Grant Agreement Number: 731993

Project acronym: AUTOPILOT

Project full title: AUTOmated driving Progressed by Internet Of Things

D.4.2

Initial Technical Evaluation

Due delivery date: 30/06/2018

Actual delivery date: 29/06/2018

Organization name of lead participant for this deliverable: IDIADA

Dissemination level		
PU	Public	
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential , only for members of the consortium (including the GSA)	X

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

Document Control Sheet

Deliverable number:	4.2
Deliverable responsible:	IDIADA
Work package:	WP4
Editor:	IDIADA

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Alexander Velizhev	IBM-RE	ave@zurich.ibm.com
Anton Dekusar	IBM-IE	ADekusar@ie.ibm.com
Bart Netten	TNO	Bart.netten@tno.nl
Carlotta Firmani	THALES	carlotta.firmani@thalesgroup.com
Filippo Visintainer	CRF	Filippo.visintainer@crf.it
Georgios Karagiannis	HUAWEI	georgios.karagiannis@huawei.com
Gurkan Solmaz	NEC	gurkan.solmaz@neclab.eu
Haibo Chen	UNL	h.chen@its.leeds.ac.uk
Jordi Pont	IDIADA	Jordi.pont@idiada.com
Jos Den Ouden	TUE	j.h.v.d.ouden@tue.nl
Juan Villar	CTAG	Juan.villar@ctag.com
Liuxin Walle	HWC	walle.liuxin@huawei.com
Lorenzo Viola	HUA	lorenzo.viola.ext@huawei.com
Louis Touko Tcheumadjeu	DLR	Louis.toukotcheumadjeu@dlr.de
Martin David	GEMALTO	martin.david@gemalto.com
Moises Rial	CTAG	Moises.rial@ctag.com
Pablo Dafonte	CTAG	Pablo.dafonte@ctag.com
Robert Kaul	DLR	robert.kaul@dlr.de
Rosa Blanco	CTAG	Rosa.blanco@ctag.com
Rubén Heras	IDIADA	Ruben.heras@idiada.com
Thomas Reschka	CET	Thomas.Reschka@cetecom.com

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.1	14/03/2018	Structure of the document	IDI
V0.2	09/04/2018	Added content for Introduction and Technical Evaluation methodology	IDI
V0.3	10/04/2018	Privacy contribution from GEM	GEM
V0.4	18/04/2018	Added content for Position and Navigation and Safety	IDI
V0.5	03/05/2018	Replicability contribution from TUE	TUE
V0.6	08/05/2018	Security contributions from THA	THA
V0.7	09/05/2018	Privacy contributions from GEM	GEM
V0.8	11/05/2018	Car Rebalancing contributions from HUA, TUE and NEC	HUA, TUE, NEC
V0.9	14/05/2018	Added content for data management, interoperability and	IBM-RE, IBM-IE

		car sharing sections	
V0.10	30/05/2018	Contribution to Executive summary, Introduction and Technical Evaluation Methodology	TNO
V0.11	06/06/2018	Platooning contribution	TNO
V0.12	07/06/2018	Update data management and interoperability	IBM-RE, IBM-IE
V0.13	08/06/2018	Added content for sustainability	DLR
V0.14	11/06/2018	Added content for Environmental Detections and Replicability	TUE
V0.15	13/06/2018	Final contribution to Position and Navigation, Safety and add Annex 2	IDI
V0.16	13/06/2018	Contribution to AVP	DLR
V0.17	14/06/2018	Contribution to Highway Pilot	CRF
V0.18	14/06/2018	Conclusions, Abstract and general comments	IDI
V0.19	15/06/2018	Updates on Annex 2, Environmental Detections, Replicability, Sustainability, Interoperability and Car Rebalancing	UNL,TUE,IBM,DLR
V0.20	15/06/2018	Contribution to Data Communication	TNO
V0.21	15/06/2018	Contribution to Urban Driving and Data Management	CTAG
V1.0	15/06/2018	Version for peer review	IDI
V1.1	27/06/2018	Remarks and editions for last version	TNO
V1.2	28/06/2018	Final version	IDI
V2.0	29/06/2018	Final for submission to EC	ERTICO

Abstract

This document presents the methodology that will be used to evaluate the IoT technologies applied to the autonomous vehicles in the different Pilot Sites. The definition of this methodology was started in D4.1 and is fully developed in this deliverable. D4.2 defines the technical research questions, hypotheses, key performance indicators (KPI) and measurements to evaluate the Use Cases and Services implemented at the Pilot Sites. The methodology aims to evaluate the added value of IoT for connected and automated driving functions and services in a common approach across pilot sites and use cases. Essential in this approach is to evaluate topics that are common to the piloted systems and services; IoT data management, data communication, positioning, localisation, navigation, and environmental detections. Furthermore, the methodology is defined for the assessment of the safety of the IoT enabled vehicles, and the interoperability, replicability and sustainability of the IoT architectures, and the security and privacy of the IoT enabled solutions.

Legal Disclaimer

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

Abbreviations and Acronyms

Acronym	Definition
CAD	Connected and Automated Driving
CEMA	Crowdedness Estimation Multimodal Actors
CO_2	Carbon Dioxide
COTS	Commercial off-the-shelf
CSV	Comma-Separated Values
EC	European Commission
FMS	Fleet Management System
GA	Grant Agreement
GMT	Greenwich Mean Time
GPS	Global Positioning System
HD-Maps	High Definition Maps
HY	Hypotheses
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LIDAR	Light Detection and Ranging
MAC	Mandatory Access Control
MAV	Micro Air Vehicle
MCA	Micro Channel Architecture
MITM	Man In The Middle
PO	Project officer
RADAR	Radio Detection And Ranging
RQ	Research Question
RTK	Real Time Kinematic
SQL	Structured Query Language
UA	User Acceptance
UAC	User Account Control
UTC	Universal Time Coordinated
WP	Work Package
XML	eXtensible Markup Language

Table of Contents

List of Figures

List of Tables

Executive Summary

The aim of the AUTOPILOT project is to bring together knowledge and technology from the automotive and the Internet-of-Things (IoT) value chains in order to develop IoT-architectures and platforms that will advance autonomous driving (AD) in a connected environment in order to assess how IoT can improve AD functionalities and services. AUTOPILOT will develop new automated driving services by connecting automated driving equipped vehicles over IoT. The services being developed will accelerate, enhance or enable fully autonomous driving.

The resulting system consisting of several Internet of Things Platforms and its connected devices needs to be evaluated from a technical point of view. This document presents the methodology for evaluating several technical topics – functionality, performance, safety, security and privacy, replicability, sustainability and interoperability – related to AUTOPILOT's use of IoT technologies for advancing AD.

AUTOPILOT Deliverable D4.1 [1] – presented the overall "Methodology for Evaluation" as a common approach to technical evaluation and the assessment of the impact on business, quality of life and user acceptance. This deliverable fully defines the technical evaluation starting from the D4.1 common approach (D4.1 section 5) and hypotheses, indicators and measurements (D4.1 Annex 1), pilot scenarios (D4.1 section 9), the data provisioning and quality (D4.1 section 10), the data requirements (D4.1 Annex 2) and the data that has been agreed to be provided by the pilot sites in cooperation with WP2 and WP3. Given the diversity of implementations in the different Pilot Sites, an effort has been made to define KPIs and measurements that can be carried out in all the Pilot Sites in order to achieve an evaluation that allows for a fair comparison of the implementations. This has required an effort in the coordination with the different pilot sites and, in some cases, it was necessary to adapt some measurements in order to achieve this goal.

This document will be updated in M34 in deliverable D4.3: *Final Technical Evaluation*. D4.3 will present the outcome of the activities carried out in T4.2 and provide both the data from the final results of technical evaluation at the pilot sites and the proved enhancements which IoT offers to connected and automated driving.

1 Introduction

1.1 Purpose of the document

The AUTOPILOT project brings together knowledge and technology from the automotive and the Internet-of-Things (IoT) value chains in order to develop IoT-architectures and platforms that will advance autonomous driving (AD) in a connected environment. As a potential disruptive technology, IoT brings the possibility to tackle a number of technical challenges for automated driving functions and services.

D4.2 - *Initial Technical Evaluation*- aims to present the methodology that will be used to evaluate the IoT technologies applied to the autonomous vehicles in the different Pilot Sites. The definition of this methodology was started in D4.1 [1] and is fully developed in this document. D4.2 sets the KPIs with needed measurements to compute them, used to evaluate the Use Cases and Services implemented at the Pilot Sites once the pilot test iterations begin. Furthermore, it sets the methodology for the assessment of the developed IoT systems safety, the interoperability, replicability and sustainability of the IoT architectures, and the security and privacy of the solutions.

This document will be updated in M34 in deliverable D4.3: *Final Technical Evaluation*. D4.3 will present the outcome of the activities carried out in T4.2 and provide the data from the final results of the technical evaluations at the pilot sites.

1.2 Intended audience

The Technical Evaluation concerns all the WPs because it will show the way in which the use cases and services developed by all the project beneficiaries will be technically evaluated.

D4.2 is a public deliverable and also of potential interest to an external audience concerned with the technical implications of IoT and/or AD or with evaluation methodologies.

However, this is an initial technical evaluation document and should be considered as a working document.

1.3 Terminology

User
Users are understood here in a wide definition as "*anyone who uses the AUTOPILOT services*". This definition is congruent with the approach taken in the unpublished position paper by the CARTRE thematic interest group.

Other road users
Road users that are indirectly affected by the use of the technology (i.e. in the single use cases), e.g. cyclist, pedestrian, drivers of conventional vehicles.

Position
Absolute position of an object in WGS'84 or GPS coordinates in latitude, longitude, and optionally with an altitude.

Location
Relative position of an object on the road defined by lane number, lateral road or lane offset, and optionally with a map matched position with a longitudinal offset to a road reference point, or road identifier

Measure
Parameter or property intended to be measured in a unit.

Measurement
Operation to determine the value or quantity of a measure at a given time.

1.4 Structure of the report

Chapter 1 introduces the purpose of the document, the intended audience, the terminology used in the document and the structure of the report.

Chapter 2 details the methodology used for technical evaluation in AUTOPILOT. It is divided in four parts devoted to the definition of what are: 1) the topics that will be used to evaluate the use cases and services, 2) research questions and hypotheses derived from the topics, 3) indicators and measurements used to answer the research questions, and 4) test scenarios to be reproduced at the Pilot Sites in order to obtain the data needed to compute the indicators.

Chapter 3 defines the methodology for evaluating each topic. It will collect a set of research questions and hypotheses to fully cover the topic in each of the use cases. It will also list both the indicators and measurements to evaluate the hypotheses mentioned before. The topics for the evaluation are: Data Management, Data Communication, Positioning, Localisation and Navigation, Environmental Detections, Safety, Security and Privacy, Replicability, Sustainability and Interoperability.

Chapter 4 provides the methodology to evaluate each use case or service with reference to all the topics described in the previous section. The use cases and services are: Automated Valet Parking, Urban Driving, Highway Pilot, Platooning, Car Sharing and Car Rebalancing.

Chapter 5 presents the conclusions obtained by the elaboration of the evaluation methodology.

2 Technical Evaluation methodology

2.1 What is the added value of IoT for Automated Driving?

The objectives of the AUTOPILOT project are to define and implement an IoT architecture for Automated Driving (AD), and to realize IoT-based AD use cases. The main research question to answer in the evaluations of the pilots is "What is the added value of IoT for Automated Driving in the piloted Use Cases?" The main hypotheses to test, qualify and quantify the added value are:

- IoT is *accelerating* the development and deployment of automated driving functions.
- IoT is *enhancing* the functionality or performance of automated driving functions.
- IoT is *enabling* new automated driving functions.

Potentially IoT devices can provide information on other vehicles, emergency and heavy good vehicles, stationary and illegally parked vehicles, etc. IoT devices may also provide information on vulnerable road users such as pedestrians, bicyclists and motorbikes, or wheel chairs. A vehicle's host sensors and ITS-G5 communication can also provide similar information within the range of the sensors or communication. 'Similar' is interpreted as information of similar type, contents and quality. IoT can accelerate for example with a cheaper solution, by increasing the penetration rate of probed devices, or extending the 'range of view' for *similar* information.

If the quality or contents of IoT data is better than existing data, then the AD functionality can be enhanced, and performance can be improved. IoT data may provide more information directly from other road users or obstacles for example, or may provide more accurate positioning, localisation or navigation information.

Whether IoT or IoT data is accelerating or enhancing AD may not always be clear to distinguish a priori. It depends on the existing equipment and infrastructure of use case implementations, which may differ between pilot sites for example. The evaluations should test and classify this later. Fortunately, similar test scenarios can be defined for both types of hypotheses; with a baseline scenario for the existing situation without IoT data, and comparative evaluations of test scenarios with IoT data.

The third type of hypotheses requires different test scenarios as the pilot system can only be tested with IoT data source to enable new automated driving functions and services. Hence the added value of IoT can be assessed on feasibility for example. A baseline scenario without IoT would not be meaningful or executable, and a comparative evaluation against a 'without IoT' baseline is not possible.

2.2 Topics of the evaluation

All Automated Driving functions and services use technologies that can potentially be improved by using IoT provided data. These common technologies are called topics in the evaluation methodology developed in this document. This chapter introduces the main topics that will be used for the Technical Evaluation, which have been chosen to cover the technologies used in the developed use cases and services. A differentiation is done between the topics to be evaluated (data management, data communication, position and navigation, environmental detections, replicability, sustainability and privacy) and the topics to be assessed (safety, interoperability and security) should be differentiated.

The **Data Management** refers to the capability of IoT devices, such as the automated vehicles being tested, to manage the data needed for the automated driving functions and services. ***Data management on an in-vehicle IoT platform*** includes the processes to discovery relevant IoT data sources, to subscribe and process relevant IoT data including the assessment of the quality or the data and fusion with on-board sensor data, and to manage alternative communication channels to search and retrieve required data. ***Data management on a cloud-based IoT platform*** includes device and subscription management, the up and down loading of data from IoT devices, data brokering, discovery services, data aggregation services, (semantic) data transformations to data formats requested by automated vehicles, and the interaction with other IoT cloud services and (federated) platforms.

The **Data Communication** functionality is provided through alterative communication modes and media. Technical evaluation will focus on the performance comparison of alternative communication channels for ***Ad-hoc V2X communication*** and ***Vehicle – IoT Platform communication***. The objective is evaluating the realized communication performances in each of these situations and proposing feasible performance levels.

The **Position and Navigation** compares the information related to RTK-GPS, HD maps, parking spots information or routes received by IoT cloud services with the existing vehicle sensors and maps data. The objective is to evaluate the improvement of the internal state, motion planning and routing within automated vehicle functions and services. **Localisation** and navigation is evaluated on accuracy for determining the relative position on the road; i.e. the longitudinal and lateral position on a road and in a lane.

The **Environmental detections** refer to the capability of IoT Platforms to acquire information from the environment, such as obstacles and road hazards, other road users, traffic information and environmental conditions. From a technical perspective environmental data may enhance or enable environmental detections for example for VRU or pothole detection, traffic control and status. Potential improvements in detection performance can be measured for example by the type of environmental objects, detection accuracy, rate, and delay, and the geographic position, location and coverage of detections.

Safety has a very high importance in the project and is considered in many of the development and deployment phases. Obviously, the use of IoT data may affect the **Safety** of automated driving and, therefore, any incidents should be reported, investigated and assessed.

The **Privacy** will be assessed from multiple points of view to ensure that a correct approach has been followed. Relevant issues to this respect are that the user tracking possibilities are limited to a minimum, the project is compliant to GDPR regulation and an appropriated level of privacy is perceived by the end users, in order to ensure that the project is well accepted. The **Security** will be assessed concerning the most common security threats related to IoT.

