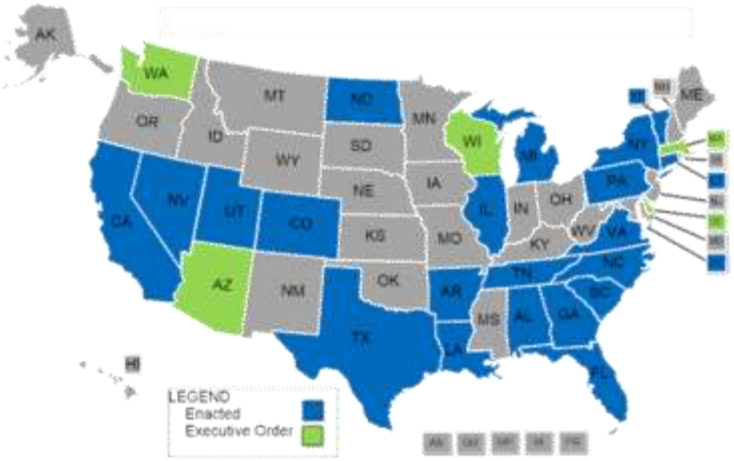


Figure 6: States with enacted autonomous vehicle legislation, Source NCSL [1]

2.9 Legislation in China

China plans to adopt the UN Regulations and is preparing extensive new regulations (30 new standards until 2020 and 100 new standards until 2025) [84]. However, China has a set of national standards for testing autonomous vehicles on roads. Approximately 12 regional governments have issued guidelines for road testing of autonomous vehicles. The alliance with several industries was commissioned by the Ministry of Industry and Information Technology (MIIT). Safety has been considered an overriding necessity and the set of standards cover vehicle tests in 34 different traffic conditions [94]. The National Rules have been issued following the local regulations on autonomous vehicles in Beijing, Shanghai and Chongqing [95]. The MIIT, Ministry of Public Security (MPS) and Ministry of Transport (MOT) are the regulators for autonomous vehicle testing. The local authorities require to report on autonomous vehicle testing in their respective provinces to the regulators. The test applicant under the National Rules is required to be an independent legal entity registered in China who is in the business of auto or component manufacturing, technology, vehicle testing or R&D. Moreover, the test applicant is required to have an assessment program, along with remote monitoring capability. They should have an ability to record, analyse and remake the incident of the autonomous test vehicles. The test applicant is also required to have the financial capability for any personal injury or property damage caused during the testing. The test driver is required to hold a valid driving license with three years unblemished driving experience and a good technical understanding of the autonomous drive testing program and operation methods.

Requirements on the test vehicles under the National Rules are mostly same as under the Local Regulations. Test vehicles cover passenger and commercial cars but not low-speed vehicles or motorcycles. The test vehicles should meet all statutory testing requirements except for endurance and should not be already registered with the authority. The National Rules specify that the test driver must sit in the driver seat and monitor the status of the test vehicle and the driving environment. Test vehicles must be able to shift from self-driving to conventional modes of driving, in order to ensure that the test driver can quickly take over control in case of a malfunction or an emergency. Test vehicles should be able to monitor the status of the test vehicle online and should be able to transfer in real time information the control mode of the test vehicle, vehicle location and vehicle speed and acceleration. Test vehicles must be able to record and store specific information for minimum 90 seconds prior to an accident or malfunction and based on the National Rules, this data should be available for at least three years. The autonomous function of the test vehicles should be tested and verified by third party testing institutes recognised by the authorities [96]. The National Rules require that the local authorities should select suitable roads for autonomous car testing and should make the information available to the public. The test applicant must provide the necessary technical materials to the local authorities for examination. The local authorities should issue a test notice letter to qualified test applicants. The test applicant must obtain a road accident insurance, not less than RMB 5 million or an undertaking letter to compensate for an equivalent level of accident liability. The testing vehicle must complete pre-required tests in a closed testing area, simulating real traffic environment. In addition, the test vehicle also needs to meet the compulsory national testing standards for normal vehicles.

Test vehicles are issued a temporary vehicle plate which must to be returned to the authorities after the test period. The temporary car plate must be obtained in the province where it will be tested. In case the test is conducted in another province, a new temporary car plate should be obtained, or the condition should be waived locally. Autonomous vehicles test can only be conducted on designated roads and in designated periods. The test drivers and the test applicants are liable for any violation of traffic laws and any traffic accidents caused. Where an accident causes serious personal injury, vehicle damage or death, the test applicant is required to submit a report to the local authorities within 24 hours, which is submitted to the regulators within three working days. Within five working days after liability is determined, the test applicant must submit an accident report to the local authorities, who will then submit it to the regulators. Based on the *Guidelines on Standards for Connected Vehicles Industry* (Standard Guidelines), autonomous vehicles are divided into 'assisted control' and 'automated control', with five levels of automation

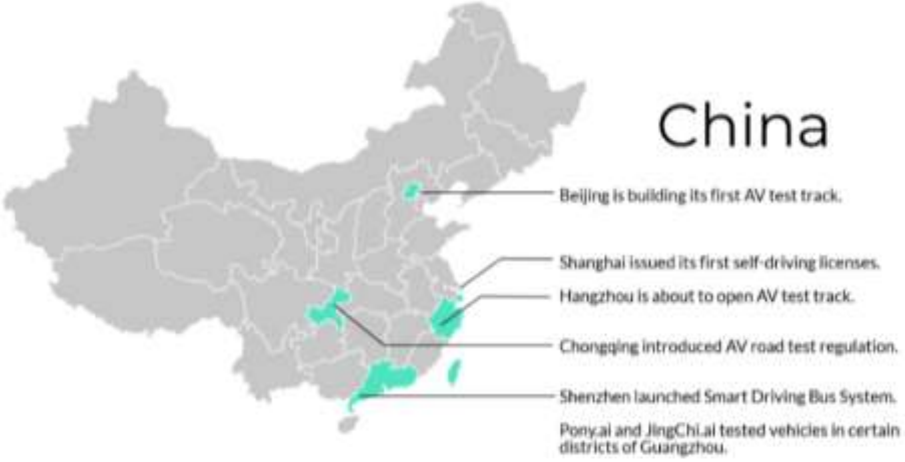
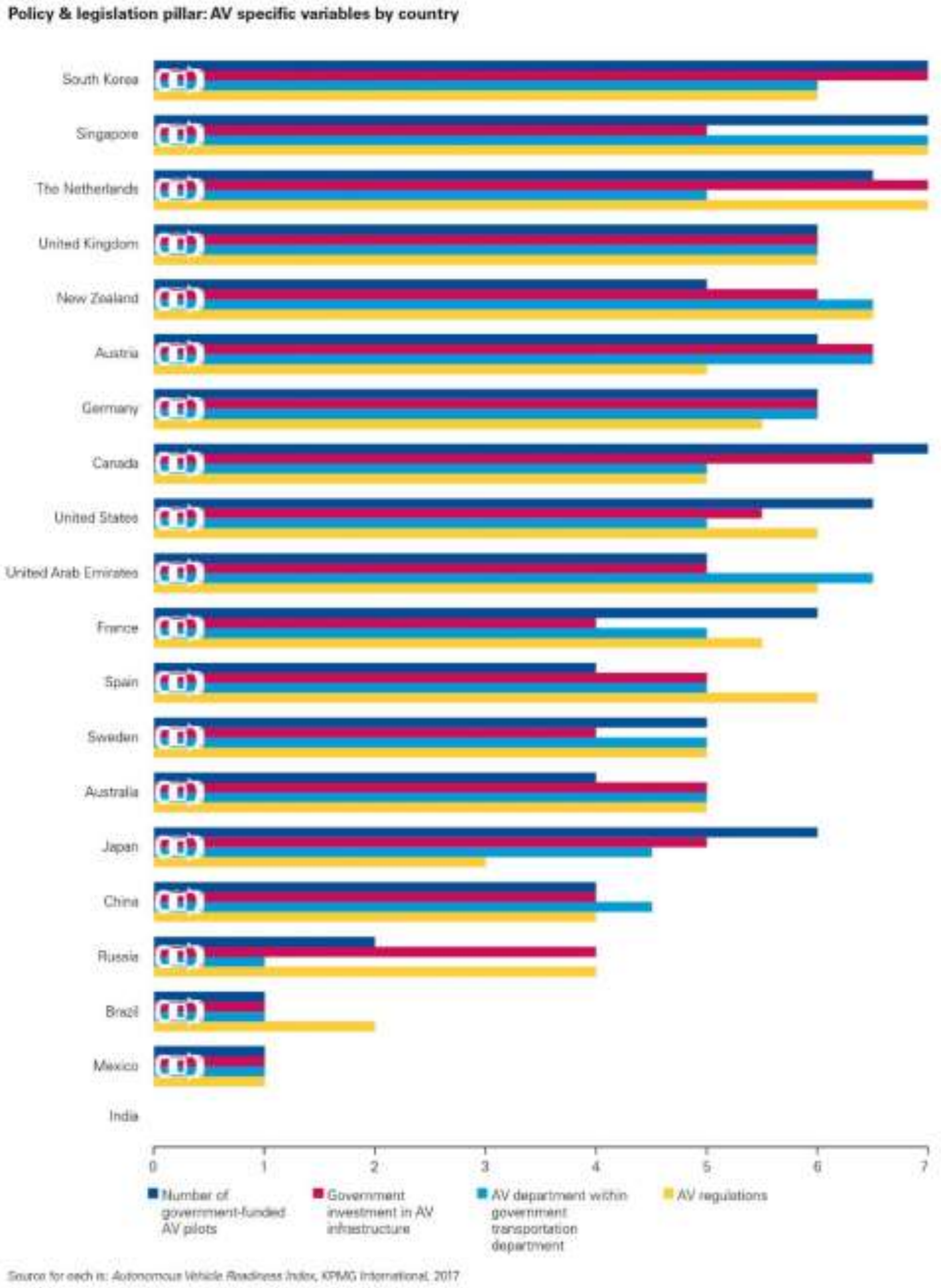

China
Beijing is building its first AV test track.
Shanghai issued its first self-driving licenses.
Hangzhou is about to open AV test track.
Chongqing introduced AV road test regulation.
Shenzhen launched Smart Driving Bus System.
Pony.ai and JingChi.ai tested vehicles in certain districts of Guangzhou.

Figure 7: Autonomous vehicle testing in China [97]

. The automation level of the self-driving cars under the National Rules includes conditional automation, high-level automation and full automation. The issuing of the National Rules adds momentum to China's regulation for road testing of autonomous vehicles and allows for increased road testing of autonomous vehicles across China. In March 2018, Shanghai issued the first autonomous driving licenses to allow the testing of autonomous vehicles. In January 2018, the Beijing Municipal Traffic Commission announced the building of autonomous driving tracks while China's autonomous vehicle industry hub, Guangzhou, allowed Pony.ai and JingChi.ai to test vehicles in certain areas [97]. The country also has the second highest density of electric charging stations and one of the highest consumer acceptance scores for autonomous vehicles [31]. Figure 7 provides an overview of autonomous vehicle testing in China [97].

2.10 Legislation in Singapore

Singapore is widely considered to be at the forefront of automated vehicle (AV) adoption [21], and is ranked top in Policy and Legislation in the KPMG Index of Automated Readiness [31]. An overview on several countries on different continents is presented in Figure 8 to visualize the global policy and legislation readiness index.



Source for each is: *Autonomous Vehicle Readiness Index*, KPMG International, 2017

Figure 8: **AV Policy and Legislation variable scores in the KPMG Autonomous Vehicle Readiness Index** [31]

The autonomous vehicle high readiness index for Singapore shown in Figure 8 confirm the importance of having government funded pilots and infrastructure investment, a single department for AV policy (the Singapore Automated Vehicles Initiate, established in 2014) and Regulations tailored for AV. The existing Road Traffic Act includes powers to exempt or modify existing provisions, so changes can be made quickly to adapt to new technologies, and additional legislative amendments will give the Minister for Transport the power to make subsidiary legislations to regulate the use of AVs [32]. The Committee for Autonomous Road Transport for Singapore (CARTS), which was set up in 2014 and consists of both government agencies and private organizations [33], have a working group on Regulations and Implementation [32]. As an early adopter of V2X technologies, Singapore established a taskforce to address 5.9GHz dedicated short range communication (DSRC) Standards, releasing a dedicated technical standard for intelligent transport systems in October 2016.

Trial Approval Rules

New legislation is billed for late 2018 [34], but the key piece of legislation already passed in Singapore is the Road Traffic (Autonomous Motor Vehicles) Rules 2017. This came into operation in August 2017 and sets out provisions to approve trials or special uses of autonomous vehicles and duties of specified persons. Within this, fines of up to $5000 may be imposed if an autonomous vehicle (or technology) is trailed or used on the road without the correct authorization. This also sets out the requirements of an application to undertake a trial, the associated costs, reasons for cancelling/suspending authorization and liability insurance. Conditions of granting trial authorizations may be related to:

- Geographical area;
- Requirements of safety driver;
- Carriage of passengers;
- Hire and reward for using vehicles;
- Named participants, and;
- Technical specifications.

The Rules also set out duties for specified persons within the trials. This includes maintenance (which carries fines when not ensured), data collection and storage, and a duty for recording, reporting and testing. The following data must be collected and stored for at least 3 years, with a fine imposed if it is not correctly maintained, edited or failed to be provided on request by the authority. A fine is also imposed if records are not maintained, incidents and accidents are not reported and if requested tests are not carried out.

- Date and time;
- Location;
- Speed;
- Status;
- Over-ride history;
- Sensor data, and;
- Camera/video footage.

2.11 Legislation in South Korea

The South Korean government has made heavy investments in automated vehicles [97], scoring highly in the KPMG AV Readiness scores (Figure 8) for government investment in both pilot tests and infrastructure [31]. In 2016, the Ministry of Land, Infrastructure and Transport (MOLIT) had committed to the commercialization of autonomous vehicles by 2020 [98]. Their commercialization support policy is shown in Figure 9. This was supporting by research programs, licensing and insurance development, test-driving and infrastructure design standards. Aspirations are supported by many of South Korean innovative technology companies such as Hyundai and Samsung.

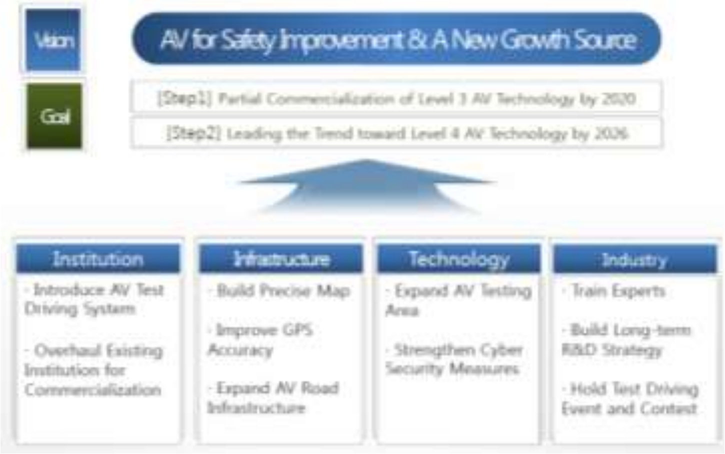

Vision
AV for Safety Improvement & A New Growth Source
Goal
[Step1] Partial Commercialization of Level 3 AV Technology by 2020
[Step2] Leading the Trend toward Level 4 AV Technology by 2026
Institution
- Introduce AV Test Driving System
- Overhaul Existing Institution for Commercialization
Infrastructure
- Build Precise Map
- Improve GPS Accuracy
- Expand AV Road Infrastructure
Technology
- Expand AV Testing Area
- Strengthen Cyber Security Measures
Industry
- Train Experts
- Build Long-term R&D Strategy
- Hold Test Driving Event and Contest

Figure 9: MOLIT AV Commercialisation Support Policy [99]

The flagship program is the building of the world's largest test-bed, K-City [31]. This complex, which opened in 2017 and is due for completion by the end of 2018, covers 363,000 M^2 at a cost of $11bn [97][100]. Rural roads, motorways, urban areas, community zones and parking facilities are all included, as depicted in Figure 10. There is a 5G network installed, and it offers 35 different driving conditions (including environmental, potholes, pedestrian crossings and toll gates), all of which will be trialled to inform regulatory development as well as technological. As part of K-City testing, the value of collected data for insurance and urban planning will be assessed [101]. In addition to K-City, there have been numerous trials, across the country, such as a vehicle fleet and shuttle service during the 2018 Winter Olympics.

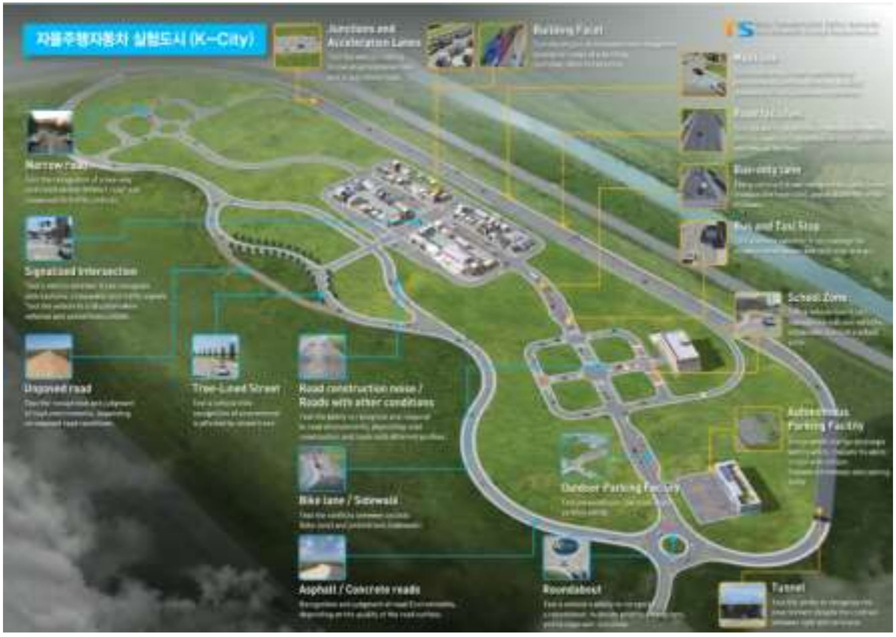
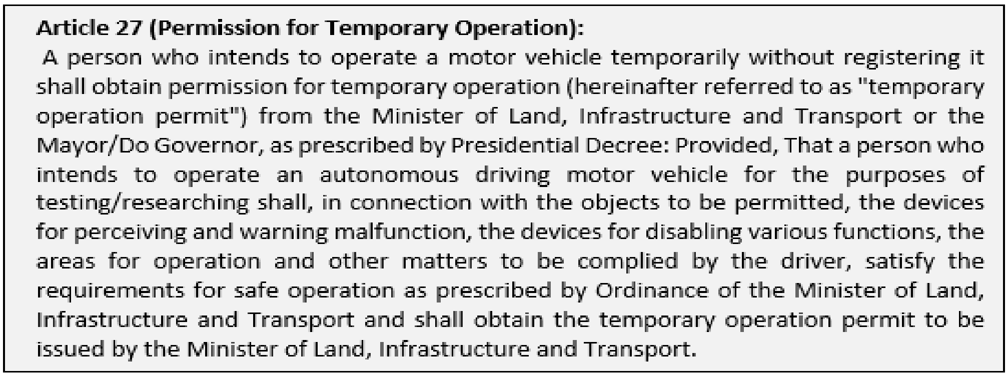


Figure 10: South Korea K-City schematic [101]

South Korea were actively involved in setting up the International Standards with UNECE/WP29, and have set up insurance policy, inspection and recall regimes. The Government are currently examining rules and regulations around AV testing, including safety evaluation technology to develop safety standards, and the revision of standards (by the end of 2018) in line with cyber security guidelines. Furthermore, major cities are being mapped to install smart systems [102], and 5000km of public roads will be included in a high precision map and equipped with smart sensors for the 2020 commercialization target [103]. Also, in support of this target, AVs are already allowed to operate under license on over 300km of public roads on pilot projects (for both technological development and public acceptance) and by mid-2018 46 licenses have been granted. This is managed by the Motor Vehicle Management Bureau and the Advanced Motor Technology Division established in 2016. In 2016, the AV Test Driving System was introduced, which included amendment of the Motor Vehicle Management Act to allow AV testing for research by qualified testers.



Article 27 (Permission for Temporary Operation):

A person who intends to operate a motor vehicle temporarily without registering it shall obtain permission for temporary operation (hereinafter referred to as "temporary operation permit") from the Minister of Land, Infrastructure and Transport or the Mayor/Do Governor, as prescribed by Presidential Decree: Provided, That a person who intends to operate an autonomous driving motor vehicle for the purposes of testing/researching shall, in connection with the objects to be permitted, the devices for perceiving and warning malfunction, the devices for disabling various functions, the areas for operation and other matters to be complied by the driver, satisfy the requirements for safe operation as prescribed by Ordinance of the Minister of Land, Infrastructure and Transport and shall obtain the temporary operation permit to be issued by the Minister of Land, Infrastructure and Transport.

Figure 11: Automated Vehicle amendment to the Motor Vehicle Management Act [104]

2.12 Autonomous vehicles readiness and ranking

The overall autonomous vehicles readiness index results and the ranking of different countries around the world, are based on four different criteria: policy and legislation, technology and innovation, infrastructure and consumer acceptance are prepared by KPMG and presented in Table 4 [31]. The table figures are also visually represented in Figure 8.

Table 4: Overall Autonomous Vehicles Readiness Index Results [31]

Overall rank	Country	Total score	Policy and legislation		Technology and innovation		Infrastructure		Consumer acceptance	
			Rank	Score	Rank	Score	Rank	Score	Rank	Score
1	The Netherlands	27.73	3	7.89	4	5.46	1	7.89	2	6.49
2	Singapore	26.08	1	8.49	8	4.26	2	6.72	1	6.63
3	United States	24.75	10	6.38	1	6.97	7	5.84	4	5.56
4	Sweden	24.73	8	6.83	2	6.44	6	6.04	6	5.41
5	United Kingdom	23.99	4	7.55	5	5.28	10	5.31	3	5.84
6	Germany	22.74	5	7.33	3	6.15	12	5.17	12	4.09
7	Canada	22.61	7	7.12	6	4.97	11	5.22	7	5.30
8	United Arab Emirates	20.89	6	7.26	14	2.71	5	6.12	8	4.79
9	New Zealand	20.75	2	7.92	12	3.26	16	4.14	5	5.43
10	South Korea	20.71	14	5.78	9	4.24	4	6.32	11	4.38
11	Japan	20.28	12	5.93	7	4.79	3	6.55	16	3.01
12	Austria	20.00	9	6.73	11	3.69	8	5.66	13	3.91
13	France	19.44	13	5.92	10	4.03	13	4.94	10	4.55
14	Australia	19.40	11	6.01	13	3.18	9	5.43	9	4.78
15	Spain	14.58	15	4.95	16	2.21	14	4.69	17	2.72
16	China	13.94	16	4.38	15	2.25	15	4.18	15	3.13
17	Brazil	7.17	20	0.93	18	0.86	19	1.89	14	3.49
18	Russia	7.09	17	2.58	20	0.52	20	1.64	18	2.35
19	Mexico	6.51	19	1.16	17	1.01	17	2.34	19	2.00
20	India	6.14	18	1.41	19	0.54	18	2.28	20	1.91

3. Autonomous vehicles and IoT policy framework

The four pillars of the autonomous vehicles (AV) and IoT policy framework are Trust, Security, Privacy and Engagement as illustrated in Figure 12.

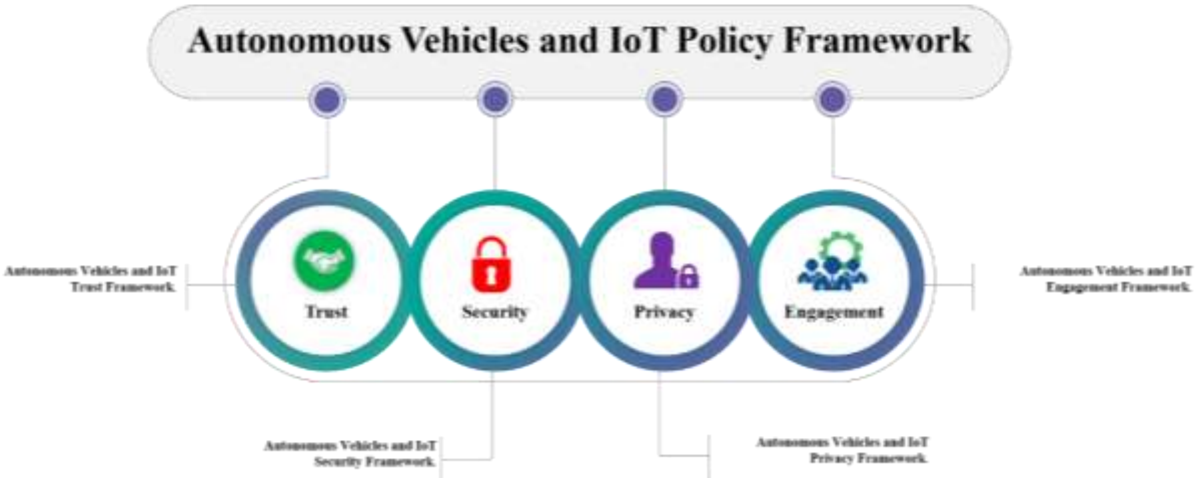

Autonomous Vehicles and IoT Policy Framework
Autonomous Vehicles and IoT Trust Framework
Trust
Security
Privacy
Engagement
Autonomous Vehicles and IoT Engagement Framework
Autonomous Vehicles and IoT Security Framework
Autonomous Vehicles and IoT Privacy Framework

Figure 12: The four pillars of AV and IoT policy framework

The autonomous vehicles and IoT applications cover several domains of interaction, communication, exchange of information and knowledge as illustrated in Figure 14. The figure illustrates all the domains of interactions between the autonomous vehicle and the environment through communication and sensing capabilities. The overall interactions are covered under the name Vehicle to Environment (V2E) and consists of communication and sensing interactions between the autonomous vehicle and the dynamically changing environment (e.g. other terrestrial vehicles, pedestrians, cyclists, aerial and naval/maritime vehicles, different types of IoT devices, etc.), the communication and sensing interactions between the vehicle and its static environment (e.g. charging stations, traffic signals, tolling systems, electronic parking, roads, buildings, home, IoT devices, etc.), communication and sensing interactions with different service providers (e.g. network communication providers, cloud/edge service providers, etc.) and the communications with the owners, users, mobility service providers (e.g. vehicle owners, users, vehicles fleet owners/operators, vehicles producers, IoT service providers, maintenance providers, etc.).

The convergence of autonomous vehicles, IoT and AI applications are accelerating the implementation of IoV concept and the move to Mobility as a Service (MaaS) and tier-one automotive companies, large technology companies and technology start-ups active involved in V2E, addressing first safety, security and privacy use cases to accelerate user acceptance and innovation.

