Autonomous Vehicles to Evolve to a New Urban Experience

DELIVERABLE

D3.7 Initial Standardisation and concentration actions report

Co-funded by the Horizon 2020 programme of the European Union

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 769033

Disclaimer

Document Information

Grant Agreement Number	**769033**
Full Title	Autonomous Vehicles to Evolve to a New Urban Experience
Acronym	AVENUE
Deliverable	D3.7 Initial Standardisation and concentration actions report
Due Date	31.10.2019
Work Package	WP3
Lead Partner	bestmile
Authors	Lisa Labriga, Frédéric Gaiddon, Anne Mellano, Jérome Caillaud, Raphael Gindrat
Dissemination Level	Public

Document History

Author	**Entity**	**Date**	**Contribution**	**Comments**
Lisa Labriga	Bestmile	March 2019	Introduction	Draft version
Frédéric Gaiddon, Anne Mellano, Raphaël Gindrat Jérome Caillaud	Bestmile	June to September 2019	Chapters 4 and 5	Draft version
Peter Lorenz, Michael Karner	VIF	June to September 2019	Chapter 6	
Jenny Ralli, Antonios Lalas, Konstantinos Votis	CERTH	January to March 2019	Chapter 7	
Frédéric Gaiddon	Bestmile	05-09-2019	Insertion of inputs from VIF and CERTH (chapters 6 and 7)	
Anne Mellano Frédéric Gaiddon	Bestmile	September 2019	Review of chapters 6 and 7	
Antonios Lalas, Konstantinos Votis	CERTH	September to October 2019	Revisions of chapter 7	
Hassane Ouchouid	Navya	October 2019	Chapter 2	
Jannie Andersen	Autonomous Mobility	September to October 2019	Review	
Lisa Labriga	Bestmile	October 2019	Inclusion of inputs & finalization of deliverable	D 3.7 Initial standardisation and concentration actions report

Index

1 Executive Summary

WP3 objective is to create a web of collaborations to reach a broad spectrum of directly and non-directly relevant parties to maximise the output value of AVENUE. The target of task T3.3 "Standardization and concentration actions" is to monitor and follow the regulations and standards in the European landscape in the domains of automated transport, electrical vehicles, sensor networks, on-demand services, security, safety and privacy.

The partners of task T3.3 and WP3 have thereby identified three main subtasks:

A. Monitor and follow the regulations and standards in the European landscape in the domains of automated transport, electrical vehicles, sensor networks, on-demand services, security, safety, privacy, and data connection (Transmodel, NeTEx, SIRI, …)
B. Gap analysis, analysis of the potential and need for new standards or amendments of existing ones.
C. Examination of EU data protection rules, both from a legal and ethical perspective of the task; look into concept of adaptive ethics.

According to the sub-tasks identified to be addressed in this deliverable, the partners involved in task 3.3 have identified the topics to be addressed and the responsible partner for each topic.

Chapter 2, authored by Navya, focuses on autonomous vehicles and highlights the applicability of regulations, discusses function safety and finishes with a gap analysis.

Chapter 3, authored by Bestmile, explains the context of autonomous vehicle protocols and the fact that there are currently no existing European regulations and standards, before going into detail on the potential for new or amended standards.

Chapter 4, also authored by Bestmile, focuses on on-demand mobility services and provides the context, as well as an overview of European regulations and standards and a view on the potential for new or amended standards this area.

Chapter 5, authored by VIF, provides an overview from the perspective of the connection of the AVENUE platform to traveller interfaces and to public transport operators. The focus is thereby on Trandmodel and its implementation in the four demonstrator sites.

Chapter 6, authored by CERTH, addresses sub-task C and focuses on safety, security, privacy and data protection.

2 Introduction

The target of the AVENUE project is to demonstrate and pilot the adaptability and efficiency of the deployment of small and medium autonomous vehicles (AV's) in Lyon, Luxembourg, Geneva, Copenhagen and 2-3 replicator cities as of the 3d year of the project. The AVENUE vision for future public transport in urban and suburban areas, is that autonomous vehicles will ensure safe, rapid, economic, sustainable[1] and personalised transport of passengers, while minimising changes in modes of transportation. The goal is to provide door to door autonomous transport allowing commuters to benefit from autonomous vehicles.

At the end of the AVENUE project – 4-year period - the mission is to have demonstrated that autonomous vehicles will become the future solution for public transport. The AVENUE project will demonstrate the economic, environmental and social potential of autonomous vehicles - for both companies and public commuters - while assessing the vehicle road behavior safety.

WP3 objective is to create a web of collaborations to reach a broad spectrum of directly and non-directly relevant parties to maximise the output value of AVENUE.

The target of task T3.3 "Standardization and concentration actions" is to monitor and follow the regulations and standards in the European landscape in the domains of automated transport, electrical vehicles, sensor networks, on-demand services, security, safety and privacy.

The partners of task T3.3 and WP3 have thereby identified three main subtasks:

D. Monitor and follow the regulations and standards in the European landscape in the domains of automated transport, electrical vehicles, sensor networks, on-demand services, security, safety, privacy, and data connection (Transmodel, NeTEx, SIRI, …)
E. Gap analysis, analysis of the potential and need for new standards or amendments of existing ones.
F. Examination of EU data protection rules, both from a legal and ethical perspective of the task; look into concept of adaptive ethics.

[1] Within urban transportation sustainable most often refers to electric vehicles.

2.1 Methodology

According to the sub-tasks identified to be addressed in this deliverable, the partners involved in task 3.3 have identified the topics to be addressed (see also figure 1), and the responsible partner for each topic:

1. Autonomous Vehicles: addressing sub-tasks A and B for all topics around autonomous vehicles: automated transport, electric vehicles, sensor networks.
   Owner: Navya
   → Chapter 3
2. Autonomous Vehicles Protocol: addressing sub-tasks A and B for the communication between autonomous vehicles and the AVENUE platform.
   Owner: Bestmile
   → Chapter 4
3. On-demand services: addressing sub-tasks A and B for on-demand services.
   Owner: Bestmile
   → Chapter 5
4. Transmodel, NeTEx, SIRI, etc.: addressing sub-tasks A and B for the connection between the AVENUE platform and traveler interfaces as well as public transport operators.
   Owner: VIF
   → Chapter 6
5. Security, safety, privacy, data protection: addressing sub-task C.
   Owner: CERTH
   → Chapter 7

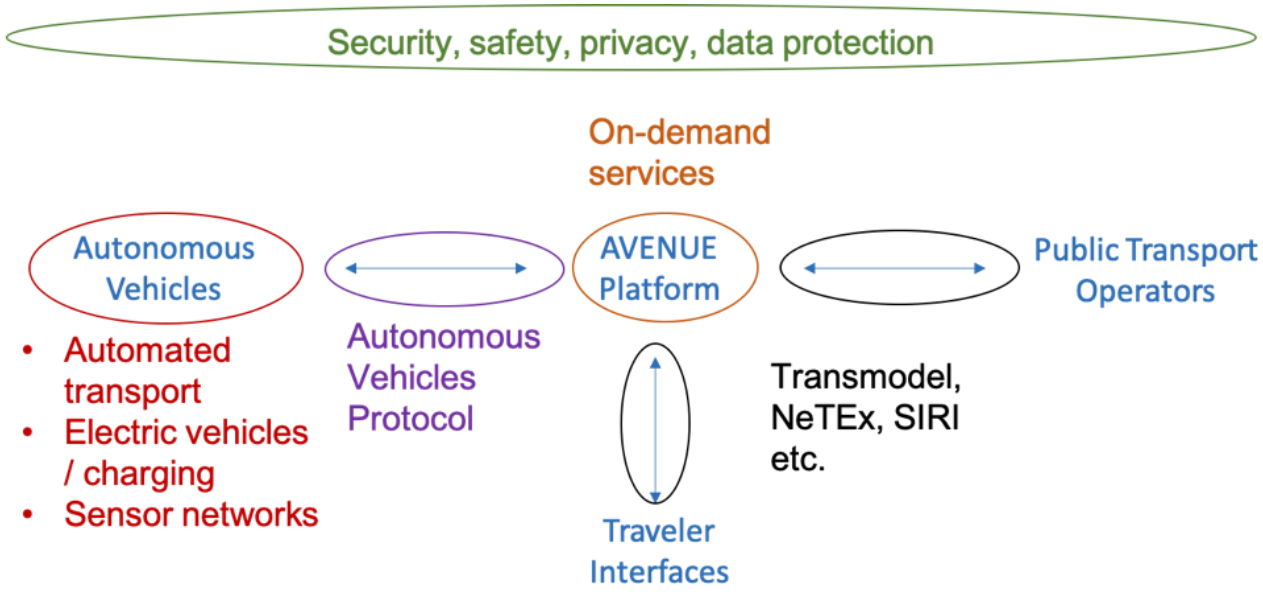


Figure 1: Topics for T3.3

3 Autonomous vehicles

3.1 Applicable EU regulations

Every moving vehicle must have a driver, the driver must constantly have control of the vehicle, which is one of the main roadblocks in the way of completely autonomous cars being implemented.

Many automotive regulations are not applicable because of the consideration of the driver. For example, the regulations of the systems of indirect vision no. 46 and the regulation of the steering equipment no. 79 are not applicable because there is no driver. Some regulations may be partially applicable, such as Regulation no. 121, there is no driver, but some pictograms must be accessible to passengers. Others are not applicable because the vehicle is fully electric (regulation R715 / 2007 or R34) or not applicable for M2 class A vehicle (Regulation R14 or R91).

Object	ECE Act	**Applicable / Not applicable**
Quiet Road Transport Vehicles (QRTV)	R540/2014 & R138	**Applicable**
Emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information	R715/2007	**Not applicable**
Prevention of fire risks	R34	**Not applicable**
Rear underrun protective devices (RUPDs)	R58.03	**Applicable**
Space for mounting and the fixing of rear	R1003/2010	**Applicable**
Steering equipment	R79	**Not applicable because there is no driver**
audible warning devices	R28	**Applicable**
Devices for indirect vision	R46	**Not applicable because there is no driver**
Breaking	R13	**Applicable**
Electromagnetic compatibility	R10	**Applicable**
Anti-theft of motor vehicles	R18	**Applicable**
Strength of seats, their anchorages and head restraints	R17.08	**Applicable**
Strength of seats and their anchorages (buses)	R80	**Not applicable**
Access, manoeuvrability and implementing	R130/2012	**Applicable**
Speedometer	R39	**Applicable**
Manufacturer's statutory plate of motor vehicles and their trailers	R249/2012	**Applicable**
Safety-belt anchorages	R14	**Not applicable**
Installation of lighting and light-signalling devices	R48	**Applicable**

Retro-reflecting devices	R3	**Applicable**
Position, stop and end-outline lamps	R7	**Applicable**
Daytime running lamps	R87	**Applicable**
Side-marker lamps	R91	**Not applicable**
Direction indicators	R6	**Applicable**
Illumination of rear registration plates	R4	**Applicable**
Headlamps (halogen sealed beam (HSB))	R31	**Not applicable**
Filament lamps	R37	**Not applicable**
Headlamps with gas-discharge light sources	R98	**Not applicable**
Gas-discharge light sources	R99	**Not applicable**
Headlamps emitting an asymmetrical passing-beam	R112	**Applicable**
Adaptive front-lighting systems (AFS)	R123	**Not applicable**
Front fog lamps	R19	**Not applicable**
Towing device	R1005/2010	**Applicable**
Rear fog lamps	R38	**Applicable**
Reversing lamps	R23	**Applicable**
Parking lamps	R77	**Not applicable**
Safety-belts	R16	**Not applicable**
Identification of controls, tell-tales and indicators	R121	**Partially applicable because there is no driver**
Windscreen defrosting and demisting systems	R672/2010	**Applicable**
windscreen wiper and washer systems	R1008/2010	**Applicable**
Heating system	R122	**Applicable**
Measurement of the net power	R85	**Applicable**
Emissions of heavy commercial vehicles (Euro IV et Euro V)	Directive 2005/55/CE	**Not applicable**
Emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information	R595/2009	**Not applicable**
Safety glazing	R43	**Applicable**
Installation of their tyres	R458/2011	**Applicable**
Tyres for commercial vehicles and their trailers	R54	**Applicable**
Tyres, rolling resistance, rolling noise and wet grip	R117	**Applicable**
Speed limitation of devices	R89	**Applicable**
Masses et dimensions	R1230/2012	**Applicable**
Mechanical coupling	R55	**Applicable**
General construction of buses and coaches	R107	**Partially applicable**
Strength of superstructure (buses)	R66	**Not applicable**
Hydrogen-powered motor vehicles	R79/2009	**Not applicable**
Advanced emergency braking systems	R347/2012	**Not applicable**
Installation of lane departure warning systems	R351/2012	**Not applicable**
LPG vehicles	R67	**Not applicable**
Electric power trained vehicles	R100	**Applicable**

CNG and LNG vehicles	R110	**Not applicable**

Acts according to the directive 2007/46/EC

In each regulation there is a chapter about testing methods explaining how to validate technical solutions. The testing methods presented are not all suitable for autonomous vehicles. Moreover, other verification methods such as simulation or formal proofs need to be developed via documents to demonstrate our compliance with the requirements.