The three topics of Replicability, Sustainability and Interoperability will be assessed together. The **Replicability** is the feasibility to deploy one use case or service developed in a given Pilot Site in another Pilot Site. To that aim, the higher the standardization level in the development of the use case or service, the more feasible should it be to replicate it. For this reason, replicability is strongly related to standardization. Therefore, taking as input the level of standardization of Pilot Sites and the related developments, the goal of the replicability assessment is to assess the feasibility of replicating use cases and services between Pilot Sites. The **Sustainability** is the process of using resources, technological innovation and investments in a balanced manner to the benefit of humankind and the environment. Sustainable Development has been defined by the “Brundtland Report” of the World Commission on Environment and Development stating “to meet the needs of the present without compromising the ability of future generations to meet their own needs” [2]. This concept has been structured in a technical way as described in section 3.8. The **Interoperability** topic will assess the different IoT technologies and IoT architectures between the Pilot Sites. For example, the vehicles used to evaluate the Versailles Pilot site will also be tested on Brainport to evaluate their use cases.

2.3 Technical Research Questions and Hypotheses

The formulation of research questions is an elaborate and iterative process; taking both a top-down approach (start with impact areas) and bottom-up (start with use-cases). More precisely, on AUTOPILOT project, the research questions are focused on how IoT could offer potential improvements to automated driving functions or driving modes, and how could enable services involving connected and automated vehicles. Consequently the possible ways in which IoT can improve AD, namely by Accelerating, Enhancing or Enabling new services or automated driving functions are defined. This distinction helps to focus on the future benefits of deploying automation, and steers away from the specific implementation and testing of functions. When accelerating, the IoT is improving the AD deployment or the business case; when enhancing, IoT is improving AD functionality or performance and when enabling, the IoT is adding new AD functionalities.

From research questions hypotheses can be formulated. The definition of a hypothesis is: "A specific statement linking a cause to an effect and based on a mechanism linking the two. It is applied to one or more functions and can be tested with statistical means by analysing specific performance indicators in specific scenarios. A hypothesis is expected to predict the direction of the expected change."[1]

A large number of research questions and hypotheses have been generated during the first year of the project in Deliverable D4.1 [1]. A limited set of research questions and hypotheses from Annex 1 in [1] able to cover the entire project technical scope has been selected[2].

2.4 Technical indicators, measurements and metrics

The indicators are quantitative or qualitative indicators, derived from one or several measures, agreed on beforehand, expressed as a percentage, index, ate or other value, which are monitored at regular or irregular intervals and can be compared to one or more criteria. During the process of developing hypotheses, it is important to choose appropriate indicators that will allow answering the hypotheses, being also obtainable within the budget and other limitations of the project. Performance indicators are based on measures.

On basis of the previous steps, it can be determined what needs to be measured and how, e.g. collect background data, logging data from sensors and application software, and questionnaires. In FESTA, all the data sources mentioned are considered sensors. Subsequently all data can be acquired, stored, and processed in a generalised way.

A spreadsheet with the minimum data requirements and data quality to be accomplished by the Pilot Sites (Annex 2 of [1]) has been defined.

2.5 Test scenario, use cases and services definition

A Pilot Plan has been defined[3] in [3] in order to group in one spreadsheet all the activities to be done and to be evaluated on each Pilot Site. The part related to the Technical Evaluation is on the fifth tab, where the scenario is described with the following information:

1. **Outline of the scenario**. This part describes the test environment, setup, starting positions of vehicles, IoT devices and data sources/cloud services to be used, including a map of events.
2. **Description of the scenario**. This includes the procedure/steps: precondition, actions or events (1, 2, 3, etc.) and their order or timing or spacing. It will also define the relevant situations (traffic or weather status, automated driving functions and modes and services).
3. **Baseline**. Definition of the baseline which will be used to compare with the test results. It also contains a list of devices or services added to the baseline.

[1] http://wiki.fot-net.eu/index.php?title=Hypothesis

[2] https://service.projectplace.com/pp/pp.cgi/r78053647

[3] https://service.projectplace.com/pp/pp.cgi/r823175960

4. **Hypotheses to be tested**. The hypotheses of the spreadsheet which will be evaluated in this scenario.
5. **Results**. In the first column, the expected results from the test to be reported. In the second column the observed results from users reproducing the scenario will be listed.
6. **List of log files generated**. List of log files generated in the experiment.
7. **Safety interventions**. Report of the safety interventions occurred during the scenario.

3 Topics

This section presents the evaluation methodology of the essential technologies or topics introduced in section 2.2. The topics are evaluated from the data collected during technical test scenarios for the use cases presented in section 0.

3.1 Data management

IoT **Data Management** refers to the capability of IoT devices, such as the automated vehicles being tested, to manage the data needed for the automated driving functions and services.

The main research question is how IoT data management can add value to automated driving. The main hypothesis is that IoT data management enables to complement the on-board sensor data with data from IoT data sources to increase the data quality and to accelerate or enhance the functionality and performance, or enable new automated driving functions and services.

Technical evaluation of these hypotheses on IoT Data Management is divided into two sections that should be evaluated in conjunction:

- In-vehicle IoT-platform data management
- Cloud based IoT-platform data management

3.1.1 In-vehicle IoT-platform data management

Data management on an in-vehicle IoT platform includes several data management tasks:

- Processes to discovery and subscribe to relevant IoT data sources via an IoT platform.
- Processing of published IoT data, including the assessment of the relevance and quality of received data itself and for fusion with on-board sensor data.
- Management of alternative communication channels to search and retrieve required data.

3.1.1.1 Technical Research Questions and Hypotheses

This section refines the main research question and hypothesis for specific IoT data management tasks on the in-vehicle IoT Platform. The evaluation will focus on the relevance and quality of data and the reliability of providing data via alternative communication paths. The topics in following subsections and the use cases will evaluate in more detail how and how much the automated driving functions can be improved. As discovery, publish and subscribe functionalities are provided in standard IoT platforms, these tasks will not be evaluated specifically here.

***RQ:** What is the delay required to discover, subscribe and receive published data?*

HY: When a new vehicle or other relevant data source becomes relevant to an automated vehicle, some delay is introduced to discovery the new data source and provide first data, in comparison to peer-to-peer communication.

***RQ:** Can meta data be provided, independently of the make or type of the service, vehicle, device or sensor?*

HY: Meta data enables a vehicle to discovery, request, select and receive IoT data based on criteria for the required relevance and quality for automated driving

***RQ:** Can vehicle sensor data be provided through an IoT platform in a vehicle-independent manner?*

HY: Sensor data originating from different types of vehicles or road users and in different formats (such as C-ITS, DATEX2 or Sensoris) can be transformed and received in the standard format of preference of the host vehicle.

***RQ:** Can communication reliability be increased through IoT?*

HY: Data can be sent and received via alternative communication media, channels and routes to and from IoT Platforms, thereby improving the reliability of communication in comparison to using a single peer-to-peer communication route.

RQ: *Can a vehicle IoT platform optimise communication facilities?*

HY: A vehicle IoT platform can select and optimize communication channels based on the quality, such as availability, congestion, reliability and redundancy of data feeds.

RQ: *Can the quality of cooperative or situational awareness be improved with data received from an IoT platform?*

HY: The integration in IoT platforms of several communication channels 3G/4G, ITS-G5, LTEv2x increases the reliability by offering redundant information and enabling the optimisation of communication channels according to required quality of communication services such as cost, availability, congestion, latencies, or coverage.

HY: IoT data is able to complement the AD sensor data and provides more accurate results. Moreover, the redundancy of the rest of the data increases the confidence of it. The data redundancy also means an increase of the quality of the data.

3.1.1.2 Technical indicators, measurements and metrics

The following set of indicators is used to test the above mentioned hypotheses. The benchmark or baseline providing the metric for data management on in-vehicle IoT platforms is typically the existing predefined data flows via direct peer-to-peer or V2X communication.

The **delay** in discovery, subscription and publication is measured from the delay in different data flows:

- Delay between an initial discovery request from the vehicle to the response from the IoT platform (list of services) received by the vehicle.
- Delay between an initial subscription request from the vehicle to first reception of a published IoT message at the vehicle.
- When similar information is also exchanged via peer-to-peer or V2X communication, then the delay from the above two steps can be compared to the delay between generation time and reception time of the same information / messages. In this case, the delay in direct communication is the metric for the delay in communication via the IoT platform.

The delay measurements are obtained from data communication evaluations in section 3.2 for the mentioned data flows.

The **metadata** of IoT messages can be evaluated at design time. The indicator for vehicle-independence of the metadata is the level of standardisation and the replicability of the meta data, and the number of pilot sites or use case implementations using the same meta data. During the pilots, the indicator is the number of different types of vehicles using the same, or similar, IoT data streams.

The indicator to measure the use of **sensor data** in a vehicle-independent manner is the number of vehicle originating data flows and message types that are exchanged via IoT platforms by vehicles from other types. A condition for this indicator is that the standardised IoT messages are exchanged, as defined for example in the common IoT data model ([4] section 7).

The indicator for testing the **communication reliability** and optimisation of communication facilities is indicator for communication reliability provided by the evaluation of data communication in section 3.2. To differentiate between communication channels and media, the communication profile should be logged with the sending and reception of messages on the communication units and IoT platforms. The communication reliability for direct peer-to-peer or V2X communication is the metric for reliability improvements by IoT data management on in-vehicle IoT platforms.

The **relevance of data** received from the IoT platform or other communication channels need to be determined. Relevance is a context dependent criterion and can be determined for example from the time or location validity of the information, and minimum data quality. The data quality can be defined in several standardized criteria such as the information quality level and authorisation level of the data provider, the accuracy and confidence of the information, and the completeness of mandatory and optional parameters (i.e. missing data).

The relevance can be expressed as a Boolean; i.e. the data is relevant and used for fusion in automated driving functions, or the data is not relevant and not used. The relevance could also be expressed on more detailed qualitative or quantitative scales but that is necessary for data management evaluation.

Ideally, the relevance is determined and logged from the vehicle IoT platform upon reception of data. The relevance qualification can be included in the application logging of Annex 7.1.3. Examples of context specific relevance qualification are given for the platooning use case in section 4.4. Alternatively, the relevance can also be assumed from the changes in automated function behaviour upon reception of IoT data. Indicators for the latter approach are obtained from the evaluation of other topics and use cases.

To compute and assess indicators the following measurements needs to be logged and collected:

- Messages passing through the vehicle IoT platforms and communication units, with the message or payload type, sent or reception time, originator, communication channel or profile.
- Meta data used for discovering services, submitting and receiving data from cloud IoT platforms.
- Relevance, as assessed by the host vehicle applications, of received data passing through the vehicle IoT platforms and communication units. Relevance can be logged as specified in Annex 7.1.3.

3.1.2 Cloud based IoT-platform data management

Data management on a cloud-based IoT platform includes several data management tasks:

- Device and subscription management
- Up and down loading of data from IoT devices
- Discovery services for data brokering, data aggregation services, and (semantic) data transformations to data formats requested by automated vehicles
- Interaction with other IoT cloud services and (federated) platforms.

AUTOPILOT deploys standard and commercial cloud-based IoT platforms that are also applied for other application domains and markets. The goal of this section is to provide the methodology to evaluate the added value of the IoT infrastructure deployed and managed in the project to the IoT-enabled vehicles and corresponding cloud services developed in the project. Standard IoT platform functionality and performance are not evaluated per se.

3.1.2.1 Technical Research Questions and Hypotheses

This section refines the main research question and hypothesis on how cloud IoT data management adds value to the IoT of automated and connected vehicles. Nowadays, most in-vehicle systems are not connected to Internet and the more so don't use any cloud services. In recent years, almost all the automotive manufacturers are trying to add new features that depend on the vehicle's connectivity. This research question should be refined to answer what exactly this connectivity and cloud data management gives to the IoT-enabled vehicles.

A basic but very important question that may seriously affect the adoption of the IoT-technologies and techniques in the automotive industry should be answered. Since the main goal of the project is to investigate the applicability of the IoT technologies for AD-vehicle, on the following research question has to be focused:

***RQ:** How cloud IoT data management adds value to the IoT-connected vehicles?*

HY: Nowadays most vehicles are not connected to Internet and the more so don't use any cloud services. In recent years, almost all the automotive manufacturers are trying to add new features that depend on the vehicle's connectivity means. So a set of more specific questions and corresponding hypotheses that should give insight into understanding what exactly this connectivity and cloud data management gives to the IoT-enabled vehicles:

***RQ:** Can we achieve the same level of functionality without using cloud data management?*

HY: The use cases are being developed in the project are barely possible to be implemented without cloud-based data management

***RQ:** Do the IoT-enabled vehicles make use of the cloud data collected by other IoT-enabled sensors, devices or vehicles and managed by a cloud IoT-platform?*

HY: The IoT-enabled vehicles are connected to the cloud services and cloud data management leverages their driving features.

- How many down- and up- streams from/to the cloud IoT-platform are implemented comparing to the number of communication streams with the road-side infrastructure and vehicle-to-vehicle communications (local infrastructure)?
- Is collected cloud data available to all the connected vehicles and should be used by a number of vehicles (Cloud data should be propagated to all the vehicles, only some of them, or just one? Ideally, cloud stored data should be consumed by as many vehicles as possible)?
- Do cloud services process collected data from the vehicles/devices and give insights into the data (vehicles might be interested in aggregated values computed from raw data or mined data)?

***RQ:** How does the data available on the cloud based IoT infrastructure enable AD- and IoT-related features?*

HY: The cloud-based data management improves the quality of the driving features of the connected vehicles.

- How many driving features are affected by the down-streamed data from the cloud-based IoT platforms? Bear in mind that latency connecting to a cloud could be much larger comparing to latency communicating short range with road-side infrastructure.
- How many driving features are using cloud data for production of derivative products (e.g. car sharing)?

3.1.2.2 Technical indicators, measurements and metrics

Based on the proposed research questions and hypotheses we suggest to measure a set of indicators that shed a light on the cloud IoT data management enhancements for the autonomous driving features:

- **Actual number of components connected to the IoT infrastructure**. A comparison of the number of the cloud connected components with the total number of the components defines the value of the cloud infrastructure. There is no unanimous consensus for this relation on scientific literature, but in general higher the value the more important cloud infrastructure is to the services provided.
- **Actual data flows between the components**. The flows and data types define the importance of cloud services and hence cloud data management.

The indicators computation and assessment should be based on the collection of the following data:

- **Messages passing through the cloud IoT infrastructure**. This measurement allows assessing the load to the cloud infrastructure and can provide a rough estimate of the quantity of information run by cloud data management.
- **Origin of a message**. The number of producers and consumers give us an estimation of the number of the cross service or cross use case communications.
- **Destination of a message**. Should be used in combination with the origin of the message.
- **Payload type**. The type of the message dictates the consumption strategy and gives us an insight to the popularity of the cloud services.
- **Data discovery requests.** Used data discovery requests and filtering criteria in terms of meta data.

3.2 Data communication

The Data Communication functionality is provided through alterative communication modes, channels and media. Technical evaluation will focus on the comparison of the communication performance of alternative communication channels for Ad-hoc communication, peer-to-peer or device-to-device communication, and communication with data brokers via IoT Platforms in the cloud. Alternative communication media are used such as UWB, LTE, ITS-G5 as well as fixed Ethernet. The objective is to evaluate the realized communication performances in each of these situations and determine feasible performance levels for communication channels and media.

3.2.1 Technical Research Questions and Hypotheses

The main research question is “How is data communication improved by IoT?” The baseline for data communication for automated driving is the existing infrastructure for V2X communication, typically using ITS-G5 or UWB short range ad-hoc communication between automated vehicles and road side units and peer-to-peer communication with service providers via LTE/4G cellular networks.

Incorporation of IoT requires data communication via IoT platforms and cloud services.