3.1 Communication technologies

3.1.1 V2X communication technologies

Through C-ITS platform Phase II, EU has worked out a Certificate Policy for Deployment and Operation of C-ITS [125][126]. The EU is preparing a Delegated Act for C-ITS (Cooperative Intelligent Transport Systems). Regarding future autonomous driving and a corresponding traffic control, this act will define how the communication between vehicles and with the infrastructure should be carried out [124]. This will regulate V2X communication and put requirements on C-ITS stations and priority services (e.g. traffic lights), as well as security and privacy issues.

For autonomous vehicles and IoT applications the communication technologies used cover the licensed and unlicensed spectrum. The communication systems used by autonomous vehicles applications for providing V2X services are cellular 4G/LTE, LTE-V2X (3GPP R14), 5G NR network in cm- and mm-Wave frequency bands, ITS-G5 and Vehicular Visible Light Communication (VVLC).

Table 5 presents the main categories of V2X use cases and their key performance requirements in terms of reliability, communication latency, and the expected data rate per vehicle as analysed by 3GPP for C-V2X communications [82].

Table 5: Performance requirements of different V2X use cases [82]

Use Case Type	V2X Mode	End-to-End Latency	Reliability	Data Rate per vehicle (kbps)	Comm. Range*
Cooperative Awareness	V2V/V2I	100ms-1sec	90-95%	5-96	Short to medium
Cooperative Sensing	V2V/V2I	3ms-1sec	>95%	5-25000	Short
Cooperative Manoeuvre	V2V/V2I	<3ms-100ms	>99%	10-5000	Short to medium
Vulnerable Road User	V2P	100ms-1sec	95%	5-10	Short
Traffic Efficiency	V2N/V2I	>1sec	<90%	10-2000	Long
Teleoperated Driving	V2N	5-20ms	>99%	>25000	Long

**Communication range is qualitatively described as "short" for less than 200 meters, "medium" from 200 meters to 500 meters, and "long" for more than 500 meters.*

Table 6 summarises the quality assessment of communication technologies to support use case categories. These communication systems support use cases that have less stringent requirements (e.g., Traffic Efficiency by LTE-V2X and Cooperative Awareness by both LTE-V2X/C-V2X and IEEE 802.11p, V2X ITS-G5, DSRC). The technologies fall short of supporting the complete set of requirements. Future developments need to address the gaps.

Table 6: Quality assessment of communication technologies to support V2X use cases [78][79][80]

Use Case Type	LTE-V2X	ITS-G5	mmWave	VVLC
Cooperative Awareness:				
Emergency Vehicle Warning	++	++	-	-
Forward Collision Warning	++	++	+	+
Cooperative Sensing:				
See-through	+	+	++	+
Sensor Sharing	+	+	+	+
Cooperative Manoeuvre:				
Platooning	++	+	+	+
High Density Platooning (require C-V2X)	-	-	-	-
Cooperative Adaptive Cruise Control	+	+	-	-
Cooperative Intersection Control	+	+	-	-
Vulnerable Road User	+	+	-	-
Traffic Efficiency	++	+	-	-
Remote-operated Driving	+	-	-	-

++: suitable technology to support the use case and requirements under all circumstances with no (or with minor) configuration;

+: suitable technology to support the use case and performance requirements under specific conditions (e.g., low congestion level);

-: not suitable technology because the specific use case or its performance requirements are not supported

Licensed cellular technologies cover both cellular vehicle-to-everything (C-V2X) specific for autonomous vehicles and narrowband IoT (NB-IoT), LTE for Machine Type Communications (LTE-M) and Enhanced Coverage GSM (EC-GSM) used for specific IoT services based on the existing cellular networks. 5G brings additional capabilities to support new services and new markets:

- **Enhanced Mobile Broadband (eMBB)** providing higher data rates, higher traffic or connection density, high user mobility, and support for several different deployment and coverage scenarios. eMBB support different service areas (e.g., indoor/outdoor, urban and rural areas, office and home, local and wide areas connectivity), as well as special deployments (e.g., massive gatherings, broadcast, residential, and high-speed vehicles).
- **Critical Communications (CC) and Ultra Reliable and Low Latency Communications (URLLC)** providing very low latency and very high communications service availability enabling new services such as industrial automation. For example, in the context of remote control for process automation, a reliability of 99,9999% is envisioned, with a user experienced data rate up to 100 Mbps and an end-to-end latency of 50 ms, provided through Edge Computing.
- **Massive Internet of Things (mIoT)** enabling very high traffic densities of devices and enhanced operational capabilities to support the wide range of IoT devices and services anticipated in the 5G timeframe.
- **Flexible network operations** aimed primarily at enabling independent support of diverse network requirements on the same physical network (network slicing).

Table 7, obtained from 3GPP-TS22.261 [74], outlines the 5G performance requirements for different scenarios. Note that all the values in this table are targeted values and not strict requirements.

Table 7: Target 5G performance requirements [74]

Scenario	Experienced data rate (DL)	Experienced data rate (UL)	Area traffic capability (DL)	Area traffic capacity (UL)	Overall user density	Activity factor	UE speed	Coverage
Urban macro	50 Mbps	25 Mbps	100 Gbps/km^2 (Note 4)	50 Gbps/km^2 (Note 4)	10000 per km^2	20 %	Pedestrians and users in vehicles (up to 120 km/h)	Full network (Note 1)
Rural macro	50 Mbps	25 Mbps	1 Gbps/km^2 (Note 4)	0,5 Gbps/km^2 (Note 4)	100 per km^2	20 %	Pedestrians and users in vehicles (up to 120 km/h)	Full network (Note 1)
Indoor hotspot	1 Gbps	500 Mbps	15 Tbps/km^2	2 Tbps/km^2	250000 per km^2	Note 2	Pedestrians	Office and residential (Note 2, 3)
Broadband access in a crowd	25 Mbps	50 Mbps	[3,75] Tbps/km^2	[7,5] Tbps/km^2	[500000] per km^2	30 %	Pedestrians	Confined area
Dense urban	300 Mbps	50 Mbps	750 Gbps/km^2 (Note 4)	125 Gbps/km^2 (Note 4)	25000 per km^2	10 %	Pedestrians and users in vehicles (up to 60 km/h)	Downtown (Note 1)
Broadcast like services	Maximum 200 Mbps (per TV channel)	N/A or modest (e.g. 500 kbps per user)	N/A	N/A	[15] TV channels of [20 Mbps] on one carrier	N/A	Stationary users, pedestrians and users in vehicles (up to 500 km/h)	Full network (Note 1)
High speed train	50 Mbps	25 Mbps	15 Gbps/Train	7,5 Gbps/Train	1000 per Train	30 %	Users in trains (up to 500 km/h)	Along railways (Note 1)
High speed vehicle	500 Mbps	25 Mbps	[100] Gbps/km^2	[50] Gbps/km^2	4000 per km^2	50 %	Users in vehicles (up to 250 km/h)	Along roads

Airplane connectivity	15 Mbps	7,5 Mbps	1,2 Gbps/Plane	0,6 Gbps/Plane	400 per Plane	20 %	Users in airplanes (up to 1 000 km/h)	(Note 1)
NOTE 1: For users in vehicles, the UE can be connected to the network directly, or via an on-board moving base station. NOTE 2: A certain traffic mix is assumed; only some users use services that require the highest data rates [75]. NOTE 3: For interactive audio and video services, for example, virtual meetings, the required two-way end-to-end latency (UL and DL) is 2-4 ms while the corresponding experienced data rate needs to be up to 8K 3D video [300 Mbps] in uplink and downlink. NOTE 4: These values are derived based on overall user density. Detailed information can be found in [76].								

Unlicensed technologies like Wi-Fi, ZigBee, 6LoWPAN, LoRa are used for IoT applications while dedicated short-range communication (DSRC) in US and ITS-G5 in the European Cooperative Intelligent Transport Systems (C-ITS) initiative are used for dedicated autonomous vehicle and driver assisting functions. ITS G5 is a short-range communication technology used for V2V and V2I communication. The applications are not restricted to autonomous vehicle functions, but also driver assisting functions (SAE level 1 and 2).

ITS-G5 is designed to allow vehicles in the intelligent transportation system (ITS) to communicate with other vehicles or infrastructure technologies. ITS-G5 technology operates on the 5.9 GHz band of the radio frequency spectrum and is effective over short to medium distances. ITS-G5 has low latency and high reliability, is secure, and supports interoperability. It receives very little interference, even in extreme weather conditions, because of the short range that it spans. ITS-G5 and C-V2X are rooted from different technologies, leading to fundamentally different operational methods. ITS-G5, derived from Wi-Fi, is optimized for cost and simplicity, and inherently supports distributed operation. C-V2X, derived from Long-Term Evolution (LTE) standard for high-speed wireless communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies, added new mechanisms to enable distributed operation. The initial V2X standard is based on a Wi-Fi, IEEE 802.11p (part of the IEEE's WAVE, or Wireless Access for Vehicular Environments program), running in the unlicensed 5.9GHz frequency band. V2X communication via 802.11p extend the line-of-sight-limited sensors such as cameras, radar and LIDAR, and covers V2V and V2I use cases such as collision warnings, speed limit alerts, and electronic parking and toll payments. The functional characteristics of 802.11p include short range (under 1km), low latency (~2ms) and high reliability, works in high vehicle speed mobility conditions and delivers performance immune to extreme weather conditions (e.g. rain, fog, snow etc.)". IEEE 802.11p is independent on the presence of cellular network coverage, and solutions onboard units (OBUs) and road-side units (RSUs).

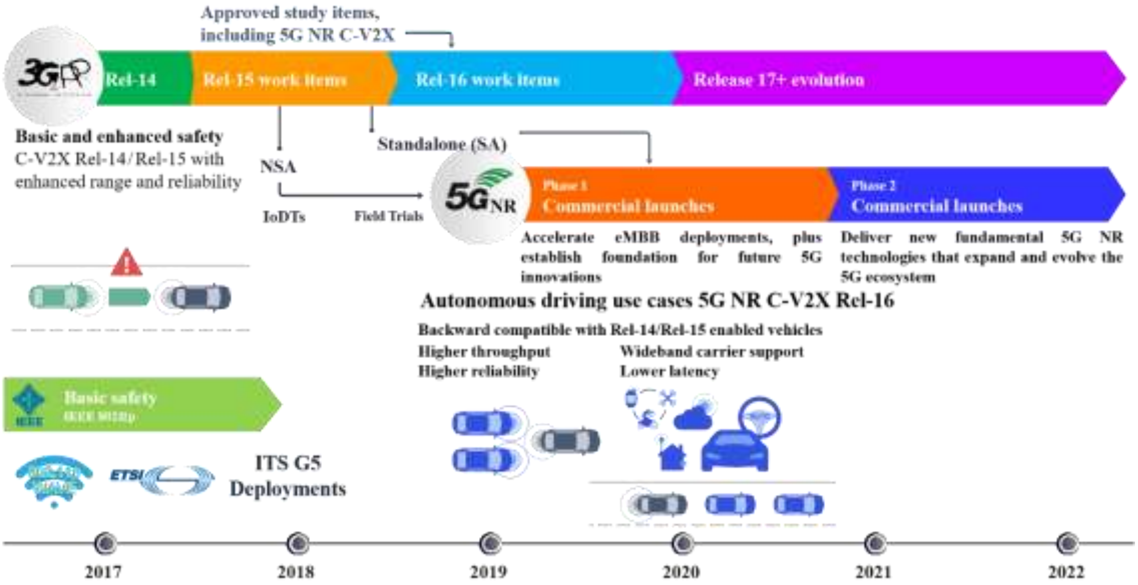

Approved study items, including 5G NR C-V2X
3GPP
Rel-14
Rel-15 work items
Rel-16 work items
Release 17+ evolution
Basic and enhanced safety
C-V2X Rel-14/Rel-15 with enhanced range and reliability
NSA
Standalone (SA)
IoDTs
Field Trials
5G NR
Phase 1
Commercial launches
Phase 2
Commercial launches
Accelerate eMBB deployments, plus establish foundation for future 5G innovations
Deliver new fundamental 5G NR technologies that expand and evolve the 5G ecosystem
Autonomous driving use cases 5G NR C-V2X Rel-16
Backward compatible with Rel-14/Rel-15 enabled vehicles
Higher throughput
Higher reliability
Wideband carrier support
Lower latency
IEEE
Basic safety
IEEE 802.11p
ETSI
ITS G5
Deployments
2017
2018
2019
2020
2021
2022

Figure 13: Roadmap for development and deployment of V2X and C-V2X technologies

The cellular V2X technology to be fully implemented in 5G NR has two operational modes which, between them, cover most eventualities. One has low-latency C-V2X direct communications over the PC5 interface on the unlicensed 5.9GHz band and is designed for active safety messages such as immediate road hazard warnings and other short-range V2V, V2I, and V2P situations. This mode aligns closely with what's offered by the incumbent IEEE 802.11p technology, which also uses the 5.9GHz band. The other mode has communications over the air interface (Uu) on the regular licensed-band cellular network and can handle V2N use cases like infotainment and latency-tolerant safety messages concerning longer-range road hazards or traffic conditions. IEEE 802.11p can only match this mode by making ad hoc connections to roadside base stations, since the protocol does not make of use cellular connectivity. IEEE 802.11p and C-V2X could be integrated both in the autonomous vehicle combining the strongest points of each technology. Next generation technologies (e.g. high-frequency (e.g. 60GHz), high-bandwidth mmWave, VVLC (Vehicular Visible Light Communication), etc.) could be incorporated in the 5G V2X access network architecture to support specific V2X use cases to maximise the benefits for the vehicle users. For IEEE802.11p a group in IEEE started studying how to enhance the technology with NGV (new generation V2X). LTE-V2X will be further improved in 3GPP towards release 15 and then 16. New Radio V2X (NR-V2X) is synonym to 5G-V2X and starts development in 3GPP with release 16. Cellular V2X (C-V2X) groups the LTE-V2X family and NR-V2X together [117]. The roadmap for development and deployment of V2X and C-V2X technologies is presented in Figure 13.

The direct communication in autonomous vehicles and IoT applications is a specific matter of trust, and for several IoT applications 3rd party service providers such as network operators, could be involved in establishing a communication (see [66]). For the autonomous vehicles specific operations if one vehicle is not able to trust the information transmitted via V2X communication, e.g. a hazard warning as Decentralised Environmental Notification Messages (DENM), it might not make use of this information.

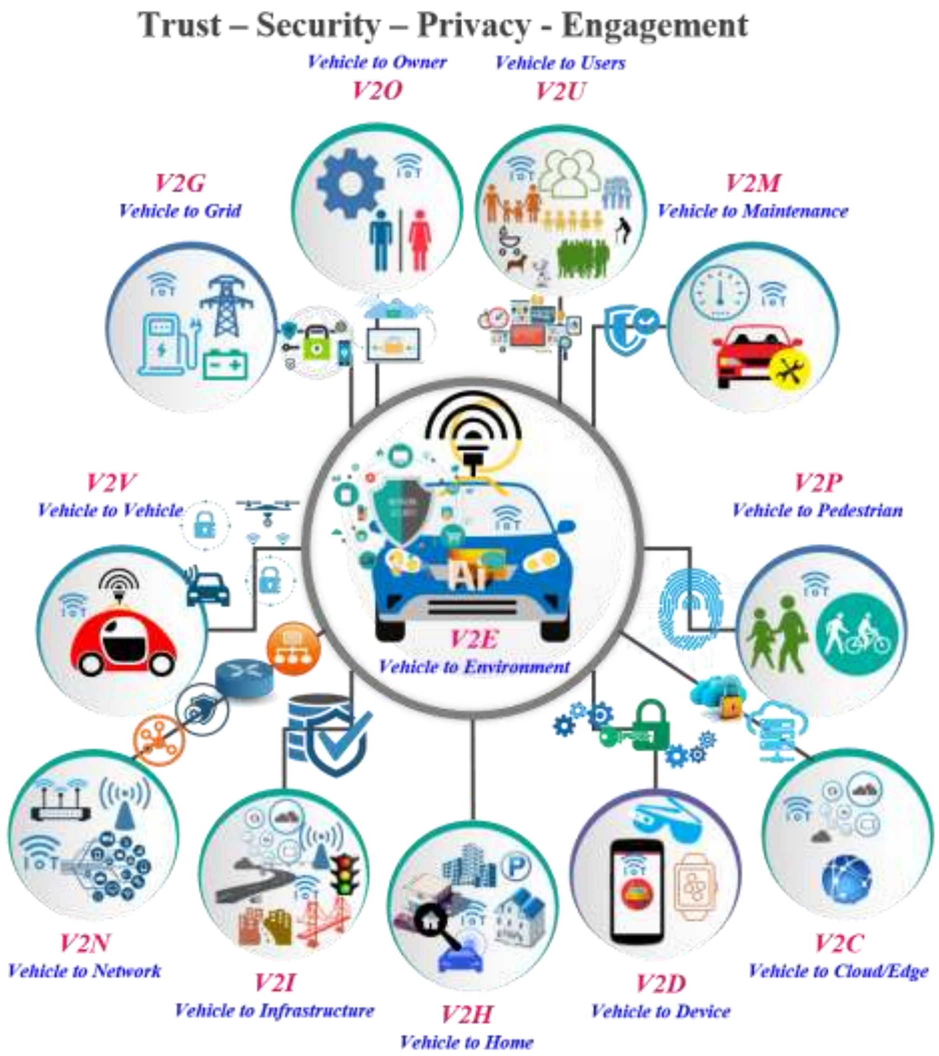


Figure 14: AVs and IoT policy framework covering all the domains of interaction

Security systems for direct communication are supported by C-V2X as security and data privacy rules can be deployed for the C-V2X direct communication in the same way as they are specified for ITS G5 and can benefit from the V2N capabilities for the operational purposes, such as distribution and renewal of certificates and certificate revocation lists. This covers different types of C-V2X user equipment (vehicles, pedestrian, road side infrastructure) involved, different network providers involved, including that no network coverage exists, and security management system components which establishes a level of trust between the various entities.

Table 8: Comparison of V2X communications features [110][111][112][113][114]

Feature	IEEE 802.11p	IEEE 802.11px	IEEE 802.11ad (mmWave)	C-V2X
Frequency Band	5.85 GHz-5.925 GHz	5.85 GHz-5.925 GHz	57.05 GHz -64 GHz	450 MHz-4.99 GHz 5.725 GHz-5.765 GHz
Channel Bandwidth	10 MHz	10 MHz	2.16 GHz	Up to 640 MHz
Range	≤ 1 km	≤ 1 km	≤ 50 m	≤ 30 km
Bit Rate	3 Mbps-27 Mbps	Up to 60 Mbps	Up to 7 Gbps	Up to 3 Gbps
End-to-End Latency	≤ 10 ms	≤ 10 ms	≤ 10 ms	30 ms-50 ms (UL/DL) 20 ms-80 ms (V2V)

Link Establishment Latency	~0 ms	~0 ms	10 ms-20 ms	40 ms-110 ms
Coverage	Intermittent	Intermittent	Intermittent	Ubiquitous
Mobility Support	≤ 130 km/h	Under Investigation	≤ 100 km/h	≤ 350 km/h
QoS Support	Yes	Yes	Yes	Yes
Broadcast Support	Yes	Yes	No	Yes
V2I Support	Yes	Yes	Yes	Yes
V2V Support	Yes	Yes	Yes	Over PC5 Interface
Relay Mode	Yes	Yes	Yes	Yes
MIMO	No	Yes	Yes	Yes

Table 9: Comparison of IEEE 802.11p and C-V2X, Source Autotalks Ltd. [57]

Topic	IEEE 802.11p	C-V2X (rel. 14/15)	C-V2X (rel. 16)
Goal	Direct real-time safety communication between vehicles to road users and vehicles to infrastructure.		
Specification completed	Completed	Rel-14 completed in 2016. Rel-15 completed in 2018.	Rel-16 to be completed in 2019.
Deployment	Since 2017, mass market in 2019.	Ready for commercialization in 2019.	
Use cases	Safety	Safety and enhanced safety use cases	Advanced use cases to assist in autonomous driving (ranging assisted positioning, high throughput sensor sharing and local 3D HD map updates)
Cellular connectivity	Hybrid model. Can be used with any cellular network (4G/5G) for non-safety services.		
Communication technology	OFDM with CSMA. Offers robust communication in dense and dynamic environment. No dependency in GPS signal.	SC-FDM with semi-persistent sensing. Optimized for long communication range.	
Security	Public key cryptography and infrastructure. Lack of V2X isolation from non-safety domain would create a cybersecurity risk.		
Coexistence in 5.9GHz (see [122])	Adjacent channel with 3GPP technology	Adjacent channel with 802.11p technology; co-channel coexistence from R14 onwards	Adjacent channel with 802.11p technology; co-channel coexistence from R14 onwards and Wi-Fi
SIM-less operation	Yes.	Yes.	Yes.
Security and privacy on V2V/V2I/V2P	As per IEEE WAVE and ETSI-ITS security services	As per IEEE WAVE and ETSI-ITS security services	As per IEEE WAVE and ETSI-ITS security services
Infrastructure investment	Dedicated camera and traffic light-based infrastructure can enhance safety.		
Roadmap	802.11NGV targets interoperability with 802.11p.		C-V2X rel. 16 based on NR (5G). Operates in a different channel than rel. 14/15.

Origin	Wi-Fi	LTE uplink	
Modulation	OFDM	SC-FDM	
Transmission time	Varying according to packet length, typically 0.4mS. Capable of copying occasional long packets.	1mS. Increasing energy per bit for long communication range.	
Concurrent transmission	No	Yes. Decreasing range due to "half-duplex" and "near-far" problems.	
Transmission range @90% error, 280 km/hr relative speed	Up to 225m.	Over 450m using direct mode and very large range via cellular infrastructure.	Over 450m using direct mode and very large range via cellular infrastructure.
Typical transmission frequency for periodic traffic	One every 100ms (50 ms is possible).	One every 100ms (50 ms is possible).	Supports packet periodicities of a few ms.
Symbol duration	8µs. Fast channel tracking.	71µs.	
Line coding	Convolution code.	Turbo code. High processing gain for long communication range.	
Transmission scheduling	CSMA: Transmit when no ongoing reception. No pre-determined transmission slots fitting facilities layer per-cycle decision whether to transmit.	Semi-persistent sensing of least occupied resource. Collision are not sensed. Slow response to changing environment.	
Retransmission	None.	Yes. Typically activated in high-speed. Overcoming network collisions and increasing communication range.	
Time synchronization	Loose asynchronous.	Very tight synchronous requirements.	
Range/Reliability	LOS: NLOS:	LOS: NLOS:	

A different comparative evaluation of the communication infrastructure technologies is presented in [115].

Table 10: Comparison of communication infrastructure technologies [115]

	VEHICLE-BASED SENSORS	**802.11P**	**C-V2X (rel. 14/15)**	**C-V2X (rel. 16)**
Range	10s of meters	100s of meters	Cellular + sidelink	Cellular + 5 hops
Frequency Band	N/A	5.9 GHz	700, 1800, 2600	Tbc
Bandwidth	N/A	30 MHz (in the EU)	20 MHz	< 100 MHz
Coverage	N/A	Medium	High	Very high
Robustness Doppler/Delay	N/A	High due to large carrier spacing	Medium. Doppler effects need to be compensated at the receiver. This leads to inefficiency	High. New waveform supporting highly dispersive channels in time and frequency
Interference	N/A	Limited to low interference levels	Sidelink causes UL interference	Cellular and *ad hoc* in parallel
Maturity	Available	SAE J2735: BSM IEEE 1609.X IEEE 802.11p	2019	Starting 2020 General adoption 2025

Protocol Type	N/A	CAM DENM	ProSec, Day1&2	Day 1,2,3
SERVICES				
Self-parking	Yes	N/A	N/A	N/A
Emergency Braking	Yes	Yes	Yes	Yes
Lane Merging	No	No	No	Yes
Assisted Driving	Limited	Same	Same	Yes
Autonomous Driving	Limited	Limited 100 ms 90% reception	Limited 100 ms 90% reception	1 ms 99.999% hard real-time

Note: Ad hoc communication is a term used within the IEEE community for networks that are established and released. In this context, it refers to, say, a group of vehicles (not necessarily all travelling in the same direction) forming a group for a limited time, to communicate between themselves. The idea is different from broadcasting, as used in IEEE 802.11p, where there is no acknowledgement of messages.

3.1.2 IoT communication technologies

IoT communication technologies covers a wide range of data rates, protocol and frequency spectrum. The integration of autonomous vehicles, IoT and AI must consider the IoT connectivity protocols and standards such as Wi-Fi, ZigBee, Z-wave, BL, BLE, NB-IoT, LoRa and SigFox, GSM, 2/3/4/5 G, etc. based on their technical features, optimizations and use cases. Based on these IoT connectivity protocols the IoT solutions connect to their closed service layers using different messaging protocols (CoAP, MQTT, HTTP, AQMP), data-models and proprietary APIs, providing service integration into IoT platforms. An overview of these IoT connectivity and messaging protocols is given in the following paragraphs.

Short-Range Wireless IoT:

- **Bluetooth and BLE** (Bluetooth Low-Energy) is a protocol for IoT applications. BLE (also called Bluetooth Smart) offers similar range as Bluetooth but has been designed to offer significantly reduced power consumption [131]. BLE is part of part of the Bluetooth v4.0 and the recent v4.2 stack and has an advantage in a more personal device context given its widespread integration in smartphones and many other mobile devices. BLE use the 2.4GHz ISM frequency band, the data rates are 1Mbs and range approximately 50-150 metres. The IEEE standardized Bluetooth as IEEE 802.15.1, but are no longer maintaining the standard [130]. The Bluetooth special Interest Group (SIG) oversees development of the specification, manages the qualification program, and protects the trademarks. BLE is not an open wireless technology standard and does not support open firmware and hardware.
- **RFID** (Radio frequency identification) refers to a system of storing and retrieving data wirelessly using tags, smart cards or RFID transponders [129]. It uses electromagnetic fields to identify tags attached to objects which should be brought into proximity of a reader with a typical coverage of a couple of centimetres. Tags can be passive (not battery powered/limited coverage) or active (battery powered/extended coverage). RFID is commonly embedded into IoT applications and deployments as an easy way to identify devices and interact with humans.
- **IEEE 802.15.4** is a technical standard which defines the operation of low-rate wireless personal area networks and specifies the physical layer and media access control [130]. It is the basis for the Zigbee, ISA100.11a, WirelessHART, 6LoWPAN, Thread and SNAP specifications, each of which further extends the standard by developing the upper layers which are not defined. 6LoWPAN defines a binding for the IPv6 over WPANs and is used by upper layers like Thread.
- **Zigbee** is based on the IEEE 802.15.4 specification for a suite of high-level communication protocols used to create personal area networks [130] and operates on the physical radio specification and in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz. Zigbee is a

low-power, low data rate, and proximity wireless ad hoc network. Zigbee PRO and Zigbee Remote Control (RF4CE) are among the profiles [131]. Zigbee RF4CE has some advantages in complex systems offering low-power operation, high security, robustness and high scalability with high node counts which could be an advantage of wireless control and sensor networks in M2M and IoT applications. The Zigbee 3.0 solution includes testing, certification, branding and marketing support to make it easier to develop and sell interoperable products and solutions. Zigbee 3.0 is built on the Zigbee PRO, which enhances the IEEE 802.15.4 standard by adding mesh network and security layers along with an application framework and to become a full stack, low-power certifiable, interoperable Zigbee solution. The Zigbee 3.0 device with routing capabilities (router or coordinator) has to implement Green Power Basic Proxy (GPBP) functionality for forward compatibility. GPBP enables routing devices to tunnel Green Power Device Frames (GPDF) from Green Power Source to Sink devices, making Green Power functionality possible on any Zigbee 3.0 network, regardless of a specific device's own application.