Currently many other AV specific points are pending since there is no regulation mentioning them. Indeed, autonomous shuttles contain operating specificities, construction and onboard equipment that are not found on traditional vehicles and for which there is no associated regulation like lidars, GNSS antenna, GSM with radio antenna.

3.2 Function safety voluntary standards

ISO26262:

ADS Safety relevant function is different from not automated vehicle:

The standard ISO26262 considers the controllability of the driver while the level of automation from the SAE J3016 requires a full fallback from the system. The standard could be applied with an improved controllability but that lead to ASIL levels superior than usual in the industry. Functions that are not safety-relevant for not automated vehicles become safety-relevant and require reaching normative targets to ensure the safety. The main industrial suppliers in the automotive and/or public transport domain are not mature enough for this type of function in terms of functional safety process application and cannot be compliant with the requirements.

Example: Air conditioning and access facilities.

Integration of safety-related systems not developed according to ISO 26262:

The standard ISO26262 v2018 allows to integrate safety relevant systems not developed according to ISO26262 for Truck & Bus categories. In these categories, there is an opportunity for ADS in these categories to reach target on systems otherwise used in another domain (lidar for example). Even if development process requirements are relatively equivalent, the target for the reliability data and their application are not always comparable and, in some domains, it is not convenient to provide details to the customer. It could be useful to have an official comparison of level of integrity or level of performance of the safety and what is acceptable by ASIL target.

For example, the diagnostic coverage and the failure rate according to ISO13849 are not considering the type of failure as ISO26262.

ISO/PAS 21448:

The publicly available specification ISO/PAS 21448 related to the safety of the intended functionality request to define an acceptance criterion that could be a validation target.

The definition of target guides the applicant of the specification without official target. It seemed necessary to have a common approach to validate the target according to the ethical character of the topics based on accident data as defined by the European commission.

The calculation methods of the validation criteria are not specified, and subject to interpretations like qualitative evidence, projection calculation from test & simulation… And those methods must be clarified to make sure that the target has been reached.

3.3 Gap analysis and potential for new or amended standards

Each authority has their own requirements and “feelings” of what is adequately safe:

- It is time consuming to consult each authority in each country (each time, need to find the right contact with the authorities, present our mobility system which is very technical).
- Specific requirements depending on each country leading to specific vehicle configuration. The shuttle’s builders are SMEs or start-ups, and it is difficult for them to handle the involved costs to make specific changes between countries. Some requirements are sometimes contradictory and so the shuttle must be "tailor-made".
- Different validation process, for some it’s only document validation or static validation or dynamic validation. For dynamic validations, there is no harmonization either, which leads to custom-made test cases depending on the authority.
- As no harmonization = no framework. Some countries do not necessarily have the resources and / or the skills to build a framework to allow autonomous shuttles, so they do not know how to do an authorization and this is blocking in several countries while there is a real demand from customers and the market.

News functions:

Dismounted system:

The ADS require dismounted system for communication with infrastructure, monitoring center, other road users, etc. That’s a new problematic for AVs and there is actually no existing standard. That requires a clarification of some points to ensure safety regarding the impact of the dismounted system on the vehicle:

- How to ensure the reliability & integrity of the data used by the vehicle?
- What standards could be applied for Functional safety (ISO26262, IEC61508 or other(s))?
- What is required & acceptable to ensure a safe remote monitoring?

Emergency stop:

According to controllability issues, emergency stop buttons are integrated in ADS vehicle. For now, a standard from Machinery the ISO13850 specified the requirement of design and application of the Emergency stop function. Obviously, some parts are not applicable or adaptable. The automotive

domain requires an adaptation of what is the design and the expectations of an emergency stop functions in an ADS are.

4 Autonomous Vehicles Protocol

4.1 Context

The Two Roads to Robotaxis

The development of fully autonomous vehicles and services, the end goal of which is an on-demand "robotaxi" service, has evolved different ways in different parts of the world. In the U.S. technology companies like Waymo and Argo AI developed AV driving systems and bolted them on to conventional vehicles. They have been testing the technologies by driving millions of miles on public roads with backup drivers to intervene if the technology fails. In Europe, back in 2012, new companies like EasyMile and Navya developed purpose-built electric autonomous shuttles, with no steering wheels, designed to work in conjunction with public transit. Many of these shuttles are now operated by public transport agencies on fixed routes with "safety drivers" aboard to educate riders and intervene in the case of malfunctions.

U.S technology companies have been focused on increasing the automation capabilities of conventional individual vehicles with the goal of reaching full Level 5 autonomy in the long term. In Europe, firms have taken the approach of developing a completely new kind of vehicle with onboard self-driving technology: autonomous shuttles. These approaches are likely to continue to evolve as both sides learn about the challenges of full autonomy. French shuttle maker Navya, partner of the Avenue project, recently announced that it would focus on selling its self-driving technology to other manufacturers.

While autonomous vehicle technology makers and vehicle manufacturers alike predicted full-fledged robotaxi services would be available in 2019, that prediction has been proven to be overly optimistic. Creating an autonomous vehicle that can safely go anywhere at any time in any condition is turning out to be tremendously difficult. Also, much-publicized accidents, including a pedestrian fatality, have made the public wary of the real-world utility of autonomous mobility.

European Autonomous Journey

Thus far Europe leads the world in the use of autonomous vehicles on public streets in conjunction with public transport agencies. Beginning in 2012, the first autonomous shuttles were deployed in pilot projects in low-traffic, low-speed environments like university campuses. The knowledge gained from these projects enabled the technology and vehicles to evolve and currently, there are public autonomous shuttle services on public streets.

Testing of autonomous shuttles in Europe began with the CityMobil2 project in September 2012. The project involved 45 partners drawn from vehicle manufacturers, system suppliers, city authorities (and local partners), the research community and networking organizations. Five sites were selected

where fleets of up to six vehicles would be deployed on fixed routes. One of the sites selected was the technical university of Lausanne (EFPL), where an on-call service was tested. The vehicles still followed a fixed route but could be requested via a smartphone app that was developed for the project.

Following the success of the CityMobil2 project, in 2016 PostBus - the largest public transport operator in Switzerland - contacted EPFL to consider replicating the CityMobil2 demonstration in the urban center of the city of Sion. The goal was to test the acceptance of autonomous mobility by a more diverse population than the one on the EPFL campus and on public streets. The project, named "SmartShuttle" transported passengers around the city of Sion in areas that are difficult to reach with traditional buses. The project was later expanded to connect the shuttles with the city's train station and has been in continuous operation for three years.

In 2017, French mobility service provider RATP launched a test using autonomous shuttles from two different manufacturers, EasyMile and Navya, in the same fleet. The service connected the Château de Vincennes and Parc floral du bois de Vincennes in Paris.

All of these deployments have been on fixed routes and were not required to adhere to a schedule. The EPFL project tested a limited on-demand capability, while others were headway-based.

From Vehicles to Services

While much of the world has been focused on automotive vehicles and self-driving technologies, projects like Avenue call attention to the need for these vehicles to be able to work together as fleets in order to offer intelligent services. Once vehicles can drive safely on public streets, how do they know where to go? How will travelers request rides? What kind of information needs to be exchanged? For on-demand services, this is particularly challenging when hundreds or thousands of travelers are simultaneous requesting rides to different destinations. Optimizing vehicles' capacities and routing them efficiently with predictable ride times and wait times is essential for operators and passengers alike and requires what has been come to be called "fleet orchestration."

This type of orchestration requires a supervisory layer of fleet communication that functions like a control tower for aircraft. At airports around the world, vehicles from different manufacturers and different services providers are carefully guided by control tower technology from gate to gate.

4.2 Existing European regulations and standards

A challenge in orchestrating fleets is to enable vehicles with diverse proprietary self-driving technologies to communicate without interfering with the highly sensitive AV tech, and without giving outside developers access to proprietary data. The orchestration layer described above requires a vehicle agnostic solution that would enable connected vehicles of any brand or type to communicate with one another and with the orchestration engine to deliver full-fledged services like those envisioned by Avenue.

Currently no European or International standard exists for the connection of autonomous vehicles to a 3rd-party platform. As the industry is nascent, each manufacturer develops its own technology and, in its way, considers the possible connection points for third-party systems.

4.3 Potential for new or amended standards

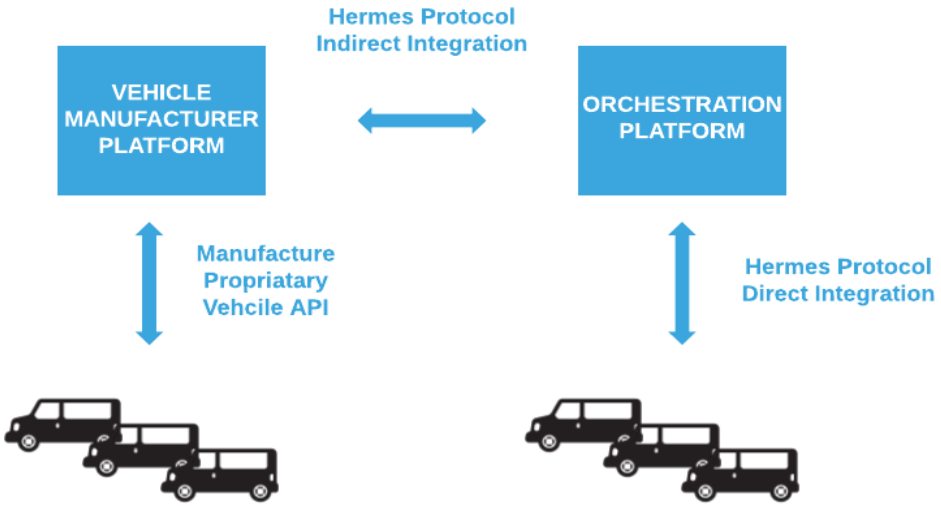
4.3.1 Need for Standardized Communication

Partners in the Avenue consortium identified the need for standardized communication among diverse vehicles in fleets as early as 2014. The need for orchestration—to send missions to vehicles and to receive mission status from vehicles—was required to enable fleet services that could provide predictable service levels for travelers. As nothing was available on the market, a vehicle agnostic autonomous vehicle protocol was developed by consortium partner Bestmile. This open, bidirectional protocol enables standardized communication and can be used by any vehicle to connect to the orchestration layer such that it would not require access to the vehicles' onboard technology. This protocol enables fleets of divergent vehicles with divergent technologies to work together. Operators can send missions to vehicles and vehicles can report their location and status as they execute these missions.

4.3.2 Hermes Protocol description

Hermes protocol is an open source two-way communication protocol that supports reporting vehicle telemetry to the orchestration platform as well as sending missions to the vehicle. It provides a manufacturer agnostic abstraction allowing the Avenue platform to remain open to any vehicle manufacturer.

Hermes can either be integrated directly in the vehicle or indirectly in the vehicle manufacturer platform.