Incorporation of IoT requires data communication via other communication infrastructures, such as cellular communication using LTE/4G between automated vehicles and the communication network infrastructure, and IP network communication between IoT platforms and cloud services.

The main research question can be refined to the following two questions and corresponding hypotheses:

RQ: *What are the communication performance differences between different communication technologies?*

This question firstly evaluates and compares the performance of alternative communication networks as used in the pilots. In situations where similar information is exchanged via alternative communication channels, the difference in performance can be compared directly. The hypotheses on communication performance differences are:

HY: The end-to-end latency is high when V2V or I2V data is exchanged via an IoT platform, in comparison to V2X ad-hoc communication.

HY: The communication range limitations from ad-hoc V2X communication networks is alleviated by communication via IoT platforms.

RQ: *Can communication reliability be increased by offering redundant communication channels provided by IoT?*

HY: The hypothesis is that the *c*ombination of existing communication networks and IoT potentially provides alternative communication flows thereby increasing the reliability of communication to support automated driving functions in comparison to the baseline of V2X ad-hoc communication.

Answering this question should also consider the implementations in the pilots, and the side-effects on other communication performance indicators such as latency.

3.2.2 Technical indicators, measurements and metrics

The indicators and metrics to measure and evaluate communication performance are a subset of those defined in Deliverable D1.7. Section 5 of [5] specifies minimum communication performance requirements per use case and device interaction. The objective is to evaluate the realised communication performances in each of these situations and propose feasible performance levels.

V2X communication and communication with IoT platforms is evaluated on the following performance criteria (see also section 5 and Table 20 of [5]):

- End-to-end communication latency; from the generation of a message by the sender, till the reception of the message by receivers.
- Reliability of communication by the packet loss rate or packet delivery ratio of set and received messages.
- Communication range is measured from statistics on and distributions of distances between senders and receivers.

Communication performance is measured for all relevant communication media, speed ranges of devices, and environmental situations experienced at the pilot sites. The measures are summarised in Table 1 and more detailed specifications are provided in Annex 7.1.2. Communication performance is measured at the facilities or application layers in stations and servers. Note that communication performance indicators for bandwidth and node density may not be evaluated if the node density is too low to experience bandwidth issues during the pilots.

The communication between IoT platforms in the cloud and in vehicles, and between federated IoT platforms are subject of evaluation. The communication between various IoT devices (other than the devices directly participating in the pilots) and IoT platforms is not directly evaluated. The communication for example to road side sensors, drones in ‘the cloud’, and smartphones of anonymous bystanders will not be evaluated. This communication is indirectly evaluated as it is included in the end-to-end delay from detection time at these IoT devices till the reception of the detections and derived information in the automated vehicles.

On the same note, the communication within a vehicle, and between communication layers within a station, are not evaluated directly either. The net effects of communication performance within and between in-vehicle systems will be evaluated in terms of delays in application decisions and actions, and the overall automated driving performance such as positioning improvements.

To evaluate the performance of communication the locations and timestamps upon sending and reception should be logged. To extract motion states or to evaluate use case related information, (part of) the message contents should also be logged. The following approach is proposed to minimise the required logging resources:

- The relevant contents of messages need only be logged once, typically by the sender.
- Receivers only need to log the message elements to uniquely identify the message.

Details on the identification of messages, collection of sent and receptions timestamps for latency measurements and location information for range measurements are detailed in the common communication logging formats.

The communication range is determined from the positions of the vehicles or other devices upon sending or receiving messages. Position information is either extracted from the message payload (e.g. from an ETSI CAM) or from the positioning evaluation in section 3.3.

Name	Type	Range	Unit	Description
log_stationid	long	from 0 to 4294967295 (= 2^{32}-1)	[N/A]	Identifier of the host station that logs the sent or received message
log_action	enum	['SENT', 'RECEIVED']	[N/A]	Action in communication data flow
log_communicationprofile	enum	['ITS_G5', 'CELLULAR', 'UWB', 'LTE_V2X']	[N/A]	Communication medium or channel over which the message is sent or received
log_timestamp	long	From 0 to 4398046511103 (=2^{42}-1)	[msec]	Timestamp of sending or receiving the message. Elapsed time since midnight January 1st 1970 UTC.
log_messagetype	enum		[N/A]	Type of standardised message, used for automated processing in case multiple message types are combined in a single log file. The enum fields refer to the <standardisation organisation>.<message type>.
log_messageuuid	uuid		[N/A]	Universal Unique Identifier of the message. This is an alternative for the identification of messages from the message contents. If used, then the uuid should also be included in the payload of the message and communicated between senders and receivers.
payload				Payload of the logged message as specified in Annex 7.1.2.

Table 1 - Data communication measurements

3.3 Position, localisation and navigation

The **Position, Localisation and Navigation** compares the information related to RTK-GPS, HD maps, parking spot information or routes received by IoT cloud services with the existing vehicle sensors and maps data. The objective is the improvement of the internal state, motion planning and routing within automated vehicle functions and services. Localisation and navigation is evaluated on accuracy for determining the relative position on the road; i.e. the longitudinal and lateral position on a road and in a lane.

From a technical perspective, the performance using existing vehicle sensors and maps can be compared with the performance while using for example for RTK-GPS, HD maps, parking spot information or routes to available parking spots received from IoT cloud services and data sources. The general hypotheses are that IoT enabled position and localisation should improve the smoothness of driving, manoeuvring and lateral behaviour, while navigation and routing should be more efficient and avoid more obstacles and delays. The performance of in-door positioning and navigation enabled by IoT for Automated Valet Parking in Vigo will also be evaluated.

3.3.1 Technical Research Questions and Hypotheses

The IoT cloud services and data sources identified before are essential technical measures for improvement of the internal state, perception systems, motion planning and routing within automated vehicle functions and services. Technical improvements are highly relevant for all automated vehicles and use cases. Examples for improvements are:

- RTK-GPS for accurate positioning with reference signals provided via an IoT platform.
- The use of HD-maps provided and updated via IoT cloud services, in combination with on-board camera's and sensors, to improve localisation of the relative position on the lane or road.
- In-door and out-door routing and navigation using IoT devices.
- Optimised routes to navigate to an available parking spot using IoT services.

The general hypothesis is that the added value of IoT platform and cloud services should improve the accuracy and reliability of positioning, localisation and navigation. Performance indicators are, therefore, defined for accuracy and reliability.

Situations are distinguished by pilot site location, i.e. geographic areas that affect the performance, for example for indoor navigation in Vigo, GPS accuracy in Finland, RTK-GPS services in Brainport and vulnerable road user detection in Versailles and Livorno.

The research questions are related to the Global Positioning System and the Inertial Navigation system, including the positioning data, the data related to the navigation systems and the localisation of the vehicle respect to the other elements of the road. The range and the accuracy with timing references and also the changes with the on-board maps with the IoT will be evaluated.

RQ: *How IoT adds value to positioning, localisation and navigation for Automated Driving functions?*

HY: The position, localisation and navigation data provided by IoT is enhancing motion planning and routing within automated vehicle functions and services.

RQ: *To what extent can IoT improve positioning and navigation?*

HY: The IoT data increases positioning accuracy with reference signals provided via an IoT platform and improve navigation by providing new reliable information about the environment, traffic, obstacles and VRU's.

RQ: *What is the improvement in host positioning accuracy?*

HY: The error from latitude and longitude is decreased because of new signals providing positioning compared to the baseline and the signal lost time is also reduced because of more devices providing positioning when GPS is not available.

RQ: *Does IoT improve short range navigation?*

HY: The use of dynamic HD-maps, in combination with on-board camera's and sensors, improves localisation of the relative position on the lane or road.

RQ: *Does IoT reduce the time needed to park a vehicle?*

HY: Thanks to the IoT data, the vehicle receives more precise information about the environment and itself that reduces the number of manoeuvres to park and reduces the time needed.

RQ: *Does IoT optimize the energy consumption of the vehicle?*

HY: Driving in the same route, the speed profile improves in a smarter way because of more information about the environment that lead up to a reduction of the energy consumption.

RQ: *Does the IoT information send and received in the vehicles affect to the state of the traffic?*

HY: Traffic could be better balanced if all the vehicles followed the instructions provided by IoT.

RQ: *Does IoT reduce the waiting or travelling time for the Car Sharing / Car Rebalancing service?*

HY: The pick-up or drop-off time of the vehicles can be reduced thanks to real time environmental information available as a result of IoT data.

3.3.2 Technical indicators, measurements and metrics

The next indicators will be measured following the same procedures in the baseline and in the IoT enhanced vehicle and comparing both results. The technical indicators used to evaluate the position and navigation topic are:

1. **Travel time to drive.** Travel times will be measured for relevant parts of the routes, and sub-scenarios, such as passing a controlled intersection, manoeuvring into a parking space, or the platoon formation process. Travel times are also compared to predicted travel times for advices or planned routes (a decrease means an improvement):
    a. **To / from parking spot.** Travel time from the drop off point to the parking spot. It will be measured with both timestamps, in the drop off point and when the vehicle arrives to the parking spot.
    b. **Highway route**. Route time from point A to point B (e.g. Highway Pilot from Livorno, from Florence to Livorno). The travel time will be measured checking both timestamps, when leaving point A and when arriving point B.
    c. **Urban route**. Route time on an urban environment (e.g. city centre of Versailles or University Campus from Eindhoven). The travel time will be measured checking both timestamps, when leaving the starting point and when getting to the arriving point.
2. **Distance to drive** (a decrease means an improvement):
    a. **To / from parking spot**. Travel distance from the drop off point to the parking spot. It will be measured with both timestamps (start and final) and the own distance (for Vigo and Brainport) or the GPS points (for Tampere where is not available the data from the odometer in the vehicle).
    b. **Highway route**. Distance will be fix, since there are only stationary routes (no adaptations are done depending on the information collected by the IoT platform), therefore, it makes no sense to compute this KPI for the use cases using highway routes.
    c. **Urban route**. Urban routes can be adapted depending on several measurements as, e.g., pedestrian density in the car rebalancing service in Brainport. Nevertheless, this feature has been not yet implemented. Therefore, the measurement of this KPI will only be possible as soon as the route adaptation feature is implemented.

3. **Position accuracy** (an increase means an improvement):
    a. **In-door accuracy.** The IoT is enabling the in-door positioning; otherwise we could not have positioning inside. It will be measured with the latitude and longitude in a map provided by the parking management system.
    b. **Out-door accuracy.** The positioning accuracy KPI will compare the one obtained by the GPS to the one that could be provided by other signals through IoT (like Wi-Fi positioning). We also need to consider that IoT positioning could provide a position more accurate where the GPS signal is low.
4. **Time to park** (decrease meaning an improvement). Time spent manoeuvring in the parking spot. It is measured with the difference between two timestamps: when the vehicle arrives to the parking slot and when the vehicle is parked.
5. **Energy consumption** (decrease meaning an improvement). We have two different ways to calculate energy consumption depending on the source of energy of the vehicle (fuel or electric). If the vehicle is using fuel, it will be measured using the fuel consumption during the route. If the vehicle is electric, we will compare the State of Charge of the battery at the start of the route and when is ended. The average speed during the trip will also be measured to establish a relation between the energy consumption and the speed profile.
6. **Traffic balance**. Traffic can be better balanced if route planning is done in a centralized manner. Nevertheless, in order to achieve such a balance, all the traffic actors should obey the planning of the central entity, which will not be the case in the AUTOPILOT project. Therefore, even if this could be one of the achievements of involving IoT information in CAD, it will not be demonstrated (and, therefore, also not evaluated) in the AUTOPILOT project.
7. **Vehicle pick-up/drop-off time delays** (decrease meaning an improvement). The car sharing service provides an estimate time for the vehicle to arrive where the user is waiting for. It also provides the time estimation to arrive to the destination. The measurement will be difference between timestamps, the estimated one and the real one.

In order to compute these KPI's we need to log in each vehicle several measures in a specific format as shown in the next table:

Name	Type	Range	Unit	Description
Timestamp	long	From 0 to 4398046511103 (=2^{42}-1)	[msec]	Elapsed time since midnight January 1st 1970 UTC.
Own distance	double	From 0 to 5000	[km]	Total kilometrage per day or trip or road type etc.
Fuel consumption	double	From 0 to 1	[L/km]	Average fuel consumption during a route or trip.
Battery SoC	double	From 0 to 100	[%]	Percentage of the battery of the vehicle.
Speed	double	From 0 to 163.82	[m/s]	Speed over the ground.
Latitude	double	From -180 to 180	[degree]	Geographic coordinate that specifies north-south position.
Longitude	double	From -90 to 90	[degree]	Geographic coordinate that specifies east-west position.

Table 2 - Position and Navigation measurements

3.4 Environmental detections

Environmental detections refer to the capability of automated driving functions and services to acquire information from the environment for cooperative and situational awareness. Relevant detections from the environment are obstacles and hazards in the vicinity and en-route of the vehicles, such as:

- other road users like vehicles and vulnerable road users
- road surface hazards like potholes and puddles
- traffic signs and (dynamic) speed limits
- traffic conditions and information on congestion, or
- adverse weather conditions

The baseline situation is that on-board sensors, such as camera, laser scanners and radars, can detect nearby road users, lane markings, parking spaces.... The main technical hypothesis is that IoT data from the environment can also be obtained from IoT devices and cloud services via IoT platforms, and that the world model, or situational awareness, of automated driving vehicle functions and services can be enhanced with these additional data sources. The added value for environmental detection quality in this context is defined by the performance of detection, localisation and classification of an object or hazard.

It is important to note here, that the localisation and classification of those detections is the actual added value. Detections are for the technical evaluation mostly just 'event-data', whereas when these detections are also linked to a location, this data becomes much more valuable and usable for evaluation. Therefore in the indicators and measures, also position (in longitude and latitude) is considered here, however these is now focused on the obstacles as detected by environmental sensors (and not the location of the vehicle itself).

3.4.1 Technical Research Questions and Hypotheses

The technical research questions below which require use of environmental sensors have been derived:

RQ: *How are the environment detections enhanced by the IoT technology?*

HY: The IoT technology provides more accurate localization of the object in question and thus enhances the environment detections and in turn improves Automated Driving functionalities and enables new functionalities to be added.

RQ: *Can IoT be an enabler for safety applications?*

HY: IoT will increase safety by integrating additional / redundant sensor information (e.g. environmental data, hazards) to improve detection rate and reduce reaction time. As a result, it will increase the number of detected environmental objects and the range of its detection.

RQ: *Can heterogeneous IoT sources provide additional environment detections?*

HY: IoT will increase the interoperability between heterogeneous IoT sources and increase environmental context even if the vehicle is not directly using the sensor.

RQ: *How can VRUs be detected by IoT?*

HY: IoT is capable of integrating the sensors that VRUs may carry and provide more cautious reactions in the presence of pedestrians and hazards.

RQ: *How can IoT weather information improve the behaviour of the AD car?*

HY: The weather information can help AD cars avoid hazards or handle a hazardous situation (if it can't be avoided), improves routes and navigation and adapts its speed depending on the weather conditions. Proper adaptation of in-vehicle environmental sensors to weather conditions can also improve the performance of the AD car.

3.4.2 Technical indicators, measurements and metrics

Potential improvements in environmental detection performance can be evaluated by indicators for the type of environmental objects, detection accuracy, detection rate, detection delay, and the geographic position, location and range of detections. Technical indicators used to evaluate the environmental detections topic are:

- **Relative position accuracy**. The relative position of an object with respect to the host vehicle's attitude is a measure of how accurate objects are positioned for situational awareness. Relative positioning accuracy can be evaluated from alternative sensor data and from (accurate) absolute positioning of the environmental objects (e.g. VRUs and other vehicles) and maps.
- **Classification accuracy** of object type, such as vehicle, road, hazard, or VRU. Detection of objects (false positives) is a measure to classify objects accordingly. This can be compared with the data received from an IoT device, for matching and preventing possible false positive detection by one environmental sensor. This can be road detections, vehicle detections, VRU detections, hazard detections etc.
- **Detection range** of the environmental perception (early detection of objects): IoT can increase the 'world model' of the AD vehicle extending its range beyond the on-board sensors. Measuring occluded view of in-vehicle camera for example and adding IoT information can possibly extend the vehicle awareness of important objects, like VRUs.