- **Z-Wave** is a low energy radio frequency technology for sub-GHz communications e.g. 900MHz with 9.6/40/100 kbit/s data rates, using a mesh networking protocol, adopted for home automation, security systems, and lighting controls. Z-Wave protocol allows faster and simpler development and supports full mesh networking without requiring a coordinator node and is highly scalable [136].
- **6LoWPAN** encapsulates IPv6 headers in IEEE 802.15.4 frames. The standard is independent of the underlying physical layer and frequency band and can be also employed over different communications platforms, including Ethernet, 802.15.4, Wi-Fi, and sub-1GHz ISM (Industrial, Scientific, and Medical) radio channels [137].
- **WirelessHART** is a wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol (HART) [130]. Developed as a multi-vendor, interoperable wireless standard and defined for the requirements of process field device networks.
- **ISA100.11a** - The International Society of Automation’s ISA100.11a industrial control standard is used in process control applications. It adds channel hopping, variable time-slot multiplex options, and mesh networking to the 802.15.4 base.
- **Thread** is an IPv6-based, low-power mesh networking technology for IoT products, intended to be secure and future-proof [130]. Thread uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication. Thread is IP-addressable, with cloud access and AES encryption.
- **802.11** - IEEE 802.11 known as Wi-Fi is deployed Wireless LAN (WLAN) technology that provides wireless connectivity to various devices. The IEEE 802.11ah amendment introduced the Sub-1 GHz bands that facilitate and support saving transmission power. It is suitable for IoT by supporting numerous devices on an individual Basic Service Set (BSS) and by providing energy conservation techniques which allow wireless stations to transit from sleep mode to save power. The Wi-Fi Alliance has defined version numbers as following Wi-Fi 1 - 802.11b, released in 1999, Wi-Fi 2 - 802.11a, released in 1999, Wi-Fi 3 - 802.11g, released in 2003, Wi-Fi 4 - 802.11n, released in 2009, Wi-Fi 5 - 802.11ah, released in 2014 and Wi-Fi 6 - 802.11ax, to be released in 2019. Wi-Fi 6 can divide a wireless channel into many subchannels. Each of these subchannels can carry data intended for a different device. This is achieved through Orthogonal Frequency Division Multiple Access, or OFDMA. The Wi-Fi access point can talk to more devices at once. The Wi-Fi 6 standard also has improved MIMO -Multiple In/Multiple Out. This involves multiple antennas, which let the access point talk to multiple devices at once. With Wi-Fi 5, the access point could talk to devices at the same time, but those devices couldn’t respond at the same time. Wi-Fi 6 has an improved version of multi-user or MU-MIMO that lets devices respond to the wireless access point at the same time. Wireless access points near each other may be transmitting on the same channel. In this

case, the radio listens and waits for a clear signal before replying. With Wi-Fi 6, wireless access points near each other can be configured to have different Basic Service Set (BSS) “colours.” This “colour” is a number between 0 and 7. If a device is checking whether the channel is all clear and listens in, it may notice a transmission with a weak signal and a different “colour.” It can then ignore this signal and transmit anyway without waiting, so this will improve performance in congested areas, and is also called “spatial frequency re-use” [132].

LPWAN:

- **LoRaWAN** (Long-range Wide Area Network) is a wireless technology for long-range radio, low power, and low data rate IoT applications are based on spread spectrum chipsets from Semtech Corporation but promoted by the non-profit association LoRa Alliance [129]. Typical characteristics are distances of up to 20 km, battery- powered end-nodes of up to 10 years’ lifetime, and data rates ranging from 0.3 kbps to 50 kbps in the 869 and 900 MHz ISM bands. Switching between LoRa chirp spread spectrum (CSS) and frequency-shift keying (FSK) modulation are facilitated. The network server hosts the system intelligence and complexity (e.g., duplicate packets elimination, acknowledgement scheduling, data rate adapting). All connections are bidirectional, support multicast operation, and forms a star of stars topology. To serve different applications, the end-nodes are classified in three different classes, which trade off communication latency versus power consumption. Class A is the most energy efficient and is implemented in all end-nodes. Classes B and C are optional and must be class- A- compatible. A spreading factor (SF) is used to increase the network capacity. A higher SF gives longer communication range, but also implies decreased data rate and increased energy consumption. For frequent data sampling, LoRa systems use an SF as small as possible to limit the airtime, which requires end-nodes located closer to the gateways. LORAWAN standard uses symmetric-key cryptography to authenticate end devices with the network and preserve the privacy of application data.
- **SigFox** is a wide-range wireless technology (range between Wi-Fi and Cellular)[131]. It uses the ISM frequency bands to transmit data over a narrow spectrum to and from connected objects. Typically used for M2M applications that run on small batteries and only require low levels of data transfer. SigFox uses a technology called Ultra Narrow Band (UNB) and is only designed to handle low data-transfer speeds of 10 to 1000 bps, consumes only 50µW, and can deliver a typical stand-by time of 20 years with a 2.5Ah.
- **Weightless** is a UNB standard with several alternative schemes. Weightless-N is supporting one-direction communications from end devices to a base station, achieving notable power conservation and reduced cost. Weightless-N is an unlicensed spectrum narrowband protocol like SigFox, but it exhibits different MAC layer implementation. Weightless-N is an open standard that operates in sub-1GHz unlicensed spectrum. Weightless-W is intended to operate in TV White Space (TVWS) bands as an open standard. It can function under several modulation schemes, including Differential-BPSK (DBPSK) and 16-Quadrature Amplitude Modulation (16-QAM). The packets larger than 10 bytes can be transferred at rates between 1 kbps and 10Mbps. Weightless-P provides mixed two-direction connectivity with two non-proprietary physical layers. It performs signal modulation utilizing Quadrature Phase Shift Keying (QPSK) and Gaussian Minimum Shift Keying (GMSK) and operates in sub-GHz ISM bands and each single 12.5 kHz narrow channel provides capacity between 0.2 kbps to 100 kbps [138].

Cellular IoT:

3GPP is expanding its existing cellular standards to reduce complexity and cost, improve the range and signal penetration, and prolong the battery lifetime to address IoT applications across various industrial sectors including automotive.

- **GSM and EC-GSM** –Global System for Mobile Communications (GSM) is announced to be decommissioned in certain areas on the globe, and Mobile Network Operators (MNOs) try to extend their operation in certain markets by the extended coverage GSM (EC-GSM) standard that aims to extend the GSM coverage by +20dB using SUB-GHZ band for better signal penetration in indoor environments. A link budget in the range of 154 dB-164 dB is aimed depending on the transmission power. The implementation requires a software upgrade of GSM networks allowing the legacy GPRS spectrum to pack the new logical channels defined to accommodate EC-GSM devices. Two modulation techniques namely Gaussian Minimum Shift Keying (GMSK) and 8-ary Phase Shift Keying (8PSK) provide variable data rates with the peak rate of 240 kbps with the latter technique. The standard aims to support 50k devices per base station and enhanced security and privacy features compared to conventional GSM based solutions.

- **LTE** - Long Term Evolution (LTE) has a number of technical elements that make LTE and LTE-A superior to 3G technologies such as the efficient adoption of Orthogonal Frequency Division Multiple Access (OFDMA) in combination with smart antennas supporting Multiple-Input Multiple-Output (MIMO) in the uplink and downlink directions.
- **LTE Cat-4, Cat-1, Cat-0, and Cat-M1** - Conventional LTE end devices offer high data rate services at a cost and power consumption not acceptable for several Machine Type Communications (MTC) use cases. To reduce the cost while being compliant to LTE system requirements, 3GPP reduces the peak data rate from LTE Category 1 to LTE Category 0 and then to LTE Category M, the different stages in the LTE evolution process. Cost reduction is achieved by supporting optional half-duplex operation in Category 0. This choice reduces the complexity of modem and antenna design. From Category 0 to Category M1 (e.g. eMTC), a drop in the receive bandwidth from 20 MHz to 1.4 MHz in combination with a reduced transmission power results in more cost-efficient and low-power design.
- **NB-IoT** (Narrow Band IoT) is a low power wireless area network (LPWAN) radio technology standard developed by 3GPP to enable the connection of low-power IoT devices to the Cellular network telecommunication bands [129]. NB-IoT specification was frozen at Release 13 of 3GPP specification (LTE-Advanced Pro) in June 2016. It focuses on indoor coverage enabling long-life battery-powered device applications while increasing the number of connected devices. NB-IoT is not compatible with 3G but can coexist with GSM, GPRS and LTE. NB-IoT can be supported with only a software upgrade on top of existing LTE infrastructure. It can be deployed inside a single GSM carrier of 200 kHz, inside a single LTE physical resource block (PRB) of 180 kHz or inside an LTE guard band. Compared to eMTC, NB-IoT cuts the cost and energy consumption further by reducing the data rate and bandwidth requirements (needs only 180 kHz) and simplifying the protocol design and mobility support. NB-IoT aims for a 164 dB coverage, serving up to 50k end devices per cell with the potential for scaling up the capacity by adding more NB-IoT carriers. NB-IoT uses single-carrier Frequency Division Multiple Access (FDMA) in uplink and Orthogonal FDMA (OFDMA) in downlink. The data rate is limited to 250 kbps for the multi-tone downlink communication and to 20 kbps for the single-tone uplink communication [139][140].
- **5G** is the technology designation of the next generation mobile network also feasible for IoT applications (5G IoT). Standardization work through ITU-R / IMT-2020 is expected to be completed by 2020 [129]. However, it will take several years before "all" expectations are met and widely available (e.g. implementation of frequencies up to 30 GHz). There are high expectations and requirements with respect to speeds, latency and energy efficiency. A very large increase in capacity and much faster internet on mobile phones is expected. The frequency bands are not finally established; however, the EU advisory body Radio Spectrum policy Group proposes three pioneer frequency bands for fifth generation mobile services: 694-790 MHz, 3.4-3.8 GHz, and 24.25-27.5 GHz.

Satellite IoT:

Satellite-enabled IoT is dominated by narrowband providers, such as L-band. The developments of high-throughput Ku-band and Ka-band satellite connections, allow for new capabilities in orbit to create broadband connectivity for IoT applications and autonomous systems. The global network of satellite systems and the ability to broadcast to multiple points is an efficient signal delivery on earth. Satellite broadcasts can work seamlessly with terrestrial cell carriers to achieve global coverage and enable auto manufacturers to reach all of their vehicles on a single network. This is important for covering the remote areas and assure the connectivity requirements on IoT and autonomous vehicles applications. Satellite communications will play an important role in the connectivity and autonomy of intelligent cars. Autonomous vehicles need different types of external connectivity and the steering/braking functions of the vehicle need information about different vehicles on the roads using terrestrial networks with very low latency due to time-critical nature of actions. There are several vehicle functions that need information about conditions ahead, local imaging of city streets and mapping of selected routes that can rely on satellites for communications due to ubiquity and broadcast for satellite technology. These elements can be integrated with IoT applications and integrated into autonomous mobility applications. The advantages of satellite connectivity for IoT and autonomous vehicles are presented below [133]:

- Wide area coverage including those difficult to access with terrestrial technologies due to economical and accessibility conditions (e.g. rural, mountain, remote valleys, etc.
- Global availability on land, ocean, air, etc.
- Support for high mobility
- Reliable message delivery with one transmission (< 0.1% PLR, e.g. important for mission critical applications
- Broadcast and multicast capabilities (e.g. software updates, supervisory control)
- Immune towards natural and man-made disasters
- High capacity using relatively low bandwidth resources
- Lowest cost IoT communication proposition for massive IoT deployments.
- Secure and high-availability data services for professional users (trust and data privacy).
- Dedicated network with cognitive machine intelligence capabilities (LTE inspired).
- Reliability as key requirement for effective IoT deployments.
- Low latency for L-band services appropriate for applications such as remote asset monitoring that requires reliable, always-on connectivity.
- Optimised speed for IoT applications requiring data rates to support bandwidth-intensive applications in real-time.

Satellite IoT and autonomous vehicles services are planned by different satellite stakeholders. INMARSAT offers L-band M2M solutions (fixed satellite with 100kbps data rate transmission) for messaging and using satellites to connect LoRA aggregators. Globalstar offers simplex and duplex solutions. Iridium plans to launch Certus100 (88 Kbps for small, portable devices optimized for email, weather files, photo transfer, and internet credit card processing) and Certus20 (22 Kbps for small, battery-powered, highly mobile devices optimized for asset tracking, remote monitoring, aircraft telemetry and communications, and maritime distress and safety applications) for addressing IoT applications. Terrestar and EML satellites are designed to support handheld terminals with very large reflector antennas for applications covering vehicle and asset tracking, flight safety and entertainment, environmental monitoring, public protection and disaster response (PPDR) etc. that can be used to enhance the autonomous driving capabilities in different autonomous mobility applications. 5G wireless technology may be applied to Non-Terrestrial Networks (NTN) including both satellite and high altitudes platforms (HAPS) and the Non-orthogonal Multiple Access (NOMA) standardization is evaluated as part of the New Radio (NR) for 5G [135]. Satellite is providing connectivity solutions for the automotive community that not only complement existing terrestrial options but when combined offers a more reliable, cost-efficient communications [134].

IoT messaging protocols

Hypertext Transfer Protocol/Secure (HTTP/S) and WebSockets are common standards, together with the eXtensible Markup Language (XML) or JavaScript Object Notation (JSON). By using a standard web browser (HTTP client), JSON provides an abstraction layer for Web developers to create a stateful Web application with a persistent duplex connection to a Web server (HTTP server) by holding two HTTP connections open.

- **HTTP** - HTTP is the foundation of the client-server model used for the Web. The safest method with which to implement HTTP in your IoT device is to include only a client, not a server. In other words, it is safer when the IoT device can initiate connections to a web server but is not able to receive connection requests; we don't want to allow outside machines access to the local network where IoT devices are installed.
- **WebSocket** - WebSocket is a protocol that provides full-duplex communication over a single TCP connection through which messages can be sent between client and server. It is part of the Hypertext Markup Language 5 (HTML5) specification. The WebSocket standard simplifies much of the complexity around bi-directional Web communications and connection management.
- **XMPP** - Extensible messaging and presence protocol (XMPP) is a good example of an existing Web technology finding new use in the IoT space. XMPP has its roots in instant messaging and presence information, and has expanded into voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data. It is a contender for mass scale management of consumer white goods such as washers, dryers, refrigerators, and so on. XMPP's strengths are its addressing, security, and scalability. This makes it ideal for consumer-oriented IoT applications.
- **CoAP** - CoAP, as HTTP, is a RESTful (the ability to manipulate resources and resource identifiers via a uniform application programming interface (API)) protocol. CoAP is semantically aligned with HTTP, and even has one-to-one mapping to and from HTTP. CoAP is a good protocol for devices operating on a battery or energy harvesting. CoAP uses UDP and some of the TCP functionalities are replicated directly in CoAP. Requests and responses are exchanged asynchronously over CoAP messages (unlike HTTP, where an existing TCP connection is used). The headers, methods, and status codes are binary encoded, which reduces protocol overhead. However, this requires the use of a protocol analyser to troubleshoot network issues. CoAP fully addresses the need for a light protocol exhibiting a behaviour similar to a permanent connection. It has semantic familiarity with HTTP and is RESTful. If you have a web background, using CoAP is relatively easy.
- **MQTT** - Message Queue Telemetry Transport (MQTT) is an open source protocol that was developed and optimized for constrained devices and low-bandwidth, high-latency, or unreliable networks. It is a publish/subscribe messaging transport that is extremely lightweight and ideal for connecting small devices to networks with minimal bandwidth. MQTT is bandwidth efficient, data agnostic, and has continuous session awareness, as it uses TCP. It is intended to minimize device resource requirements while also attempting to ensure reliability and some degree of assurance of delivery with grades of service. MQTT targets large networks of small devices that need to be monitored or controlled from a backend server on the Internet. It is not designed for device-to-device transfer, nor is it designed to "multicast" data to many receivers. MQTT is simple, offering few control options. Applications using MQTT are generally slow in the sense that the definition of "real time" in this case is measured in seconds.

An overview of the interactions of technologies for providing Internet of Vehicles autonomous mobility applications is illustrated in Figure 15.

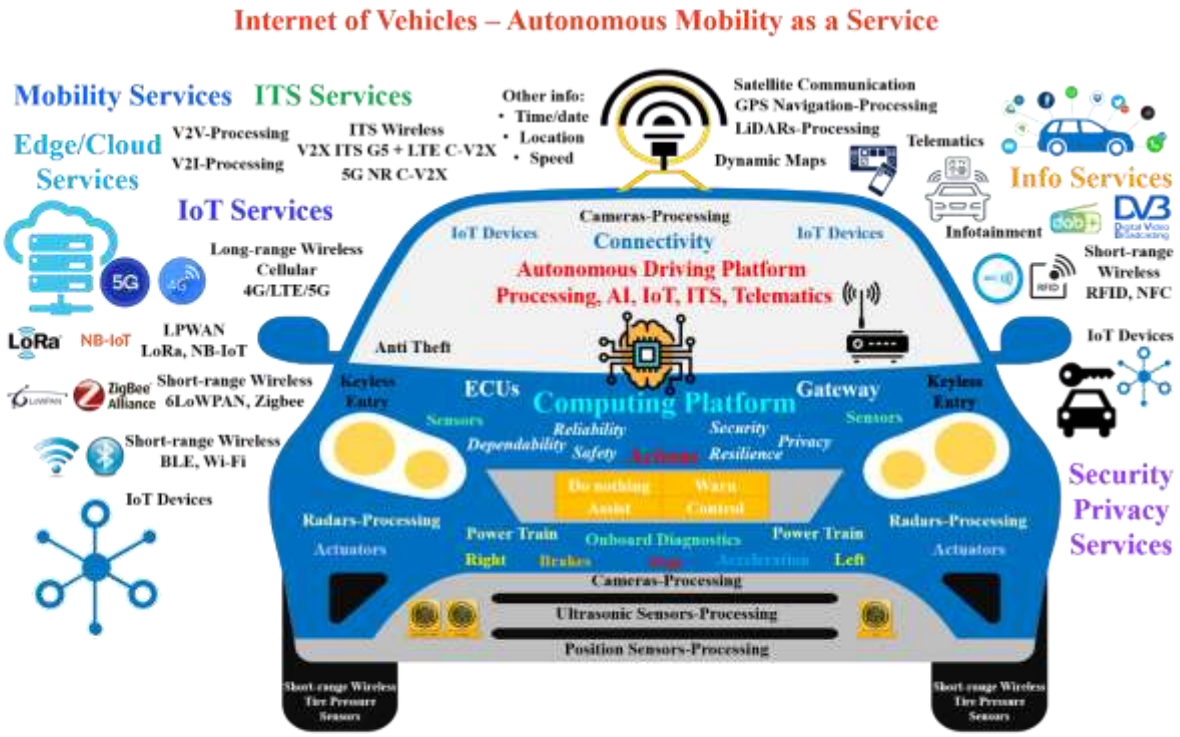


Figure 15:Integration of technologies in Internet of Vehicles Autonomous Mobility Applications

3.2 Artificial intelligence in trust, security, privacy and engagement

Artificial intelligence (AI) is a promising technological innovation, raising already high expectations for 2025 [64]. The IoT is the source of data for AI and machine learning applications, as fleets of connected autonomous vehicles (or IoT devices) need to be automated to allow them to react to environmental conditions in real-time. By 2021, AI will support more than 80% of emerging technologies, while, in the following year, it will support more than 80% of enterprise IoT projects, according to Gartner.

The IoT are evolving towards the next generation of Tactile IoT, which will bring AI together with hyperconnectivity, edge computing, and Distributed Ledger Technologies (DLTs) [64]. Future IoT applications will apply AI methods, such as machine learning (ML) and neural networks (NNs), to optimize the processing of information, as well as integrating autonomous vehicles, augmented and virtual reality (AR/VR), and digital assistants. These applications will engender new products, services and experiences that will gain new autonomous vehicles possibilities. A more human-centred perspective will also allow us to maximise the effects of the next generation of IoT technologies and applications as we move towards the integration of intelligent objects with social capabilities that need to address the interactions between autonomous systems and humans in a seamless way.

The development of autonomous vehicles and IoT applications will accelerate the combination of emergent technologies for information processing and distributed security, e.g. artificial intelligence (AI), distributed ledger technologies (DLTs) [121], blockchains, edge computing, and 5G connectivity. These bring new challenges in addressing distributed IoT architectures and distributed security, privacy and trust mechanisms that form the foundation of a dynamic autonomous vehicles and IoT policy framework.

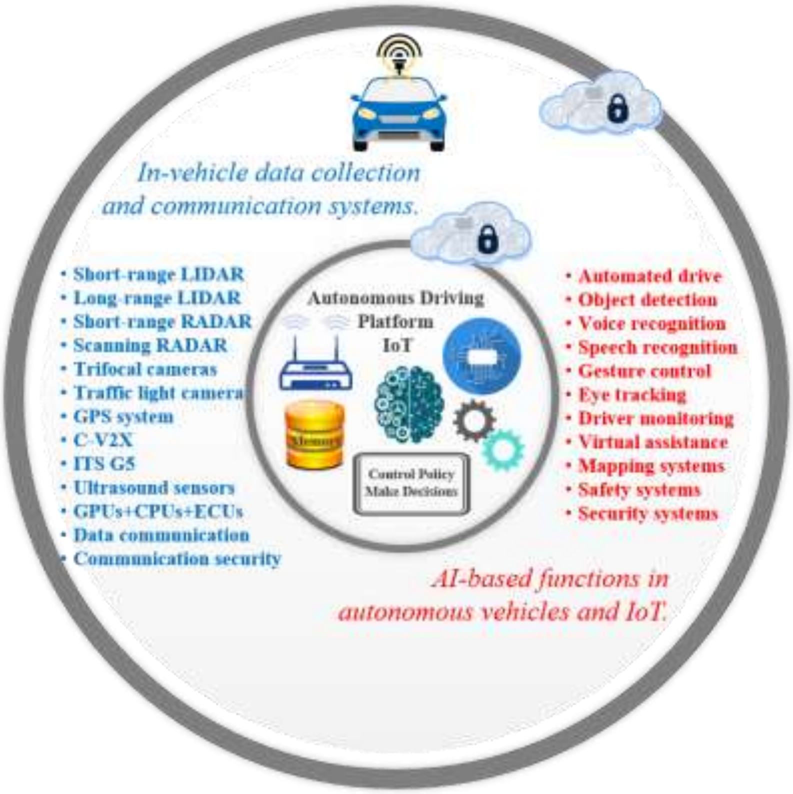


Figure 16: IoT policy framework - Extending in-vehicle and AI-based functions in AVs and IoT applications

AI is driving the development of autonomous vehicles' level 4 and level 5 further. The AI functions implemented in the vehicles, in the infrastructure, and as part of the services of will influence and need to be considered when defining the autonomous vehicles and IoT policy framework. Examples of AI-based functions and in-vehicle data collections and communication systems for autonomous vehicles and IoT systems are presented in Figure 16. AI-based systems are first adapted in infotainment human-machine interface, including speech recognition, gesture recognition (including hand-writing recognition), eye tracking and driver monitoring, virtual assistance and natural language interfaces and in advanced driver assistance systems (ADAS), including camera-based machine vision systems, radar-based detection units, driver condition evaluation, and sensor fusion engine control units (ECU).

Deep learning can be used for detection and recognition of multiple objects, and improves perception, reduces power consumption, supports object classification, enables recognition and prediction of actions, and reduces the development time of ADAS systems.

The autonomous vehicles and IoT policy framework need to capture the end-to-end, dynamic, on-demand and real-time connectivity including intelligent automation at scale based on AI techniques and methods.

3.2.1 Requirements for complex autonomous and IoT systems that have embedded AI techniques and methods

The applications across industrial sectors integrating AI and IoT need to address a multitude of requirements in order to fulfil the integration of functional and non-functional attributes for such complex systems. The autonomous vehicles and IoT functions and operational modules will be based on embedded AI techniques and methods. The requirements for complex autonomous vehicles and IoT/IIoT (industrial IoT) systems that have embedded AI techniques and methods can be summarized as presented in the following list [64]:

Explainability: Enables human users to understand the decisions made by AI systems and the rationale behind them. This ability will make it easier to track down eventual failures and assess decisions' strengths and weaknesses. Ultimately, this will increase the trust in the systems' decisions. This ability will have to integrate with human-computer interface techniques which are able to track complex reasoning processes.

Availability: Enables IoT applications to provide data and resources in a timely manner for a set percentage of time (i.e., the uptime) as well as retain their core functionality, even if the system has undergone a security attack. Industrial IoT applications may target mission-critical tasks along the production line; system outages will therefore have direct economic impact. It is envisaged that IoT systems, due to embedded AI, will be able to perform autonomously via online learning over their lifetime and remove even the downtime needed for maintenance. AI systems should be available in terms of integration into new applications and process steps.

Trustworthiness: Enables IoT systems to be trusted, only allowing authenticated devices or services that can be uniquely identified to participate in the decision-making processes of the system. This makes it possible to report the source of vulnerabilities and inconsistencies. As more and more AI-enabled systems become connected through the IoT, trustworthiness becomes an indispensable requirement. Precisely due to the AI, trustworthiness will become multi-dimensional, far beyond verifying identity. Consequently, trust will no longer be 'true' or 'false', but rather about degrees of trustworthiness that will control the access levels of devices/users to critical services.

Security: Enables systems to guarantee distributed end-to-end security, which is essential to ensure robustness against all types of attack vectors in the IoT. This includes securing the AI system itself as well as securing communication between edge computing IoT devices with encryption and authentication mechanisms against attacks with manipulated input data.

Safety: Enables systems to protect persons and objects during operation. AI systems that operate physically next to and collaboratively with humans through robots or other machines must not exhibit random or unpredictable behaviour. Safety by design is essential, entailing compliance with relevant safety standards. Importantly, the employed AI and IoT systems must be robust against implausible data and operate with extremely low latency to quickly and appropriately react to unforeseen events (i.e., to prevent accidents).

Privacy: Enables IoT and AI-based systems that operate on mission- and business-critical data to keep this data private. This entails both limiting access to and placing restrictions on certain types of information with the goal of preventing unauthorized access (confidentiality) as well as protecting data from being modified or corrupted without detection. Such data must therefore be processed locally at the edge and only leverage data available within privacy limits (smart data).