The protocol is intended to be used either by:

- Vehicle manufacturers who want to be compatible with the Bestmile platform
- Fleet monitoring software providers who wish to benefit from Bestmile's fleet orchestration services

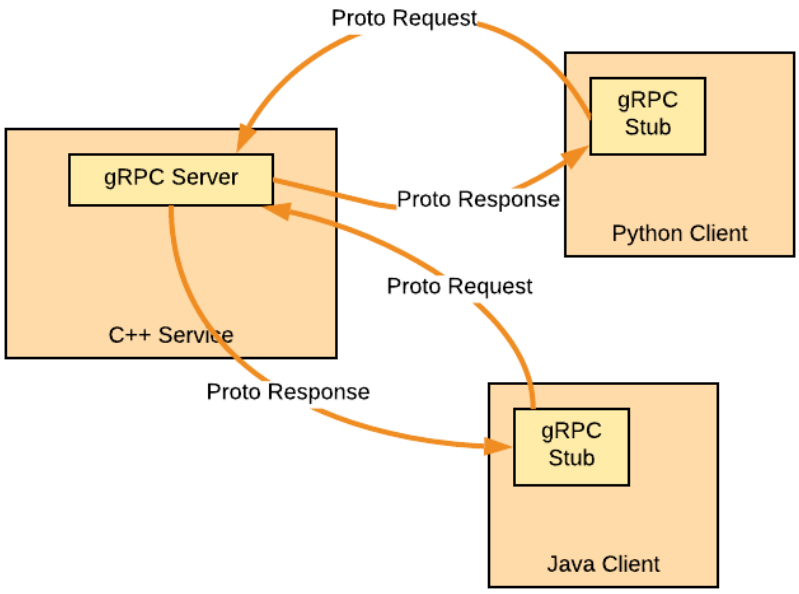
Protocol technical overview:

Hermes is based on open source protocol layers. It uses Protobuf to binary encode the messages and gRPC to transport the messages.

The Hermes protocol is a flow of binary messages exchanged over gRPC. Messages are described by a Protocol Buffer specification.

Hermes messages can be exchanges through a gRPC connection as it uses protocols buffers as both its Interface Definition Language (IDL) and as its underlying message interchange format (https://grpc.io).

In gRPC a client application can directly call methods on a server application on a different machine as if it was a local object, making it easier for you to create distributed applications and services. As in many RPC systems, gRPC is based around the idea of defining a service, specifying the methods that can be called remotely with their parameters and return types. On the server side, the server implements this interface and runs a gRPC server to handle client calls. On the client side, the client has a stub (referred to as just a client in some languages) that provides the same methods as the server.



gRPC clients and servers can run and talk to each other in a variety of environments and can be written in any of gRPC's supported languages. So, for example, you can easily create a gRPC server in Java with clients in Go, Python, or Ruby.

4.3.3 On-going initiatives: ITxPT and SPACE

On a European level, several initiatives are flourishing which are discussing potential new standards for the communication with autonomous vehicles. Some AVENUE partners contribute to some of these initiatives with their expertise.

UITP SPACE:

Bestmile is active in UITP SPACE project which is focused on Shared Personalized Autonomous Connected Vehicles. Working Group 2 focus is to identify the high-level reference architecture focused on the integration of AVs in the PT ecosystem, ensuring interoperability as well as performances, efficiency, safety and security.

This working group is currently evaluating if Hermes could become a standard for the vehicle to platform communication stack.

ITxPT:

A standard protocol for back-office interoperability (TiGR - Telediagnostic for Intelligent Garage in Real-time) has been specified. It provides Transport Operators (PTOs) a homogeneous monitoring of their heterogeneous fleets. The organization defines interoperability on three levels: hardware (installation rules, space requirements, connectors, etc.), communication protocol (interfaces, declaration of service, etc.) and service (list of services, format of the service, format of data, etc.

ITxPT has published specifications that are designed to provide public transport authorities and operators with recommendations and requirements to support the purchase and integration of interoperable IT architecture. Industry suppliers use the specifications to design ITxPT-compliant equipment and services. ITxPT began in 2013 and announced the first product to receive certification in 2017. Bestmile joined the organization in 2018. Thus far a handful of devices that connect data and communications on buses with back office systems have received certification.

4.3.4 Automotive space

Standardization in the Automotive Industry

The automotive industry is no stranger to standardization. While autonomous vehicles and technology have moved beyond the scope of existing standards, the industry has collaborated for generations to create uniform requirements to facilitate manufacturing. The balance for manufacturers is often between leveraging proprietary technology for competitive advantage and standardizing commoditized to streamline production. While autonomous vehicle businesses are guarding their intellectual property, there is little doubt that the standardization will continue to evolve.

Conditions for Standardization

There are multiple conditions that need to be met for any standard to be developed and adopted widely by any industry.

Such conditions are for example:

- A mature technology
- A strong user and/or customer demand
- The availability of (good) products that meet customer expectations
- Favorable economic conditions

- A favorable legislative environment

Progress has been uneven in the development of mature technologies for connected vehicles. Conditions are now favorable for some services to be widely available. For instance, two-way communication protocols, like 4G (even more with the LTE/5G) are nearly ubiquitous. As these technologies are becoming affordable, it helps then to make such services available at lower prices, further accelerating adoption.

It is becoming clear that auto users want to continue their digital experience while in cars. Simple, useful and personalized products and services have been developed such as auto-check of the vehicle health and tele-diagnostic, infotainment like traffic info and streaming music, smartphone integration to make calling easier and safer, etc.

The car economy hit a crisis but then it also served as a starter for some car makers to reinvent themselves, they notably understood that they had to provide more and more services in (but not only) the car. This was particularly true for navigation/infotainment services.

One last dimension is the legislation. One way in which legislation has enabled connected vehicles is the elimination of most roaming charges within the European Union. This has facilitated the availability and affordability of connected services.

Auto Standards History

Since 1958 vehicle manufacturing in European Union countries has been regulated mainly by international standards established by the European Union and the United Nations Economic Commission for Europe (UNECE). These regulations have evolved to 1998's EU Whole Vehicle Type Approval. This agreement established global technical rules to increase the convenience of manufacture and removal of barriers to trade.

The auto industry relies on more than just standardized manufacturing. Road infrastructure such as signals, signage, fuel stations, parking requirements have all been developed to streamline the use of autos. The 1968 Vienna Convention on Road Traffic has provided standards for this infrastructure.

Automated Vehicle Standards

In 2016 UNECE amended the Vienna Convention with guidelines to allow automated vehicles on roads. This opened the door to the testing of autonomous vehicles on public roads, which is taking place through regulatory agencies in various countries.

- In the U.K., the Centre for Connected and Autonomous Vehicles (CAV) has been created by the government to work on legislation to allow testing on motorways in the country. The organization has funded some 200 initiatives to work collaboratively on projects to streamline the advent of autonomous mobility.
- Germany enacted the Autonomous Vehicle Bill in 2017—an update of the country's Road Traffic Act to define the requirements for highly and fully automated vehicles. The legislation addresses issues like the definitions of automated vehicles, how those vehicles must comply with traffic laws, and how the vehicles will interact with human-driven vehicles.

- France announced in 2018 that it would create legislation to allow the testing of autonomous cars on public roads by 2019, with a goal of "highly automated vehicles" operating by 2022.
- Spain has made the city of Barcelona a testing ground for autonomous mobility and is working with private technology Mobileye to launch a fleet of 5,000 vehicles.

Safety Standards

Standards are also emerging for example for ADAS/safety in-car services. In 2018, the European Transport Safety Council announced that all new car models sold in the EU must be fitted with standardized GPS devices and be capable of communication over the GSM phone network for emergency and breakdown calls. This will facilitate the introduction of future safety systems such as Intelligent Speed Assistance, which can use GPS to locate speed limits on digital maps.

In 2019, the EU published standards and made the following safety technologies mandatory for automobiles:

- Warning of driver drowsiness or distraction
- Intelligent speed assistance
- Backup cameras and reverse sensors
- Data recorders for accidents
- Lane-keeping assistance
- Advanced emergency braking
- Improved safety belts

Vehicle Everything Communication

Earlier in 2019, the European Union announced that wireless Dedicated Short-Range Communication (DRSC) ITS-G5 would be the standard for "Vehicle to Everything" communication. The announcement sets a standard for how vehicles will communicate with other vehicles and with infrastructure such as roads, buildings, traffic signals, and charging stations and more.

Vehicle to Platform Communication

Currently no European or International standard exists for the connection of autonomous vehicles to another platform. Each autonomous vehicle manufacturer has a different way of sending/receiving information.

This is important when it comes to the ability to send instructions, or missions, to vehicles to tell them where to go and how to get there. Thus far, the conditions for the deployment and mass adoption of such a standard have not been met. The current state of the autonomous shuttle vehicles and services today is in an experimental state with many operators running pilot projects with few vehicles. The demand for mass production of vehicles has not yet arrived, and the focus of developers have been on vehicle performance and safety and not on communication protocols.

Also, because of the perceived value of the mobility market, many automakers and AV technology companies are attempting to build as much of the value chain as they can alone. This does not facilitate the creation of standards. But we expect the situation to evolve and with conditions

becoming more and more favorable such standards will be developed and widely used. This will be driven by two expected trends:

- Consolidation within the Industry of SAEV manufacturers. The battle for leadership in standards that will be established by the winners.
- The need of data security and physical safety will push manufacturers to share standards. Legislation regarding AV will be primarily focused on these aspects.

Avenue Vehicle to Platform Communication

Even in the absence of universal standards, for the Avenue project vehicles providing autonomous services will need to receive missions from a dispatching system. The missions must be sent to the vehicles' onboard autonomous driving technology with instructions for where to go and how to get there. Different fleet operators will have different requirements for fleet performance and will direct vehicles based on business requirements such as distance and wait time thresholds. The Avenue consortium identified the lack of a standard for fleet communications that can work with and vehicle brand and type. To this end, the consortium has adopted an Autonomous Vehicle Protocol that enables bi-directional communication between vehicles and fleet operators. The protocol makes it possible to send missions to the vehicles based on operator-defined thresholds such as vehicle utilization and passenger ride times and wait times.

5 On-Demand mobility services

5.1 Context

The convergence of widespread smartphone adoption, the sharing economy, and the financial crisis of 2008 gave rise to a new type of mobility service—on-demand peer-to-peer ridesharing. Their services are offered by what has come to be called Transportation Network Companies (TNCs).

TNCs have allowed anyone with a car and a smartphone to earn extra money, and anyone with the TNC's smartphone app to get a convenient, inexpensive ride. These services also promised to make private auto ownership unnecessary for urbanites, complement public transport, and in so doing, to reduce congestion in cities.

The ensuing popularity of TNCs services has given rise to more on-demand mobility options. Currently, many European cities feature a mix of:

- Traditional taxi services where rides are hailed manually via phone calls or on street corners
- Peer-to-peer TNC services
- Micro-transit services run by transit agencies to offer first/last-mile transport
- Micro-mobility services (scooters, bicycles)
- Car sharing services that enable app-based on-demand car rental

As data has accumulated about the impact of TNCs, it has become clear that the services have failed to achieve the goals of reducing congestion or complementing public transport. Multiple studies have shown that the services have worsened traffic in cities, in part because travelers are using TNCs in place of public transportation. In the United States (the market that has been the subject of most research), TNCs have added 5.6 billion vehicle miles in major cities. Another study found the services responsible for 1.3 percent reduction in public transport use in U.S. cities. London's mayor Sadiq Khan said when calling for restrictions on TNCs in the city, "the huge increase in private hire drivers on London's roads in recent years is causing increased congestion, polluting our air and leaving many drivers struggling to make enough money to support themselves and their families".

Meanwhile the leading TNCs, Uber and Lyft, have forged partnerships with some in the U.S., U.K., and Australia that include adding public transport schedules and booking capabilities to their mobile apps. The goal is to support public transport utilization. The idea is that if travelers see train and bus schedules and fares, they will be more likely to use the TNC service in conjunction with public transportation.