In order to compute these KPI's we need to log in each vehicle several measures in a specific format as shown in Table 3. More details on the measurements, logging and codes are provided in Annex 7.1.1 and D2.1 [6]. The measurements in this table are generic and can be logged from several on-board sensors and IoT devices. The sensor or device logging the measurements is uniquely identified by the log_applicationid of the log_stationid as described in Annex 7.1. The position of a detected environmental object, or obstacle, is logged either as an absolute position in WGS84 coordinates with a latitude and longitude, or as a relative position in local vehicle (x, y) coordinates – corrected for the mounting location of the sensor on the vehicle.

Name	Type	Range	Unit	Description
longitude	double	from -90 to 90	[degree]	Main object transformed to geolocalized coordinates longitudinal (log_applicationid identifies the sensor providing this measurement (e.g., camera, LIDAR, radar...)).
latitude	double	from -180 to 180	[degree]	Main object transformed to geolocalized coordinates lateral position (log_applicationid identifies the sensor providing this measurement (e.g., camera, LIDAR, radar...)).
obstacle_ID	int	from 0 to 1000	[-]	ID of the obstacle detected by environmental sensors.
x	double	from 0 to 500	[m]	Main object relative distance longitudinal / x-direction (log_applicationid identifies the sensor providing this measurement (e.g., camera, LIDAR, radar...)).

Name	Type	Range	Unit	Description
y	double	from -50 to 50	[m]	Main object relative distance lateral / y-direction (log_applicationid identifies the sensor providing this measurement (e.g., camera, LIDAR, radar…)).
obstacle_covariance	float64			Covariance matrix of positions of longitude, latitude, altitude of RADAR detected objects.
ObjectClass	int	from 0 to 65	[-]	65 classes from Mapillary dataset[4]
lanewidthsensorbased	double	from 0 to 10	[m]	Lane width measured by on-board sensor(s).
lanewidthmapbased	double	from 0 to 10	[m]	Lane width from map information.
trafficsigndescription	string		[N/A]	signrecognition[5]
speedlimit_sign	double	from 0 to 250	[km/h]	signrecognition [6]
servicecategory	enum	['dangerWarning', 'regulatory', 'informative', 'publicFacilities', 'ambientCondition', 'roadCondition']	[N/A]	signrecognition [7]
servicecategorycode	int	[11, 12, 13, 21, 31, 32]	[N/A]	signrecognition[8]
countrycode	string		[N/A]	signrecognition [9]
pictogramcategorycode	int	from 0 to 999	[N/A]	signrecognition [10]
VRU_pedestrian_class	int	from 0 - 3	1 = children, 2 = adults, 3 = elderly	Sub classes of pedestrians.
VRU_cyclist_class	int	from 0 - 3	1 = children, 2 = adults, 3 = elderly	Sub classes of cyclists/riders.
confidence_levels	double	from 0 - 100	[%]	Indication for false positive detections (minimum default

[4] http://research.mapillary.com/publication/iccv17a/

[5] IVI - ISO TS 19321 (2015) v1: https://www.iso.org/standard/64606.html

[6] IVI - ISO TS 19321 (2015) v1: https://www.iso.org/standard/64606.html

[7] IVI - ISO TS 19321 (2015) v1: https://www.iso.org/standard/64606.html

[8] IVI - ISO TS 19321 (2015) v1: https://www.iso.org/standard/64606.html

[9] ISO 3166-1 alpha-2: https://www.iso.org/iso-3166-country-codes.html

[10] ISO TS 19321 (2015) v1: https://www.iso.org/standard/64606.html

Name	Type	Range	Unit	Description
				level).
Environ_info	int	from 1 - 6	[-]	1=sunny/day, 2=raining/day, 3=snow/day, 4=night/dry, 5=raining/night, 6=snow/night
Road_hazard	int	from 0 to 42	[N/A]	No standardized dataset available --> current proposal: pothole detection, slippery road, black ice etc.
sensor_position	int	from 0 to 1000	[mm]	Position of sensor on vehicle wrt. CoG. required for correlating to environmental detection with IoT detections.
process_delay	int	from 0 to 1000	[ms]	Is processing delay known or unknown?

Table 3 - Environment sensor measurements

3.5 Safety

A numerical evaluation of **Safety** which could be then compared with a baseline is beyond the scope of AUTOPILOT. However, **Safety** has a very high importance in the project and is considered in many of the development and deployment phases. Obviously, the use of IoT data may affect the **Safety** of automated driving and, therefore, any incidents should be reported, investigated and assessed. Any human intervention, e.g. by a test or co-driver, to disengage an automated driving mode, function or (safety-relevant) service in real-traffic conditions is considered as an incident that should be reported. Factors that might have caused the incident to report include weather conditions, inattentive road users, unwanted vehicle manoeuvres, and hardware or software failures.

This chapter describes the methodology for assessing the safety in each Pilot Site and in each use case. Recommendations will be provided in order to accomplish an acceptable level of safety.

3.5.1 Assessment methodology

The safety assessment will be done taking as the main input the safety audit done in the verification phase (task 2.5, deliverable 2.6 [7]). This safety audit consists in a list of inquiries on how IoT data can affect the Autonomous Driving functions. It also takes into account the number and type of users involved and how they interact with the use case. Using this information an analysis will be done in order to detect possible risks and recommendations will be provided. The questions that will be assessed in the audit are:

- Are there persons involved in the test cases? What is the role of these persons (VRU, naïve users, expert drivers or operators)?
- How many IoT objects are involved in the Use Case / Service? Among them how many vehicles?
- To which IoT objects is the vehicle connected during a Use Case?
- What data does the IoT provide to the vehicle?
- What does the vehicle do with IoT data? Has the software/hardware of the vehicle been modified? If so, which measures have been taken against software/hardware malfunctions?
- Can the AD functions be affected by IoT? If so, which of them and how?
- Is IoT able to modify or control vehicle motion? (i.e. longitudinal or lateral control)
- Is there any possibility to fall-back to the vehicle original state (override IoT functionality)?
- Which source of data has priority and how is it weighted data from IoT or data from vehicle sensors?

- What happens if IoT data is missing, delayed or corrupted? (Is there any possibility/tool to test this in the current implementation of the Use Case / Service?)
- Has the safety of the intended function been tested? (known safe, unknown safe, known unsafe and unknown unsafe)

Together with this information, a report of incidents after test iterations will be requested from each Pilot Site which will complement the safety audit done previously. The list of incidents to be reported is:

- Incidents caused by weather conditions.
- Incidents caused by inattentive road users.
- Incidents caused by unwanted vehicle manoeuvres.
- Incidents caused by perception discrepancies.
- Incidents caused by HW malfunctions.
- Incidents caused by SW malfunctions.
- Incidents caused by road works.
- Incidents caused by emergency vehicles.
- Incidents caused by road surface conditions.
- Incidents caused by objects on the roadway.

These incidents will be evaluated taking into account:

- **Incident rate per time and distance travelled**. The number of incidents reported by use case and by Pilot Site during a defined period of time or a certain distance travelled.
- **Traffic environment**. The number of incidents reported that could affect the travel environment and the severity of the issue.
- **Traffic situation**. The global traffic situation according real-time information during the use cases and services testing.

With all the information collected, this task will provide a list of recommendations to be implemented in the Pilot Sites in order to accomplish a minimum level of safety and to ensure that all the situations of a use case achieve an acceptable level of safety.

3.6 Security

The security will be assessed concerning the most common security threats related to IoT. This section describes the information related to security that should be provided by all pilot sites for the evaluation of security aspects in the project.

3.6.1 The research question

The main research question of the security aspects of the Autopilot project is:

RQ: *How far is Autopilot security from readiness to hit the real streets?*

Security must be assessed from multiple points of view to ensure that a security by design approach was correctly applied, the attack surface is minimized and the identified risks are mitigated.

In cases where, for budget or timing constraints, development teams have not been able to implement security measures to mitigate all the identified risks we will research whether the development team has a rationale for not mitigating some risks.

3.6.2 Assessment methodology

The main objective of this assessment is focused on the security of all the devices (or at least device models) used in the implementation and also all the layers of the AUTOPILOT ecosystem. A questionnaire has been set up in order to achieve this objective. The questionnaire covers the main aspects of the topic and has to be answered by each Pilot Site.

The aspects that will be covered by the security questionnaire are:

- **Physical security**. Measure the protection of personnel, hardware, software, networks and data from physical actions and events.
- **Wired network security**. Measure the network parameters as: segregation, firewalls and routers rules
- **Wireless network security**. Measure what protections are in place to protect wireless communications.
- **Device security.** Measure if there is an inventory of installed devices. Measure if an update plan is possible with the current implementation. Measure if devices are baked up and can be recovered in case of disaster.
- **Logs availability**. Measure the availability of log files and if/how they are kept safe.
- **Application security**. Measure how updates are propagated to servers and devices. Measure if the application code is securely executed (minimum privileges principle).
- **Protocols security.** Measure if protocols are resistant to MITM attacks, eavesdropping, and injection.
- **User / device authentication and authorization**. Measure how strong the passwords are and how UAC/MAC is able to correctly identify and authorize users**.**
- **Perception of security**. Measure how the users are impeded by security features.

3.7 Privacy

The **Privacy** will be assessed from multiple points of view to ensure that a correct approach has been followed. Relevant issues to this respect are that the user tracking possibilities are limited to a minimum, the project is compliant to GDPR regulation and an appropriated level of privacy is perceived by the end users, in order to ensure that the project is well accepted.

This chapter describes the methodology and the required documentation that should be provided by the pilot sites for the assessment of the protection of privacy in AUTOPILOT. The privacy requirements are described in D1.9 [8].

3.7.1 Assessment methodology

Privacy requirements of the solution were defined in D1.9. The main inspiration of the requirements is a GDPR regulation starting on 25th May 2018. The research questions defined reflect the regulation:

RQ: *Is Autopilot GDPR compliant?*

RQ: *How difficult is to track user using all information in the IoT cloud?*

RQ: *What is perception of privacy of Autopilot users?*

The evaluation should ensure that:

- AUTOPILOT is compliant with the regulation and follows “Privacy by Design” principle.
- User tracking and other privacy disclosures are limited to required minimum.
- Privacy is well perceived by users and contributes to acceptance of the project.

The evaluation should consider all private information entering the system as well as pieces of information that are not necessarily private, but may be used to obtain the private information when combined with pieces from other sources; privacy may be compromised by disclosing the information directly and also by calculation of the private information from several sources of seemingly anonymous information. Specific private information is also user tracking where user journey may be calculated from many sources that collect information for different purposes (e.g.

non-anonymised vehicle localization data).

For this reason, the evaluation should assess information flow of each use case and also supporting information submitted into the platform and used indirectly such as video data.

3.7.2 Assessment of use case data flows

Data flow analysis will start at the point where the user enters the system (registration, authentication) and follow the information flow through all the layers during the pilot scenarios. Following points will be reviewed:

- The information that is entered.
- Whether the information is persisted (in log, audit trail or as a part of platform data).
- Translation of the information between layers and possible disclosure.

The documentation of the data flows should be provided by each use case implementation team and should follow example provided in this document.

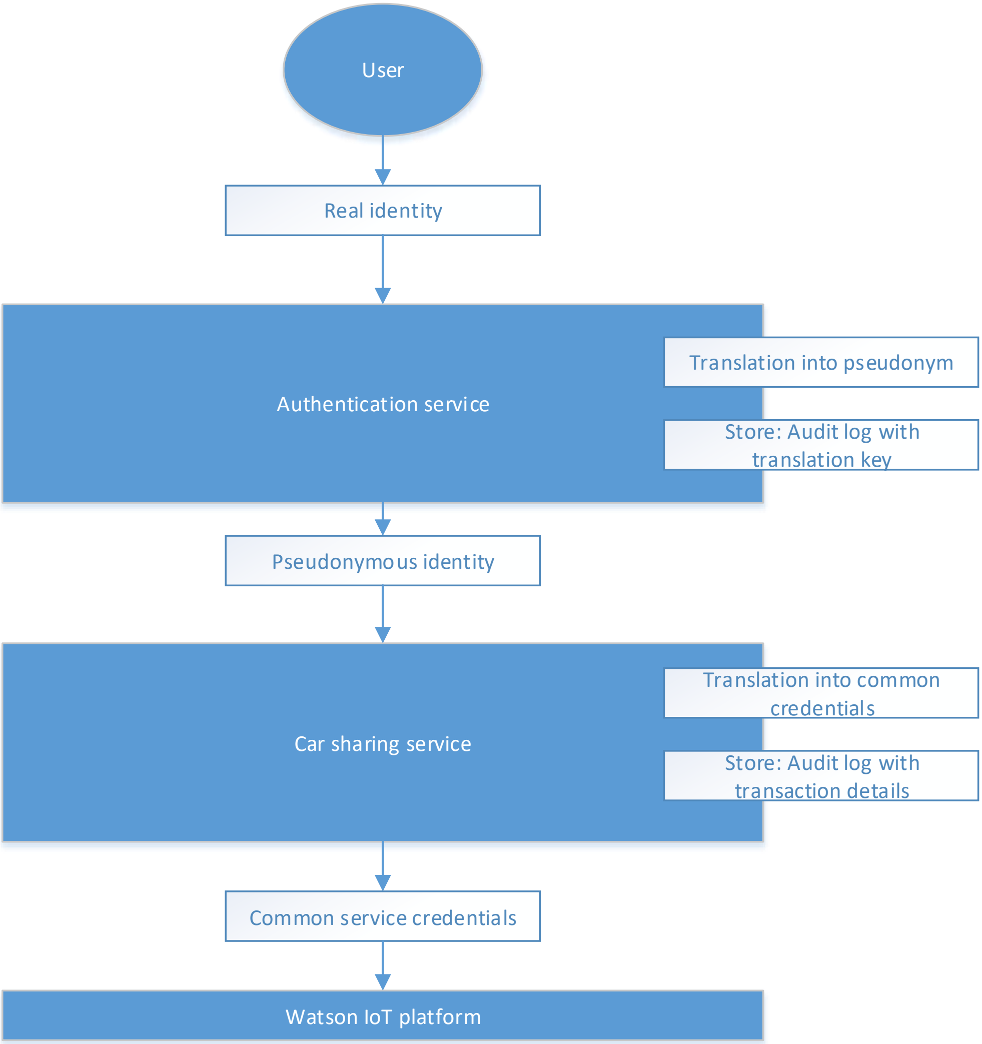

User
Real identity
Authentication service
Translation into pseudonym
Store: Audit log with translation key
Pseudonymous identity
Car sharing service
Translation into common credentials
Store: Audit log with transaction details
Common service credentials
Watson IoT platform

Figure 1 - Example of information flow of Car sharing use case

3.7.3 Assessment of user tracking

In order to analyse user tracking additional flow will be analysed:

- Information about user position via information from other devices. Typical example is information about users entering a vehicle at a specific position and tracking of the vehicle.

- Collateral information of the use case available in the platform that may be used for tracking. Example may be information about users on pedestrian crossing with possible unique identification or information collected by roadside units.

3.7.4 Assessment of information in the ecosystem and possible privacy leaks

The information submitted into the system may be exploited on several layers: it may be disclosed by the services via data provided to service providers or disclosed directly as data persisted in the IoT. In order to cover both privacy threats the analysis must cover both data submitted and persisted by the platform and data made available by services accessible from the outside.