Transparency: Enables IoT and AI-based systems to provide insight into devices and processes in situations such as auditing, inspections to assess vulnerabilities, or when security breaches arise. This may be supported by digital twins that represent the complete system state at any point in time. AI methods for data visualization can further enhance transparency and contribute to making the systems state easier to understand.

Fairness: Enables IoT systems which embed AI technologies to support or automate decision processes while adhering to the same fairness and compliance standards as humans.

Inclusiveness: Enables AI-based IoT systems to allow human intervention even in the most automated decision and communication processes. This is essential to avoid the formation of isolated non-AI capable subsystems within a process, production system or supply chain.

Collaboration: Enables AI-based IoT systems to self-organize around a common goal; for example, in the presence of a threat, as well as to collaborate with humans, both physically (e.g., human-robot collaboration) and by exchanging information (human-machine interfaces). Collaboration is an emergent property of complex interactions and dynamics, increasingly present in industry. Industry-grade AI will not be concentrated on a single device or system. Instead, many different AI-enabled subsystems will be distributed (distributed AI) across IoT nodes, embedded devices and other edge devices (embedded AI).

Integration: Enables IoT-embedding AI systems to exhibit an open and flexible perspective by consolidating insights from all existing systems and processes. Bridging possible gaps is a key prerequisite of the establishing AI methods in the industry according to a sustainable roadmap.

Reliability: Enables IoT systems to operate without systems outages and regular human intervention. Reliability is essential for productivity and is a key prerequisite for AI systems that are put into continuous operation with short maintenance time in mission-critical production environments.

Resiliency: Enables IoT with embedded AI to always operate in stable states, including to return to such states after failures. Resilience is essential for their safe support for our digital economy. In the future, they should even be able to detect failure and initiate measures for compensating it.

Accountability: Enables IoT systems with embedded AI systems that support or even replace human decisions to be accountable to their customers, partners and regulators. Normally, accountability features will be integrated "by design" and will be available via the supplier of these systems.

Verifiability: Enables IoT and AI-based systems to demonstrate the functionality and properties they are supposed to have. AI systems for industrial applications must fulfil the same standards as legacy systems and will be applied to safety-, mission- and business-critical tasks. This requires that AI embedded systems can be validated (to reach correct results), verified (verifiable AI) and certified (certifiable AI) for the targeted applications

As machines are becoming increasingly intelligent and more highly capable of doing tasks once thought only humans could complete, it is increasingly important to consider the laws that must govern their behaviour. The proliferation of interaction between humans, autonomous systems, IoT and AI demands increased regulation with increased sensitivity to both humans and AI.

The adoption of the Asilomar Principles [65] is essential to the continued harmonious growth and development of autonomous systems, autonomous vehicles, IoT and AI. The list of Asilomar AI Principles is presented below [65]:

- Research Goal: The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.
- Research Funding: Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:
  - How can we make future AI systems highly robust, so that they do what we want

  - without malfunctioning or getting hacked?
  - How can we grow our prosperity through automation while maintaining people’s resources and purpose?
  - How can we update our legal systems to be fairer and more efficient, to keep pace with AI, and to manage the risks associated with AI?
  - What set of values should AI be aligned with, and what legal and ethical status should it have?
- Science-Policy Link: There should be constructive and healthy exchange between AI researchers and policy-makers.
- Research Culture: A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.
- Race Avoidance: Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.
- Safety: AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.
- Failure Transparency: If an AI system causes harm, it should be possible to ascertain why.
- Judicial Transparency: Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.
- Responsibility: Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.
- Value Alignment: Highly autonomous AI systems should be designed so that their goals and behaviours can be assured to align with human values throughout their operation.
- Human Values: AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.
- Personal Privacy: People should have the right to access, manage and control the data they generate, given AI systems power to analyse and utilize that data.
- Liberty and Privacy: The application of AI to personal data must not unreasonably curtail people’s real or perceived liberty.
- Shared Benefit: AI technologies should benefit and empower as many people as possible.
- Shared Prosperity: The economic prosperity created by AI should be shared broadly, to benefit all of humanity.
- Human Control: Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.
- Non-subversion: The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.
- AI Arms Race: An arms race in lethal autonomous weapons should be avoided.
- Capability Caution: There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.
- Importance: Advanced AI could represent a profound change in the history of life on Earth and should be planned for and managed with commensurate care and resources.
- Risks: Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.
- Recursive Self-Improvement: AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.
- Common Good: Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization.

All these new developments bring new challenges to security, privacy and trust for autonomous vehicles and IoT applications and they need to be addressed in a holistic policy framework.

3.3 V2X application and use cases

Next-generation Cooperative ITSs (C-ITSs) are expected to bring the paradigm of Mobility-as-a-Service (MaaS) to a whole new level by means of autonomous vehicles, AI and IoT. A critical factor in an autonomous vehicles -based MaaS paradigm is represented by autonomous vehicles that cease to be autonomous systems and become cooperative entities. Specifically, cooperation among autonomous vehicles is enabled by the sharing of sensor data and manoeuvring intentions in V2V and V2I fashion. Table 11 ITS service and the estimated amount of sensor data to be transmitted/received on V2X [119].

Table 11: ITS service and estimated sensor data to be transmitted/received [119]

ITS Services	Message Types	Estimated data transmitted/received	Influence on ITS Services
Intelligent Traffic Planning	Area map grids and road shape reports.	10 Kbps - 10 Mbps	Enabling the origin-to-destination long-term journey planning
	Area knowledge of autonomous vehicles positions	10 Kbps - 800 Kbps	Congestion prevention
	Routes and destination in low resolution	80 Kbps - 800 Kbps	Congestion prediction and high-level rerouting
Emergency Vehicle Routing	LiDAR sensor raw data streams exchanged and processed in real-time	50 Mbps - 250 Mbps	Precise high-mobility manoeuvres
	Accurate representation of the nearby moving obstacles	80 Kbps - 800 Kbps	Decision making through accurate object tracking
	Trajectory paths with time profiles	80 Kbps - 800 Kbps	Enhanced cooperation between autonomous vehicles improving long-term manoeuvre smoothness
Multimodal Commute	Available parking spaces in proximity	10 Kbps - 10 Mbps	Reducing the overall commuting time
	Area knowledge of autonomous vehicles positions	10 Kbps - 800 Kbps	Refinement of the expected arrival time
	Information on road disruptions (e.g., accidents, adverse weather conditions, road conditions, etc.)	30 Kbps - 100 Kbps	Autonomous vehicles rerouting

Safety critical systems, like self-driving vehicles, require detection accuracy much higher than in the internet industry. These systems are expected to operate flawlessly irrespective of weather conditions, visibility, or road surface quality. A fleet of 100 cars instrumented with 5 cameras each generates in excess of one million hours of video recording in a year. A typical vehicle used for data collection in the self-driving vehicle use case is equipped with multiple sensors. This includes technologies such as radar, cameras, lidar, ultrasonic sensors, and a wide range of vehicle sensors distributed over the vehicle's Controller Area Network (CAN), Flexray, automotive ethernet and other networks. Typical test vehicles are equipped with multiple cameras, radars and other sensors to provide the computer system with added visibility and redundancy, which protects the vehicle against adverse weather conditions or failure of individual components. It is estimated that the volume of data generated by a single vehicle is equal with 1 TB+ / h and 100 vehicles operating for 8h/day * 260 working days / year will generate 204.8PB of data, resulting in a total data volume after pre-processing of 104 TB [118]. In this context, the training process computational requirements using neural network architectures of automotive detection networks for addressing tasks such as pedestrian detection, object classification, path planning, etc. is presented in [118]

Table 12: Assumptions and estimates for computational requirements for training based on data collected from a fleet of 100 autonomous vehicles [118]

Assumptions	Very Conservative estimate	Less Conservative estimate
Fleet size	100	125
Duration of data collection	1 working year / 8h	1.25 working year / 10h
Volume of data generated by a single car	1TB/h	1.5TB/h
Data reduction due to pre-processing	0.0005	0.0008
Research team size	30	40
Proportion of the team submitting jobs	20%	30%
Target training time	7 days	6 days
Number of epochs required for convergence	50	50
Calculations		
Total raw data volume	203.1 PB	595.1 PB
Total data volume after pre-processing	104 TB	487.5 TB
Training time on a single DGX-1 Volta system (8 GPUs)	166 days (Inception V3) 113 days (ResNet 50) 21 days (AlexNet)	778 days (Inception V3) 528 days (ResNet 50) 194 days (AlexNet)
Number of machines (DGX-1 with Volta GPUs) required to achieve target training time for the team	142 (Inception V3) 97 (ResNet 50) 18 (AlexNet)	1556 (Inception V3) 1056 (ResNet 50) 197 (AlexNet)

The new complex MaaS applications including autonomous vehicles and IoT will attract new type of V2X treats and attacks. Table 13 shows the security type of treat and attacks on V2X.

Table 13: V2X treats and attacks [108]

Confidentiality	Integrity and data trust	Availability	Privacy	Authentication and Identity
Eavesdropping	Message fabrication, suppression	Denial of service	Location tracking	Sybil attack
Information gathering	Information forgery	Jamming	Identity disclosure	Impersonation
Bogus information sharing	Masquerade	Broadcast tampering	Digital identity theft	Masquerade
Traffic analysis	Replay	Spamming		Replay attack
Location spoofing	Deletion			GPS spoofing
	Man in the middle attack	Black hole attack		Tunnelling
				Key/certificate replication
				Message modification/alteration
				Message tampering

Table 14 shows a basic set of application classes together with applications and use cases [77]. The use cases place emphasis on Confidentiality (C), Integrity (I), Availability (A), Privacy (P), and

Authentication (AU) as follows.

Table 14: ETSI ITS Basic set of applications definitions [77]

Application class	Application	Use cases	C	I	A	P	AU
Active road safety	Driving assistance: Co-operative awareness (CA)	Emergency vehicle warning	-	++	++	++	++
		Slow vehicle indication	-	++	++	++	+
		Intersection collision warning	-	++	++	-	+
		Motorcycle approaching indication	-	++	++	++	++
		Overtaking vehicle warning	-	++	++	+	+
		Lane change	-	++	++	+	+
		Glare reduction	-	++	++	++	+
	Driving assistance: Road Hazard Warning (RHW)	Emergency electronic brake lights	-	++	++	-	+
		Wrong way driving warning	-	++	++	-	+
		Stationary vehicle	-	++	++	-	+
		Traffic condition warning	-	++	++	-	+
		Signal violation warning	-	++	++	-	+
		Roadwork warning	-	++	++	-	++
		Collision risk warning	-	++	++	+	+
		Decentralized floating car data	-	++	++	-	+
		Collision unavoidable	-	++	++	-	+
Co-operative traffic efficiency	Co-operative speed management (CSM)	Regulatory/contextual speed limits notification	-	+	+	-	++
		Traffic light optimal speed advisory	-	+	+	-	++
	Co-operative navigation (CoNa)	Traffic information and recommended itinerary	-	+	+	-	++
		Enhanced route guidance and navigation	-	+	+	-	++
		Limited access warning and detour notification	-	+	+	-	++
		In-vehicle signage	-	+	+	-	++
	Other	Platooning	-	++	++	++	++
		Adaptive cruise control	-	++	+	++	++
Co-operative local services	Location based services (LBS)	Point of interest (POI) notification	-	+	+	-	+
		Automatic access control and parking management	++	++	+	++	++
		ITS local electronic commerce	-	+	+	-	-
		Media downloading	++	++	+	++	++
Global internet services	Communities services (ComS)	Insurance and financial services	++	++	+	++	++
		Fleet management	++	++	+	-	++
		Loading zone management	++	++	+	++	++
	ITS station life cycle management (LCM)	Vehicle SW/data provision and update	+	++	+	-	++
		Vehicle and RSU data calibration	+	++	+	-	++
	Other	Instant messaging	++	++	+	++	++
		Personal data synchronization	++	++	+	++	++
		Stolen vehicle alert	-	++	+	-	++
		Remote diagnosis	++	++	+	++	++
*Note: The use cases place emphasis on Confidentiality (C), Integrity (I), Availability (A), Privacy (P), and Authentication (AU) as follows: **++** = strictly required, **+** = intermediate,**-**=notrequired*							

3.4 Autonomous vehicles IoT trust framework

Considering that user’s needs and expectation are highly important when developing autonomous vehicles and IoT, a trust framework that consists of attributes and related properties based on the perspectives of the users need to be addressed. The autonomous vehicles and IoT Trust Framework presented in this document intends to provide a set of principles and the underlying structure that exhibit the trustworthiness, dependability and privacy for autonomous vehicles and IoT solutions into a holistic manner. The framework integrates the concepts of availability, reliability, safety, security, resilience, privacy and sustainability best practices, embracing “privacy and security by design” as a model for an implementable autonomous vehicle and IoT code of conduct and engagement.

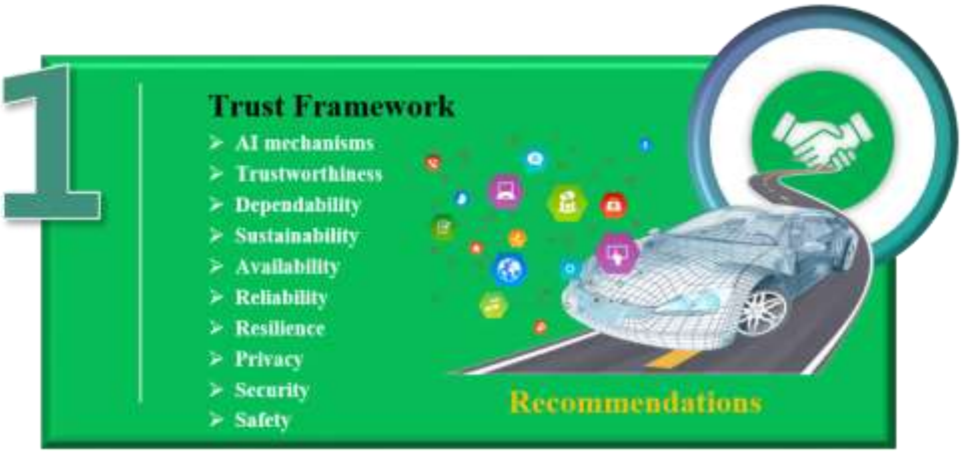


Figure 17: Autonomous vehicles IoT trust framework

Requirements are necessary for autonomous vehicles and IoT to fulfil specific demands, certain functions, qualities, the customer wants that requirements are part of the development of autonomous vehicles and IoT applications. Requirements consists of functional and non-functional requirements elements. Functional requirements such as technical details or specific functionalities define what autonomous vehicles and IoT systems are supposed to accomplish in order to be useful to the users. Non-functional requirements for autonomous vehicles and IoT systems define the properties, such as safety, security and privacy, which are critical to the product’s success based on the user’s expectations and demand.

The importance of trust in the autonomous vehicles and IoT systems is related to the factors for creating willingness to use autonomous vehicles and IoT applications and ensuring the correct usage.

3.4.1 AI mechanisms and trust

Trust and trustworthiness are well connected and becomes an indispensable requirement for autonomous vehicles IoT systems based on AI mechanisms, allowing authenticated devices or services that can be uniquely identified to participate in the decision-making processes of the autonomous vehicle IoT system. This makes it possible to report the source and act on vulnerabilities and inconsistencies [64]. Due to the AI mechanisms, trustworthiness will become multi-dimensional, far beyond verifying identity. Consequently, trust will no longer be "true or false", but rather about degrees of trustworthiness that will control the access levels to critical services.

The accuracy and quality of the data that are used by the AI learning algorithms influence the decisions of an IoT application involving autonomous vehicles [73]. In these safety and mission critical applications reliable data are crucial. The use and processing of data from reliable sources are an important element in maintaining confidence and trust in the AI technology and its mechanisms.

3.4.2 Trustworthiness

Trustworthiness is a property of people that engenders trust in the autonomous vehicles system, including IoT technologies. If the user has a choice to use one service or another, decision will depend of the degree of trustworthiness that the user has on the service.

There are several criteria that influence the trust that users can have on autonomous vehicle system and IoT technologies. For example, they need to be sure that the system is not increasing the risks on roads or to know how their data are used.

The clients' truth is one of the main points of autonomous vehicles and IoT policy framework, it is necessary to work on the reputation of the system and on the transparency with the user.

Important for the notion of trustworthiness is reliability and accuracy as autonomous vehicles, IoT and AI systems are trustworthy if the users and other autonomous systems can rely on them being right. Reliability is necessary for trust in autonomous vehicles, IoT and AI systems but is not enough. In this context, there should be considered the difference between human-human trust and human-AI-autonomous trust violations as there are different levels of competence required for humans to trust other humans versus trusting AI. Trust built up inductively between humans and autonomous systems IoT and AI can be destroyed with single instances of inaccuracy or unreliability.

Building trustworthy autonomous vehicles, IoT and AI systems requires understanding trust in human-human relationships, human-autonomous systems and autonomous systems to systems interactions.

3.4.3 Dependability

Dependability in complex autonomous vehicles, IoT and AI system represents the degree to which the system can perform its required function at any randomly chosen time during its specified operating period, disregarding non-operation related influences. Dependability for autonomous vehicles, IoT and AI systems is the property that integrates reliability, availability, safety, security, survivability, confidentiality, integrity, maintainability attributes to resist to threats such as faults, errors and failures by means such as fault prevention, fault tolerance, fault removal and fault forecasting.

Dependability of complex autonomous vehicles, IoT and AI applications is the ability to deliver the autonomous mobility service that can justifiably be trusted. The autonomous mobility service delivered by such systems are the behaviours of autonomous vehicles as are perceived by the user(s) and by other similar autonomous systems. A user is another system (physical, human) that interacts with autonomous vehicles, IoT and AI applications at the service interface.

The functions of autonomous vehicles, IoT and AI systems are what the systems are intended to do and is described by the functional specification. Correct autonomous mobility service is delivered when the autonomous mobility service implements the autonomous vehicles, IoT and AI systems functions. A system failure is an event that occurs when the delivered autonomous mobility service deviates from correct autonomous mobility service. A failure is thus a transition from correct autonomous mobility service to incorrect autonomous mobility service, i.e., to not implementing the autonomous vehicles, IoT and AI systems functions. The delivery of incorrect autonomous mobility service is defined as autonomous vehicles, IoT and AI systems outage. A transition from incorrect autonomous mobility service to correct autonomous mobility service is defined as autonomous mobility service restoration.

Dependability is important to autonomous vehicles, IoT and AI systems trustworthiness because it establishes the conditions and requirements that the systems functions and behaviours are consistent and repeatable.

3.4.4 Sustainability

Sustainability is the ability of the autonomous vehicles system and its constituent IoT parts to continue over time. To achieve this, the developments must be future-oriented with respect to technologies, applications and businesses activities, and facilitating improvements through software updates or even hardware exchange. The users of autonomous vehicles services must be able to trust that they always have the latest software and the best equipment within security and safety for example. To develop sustainable autonomous vehicles services, also the public authorities should contribute through regulatory strategies and promote the usage of autonomous vehicles.

3.4.5 Availability

Availability is the ability of the autonomous vehicles system, including IoT technologies, to be used at any time. Availability is a measure of the delivery of correct autonomous mobility service with respect to the alternation of correct and incorrect autonomous service.

In order to have a functional system, it is important to be able to get all the necessary data when it is needed. Using the IoT technologies, the connection with the network is one of the main constraints. There are always new technologies that are increasing the network coverage and then the availability of the system. For example, the 5G network will help to handle more connected devices without degrading performances than other networks.

3.4.6 Reliability

Reliability is the ability of the autonomous vehicles system, including IoT technologies, to deliver and accomplish services as specified within given constraints. Reliability is a measure of the continuous delivery of correct autonomous mobility service or, equivalently, of the time to failure.

It is more than important to be sure of that the data used by the system are valid. With autonomous vehicles system using IoT technologies, we need to get precise values, but more important, these values should still be valid when we need it. Indeed, the main point is that if we want a reliable system, this one must be able to get data in a short time. Because of the quickly changing environment on the roads, values are becoming obsolete in a short amend of time.

Reliability relates to the ability of the autonomous vehicles, IoT and AI applications to perform well consistently. Autonomous vehicles that receive high level of reliability influence user’s acceptance.

3.4.7 Resilience

Resilience is the ability of the autonomous vehicle system, including IoT technologies, to transform, renew, resist, respond and recover timely from damaging effects and states.

Resilience includes the agility of both defence and recovery capabilities for autonomous vehicles, IoT and AI applications. Resilient autonomous vehicles, IoT and AI systems help autonomous services to sustain operations when possible damaging effects and states, and to rapidly recover in the event of disruption.

If anything happened to the system and forced this one to restart for example, it is important that the system will be able to recover quickly and restart its services. Using IoT technologies is helping the resilience of the system. Indeed, almost all the needed data are accessible by the IoT platform, so the AV system can recover as fast as possible its previous state.

Resilience for the autonomous vehicles, IoT and AI systems includes the ability as well to resist the loss of autonomous traffic-serving capability by using traffic (e.g. geometric) and control system design (i.e. the inherent resilience) and by dynamically activating capacity-enhancing measures (i.e. the dynamic resilience).

There are many facets of resilience of the autonomous mobility systems that includes the resilience of adaptive capacity in autonomous mobility traffic networks with intelligent systems and advanced methods based on real-time use of autonomous mobility traffic assignment (i.e. dynamic or system-optimal) and route guidance parts of active autonomous mobility traffic management.

3.4.8 Privacy

The notion of privacy refers to all the organisational and technical measures implemented for any processing of personal data in order to guarantee the protection of such data and the rights of the data subjects.

Privacy refers to the data used by the autonomous vehicle system, including IoT technologies. More precisely, it refers to how these data are used and by whom.

For autonomous vehicles, IoT and AI applications the privacy has to be considered from different angles in order to address the complexity of different issues.

Privacy in the case of autonomous vehicles, IoT and AI applications should be considered to be contextual, in the sense that information flows of personal information could be seen as appropriate or not depending on the context where these flows happen, and each context could have a number of norms, or rules that govern the flow of personal information.

Privacy in human to human relationships is focusing on how individuals interact with others, continuously negotiating the information they reveal/conceal to/from others.

In autonomous vehicles, IoT and AI applications there is a need to acknowledge the plurality of privacy,
focusing on the information-related activities, how the activities are performed, what type of data is involved, who uses/handles/transfers/stores the data, personal and cultural factors, habits, preferences, etc.

Detecting when and where a privacy breach may happen when dealing with personal information and hence privacy-respecting mechanisms in autonomous vehicles, IoT and AI applications and what specific mechanisms and how they could be used to design privacy-respecting autonomous systems need to be addressed.

The trust is influenced by the privacy information generated and used by a system and is particularly important in autonomous vehicle applications. A separate privacy framework is covered in section 3.6 to get deeper into the important aspects of privacy issues.

3.4.9 Security

Security is the ability of the autonomous vehicle system, including IoT technologies, to protect the users/passengers, the pedestrians and other road users, the system itself and the information from unauthorised actions, deliberate and accidental intrusion or attacks.

The trust is influenced by the security level of a system and is particularly important in autonomous vehicle applications. A separate security framework is covered in section 3.5 to get deeper into the important aspects of security issues.

Security measures are implemented in the information system in order to mitigate security risks. Security is one of the main concerns regarding IoT, which needs to be addressed along with the paramount need for safety [43].

Security attributes is one of the main determinants for users to accept the autonomous vehicles, IoT and AI applications. Security relates to an attribute that protects the digital information and data from any danger or threat from any malicious.

Information security addresses the protection goals confidentiality, integrity, availability. These goals are important and also form a privacy and data protection perspective that specifically requires that unauthorised access and processing, manipulation, loss, destruction and damage are prevented [44].

Components of the system, the services that they and the system use, and the services the system provide shall be secure [45]:

- By design – the product, or service has been conceived, designed and implemented to ensure the key security properties and maintained: availability, confidentiality, integrity and accountability;
- By default – the product, or service, is supplied with the confirmed capability to support these security properties at installation;
- Throughout their lifecycle – security should be maintained from initial deployment through maintenance to decommissioning
- And that each of the above principles should be verifiable.

Security in an autonomous driving IoT systems is more than just information security because assets are not just data and IT infrastructure, and because securing a distributed network of devices presents different challenges. This leads us to section 3.7.3 (Guidelines and standards), the adoption of the ISA IEC 62443 standard that is thought for Industrial Automation Control Systems (IACS).

3.4.10 Safety

Safety is the freedom from unacceptable risks. As an engineering discipline, safety (or functional safety as it is named in the automotive domain) allows to produce systems, in which the absence of catastrophic consequences of failures is guaranteed with an acceptable level of risks. For AUTOPILOT it is needed to address road safety (avoiding traffic incidents) as part of the infrastructure.

Safety relates to the ability of the autonomous vehicles, IoT and AI applications to ensure safety of its users and other people surrounding it.

In the context of the AUTOPILOT project, safety is thus the ability of the autonomous vehicle system, including IoT technologies, to operate without harmful states and catastrophic failures and avoid traffic incidents.

In automotive, functional safety is ensured by the following of the ISO 26262 standard. This standard is intended to be applied to safety-related embedded systems that are installed in series production passenger vehicles and does not intent to be applied to IoT technologies as they are not installed yet in series production passenger's vehicles. It is also important to note that there is currently no functional safety standard for IoT technologies.

One option could be to consider applying the ISO 26262 standard to IoT technologies, but this standard would not fit this purpose and its application to these technologies would be very difficult as it relies on classical system engineering, decomposing a global system into smaller parts, and so on until a hardware subsystem and a software subsystem.

Therefore, the functional safety recommendations would be to develop the IoT technologies following the best practices that are currently the state of the art to guarantee that the IoT part of the system has been developed and designed with a particular attention and to avoid as much as possible failures. Following the use of the IoT technologies, the risk might be different and the attention that should be payed to the system design and development depends on this risk level. For example, the IoT system delivering entertaining content (e.g. music, video, etc.) is not at the same risk level than an IoT system delivering information on the environment of the vehicle, and then the development effort regarding safety is not at the same level.

However, one important thing to note is that the introduction of IoT technologies enables the global safety enhancement by providing the driver and/or autonomous vehicle with a better and increased awareness, thus potentially reducing the number and seriousness of accidents.

3.4.11 Requirements and recommendations

Table 15 provides a list of trust related requirements and recommendations applicable to IoT enabled autonomous driving environments. Note that some of the points are based on requirements and recommendations given by OTA [85].