Uber has publicly stated that it aims to become "the Amazon of transportation," with its mobile app serving as a one-stop-shop for all forms of transport for door-to-door journeys. Observers have suggested that this may be the only path to profitability for TNCs, especially in the event of the mass adoption of autonomous vehicles. Today, TNCs own no assets (and still lose money) and only pay drivers when a paying passenger is on board. With autonomous robotaxi services, the service provider will need to own or lease the vehicles, and any empty miles will drain revenues. TNCs would then become transit marketplaces rather than transit providers.

It has also been pointed out that cities should be wary of placing their transit schedules and bookings into the hands of a private business. TNCs have no incentive or duty to reach low-income passengers, disabled passengers, etc. And while the trial programs are free for public transport operators, TNCs could in the future use leverage to exact fees or otherwise exert control over public agencies.

5.2 Existing European regulations and standards

Before the arrival of TNCs, on-demand mobility was regulated and restricted in most countries. Taxi licenses are allocated based on population density in many cities and have cost as much as €250,000 in Paris and $750,000 in New York. Other cities and countries require taxi drivers to be professional drivers, passing tests, and paying fees to do so.

TNCs have attempted to skirt these regulations and restrictions, to the chagrin of taxi companies and some cities. England and Germany are two examples of countries that have attempted to force TNC drivers to be licensed just like any other traditional taxi driver.

On-demand services offered by public transport, on the other hand, is a newer phenomenon. Some have provided niche services for elderly or disabled persons, sometimes making advance appointments but with phone calls, not mobile or online booking systems. There is little in the way of regulation or standardization of service infrastructure or service level requirements for these services.

Mobile app-based services, where deployed, have typically involved fixed-routes that take passengers to and from public transport stations to places like business parks; or station-based services that gather nearby travelers and take them to common destinations. Several of these micro-transit services, even when offered free of charge, have failed to catch on with travelers. Ford's Chariot is the most notable failure in the U.S. In Europe, Kutsuplus in Finland and Slide in the U.K. have also shut down. The reasons given for the failures had a common complaint—the rides were not convenient enough whether due to waiting times or pickup and dropoff locations.

5.3 Potential for new or amended standards

The development of standards for shared, on-demand mobility services for public transport has the potential to speed adoption by creating a consistent, convenient passenger experience that also meets operator business requirements. This includes creating a type of Mobility as a Service (MaaS) offering that enables agencies to offer door-to-door journeys using multiple modes of transport.

As noted in the concerns about integrating with private TNC apps, it would be advantageous to public transport agencies to be the entities that ultimately control the MaaS platform. This would allow them to determine the terms for third-party operators to participate.

A critical challenge for growing cities facing increasing congestion is finding ways to increase public transit utilization. Cities will need to find a way to balance the supply and demand ratio of TNC-type services and private autos on streets. Success will hinge in part that services meets passenger requirements for cost and convenience.

For public transport operators to offer networks that include on-demand services and door-to-door journeys, a booking platform will require open interfaces (Application Programming Interfaces, or APIs) that facilitate the integration of multiple modes of transit. Travelers will want a one-click booking capability that will book each leg of the journey, even when using various providers. It will also be critical to make transit data available so that service utilization can be measured, and services continually improved to meet traveler needs. Standards must be set for how and with what entities that data may be shared. It also may be necessary to form regulations regarding the pricing of third-party providers to ensure equitable access.

6 Connecting the AVENUE platform to traveller interfaces & to public transport operators

6.1 Existing European regulations and standards

There are a number of existing European public transport standards which are regularly published on the standards.cen.eu website. Transmodel-cen.eu is a dedicated website for EN 12896 (CEN, 2015) covering both the 2006 version (Transmodel V5.1) and the new, not yet published, multipart version (Transmodel V6). The architecture is provided for download in HTML and Enterprise Architect formats (0302, 2016) (0302, 2017).

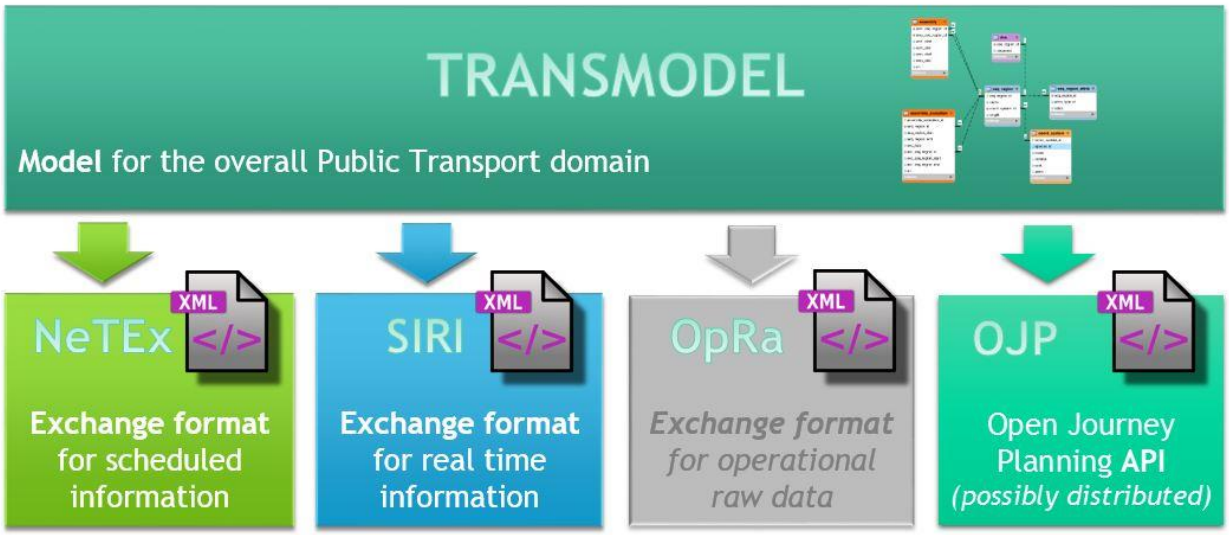


Figure 1: Transmodel Overview (CEN, 2016).

As in the Figure 1, several different data exchange services can be implemented:

- DVC (Data Communication on Vehicles)
- IFOPT (Identification of Fixed Objects in Public Transport)
- SIRI (Standard Interface for Real-Time Information)
- DJP/OJP (Open API for distributed journey planning)
- NeTEx (Network Timetable Exchange)
- OpRa (Operating Raw Data and statistics exchange)

where SIRI and NeTEx stay in our focus.

SIRI is a CEN Technical Standard that specifies a European interface standard for exchanging information about the planned, current or projected performance of real-time public transport operations between different computer systems.

XML protocol allowing distributed computers to exchange real time information about public transport services and vehicles. The protocol is a CEN technical specification, developed with initial participation of France, Germany (Verband Deutscher Verkehrsunternehmen), Scandinavia, and the UK (RTIG). SIRI is based on the CEN Transmodel abstract model for public transport information, and comprises a general-purpose model, and an XML schema for public transport information.

The following countries (Countries, 2014) are already using the Transmodel: France, Germany, Great Britain, Italy, Norway, Slovenia, Spain, Sweden, Switzerland. Following countries are implementing the Transmodel: Belgium, Denmark and Finland. Each country has documented its implementation of the Transmodel. For example, Norway (Norway, 2018) uses open source tools

1. Network and timetable database (Chouette) – www.chouette.mobi/en
2. IFOPT-based national stop registry (in-house development) – www.github.com/entur
3. Real-Time Proxy for SIRI-feeds (in-house development) – www.github.com/entur
4. Search engine (Open Trip Planner) – www.opentripplanner.org

6.2 Existing regulations and standards outside of Europe.

6.2.1 Regulation and standard in America.

In America, there is the American Public Transportation Association (APTA). It is a non-profit international association of more than 1,500 public and private sector member organizations.

The Transit Communications Interface Profiles (TCIP) Standard (APTA Standard for Transit Communications Interface Profiles - Annexes F - K) (APTA Standard for Transit Communications Interface Profiles - Narrative) (TCIP Data and Dialog Definitions) (TCIP XML Schema) constitutes the transit industry standards component of the US Intelligent Transportation Systems (ITS) program. TCIP is an interface standard. Its primary purpose is to define standardized mechanisms for the exchange of information in the form of data among transit business systems, subsystems, components and devices. For example, if a user requests a trip itinerary from a traveller information system, TCIP does not specify the screens, user interactions, etc. TCIP does provide the dialogs or file transfers to facilitate the traveller information system obtaining schedule information from the scheduling system.

TCIP also provides dialogs to allow one traveller information system to provide itinerary information to another (e.g., to another agency). TCIP uses extensible mark-up language (XML) to provide a widely known and supportable data exchange format between business systems but allows for other transfer syntaxes to be used.

6.3 Gap analysis and potential for new or amended standards

The goal is to fill the gap between the AVENUE Platform, the traveller interfaces and the public transport operators. The difficulty is that every country/city has its own implementation of the Transmodel, but the Transmodel-NeTEx is online available (CEN, 2009), which is one realization of the abstract model. Since it is only an abstract model, each implementation must be considered to communicate with AVENUE platform. A generic solution is pursued. At first, the participating cities needs to be investigated for common trends:

- Lyon: http://www.transmodel-cen.eu/implementations/france/lyon
- Luxembourg: N/A
- Geneva: http://www.transmodel-cen.eu/implementations/switzerland
- Copenhagen: http://www.transmodel-cen.eu/implementations/denmark/

In Lyon, it uses the Transmodel V5 that was the result of the EU project TITAN, which is also used on the pilot sites Hannover and Salzburg. Transmodel V5 uses also SIRI to exchange real-time data.

In Copenhagen, it uses the Nordic Public Transport Interface Standard (NOPTIS), see http://www.transmodel-cen.eu/implementations/sweden/. NOPTIS is a set of aligned Transmodel-based interfaces supporting the interconnection of subsystems within a public transport information system, including planning systems, schedule databases, GIS-systems, real-time vehicle reporting systems, traveller information systems, travel-planning systems, etc.

VSI is a vehicle-centric XML/XSD-based interface for transferring real-time information, while ROI is a stop- and vehicle journey-centric XML/XSD-based interface for providing passenger information systems with applied real time information. NOPTIS DII was a significant input to NeTEx. There exists a mapping (Official Website, 2014) between NeTEx and NOPTIS DII covering the Calendar, Timetable and Vehicle Schedule aspects showing how to use NeTEx in a way that supports parallel partial data deliveries as in NOPTIS.

The Geneva public transport implementation already supports the target users: operators, data consumers (application providers), open data users, that would cover the requirements. Moreover, the timetable data exchange and real time data exchange with NeTEx and Siri is already implemented between SNCF (Société Nationale des Chemins de fer Français) and SBB (Schweizerische Bundesbahnen). The Switzerland Transmodel can handle cross-border traffic and lines (from Germany and France). Definition on the profiles to be used have started and experimental export of the data was done. The current implementation will act as a transformer HRDF ↔ NeTEx and VDV ↔ Siri (HRDF – **H**afas **R**oh**d**aten**f**ormat = Hafas raw data format[2][3]). For the AVENUE-Platform, we will need such transformers that might need to be configured for each city/country.

[2] https://opentransportdata.swiss/de/cookbook/hafas-rohdaten-format-hrdf

[3] https://www.vdv.de

6.4 Conclusion

There are already existing deployments, where the Transmodel is used as a role-model. Switzerland has already implemented converters between French/German and Swiss train systems. This implementation could be expanded so that also transformers between French and German train systems are supported.

Transformer needs to be defined for the Transmodel of Lyon and for NOPTIS in Copenhagen to extend the Swiss Transformer model. The XML of SIRI can be used.

7 Security, safety, privacy, data protection

7.1 Cyber Security Aspects in Autonomous Vehicles

Nowadays, the automated and connected vehicle technologies are among the most researched topics. By extension, the security objective is of utmost importance, as we have to ensure the safety of the passengers. In order to create a secure and trustable autonomous vehicle ecosystem, we have to implement proper security principles and standards to strengthen ourselves against possible threats and vulnerabilities. Autonomous vehicles, such as the NAVYA fleet, have increased levels of connectivity and automation because they are composed by a plethora of networked computing components. This nested network creates multiple attack surfaces for a potential attacker to try to exploit possible vulnerabilities [1].