Each data source of the platform should be analysed for potentially sensitive data and data flows should be provided describing how the data enters the platform, whether data is persisted and describe information that is derived from the data.

The data may impact privacy on two levels: when the data enters the pilot site platform or local services and when the data is shared with interoperable platforms. The evaluation should ensure the privacy by design principle is followed for all information entering the platform: that only required information is collected, anonymised as soon as it enters the platform and it is not shared with other platforms if not necessary.

In order to simplify the assessment task the data analysis should be limited to information impacting privacy: position data (of vehicles and other traffic actors), unique identifiers (such as pseudonymous credentials, MAC addresses) and video data.

3.8 Replicability, sustainability & interoperability

Replicability, sustainability and interoperability will be assessed together. The **Replicability** is the feasibility to deploy one use case or service developed in a given Pilot Site in another Pilot Site. The higher the standardization level in the development of a use case or service is, the more feasible it should be to replicate it elsewhere. For this reason, the replicability is strongly related to the standardization. Therefore, taking as input the level of standardization of the Pilot Sites and its developments, the objective of the replicability assessment is to assess the feasibility of replicating use cases and services between Pilot Sites. The **Sustainability** is the process of using resources, technological innovation and investments in a balanced manner to the benefit of humankind and the environment. Sustainable Development has been defined by the "Brundlandt Report" [2] of the World Commission on Environment and Development as the ability "… to meet the needs of the present without compromising the ability of future generations to meet their own needs". In the AUTOPILOT project, this concept will be transferred to a technical point of view. The **Interoperability** topic will assess the different IoT technologies and IoT architectures between the Pilot Sites of the project. For example, the vehicles used to evaluate the Versailles Pilot site will also be used on Brainport to evaluate their use cases.

3.8.1 Research Questions and Hypotheses

Replicability is the feasibility to deploy one use case or service developed for a given Pilot Site in another Pilot Site: to reproduce / replicate the same functionality in a different physical environment. For this reason, three evaluations are important to conduct: comparable use case functions, comparable technical implementation & use of same standards.

Sustainability is an elaborated concept which covers many different disciplines and thematic issues. However, in this technical evaluation document only the evaluation of sustainability from a technical point of view will be analysed. In this context, sustainability focusses on the acceptance by industry by using widely accepted standards, so that the product/service can be implemented quickly and be used for longer periods of time.

Interoperability mainly addresses the communication between separate components: the ability to exchange and make use of information between multiple computer systems or software. This requires standardization on the communication level.

For all three topics, the higher the standardisation level in the development of the use case or service, the more feasible it is to be replicated and to be sustainable or interoperable with other IoT platforms. Therefore, taking as input the level of standardization of the Pilot Sites and its developments, the objective of the replicability, sustainability & interoperability assessment is to assess the feasibility of changing use cases and services between Pilot Sites.

In WP5, Task 5.5 (D5.7 [9]), there is a list with all the standards involved by AUTOPILOT area of interest (IoT Platform and architecture, Vehicle IoT Integration and platform, Communication network, IoT Eco-system) grouped also by keywords / knowledge areas (Communication and connectivity, Integration and interoperability, Application, Infrastructure, IoT Architecture, Devices and sensor technology, Security and Privacy and Conformance and testing). The replicability assessment will include a study of these standards and a check of which of them are applied to the Pilot Sites and if they are the same among all the AUTOPILOT Pilot Sites. Since the FESTA methodology is more focused on the performance evaluation of a developed system, this methodology will not be applied for the replicability assessment, which will be given or not.

Research questions and hypotheses

The AUTOPILOT IoT architecture is designed as a federation of IoT platforms, allowing it to be open and flexible. Developers may plug their own (proprietary) IoT platforms or devices in the architecture and exchange data with existing IoT platforms and devices. As each IoT platform provides a different set of services (features) and may expose a different interface and use a different data exchange protocol, an effort is needed to achieve interoperability while allowing for openness and flexibility. In this architecture, data providers or consumers, such as applications, may use any of the available IoT platforms according to their requirements. Therefore the following research questions have been derived with an accompanying hypothesis:

RQ: *Can we achieve the same level of functionality without introducing interoperability features/services between various IoT technologies and platforms?*

HY: Due to various technologies being used on the pilot sites we believe that without an additional interoperability layer it is hardly possible to achieve smooth interoperability between devices/services.

RQ: *What is the value of the interoperability between IoT technologies and IoT architectures? (It helps to unify different formats and data streams).*

HY: Data and protocol standardization improve interoperability between the devices/services deployed on the pilot sites.

RQ: *How many (percentage or another relative measure) AD- and IoT-related services are using data coming from different IoT-platforms?*

HY: Even a simple case would probably involve usage of several devices, platforms, and technologies that may be incompatible out of box requiring additional setup.

RQ: *How many (percentage or another relative measure) data messages used by the vehicles are coming from different IoT-platforms?*

HY: Even a simple case would probably involve usage of several devices, platforms, and technologies that may be incompatible out of box requiring additional setup.

RQ: *How can it be guaranteed that the different Use Cases from the project can adhere to a single* *standard during testing which allows implementing them in different future applications?*

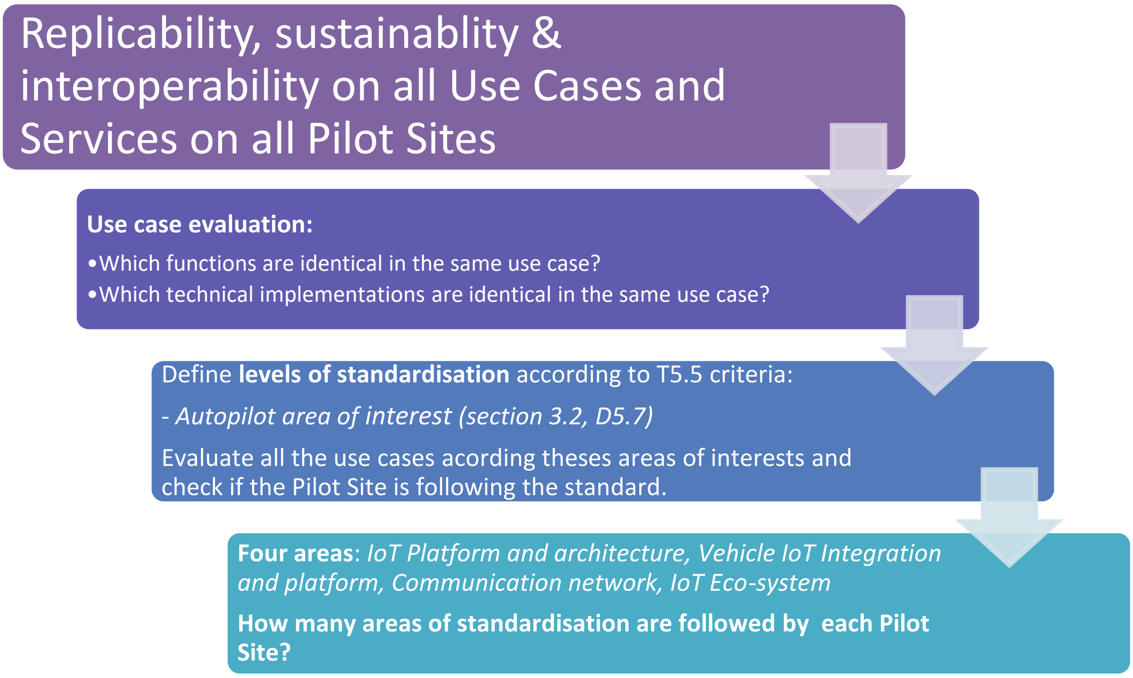
HY: This is in particular an important issue when the final product should be taken over by the industry.

RQ: *Can the system be designed in a way that the automotive industry accepts the product and integrate these newly developed services into their product catalogue?*

HY: This is important because it will benefit not only the industries but also the end customers' acceptance towards the range of products. The evolution from research activities into an industry product will benefit the whole transformation process.

3.8.2 Assessment methodology

For the purpose of technical evaluation, the following methodology is proposed:



Replicability, sustainablity & interoperability on all Use Cases and Services on all Pilot Sites

Use case evaluation:

- Which functions are identical in the same use case?
- Which technical implementations are identical in the same use case?

Define **levels of standardisation** according to T5.5 criteria:

- Autopilot area of interest (section 3.2, D5.7)

Evaluate all the use cases acording theses areas of interests and check if the Pilot Site is following the standard.

Four areas: *IoT Platform and architecture, Vehicle IoT Integration and platform, Communication network, IoT Eco-system*

How many areas of standardisation are followed by each Pilot Site?

Figure 2 Replicability, Sustainability and Interoperability methodology

First we need to evaluate and compare the functionality of each of the use cases (i.e. function: vehicle needs to be able to detect VRUs) for each of the Pilot Sites, since replicability is to reproduce the same functionality in another environment.

Then, the analysis on technical implementation (i.e. VRU detection with communication using ITS-G5 vs. 4G communication) is required, since different technical implementations might already be a bottleneck in implementing interchangeability & replicability between Pilot Sites.

Since standards apply to technical implementations, this is the next logical step to be evaluated. Therefore a questionnaire list has been extracted from D5.7 [9] and converted into the checklist to be filled in by the Pilot Sites, in order to evaluate which of these pre-defined standards are being used (see Annex 7.1).

Standards evaluation

This list is extensive and covers standards on the following areas (in line with D5.7):

- IoT Platform and architecture → replicability, interoperability
- Vehicle IoT integration and platform → replicability, interoperability
- Communication network → interoperability

- IoT eco-system → sustainability, interoperability

The same list can be used to evaluate interoperability, replicability and sustainability, when clustering the same standards to the following keywords:

- Communication and Connectivity
- Integration and interoperability
- Application
- Infrastructure
- IoT Architecture
- Devices and sensor technology
- Security and Privacy
- Conformance, Testing

Implementation of methodology for replicability, sustainability & interoperability

Based on the overview of standards, the following 3 possible methods can be used to technically evaluate the different use cases over the pilot sites:

1. (Step 1) Use the same IoT platform, e.g., oneM2M on the different pilot sites and (Step 2) taking an IoT equipped vehicle/device from one Pilot Site and deploying it on another Pilot Site and (Step 3) is executing the same use case.
2. (Step 1) Use different combinations of "3rd party IoT platform/oneM2M" in different pilot sites, but where one of these platforms is used as an interoperability platform, and (Step 2) taking an IoT equipped vehicle/device from one Pilot Site and deploying it on another Pilot Site and (Step 3) is executing the same use case.
3. (Step 1) Use different combinations of "3rd party IoT platform/oneM2M" in different pilot sites, but where the oneM2M platform is used as an interoperability platform, and (Step 2) using oneM2M MCA interface and defined data models for the oneM2M MCA interface and (Step 3) is executing the same use case.

A first evaluation between pilot sites on this topic has been initiated with Brainport, Versailles & Vigo Pilot Sites.

In the next phase of the project, this needs to be further evaluated using the above-mentioned approach and the technical indicators described in the following section.

3.8.3 Technical indicators, measurements and metrics

In order to ensure the quality of developed services we have to develop indicators which show if it complies with agreed criteria. Below the list of criteria identified for technical evaluation.

No.	Technical Evaluation Criteria	Applies to:	Checklist
	Is the standard used compatible?		
1	Standard used by communication system is compatible?	Replicability / interoperability	10%
2	Has an international standard (like ISO) been applied?	Replicability / interoperability	10%
3	Are communication standards being used by the system?	Replicability / interoperability	10%
4	Have standards for **scalability** being covered. Does the system scale, when used in a large scale scenario?	Replicability / interoperability / sustainability	10%
5	Have standards for **interoperability** being used by the system?	Replicability / interoperability	10%
6	Can the standard be easily adapted to industry	Sustainability	10%

No.	Technical Evaluation Criteria	Applies to:	Checklist
	products?		
7	Is **reusability** of system components ensured?	Replicability / sustainability	15%
8	Is the system build in a **modular** and standardized fashion, so that it integrated into existing components with minimum overhead?	Interoperability / sustainability	15%
9	Is the implementation of the technical solutions (live cycle) cost effective?	Sustainability	5%
10	Can the system components be maintained in a standardized way?	Sustainability	5%
	Total:		**100%**

Table 4 - Replicability, Sustainability and Interoperability technical indicators

Regarding interoperability, we suggest to measure, based on the proposed research questions and hypotheses a set of indicators that shed a light on the cloud IoT data management enhancements for the autonomous driving features:

- Actual number of components connected to the IoT infrastructure
- Actual data flows between the components

To compute and assess indicators we suggest collecting the following data:

- Messages passing through the cloud IoT infrastructure
- Origin of a message
- Destination of a message
- Payload type

4 Use cases and services

In the next section, the methodology for evaluating the use cases and services is described. Even though the use cases may have different implementations in the Pilot Sites, the evaluation has been harmonized in order to be able to evaluate the use cases with the same KPIs in a comparable manner. Nevertheless, this is the first iteration of the evaluation methodology harmonization and it might happen that the methodology needs to be refined at some points in order to achieve a full harmonization. Eventual new updates on the methodology will be presented in the next deliverable of the task (D4.3).

4.1 Automated Valet Parking

Automated Valet Parking (AVP) is an automated driving function that can be integrated with different end-user services and scenarios. AVP is realized in AUTOPILOT in the pilot sites Brainport, Vigo and Tampere. Two major scenarios are addressed by AVP; the ‘drop-off’ and the ‘pick-up’ scenarios.

In the drop-off scenario a driver drives his vehicle to a specific drop-off area and stops the vehicle. After the driver has left the vehicle he sends his car via a smart-phone application to the parking area. The vehicle finds its route and parks itself automatically. This scenario has two variants for detecting empty parking spots:

- In the ‘camera’ sub scenario, road side cameras mounted along the route and on the parking area identify free parking spots.
- In the ‘MAV’ sub scenario, a drone (MAV: Micro Air Vehicle) hovers over the parking area to identify free parking spots.

In the pick-up scenario a driver waits at a pick-up area and calls his car back via a smart-phone application. The vehicle leaves the parking spot and drives to the pick-up area automatically. After the car has stopped at the pick-up area the driver gets in the vehicle and leaves the pick-up area.

In the basic versions of the drop-off and pick-up scenarios there are no obstacles blocking the vehicle’s route, and the vehicle selects the shortest and fastest route. In the ‘route’ sub scenario, there are obstacles blocking the shortest route. The road side cameras detect the obstacles and send the data via the IoT platform to the vehicle. The vehicle calculates the optimal (fastest) route to the free parking spot bypassing the blocked route.

For testing the AVP hypotheses the 'traditional parking' process is defined as a baseline. Traditional parking means that the entire parking process is done manually by a driver without the support of any IoT devices or IoT ecosystem. The traditional parking process starts from a predefined drop off into a parking space, and vice versa to the pick-up location, without the use of the smart-phone application, roadside units, cameras, Micro Air Vehicle (MAV) or IoT platforms.

4.1.1 Research Questions and Hypotheses

The main research questions are related on how the IoT based services can improve the efficiency of the parking process. Based on the main topics and the functions involved in the use case, we can derive the following research questions:

RQ: *Is the detection of free parking spots faster compared to traditional parking?*

HY: The parking slots are detected faster thanks to the use of the infrastructure of the parking and the IoT compared to the traditional parking.

RQ: *Is the fastest route selected (based on potential obstacles on the route) compared to traditional parking?*

HY: The IoT calculates the best route for the vehicle in order to reduce the distance and time to travel, which means that the route calculated should be the best option and, therefore, fastest than the traditional parking.

RQ: *Is the parking process faster compared to traditional parking?*

HY: The parking manoeuvres are done autonomously with all the environmental information thanks to the IoT, so, it should take less manoeuvres and time to park the vehicle into the parking spot.