Table 15: Trust - Requirements (Req) and Recommendations (Rec)

No.	Trust framework	Req.	Rec.
3.4.1	Ensure and substantiate the accuracy and quality of the data that are used by the AI learning algorithms which influences the decisions of an IoT application involving autonomous vehicles. In these safety and mission critical applications reliable data are crucial. The use and processing of data from reliable sources are an important element in maintaining confidence and trust in the AI technology and its mechanisms.	X	
3.4.2	Achieve trust and trustworthiness by ensuring and proving excellent safety, security, privacy, resilience, reliability, and dependability properties for the autonomous vehicles and driving applications.	X	
3.4.2	Achieve trust and trustworthiness by ensuring high quality of information, service and experience (QoI, QoS and QoE) for the autonomous vehicles and driving applications.		X
3.4.2 3.4.8 3.4.9 3.4.10	Updates and patches should not modify user configurated settings without user notification. If modified, the user should be provided the ability to review on the first use, and if not safety/security/privacy critical the ability to select settings.	X	
3.4.6	Validate that the system gets the waited data in requested time (latency requirements for that function), otherwise the data will be outdated.	X	
3.4.2 3.4.9	Don’t hand out users’ information and data without the users’ permission	X	
3.4.2 3.4.9	If you need to transfer users’ information or data to another third part, you should share only the needed users’ information and data.		X
3.4.5	Verify that your system gets the needed data at every moment even in the worst-case situation.		X

3.5 Autonomous vehicles IoT security framework

Security as an element of trust were already introduced in section 3.4.9. The autonomous vehicles and IoT Security Framework are based on elements such as AI security mechanisms, identification, authentication, authorization, availability, confidentiality, integrity, secure analytics, network prescribed policy and secure communication, as well as security by-default, by-design and best practices.

These elements must be applied throughout the lifecycle processes of autonomous vehicles and IoT systems, which includes impact assessment (when risks are assessed) and design of controls (when risks are mitigated).

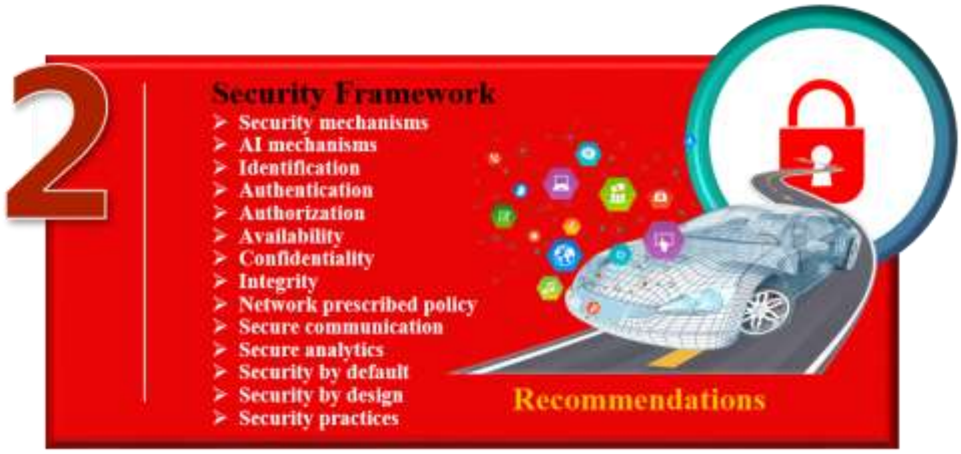


Figure 18: Autonomous vehicles IoT security framework

Autonomous vehicles and IoT applications allow the vehicles to be connected wirelessly to other vehicles, infrastructure, devices, service providers, and software controls critical driving functions. If actors can access and modify or corrupt the software, it can lead to accidents and potential fatalities. As the autonomous vehicles and IoT applications require large amount of software in an automobile, the vehicle attack surface increases.

As autonomous automobiles and IoT connects the vehicles and the infrastructure by wireless means this further increases the vulnerability problem in so far as the number of access points through which a vehicle may be breached and then infect other vehicles or the supporting infrastructure.

The end-to-end security is a key element for autonomous vehicles and IoT as the electronics in a vehicle and IoT devices (hardware + software) is built from components supplied by several vendors in multiple tiers who probably not have common security standards to adhere to as they build their components. This makes the supply chain for the autonomous vehicles and IoT complex and penetrable in respect to security. Every vendor and every component are a point of vulnerability.

The electronics in an autonomous vehicle are a complex network of distributed computing/processing systems called electronic control units (ECUs). An ECU is a piece of hardware and software that controls an important function in the autonomous vehicle such as braking, autonomous steering, power train, connectivity, infotainment and more banal functions such as window control and air-conditioning. The ECUs are networked by buses (copper wires/optical fibre), which carry messages using some defined protocol. This interconnected network allows ECUs to talk to each other. Safety critical and non-safety critical ECUs interact through this network. Some of these ECUs can be accessed by wireless means or physical access. Access to the ECUs means a potential point of vulnerability and requires isolating safety-critical and non-safety critical ECUs.

The lifetime for an autonomous vehicle varies between 5 to 15 years, while the lifetime of IoT components may be much shorter. Over the lifetime of autonomous vehicles and IoT devices the software, communication protocol and security must be updated. This time period brings risk, as hackers become more sophisticated over time and users of autonomous vehicles and IoT applications may download software that may contain malware.

The standards and security practices used today are not adequate for autonomous vehicles and IoT applications. Functional safety standards like ISO 26262 (ASIL-A to ASIL-D), information sharing like Auto-ISAC, software coding guidelines like the MISRA, EURO NCAP and NHTSA 5-Star overall safety scores (which is more to do with collision) do not solve the security and safety issues that autonomous vehicles and IoT applications are facing.

In this context a holistic autonomous vehicle and IoT security Framework is needed to support the deployment, acceptance and adoption of autonomous vehicles combined with IoT applications.

3.5.1 Security mechanisms

The goal of security is to maintain the confidentiality, integrity and availability of assets in order to enable successful business operations. The goal is accomplished through the implementation of security controls: actions that mitigates a potential vulnerability and helps ensure that the software behaves only in expected manner [46]. The implementation of connected device ecosystems imposes very specific operational and security challenges, especially as the number of points of attacks became greater [47].

An IoT implementation usually covers a diverse set of devices with a diverse set of capabilities that are connected to a single platform or series of platforms. If many of these devices were designed to work in confined environments, now more widely available connectivity technologies are opening connection introducing a new set of threat vectors requiring a new approach to handle system security and integrity [47].

A connected vehicle requires a security mechanism that should take care of the device and individual component identity to ensure that all interactions are authenticated and authorized [47]. In order to quantify the threats, it is important to list the information assets which must be protected. To assess security issues, threats and countermeasures have been defined in AUTOPILOT by referring directly to the main current standards. AUTOPILOT has started a process of securing infrastructure based on ITS-G5 standard in order to ensure autonomous driving in safety. This can be done by:

- Providing policies and services of strong authentication of both vehicle and infrastructures.
- Performing more and more risk assessments and mapping them into requirements of the ISA/IEC 62442 set of standards.
- Dealing the project pilot use cases as special instances of Industrial Automation Control Systems (IACS).

3.5.2 AI mechanisms and security

Autonomous vehicle IoT systems need to guarantee distributed end-to-end security AI mechanisms. It is essential to ensure robustness against all types of attack vectors in the systems [64]. This includes securing each AI mechanism system itself, as well as securing the communication between edge computing devices or vehicles with encryption and authentication mechanisms against attacks with for example manipulated input data.

AI mechanisms and cognitive IoT technologies allow embedding intelligence into autonomous vehicle IoT systems and processes, enabling the digital mesh to expand the set of endpoints to access information or interact through applications [73]. As the device mesh evolves, connection models expand and greater cooperative interaction between devices emerges, creating the foundation for a new continuous and ambient digital experience. The information exchanged by autonomous vehicle IoT applications is managed by IoT platforms using cognitive systems with new components addressing the information systems, customer experience, analytics, intelligence and business ecosystems in order to generate new and better services and use cases in the digital business environment.

The AI mechanisms and the cognitive IoT capabilities at the edge integrate the functions of the intelligent digital mesh and related digital technology platforms and application architectures at the cloud level, while increasing the demand for end-to-end security solutions [73]. In addition to the use of established security technologies, it is critical to monitor user and entity behaviour in various scenarios. IoT edge is the new frontier for security solutions creating new vulnerability areas that require new remediation tools and processes that must be embedded into IoT platforms.

Security and safety are critical for IoT technologies using AI integrated with autonomous systems. Cognitive techniques and AI agents are used to learn about and interact with smart environments, and must detect unpredictable and harmful behaviour, including indifference to the impact of their actions that can be interpreted as a form of hacking [73]. In this context, the actions of an AI agent may be limited by how it learns from its environment, how the learning is reinforced and how the exploitation dilemma is addressed. All IoT systems, including autonomous vehicle IoT systems could be exposed to malicious actors trying to manipulate the algorithm by using "adversarial learning" mechanisms to influence the training data for abnormal traffic detection, and which demonstrates that security and safety considerations must be considered in the debate around transparency of algorithmic decisions.

Accountability is another factor that must be considered for autonomous vehicle IoT systems based on AI and cognitive technologies where things learn on their own, and humans have less control [73]. Machine learning can create situations that bring into question who is accountable; is it the developers, the manufacturers, the service provider, the fleet manager, the collaborative network, etc. The advancement of AI mechanisms in autonomous vehicle IoT systems, requires the issue to be addressed, as flaws in algorithms may result in collateral damages, and there is a need for clarification regarding liability. AI and cognitive techniques introduce another dimension, as the training data, rather than the algorithm itself, could be the problem.

3.5.3 Identification

The identification is allowing an IoT device, and autonomous vehicle or service to be specifically and uniquely identified without ambiguity. This may take the form of different identifiers, IP addresses, global unique identifiers, electronic/physical licence plate, SIM, functional or capability identifiers, or data source identifiers. The IoT devices shall be able to identify themselves uniquely and in a way that makes it impossible to spoof identities

3.5.4 Authentication

Used for confirming the truth of an attribute of an entity or a single piece of data by using passwords, PINs, smart cards, digital certificates, or biometrics to sign in the IoT applications or access autonomous vehicles or/and IoT devices. Authentication is the process of confirming the identity of an IoT device, autonomous vehicle or confirming that data arriving or leaving are genuine and have not been tampered with or forged. Non-repudiation is an aspect of authentication that enables autonomous vehicles and IoT systems to have a high level of mathematical confidence that data, including identifiers, are genuine. This ensures that either a transmitting or receiving party cannot later deny that the request occurred and provides data integrity around the autonomous vehicles and IoT applications. This is very important in terms of tracking illegal activities within autonomous vehicles and IoT systems, as it allows for accountability to be enforced.

Authentication means assuring the authenticity of every device. It can be defined as a set of controls that are used to verify the identity of a user, or other entity or device. Authentication is how a person, or a system proves their identity. Three methods of authentications are [48]: provide something you know, something you have, or something you are. A Private Key Infrastructure (PKI) can be used to verify authentication of users and devices under a chain of trust principle, thanks to digital certificates.

3.5.5 Authorization

Used as function for specifying access rights to resources within autonomous vehicles and IoT systems and ensuring that any request for data or control of an external system is managed within these policies. Authorization mechanisms for autonomous vehicles and IoT systems to be centralized, decentralised, distributed or a combination of them. Decentralized solutions without an authority involved or distributed solutions allows different degrees of democratized authorization, where more entities can grant permissions implementing an authorization system that must be consistent, persistent and attack resistant.

Access Control, also known as Authorization – is mediating access to resources based on identity and is generally policy-driven [49]. Access Control govern decisions and processes of determining, documenting and managing the subjects (users, devices or processes) that should be granted access and the objects to which they should be granted access: essentially, what is allowed [49].

3.5.6 Availability

Autonomous vehicles and IoT systems must provide data and resources in a timely manner for a set percentage of the time (e.g. 99.99% uptime availability), and it is critical that the autonomous vehicles and IoT devices are available or retain their critical functionality, even if parts of the system/application/service have undergone an attack. Availability is a measure of a system's accessibility and usability [46].

3.5.7 Confidentiality

Represent the set of functionalities that limits access or places restrictions on certain types of information to autonomous vehicles and IoT systems with the goal of preventing unauthorized access. Confidentiality is usually achieved through encryption and cryptographic mechanisms and is essential within autonomous vehicles and IoT ecosystems where a large amount of information is exchanged among autonomous vehicles, IoT devices, infrastructure. Confidentiality ensures that information is disclosed only to authorized parties [46].

3.5.8 Integrity

This represents a critical measure in information assurance for autonomous vehicles and IoT systems and by providing consistency or a lack of corruption within the autonomous vehicles and IoT systems. This requires that the final information received to correspond with the original information sent and that data cannot be modified without detection. Malicious modification of the information exchanged may disrupt the correct functioning of entire autonomous vehicles and IoT systems ecosystems. Integrity is the assurance that information is accurate, complete and valid, and has not been altered by an unauthorized action [46].

3.5.9 Network prescribed policy

The V2X systems are not compatible with each other and DSRC and C-V2X, have different architectures, making it difficult to harmonize a single global solution. For the point of view of security and safety the systems need to offer the capabilities required by the autonomous vehicles and IoT applications.

Co-existence and dual-mode functionality (DSRC and C-V2X) could be the solution for a global dual-mode V2X platform. There are additional costs associated with implementing a dual-mode solution, but the infrastructure can be shared in the dual-mode approach. The total cost for DSRC deployment includes costs for the on-board equipment, communications infrastructure, the Security Credentials Management System (SCMS) with additional costs for a second radio on-board each vehicle, as well as for modifications to the applications software (to address receiving messages from other vehicles over multiple media, including potentially receiving identical messages from the same vehicle on each medium). V2X applications have the same requirements for privacy and security regardless of communications media and it is assumed that both DSRC and C-V2X systems could use the same security communications system as well as the same SCMS.

The technology-neutral nature of spectrum regulations in Europe means that both LTE-V2X and ITS G5 have equal rights to operate in the 5.9 GHz band, subject to compliance with the relevant regulatory technical conditions and each of C-V2X and ITS G5 can operate safety-related ITS services free from co-channel interference from the other technology.

The autonomous vehicles and IoT policy framework need to be aligned with stakeholders involved in the whole ecosystem including IoT application providers, mobile operators, automakers and suppliers, relevant industry associations and regulatory by agreeing a common approach to security, regulatory and infrastructure solutions to provide a common approach to security and spectrum harmonisation.

AUTOPILOT network is mainly built by three building blocks: the in-vehicle network, the cloud IoT platform, and the V2X and IoT network of connected devices. The in-vehicle IoT network requires a specific attention compared to the other two blocks; the IoT and V2X zone covers the medium range communication whereas the IoT Cloud Platform collects and exploits data from IoT peripheral devices.

Where designing a network architecture for an Industrial Control System (ICS), one of the main recommendations that should be considered is to ensure its segregation from existing corporate or traditional networks, to reduce the attack surface [50].

Moreover, following the zoning principles from ISA IEC 62443 is very important to derive security measures with a risk-based approach.

3.5.10 Secure communication

The majority of V2X messages are safety-related broadcast, with no restriction on which vehicles within range are allowed to read them. This includes V2V Cooperative Awareness Messages (CAMs) and I2V/V2I Decentralized Environmental Notification Messages (DENMs), as well as the Basic Safety Message (BSMs) outside Europe. Additionally, come IVIM, SPATEM and MAPEM, see [127][128]. These messages are not confidentiality protected. They are signed, to ensure that they come from an authorized sender, have not been tampered with and are anti-replay protected, to ensure that the time of transmission is also authentic.

The non-safety messages have a pre-determined audience and are represented by unicast or multicast messages that can be encrypted for confidentiality and signed for integrity and authenticity.

The EU Certificate/Security Policy (CP/SP) policy is technology agnostic, so should also apply for C-V2X. The policy is based on two types of certificates: a long-term certificate for device enrolment, and short-term certificate (Authorisation Tickets). The short-term certificates in the EU CP/SP cannot be revoked (as the devices are not continuously connected to the internet) [127][128].

A security-related requirement, for safety-related messages, is that the senders should be trustworthy and accountable and, hence, the removal/revocation of detected misbehaving participants from the V2X system is key and the requirement need to be supported by appropriate technical measures and certification procedures for the underlying software and hardware.

Availability as security requirement for safety-related messages, can be complicated by the scalability issues in some environments. Denial of service (DoS) attacks therefore need to be considered with respect to both illegitimate and legitimate entities including detection and if possible, mitigation of rough, localized radio jamming, plus prevention and/or early detection of more efficient DoS attacks, e.g., based on spoofed signalling messages that disable service for an extended time, or on spoofed safety messages being "amplified" by being replayed multiple times by legitimate entities and hence flooding the airwaves.

The measures are required to block the possibility for an attacker from the Internet to cause messages to be broadcast that are disruptive by their nature or their frequency; this is most naturally achieved in the system by clear authorization and authentication of parties that can trigger message broadcast at all.

In the case of spoofed messages from vehicles, the system includes the ability to revoke misbehaving vehicles. Timely and efficient revocation of vehicles that are identified as sending spoofed messages is not easy as the action need to be addressed in real time and/or periodically, for example at the start of each ride.

The aspects of security for LTE-V2X and ITS G5 are addressed by higher-layer standards developed by ETSI IEEE. LTE-V2X facilitates the provisioning and management of security for V2X applications in slightly different way than ITS G5.

For the case of certificates there is flexibility and uncertainty about how they are delivered. ETSI TS 102 941 [66] provides a list of examples:

- An ITS G5 communication via an RSU.
- A WLAN consumer network using IEEE 802.11 protocol (via a public or private hotspot or a home network).
- A Cellular network connection by a mobile network operator (3G, 4G or LTE).
- A wired or wireless connection at EV Charging station.
- Using the Vehicle On-Board Diagnostic (OBD) port and a diagnostic system at the Service Garage or inspection workshop.

C-V2X (LTE or 5G) is expected to provide a wide area connection almost all the time that allows either certificates or revocation lists to be updated regularly and timely. The EU Certificate Policy approach to pseudonym certificate management requires frequent issuance of new certificates to vehicles, while the IEEE/SAE approach requires regular updates to certificate revocation lists at the vehicle. Both approaches require wide area connectivity. ITS G5 does not has this (but the certificates can be updated when a vehicle passes an RSU, which is connected to the internet), while LTE does (although vehicles using ITS G5 for safety messages may have wide area connectivity anyway).

Wide area connectivity supports software/firmware updates, including security patches as ensuring the software integrity (e.g., at the start of each ride) is key for the V2X system to function properly. The scalability in the V2X system can be better addressed with the support of network infrastructure in LTE-V2X than in ITS G5.

The security of V2X management and provisioning messages, between the vehicle and the V2X Control Function or V2X Application Server are implemented in LTE-V2X that specifies a mechanism to provision security for these communication channels, using the Pre-Shared Key (PSK) TLS protocols based on LTE pre-shared keys [67][68] according to the Generic Bootstrapping Architecture (GBA) specified in 3GPP TS 33.220 [71]. This ability to use GBA for provisioning the initial cryptographic session/service keys at the transport or application layer is specific to cellular, due to the existing PSK infrastructure. Being based on symmetric keys pre-shared with the network, GBA thus relies on the trustworthiness of the mobile operator. There may be some further scope to use GBA to facilitate the creation of secure connections over which other management messages, including certificates or certificate revocation lists, could be sent. There may also be scope for manufacturers or operators to offer services based on this.

LTE subscription identifiers and credentials can be used in the enrolment and/or registration phase of both ETSI ITS and IEEE/SAE (with SCMS) approaches when built upon LTE-V2X. The PSK infrastructure provided by mobile operators can natively support symmetric-key credentials and certificates, which can be used within the ETSI ITS approach, possibly for some use cases in the multicast scenario.

3.5.11 Secure analytics

Organization of all types and sizes collect, process, store and transmit information in many forms including electronic, physical and verbal [51]. Given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present [51]. Information security is achieved by implementing a suitable set of controls, including polices, processes, procedures, organizational structures and software and hardware functions [51]. Information has a natural lifecycle, but information security remains important to some extent at all stages [51].

One often overlooked aspect of analytics is the need to protect raw data and data collection processes. Both analytics and machine learning can potentially be compromised by altering input data. Secure Analytics helps to detect both known and unknown attacks on the increasingly complex attack surface of IoT systems. In principle any security event should be collected, logged, correlated and analysed automatically. Only when the automatic analysis detects an anomaly the operators must be warned. At the scale of the AUTOPILOT use cases it would be unfeasible to do otherwise. Even for the setup of this continuous monitoring measures it is paramount to derive rules and priorities following a principled risk analysis methodology.

3.5.12 Security by default

Systems not designed with security by default are not secure without configuring them in a secure way. Thus, they require the users to know about security, and to invest time to manually secure it. Technology which is secure by default has the opposite approach. The devices are produced with a very secure default configuration and the user needs to modify the configuration to enable features that potentially make the system more vulnerable.

Technology which is secure by default has the best security it can without you even knowing it is there or having to turn it on. The secure by default principles we prescribe are:

- Security should be built into products from the beginning, it can’t be added in later;
- Security should be added to treat the root cause of a problem, not its symptoms;
- Security is never a goal in and of itself, it is a process – and it must continue throughout the lifetime of the product;
- Security should never compromise usability – products need to be secure enough, then maximise usability;
- Security should not require extensive configuration to work, and should just work reliably where implemented;
- Security should constantly evolve to meet and defeat the latest threats – new security features should take longer to defeat than they take to build;
- Security through obscurity should be avoided;
- Security should not require specific technical understanding or non-obvious behaviour from the user.

A system is secure by default when the default settings put the system in a secure state. To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities, security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities [51]. Identification and management of information security requirements and associated processes should be integrated in early stages of information projects. Early consideration of information security requirements, e.g. at the design phase, can lead to more effective a cost-efficient solution [51].

Service providers should design their products with a view to protect privacy by default, without preventing users from sharing life-logging data more widely when they are aware of the potential risks that entails [52]. Regulators should in general create strong incentives for companies to consider privacy requirements in early stages of product development [52].

3.5.13 Security by design

Security by design is achieved by embedding security in the design process. Security requirements are elicited, addressed and upgraded during the whole system lifecycle starting from the development phase. Risk driven design is a very similar concept that focuses on the idea that security requirements must be generated in accordance to real system/project risks. Security by design also deals with putting in place secure development processes and the adoption of good practices. Embedding security early into the design process is an enabler for cost reduction and security performance of the system. Developing security as an "add-on" is always worse in terms of costs and effectiveness.

We propose some guidelines established by the Department for Digital, Culture, Media and Sport in UK [39]:

- **No default passwords:** All IoT device passwords shall be unique and not resettable to any universal factory default value.
- **Implement a vulnerability disclosure policy:** All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.
- **Keep software updated:** Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.
- **Securely store credentials and security-sensitive data:** Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.
- **Communicate securely:** Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.
- **Minimise exposed attack surfaces:** All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.
- **Ensure software integrity:** Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the

consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.
- **Ensure that personal data is protected:** Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
- **Make systems resilient to outages:** Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, considering the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.
- **Make installation and maintenance of devices easy:** Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.
- **Validate input data:** Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

Architects and solution providers need guidance to produce secure applications by design, and they can do this by not only implementing the basic controls documented in the main text, but also referring to the underlying “Why?” in these principles. Such as confidentiality, integrity and availability [53]. The security should be considered no later than the design phase, to avoid unnecessary workarounds, refactoring costs, or worse [54]. In particular, the secure design should demonstrate how the vehicle security covers the threats identified in the risk assessment. Design should also consider cybersecurity key principles such as defence in depth or principle of least privilege, or the use of a hardware-supported Trusted Computing Base (TCB) small, secure and trusted, for critical services [54]. As in "Indispensable baseline security requirements for the procurement of secure ICT products and services" [45], the provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.

3.5.14 Security practices

Security criteria are the primary asset characteristics to be considered in the study which can be compromised or affected by a threat scenario:
- **Integrity:** accuracy and completeness of information.
- **Availability:** accessibility of Information when needed by authorised persons.
- **Confidentiality:** information only available to authorised persons.

Today more and more of our personal lives is spent connected to the Internet. Our personal computers are often connected to the internet 24/7 via high speed data lines, wireless connection extend the boundaries of our houses and now our home appliances are even exposed to the internet through web interfaces. We use this system because it makes life easier. These new technologies can also make life easier for attackers so below are it possible to find ten habits that normal users can be used to safeguard against common attacks [48]:
- **Protect your Secret:** use different passwords for each site.
- **Guard your Privacy:** limit the information on social media.
- **Use of security software and services:** install anti-virus software.
- **Secure your environment:** change all default passwords.
- **Perform routine maintenance:** use modern browsers.
- **Think twice before trusting:** do not click on links from unknown users.

- **Plan for the worst:** backup important data and store offsite.
- **Clean-up your devices and accounts:** logout of accounts when you are done using them.
- **Avoid unnecessary risks:** avoid malicious/underground websites.
- **Be vigilant and on alert:** review online account activity.

3.5.15 Requirements and recommendations

Good security practices are of fundamental importance. Even if there will probably never exist a finite set of tools and practices that can mechanically protect against all threats, what is very important is to raise awareness about security among all the stakeholders.

For system developers, maintainers and integrators following risk based secure development is paramount. Awareness at all levels and technology that does not impede usability and does not "get in the way" of user interactions with the systems are the keys to develop security properly. The protection of smart vehicles depends on the protection of all systems involved (cloud services, applications, car components, maintenance and diagnostic tools, etc.) [54].

The risk to the driver, their passengers and other users of the road makes it a matter of national end European interest. For this purpose, the following recommendations have been developed [54]:

- Recommendations for smart vehicle manufacturers, tiers and aftermarket vendors:
  - Improve cyber security in smart vehicles.
  - Improve information sharing amongst industry actors.
  - Improve exchanges with security researches and third parties.
- Recommendations for smart car manufacturers, tiers, aftermarket vendors and insurance companies:
  - Clarify liability among industry actors.
- Recommendation for industry groups associations:
  - Achieve consensus on technical standards for good practices.
  - Define an independent third-party evaluation scheme.
- Recommendation for industry groups and associations and security companies:
  - Build tools for security analysis.

It is important to understand that software vulnerabilities can have a scope beyond the software itself. Depending on the nature of the software, the vulnerability and the supporting infrastructure, the impact of a successful exploitation can include also the software and its associated information, the operating systems of associated servers, the backend database other applications in a shared environment, the user's system, and other software that the user interacts with [46].

Table 16 provides a list of security related requirements and recommendations applicable to IoT enabled autonomous driving environments. Note that some of the points are based on requirements and recommendations given by OTA [85], and ENISA in "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [43].

