SHared automation Operating models for Worldwide adoption

SHOW

Grant Agreement Number: 875530

D4.1: Open modular system architecture and tools - first version

This report is part of a project that has received funding by the European Union's Horizon 2020 research and innovation programme under Grant Agreement number 875530

Legal Disclaimer

This report is subject to a disclaimer and copyright. This report has been carried out under a contract awarded by the European Commission, contract number: 875530. The content of this publication is the sole responsibility of the SHOW project.

Executive Summary

In cities, where public transportation (PT) plays a critical role, the orchestration of the newly introduced Autonomous Vehicles (AVs) within the PT system emerges as a prosperous line of research for improving inter-modality, performance and individualization of the transit service. Towards rapid implementation, high bandwidth communication availability coupled with modern service-oriented data platform architectures harvesting rich streaming data from connected PT users, infrastructure and systems along with AI enabled tools for smart big data analysis provide the required momentum and the accompanying software framework for the road transport Web of (moving) Things to flourish.

As part of the automotive industry changes focus from vertical, industry-based approaches, to delivering horizontal solutions across multiple industries (e.g., Internet of Things that *move*), an expanding industry ecosystem is being created that includes OEMs and their Tier 1 suppliers, cloud services providers, connected vehicle platform providers, independent software vendors and system integrators. All these actors need access to the *data*, *interfaces* and *services* offered by vehicles (this includes cars, trucks, bikes, buses, etc.) and this motivates common descriptions of those.

Looking at the automation aspect, the technology supporting automotive transport has been rapidly evolving over the last few years. Connected vehicles and complementary backend and infrastructure communication systems are a reality, while increased automation is on the horizon. The term “connected and autonomous vehicles” (CAVs) is now widely used to refer to vehicles that include aspects of these new technologies. CAV technology is seen as potentially enabling increased safety, road capacity and reduced congestion, as well as the inclusion and accessibility for people unable to drive or access conventional modes of transport.

Making a step further, presence of collaborative CAVs (CCAVs) able to exchange information and coordinate with other CAVs, other road users and any cloud orchestrating system introduces the possibility of a more interactive automation landscape promising an increased level of safety and efficiency and more intuitive driving interactions among AVs and other road users in mixed traffic conditions. Still, the implementation of C-ITS framework in urban road networks and consequently also in public transport (as pursuit by the well-established CEN TC278 WG3) remains a challenge due to the specificities and complexity of the urban road traffic context, which is very different to the well-controlled motorway environment, and requires high accuracy in positioning, granularity in location referencing and continuous connectivity to enable cooperative services.

The main design target of this work is to create a modular inclusive architecture which can efficiently integrate with existing fleet management and PT backend systems and provide support for the CCAM services of the future as these are envisioned within SHOW. The core output of this deliverable is the SHOW reference architecture which models the attributes of and the interaction among the SHOW system actors in an integrated system (AV operators, PT operators, riders, other road users, public authorities, 3^{d} party services providers, and automakers). Based on data integration principle differentiations, three architecture variations that exhibit different manners of interoperability among the actors of the integrated system are derived, whilst cyber security mechanisms and communication protocols which apply vertically to all system layers are proposed.

Document Control Sheet

Start date of project:	01 January 2020
Duration:	48 months
SHOW Del. ID & Title:	D4.1: Open modular system architecture and tools - first version
Dissemination level:	PU
Relevant Activities:	A4.1, A4.2, A4.3, A4.4, A4.5, A4.6
Work package:	WP4: System architecture & tools
Lead authors:	Anastasia Bolovinou (ICCS)
Other authors involved:	Thanh Bui, Valentina Ivanova (RI.SE), Anne Melano (Bestmile), Pierre Chehwan, Sophie de Lambert de Boisjean (NAVYA), Sam Lysons, Mihai Chirca (Transdev), Evangelos Antypas, Alexandros Papadopoulos, Athanasios Sersemis, Iordanis Papoutsoglou, Nikolaos Sakellariou, Konstantinos Giapantzis, Georgios Spanos, Antonios Lalas, Konstantinos Votis (CERTH/ITI), Maria Gemou, Matina Loukea (CERTH/HIT), Sven Salomon (Easymile), Emmanuel de Verdalle (ITxPT), Henriette Cornet (UITP)
Internal Reviewers:	Stefan Abendroth (Mobility Systems Engineering) – Robert Bosch GmbH Joachim Rentel (Cross Domain Computers) – Robert Bosch GmbH Maria Gemou – CERTH/HIT
External Reviewers:	N/A
Actual submission date:	04/02/2021
Resubmission date:	08/06/2022
Status:	RESUBMITTED
File Name:	SHOW_D4.1_SHOW_D4.1_system_architecture_and_tools_revised_V2