RQ: *Is the driver reliably informed about the parking and pick-up process of the vehicle?*

HY: The IoT is correctly sending a notification to the smartphone of the user informing the status of the parking process.

Based on the log files generated during the tests (see chapter below) quantitative statements can be made about the improvement of efficiency in the context of AVP enhanced by IoT.

4.1.2 Technical indicators, measurements and metrics

The hypotheses can be tested using the following indicators:

- Parking duration
- Detection performance of free parking spots
- Optimal driving route to free parking spot
- Reverse parking process into a parking space
- Reliable information of the driver about the parking process

During the technical evaluation tests log files of the following components will be generated:

- Vehicle state log files
- Roadside unit log files
- Camera log files
- Micro air vehicle log files
- Communication log files
- IoT log files

4.2 Urban Driving

The main objective of the Urban Driving use case is to implement automated driving in urban environments taking into account the information provided by external sources that could be accessed via IoT platforms. In this way it is possible to extend the electronic horizon or situational awareness of the vehicle. The relevant external environmental information considered in the project is:

- Traffic light states at intersections
- Detections from infrastructure cameras (e.g. pedestrians, bicycle, obstacles, etc.)
- Information from vulnerable road users (VRU).
- Information from other vehicles captured by their own sensors and shared as IoT elements.
- Information about events in the road (e.g. traffic jumps, road works, accidents…) provided by traffic management centres through the IoT infrastructure.

In the project framework this function is going to be tested at the following pilot sites: Tampere, Versailles, Livorno, Brainport and Vigo.

The baseline scenario is where the automated vehicle uses its own sensors, and V2X communication with the road side units, to detect the environment and receive traffic light controller information. Urban Driving consists of the following pilot scenarios:

- **VRU interactions**. Receiving the information through an IoT platform, the vehicle can be informed that a camera or other sensor has detected pedestrians crossing a zebra crossing, allowing the car to adapt its speed before its own sensors detect the pedestrian.

- **Interaction with traffic lights and traffic signs.** When approaching the vehicle in autonomous driving mode at a controlled intersection, the tests will check whether the IoT improves safety and reduces travel times.
- **Approach to a road hazard:** By receiving the information through an IoT platform, the vehicle can be informed of hazards on the road such as road works, accidents or adverse weather conditions, allowing the car to adapt its speed before its own sensors detect the hazard.
- **Interaction with legacy cars and environmental data.** The same as before with the other cars on the road and the environmental data. We need to log the interaction with them to ensure the correct behaviour. The V2V messages and the vehicle data and sensors are the main indicators.

Urban Driving will also be tested in conjunction with the Rebalancing services on the Versailles and Brainport pilot sites.

4.2.1 Research Questions and Hypotheses

When evaluating the Urban Driving hypotheses, a comparative approach will be used between the system with and without IoT, in order to check whether it brings significant improvements to the user's safety and reduces travel times.

RQ: *What is the accuracy of anticipating (detecting and avoiding collisions with) VRUs, legacy vehicles and road hazards when IoT data management and communication are used?*

HY: The use of data generated by the IoT devices, e.g. carried by VRUs, vehicles or road side systems, or cloud services improves the accuracy of detecting VRUs, legacy vehicles and road hazards in vehicles.

HY: The use of data generated by the IoT devices, e.g. carried by VRUs, vehicles or road side systems, or cloud services improves the anticipation by automated and connected vehicles, e.g. earlier and smoother speed adaptation.

HY: VRUs receive warnings via IoT from detections by automated or connected vehicles can be

RQ: *Is the end user quality of experience (better traveling times, waiting times, and journey times) improved when IoT data management and communication are used?*

HY: The end user quality of experience (better traveling times, waiting times and journey times) is improved when IoT data is used.

4.2.2 Technical indicators, measurements and metrics

The following are indicators with respect to the case of using an automated driving car with and without IoT.

- **Speed profile variation comparison**. It will allow concluding if the IoT reduces travel times.
- **Acceleration profile comparison**. It will allow concluding if IoT smooths the accelerations and decelerations of the journey.
- **Number of hard braking events comparison**. It is expected that IoT will reduce the number of hard braking events by increasing the distance at which information is received from the environment.
- **Fuel consumption and CO2 emissions comparison**: As a consequence of the adaptation of the vehicle speed to the information received by IoT (e.g. the state of a traffic light) a reduction in fuel consumption and emissions are expected.

- **Time of detection of pedestrian by the vehicle**. The information received from the cameras will allow the car to adapt its speed before it detects the pedestrian with its own sensors.

4.3 Highway Pilot

Highway Pilot is an Automated Driving System which provides automated functionalities to highway driving, performing both longitudinal and lateral vehicle motion control in a specific operational design domain (i.e., only on Highways).

The monitoring of the driving environment is a key component for this system and is usually performed by on-board sensors characterized by a limited range and field of view. The AUTOPILOT IoT architecture is aimed at enhancing detection capabilities and automated responses of vehicles with respect to potential road hazards en route. Several events and situations can be identified as potential road hazards but the testing activities performed in Livorno and Brainport pilot sites will focus on road defects (potholes), weather related road changes (puddles), and road works.

Anomalies can be merged from different devices, sensors and algorithms, and from different sources such as private and service vehicles, other road users and personal devices, fixed road side sensors back office systems for planning road maintenance and constructions, or traffic information services.

The AUTOPILOT goal is to extract specific, reliable, and location-based alerts that can support the environment perception of automated vehicles in controlling speed and headway distance, anticipate and smooth lane change manoeuvres or deactivate the automated functions.

4.3.1 Research Questions and Hypotheses

IoT is expected to positively contribute to both the detection phase and automated responses. IoT can for example improve the number of detected events, accuracy of their localisation, and timeliness of detections, while also the effectiveness of the safety response and related comfort can improve. In such a context it is possible to identify two main research questions which will be hereinafter analysed, together with the underlying hypotheses and the technical indicators which can be used to test them.

RQ: *Can IoT improve situation awareness?*

In both Brainport and Livorno pilot sites, data collection, aggregation and event triggering through the IoT can feed the Autonomous Driving functions for the Highway Pilot, enabling a more effective data fusion for situation awareness. While Livorno focusses on the detection and aggregation from mobile probes, fixed sensors and road maintenance plans (road works), Brainport showcases how IoT enables the data sharing among different parties.

For situation awareness, the process is considered from the occurrence or emergence of the hazard, the detection, the collection of detections until validation of the hazard and the triggering of a validated hazard warning towards drivers and automated vehicles. The performance of detection and situation awareness is a trade-off between latency, reliability and accuracy of hazard warnings. On the one hand, the earlier a warning is published, the higher is the positive impact on traffic safety and efficiency. On the other hand, insufficient data collection and validation of hazard warnings increases the false alarm rate and negatively impact the trust and compliance of users to the warnings. To report extreme cases: discontinuous set of generic anomalies with low reliability in the next kilometres will simply cause the deactivation of the highway pilot on the whole highway. If this alerting has also some latency in being produced, it will maybe target just half of the interested AD vehicles (the other half having transited before); on the other hand, prompt, reliable punctual notifications can support longitudinal and lateral control by giving detection redundancy, and anticipating the danger.

Situation awareness improvements can be tested by the following hypotheses:

HY: IoT improves the detection performance of road hazards when anomaly detections are received and integrated from multiple and heterogeneous IoT data sources compared to using any single data source.

HY: Latency in validated hazard warnings can be reduced when using multiple and heterogeneous sources compared to using any single source of data.

***RQ:** Can IoT improve automated driving response and driver response?*

The highway functionalities are demonstrated by CRF and VALEO vehicles in Brainport and Livorno, respectively. The common, measurable functionalities in terms of vehicle response are: longitudinal speed profiling, timing headway from the vehicles in front, command to start lateral shift/lane change. In addition, for Brainport, activation/deactivation of AD can be measured (time it takes for the driver to take again the control of the car). In both vehicles, in addition, the CAN data are used for comparing the vehicle kinematics.

HY: validated hazard warnings and driving recommendations can target relevant vehicles based on location.

HY: Proposed hazard warnings and driving recommendations eventually result in a better handling of the hazardous situation by the vehicles and drivers.

4.3.2 Technical indicators, measurements and metrics

The hypotheses on anomaly detection and validation performance can be tested using detection performance indicators for detection rate, accuracy and latency. In both pilots, the anomaly detections are collected and validated by a human operator before publishing warnings and alerts to drivers and automated vehicles. Hence the false alarm rate of published warnings is not a relevant criterion to evaluate the added value of IoT.

- **Detection rate** is measured by the number and type of anomalies that are detected by single sources and after fusion and validation by the operator.
- **Detection accuracy** is measured by the location accuracy of anomalies and hazards by the single sources and after fusion and validation by the operator. Location accuracy is measured as the distance or offset between anomaly detections and the true hazard location. If the ground truth is unknown, the validated hazard location can be used as the metric.
- **Detection reliability** is measured by the rate of correct classifications of anomalies; i.e. the confusion matrix of true/false positive/negative detections. In this case, IoT enabled data fusion/aggregation could be compared with single in-vehicle sensors performance. In case the latter information is not available from the AUTOPILOT testing, one could refer to literature information about sensing performance.
- **Validation latency** is measured as the duration between first occurrence or detection of an anomaly and the triggering of the validated hazard warning to drivers and automated vehicles. This duration includes the collection of one or more anomaly detections, validation by the operator and triggering of the hazard warning. This duration includes implicitly the detection delay by any anomaly detection system generating the IoT anomaly detections. This indicator may be rather difficult to assess through real data only, given the limited numbers of vehicles and anomaly cases. However, at least some indications could be extracted by merging single detections on field (e.g. potholes) with traffic flow data. These should be confronted with single sensor performance.

The hypotheses on automated driving response and driver response can be tested using following performance indicators:

- **The latency between the triggering of the validated hazard warnings and initial response**

of the driver or automated vehicle functions. This indicator measures the IoT "service chain" after validation, from the IoT platform to the AD vehicle data fusion, and it could avail of timing checkpoints: data communication (section 3.2), IoT data management and the evaluation of the relevance of IoT data for data fusion, actuation and application logic (section 3.1). For immediate local warnings response can be defined from the AD vehicle kinematic response (speed, etc.) or more in general the AD activation/deactivation, or presentation of driver warnings. However, this is not valid for warnings that are stored in the car and taken as input later on.

- **Smoothness in longitudinal and lateral manoeuvres** of automated responses. The speed profile could be measured, time-and position-reference, with and without the IoT warning (section 3.3).
- **Occurrence of emergency responses** such as hard braking or steering. Kinematics data of the vehicle during the trials could be measured (with and without the IoT warning) to check if there are peak events (sharp braking, deactivation of AD, etc.). Actually, it is quite difficult to obtain an indicative and robust measurement with such a small amount of expected AD vehicles statistics on the specific site, so it is suggested to try and compare the data with ordinary traffic data, if available from the road operator.

4.4 Platooning

Platooning is an automated driving function that can be integrated with several end-user services and scenarios. In AUTOPILOT, platooning is implemented in two different scenarios; i.e. as a function in the car sharing service in Brainport, and as a function for automated fleet rebalancing and parking in Versailles. Consequently the pilot scenarios and situations in which platooning are executed will be different. For example in Brainport, platooning brings end-users from their pick-up point to their destination, while in Versailles platooning returns empty vehicles back to a pick-up point. In Versailles the automated vehicles travel at moderate speeds in an urban environment, while in Brainport the vehicles also travel on the motorway.

This section addresses the common two automated sub functions: platoon formation and platooning. Platoon formation is the process of searching other vehicles and match making to organize a platoon, to navigate the vehicles to a rendezvous point in time, and to organize the vehicles to form and join a platoon. Platooning is the automated driving function to control a string of vehicles as a platoon through traffic.

Both platoon formation and platooning can be considered as processes with a state machine with an entry event (1), main activities (2) and an exit event (3) to the next state or process in the pilot scenario.

Platoon Formation

1. Both implementations at Brainport and Versailles have a process to form the platoon of automated vehicles.
    a. A user (operator or driver) initiates the platoon formation with a request to a cloud service (Fleet Management System or Platooning Service) to form a platoon.
    b. The initial request triggers a platoon formation process in the cloud service. The internal process of the cloud service is not in scope of the research questions or evaluations.
    c. The outcome of the cloud service processing is a reply IoT message to every vehicle in the platoon with instructions on the location where the platoon should be formed, its position or relative location in the platoon, and instructions how to get to the location in the right order.
2. The platoon formation activity starts in the vehicle upon reception of the instruction from 1c.
    a. Upon receipt of the instructions in the vehicle, a route is constructed as a trajectory

of set points to the rendezvous point.

   b. The vehicle starts driving (automatically) towards the rendezvous point.
   c. Upon any deviation or obstruction, the vehicle sends an (IoT) message to inform the cloud service and other platooning partners of the deviation. This step may not exist in the implementation in Versailles.
      i. The deviation message may trigger an updating process in 1b, and consequently in 1c and 2a.
      ii. The platoon formation process may not succeed to form a platoon and can also be aborted, manually or automatically.

3. The platoon formation ends when the platoon is formed, or the process is aborted. Successful platoon formation is an event that is detected by the platoon formation function in the vehicle. The cloud service or other platooning vehicles are informed with an (IoT) status update message. The criteria for successful platoon formation and the detection may differ per implementation:
   a. The operator or driver in the vehicle decides that the platoon is formed and initiates the platooning phase.
   b. Alternatively the vehicles in the platoon detect the successful platoon formation state and proceed to platooning.

Platooning

1. The entry event is that the platoon is successfully formed, and automated platooning is initiated. In both the Brainport and Versailles implementations, the lead vehicles are manually driven, and the other vehicles follow the leader automatically through traffic.
2. Platooning activities can be differentiated in following simultaneous processes:
   a. Car following:
      i. Longitudinal control in which a gap is maintained with minimal fluctuations.
      ii. Lateral control in which the leader is followed in his lane and path with minimal lateral deviations.
   b. The lead vehicle requests and receives traffic information and traffic management, such as the traffic light states, traffic light priority, lane priority, and congestion. The driver in the lead vehicle has the responsibility to adapt driving to the situation and information. The information is sent and received as I2V and / or IoT messages. The reception of such a message can trigger a reaction of the driver or vehicle controller as an event, such as a speed adaptation, stopping for an intersection or obstacle, or a route change.
3. Platooning is ended by the driver in the lead vehicle, either because the destination is reached, or by intervention.

Evaluation of all topics from section 3 is highly relevant and provides input for the evaluation of the platooning use case. The methodology evaluates how IoT can affect these events and activities and improve or enable automated driving functions. The following basic steps are applied:

1. Define criteria to measure the performance of the automated functions in step 2 of platoon formation and platooning, including positioning, localization and navigation (section 3.3).
2. Define the timing and triggers of the events and activities in steps 1 – 3 of platoon formation and platooning, including the reception and relevance of IoT and V2X messages from data communication evaluation (section 3.2) and data management (section 3.1).
3. Associate the IoT related triggers and events from 2 to patterns in the performance of 1.

4.4.1 Research Questions and Hypotheses

The main research question “How can IoT improve platooning?” can be refined in sub questions addressed in the following sub sections. The baseline scenario is that vehicles are already equipped with V2X communication, automated longitudinal and lateral control, and platooning functionality.

The connection to the IoT platforms is added to test potential improvements of platoon formation and platooning, and to classify the improvements as accelerating, enhancing or enabling.

RQ: *Can IoT improve match making for platoon formation?*

This is the first step in the platoon formation process described above, where passengers and vehicles have to be matched to start the platoon formation process. This is also an important capability for integrating platooning in mobility service concepts such as car sharing and rebalancing

In baseline situations, the vehicles can only communicate using V2X to find potential other vehicles. The vehicles, however, do not have the functionality to organize a platoon, i.e. agree a suitable rendezvous point, navigate to that point, arrive in the intended order and initiate and join the platoon. Hence the platoon formation service is enabling these new services.