Table 16: Security - Requirements (Req) and Recommendations (Rec)

No.	Security framework	Req.	Rec.
3.5.1 3.5.2 3.5.14	Raise awareness for the need for IoT cybersecurity in autonomous vehicles and IoT systems, promote harmonization of cybersecurity initiatives and regulations, and foster economic and administrative incentives for cybersecurity.	X	

3.5.1 3.5.8 3.5.9 3.5.14	Achieve consensus for interoperability across the autonomous vehicles and IoT ecosystem and clarify liability among the stakeholders.	X	
3.5.2	Ensure and substantiate the robustness against all types of attack vectors in the IoT systems based on AI mechanisms. This includes securing each AI mechanism system itself, as well as securing the communication between edge computing devices or vehicles with for example encryption and authentication mechanisms against attacks.	X	
3.5.1 3.5.12 3.5.13 3.5.14	Disclose whether the autonomous vehicles IoT system is able to receive security related updates. If yes, disclose if the systems' constituent parts can receive and update security updates automatically. If any user action required, explain what user action is required to ensure correct update.	X	
3.5.1 3.5.6 3.5.9 3.5.14	Disclose what and how autonomous vehicles and driving features will fail to function if connectivity or backend services becomes disabled or stopped, including potential impact and necessary action. Include also the potential consequences and necessary action if the system/device no longer receives security updates.	X	
3.5.1 3.5.3 3.5.4 3.5.10 3.5.14	Ensure mechanisms is for automated safe and secure methods to provide software and firmware updates, patches and revisions. Such updates must be verified as coming from a trusted source.	X	
ALL	Ensure IoT devices, such as autonomous vehicles including their embedded IoT gateways, sensors and actuators, and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI, cellular (e.g., 4G) and Bluetooth connections.	X	
3.5.9 3.5.10	All IoT support web sites must fully encrypt the user session, from the device, such as autonomous vehicles including their embedded IoT gateways, sensors and actuators, to the backend services. Current best practices include HTTPS and/or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices, such as autonomous vehicles including their embedded IoT gateways, sensors and actuators, should include mechanisms to reliably authenticate their backend services and supporting applications.	X	
3.5.13 3.5.14	Ensure all IoT devices, including autonomous vehicle including its embedded IoT gateways, sensors and actuators, and associated software, have been subjected to a rigorous, standardized software development lifecycle testing including unit, system, acceptance, and regression testing and threat modelling, along with maintaining an inventory of the source for any third party/open source code and/or components. Employ generally accepted code and system hardening techniques across a range of typical use case scenarios, including preventing any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project's inception through implementation, testing, and deployment. IoT devices should ship with current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	X	
3.5.1 3.5.14	Define secure software and hardware development lifecycle guidelines for autonomous vehicles and IoT; and establish secure autonomous vehicle and IoT products and services lifecycle management.	X	

3.5.13	Design IoT devices, such as autonomous vehicle including its embedded IoT gateways, sensors and actuators, to minimum requirements necessary for operation. For example, USB ports or memory card slots should only be included if they are required for the operation and maintenance of the device. Unused ports and services should be disabled.	X	
3.5.1 3.5.12 3.5.13 3.5.14	Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain use cases a user may want the ability of deciding how and when the updates are made including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely automatic updates are pushed to the IoT device seamlessly without user interaction and may or may not provide user notice. Note that an IoT device can be an autonomous vehicle including its embedded IoT gateways, sensors and actuators.	X	
3.5.4 3.5.12	Include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	X	
3.5.1 3.5.13 3.5.14	Implement measures to help prevent and make evident any physical tampering of autonomous vehicle system and its constituent parts (e.g. IoT devices). Such measures help to protect the system and its AD functionality from being modified for malicious purposes.	X	
3.5.1 3.5.13 3.5.14	Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to vehicle and product features, functionality, security and privacy.	X	
3.5.1 3.5.14	Disclose the duration and end-of-life security and patch support, (beyond product warranty). Ideally such disclosures should be aligned to the expected lifespan of the device. It is recognized IoT devices cannot be indefinitely secure and patchable. Communicate the risks of using a device beyond its usability date, and impact and risk to others if warnings are ignored or the device is not retired.	X	
3.5.1 3.5.14	If the users must pay any fees or subscribe to an annual support agreement this should be communicated/disclosed prior to the purchase, and security related functions or other important functionalities should not stop working due to non-payment.	X	

3.6 Autonomous vehicles IoT privacy framework

The autonomous vehicles and IoT Privacy framework is based on the human-centred concept using as a benchmark point of reference for the user centred concerns associated with privacy by addressing the basic requirements of European Data Protection Law (e.g. principle of data minimisation, privacy by design etc.).

A harmonised legal framework needs to provide a level playing field for stakeholders involved in autonomous vehicles and IoT applications.

A regulatory framework needs to be adaptable and flexible to allow innovation, experimentation and large sale deployment and include a mix of binding regulations as well as industry standards and code of practice. This allows to promote innovation and encourage adoption autonomous vehicles and IoT applications while addressing the data privacy challenges.

Privacy by design, transparency, and/or privacy norms could help to mitigate privacy threats that autonomous vehicles, IoT and AI systems are facing.

An appropriate regulatory framework and requirements need to be in place so that developers and vendors are required to design and develop privacy enhancing and respecting autonomous vehicles, IoT and AI systems.

Regulations are important in terms of the information and knowledge ecosystems that emerge from the adoption of autonomous vehicles, IoT and AI systems, particularly regarding information/knowledge processing, exchange, store, communicate and the impact on autonomous services and experiences.

Autonomous vehicles technologies are based on integrated sensors to gather information about the environments, increasingly sophisticated algorithms to process sensor data and control the vehicle, and computational power to run them in real time. The autonomous vehicles utilise on-board Global Navigation Satellite Systems (GNSS) to recognise the roads and the environment around them; and radar and laser-sensing technology (such as LIDAR) which measures distance by pointing lasers at targets surrounding the vehicle and analysing the light that's reflected and building real-time maps of the environment. Considering various autonomous vehicles and IoT solutions used, it is important to recognize the distinction between vehicles that are fully autonomous and those that are semi-autonomous and the IoT services used because the different solutions will have different effects on privacy.

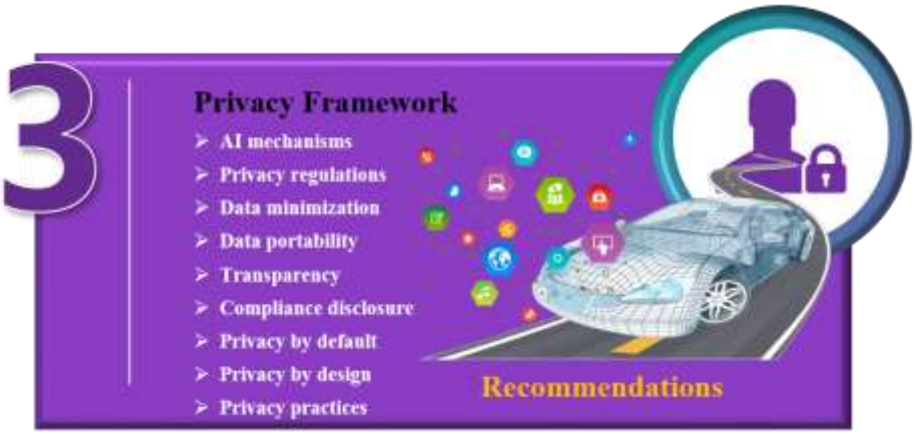


Figure 19: Autonomous vehicles IoT privacy framework

Level 4 autonomous vehicles are data-intensive and rely on real-time data tracking and the vehicles are connected to wireless networks through V2X technologies, mobile phones or Wi-Fi connections, in order to take advantage of the IoT applications and services. In this context, the risks to privacy breaches increases.

Autonomous vehicles and IoT applications, collect, use and share personal information about the persons using the vehicles, and legal privacy issues are raised that the different stakeholders must be conscious of data localization laws or valid consent to collect, share and sell the individual's personal information for all purposes. The data, the individuals, and the vehicles crossing borders need to address data privacy laws depending on the jurisdiction, that brings up interesting compliance and enforcement issues and challenges for policy-makers drafting domestic regulations while considering
international laws and the impact regulations on business development. Level 4 autonomy, and a fully self-driving fleet can offer new and improved forms of sharing [120].

The "sharing economy" and MaaS are trends that will influence vehicle ownership, as well as on current conceptions of data privacy and data privacy laws.

In autonomous vehicles and IoT applications there are several possible owners of in-vehicle data such as vehicle manufacturers, vehicle owners, the individual whom the information is about, the IoT service and platforms providers, the connectivity providers, the after-market applications that consumers or service businesses add to the vehicles, etc. The issues of ownership and access of the data is important because the entity that owns the data, as well as the messaging platform to the consumer, gains a controlled messaging environment, which results in an advantage over competitors

In order to help data controllers to build and demonstrate compliance now that GDPR has become applicable, the privacy impact assessment has become more practical to foster collaboration between stakeholders. Privacy impact assessment (PIA) is a process which helps an organisation to identify and reduce the privacy risks of a project. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved [58].

The GDPR applies to information concerning an identified or identifiable natural person. But does not apply to anonymous information, which is information that does not relate to an identified or identifiable natural person, or that has been made anonymous so that the individual is no longer identifiable. Consent must be clearly distinguishable, freely given, as easy to withdraw as it is to give, and auditable or verifiable. Consent must be unambiguous and not a passive activity, such as visiting a website with a pre-checked box to receive marketing emails.

For autonomous vehicles and IoT applications it is important to stress that consent must be distinguishable. Consent cannot be included in a long privacy policy and consent for one use, like marketing, cannot be merged with all types of consents. Providing a context-based option for users to withdraw consent is a challenge for autonomous vehicles and IoT applications considering that consent for marketing must not be a condition to receive the service. The GDPR recognizes a right to data portability, which is related to the principle of consent and it allows the consumer to request the transfer of their information from one provider to another. This right has implications for harmonising standards between jurisdictions and organizations and stakeholders in different ecosystems because organizations and ecosystems need to ensure that their processes for collecting and storing personal information are sufficiently compatible with the processes used by competitors.

The GDPR recognizes that Member States may have sector-specific laws in areas that need special attention. This can also mean specifying rules for special categories of personal data. In this regard, there are regulatory gaps in sector-specific laws, and it is difficult to define where the autonomous vehicles and IoT applications begins and ends or when the laws are too specific and not technologically neutral.

Performed in principle by a controller or provider, the purpose of a PIA is to build and demonstrate the implementation of privacy protection principles so as to empower data subjects. This is an iterative methodology, which should guarantee a reasoned, reliable use of such data during processing. PIAs are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach.

The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project. These can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy [59].

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of a project. In summary, it is necessary to:

- Define and describe the context of the processing of personal data under consideration and its stakes;
- Identify existing or planned controls (to comply with legal requirements and to treat privacy risks in a proportionate manner);
- Assess privacy risks to ensure they are properly treated;
- Make the decision to validate the way it is planned to comply with privacy principles and treat the risks or review the preceding steps.

3.6.1 AI mechanisms and privacy

In many cases, autonomous vehicles IoT systems based on AI mechanisms operate on mission critical data which shall remain private. This entails both limiting access to and placing restrictions on certain types of information with the goal of preventing unauthorized access as well as protecting data from being modified or corrupted without detection [64]. It is highly recommended that such data are processed locally at the edge and only leverage data available within privacy limits.

When using IoT technologies based on AI mechanisms for performing tasks ranging from self-driving vehicles to managing parking lots, there is a need for a robust and clear basis for the decisions made by an AI agent [73]. Transparency is covered later in section 3.6.5, however transparency around AI algorithmic decisions is in many cases challenged by limited by technical secrecy or literacy. Machine learning creates further challenges as the internal decision logic of the model is not understandable even for the developers, and even if the learning algorithm is open and transparent, the model it produces may not be. IoT applications involving autonomous systems need to understand why a self-driving vehicle chooses to take specific actions and need to be able to determine liability in the case of an accident.

3.6.2 Privacy regulations

The IoT requires pervasive collection and linkage of user data to provide personalised experiences based on potentially invasive inferences. Consistent identification of users and devices is necessary for this functionality, which poses risks to user privacy. The General Data Protection Regulation, or GDPR, sets a new bar globally for privacy rights, security, and compliance. It imposes a wide range of requirements on organizations that collect or process personal data, including a requirement to comply with six key principles:

- Transparency, fairness, and lawfulness in the handling and use of personal data. You will need to be clear with individuals about how you are using personal data and will also need a “lawful basis” to process that data.
- Limiting the processing of personal data to specified, explicit, and legitimate purposes. You will not be able to re-use or disclose personal data for purposes that are not “compatible” with the purpose for which the data was originally collected.
- Minimizing the collection and storage of personal data to that which is adequate and relevant for the intended purpose.

- Ensuring the accuracy of personal data and enabling it to be erased or rectified. You will need to take steps to ensure that the personal data you hold is accurate and can be corrected if errors occur.
- Limiting the storage of personal data. You will need to ensure that you retain personal data only for as long as necessary to achieve the purposes for which the data was collected.
- Ensuring security, integrity, and confidentiality of personal data. Your organization must take steps to keep personal data secure through technical and organizational security measures.

Connected products often collect data through device sensors or by logging user commands. The distinction between personal user data and environmental data becomes fluent. All data is assumed to be personal. In order to provide a technical assessment tool that have an impact on business models, customer support, end of life care, customer experience and more and is also important to consider in the early stages of a business, the free community Open Internet of Things Certification Mark [60] made a free, accessible, open checklist aimed at start-ups and SMEs to help them design better connected IoT products. In the list below, this is a set of principles that any connected product manufacturer, team or founder would use to make a responsible, secure, well designed connected product.

- The vendor MUST allow users to access their collected data, free of charge: the vendor submits a link to public documentation explaining how to export collected data, and a link to the respective section in terms & conditions.
- The vendor MUST submits a link to its public privacy policy explaining how the collected data is used.
- The vendor MUST allow users to migrate their collected data to another backend and to delete their collected data, submitting a link to public documentation (section terms & conditions).
- The vendor MUST allow users to easily opt out of direct marketing based on their collected data.
- The vendor MUST submits a link to public documentation explaining how to restrict and/or update the use of the collected data.
- The vendor MUST allow users to stop automated decisions being made, if there are personal legal or significant consequences: the vendor submits a link to public documentation explaining how to stop automated decisions and get a human to re-evaluate the decision.

3.6.3 Data minimisation

The principle of "data minimisation" means that the autonomous vehicles and IoT service providers should limit the collection of personal information to what is directly relevant. The stakeholders involved in autonomous vehicles and IoT application should retain the data only for as long as it is necessary to fulfil the purpose of the services, which means collecting only the personal data really needed and should keep it only for as long as is used.

Privacy data becomes more difficult to handle due to the increased number of data and the dispersed number of data sources. It is important to reduce the severity of the risks by minimizing the number of personal data that will be processed, by limiting such data to what is strictly necessary for the purposes for which they are processed (otherwise they should not be collected). Then, it also becomes possible to minimize the data themselves, via controls aimed at reducing their sensitivity.

This practice essentially reduces two risks in one: if a company is not storing large amounts of data it is less of a target to data thieves or hackers, the less data that is collected and the less time it is stored so that the data are not used to contradict user expectations. It can be possible to choose to collect no data, collect data limited to the categories required to provide the service offered by the device, collect fewer sensitive data, or de-identify the data collected.

The autonomous vehicles and their chain of IoT providers stretches, and the allocation of responsibilities and enforcement of data protection law is becoming more complex. The principles of purpose limitation and data minimisation could be difficult to follow.

Only necessary data should be collected, transmitted, stored, shared and used. The use of edge computing is an example of technology that usually reduces the amount of data transmitted and stored, since only the data needed for the actual autonomous vehicle application are transmitted. But if the data is not depersonalized, it is not given that this information is less private.

3.6.4 Data portability

Data portability is highly relevant for autonomous vehicles and IoT ecosystems and applies to access of personal data by promoting interoperability to protect the users from having personal data stored in an incompatible format or manner. Developing interoperable formats that enable data portability across applications and platforms in the ecosystem also supports the digital single market in general. The right to data portability allows data subjects to receive personal data they provided to a controller in a structured, commonly used and machine-readable format and to transmit those data to another controller, and is one of the fundamental data subject rights in the GDPR, (Chapter 3 - Rights of the data subject; Article 20 - Right to data portability) [37][38].

Interoperability is about making it technically possible to use devices, backends and clients of the vendor with those of a third party. Interoperability does not imply unrestricted access to user data. In the list below, this is a set of principles that any connected product manufacturer, team or founder would use to make a responsible, secure, well designed connected product:

- The vendor SHOULD allow third parties to connect clients to its backend, submitting a link to public documentation of the client-specific backend API.
- The vendor SHOULD grant third party clients the same functional scope on the backend as its own clients: some client-specific backend APIs delay measurements they make available to third party clients, preventing them from making real-time decisions.
- The vendor MAY allow third parties to connect devices to its backend.
- The vendor SHOULD allow third parties to communicate directly with its devices, without going through the backend.

3.6.5 Transparency

The protection goal of transparency is defined as the property that all privacy relevant data processing can be understood and reconstructed at any time, including technical, organizational, and legal issues, and covers the entire ecosystem and the entire life cycle [35].

Transparency is fundamental for both privacy and autonomous vehicles, IoT and AI systems. For privacy, transparency enables users to know how an autonomous mobility service and system works and how the personnel data will be used. Transparency is associated with several the privacy by design strategies such as informing, controlling and demonstrating. For autonomous vehicles, IoT and AI systems transparency can be used to allow a better human understanding of autonomous services and systems and the decisions taken, which could increase the trust.

For autonomous vehicles, IoT and AI systems opening the source code may not be enough to know how the system works as one important element could be not available e.g. data training sets, which are used for the autonomous system. Transparency in this context need to address fair computations, including fair machine learning and fair connectivity to maximize the utility of the classification tasks subject to a particular fairness constraint, like that users should not be discriminated based on their membership to a specific group of users.

Privacy and transparency in autonomous vehicles, IoT and AI systems could mean different things for the stakeholders involved, especially when transparency means knowing the current state of reasoning of an autonomous system and the data underpinning that state as in some cases the decision could be made based on knowing private date.

Data collection through IoT devices and the use of these data is an important to achieve autonomous vehicles and driving. It could be both real-time and historical data that to a greater or lesser extent are influencing privacy. The quality of transparency is important, i.e. openness without secrets. User knowledge, acceptance, and access are highly important. The autonomous vehicle users should be aware of what information is being collected, and how it is being stored, used and shared with other entities. "Is the data depersonalized?" and "what is the duration of data storing?" are examples of questions that will appear. The relevant service providers should provide accurate and understandable disclosures of their privacy practices.

However, autonomous vehicles and driving also needs more transparency according autonomous vehicle decision making [36]. Today, we have transparency according to mileage and human intervention, but what does it mean to be in a dangerous situation and what does it mean to get out of such a situation? To get more transparency in this field we need definitions in such a way that regulators, the vehicle industry and IoT technology providers can agree on a common standard or possible a selection of standards.

Hardware developers therefore must strike a balance between prioritizing security without diminishing the user experience. Leveraging Public Key Infrastructure (PKI) and digital certificates can be used to meet these requirements. In the list below, this is a set of principles that any connected product manufacturer, team or founder would use to make a responsible, secure, well designed connected product.

- The vendor MUST make explicit the legal implications of substantially changing device usage: the vendor submits a link to public user documentation explaining the (secondary) legal implications of changing how the device is used or taking it offline.
- The vendor MUST make explicit the expected duration of the terms of service.
- The vendor MUST ask permission from users before changing the terms of service, the vendor submits proof that terms and conditions changes are communicated to users and their permission is sought explicitly.
- The vendor MUST inform users about substantial firmware upgrades, submitting a link to a blog or feed or other public, auditable trail of firmware revisions.

3.6.6 Compliance disclosures

Even the strongest privacy policy is only as good as those who enforce it. Train employees on the requirements of any IoT policy and build privacy and security compliance into the company culture. Training employees is a relatively minor investment with a major return.

Companies have advanced their IoT initiatives beyond the experimentation phase, and they are poised to innovate with serious IoT rollouts. The challenge companies face is balancing the speed of deployments with the time needed to ensure IoT privacy compliance.

It is tempting to sacrifice compliance in a rush to take a product to market, but companies should resist the urge to cut corners. Remember, consumers, regulators and plaintiff’s firms are watching. The stakeholders who develop and offer services should explain how they addresses prevailing standards, regulations, and laws within all aspects of the autonomous vehicles and IoT ecosystem (security, safety, GDPR, ITS-G5, C-V2X, etc.). The targeted recipients may be the application users, equipment and system suppliers (automotive manufacturer, IoT manufacturer, etc.), network operators, service providers, politicians and decision-makers, national and international authorities (public roads authorities, communications authorities, etc.) within the autonomous vehicles and IoT fields.

3.6.7 Privacy by default

Privacy enhancing capabilities should be built in the IoT devices and smart services with an aim to prevent privacy invasive events. Anticipating IoT privacy events early during the ideation and development phases will help to prevent reactive responses to privacy breaches that can cause distrust among users.

All the data should be protected by default setting built into the IoT devices and smart services with no additional individual effort necessary to protect personal data. The accountability of privacy preservation should be on the IoT device manufacturers and smart service providers. This will help to build trustworthy IoT offerings for wider acceptability and adoption. A default privacy setting will automatically protect Personally Identifiable Information without the need of user intervention.

Many new products and services are based on so called plug-and-play devices, and the privacy settings can be programmed as default values from the producers or developers. The strictest functional privacy settings and mechanisms should automatically be set and apply once a user acquires a new product or service, and all future software updates should do the same. No manual change to the privacy settings should be required by the users, if they do not want to go easy on the privacy demands. However, the users should be clearly warned about possible consequences.

3.6.8 Privacy by design

Following the French Data Protection Authority, personal data shall mean any information relating to a natural person who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more pieces of information specific to that person. Thus, personal data include all data that, taken alone or in combination with others, can be linked to an identified or identifiable user, especially via the vehicle serial number or the vehicle licence plate number, whether by the data controller or by any other person. As an example, personal data include data relating to journeys made, the wear and tear on vehicle parts, the dates of technical controls, mileage, or driving style, to the extent that they can be linked to a natural person, especially via the vehicle serial number or the vehicle licence plate number, whether by the data controller or by any other person. Therefore, personal data are not just nominative data (surname and first name).

The working group on data protection and privacy continued the analysis on the implications of the General Data Protection Regulation on C-ITS [125]. In order to have a European-wide interoperable system, an enactment of an EU-legal instrument is needed. In parallel with developing the legal framework at European level, the working group recommends that a Data Protection Impact Assessment in accordance with the GDPR is conducted, including the assessment of risks, indicators, methodology for indicators and further requirements for data protection by design [125].

Designing an architecture integrating services to users/drivers has to be set up from the origin. The privacy by design is a mechanism able to handle the data control and the general flow of information going through the system. The data control shall only collect personal data that are strictly necessary for the processing. In the case of a contract for the provision of services, the only data that can be collected are those that are essential for the provision of service. Controlling privacy is defined by the capacity to:

- Configure by default the protection of privacy;
- Enable users to easily modify those configurations, during the entire processing period,

especially for activating or deactivating services based on consent or on the performance of a contract (e.g. commercial offers personalised based on geolocation or breakdown assistance);
- Enable users to adjust the level of detail of the data collected to the level of service requested, e.g. by accessing a map without being geolocated if they do not wish to be guided;
- Enable users to access all data easily.

The principles of the Privacy by Design must be at every step of a device development. Privacy regarding the data collected from users should be built in, and not be an afterthought. Assessing an IoT application in order to find privacy gaps is a complex task that requires systematic guidance. For these reasons, we believe that IoT development would benefit from having a privacy-by-design framework that can systematically guide software engineers to assess (and potentially design new) IoT applications and middleware platforms. Typically, systematic guidelines will generate a consistent result irrespective of who carried out a given assessment. Such a framework will also reduce the time taken to assess a given application or platform.

IoT privacy needs should be addressed to realize the potential of this technology. A 'Privacy by Design' approach is required for this emerging technology and smart services to address the growing privacy concerns and needs. We have presented here the seven principles of "IoT Privacy by Design". These are adaptive principles based on Dr. Cavoukian's 'Privacy by Design' principles that have been accepted globally [61].

- *Principle 1: Proactively Prevent Privacy Invasive IoT Events*
  Privacy enhancing capabilities should be built in the IoT devices and smart services with an aim to prevent privacy invasive events.
- *Principle 2: Ensure IoT Privacy by Default*
  The accountability of privacy preservation should be on the IoT device manufacturers and smart service providers. This will help to build trustworthy IoT offerings for wider acceptability and adoption.
- *Principle 3: Embed Privacy Enhancing Capabilities into IoT Service Design and Device Architecture*
  By identifying sensitive data components early in the design phase and embedding privacy enhancing capabilities into the IoT device architecture and smart service design it is possible to have reliable and trustworthy IoT offerings that complies with privacy requirements without affecting the core functionality.
- *Principle 4: Adopt a Stakeholder Approach to IoT Privacy for Full Functionality, Positive Sum Outcome*
  Privacy with security and safety results in a positive sum outcome for IoT offerings for all stakeholders as there is no compromising factors like 'privacy at the cost of security/safety' or vice versa.
- *Principle 5: Provide Full Lifecycle Protection of IoT Data for End-To-End Security and Privacy*
  The contextual data collected by the IoT devices and smart ser-vices should be preserved with appropriate security and privacy measures for the entire duration of the data lifecycle and then it should be destroyed ensuring no remanence.
- *Principle 6: Opt for a Verification Based Trust Approach to IoT*
  A verification-based trust approach to IoT technology, devices and data components is necessary for transparency in IoT operations.
- *Principle 7: Consider Users at the Core of IoT Services*
  Privacy being one of the key user requirements, a 'Users First' strategy for IoT will help to build user trust and confidence for these IoT offerings and ensure wider acceptance.

3.6.9 Privacy practices

As mentioned in section 3.6.5 (Transparency), the relevant service providers should provide accurate and understandable disclosures of their privacy practices, which should be which must be in accordance with applicable laws and regulations.

There is little difference between the IEEE/SAE and EU/ETSI security architectures and functions at a high-level as same messages are protected in the same way, with some differences in the cryptographic details, and some different efficiency optimizations in the two sets of standards.

The security functions deal with enrolment, registration, authentication, authorization, revocation, security associations, and standard security functions providing confidentiality and integrity, anti-replay and accountability. Both approaches relate to digital signatures and PKI for handling the certificates and credentials needed for implementing the security functions. Both approaches address privacy as an important requirement and use temporary identifiers with a limited lifecycle for this scope.

To prevent privacy-related abuses and encourage voluntary participation in the V2X system, it is important to minimize the risk of tracking the vehicles by monitoring the messages transmitted in the system, especially because they are broadcasted. The requirements of un-traceability and un-linkability should be implemented and respected. Un-traceability means that, except for authorised entities, it should be hard to derive the vehicle long-term identifier from temporary identifier(s), and that un-linkability means that, except for authorised entities, it should be hard to track the movement of the same vehicle on the basis of (temporary) identifier(s) used in the system.

Privacy is conditioned on the correct behaviour in the autonomous vehicles and IoT system. To minimize the risk of abuses, the conditions under which privacy can be revoked should be clearly specified and made known to the user (e.g., vehicle owner), and should preferably involve at least two independent authorised entities accountable for their actions. Privacy-related requirements (in line with GDPR [38]) also include the minimality principle with respect to data disclosure and data retention. Namely, the data regarding the user can be disclosed outside the V2X system (including vehicles) only with the user’s consent and retained in the V2X system no longer than necessary.

For autonomous vehicles transporting several passengers disclosing the data regarding the users of the services outside the V2X system could be an issue. To avoid consumer or regulatory concerns, there should be established requirements that third parties (outside the V2X system) should not be able to use V2X messages to track a user over an extended period.