Common cybersecurity attacks

The most common employed attacks are reported next, since there are numerous alterations and versions, depending on the target, the expertise and the intentions of the attacker.

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks the target to lose the control of the system. Some versions of this attack are TCP/SYN flood, teardrop, smurf, ping of death and botnets [2].
2. Man in the middle attacks occurs when a malicious user gets between the communications between a client and a server, getting access to all the packets sent in the connection. The usual versions of this kind of the attack are session hijacking, IP spoofing and replay [3].
3. Phishing and spear phishing attacks exploit the ignorance of some users and send emails that appear to be from trusted sources with the goal of gaining personal information.
4. Password attacks, target the passwords, as they are the most common way to authentication to a system.
5. Eavesdropping attacks occur through the interception of network traffic. These attacks allow an attacker to obtain credentials and confidential information that users send over the network.
6. Cross-site scripting attacks, take advantage of the third party web resources to run scripts in the victim's web browser or a scriptable application.
7. SQL injection attacks are applied on databases of cyber-physical systems, such as our autonomous vehicle ecosystem.
8. Malware attacks are software, which is installed in the system without the authorization of the administrator.

It is preferable to create a robust defence system via implementing core security principles by design and utilizing state of the software and hardware. The goal of these principles is to integrate appropriate cyber security technologies and solutions against cyber threats [4].

Mitigation and prevention countermeasures for security risks

- Cyber security by design. Cyber resilience will be most effectively implemented and maintained if it is established in the design phase of the technology – not retrofitted at the end. These attributes are used to provide a framework for the introduction of encryption, digital signatures and securing a place-bound system. The characteristic attributes of security by design are [5]:
    - Confidentiality: It is the insurance that information is accessible only to those authorized to have access;
    - Integrity: It is the accuracy and completeness of information and processing methods;
    - Availability: It is ensuring that authorized users have access to information and associated assets, when required.
- Firewall is a critical defensive mechanism that inspects incoming and outgoing network traffic and permits it or blocks it, based on predefined rules. There may be multiple firewalls within the network and they must be placed at crucial nodes of the ecosystem [6].
- Security information and event management (SIEM) is a software solution that aggregates and analyses the activity from different resources across the network. SIEM collects security data, which is stored, normalized and fed to analytics processes, in order to discover trends, detect threats, and investigate alerts [7].

Indicative vulnerabilities that are found in the autonomous vehicles ecosystem are:

- Designer vulnerability: Source code, architecture, component specification, and product whole life design and support.
- Manufacturer vulnerability: Component selection and manufacture (cheap/ potentially compromised), threat identification and mitigation, software/ firmware update creation, and version control.
- Vendor vulnerability: Inventory management, inventory protection, version management. A special consideration is the extent to which sensing and other critical sub-components are designed manufactured and programmed with attention to security.
- Maintainer vulnerability: Version management, design integrity management, platform protection, 3rd Party Engineering/Customisation/Enhancement Compatibility and Vulnerability Management.
- Infrastructure Provider Vulnerability: Direct network attack, jamming of communications and location services, spoofing, impersonation, and interfaces to/ from other public systems.
- Law enforcement and traffic management vulnerability: Direct network attack, jamming of communications and location services, spoofing, and impersonation.
- End point vulnerability: On-board interface (external or internal attack), individual vehicle, control, access, disruption of operation, selective/ non-selective, and ransom, kidnapping, or theft of data.

7.2 Comprehensive security frameworks for privacy and data protection

The **EU Cybersecurity strategy** was introduced in 2013, followed by the Directive on the security of network and information systems (**NIS directive**) in 2016. The latter was the first EU-wide legislation

on cybersecurity. Further efforts have been taken by various EU organisations to raise awareness and provide recommendations on how to address cybersecurity issues. In 2016, the EU's independent advisory body on data protection and privacy, the Data Protection Working Party, published its views to raise awareness about developments in the IoT and its associated security issues.

7.2.1 List of available standards

Below is a list of available standards that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that processes and services of automated driving are fit for their purpose [8], [9], [10], [11], [12].

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
- 26262: This standard is derived from IEC 61508, which was developed for all electrical/electronic safety-related systems. ISO 26262 is specifically targeted for automotive safety. ISO 26262 also defines the Automotive Safety Integrity Level (ASIL).
- 27001 – Information security management system
- 27002 – Code of practice – security – provides recommendations for information management (contains guidance on access control, cryptography and supplier relationship)
- 27010 – Information security management for inter-sector and inter-organizational communications
- 27018 – Code of practice – handling PII (Personally Identifiable Information) / SPI (Secured Private Information) (privacy) – protection of PII in public clouds
- 27034 – Application security techniques – guidance to ensure software delivers necessary level of security in support of an organizations security management system
- 27035 – Information security incident management
- 29101 – Privacy architecture framework
- 29119 – Software testing standard

DEFSTAN

- 05-138 – Cyber security for defense 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
- ASIL includes Severity classification (S0 – S3), Exposure classification (E0 – E4) and Controllability classification (C0 – C3) to quantify the severity of an injury, probability of occurrence and controllability of the situation, respectively. ASIL is expressed as follows. ASIL = Severity × Exposure × Controllability where the higher level of ASIL (Automotive Safety Integrity Level) indicates a more grievous situation. In the context of AV, it can be noted that the controllability level is extremely high for level 3 upwards. To assess the ASIL, one can adopt techniques such as, Hazard Analysis and Risk Assessment (HARA), Fault Tree Analysis (FTA), and Failure Mode and Effects Analysis (FMEA)

7.2.2 Key Principles of Cyber Security for Connected and Automated Vehicles

In 2017, the UK Department for Transport (DfT) in conjunction with the UK Centre for the Protection of National Infrastructure (CPNI) released such high-level guidance for the automotive sector, the automated driving and intelligent transportation system ecosystem and their collective suppliers. This document is the only publicly available among European countries and will probably formulate the base for future national directives within Europe. The “Key Principles of Cyber Security for Connected and Automated Vehicles” [9] outlines eight fundamental building blocks that should underpin systemic cybersecurity best practices. These principles set out a comprehensive framework for addressing cybersecurity issues in the automated driving ecosystem but standards are required to deliver effective cybersecurity. According to the DFT and CPNI, these principles are:

Principle 1 - organisational security is owned, governed and promoted at board level

Principle 1.1: There is a security program, which is aligned with an organisation’s broader mission and objectives.

Principle 1.2: Personal accountability is held at the board level for product and system security (physical, personnel and cyber) and delegated appropriately and clearly throughout the organisation.

Principle 1.3: Awareness and training is implemented to embed a ‘culture of security’ to ensure individuals understand their role and responsibility in ITS (Intelligent Transport System) /CAV (Connected and Autonomous Vehicle) system security.

Principle 1.4: All new designs embrace security by design. Secure design principles are followed in developing a secure in ITS (Intelligent Transport System) /CAV (Connected and Autonomous Vehicle) system, and all aspects of security (physical, personnel and cyber) are integrated into the product and service development process.

Principle 2 - security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain

Principle 2.1: Organisations must require knowledge and understanding of current and relevant threats and the engineering practices to mitigate them in their engineering roles.

Principle 2.2: Organisations collaborate and engage with appropriate third parties to enhance threat awareness and appropriate response planning.

Principle 2.3: Security risk assessment and management procedures are in place within the organisation. Appropriate processes for identification, categorisation, prioritisation, and treatment of security risks including those from cyber are developed.

Principle 2.4: Security risks specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices.

Principle 3 - organisations need product aftercare and incident response to ensure systems are secure over their lifetime

Principle 3.1: Organisations plan for how to maintain security over the lifetime of their systems, including any necessary after-sales support services.

Principle 3.2: Incident response plans are in place. Organisations plan for how to respond to potential compromise of safety critical assets, non-safety critical assets, and system malfunctions, and how to return affected systems to a safe and secure state.

Principle 3.3: There is an active programme in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner.

Principle 3.4: Organisations ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber (or other) incident.

Principle 4 - all organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system

Principle 4.1: Organisations, including suppliers and third parties, must be able to provide assurance, such as independent validation or certification, of their security processes and products (physical, personnel and cyber).

Principle 4.2: It is possible to ascertain and validate the authenticity and origin of all supplies within the supply chain.

Principle 4.3: Organisations jointly plan for how systems safely and securely interact with external devices, connections (including the ecosystem), services (including maintenance), operations or control centres. This may include agreeing standards and data requirements.

Principle 4.4: Organisations identify and manage external dependencies. Where the accuracy or availability of sensor or external data is critical to automated functions, secondary measures must also be employed.

Principle 5 - systems are designed using a defence-in-depth approach

Principle 5.1: The security of the system does not rely on single points of failure, security by obscuration or anything, which cannot be readily changed, should it be compromised.

Principle 5.2: The security architecture applies defence-in-depth and segmented techniques, seeking to mitigate risks with complementary controls such as monitoring, alerting, segregation, reducing attack surfaces (such as open internet ports), trust layers / boundaries and other security protocols.

Principle 5.3: Design controls to mediate transactions across trust boundaries, must be in place throughout the system. These include the least access principle, one-way data controls, full disk encryption and minimising shared data storage.

Principle 5.4: Remote and back-end systems, including cloud-based servers, which might provide access to a system, have appropriate levels of protection and monitoring in place to prevent unauthorised access.

Principle 6 - the security of all software is managed throughout its lifetime

Principle 6.1: Organisations adopt secure coding practices to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place.

Principle 6.2: It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components.

Principle 6.3: It is possible to safely and securely update software and return it to a known good state if it becomes corrupt.

Principle 6.4: Software adopts open design practices and peer reviewed code is used where possible. Source code is able to be shared where appropriate.

Principle 7 - the storage and transmission of data is secure and can be controlled

Principle 7.1: Data must be sufficiently secure (confidentiality and integrity) when stored and transmitted so that only the intended recipient or system functions are able to receive and / or access it. Incoming communications are treated as unsecure until validated.

Principle 7.2: Personally, identifiable data must be managed appropriately. This includes: what is stored (both on and off the ITS / CAV system), what is transmitted, how it is used, the control the data owner has over these processes. Where possible, data that is sent to other systems is sanitised.

Principle 7.3: Users are able to delete sensitive data held on systems and connected systems.

Principle 8 - the system is designed to be resilient to attacks and respond appropriately, when its defences or sensors fail

Principle 8.1: The system must be able to withstand receiving corrupt, invalid or malicious data or commands via its external and internal interfaces while remaining available for primary use. This includes sensor jamming or spoofing.

Principle 8.2: Systems are resilient and fail-safe if safety-critical functions are compromised or cease to work. The mechanism is proportionate to the risk. The systems are able to respond appropriately if non-safety critical functions fail.