HY: Provide discovery services, car sharing or ride sharing services to search and match passengers and vehicles to form platoons with compatible travel plans, origins and destinations, and platooning capabilities.

HY: Extend the scope for searching drivers and vehicles beyond the local V2X ad-hoc communication network and communication range.

RQ: *Can IoT improve platoon formation?*

This is the second step in the platoon formation process, starting with the first platoon formation instructions.

In the baseline situations, the test vehicle would have to navigate to the rendezvous point. In the test scenarios, IoT information is provided for re-routing and updating the rendezvous point or expected time of arrival of the host vehicle or other platoon members. The routing efficiency of in-vehicle or cloud services is not subject of evaluation.

HY: A host vehicle is informed of any delays or problems in the activities of other platoon members that affect the platoon formation of the host vehicle.

HY: A host vehicle receives updated instructions how to adapt its platoon formation activities in coordination with the other platoon members.

RQ: *Can IoT improve platooning?*

This is the activity (step 2) in the platooning process. This evaluation may also apply to automated driving to the rendezvous point (step2) in the platoon formation process.

In the baseline situation, the following vehicles are assumed to be capable of platooning and car following. The added value of IoT is to provide environmental and situational information that improves the performance of platooning; assuming the driver in the lead vehicle uses the IoT information efficiently. The evaluation is divided in two parts:

1. Evaluation of the data management of in-vehicle and cloud IoT platforms to discover, request and provide relevant data on traffic state, congestion, traffic lights, traffic incidents and accidents, map or location information, or other road hazards for example from the highway pilot use case. These are examples of data management evaluation (section 3.1).
2. Assuming data management is successful in delivering relevant information and the (lead) vehicle uses to this information to improve platooning, and then this section evaluates the performance improvements of platooning.

HY: Vehicles can subscribe to IoT information that may also be available from V2X communication to improving the communication performance.

HY: Vehicles can subscribe to IoT information that is relevant for improving platooning. Relevance is defined by the potential improvements:

- Relevant to improve the accuracy of localization on the road, e.g. for map updates or hazard locations, to reduce fluctuations in longitudinal gap control and lateral control (lane keeping or changing).
- Relevant to improve the accuracy of object location, e.g. environment detections, to reduce the fluctuations in longitudinal or lateral gap control and car following, and to avoid conflicts or reduce to risk on conflicts. Effects should be differentiated for interactions within the platoon, with surrounding vehicles, vulnerable and other road users or physical objects.
- Relevant to anticipate traffic situations ahead, like congestion, (controlled) intersections or hazards, and smoother or earlier adaptation of speed, gap, lane or route.

4.4.2 Technical indicators, measurements and metrics

Indicators to test the hypotheses on match making are:

- Percentage of successful matches of test vehicles for platoon formation.
- Causes for failed matching attempts.
- Duration of successful matching between initial request by a test vehicle and first instructions for platoon formation.
- Range between test vehicles for successful match making.

Indicators to test the hypotheses on platoon formation are:

- Delay between the detection of an issue in the execution of the platoon formation in one test vehicle and the reception of updates of the platoon formation instructions.
- Percentage of received instruction updates.
- Causes for failed instruction updates, such as detection or communication failures. If instructions are received to abort the platoon formation, then this is also classified as a "successful" update.
- Percentage of successfully completed platoon formations.
- Causes for failed platoon formations, such as technical failures of a vehicle, driver interventions, delays due to traffic congestion or traffic lights, incorrect vehicle order, and abort instructions.
- Delay between arrival of the first and last vehicle at the rendezvous point.

These indicators can be measured or calculated from the application logging of the platoon formation service and communication. The evaluations are examples of IoT data management evaluations (section 3.1) and data communication (section 3.2):

- Successful matches and platoon formation instructions are logged as events and actions in the applications of the in-vehicle and cloud services, and can also be extracted from the communication of standardised IoT messages such as "platoon_formation" and "platoon_state" messages. Table 5 - Platform formation eventslists the events and actions that are defined for the application logging in Annex 7.1.3. An event model defines the relevant actions that an application can make for a specific service. The cloud service for platoon formation for example can take three decisions; initialisation with a message to the intended platoon leader, and new and updated formation messages with a rendezvous point and ETA to all participating vehicles. Events are also defined for the discovery of platoon services, assignment and acknowledgement of the state of a vehicle in the platooning process, and the role of a vehicle in the platoon.
- Failures and detected causes are also included in the application logging (see Annex 7.1.3 for details and examples).
- Statistics on successes and failures, durations and delays ranges can be calculated from the actions.

Event Model	Action / Decisions
Discover Platoon Service	1. send request for service discovery 2. receive discovered services list 3. send request for service subscription
Platoon Formation	1. initialisation to platoon leader 2. new join for new follower 3. update join with
Platoon State	1. None 2. Standalone 3. VehicleEngaging/Assembling 4. Platooning 5. VehicleDisengaging 6. DisengagingAll
Vehicle Role	1. None 2. Standalone/Ready-for-leading 3. Trailing 4. Following 5. Leading 6. Ready-for-leading

Table 5 - Platform formation events

Indicators to test the hypotheses on platooning are:

- **Longitudinal control**. Fluctuations in gap time or distance, accelerations and string stability.
- **Lateral control for lane keeping and lane changing**. Fluctuations in lane location and accelerations.
- **Anticipation to traffic situations and obstacles**. Distance and lead time to start adapting speed, gap, and lane or update the route.

These indicators are examples of the evaluation of positioning, localisation and environment detections in sections 3.3 and 3.4:

- Ranges between vehicles during platoon formation and the accuracy of the final platoon formation
- Relative positioning as gaps between platooning vehicles
- Relative location of test vehicles on the road and lane
- Relative location of objects
- Correlation between relative and absolution positions of objects
- Delay in detection of targets and objects in the automated functions of test vehicles from different sources; i.e. on-board sensors, V2X communication and received IoT information
- Accuracy and reliability of object classification from these different sources

Differences in the communication performance of V2X communication for platooning and of IoT messages, such as the communication reliability, range and latency are evaluated as presented in section 3.2.

The functionality and performance of IoT data management is evaluated on the vehicle IoT platform as well as on the platoon formation cloud service in terms of the relevance of the received data. These are examples for the evaluation in section 3.1. The relevance can either be determined by:

- Explicitly measured and logged by the automated driving functions and applications on the vehicles. Relevance can be measured for example as:
  - Timeliness of information received from different sources; i.e. is it received in time to react
  - Location where information is detected or received and remaining distance to the event location.

  - Quality of the received data e.g. is the accuracy and confidence of an event location.
- Implicitly derived from the platooning performance, for example from changes in the control and anticipation.

4.5 Car Sharing

4.5.1 Technical Research Questions and Hypotheses

To assess a car sharing use case we will investigate a top level research question and verify a set of corresponding hypotheses provided below. The top-level research question is:

RQ: *Is the end user quality of experience (traveling times, waiting times and journey times) improved when IoT infrastructure is used in the car sharing application?*

It is expected that by leveraging the IoT infrastructure the car sharing application will be able to provide more accurate pick-up and drop-off time as well as more reliable and robust routing information either to the driver or to the AD functionalities, and, in overall, will improve user quality of experience.

Having mentioned that, we believe that usage of IoT infrastructure will prove following hypotheses:

HY: Pick-up and drop-off delays are reduced when IoT infrastructure is used.

HY: Journey times are reduced when IoT infrastructure is used.

HY: The number of the un-predicted events is reduced, and the overall travel time is decreased to due to better routing.

4.5.2 Technical indicators, measurements and metrics

The following are the indicators with respect to the case of using a personal car without car sharing should be used for the evaluation purposes:

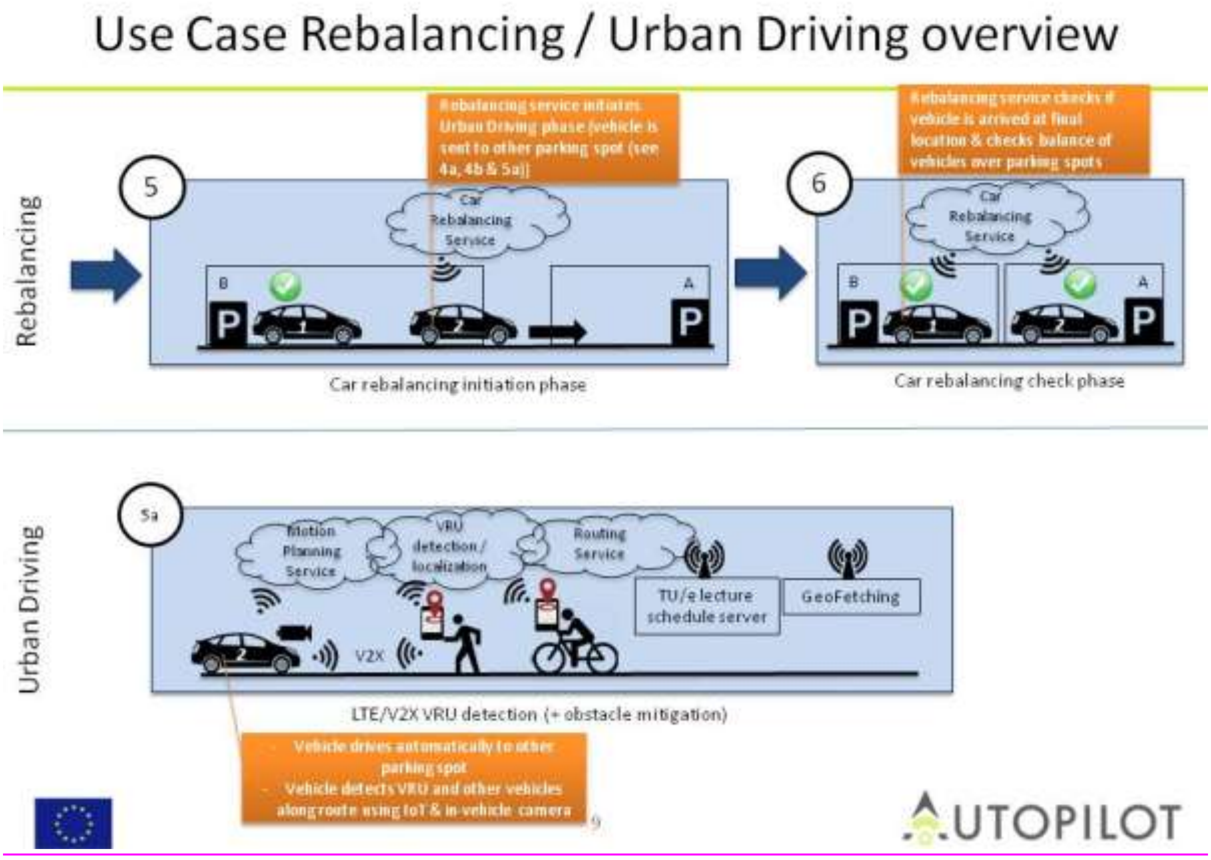
- Cumulative travel times
- Cumulative travel distance
- Average waiting time for customers (outside the specified time window)
- Distribution of waiting times
- Probability of constraint violation (pick-up and drop-off outside the specified time windows)

Specified above indicators are solely available for collection from the data available in the car sharing use case implementation and barely derivable from the other sources in the project, like IoT-platforms. We suggest computing specified indicators in the car sharing applications itself or in a separate application that may be considered as a part of the use case. In this case no additional measurements and metrics are required to expose to the external consumers for the technical evaluation.

4.6 Car Rebalancing

A Car Rebalancing service receives requests to manage the demand of vehicles at specific locations, relocate vehicles if necessary, and handle any events during the relocation. Car Rebalancing is a service that is piloted in scenarios with other use cases. In Versailles, Car Rebalancing service is used in the Platooning use case. In Brainport Car Rebalancing is used as part of the Urban Driving use case. The use case specific events, such as delays due to traffic lights and avoiding collisions with Vulnerable Road Users (VRUs), are covered in the respective sections and technical evaluations.

When evaluating the Car Rebalancing service, a comparative approach will be used between the system with and without IoT, in order to check whether it brings significant improvements to route calculations and event detections. The scenario in Figure 3 will be used to evaluate the service.



Use Case Rebalancing / Urban Driving overview

Rebalancing service initiates Urban Driving phase (vehicle is sent to other parking spot (see 4a, 4b & 5a))

Rebalancing service checks if vehicle is arrived at final location & checks balance of vehicles over parking spots

Car rebalancing initiation phase

Car rebalancing check phase

LTE/V2X VRU detection (+ obstacle mitigation)

- Vehicle drives automatically to other parking spot
- Vehicle detects VRU and other vehicles along route using IoT & in-vehicle camera

Figure 3 Car Rebalancing overview

Precondition

A vehicle has been parked at pre-defined parking spots. Rebalancing service has already checked that there is a need for 1 vehicle to move from parking A to parking B & initiated that vehicle to start moving.

Actions or events

1. Vehicle receives crowd information from the lecture schedule and/or CEMA to check optimal time and route to drive (possibly manual set).
2. Vehicle drives to other parking spot.
3. VRUs are crossing the street in front of the vehicle.

Relevant situations

1. Vehicle detects VRUs on route towards other parking spot
2. VRUs receive warning of approaching AD vehicle on their smartphones

Baseline

1. While driving: detecting VRU equipped with an ITS-G5 unit, compared to VRU equipped with a smartphone having an app. Both communicating GPS locations to the vehicle.
2. Without driving: vehicle needs to receive a trigger from the rebalancing service (IoT cloud) to start driving. Baseline: only possible manually.

Results

1. Vehicle detects VRU also out of line of sight of in-vehicle sensors (using both ITS-G5 as well as 4G of smartphones) and brakes earlier.
2. Vehicle detects crowdedness through high level of Wi-Fi sniffing activity and decides on different routing.

4.6.1 Research Questions and Hypotheses

From this scenario, we can derive the next research questions and hypotheses:

***RQ**: Is the tracking and communications of VRUs fast enough so that their locations can be sent to automated cars and be used for **IoT enhanced AD**?*

***RQ:** Can IoT be used to dynamically relocate AD vehicles, based on crowdedness and demand?*

HY: IoT will extend the detection of VRUs over longer distance (from blocked view).

HY: IoT will warn VRUs of an approaching AD vehicle through their smartphones.

HY: IoT will enable relocating AD vehicle more efficiently, by checking blocked routes (crowdedness).

4.6.2 Technical indicators, measurements and metrics

The indicators to test these hypotheses are the functionality and performance of positioning, localization and environment detections:

- Absolute location of AD vehicles on the TU/e campus
- Relative location of VRU
- Correlation between relative and absolution positions of objects
- Delay in detection of targets and objects in the automated functions of test vehicles from different sources; i.e. on-board sensors, V2X communication and received IoT information
- Matching of crowd estimation data with actual detection/localization by use of vehicle sensors
- Accuracy and reliability of object classification from these different sources
- Vehicle dynamics sensors: longitudinal & lateral accelerations
- Travel time end-to-end (driving from A to B location according to test routes)
- Reaction time of VRU on approaching AD vehicle

5 Conclusion

This document presents the methodology that will be used to evaluate the IoT technologies applied to the autonomous vehicles at the different Pilot Sites. The definition of this methodology was started in deliverable D4.1. This document, D4.2, sets the KPIs, and the measurements needed to compute them, that will be used to evaluate the Use Cases and Services implemented at the Pilot Sites. Furthermore, it sets the methodology for the assessment of the developed IoT systems' safety, interoperability, replicability and sustainability of the IoT architectures, and the security and privacy of the solutions. Given the diversity of implementations in the different Pilot Sites, an effort has been made to define KPIs and measurements that can be carried out in all the Pilot Sites in order to achieve an evaluation that allows for a fair comparison of the implementations. This has required an effort in the coordination with the different pilot sites and, in some cases, it was necessary to adapt some measurements in order to achieve this goal. Nevertheless, this is the first iteration of the evaluation methodology harmonization and it might happen that the methodology needs to be refined at some points in order to achieve a full harmonization. Eventual new updates on the methodology will be presented in the next deliverable of the task (D4.3).