Some local or regional regulations may contain explicit requirements on the prevention of vehicle tracking. For communications over V2X interface, both ETSI ITS and IEEE/SAE (with SCMS) standards include mechanisms for issuing pseudonym certificates to vehicles. There are differences in how these certificates are issued, and how they are revoked for a misbehaving device. In EU, short term authorisation tickets cannot be revoked.

The concept of privacy and data protection must not be reduced to protection of data. In fact, the concepts have to be understood more broadly: they address the protection of human beings and their personal rights as well as democratic values of society [44]. In 2011, the “Privacy framework” (ISO/IEC 29100) from the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) was published as an international standard. When privacy and data protection requirements exist, the standard is to be complementary [44].

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store specific types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. The costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

3.6.10 Requirements and recommendations

In today's information and communication technology landscape, privacy by design usually does not happen by itself, but it needs to be promoted [44].

Table 17 provides a list of privacy related requirements and recommendations applicable to IoT enabled autonomous driving environments. Note that some of the points are based on requirements and recommendations given by OTA [85].

Table 17: Privacy - Requirements (Req) and Recommendations (Rec)

No.	Privacy framework	Req.	Rec.
ALL	Provide and disclosure data solutions for the autonomous vehicles and IoT ecosystem in accordance with GDPR.	X	
3.6.1	If IoT systems based on AI mechanisms operate on mission critical data which shall remain private, process such data locally at the edge and only leverage data available within privacy limits.		X
3.6.2 3.6.5 3.6.6 3.6.9	Provide accurate and understandable disclosures of all the relevant autonomous vehicles service providers' privacy practices in accordance with applicable laws and regulations.	X	
3.6.2 3.6.5 3.6.6 3.6.9	Ensure that privacy together with security and support policies are accurate and understandable, and easily available for review prior to purchase, activation, download, or enrolment. In addition to prominent integration and placement suitable for the autonomous vehicle applications, the information should be available on product packages, websites, and contracts.	X	

3.6.2 3.6.5 3.6.9	Updates and patches must not change privacy settings or modify user configurated privacy preferences without user notification. If changed or modified, the user must be provided the ability to review and select privacy settings on the first use.	X	
3.6.3 3.6.9	Aim at data minimisation; only necessary data for the autonomous vehicle applications should be collected, transmitted, stored, shared and used.		X
3.6.2 3.6.4 3.6.9	Ensure and disclosure the rights of the data subjects and the right to data portability.	X	
3.6.2 3.6.5 3.6.9	Disclose the data storage policy and storage duration of personally identifiable information.	X	
3.6.5 3.6.9	Explain clearly what personally identifiable and sensitive data types and attributes are collected, how they are used, and how privacy is ensured. Limit the collection to data which are necessary and useful for the autonomous vehicles' application functionality and purpose. If the collected data are used for other purposes than intended, the consumers and other relevant stakeholders must be informed and obtain acceptance.	X	
3.6.2 3.6.3	The system can limit data access according to the "need to know" principle. The system can separate the sensitive data and apply specific access control policies. The system can also encrypt sensitive data to protect their confidentiality during transmission and storage. Access to temporary shadow files which are produced during the data processing must also be protected.	X	
3.6.4 3.6.8 3.6.9	Encrypted data communication would reduce the potential privacy risks due to unauthorised access during data transfer between components. There are multiple data communication approaches based on the components involved in an IoT application, namely, 1) device-to-device, 2) device-to-gateway, 3) device-to-cloud, and 4) gateway to-cloud.		X
3.6.5 3.6.6	Provide guidance on best practices in notification in privacy policies and also require to companies to collect feedback to assess consumers' comprehension of privacy policies. Manufacturers disclose what sensors are onboard devices and what they collect, in order to expand the definition of personally-identifiable information to include data collected by IoT sensors.	X	
3.6.8 3.6.9	The IoT ecosystem has multiple stakeholders who play significant roles in providing end-to-end IoT service. The privacy warp should run through the fabric of IoT components as a key enabler for all stakeholders to provide full functionality along with other key requirements like security and safety.		X
3.6.2	The vendor must allow users to access their collected data, free of charge, submitting a link to its public privacy policy explaining how the collected data is used. The vendor must allow users to migrate their collected data to another backend and to delete their collected data, with public documentation explaining how to restrict and/or update the use of the collected data The vendor must allow users to easily opt out of direct marketing based on their collected data.	X	
3.6.4	The vendor must make explicit the expected duration of the terms of service, the legal implications of substantially changing device usage and must ask permission from users before changing the terms of service or for upgrade firmware.	X	
3.6.5	The vendor should grant third party clients the same functional scope on the backend as its own clients and allows third parties to connect clients/devices to its backend (also direct communication with its devices, without going through the backend).		X

3.6.2 3.6.5 3.6.9	Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings. Note that an IoT device can be an autonomous vehicle including its embedded IoT gateways, sensors and actuators.	X	
3.6.5 3.6.7 3.6.9	IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services. Note that an IoT device can be an autonomous vehicle including its embedded IoT gateways, sensors and actuators.	X	
3.6.5 3.6.6 3.6.9	Commit to not sell or transfer any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained.	X	
3.6.5 3.6.6 3.6.8 3.6.9	Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to privacy.	X	

3.7 Autonomous vehicles IoT engagement framework

The autonomous vehicles and IoT Engagement Framework is a component of the overarching autonomous vehicles and IoT Policy Framework integrating several engagement mechanisms such as ethics, standards and guidelines, legislation and contractual arrangements.

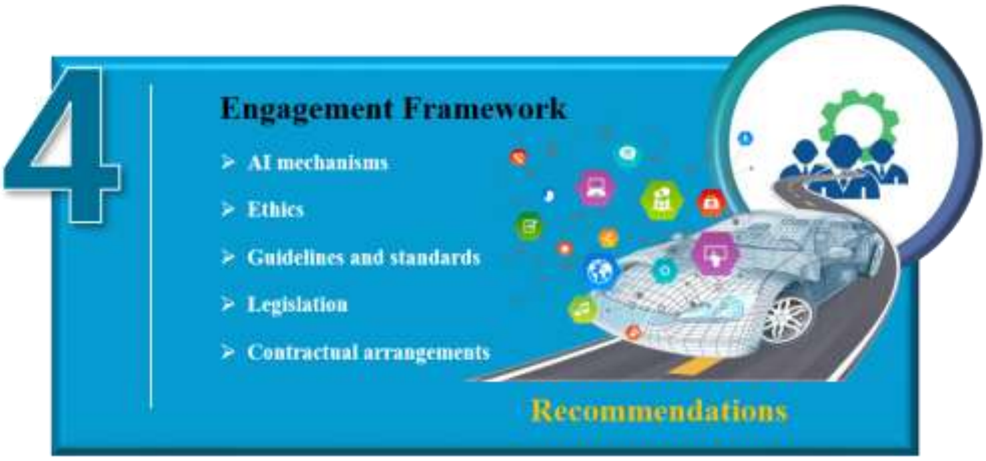


Figure 20: Autonomous vehicles IoT engagement framework

3.7.1 AI mechanisms and engagement

The AI mechanisms and engagement are closely linked to the other pillars; trust, security and privacy. In addition, it is closely linked to the user experience and the improved user experience compared to current situation.

The increased possibilities in data collection and communication technologies make the AI mechanisms able to detect objects in the road, manoeuvre through the traffic without human intervention and safely reach the destination [72]. The autonomous vehicles can also be equipped with voice and speech recognition, gesture controls, eye tracking and other driving monitoring systems, virtual assistance, mapping and safety systems etc. These AI-based functionalities have been created to give the users great user experience and keep them safely on the road. It is difficult, if not impossible, to make sure that the automotive vehicles stakeholders can reach SAE driving automation levels 4 and 5 without using AI mechanisms. The stakeholder's engagement requires understanding of AI methods like deep learning neural networks to optimize the processing of information as wells as anticipate users' needs and take ethical precautions.

3.7.2 Ethics

An important challenge that has been addressed from an ethical perspective, concerns the human complexity and "drivers" liability in case of road accidents [87]. It is for example crucial to establish how the automated vehicle system will decide on questions of life and death, (e.g. choosing between putting passengers or pedestrians at risk). Whether a human should be able to change the decision process of the vehicle on such ethical questions, and accident liability should be removed from "drivers" of conditionally automated vehicle who show typical and reasonable user behaviour is still controversial [87].

Autonomous vehicles, IoT and AI applications are supposed to operate safely and efficiently for all type of vehicles, in any conditions and any context. In operating a vehicle today, the laws place the responsibility on the driver to ensure that everyone’s well-being, both inside the vehicle and outside the vehicle, are protected and that harm does not come to oneself or others, or in case of extreme situations must be minimised as much as possible.

Autonomous vehicles, IoT and AI applications address the vehicle as a tool whose primary function is to get people from A to B safely and efficiently.

The autonomous vehicles, IoT and AI applications stakeholders and industry players are considering several scenarios for further developments, some considering that autonomous vehicles are basing the decisions only on what the sensors signals, some other advocate the use of information received from other vehicles (V2V communication), other group of players that propose that autonomous vehicles use information received from the infrastructure (V2I) or from the whole environment (V2E) and other considering a combination of information received from vehicles, infrastructure, IoT devices/platforms, pedestrians and devices (V2V, V2I, V2P, V2D, etc. communication). The latter implies reliance on connectivity networks (5G and IoT networks), LiDAR sensors, and other fixed and wireless infrastructure sources.

The amount of information that is processed by an autonomous vehicle in real-time is very large and stakeholder consider the use of IoT, AI and distributed ledger architectures to be used to build a real-time shared description of the state of the road infrastructure (including the presence of humans).

This could reduce the investment in multi-technology systems integrated into autonomous vehicle and within the surrounding "intelligent" infrastructure. In this context, autonomous vehicles are coordinated based on verifiable description of the current state of the road.

Autonomous vehicles, IoT and AI applications require ethically aligned design principles which define accountability that can support in proving why autonomous vehicles, IoT and AI systems operates in certain ways to address legal issues of culpability, and to avoid confusion or fear within the general public. Transparency is an important attribute for defining key principles of accountability, which include responsibility, explainability, accuracy, auditability and fairness.

If the autonomous vehicle could consider personally identifiable data when deciding how to solve a certain dilemma, and who to save in a case of an imminent accident. If the autonomous vehicle can only detect the age of the pedestrians involved, then it might decide to opt for a certain age group. If the autonomous vehicle could know more then it could choose based on the perceived contribution to social welfare of the individuals involved, and even information on their social status.

Eliminating algorithmic biases and reaching a balance between algorithmic efficiency and adequate protection of users' privacy are very important issues to be addressed by autonomous vehicles, IoT and AI applications as the right decision depends on the values expressed by the human communities, that are context dependent and which can differ significantly across the regions and across the globe.

The level of autonomy of autonomous vehicles, IoT and AI systems are today not advanced enough to really earn these systems the right to be treated as legal entities. From a legal perspective today autonomous vehicles, IoT and AI systems are linked to their developers. A different approach would be considered when complex autonomous vehicles, IoT and AI systems are treated as animals under civil law rules, which entails that any damage they cause would be attributable to their owners whenever negligence in custody can be proved.

In this context, a proper understanding of ethics must be addressed as ethical judgments are a multifaced subject that bring different factors or perspectives including the standard of judging or norm, the contextual situation and environment, the relationship and impact relative to a person, both internally and externally and the laws and regulations. An optimal ethical judgment needs to consider all of these various factors appropriately and correctly and properly implement them in the "cognitive" units of autonomous systems.

3.7.3 Guidelines and standards

The autonomous vehicles systems are emerging. Indeed, we can find more and more communication-related applications for connected cars. Therefore, is needed to standardize the way of communication, the security and the management [40]. ETSI's Technical Committee Intelligent Transport Systems (TC ITS) created several standards for these topics. For example, the Cross layer Decentralized Congestion Control (DCC) is providing resource management when there are many ITS messages. There is also standardization in the type of messages send between autonomous vehicles and other systems. Indeed, it is necessary to know the type of messages that the vehicles send or received in order to understand the information inside of them.

In the same way, there are more and more new IoT platforms and we want all the systems to be able to communicate with each other and to do this securely. For AV systems, we need to communicate with several smart objects around them. Therefore, ETSI oneM2M standard is used [41]. With this standard we want to enable the interoperability of the communication between all connected objects. Indeed, the oneM2M standard allow the communication Machine-to-Machine even if they don't use the same IoT platform.

ISA 99/IEC 62443 is focused on cyber security in industrial environments [55]. As reported in the 62443 series of standards - Industrial Automation and Control Systems Security [56], the 62443 series of standards have the goal to improve safety, availability, integrity and confidentiality of components or systems used for industrial automation and control.

Group 2 of the 62443 refers to Policies and Procedures: elements in this group focus on the policies and procedures associated with IACS security. Within this group the 62443-2-1 standard describes what is required to define and implement and effective IACS cyber security management system: the intended audience includes end users and asset owners who have responsibility for the design and implementation of such a program [56]. The 62443-2-4 standard specifies requirements for suppliers of IACS. Here the principal audience include suppliers of control systems solutions [56].

3.7.4 Legislation

The development of complex autonomous vehicles and IoT/IIoT systems that have embedded AI techniques and methods creates a new paradigm where the vehicles are connected to infrastructure (e.g. road networks, IoT platforms, infrastructure services, satellite networks, etc.) other vehicles on the road, in the air or water, the smart grid and retail opportunities, and become able to operate and cooperate with other autonomous vehicles. The vehicles have cognitive/intelligent functions that allow them to take autonomous decisions, are connected with other vehicles and IoT mobile and fix devices, which in turn change the entire business models for the automotive industry that becomes part of wider technological advances typified by developments such as electric vehicles, autonomous vehicles, IoT/IIoT, hyperconnectivity, AI and cyber-security.

This new paradigm requires addressing new legal issues that are facing the autonomous vehicles, IoT, connectivity and AI complex systems and applications. On the following sections, these issues are explored and presented as part of the broader engagement framework.

The issues identified are the following: New regulations emerging to regulate the testing and deployment of autonomous vehicles, IoT and AI systems; Lability issues in complex autonomous vehicles, IoT and AI applications; Data analytics, AI techniques and methods, services and monetisation business models; Cyber security and the threats to complex autonomous vehicles, IoT and AI applications and services; Complex autonomous vehicles, IoT and AI ecosystems - collaborations and partnerships between automotive and IT/OT technologies stakeholders; and Autonomous vehicles as part of Internet of Vehicles (IoV) become socially networked devices (e.g. in applications such as mobility as a service (MaaS), vehicle sharing, etc.).

New regulations emerging to regulate the testing and deployment of autonomous vehicles, IoT and AI systems:
The regulatory focus today is on enabling testing of autonomous vehicles and providing guidelines for
the development of autonomous vehicles. There is no clear pan European legislation for testing complex autonomous vehicles, IoT and AI applications and the stakeholders in such ecosystems are using different guidelines, that in long term could lead to a discordant development of intelligent transportation systems (ITS) in Europe.

In the U.S., several states have introduced legislation relating to autonomous vehicles. States such as California, Florida, Michigan and Nevada have passed laws to enable the testing and operation of driverless vehicles, to varying degrees. The U.S. federal government released its first rulebook governing the manufacture and sale of autonomous vehicles, setting out a 15-point “safety assessment”, including details on how a vehicle’s software will address ethical situations on the road.

In Europe the EC published in 2010 the ITS Directive (Directive 2010/40/EU) with the objectives to establish interoperable ITS services while leaving Members States the freedom to decide what systems to invest in. The EC intends to adopt functional, technical and organisational measures to address the Europe-wide adoption of ITS solutions. The European Union’s transport ministers agreed in 2016 to support several measures to harmonise traffic and transport rules to create a regulatory environment that would make the operation of autonomous vehicles a possibility across the EU by 2019 and work on a common communication system to enable vehicles to communicate with each other and with the required infrastructure.

The automotive industry is concerned that EU is not moving fast enough to introduce changes to vehicle safety tests and even laws regulating the high-speed internet connections, 5G, ITS-G5 that connected vehicles rely on to function.

The new work on EU legislation should be followed in parallel by the development of industry-wide standards based on EU and national guidelines, while companies developing complex autonomous vehicles, IoT and AI systems need to identify the gaps in the guidelines and to ensure standards are sufficiently flexible to adapt and change in sync with the changing technology.

These new regulations must be aligned with the GDPR and new elements such as "compliance by design" in relation to each autonomous, connected and intelligent product manufactured need to be addressed under these standards.

Lability issues in complex autonomous vehicles, IoT and AI applications:
The introduction of complex autonomous vehicles, IoT and AI systems adds a new layer of complexity to attributing liability for vehicle accidents. In this context, specific legislation should define how liability is apportioned when vehicles are sold as, and drivers/owners/users expect them to be, fully autonomous.

In these cases, attributing liability, fault and responsibility for insurance has to be clarified among the stakeholders involved in complex autonomous vehicles, IoT and AI applications.

Attributing liability in complex autonomous vehicles, IoT and AI applications is a difficult issue in order to establish the responsible stakeholder(s) for incidents (e.g. vehicle manufacturer, manufacturer of software, network providers, service providers, owners, users, etc.) caused by defects in the software interface between two vehicles or between a vehicle and the road, cyber-attacks on vehicles, defects in connectivity causing the incidents, etc.

Attributing fault to determine exactly what was the cause of an accident (subject to privacy implications), requires the implementation of event data recorders or insurance black boxes in vehicles to provide the necessary information of the conditions and the state of different autonomous vehicles, IoT, AI modules at the incident moment.

Responsibility for insurance needs to address the issue who should insure the autonomous vehicles, IoT, AI systems and how the ecosystem stakeholders contribute to the insurance (e.g. vehicle owners, users, vehicle manufactures, network providers, service providers, etc.). These are important elements that need to clarify especially if the incidents in autonomous vehicles, IoT and AI systems fall under the product liability regulations preventing any limitation on the bringing of claims against the manufacturer, or if a network provider is liable, telecoms liability limitations apply, or what will be the case when the service provider is liable.

Data analytics, AI techniques and methods, services and monetisation business models:
The ability to generate, share and access data has increased due to the number of people, vehicles, IoT devices and sensors that are connected by networks. The information collected can be used for analytics purposes to create value by acquiring more accurate and detailed vehicle performance data,

that enable development of more efficient, safer or more advanced autonomous vehicles, create new in-vehicle technology (e.g. traffic routing, autonomous parking), better services (e.g. maintenance services) to meet customer needs and in-vehicle monetisation opportunities (e.g. advertising of services on route/at destination).

New business models that include MaaS and the involvement of different stakeholders in the process of collecting, processing and sharing data, information and knowledge generated by autonomous vehicles, IoT, AI systems need to be considered.

In this context, costumer awareness of how their data is used and to ensure stakeholders are carried along with the collection and use of their data, combined with the data minimisation that considers that data processing should be kept to a minimum and that data should not be held for longer than necessary is a key element. In addition, storing and processing of data and good data governance (e.g. data relating to an individual's autonomous vehicle in terms of speed, performance and location could be used for public benefit if a connected vehicle system is to operate as a whole) need to be properly defined.

Cyber security and the threats to complex autonomous vehicles, IoT and AI applications and services:
Autonomous vehicles, IoT, AI systems and applications will be subject to possible cyber threats through different channels depending on the stakeholders that are providing the services such as autonomous vehicles, IoT, AI technology manufacturers, infrastructure providers, road and other authorities and users. The connection of the vehicle to the internet, the electronic IoT devices within vehicles, opens the potential for the vehicle itself, as part of the "Internet of Vehicles", to be the target of cyber-attacks. Autonomous vehicles, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), transmit personal data about vehicle users, such as location data, which may be of interest to cyber-attackers. Network connected devices are vulnerable to attack through any of the IoT or other devices in the network as each device in a network is a potential entry point for cyber attackers.

The cyber security breaches can be caused as well by careless use of security procedures, lack of awareness of, or failure to follow, policies designed to protect data either by the personnel of the service providers or of the third-party providers used for outsourcing of services and infrastructure.

Complex autonomous vehicles, IoT and AI ecosystems - collaborations and partnerships between automotive and IT/OT technologies stakeholders:
Autonomous vehicles, IoT and AI ecosystems are becoming increasingly complex and requires cross-industry alliances and collaborations between autonomous vehicles manufacturers/original equipment manufacturers (OEMs), telecoms providers/mobile network operators (MNOs), IoT platforms providers and technology companies. These alliances between industries with traditionally different operating methods and business models requires a convergence of differing approaches in order to create coherent products, services and experiences involving autonomous vehicles, IoT and AI technologies. These complex ecosystems require addressing the issues of third-party liability, compliance with applicable laws and regulations, joint control of personal data, ownership of data, jointly/individually developed intellectual property and collaboration/competition mechanisms.

Autonomous vehicles as part of Internet of Vehicles (IoV) become socially networked devices:
Autonomous vehicles as part of Internet of Vehicles (IoV) incorporate several social media apps integrated with the vehicle users' mobile devices and IoT devices with the vehicle's digital systems, allowing the use of the dashboard monitor as an interface for car users to operate the mobile devices. The integration of autonomous vehicles functions, IoT and AI with full connectivity to the Internet allows the user of these systems to get real-time alerts for severe weather or emergency braking and road authorities being able to change traffic lights and speed limits in real-time to address the weather conditions.

3.7.5 Contractual arrangements

As the IoT expands more widely across the consumer sector it becomes more important to be sure that firstly information about devices is maintained in a way to better protect users and secondly that there is a more consistent approach in the methods for storing and retrieving identity information.

A distributed ledger technology (DLT) addresses these concerns by providing a common and highly robust approach for device identity which uses the security of strong cryptographic techniques to secure the data on the ledger, coupled with the distribution of the ledger across multiple nodes to secure against scale attacks including Distributed Denial of Service (DDoS) attacks [62].

There are many situations in the real world where it is important to know that a process, particularly where it involves multiple parties, is being properly complied with. Compliance is efficiently enabled using distributed ledgers particularly using smart contracts.

Smart contracts and distributed ledger technology (DLT) are increasingly used as a way for the derivatives industry to realise operational efficiencies and cut costs. With these new technologies potentially transforming how derivatives are executed and managed through the entire lifecycle, it seems the derivatives market is on the cusp of significant modernisation.

The concept of the smart contract is of a software function that is itself 'stored' in the ledger and is executed when there is a request to store a transaction. The smart contract can check for required pre-conditions being met. Smart contracts are generally executed by the nodes which maintain the distributed ledger network. This means there is extremely high reliability provided for applications through high redundancy against systems outages. Also, the scalability and robustness increase as the distributed ledger network expands the number of nodes supporting the ledger.

The paramount technical challenge facing DLT, and IoT convergence is the ability to scale to meet service and security requirements across a dynamic network of devices. These requirements aren't just precautions; they are foundational to running IoT in mission-critical, high-risk and high (data) volume (sometimes low-bandwidth) environments, such as healthcare, energy, transportation and beyond. This is rapidly pushing IoT data processing, management and analytics to the "edge," where compute occurs locally, instead of relying on cloud connectivity [63].

3.7.6 Requirements and recommendations

Table 18 provides a list of engagement related requirements and recommendations applicable to IoT enabled autonomous driving environments. Note that some of the points are based on requirements and recommendations given by OTA [85].

Table 18: Engagement - Requirements (Req) and Recommendations (Rec)

No.	Engagement framework	Req.	Rec.
3.7.1	Include and communicate AI-based functionalities and applications that noticeable contributes to improve the users experience (compared with the current situation) to achieve engagement.		X
3.7.2	Highlight all known ethical issues regarding the use of autonomous vehicles and driving through, and disclosure it in an accurate and understandable way.	X	
3.7.3 3.7.4 3.7.5	In order to maximize user awareness; develop good communication processes for information about both neutral, positive and negative nature. Multilingual communication should be considered and written/ pronounced in a way to maximize comprehension for the targeted recipients.	X	
3.7.5	A physical asset e.g. a smart lock is able to use a distributed ledger both to hold details of the people (or rather their keys) and times that the lock can be operated as well as to store a record of attempts and activations.		X
3.7.5	A virtual asset e.g. a server sharing a data file can similarly use a distributed ledger to hold the identity of the persons or applications that can access the file, as well as other constraints e.g. the time period they are allowed to access it, and whether they are allowed to save, print, edit or forward that file.	X	

3.7.4 3.7.5	A connected car automatically uploading journey information, faults and service data to a distributed ledger holding vehicle information so that future purchasers are protected against odometer fraud leading to over-valuation of the used vehicle and manufacturers and vehicle licensing agencies can monitor and address the occurrences of common faults.		X
3.7.4 3.7.5	Process for manufacturers to be granted permission to write their information to the ledger and it is thought there could be an opportunity for mobile operators to provide such a distributed ledger to support the IoT across the globe, administering the permissions of verified device manufacturers to write to the ledger.	X	
3.7.3	Use standards when they exist in order to improve the interoperability of the autonomous vehicles system, to have communications understandable by all systems and to improve the security of the systems.		X
3.7.3	Standards are evolving, we should use the latest standards' versions in order to keep the highest level of security for he users.		X
3.7.4	Verify that you are following all the regulations that could be applied on your autonomous vehicles systems.	X	
3.7.2 3.7.4	Consider how to accommodate accessibility requirements for disabled persons to maximize access for users of all physical capabilities.	X	

4. Conclusions

This document presents an IoT policy framework for autonomous vehicles applications focusing on the important aspects of the four pillars trust, security, privacy and engagement, together with requirements and recommendations. The document gives an overview of legislation in the field of autonomous vehicles at international, European and specific country level.

The autonomous vehicle and IoT applications cover several domains of interaction, communication, exchange of information. The domains of interaction include several communication interfaces like vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-device (V2D), vehicle-to-pedestrian (V2P), vehicle-to-maintenance (V2M), vehicle-to-grid (V2G), and vehicle-to-owner (V2O). As an example, V2I could be dived further into vehicle-to-network (V2N) and vehicle-to-cloud (V2C). All these domains of interaction are summarised as V2X (vehicle-to-everything).

The autonomous vehicles IoT Trust Framework provides a set of principles and the underlying structure that substantiate trust and trustworthiness for autonomous vehicles and IoT solutions into a holistic manner. The framework integrates the concepts of dependability, sustainability, availability, reliability, resilience, privacy, security and safety best practices.

The autonomous vehicles IoT Security Framework is based on elements such as security mechanisms, identification, authentication, authorisation, availability, confidentiality, integrity, network prescribed policy, security by default and design, and best practices. These elements must be applied throughout the lifecycle processes of autonomous vehicles and IoT systems, which includes impact assessment when risks are assessed and design of controls when risks are mitigated.

Regarding privacy, the EUs General Data Protection Regulation (GDPR) is fundamental, and the autonomous vehicles IoT Privacy Framework is based on a human-centred concept including elements as privacy regulations, data minimisation, data portability, transparency, compliance disclosures, privacy by default and design, and best practices.

Engagement is an important pillar to move on in the development, integration and use of autonomous vehicles. The autonomous vehicles IoT Engagement Framework is integrating several engagement mechanisms related to ethics, standards and guidelines, legislation and contractual arrangements.