7.2.3 Applicable standards and guidance

The benefits of autonomous vehicles (AVs) are widely acknowledged but there are concerns about the extent of these benefits and AV risks and unintended consequences. That is the reason specific standards and guidance have been created and agreed to address issues related to privacy and cybersecurity. The most important standards are described next:

- **SAE** (Society of Automotive Engineers) guidance **J3061** [10] (Cybersecurity guidebook for cyber-physical vehicle systems) and **J3101**[11] (Requirements for hardware protected security for ground vehicle applications), along with numerous **ISO** standards relating to identity management, authentication, securing information technology systems and privacy all form the base on which to build the operational framework for securing automated driving systems.
- The US Department of Transport's National Highway Traffic Safety Administration (NHTSA) has also issued guidance on cybersecurity best practices for vehicles, which builds on SAE and other recommendations [12].
- **NHTSA** has adopted a multi-faceted research approach that leverages the **National Institute of Standards and Technology Cybersecurity Framework (NIST)** [13] and encourages industry to adopt practices that improve the cybersecurity posture of their vehicles in the United States. NHTSA's goal is to collaborate with the automotive industry to proactively address vehicle cybersecurity challenges, and to continuously seek methods to mitigate associated safety risks. NHTSA promotes a multi-layered approach to cybersecurity by focusing on a vehicle's entry points, both wireless and wired, which could be potentially vulnerable to a cyberattack. A layered approach to vehicle cybersecurity reduces the possibility of a successful vehicle cyber-attack, and mitigates the potential consequences of a successful intrusion. A comprehensive and systematic approach to developing layered cybersecurity protections for vehicles includes the following:
    - A risk-based prioritized identification and protection process for safety-critical vehicle control systems;

  - Timely detection and rapid response to potential vehicle cybersecurity incidents on America's roads;
  - Architectures, methods, and measures that design-in cyber resiliency and facilitate rapid recovery from incidents when they occur; and
- Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lessons learned. NHTSA encouraged the formation of **Auto-ISAC** (Information Sharing & Analysis Center). The automotive industry established the Auto ISAC in late 2015 and it became fully operational on January 19, 2016.
- **Auto-ISAC**, an industry environment emphasizing cybersecurity awareness and collaboration across the automotive industry.
- The automotive industry should follow the **NIST** documented Cybersecurity Framework, which is structured around the five principal functions "Identify, Protect, Detect, Respond, and Recover," to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles. This approach should:
  - Be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
  - Provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
  - Design-in methods and measures to facilitate rapid recovery from incidents when they occur; and
  - Institutionalize methods for accelerated adoption of lessons learned across the industry through effective information sharing, such as through participation in the Auto ISAC.
- The **SPY Car Act** was also introduced to enhance controls on cybersecurity and privacy to all vehicles. According to this law, critical and noncritical software systems in every vehicle must be separated, and all vehicles will be evaluated using best practices. It introduces specifications to ensure the security of collected information in vehicle electronic systems while the data is on the vehicle, in transit from the vehicle to a different location or in any off-board storage.

7.2.4 Comprehensive cybersecurity frameworks for automated driving worldwide

Like Europe's GDPR, **China's latest Cybersecurity Law** represents a control-oriented strategy. Key provisions of the law are personal information protection, critical information infrastructure protection, responsibilities of network operators to ensure security, preservation of sensitive information within China, certification of security products and penalties for violations [15]. One example of network operators' responsibilities includes the requirement for critical information infrastructure operators to store personal data within China and for companies to gain approval and pass national reviews before moving data overseas. Critical cyber equipment and special cybersecurity products can only be sold after receiving security certifications 15].

The government in Singapore has also amended existing legislation to control different aspects of cybersecurity risks. **Singapore's Computer Misuse and Cybersecurity Act** was amended in April 2017 to strengthen businesses' response to computer-related offences [16]. Other steps have been taken

to raise awareness of cybersecurity, such as through local institutes of higher learning and forming partnerships between academia and the private sector. By doing so, the government aims to use this as an opportunity for Singapore to become a leading cybersecurity service provider, demonstrating an adaptation-oriented strategy; and there are plans to set up a national Defence Cyber Organisation [17].

7.2.5 NHTSA Fundamental Vehicle Cybersecurity Protections

NHTSA is leading in the studies for vehicle safety and driving behaviour, as they get their data from the National Centre for Statistics and Analysis (NCSA), an office of the National Highway Traffic Safety Administration. Thus, a wide range of analytical and statistical support is provided to them, allowing for the creation of the advanced standards. The following recommendations are based on what **NHTSA** has learned through its internal applied research as well as from stakeholder experiences shared with NHTSA. These recommendations do not form an exhaustive list of actions necessary for securing automotive computing systems, and not all items may be applicable in each case [14].

These protections serve as a small subset of potential actions, which can move the motor vehicle industry towards a more cyber-aware posture.

1. Limit Developer/Debugging Access in Production Devices

Software developers have considerable access to ECUs (electronic control units). Such ECU access might be facilitated by an open debugging port, or through a serial console. However, developer access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units. If continued developer access is necessary, any developer-level debugging interfaces should be appropriately protected to limit access to authorized privileged users. Physically hiding connectors, traces, or pins intended for developer debugging access should not be considered a sufficient form of protection.

2. Control Keys

Any key (e.g., cryptographic) or password which can provide an unauthorized, elevated level of access to vehicle computing platforms should be protected from disclosure. Any key obtained from a single vehicle's computing platform should not provide access to multiple vehicles.

3. Control Vehicle Maintenance Diagnostic Access

Diagnostic features should be limited as much as possible to a specific mode of vehicle operation, which accomplishes the intended purpose of the associated feature. Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they are misused or abused outside of their intended purposes. For example, a diagnostic operation which may disable a vehicle's individual brakes could be restricted to operate only at low speeds. In addition, this diagnostic operation might not disable all brakes at the same time, and/or it might limit the duration of such diagnostic control action.

4. Control Access to Firmware

In many cases, firmware precisely determines the actions of an ECU. Extracting firmware is often the first stage of discovering a vulnerability or structuring an end-to-end cyber attack. Developers should employ good security coding practices and use tools that support security outcomes in their development processes. Many platforms may be able to support whole disk encryption of external non-volatile media. In this case, encryption should be considered as a useful tool in preventing unauthorized recovery and analysis of firmware. Firmware binary images may also be obtained from a firmware updating process. Organizations should reduce any opportunities for a third party to obtain unencrypted firmware during software updates.

5. Limit Ability to Modify Firmware

Limiting the ability to modify firmware would make it more challenging for malware to be installed on the vehicles. For example, the use of digital signing techniques may make it more difficult and perhaps prevent an automotive ECU from booting modified/ unauthorized and potentially damaging firmware images. In addition, firmware updating systems which employ signing techniques could prevent the installation of a damaging software update that did not originate from an authorized motor vehicle or equipment manufacturer.

6. Control Proliferation of Network Ports, Protocols and Services

The use of network servers on vehicle ECUs should be limited to essential functionality only and services over such ports should be protected to prevent use by unauthorized parties. Any software listening on an internet protocol (IP) port offers an attack vector which may be exploited. Any unnecessary network services should be removed.

7. Use Segmentation and Isolation techniques in Vehicle Architecture Design

Privilege separation with boundary controls is important for improving security of systems. Logical and physical isolation techniques should be used to separate processors, vehicle networks, and external connections as appropriate to limit and control pathways from external threat vectors to cyber-physical features of vehicles. Strong boundary controls, such as strict white list-based filtering of message flows between different segments, should be used to secure interfaces.

8. Control Internal Vehicle Communications

Critical safety messages are those that could directly or indirectly impact a safety-critical vehicle control system's operation. When possible, sending safety signals as messages on common data buses should be avoided. For example, providing an ECU with dedicated inputs from critical sensors eliminates the common data bus spoofing problem. If critical safety information must be passed across a communication bus, this information should reside on communication buses segmented from any vehicle ECUs with external network interfaces. A segmented communications bus may also mitigate the potential effects of interfacing insecure aftermarket devices to vehicle networks. Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication scheme to limit the possibility of message spoofing.

9. Log Events

An immutable log of events sufficient to reveal the nature of a cybersecurity attack or a successful breach should be maintained and periodically scrutinized by qualified maintenance personnel to detect trends of cyber-attack.

10. Control Communication to Back-End Servers

Widely accepted encryption methods should be employed in any IP-based operational communication between external servers and the vehicle. Consistent with these methods, such connections should not accept invalid certificates.

11. Control Wireless Interfaces

In some situations, it may be necessary to exert fine-grained control over a vehicle's connection to a cellular wireless network. Industry should plan for and design-in features that could allow for changes in network routing rules to be quickly propagated and applied to one, a subset, or all vehicles.

7.3 Communications and Security Infrastructure for V2V & V2I

NHTSA and its partners are developing a Public Key Infrastructure (PKI) based system, termed the "Security Credential Management System" (SCMS), for ensuring trusted and secure **V2V and V2I communications**. PKI security architectures and methodologies are already used extensively in the auto industry. The SCMS would employ highly innovative methods, encryption, and certificate management techniques to address the challenging task of ensuring trusted communications between entities that previously have not encountered each other—but also wish to remain anonymous (as the case when vehicles/drivers encounter each other on the road) [19]. Communication security has to be guaranteed, as we need the passengers satisfied and the vehicle's services fully operating. The vehicle communicates with the world via V2I and V2V channels. These interfaces are possible attack surfaces, and as previously mentioned, they are vulnerable to a variety of attacks. In order to ensure the secure communication in these channels, they should be mutually authenticated, and the payload suitably protected from unauthorized disclosure or modification. Encryption, monitoring and source identification are some of the prevention techniques that can be used to protect the system from these kinds of exploitations [37]. Apart from the cyber security related to autonomous vehicles we also have to study the behaviour of them on the roads and how they coexist with other connected vehicles.

This is further detailed in NHTSA's publication, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. The safety applications according to the crash type are the following: (Crash Type --> Safety Application).

- Rear-End --> Forward Collision Warning (FCW) & Electronic Emergency Brake Light (EEBL)
- Opposite Direction --> Do Not Pass Warning (DNPW) & Left Turn Assist (LTA)
- Junction crossing --> Intersection Movement Assist (IMA
- Lane change --> Blind Spot Warning & Lane Change Warning (BSW+LCW)

Safety Regulations on Automated Transport

The regulations aim to promote the development and commercialization of safe automated vehicles by prescribing harmonization requirements to be met by "conditional automated driving" or "conditional full automated driving" function as guidelines. The regulations set the safety concept for automated driving for the first time in the world and clarify the significance of the development and commercialization of safe vehicles [26], [27], [28]. The current safety regulations are described next:

1. UNECE (United Nations Economic Commission for Europe) World Forum for Harmonization of Vehicle Regulations (WP.29). The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) is a unique worldwide regulatory forum within the institutional framework of the UNECE Inland Transport Committee. In June 2018 session, a new Working Party was established on Automated/Autonomous and connected Vehicles (GRVA).
2. European Commission & EU Member States (e.g. Germany, France, United Kingdom, Sweden and Netherlands)

EU vehicle approval framework establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles.

"Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive)"

&

"Review of Directive 2007/46/EC: Regulation (EU) 2018/858 of the European Parliament and of the Council"

This Directive contains no technical requirements. In appendix IV, it states that the majority of ECE Regulations are applicable. These regulations are formulated in accordance with the 1958 ECE Agreement – an international treaty that aims to standardise the technical requirements for vehicles and auto parts across borders. An individual ECE Regulation exists for virtually every component of a vehicle, containing the relevant technical requirements.

European Strategy on Cooperative Intelligent Transport Systems (C-ITS) (2016)

Declaration of Amsterdam

In the Declaration of Amsterdam in April 2016, European transport ministers urged the European Commission to develop a European strategy on cooperative, connected and automated vehicles. Indicative initiatives are described next:

- C-ITS Platform
- Gear 2030
- Round Table on Connected and Automated Driving

In more details:

Cooperative Intelligent Transport Systems

Allows road users and traffic managers to share information and use it to coordinate their actions. The C-ITS Deployment Platform [22] is conceived as a cooperative framework including national authorities, C-ITS stakeholders and the Commission, in view to develop a shared vision on the interoperable deployment of C-ITS in the EU. C-ITS are based on technologies which allow vehicles to "talk" to each other, and to the transport infrastructure. In addition to what drivers can immediately see around them, and what vehicle sensors can detect, all parts of the transport system are thus able to share information. For instance, vehicles automatically warn each other of potentially dangerous situations (e.g. emergency braking or end of traffic jam queue) and communicate with local road infrastructure (e.g. optimal speed advice). This improves decision-making, either by the driver or - in the future - by the vehicle itself.

While Intelligent Transport Systems (ITS) focus on digital technologies providing intelligence placed at the roadside or in vehicles, C-ITS focuses on the communication between those systems – whether it is a vehicle communicating with another vehicle, with the infrastructure, or with other C-ITS systems. Hence, it is expected to provide policy recommendations for the development of a roadmap and a deployment strategy for C-ITS in the EU and identify potential solutions to some critical cross-cutting issues. The C-ITS will allow road users and traffic managers to share information and use it to coordinate their actions. This cooperative element – enabled by digital connectivity between vehicles and between vehicles and transport infrastructure – is expected to significantly improve road safety, traffic efficiency and comfort of driving, by helping the driver to make the right decisions and adapt to the traffic situation.