Document Revision History

Version	Date	Reason	Editor
0.1	05/11/2020	Table of contents integrated after A4.1 participants approved it; Guidelines for each chapter added; Architecture diagrams (focusing on their content and not format) added	Anastasia Bolovinou (ICCS)
0.2	11/11/2020	Few more guidelines for each chapter added	Anastasia Bolovinou (ICCS)
0.2.1	20/11/2020	Inputs from Navya	P. Chehwan (Navya)
0.3	24/11/2020	Adding ICCS new diagrams and Bestmile's input plus adding ch.#7 – integration in chapter4 not complete, to be continued when ICCS resumes its work	A. Bolovinou (ICCS)

Version	Date	Reason	Editor
0.4	16.12.2020	New draft inputs from RI.SE, CERTH-ITI, ITxPT and Transdev. Updates from ICCS on chapter4 diagrams.	A. Bolovinou (ICCS), M. Chirca, S. Lysons (Transdev), A. Lalas (CERTH/ITI), T. Bui (RI.SE), E. Verdalle (ItxPT)
0.5	28.12.2020	ICCS integrates material from all partners. New table that tracks the status of local dashboards added.	A. Bolovinou (ICCS)
0.6	08.01.2021	ICCS add content in chapters 1,2,3,4 + Appendices (New table that summarizes cloud existing solutions based on Ucs added.).	A. Bolovinou (ICCS)
0.6.1	08.01.2021	Minor update chapter3	A. Bolovinou (ICCS)
0.6.2	12.01.2021	Updates by ICCS based on internal wp4 review	A. Bolovinou (ICCS)
1.0	18/01/2021	All contents integrated. Stable version sent for internal peer review.	A. Bolovinou (ICCS)
2.0	04/02/2021	Peer reviewed version sent for submission.	A. Bolovinou (ICCS)
2.1	29/11/2021	Revised version that addresses the EC review comment	A. Bolovinou (ICCS)
3.0	30/11/2021	Final revised version for resubmission by Technical Manager	Maria Gkemou (CERTH/HIT)
3.1	07/06/2022	Final revised version, as per the EC request on 27/05/2022, for resubmission by Coordinator	H. Cornet (UITP) J. Beckmann (UITP)

Table of Contents

List of Tables

List of Figures

Abbreviation List

Abbreviation	Definition
6LoWPAN	IPv6 over Low -Power Wireless Personal Area Networks
AD	Automated Driving
ADS	Automated Driving System
API	Application Programming Interface
AV	Autonomous Vehicles
AVxPT	AVs for PT (source UITP/ SPACE project)
AVL	Automatic Vehicle Location
B2B	Business to Business
BIOS	Basic Input/ Output System
CAV	Connected and (fully) automated vehicle
CCAV	Collaborative Connected Autonomous Vehicles
C-ITS	Co-operative Intelligent Transport Systems
D	Detectability
DDT	Dynamic Driving Task
DRT	Demand Responsive Transport
EC	European Commission
eFMEA	Extended Failure Mode and Effects Analysis
ETA	Estimated Time of Arrival
EU	European Union
FMEA	Failure Mode and Effects Analysis
GMPs	Good Manufacturing Practices
GNSS	Global Navigation Satellite System
HTTP	Hypertext Transfer Protocol
HW	Hardware
I2I	Infrastructure To Infrastructure (communications)
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
LIN	Local Interconnect Network
LFMP	Local Fleet Management Platform
M2M	Machine to Machine
MADT	Multi-Application Driver Terminal
MDP	Mobility Data Platform
MQTT	Message Queuing Telemetry Transport
NAP	National Access Point
NOU	National Organization Unit
O	Occurrence Probability
OBU	On Board Unit
OEM	Original Equipment Manufacturer
PSM	Process Safety Management
PT	Public Transport
PTA	Public Transport Authority
PTO	Public Transport Operators
R	Recoverability
REST	REpresentational State Transfer
RFID	Radio Frequency Identification
RN	Risk Number
RSU	Roadside unit
S	Severity
SDK	Software Development toolkit
SMDP	SHOW Mobility Data Platform
SP	Sub Project
SVI	Secure Vehicle Interface

Abbreviation	Definition
SW	Software
TD	Thing Description (na bgei k na antikatastathei sto keimeno)
TEN-T	Trans-European Transport Networks
TLS	Transport Layer Security
TMC	Traffic management centre
TSMO	Transportation Systems Management and Operations
URI	Uniform Resource Identifier
V2C	Vehicle to Cloud
V2D	Vehicle to Device
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Pedestrians
V2V	Vehicle to Vehicle
V2X	Vehicle-to-X (X represents any entity capable of receiving C-ITS communications)
VRU	Vulnerable Road User
W3C	World Wide Web Consortium
WG	Working Group
WoT	Web of Things
WP	Work Package

1 Introduction

1.1 Purpose and structure of the document

The main design target of this work is to create a modular inclusive system architecture that can efficiently integrate with existing CAV fleet management and Public Transport (PT) backend systems of the 17 cities included in the SHOW project, for improving existing transit operations. The architecture should support integration with existing local operational services and in parallel it should support the deployment of a set of advanced CCAV services for PT which will be implemented and demonstrated within SHOW. The system architecture is a significant project cornerstone as it will lead the subsequent SHOW implementation work, the SHOW system integration work as well as the subsequent SHOW system evaluation.