The described methodology will be applied in the activities of Task 4.2 based on the data collected by the pilots during their piloting activities and made available through the Central Data Server. D4.3 will present the results of this evaluation.

Topics	Evaluation	Assessment
Data Management (Performance)	✖	
Data Communication (Performance)	✖	
Position, Location and Navigation (Performance)	✖	
Environmental Detections (Performance)	✖	
Safety		✖
Security		✖
Privacy		✖
Replicability, Sustainability and Interoperability		✖

Table 6 - Evaluation - Assessment Topics

6 References

[1] *AUTOPILOT Deliverable D4.1 – Methodology for Evaluation, available on Project Place https://service.projectplace.com/pp/pp.cgi/r1690653003.*

[2] *Report of the World Commission on Environment and Development: Our Common Future, http://www.un-documents.net/our-common-future.pdf.*

[3] *AUTOPILOT PILOT PLAN TEMPLATE.xlsx, available in Annex 7.3 and on Project Place https://service.projectplace.com/pp/pp.cgi/r823175960.*

[4] *AUTOPILOT Deliverable D2.3 - Report on the Implementation of the IoT Platform, available on Project Place https://service.projectplace.com/pp/pp.cgi/r13061162.*

[5] *AUTOPILOT Deliverable D1.7 – Initial specification of communication system for IoT enhanced AD, available from Project Place https://service.projectplace.com/pp/pp.cgi/r1610425663.*

[6] *AUTOPILOT Deliverable D2.1 - Vehicle IoT Integration Report, available from Project Place https://service.projectplace.com/pp/pp.cgi/r1564018789.*

[7] *AUTOPILOT Deliverable D2.6 – Readiness verification report per pilot site per use case, available on Project place https://service.projectplace.com/pp/pp.cgi/r354064418.*

[8] *AUTOPILOT Deliverable D1.9 Initial Specification of Security and Privacy for IoT, https://service.projectplace.com/pp/pp.cgi/r1770325159.*

[9] *AUTOPILOT Deliverable D5.7 Standardisation plan https://service.projectplace.com/pp/pp.cgi/r1299785435.*

[10] *AUTOPILOT Deliverable D5.3 - Performance and KPIs for autonomous vehicles and IoT pilot impact measurement, available on Project Place https://service.projectplace.com/pp/pp.cgi/r13061162.*

[11] *InterCor Common Log Format Description, version 0.7.7, available from the TEST FESTS specifications on the InterCor project website, on http://intercor-project.eu/.*

[12] *AUTOPILOT Common Log Format Description – Extension, version 0.7.7, available from Project Place https://service.projectplace.com/pp/pp.cgi/r1080659892.*

[13] *The Mapillary Vistas Dataset for Semantic Understanding of Street Scenes, available on http://research.mapillary.com/publication/iccv17a/.*

[14] *ISO TS 19321:2015 (2015-04-15). Dictionary of in-vehicle information (IVI) data structures.*

[15] *AUTOPILOT Deliverable D2.1 - Vehicle IoT Integration Report, available from Project Place https://service.projectplace.com/pp/pp.cgi/r1564018789.*

7 Annexes

7.1 Log data specifications

This annex presents a set of specifications for structured logging to collect the measurements needed for evaluation. The basis for the specifications is provided by the InterCor project in [5] . It provides the rational, structured approach, requirements and specifications to harmonise the log data from various sources and types. These InterCor specifications are extended for automated driving functions and IoT messages in AUTOPILOT in [6], in particular for vehicle data, automated driving functions and services and for IoT messages. This annex highlights the most essential information for logging in AUTOPILOT. The reader is referred to the living documents in [5] and [6] for the updated and detailed specifications.

The approach to logging is based on several basic assumptions:

- A logical entity, such as a vehicle, device, or server, is called a station and has a globally (or project) unique identifier; the **log_stationid**.
- Every station organises and provides its own logging. The station may have one or more data sources, sensors, devices, units or applications that generate logging; the log_application. Every log_application has unique id within the log_stationid; the **log_applicationid**.
- All log information must be timestamped with a **log_timestamp.** This is the timestamp at which the log_application logs the information. This is not necessarily the timestamp at which data is generated, sent or received.
- The role of the log data in a data flow must be logged as the **log_action**. In communication for example the log_action identifies whether the message is 'SENT' or 'RECEIVED'.
- Data sources provide a data set or a message at a time to be logged by the log_application; a **log_item.** Every log_item must be logged with the meta data: log_stationid, log_applicationid, log_timestamp, log_action.
- All log data from all log_stations is collected in a central data base. Therefore:
    - All log_stations should be time synchronised and provide time-synchronised data.
    - To organise data, all log data should be collected per test run, session or experiment that has to be analysed and evaluated collectively.
    - To avoid logging duplicate data, the basic assumption is that the:
        - Provider, generator or sender of data should log all relevant data, including the unique identification information.
        - Consumer or receiver logs at least the unique identification information.
        - Application specific interpretations of data should be logged. Derived data does not have to be logged.
    - The unique identification information of log_items is defined per log_item.
- All timestamps are in a single time format: Coordinated Universal Time (UTC) in milliseconds since UNIX epoch (number of milliseconds that have elapsed since January 1, 1970 (midnight UTC/GMT).
- All locations or positions are in WGS84 coordinates: latitude, longitude, bearing/heading. Latitude and longitude should be in degrees with 10^-7 precision.

Log data is specified at 4 levels:

1. Definition of log parameters and organisation by data sources.
   Log parameters should be defined once, and reused by every data source that generates similar parameters.
    - Log parameter names are unique and generic, and do not include the name of the data source. To avoid conversion issues between tools, parameter names contain no capitals (no camel case).

   - A log_item organises all mandatory and optional parameters of a (type of) data source that are logged simultaneously (with the same log_timestamp).
2. Encodings of messages, for example in XML, JSON, or protobuf.
3. File formats, for example in CSV or XML.
4. Database structure in SQL.

The rational for the four levels is that, once the parameters and their organisation are agreed, every pilot site, partner or device can use standard or proprietary tools to encode, collect, store and manage the data. Afterwards, standard tools can be used to harmonise all data in a central data store of choice by a project or partner for data analyses and evaluations.

Specifications of log items and parameters are organised in several layers:

- Vehicle data
- Communication messages
- Application logic
- HMI events

The rational for defining layers of logging is to enable or disable logging for specific purposes such as for verification, validation or specific evaluations. Whether parameters are mandatory or optional for specific purposes is indicated in the specifications of the parameters.

The following subsections provide specifications for the log parameters and structure by data sources for different types of devices and logging components. The current specifications and requirements are maintained in spreadsheets as living documents that will be updated throughout the project.

7.1.1 Vehicle Log Data

In order to reduce the complexity of working with several data formats, a spreadsheet is defined among WP2, WP3 and WP4 where all the vehicle data is listed and the format is harmonized.

This spreadsheet provides the mandatory metadata that needs to be logged with every message and the data vehicle related needed for the evaluation. The data is divided in different tabs:

- Vehicle. Data collected from in-vehicle sensors.
- Positioning system. Positioning information provided by GNSS systems.
- Vehicle dynamics. Data describing vehicle dynamics and kinematics.
- Driver-Vehicle interaction. Data describing the interaction between driver and vehicle.
- Environment sensors (absolute and relative). Data describing the external environment.

Moreover, a part of the data format, the spreadsheet also contains the input from Technical Evaluation which consists in describing each measure as mandatory or optional for each technical topic. Finally, each Pilot Site has also provided their feedback saying if they are able to provide the measure or not.

AUTOPILOT_VehicleLogFormat_<version>.xlsx: last version available here:

AUTOPILOT_VehicleL
ogFormat_v0.6.0_TE

7.1.2 Communication Log Data

Communication Logging is the logging of the messages that are sent or received by a station via any communication medium, path or channel. The main purpose for communication logging is the data communication evaluation. Communication logging may also be used to minimize the logging for other purposes though. The contents of logged messages for example may also contain kinematic data (position, speed), other vehicle data and application data that can be extracted for evaluation.

The **log_action** in the meta data for logging identifies whether a logged message is 'SENT' or 'RECEIVED' by the log_stationid. The meta data extended with a label to identify the communication medium or channel is the **log_communicationprofile**. This enables to distinguish the performance of similar messages exchanged via peer-to-peer or ad-hoc communication and via IoT platforms for example.

To trace individual messages a unique message identifier is needed. Specific data elements are defined in the C-ITS message standards to uniquely identify messages across stations. Tracing of messages across IoT devices, IoT platforms and cloud services is not provided in the oneM2M standard, nor in all standard IoT message types in [4]. As an alternative a universal unique identifier (log_messageuuid) parameter is introduced in the logging meta data. Usage of this log_messageuuid assumes that the uuid is also included in the IoT message and used for logging by all receiving IoT devices, platforms and services.

InterCor_CommonCommunicationLogFormat_<version>.xlsx; latest version available here:

InterCor_CommonCo
mmunicationLogForm:

AUTOPILOT_CommonCommunicationLogFormat_extension_<version>.xlsx; latest version available here:

AUTOPILOT_Commo
nCommunicationLogF

7.1.3 Application Log Data

Application logging is the logging from the applications on vehicles, devices and cloud services that implement automated driving functions and services. Application logging is not restricted to software applications, and also includes control functions and HMIs to interact with human drivers for example.

Applications are typically proprietary implementations, even more so than vehicle data providers and communication units. For evaluation purposes though, applications can be considered as a black box component providing specific *high level* functionality. This high level application logic can be modelled by simple state machines to handle specific events that are relevant for evaluation purposes. Example of such events are the events for platoon formation in section 4.4.2 and hazard warnings for C-ITS messages in [5].

The application logic is represented by a set of event models. Examples of event models are the sending and reception of messages, classification of the relevance, role of a vehicle in a platoon, road hazard, and control decisions to be made. The logic within an event model is represented by a set of possible event actions that the application can take. Examples of actions for the classification of relevance are the classifications of time validity, location proximity and information quality. Examples of actions for control decisions are the longitudinal and lateral control modes.

Event models and actions can be defined simply as qualifications, classifications or enumerations. They can also be quantified with parameters for relevance, proximity or control settings for example. This makes the rational and implementation of application logic implementation independent, and easily reusable between use case implementations and projects. More details and examples are provided in following format specifications.

InterCor_CommonApplicationLogFormat_<version>.xlsx; latest version available here:

InterCor_CommonAp
plicationLogFormat_v

AUTOPILOT_CommonApplicationLogFormat_extension_<version>.xlsx; latest version available here:

AUTOPILOT_Commo
nApplicationLogForma

7.2 Standards implementation list for replicability, sustainability & interoperability

Based on the outcome of D5.7, the list of standards from that deliverable will be used to evaluate on the Pilot Sites the level of implementation of standards in use of replicability, sustainability and interoperability (see section 3.8)

T4.2_Standard-list-Im
plementation.xlsx

7.3 Pilot Plan

The Pilot Plan contains all the information to reproduce and evaluate on use case on each Pilot Site. The Technical Evaluation tab has been described in Section 2.5.

AUTOPILOT_PILOT
PLAN TEMPLATE.xlsx

7.4 Security Questionnaire

Physical security	
Are wayside devices able to detect physical attacks?	*Result*
Are on-board devices able to detect physical attacks?	*Result*
Is the system able to response, manually or automatically, to a physical attack (e.g. by revoking keys, disconnecting networks)?	*Result*

Table 7 - Physical security questionnaire

Wired network security	
Are the cloud, wayside and on-board networks segregated at least logically using e.g. firewall rules, routing policies, etc.?	*Result*
Are network devices configured with non-default/minimal configurations so to minimize attack surface?	*Result*
Are critical on board networks physically (or at least logically) separated from non-critical on board networks?	*Result*
Are wired devices allowed to connect to the network only after authentication (e.g. 802.11x)?	*Result*

Table 8 - Wired network security questionnaire

Wireless network security	
Are wireless devices allowed to connect to the network only after authentication (e.g. 802.11x)?	*Result*
Are messages sent over not encrypted radio channels protected against sniffing and spoofing?	*Result*

Table 9 - Wireless network security questionnaire

Device security	
Are device application and OS updates verified for authenticity?	*Result*
Are all devices inventoried?	*Result*
Are devices' configurations stored into a configuration management system?	*Result*
Are device backups securely stored and made available for device disaster recovery?	*Result*
Have the devices been hardened by e.g. making sure that the "attack surface is minimized" (closing ports, uninstalling unused components, etc) and that the configuration and authentication/authorization mechanisms are properly designed to minimize risks related to wrong/default configuration?	*Result*
Are devices' application and OS components remotely upgradable to fix vulnerabilities?	*Result*

Table 10 - Device security questionnaire

Log availability	
Are application level log messages securely stored and made available for accountability checks?	*Result*
Are device clocks synchronized so that complex events that involve multiple devices are detectable?	*Result*
Do log messages contain information to trace the source of events/commands in a secure way?	*Result*
Are log messages from field and remote devices collected to a central secure location where they can analysed and correlated?	*Result*

Table 11 - Logs availability questionnaire

Application security	
Do applications follow the least privilege principle?	*Result*
If applications use COTS (libraries, servers, etc.), is it available an updated list of vulnerabilities of such components?	*Result*
Are Autopilot developed applications hardened and/or tested against common security related coding errors (e.g. static analysis, fuzzing)?	*Result*
Are critical software components protected by techniques (e.g. secure code execution) to prevent compromised copies of the component to be run?	*Result*

Table 12 - Application security questionnaire

Protocol security	
Is sensible information transferred through secure and authenticated protocols?	*Result*
If applications employ non-encrypted protocols, are such protocols only used over secure connections (e.g. VPNs)?	*Result*

Table 13 - Protocols security questionnaire

User / device authentication and authorization	
Are all the Autopilot users required to authenticate and be authorized to use or control the available services?	*Result*
Are all the devices required to authenticate themselves before being able to operate within the Autopilot networks?	*Result*

Table 14 - User / device authentication and authorization questionnaire

Perception of security and user acceptance	
Are the users disturbed by being required to always be authenticated to the autopilot service before using them?	*Result*
Ideal security devices should be almost transparent to the users. Do the users perceive the Autopilot security measures as an element that disturbs their human machine interaction?	*Result*
Are users worried by the harms connected to vulnerabilities of AD cars and appreciate the security features as potentially lifesaving features?	*Result*

Table 15 - Perception of security and user acceptance questionnaire

7.5 Privacy questionnaire

If the use case employs user registration and/or authentication the flow of user information must be described and all the information of the questionnaire has to be provided.

Layer	User information	Translation	Persisted
User application	*Result*	*Result*	*Result*
Application specific layer	*Result*	*Result*	*Result*
IoT platform	*Result*	*Result*	*Result*

Table 16 - User information

List information provided by the Application specific layer:

Type of information	Details	Access control
Position information	*Result*	*Result*
Unique identifiers of actors	*Result*	*Result*
Video data	*Result*	*Result*

Table 17 - Information provided by the Application

List of information provided by IoT platform:

Type of information	Details	Access control
Position information	*Result*	*Result*
Unique identifiers of actors	*Result*	*Result*
Video data	*Result*	*Result*

Table 18 - Information provided by IoT Platform

List of information submitted into the IoT platform:

Type of information	Details	Access control	Treatment (anonymization/transformation)
Position information	*Result*	*Result*	*Result*
Unique identifiers of actors	*Result*	*Result*	*Result*
Video data	*Result*	*Result*	*Result*

Table 19 - Information submitted into the IoT Platform