In the frame of supporting the deployment of C-ITS on European roads, there are a number of C-ITS real-life pilot projects funded under Trans-European Transport Networks (TEN-T) and Connecting Europe Facility (CEF)[23] which will create new ITS services for all European road users. These projects will test vehicle-to-infrastructure and vehicle-to-vehicle interactions by using both short-range and cellular communications.

The C-ITS Platform achieved its first milestone towards connected and automated vehicles in the EU. The Commission in consequence prepared the European strategy on Cooperative Intelligent Transport Systems, based on the recommendations of the platform.

Currently, the most promising hybrid communication mix is a combination of ETSI ITS-G5 and existing cellular networks. It combines low latency of ETSI ITS-G5 for time-critical safety-related C-ITS messages with wide geographical coverage and access to large user groups of existing cellular networks.

GEAR 2030

Initiative on artificial intelligence that will support driverless vehicles shared strategy on driverless mobility - GEAR 2030 high level group. The results of the C-ITS platform feed into GEAR 2030, providing it with a transport system perspective.

Round Table on Connected and Automated Driving (CAM)

CAM refers to autonomous/connected vehicles or self-driving cars (vehicles that can guide themselves without human intervention).

Member States, industry and the European Commission collaborate to achieve the EU's ambitious vision for connected and automated mobility in a Digital Single Market, taking into consideration public authorities, citizens, cities and industry interests. These discussions have brought together the industrial players from the digital and automotive sectors to develop joint road maps and establish cross-border deployment actions. Among the main achievements of the Round Table is the creation of the "European Automotive – Telecom Alliance" (EATA) to promote the wider deployment of connected & automated driving.

With the evolution of digital technologies, such as robotics, internet of things, artificial intelligence, high-performance computers and powerful communication networks, vehicles in general, and cars in particular, are quickly changing. Therefore, policies and legislation relating to digital technology, including cybersecurity, liability, data use, privacy and radio spectrum/connectivity are of increasing relevance to the transport sector. These aspects need coordination at the European level in order to ensure that a vehicle may remain connected when crossing borders.

CEF Transport

The Connecting Europe Facility (CEF) for Transport is the funding instrument to realise European transport infrastructure policy. It aims at supporting investments in building new transport infrastructure in Europe or rehabilitating and upgrading the existing one.

7.3.1 Commission strategies and initiatives to support autonomous vehicles

The European Commission has instructed several initiatives and strategies to support the deployment and use of autonomous vehicles. The most crucial ones are explained below [26], [27], [28]:

5th generation of communication networks ("5G")

Enable interconnectivity in vehicle to infrastructure and vehicle to vehicle communication. The industry joined up to create the 5G Automotive Alliance (5GAA) [20] to specifically promote 5G [25] in the automotive sector. A Memorandum of Understanding amongst EATA and 5GAA was signed at the Mobile World Congress [21].

CAR2CAR Consortium

The CAR2CAR consortium [24] focuses on wireless vehicle-to-vehicle (V2V) communication applications based on ITS-G5 and concentrates all efforts on creating standards ensuring the interoperability of cooperative systems spanning all vehicles classes, across borders and brands. The Consortium works in close cooperation with the European and international standardisation organisations like the European Telecommunications Standards Institute (ETSI) and European Committee for Standardisation (CEN).

Space strategy and Galileo services , the European Global Satellite Navigation System (GNSS)

With Galileo, satellites working together with GPS, there are more satellites available, meaning more accurate and reliable positioning for end users. In particular, navigation in cities, where satellite signals can often be blocked by tall buildings, benefits from the increased positioning accuracy that multi-constellation provides.

7.3.2 Automated Vehicles Standards

A detailed list of standards is presented next. These standards are relevant to the global transport technology, transport journey planning and transport ticket/retailing industry.

Formal standards development organisations

The formal development of international standards is organised in three tiers of Standards Development Organisations, recognised by international agreements:

World: International Organisation for Standardisation (**ISO**). International Electrotechnical Commission (**IEC**)

Regional: Regional Standards bodies coordinate standardisation between geographically or politically connected regions with a need to harmonise products and practices. For example, in Europe, the European Committee for Standardisation or **CEN** is active.

National: e.g. Most Nations have a coordinating body responsible for organizing participation in CEN & ISO activities, for publishing ISO & CEN standards within the country, and for coordinating national standardisation activities. The National standards development organisations (SDO) in turn will delegate responsibility as appropriate to the relevant trade associations, government departments and other stakeholders for a specific technical expertise. For example, in the UK, the British Standards Institution or BSI is the National SDO.

The SDOs conduct their work through a system of working groups, responsible for different areas of expertise. These evolve over time to accommodate changes in technology. The key current working groups for transport standards are outlined below.

EUROPE

Transmodel [18], [32], [35] (formally CEN TC278, Reference Data Model For Public Transport, EN12896) is the CEN European Reference Data Model for Public Transport Information; it provides a conceptual model of common public transport concepts and data structures that can be used to build many different kinds of public transport information system, including for timetabling, fares, operational management, real time data, journey planning etc.

CEN divides its work into committees covering different aspects of industry and technology, with a well-defined process and documentation formats. Related CEN standards:

- **OpRa** is produced by Technical Committee 278 (TC278), Working Group 3 (WG3), Sub-Group 10 (SG10) [34]. Other TC278 WG3 sub-groups handle the related standards:
- Transmodel (SG4)

- **SIRI** – Service interface for Real-time Information, EN 15531 1-4 & CEN TS 15531-5 (SG7)
- **NeTEx** – Network Timetable Exchange, CEN TS 16614 1-3 (SG9) [33]

Transmodel may be applied to any framework for information systems within the public transport industry, but there are three circumstances to which it is particularly suited:

- specification of an organisation's 'information architecture';
- specification of a database;
- specification of a data exchange interface.

The Reference Data Model (Transmodel v6) covers the following data domains:

- Network Description: routes, lines, journey patterns, timing patterns, service patterns, scheduled stop points and stop places: this part corresponds to the network description as in Transmodel V5.1 extended by the relevant parts of IFOPT (EN28701);
- Timing Information and Vehicle Scheduling: runtimes, vehicle journeys, day type-related vehicle schedules;
- Passenger Information: planned and real-time;
- Operations Monitoring and Control: operating day-related data, vehicle follow-up, control actions;
- Fare Management: fare structure and access rights definition, sales, validation, control of access rights and/or travel documents;
- Management Information and Statistics including data dedicated to service performance indicators;
- Driver Management:
- Driver Scheduling: definition of day-type related driver schedules,
- Rostering: ordering of driver duties into sequences according to some chosen methods,
- Driving Personnel Disposition: assignment of logical drivers to physical drivers and recording of driver performance.

Service Interface for Real Time Information

The Service Interface for Real Time Information or SIRI is an XML protocol to allow distributed computers to exchange real time information about public transport services and vehicles. The protocol is a CEN norm, developed originally as a technical standard with initial participation by France, Germany (Verband Deutscher Verkehrsunternehmen), Scandinavia, and the UK (RTIG). SIRI is based on the CEN Transmodel abstract model for public transport information, and comprises a general purpose model, and an XML schema for public transport information.

Identification of Fixed Objects in Public Transport

IFOPT (Identification of Fixed Objects in Public Transport) is a CEN Technical Specification that provides a Reference Data Model for describing the main fixed objects required for public access to Public transport, that is to say Transportation hubs (such as airports, stations, bus stops, ports, and other destination places and points of interest, as well as their entrances, platforms, concourses, internal spaces, equipment, facilities, accessibility etc.). Such a model is a fundamental component of the modern Public transport information systems needed both to operate Public transport and to inform passengers about services.

UK

Transport Direct

The Transport Direct Programme was a division of the *UK Department* for Transport (DfT) to develop standards, data and better information technology systems to support public transport. It has developed and operates the Transport Direct Portal which is a public facing multi-modal journey planner. It also supports the creation and management of comprehensive databases of all public transport movements in the United Kingdom with Traveline.

A number of data standards were developed to support the collection, transfer and management of the required transport data:

- CycleNetXChange: a UK data protocol for exchanging information about infrastructure to support the development of a national cycle journey planning function within the Transport Direct Portal.
- JourneyWeb: a protocol to allow the development of a distributed journey planning service (which became the Transport Direct Portal).
- NaPTAN: for the exchange of information associated with bus stops, railway station and other public transport access point.
- NPTG: for the exchange of information about places and points of interest.
- TransXChange: a UK data protocol for the exchange of public transport schedules

7.4 Adaptive Ethics for autonomous vehicles

AVs are supposed to eradicate human error in crash situations and make the road safer. Nevertheless, the rate of crashes will not equate to zero. Firstly, AVs would still be dealing with non-AVs or occasionally human-driven AVs and secondly, irrespective of how complete the autonomous level is, pedestrians will always be present in any transport system. Therefore, AVs must be pre-programmed with various responses in crash conditions [31]. Many ethical issues are encountered when considering how to pre-program AVs in the event of various crash scenarios.

Below are some ethical complexities using two such scenarios:

Scenario (1) Imagine an AV is on its way down the road when it suddenly encounters another car containing two occupants, which has proceeded through or run a red light. A fatal crash is inevitable. The AV has two options: (i) press the brake pedal and hit the guilty car; or (ii) turn the wheel to the road side and brake where there is a pedestrian waiting for a green light to cross the intersection. The dilemma is whether to kill one innocent person (the pedestrian) or the two persons in the offending vehicle (including the driver who knowingly ran the red light).

Scenario (2) Consider the same circumstances as in Scenario (1), but this time, the pedestrian has been removed from the equation. Now the AV has the choice to turn the wheel to the road side and collide with a lamp post. Unfortunately, the AV does not have comprehensive insurance; rather it only has third party insurance. The two options available to the AV are as follows: (i) Hit the car knowing that the damage will be compensated by the insurance of the offending vehicle. While the AV will be replaced, the human toll is two lives, yet there will be no liability placed upon the AV.

Option (ii) is to hit the lamppost. While no lives will be lost, the offending vehicle will escape with no liability resulting in no compensation avenues open to the AV.

Ethics of Crashing

Human drivers may often make poor decisions during and before crashes. Humans must overcome severe time constraints, limited experience with their vehicles at the limits of handling, and a narrow cone of vision. While today has automated vehicles also have somewhat limited sensing and processing power, the focus is on advanced vehicles with near-perfect systems. If even perfect vehicles must occasionally crash, then there will always be a need for some type of ethical decision-making system. These advanced automated vehicles will be able to make pre-crash decisions using sophisticated software and sensors that can accurately detect nearby vehicle trajectories and perform high-speed avoidance maneuvers, thereby overcoming many of the limitations experienced by humans. If a crash is unavoidable, a computer can quickly calculate the best way to crash based on combination of safety, likelihood of outcome, and certainty in measurements, much faster and with greater precision than a human can. The computer may decide that braking alone is not optimal, since at highway speeds it is often more effective to combine braking with swerving, or even swerving and accelerating in an evasive maneuver. One major disadvantage of automated vehicles during crashes is that, unlike a human driver who can decide how to crash in real-time, an automated vehicle's decision of how to crash was defined by a programmer ahead of time. The automated vehicle can interpret the sensor data and make a decision, but the decision itself is a result of logic developed and coded months or years ago. This is not a problem in cases where a crash can be avoided—the vehicle selects the safest path and proceeds. However if injury cannot be avoided, the automated vehicle must decide how best to crash. In the example, an automated vehicle is travelling on a two-lane bridge when a bus travelling in the opposite direction suddenly veers into its lane. The automated vehicle must decide how to react using whatever logic has been programmed in advance. There are three alternatives: A. Veer left and off the bridge, guaranteeing a severe one-vehicle crash. B. Crash head-on into the bus, resulting in a moderate two-vehicle crash. C. Attempt to squeeze pass the bus on the right. If the bus suddenly corrects back towards its own lane—a low-probability event given how far the bus has drifted—a crash is avoided. If the bus does not correct itself—a high-probability event—then a severe two-vehicle crash results. This crash would be a small offset crash, which carries a greater risk of injury than the full frontal collision in alternative B. It is important to note that these outcomes can only be predicted by the automated vehicle, and are not certain. The automated vehicle's path planning algorithm would have to quickly determine the range of possible outcomes for each considered path, the likelihood of those outcomes occurring, and the algorithm's confidence in these estimates based on quality of sensor data and other factors.