An increased level of automated driving will increase the vehicle requirements to react automatically on environmental conditions in real-time. The development of autonomous vehicles and IoT applications will accelerate the combination of emergent technologies for information processing and distributed security. Artificial intelligence (AI), together with distributed ledger technologies (DLTs) and blockchains, and edge computing and 5G connectivity brings new possibilities, but also challenges in addressing distributed IoT architectures and distributed security, privacy, trust and engagement mechanisms that form the foundation of a dynamic autonomous vehicles and IoT policy framework.

5. References

[1] *Self-driving vehicles enacted legislation.* National Conference of State Legislatures (NCSL), March 2018, online at: http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx

[2] *Autonomous vehicles state bill tracking database*. National Conference of State Legislatures (NCSL), April 2018, online at: http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx

[3] *Automated Driving Systems 2.0 - A Vision for Safety*. U.S. Department of Transportation and National Highway Traffic Safety Administration. DOT HS 812 442, September 2017, online at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[4] *International Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. SAE INTERNATIONAL, J3016, September 2016.

[5] *Federal Automated Vehicles Policy - Accelerating the Next Revolution in Roadway Safety*. Department of Transportation and National Highway Traffic Safety Administration, September 2016, online at: https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf

[6] Fact sheet: Federal Automated Vehicles Policy - Accelerating the Next Revolution in Roadway Safety, 2016, online at: https://www.transportation.gov/sites/dot.gov/files/docs/DOT_AV_Policy.pdf

[7] Economic Commission for Europe, Inland Transport Committee. Convention on Road Traffic. E/CONF.56/16/Rev.1/Amend.1. Art. 8. November 1968, online at: http://www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf

[8] UNECE. *UNECE paves the way for automated driving by updating UN international convention*. March 2016, online at: http://www.unece.org/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/doc.html

[9] Legifrance.gouv.fr. *Ordonnance n° 2016-1057 du 3 août 2016 relative à l'expérimentation de véhicules à délégation de conduite sur les voies publiques*. April 2018, online at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032966695&dateTexte=20180430

[10] Tweede Kamer der Staten-General. Vergaderjaar 2017-2018. 34 838. nr. 2., online at (Dutch): https://www.eerstekamer.nl/behandeling/20171122/voorstel_van_wet/document3/f=/vkjkqandf1zk.pdf

[11] New legislation allows for the testing of cars with remote drivers. Government of the Netherlands, 24-11-2017, online at: https://www.government.nl/latest/news/2017/11/22/new-legislation-allows-for-the-testing-of-cars-with-remote-drivers

[12] Self-driving vehicles. Government of the Netherlands. Online at: https://www.government.nl/topics/mobility-public-transport-and-road-safety/self-driving-vehicles

[13] Transfer to 2040 - Flexible and smart public transport. Ministry of Infrastructure and Water

Management, January 2018. Online at: https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/documents/leaflets/2018/02/13/transfer-to-2040---flexible-and-smart-public-transport

[14] On our way towards connected and automated driving in Europe, Outcome of the first High Level Meeting (Amsterdam, 15 February 2017). Ministry of Infrastructure and the Environment, 18 May 2017, online at: https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/documents/leaflets/2017/05/18/on-our-way-towards-connected-and-automated-driving-in-europe

[15] Speech minister Schultz at the first EU Conference on connected and automated driving. Government of the Netherlands, April 2017, online at: https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/documents/speeches/2017/04/05/speech-minister-schultz-at-the-first-eu-conference-on-connected-and-automated-driving

[16] Word of welcome by Melanie Schultz van Haegen, Minister of Infrastructure and the Environment, at the High-Level Meeting on the Amsterdam Declaration. Government of the Netherlands, February 2017, online at: https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/documents/speeches/2017/02/15/word-of-welcome-by-melanie-schultz-van-haegen-minister-of-infrastructure-and-the-environment-at-the-high-level-meeting-on-the-amsterdam-declaration

[17] A fresh perspective on mobility and logistics - European Truck Platooning Challenge 2016. Ministry of Infrastructure and the Environment, ACEA (European Automobile manufactures Association), Conference of European Directors of Roads, and RDW (The Netherlands Vehicle Authority in mobility chain), October 2015, online at: https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/documents/leaflets/2015/10/06/leaflet-european-truck-platooning-challenge-2016

[18] Speech by the Minister of Infrastructure and the Environment, Melanie Schultz van Haegen, at the demonstration of connected driving with trucks in Zwolle. Government of the Netherlands. Online at: https://www.government.nl/ministries/ministry-of-infrastructure-and-water-management/documents/speeches/2015/02/09/speech-by-the-minister-of-infrastructure-and-the-environment-melanie-schultz-van-haegen-at-the-demonstration-of-connected-drivi

[19] Wet- en regelgeving; Wegenverkeerswat 1994; Hoofdstuk 1. Algemene bepalingen. De wegwijzer naar informatie en diensten van alle overheden, online at (Dutch): http://wetten.overheid.nl/BWBR0006622/2016-03-15

[20] Connected and autonomous vehicles: A UK standards strategy. Summary report. Available from: https://www.bsigroup.com/en-GB/Innovation/cav/ (accessed 18/10/18), BSI and the Transport Systems Catapult.

[21] The Pathway to Driverless Cars: A detailed review of regulations for automated vehicle technologies. London, UK, Department for Transport.

[22] The Key Principles of Cyber Security for Connected and Automated Vehicles. Available from: file:///D:/Autopilot/T5.4/cyber-security-connected-automated-vehicles-key-principles.pdf (Accessed 23/10/18), Her Majesty's Government.

[23] Automated and Electric Vehicles Act 2018. Chapter 18. H. M. Government. Norwich, UK, The Stationary Office.

[24] Connected and Autonomous Vehicles: Position Paper. London: Available from https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf , Society of Motor Manufacturers and Traders.

[25] Centre for Connected and Autonomous Vehicles, UK, online at: https://www.gov.uk/government/organisations/centre-for-connected-and-autonomous-vehicles

[26] https://www.gov.uk/government/news/government-to-review-driving-laws-in-preparation-for-self-driving-vehicles , accessed 18/10/18

[27] https://www.theregister.co.uk/2018/04/04/ukgov_driverless_car_regulation/, accessed 18/10/18

[28] http://www.nortonrosefulbright.com/knowledge/publications/154715/autonomous-vehicles-the-legal-landscape-of-dsrc-in-the-united-kingdom , accessed 18/10/18

[29] https://www.gov.uk/guidance/the-highway-code , accessed 23/10/18

[30] https://www.gov.uk/government/news/new-laws-pave-way-for-remote-control-parking-in-the-uk , accessed 18/10/18

[31] Autonomous Vehicle Readiness Index: Assessing countries' openness and preparedness for autonomous vehicles, KPMG, 2018, online at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/01/avri.pdf, accessed 18/10/18, KPMG.

[32] Self-Driving Vehicles in Singapore, Land Transport Authority.

[33] https://www.mot.gov.sg/news-centre/news/Detail/Committee-on-Autonomous-Road-Transport-for-Singapore , accessed 18/10/18

[34] https://www.cio-asia.com/article/3285729/emerging-technology/singapore-pioneers-development-of-autonomous-vehicle-technology.html , accessed 18/10/18

[35] Hansen, M., Jensen, M. and Rost, M., Protection goals for privacy engineering. International workshop on privacy engineering, May 2015, online at: http://www.ieee-security.org/TC/SPW2015/IWPE/2.pdf

[36] Autonomous driving needs transparent criteria. AutomotiveIT International, March 2018, online at: http://www.automotiveit.com/news/autonomous-driving-needs-transparent-criteria/

[37] *General Data Protection Regulation (GDPR).* Online at: https://gdpr-info.eu/

[38] Data portability under the GDPR: the right to data portability explained. i-SCOOP, online at: https://www.i-scoop.eu/gdpr/right-to-data-portability/

[39] UK, Department for Digital, Culture, Media and Sport. Online at: https://www.gov.uk/

[40] Several ETSI’s standards for Automotive Intelligent Transport Systems, online at: https://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport

[41] The ETSI’s standard for Machine-to-Machine communications for Internet of Things, online at: https://www.etsi.org/technologies-clusters/technologies/internet-of-things

[42] Public road automated vehicle testing in Finland, 16/12/2016, https://connectedautomateddriving.eu/wp-content/uploads/2017/02/FI-Presentation-Workshop-16.12.2016.pdf, accessed 9/11/18

[43] *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. ENISA, November 2017

[44] *Privacy and Data Protection by Design* (from policy to engineering). ENISA, December 2014

[45] *Indispensable baseline security requirements for the procurement of secure ICT products and services*, v.1.0 (Public). ENISA, December 2016

[46] *OWASP Secure Coding Practices, Quick Reference Guide,* v.2.0. The OWASP Foundation November 2010, online at: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[47] *Trusted devices drive the value chain: securing IoT devices during manufacturing,* (White paper). HARMAN Connected Services, August 2017

[48] *OWASP Consumer Top Ten Safe Web Habits. Online at: https://www.owasp.org/images/9/9e/OWASP_Consumer_Top_Ten_Safe_Web_Habits.pdf*

[49] Category: Access Control. OWASP, June 2016. Online at: https://www.owasp.org/index.php/Category:Access_Control

[50] Communication network dependencies for ICS/SCADA Systems. EINSA, December 2016

[51] *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls*. Second edition, 2013-10-01

[52] *Risks and benefits of emerging life-logging applications*. Final Report, EINSA

[53] *Security by Design Principles*. OWASP, August 2016. Online at: https://www.owasp.org/index.php/Security_by_Design_Principles

[54] *Cyber Security and Resilience of smart cars*. ENISA, December 2016

[55] *Certification of Cyber Security skills of ICS/SCADA professionals*. EINSA, December 2014

[56] The 62443 series of standards: Industrial Automation and Control Systems Security. Revised December 2016

[57] Autotalks Ltd. *DSRC vs. C-V2X for Safety Applications*. Online at: https://www.auto-talks.com/technology/dsrc-vs-c-v2x-2/

[58] CNIL Publications: https://www.cnil.fr/en/media

[59] ACT, Data Protection. Conducting privacy impact assessments code of practice. 2014.

[60] https://iotmark.wordpress.com/

[61] Ontario. Office of the Information and Privacy Commissioner, Cavoukian, A., & Green, S. (2012). *Privacy by Design and the Emerging Personal Data Ecosystem. October 2012*.

[62] https://www.gsma.com/iot/opportunities-distributed-ledger-in-iot/

[63] https://www.openidentityexchange.org/accord-project-id-the-smart-legal-contract-identity-and-trust-framework-standard/

[64] Vermesan, O., et.al., "The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge", chapter 3 in Vermesan, O., Bacquet, J. Eds. "*Next Generation Internet of Things - Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*". ISBN: 978-87-7022-008-8 (Hardback), 978-87-7022-007-1 (Ebook). River Publishers 2018.

[65] D. Leight, "The 23 ASILOMAR principles and why they matter, according to Stephen Hawkins and Elon Musk", 10 October, 2018 online at: https://iheartintelligence.com/asilomar-principles-stephen-hawking-elon-musk/

[66] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management" (V1.2.1; 2018-05)

[67] 3GPP TS 23.285: "Architecture enhancements for V2X services" (V14.4.0; 2017-9)

[68] 3GPP TS 33.185: "Security aspect for LTE support of V2X services" (V2.0.0; 2017-)

[69] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[70] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)". (V14.2.0; 2017-09)

[71] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)"

[72] Gadam, S. *Artificial Intelligence and Autonomous Vehicles*. Data Driven Investors (DDI). Online at: https://medium.com/datadriveninvestor/artificial-intelligence-and-autonomous-vehicles-ae877feb6cd2

[73] Vermesan, O., et.al., "Internet of Things Cognitive Transformation Technology Research Trends and Applications", chapter 3 in Vermesan o., Bacquet, J. Eds. "*Cognitive*

Hyperconnected Digital Transformation - Internet of Things Intelligence Evolution". ISBN: 978-87-93609-11-2 (Hardback), 978-87-93609-10-5 (Ebook). River Publishers 2017.

[74] 3GPP TS 22.261 v16.5.0 (2018-09). *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the 5G system; Stage 1 (Release 16)*. 5G and 3GPP September 2018. Online at: http://www.3gpp.org/ftp/specs/archive/22_series/22.261/22261-g50.zip

[75] *NGMN 5G White paper*, (v1.0). NGMN Alliance, February 2015. Online at: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[76] *Recommendations for NGMN KPIs and Requirements for 5G*, NGMN Alliance, June 2016. Online at: https://www.ngmn.org/fileadmin/user_upload/160603_Annex_-_NGMN_Liaison_to_3GPP_RAN__72_v1_0.pdf

[77] ETSI TS 102 637-1 v1.1.1 (2010-09). *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements*. Online at: https://www.etsi.org/

[78] ETSI TC ITS, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, Std. ETSI TR 102 638 V1.1.2, 2015.

[79] 3GPP TR 22.886 V1.0.0: Study on enhancement of 3GPP support for 5G V2X services (Release 15), 3GPP Std., November 2016

[80] NGMN Alliance, "NGMN perspectives on vertical industries and implications for 5g," 2015. Available online: https://www.ngmn.org/uploads/media/160610 NGMN Perspectives on Vertical Industries and Implications for 5G v1 0.pdf

[81] Festag A., "Cooperative intelligent transport systems standards in Europe," IEEE communications magazine, vol. 52, no. 12, pp. 166–172, 2014.

[82] 3GPP TR 22.186 V15.0.0: Service requirements for enhanced V2X scenarios (Release 15), 3GPP Std., March 2017.

[83] The Connected Automated Driving (CAD) Initiative. Online at: https://connectedautomateddriving.eu/

[84] Position paper on Policy and regulatory needs, European harmonisation. CARTRE, October 2018. Online at: https://connectedautomateddriving.eu/wp-content/uploads/2018/10/181016_Position-Paper_Policy_Regulatory_Harmonization.pdf

[85] The Online Trust Alliance (OTA). Internet of Things. Online at: https://otalliance.org/IoT

[86] United Nations Economic Commission for Europe (UNECE), Global Forum for Road traffic Safety (WP.1). Online at: https://www.unece.org/trans/main/welcwp1.html

[87] Position paper on Users and societal acceptance and awareness. CARTRE, April 2018, online at: https://connectedautomateddriving.eu/wp-content/uploads/2018/04/CARTRE_users-and-societal-acceptance-and-awareness_Position_Paper-1.pdf

[88] United Nations Economic Commission for Europe (UNECE), Road Traffic Safety, online at: http://www.unece.org/trans/theme_road_safety.html

[89] United Nations Economic Commission for Europe (UNECE), World Forum for the harmonization of vehicle regulations (WP.29), online at: http://www.unece.org/trans/main/wp29/presentation_wp29.html

[90] United Nations Economic Commission for Europe (UNECE). *UNECE adopts resolution on the deployment of highly and fully automated vehicles in road traffic*. Press release October 2018. Online at: http://www.unece.org/info/media/presscurrent-press-h/transport/2018/unece-adopts-resolution-on-the-deployment-of-highly-and-fully-automated-vehicles-in-road-traffic/doc.html

[91] United Nations Economic Commission for Europe (UNECE). Conversion of GRRF into GRVA. Note August 2018, online at: http://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/Conversion_of_GRRF_into_GRVA.pdf

[92] United Nations Economic Commission for Europe (UNECE). *What is the difference between EU Directives, UN Regulations and UN Global Technical Regulations (UN GTRs)?,* online at: http://www.unece.org/trans/main/wp29/faq.html

[93] Law Commission - Reforming the law. Automated Vehicles, Current project status, (accessed 03.12.2018). Online at: https://www.lawcom.gov.uk/project/automated-vehicles/

[94] Intelligent Transport. China issues national standards for the testing of autonomous vehicles, August 2018, (accessed on 30.11.2018). Online at: https://www.intelligenttransport.com/transport-news/70487/autonomous-technology-regulations-china/

[95] China Law Insight. China Issues Self-Driving Car Road Testing Regulations. King & Wood Mallesons, April 2018, (accessed on 30.11.2018)., online at: https://www.chinalawinsight.com/2018/04/articles/uncategorized/china-issues-self-driving-car-road-testing-regulations/

[96] Herbert Smith Freehills. Connected and Autonomous vehicles: Is China ready? Legal Briefings, May 2018, (accessed on 29.11.2018). Online at: https://www.herbertsmithfreehills.com/latest-thinking/connected-and-autonomous-vehicles-is-china-ready

[97] Synced - AI Technology & Industry Review. Global survey of autonomous vehicle regulations, March 2018, (accessed on 29.11.2018 and 30.11.2018), online at: https://syncedreview.com/2018/03/15/global-survey-of-autonomous-vehicle-regulations/

[98] MOLIT: A new age of hope brings about changes to create a happy life. Sejong-city, Ministry of Land, Infrastructure and Transport 2016.

[99] Kim, Y. S. Autonomous Vehicle Policy of South Korea. Conference of the International Research Council on Biomechanics of Injury, Seoul, South Korea, June 2016.

[100] Loughran, J. 5G network deployed in South Korea's driverless car test city. E&T January 2018, (accessed 29.11.2018). Online at: https://eandt.theiet.org/content/articles/2018/01/5g-network-deployed-in-south-korea-s-driverless-car-test-city/

[101] Min-Hee, J. K-City: World's Largest Test Bed for Self-driving Cars to Bee Opened in Korea. Business Korea, May 2017, (accessed 30.11.2018), online at: http://www.businesskorea.co.kr/news/articleView.html?idxno=18018

[102] Osborne, C. South Korea to map major cities for safe autonomous driving. ZDNet, March 2018, (accessed 29.11.2018). Online at: https://www.zdnet.com/article/south-korea-to-map-major-cities-for-safe-autonomous-driving/

[103] Amir, J. South Korean government promotes autonomous vehicles. HIS Markit, June 2018, (accessed 30.11.2018), online at: https://ihsmarkit.com/research-analysis/south-korean-government-promotes-autonomous-vehicles.html

[104] Motor Vehicle Management Act. Statute of the Republic of Korea. Act No. 13486, August 11 2015. Available (in English) from elaw.lri.re.kr, (accessed 03.12.18).

[105] German road traffic law – Straßenverkehrsgesetz – StVG online at: https://www.gesetze-im-internet.de/stvg/BJNR004370909.html#BJNR004370909BJNG000101308

[106] German decree of the amendment of road traffic law for autonomous driving June 20 2017, online at: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl103s0919a.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1648.pdf%27%5D__1544382293034

[107] Report of the German ethic commission "Automated and connected driving" June 2017, online at: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission-automated-and-connected-driving.pdf?__blob=publicationFile

[108] Hamida E. B. et.al. *Security of Cooperative Intelligent Transport Systems: Standards, Treats Analysis and Cryptographic Countermeasures, Electronics July 2015* (volume 4, Issue 3), online at: https://www.mdpi.com/2079-9292/4/3/380/html

[109] European Commission, Mobility and Transport, About TEN-T, online at: https://ec.europa.eu/transport/themes/infrastructure/about-ten-t_en

[110] Lauridsen, M., Gimenez, L.C., Rodriguez, I., Sorensen, T.B. and Mogensen, P., From LTE to 5G for connected mobility. *IEEE Communications Magazine,* **55**(3): 156–162, 2017, doi:10.1109/MCOM.2017.1600778CM.

[111] Molina-Masegosa, R., and Gozalvez, J., LTE-V for sidelink 5G V2V vehicular communications: A new 5G technology for short-range vehicle-to-everything communications. *IEEE Vehicular Technology Magazine* **12**(4): 30–39, 2017, doi: 10.1109/MVT.2017.2752798.

[112] Strom, E.G., On Medium Access and Physical Layer Standards for Cooperative Intelligent Transport Systems in Europe. *Proceedings of the IEEE* **99**(7): 1183–1188, 2011, doi:10. 1109/JPROC.2011.2136310.

[113] Lee, K., Kim, J., Park, Y., Wang, H., and Hong, D., Latency of Cellular-Based V2X: Perspectives on TTI- Proportional Latency and TTI-Independent Latency. *IEEE Access* **5**: 15800–15809. 2017.

[114] Ghosh, A., Thomas, T.A., Cudak, M.C., Ratasuk, R., Moorut, P., Vook, F.W., Rappaport, T.S., *et al.* (2014) Millimeter-Wave Enhanced Local Area Systems: A High- Data-Rate Approach for Future Wireless Networks. *IEEE Journal on Selected Areas in Communications* **32**(6): 1152– 1163, 2014, doi:10.1109/JSAC.2014.2328111.

[115] Communication Networks for Connected Cars, HUAWEI, Whitepaper, 2016, online at: https://www-file.huawei.com/-/media/corporate/pdf/x-lab/09-communications-networks-for-connected-cars.pdf?la=en&source=corp_comm

[116] Intelligent Connectivity, GSMA Report, 2018, online at: https://www.gsma.com/IC/wp-content/uploads/2018/09/21494-MWC-Americas-report.pdf

[117] CLEPA position on “short range” V2V, V2P and V2I within C-ITS communication technologies (5.9 GHz frequency band), October 2018, online at: https://clepa.eu/wp-content/uploads/2018/11/2018-12-CLEPA-position-5.9GHz-20180926-FINAL.pdf

[118] Grzywaczewski, A., Training AI for Self-Driving Vehicles: The Challenge of Scale, Technical report, NVIDIA Corporation, 2017, online at: https: //devblogs.nvidia.com/parallelforall/training-self-driving-vehicles-challenge-scale/

[119] Mavromatis, I., Tassi, A., Rigazzi, G., Piechocki, R.J., Nix, A., Multi-Radio 5G Architecture for Connected and Autonomous Vehicles: Application and Design Insights, Research Article, University of Bristol, Bristol, UK, 2018

[120] Griswold, A., Waymo is readying a ride-hailing service that could directly compete with Uber, February 2018, online at: https://qz.com/1208897/alphabets-waymo-googl-is-readying-a-ride-hailing-service-in-arizona-that-could-directly-compete-with-uber/

[121] Tesei, A., Di Mauro, L., Falcitelli, M., Noto, S., Pagano, P., IOTA-VPKI: a DLT-based and Resource Efficient Vehicular Public Key Infrastructure. 1st International Workshop on Dependable Wireless Communications (DEWCOM) in IEEE 88th Vehicular Technology Conference (VTC2018-Fall), Chicago, USA, 27-30 August 2018.

[122] 5GAA. Position paper. Coexistence of C-V2X and ITS-G5 at 5.9GHz. Online at: http://5gaa.org/wp-content/uploads/2018/10/Position-Paper-ITG5.pdf

[123] Wikipedia. Vienna Convention on Road Traffic. Online at: https://en.wikipedia.org/wiki/Vienna_Convention_on_Road_Traffic

[124] Upcoming Delegated Act on "Cooperative Intelligent Transport Systems" (C-ITS). BitKom, Position paper, August 2018.

[125] C-ITS platform Phase II - Cooperative Intelligent transport Systems towards Cooperative, connected and Automated Mobility, (Final report Phase II). Chaired by the EC, September 2017, online at: https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf

[126] Results of C-ITS Platform Phase II - Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1. Chaired by EC, June 2018, online at: https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf

[127] Results of C-ITS Platform Phase II - Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). Release 1, December 2017, online on: https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf

[128] ETSI TS 103 301 V1.1.1 (2016-11): Technical Specification - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services, online at: https://www.etsi.org/deliver/etsi_ts/103300_103399/103301/01.01.01_60/ts_103301v010101p.pdf

[129] Handbook to the IoT Large-Scale Pilots Programme. Online at: https://wiki.european-iot-pilots.eu/index.php?title=HANDBOOK_TO_THE_IOT_LARGE-SCALE_PILOTS_PROGRAMME

[130] Wikipedia Foundation Inc., online at: https://en.wikipedia.org/wiki/Main_Page

[131] RS Components - Design Spark. 11 Internet of Things (IoT) Protocols You Need to Know About, online at: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

[132] Hoffman, C., Wi-Fi 6: What's Different, and Why it Matters, October 8, 2018, online at: https://www.howtogeek.com/368332/wi-fi-6-what%E2%80%99s-different-and-why-it-matters/

[133] Satellite Technologies for IoT Applications. March 2017, IoTUK

[134] Briodagh. K., Globalstar Launches Automotive Team to Connectivity to Autonomous Vehicles, March 14, 2018.

[135] Lee, L-N., Advances in Satellite Communications Technology Suitable for IoT, presentation at IEEE Radio & Wireless Week (RWW2018), 2018, online at: http://sites.ieee.org/rww-2018/files/2018/01/Lin-Nan-Lee-RWW2018-presentation.pdf

[136] Barker P. and Hammoudeh, M., "A survey on low power network protocols for the internet of things and wireless sensor networks," in Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS '17), pp. 44:1–44:8, NewYork, NY, USA, July 2017.

[137] Sheng, Z. G., Yang, S. S., Yu, Y. F., Vasilakos, A. V., McCann, J. A., and Leung, K. K., "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," IEEE Wireless Communications Magazine, vol. 20, no. 6, pp. 91-98, 2013.

[138] Raza, U., Kulkarni, P., and Sooriyabandara, M., "Low power wide area networks: an overview," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855–873, 2017.

[139] Flore, D., "3GPP standards for the internet-of-things," February 2016, gSMA MIoT, online at: http://www.3gpp.org/news-events/3gpp-news/1766-iot%20progress

[140] Wang, Y.-P. E., Lin, X., Adhikary, A., Grovlen, A., Sui, Y., Blankenship, Y., Bergman, J., and Razaghi, H. S., "A primer on 3GPP narrowband Internet of Things (NB-IoT)," arXiv preprint arXiv:1606.04171, 2016.

[141] Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., and Watteyne, T., "Understanding the Limits of LoRa-WAN," IEEE Communications Magazine, vol. 55, no. 9, pp. 34–40, 2017.

[142] Hassan, S. M., Ibrahim, R., Bingi, K., Chung, T. D., and Saad, N., "Application of wireless technology for control: A WirelessHart perspective," Procedia Computer Science, vol. 105, no. supplement C, pp. 240–247, 2017, http://www.sciencedirect.com/science/article/pii/S1877050917302405.

[143] Ploennigs, J., Ryssel, U., and Kabitzsch, K., "Performance analysis of the EnOcean Wireless sensor network protocol," in Proceedings of the 15th IEEE International Conference on

Emerging Technologies and Factory Automation (ETFA ’10), pp. 1–9, September 2010.

[144] Osiegbu, C., Amsalu, S. B., Afghah, F., Limbrick, D., and Homaifar, A., “Design and implementation of an autonomous wireless sensor-based smart home,” in Proceedings of the 24th International Conference on Computer Communications and Networks (ICCCN ’15), pp. 1–7, August 2015.

[145] Gohil, A., Modi, H., and Patel, S. K., “5G technology of mobile communication: a survey,” in Proceedings of the International Conference on Intelligent Systems and Signal Processing (ISSP’13), pp. 288–292, Gujarat, India, March 2013.