Designing an Ethical Vehicle

There has been little discussion of the legal and moral implications of automated vehicle decision-making during unavoidable crashes. Most of the research in moral machines have focused on military applications or general machine intelligence. A relatively recent area of study is machine ethics, which focuses on the development of autonomous machines that can exhibit moral behavior when encountering new situations.

Safety

Safety is the most fundamental requirement of autonomous cars. The central question is then: how should a self-driving car be tested? What guidelines should be fulfilled to ensure that it is safe to use? For self-driving cars, standards are under development, based on experience. Google Car tests show one million kilometres without any accident, is this a measurement to certify its software? The source codes of autonomous cars are typically commercial and not publicly available. One possibility to assure code correctness via independent control. Should there be an independent organization to check those? However, could it actually be checked? Who else than the developers at a car manufacturer or supplier will understand such a complex system? An alternative route seems to be preferred by legislators – instead of control of the software, which is in the domain of the producers, legislation focus on behaviour that is being tested, based on the "Proven in Use" Argument. When it comes to hardware and hardware-software systems, there have been discussions about the prices of laser radars compared to cameras or ultra-sonic sensors. The economic aspects might be seen as the highest priority. Using cheap equipment might lead to wrong decision-making and in a self-driving car, it would be impossible to interfere with the decisions made. Assuming that wrong decisions may lead to a loss of human lives or property, having chosen a cheap component could therefore be ethically unacceptable.

Security

For autonomous cars, security is of paramount importance, and software security is a fundamental requirement. There have been a number of attacks at car systems and sensors (e.g., LIDAR and GPS) that were used to manipulate the cars behavior. Attacks might be inevitable, but should there be a minimum-security threshold to allow a self-driving car to be used? This leads to another question: How secure must the systems and the connections be? What about security issues and software updates? Should a self-driving car be allowed to drive, when it does not have the latest software version running? What about bugs in the new software? Should the vehicle be connected or should the vehicle be completely disconnected? Moreover, connected vehicles might receive information from other systems that will enhance the understanding of the reality, thus opening new and promising safety scenarios. Imagine, for instance, a pedestrian on the side of a building, totally invisible to the instrumentations of the car, that is approaching a cross and that will most probably have an impact with the vehicle.

Privacy

The more information taken into consideration for the decision making, the more it might interfere with data and privacy protection. For example, a sensor that detects obstacles, such as human beings in front of the car is based on visual information. Even the use of a single sensor could invade privacy, if the data is recorded/reported and/or distributed without the consent of the involved people. The general question is: How much data is the car supposed to collect for the decision making? Who will access those data? When will these data be destroyed? What about using active signals by devices people carry around to detect moving obstacles in front or near the car? What about people who do not carry such devices? Would they more likely be hit by the self-driving car, because they were not “present enough” in the data?

Trust

Trust is an issue that appears in various forms in autonomous cars e.g. in production (when assembled, trust is the requirement for both hardware and software components) as well as in zhe use of the car. A human might define where the car has to go, but the self-driving car will make the decisions on how to get there, following the given rules and laws. However, the self-driving car might already distribute data like the target location to a number of external services, such as traffic information or navigation data, which are used in the calculation of the route. Nevertheless, how trustworthy are those data sources e.g., GPS, map data, external devices, other vehicles?

Transparency

The transparency is of central importance for many of the previously introduced challenges. Without transparency, none of them could be analysed, because the important information would be missing. It is a multi-disciplinary challenge to ensure transparency, while respecting e.g., copyright, corporate secrets, security concerns and many other related topics. How much should be disclosed, and disclosed to whom? The car development ecosystem includes many other companies acting as suppliers that produce both software and hardware components. Should the entire ecosystem be transparent? In addition, to whom should it be transparent? How to manage the intellectual property rights?

Reliability

One of the basic questions is: How reliable is the cell network? What if there is no mobile network available? What if sensor(s) fail? Should there be redundancy for everything? Is there a threshold that determines when the car is reliable, e.g., when two out of four sensors fail? In connected vehicles, there are different levels that should be considered for reliability purposes. First the diagnostic of the vehicle that might be subject to failures. Then, the vehicle sensors that enable the vehicle to sense the surrounding environment of the vehicle. Finally, the data coming from external entities, like other vehicles and road infrastructures. Reliability approaches should consider all these levels.

Responsibility and Accountability

In the case of autonomous cars, responsibility will obviously be redefined. The question is how responsibility will be defined in case of incidents and accidents.

Quality Assurance Process

Detailed Quality assurance programs covering all relevant steps must be developed in order to ensure high quality components. The question is also how the decision making is going to be implemented. How to ensure overall quality of the product? What about the lifetime of components? How will maintenance be organized and quality assured? When car manufacturers follow a non-transparent process of software engineering, how could anyone make sure that the car follows a certain ethical guideline? Whose responsibility will it be that car software follows ethical principles?

All these questions are open ethical issues that must be addressed during the next years. The AVENUE project will endeavour to contribute to the tackling of these topics, based on the feedback from the pilot sites that will be gathered during the evaluation phase of the project.

8 References

8.1 References Chapter 6

0302, Project Team. 2016. Downloads. *transmodel-cen.eu.* [Online] August 2016. http://www.transmodel-cen.eu/downloads.

—. 2017. *Use of UML Transmodel - Public Transport Reference Data Model.* s.l. : transmodel-cen.eu, 2017.

APTA Standard for Transit Communications Interface Profiles - Annexes F - K. **APTA.** Vol. IV. 4.1.1.

APTA Standard for Transit Communications Interface Profiles - Narrative. **APTA.** Vol. 1. 4.1.1.

CEN. 2015. *Annex 1 - Project Plan.* 2015.

—. 2016. Implementations. [Online] 2016. http://www.transmodel-cen.eu/implementations.

—. 2009. NeTex. [Online] 2009. https://github.com/NeTEx-CEN/NeTEx.

Countries, CEN Transmodel -. 2014. CEN Transmodel . [Online] 2014. http://www.transmodel-cen.eu/implementations/countries.

Norway, CEN Transmodel. 2018. [Online] 2018. http://www.transmodel-cen.eu/implementations/norway.

Official Website, NeTEx. 2014. CEN NeTEx. [Online] 2014. http://netex-cen.eu/?page_id=14.

TCIP Data and Dialog Definitions. **APTA.** APTA TCIP-S-001 4.1.1, Vol. II.

TCIP XML Schema. **APTA.** Vol. III. 4.1.1.

8.2 References Chapter 7

[1] D. Warren, H. Clarke, J. Burger, V. Paxton, "Is Cyber Security The Greatest Threat For Autonomous Vehicles?", 10 August 2018; Available online at: https://www.corrs.com.au/thinking/insights/is-cyber-security-the-greatest-threat-for-autonomous-vehicles/

[2] Mark Lin, An Overview of Session Hijacking at the Network and Application Levels, 2005, Available online at: https://www.sans.org/reading-room/whitepapers/ecommerce /overview-session-hijacking-network-application-levels-1565

[3] Simon Parkinson, Paul Ward, Kyle Wilson, Jonathan Miller, “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges”, 6 March 2017; Available online at: https://ieeexplore.ieee.org/abstract/document/7872388

[4] A.Chattopadhyay, K.Y. Lam, "Autonomous Vehicle: Security by Design", 1 October 2018; Available online at: https://arxiv.org/pdf/1810.00545.pdf

[5] Tom Carlson, “Information Security Management: Understanding ISO 17799”, September 2001

[6] Vrizlynn L.L. Thing and Jiaxi Wu, “Autonomous Vehicle Security: A Taxonomy of Attacks and Defences,” 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), May 2016

[7] Sandeep Bhatt, Pratyusa K. Manadhata and Loai Zomlot, “The Operational Role of Security Information and Event Management Systems,” Oct. 2014

[8] "The Directive on security of network and information systems (NIS Directive)", 24 August 2018; Available online at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[9] "The key principles of vehicle cyber security for connected and automated vehicles", 6 August 2017; Available online at: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

[10] C. Schmittner, Z. Ma, "Using SAE J3061 for Automotive Security Requirement Engineering," September 2016; Available online at: https://www.researchgate.net/publication/307585960_Using_SAE_J3061_for_Automotive_Security_Requirement_Engineering

[11] Vehicle Electrical System Security Committee, "Requirements for Hardware-Protected Security for Ground Vehicle Applications", 17 January 2012; Available online at: https://www.sae.org/standards/content/j3101/

[12] "Vehicle Cybersecurity"; Available online at: https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

[13] "Cybersecurity Framework"; Available online at: https://www.nist.gov/cyberframework

[14] "Cybersecurity Best Practices for Modern Vehicles", October 2016; Available online at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[15] IT Advisory KPMG China, "Overview of China's Cybersecurity Law', February 2017; Available online at: https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

[16] H. Huifeng, "Cybersecurity law causing 'mass concerns' among foreign firms in China", 1 March; Available online at: http://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china

[17] T. Srikanthan, "Commentary: Cybersecurity is the next economic battleground", 2 april 2017; Available online at: http://www.channelnewsasia.com/news/singapore/commentary-cybersecurity-is-the-next-economic-battleground-8591642

[18] CEN European reference data model for public transport information, Available online at: http://www.transmodel-cen.eu/

[19] S.A. Bagloee, M.Tavana, M.Asadi, T.Oliver, "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies", December 2016; Available online at: https://link.springer.com/article/10.1007/s40534-016-0117-3

[20] Automotive Association, Available online at: http://5gaa.org/

[21] Mobile World Congress, Available online at: https://www.mwcbarcelona.com/

[22] C-ITS Deployment Platform, Available online at: https://ec.europa.eu/transport/themes/its/c-its_en

[23] Connecting Europe Facility, Available online at: https://ec.europa.eu/transport/themes/infrastructure/ten-t-guidelines/project-funding/cef_en

[24] Communication Consortium, Available online at: https://www.car-2-car.org/

[25] 5G: The Future of Communications Networks, Available online at: http://theinstitute.ieee.org/technology-topics/communications/5g-the-future-of-communications-networks

[26] European Commission, "Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee, The Committee Of The Regions - On the road to

automated mobility: An EU strategy for mobility of the future", 17 May 2018; Available online at: https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf

[27] European Commission, "Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility", 30 November 2016; Available online at: https://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

[28] European Commission, "Intelligent transport systems Innovating for the transport of the future"; Available online at: https://ec.europa.eu/transport/themes/its_en

[29] H.Figg, C.Lutz, N.Asselin-Miller, P.Wells, S.Amaral, G.Horton, D.Sheldon, M.Flaute, "GEAR 2030 Strategy 2015-2017 Comparative analysis of the competitive position of the EU automotive industry and the impact of the introduction of autonomous vehicles : final report - Study", September 2017; Available online at: https://publications.europa.eu/en/publication-detail/-/publication/24c9ad0e-da38-11e7-a506-01aa75ed71a1/language-en/format-PDF/source-52926290

[30] "Connected and automated mobility in Europe", 25 February 2019; Available online at: https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe

[31] Wikipedia, Transmodel 5 October 2018; Available online at: https://en.wikipedia.org/wiki/Transmodel

[32] Public Transport Reference Data Model; Available online at: http://www.transmodel-cen.eu/

[33] NeTEx - CEN Technical Standard; Available online at: http://netex-cen.eu/?page_id=111

[34] OpRa - CEN initiative; Available online at: http://www.opra-cen.eu/

[35] Standard Interface for Real-time Information (SIRI); Available online at: http://www.transmodel-cen.eu/standards/siri/

[36] T.Holstein, G.Dodig-Crnkovic, P. Pelliccione “Ethical and Social Aspects of Self-Driving Cars”, 5 February 2018; Available online at: https://arxiv.org/pdf/1802.04103.pdf

[37] Te-Shun Chou, “Security Threats On Cloud Computing Vulnerabilities”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013