In this deliverable, the SHOW integrated system reference architecture representing the high level functional requirements of the system is presented while communication, interoperability and cyber-security mechanisms addressing non-functional horizontal requirements are derived. In chapter 4 the core SHOW A4.1 work performed to move from functional and operational requirements (sec. 4.3) into the logical and functional architecture views described in chapter 3 is presented. In addition, a dedicated chapter is devoted to the SHOW Dashboard service design (chapter 5). The notion of a centralized Dashboard service was included as an important project piloting activity monitoring tool and serves the role of SHOW platform data visualization deprived of any remote control operation functionality and hence it is considered complementary to any existing local Dashboard service (see 4.4.1). The next chapter is reserved for adding two architecture deployment views corresponding to two of the SHOW CCAM envisioned services as a means of projecting the reference architecture on a service-oriented implementation level which also allowed to define the required data to be exchanged (chapter 6).

As a basis for this work a review of relevant projects, initiatives and standards, presented in chapter 2, has been preceded. The methodology adopted is presented in chapter3. In chapter 7, the output of the system's technical risks analysis (SHOW activity A4.6 output) is included. Chapter 8 concludes this deliverable.

The architecture is composed by the functional components structured into three core layers: the physical layer including all the networked Things, the cloud data management layer and the web-services layer that sits on top of the previous layer. Based on data integration principle differentiation which affects the update rate and type of data that can be made available either from the Things' or the external local fleet management subsystem side, three architecture variations, that exhibit different manners of interoperability among the actors of the integrated system, are derived. In parallel, cyber security mechanisms and communication protocols which apply vertically to all system layers are proposed. The proposed three variations are the outcome of an intense discussion among the SHOW WP4 team on how to create a generic data sharing system architecture for CCAM services and represent different alternatives for local autonomous transportation systems integration which all respect a common set of design principles. In all three approaches, the main components, their interrelations and the required interfaces from the local existing systems to the SHOW Mobility Data Platform responsible for the data retrieval, the service supervision and management, and the centralized data visualization through the SHOW Mobility Data Platform Dashboard, are outlined.

1.2 Intended Audience

The intended audience of this work includes:

- SHOW SP2 designers and developers and especially the developers of the SHOW Data Management Portal (WP5), the SHOW reference Dashboard (A4.3) and the SHOW CCAV enhanced services (WP5 and WP6): interested in SHOW system conceptual architecture, system layers and system cloud layer components.
- SHOW SP2 OEMs responsible for the CCAV deployment (and in many cases owners of CCAV fleet data stored in their private clouds) in each demo site: interested in on-board APIs, SHOW proposed data formats, SHOW proposed data exchange protocols.
- SHOW SP3 demo sites' technical teams responsible either for the CAVs operation, the service design and evaluation or/and any local systems' integration with the SHOW system (representing the CAV fleet, the demo sites' infrastructure and any local backend cloud system involved). More specifically the following groups are addressed:
    - Evaluation team of WP9
    - Technical validation team of WP11: interested in CAV data loggers and SHOW cloud databases (for SHOW historic data retrieval)
    - Experimenters of WP12 (Real-life demonstrations)

- Stakeholders and research community outside SHOW dealing with CCAVs integration in future PT landscape: Interested in the review of C-ITS, CAVs and PT relevant standards, SHOW conceptual architecture and IP-based interfaces proposed, as well as in the design alternatives proposed, which support different types of interoperability and data access principles.

1.3 Interrelations

Deliverable's main internal interrelations to other WPs/Activities have been developed throughout the first year of the project and have been supported by the WP4 interviews with the demo sites and the SP2 development teams and are presented in Figure 1 and outlined hereafter:

- A4.2-A4.5 activities that progress in parallel and gave input to this architecture deliverable
- SP2 activities regarding setting up the fleet, defining the infrastructure, defining the operational and additional services to be offered and negotiating availability of data; WP7, in specific, regarding the CAVs setup, on-board architecture, experiments with other road users.
- WP1 (Use Cases), the functional requirements of which, the Architecture and the related mechanisms by default aims to fulfil
- WP9-WP11 (sites' demos setup, evaluation and impact assessment teams).

Deliverable's interrelations to external projects, initiatives, platforms are indicated in Table 1.

Table 1: D4.1 interrelations to other projects

External initiative	Item of interest for SHOW
ITxPT organization[1]	Technical specs for backend / on-board architecture and interfaces
SPACE project[2]	Reference architecture for CAVs in PT
W3C [3]	WoTs architecture specs
Data4PT[4]	Insights from workshops with PT stakeholders, Data models to be promoted
EU EIP Guidelines for National Access Point (NAP)[5]	NAP data platform architecture / promoted data models
AVENUE project[6]	Services' specs for CAVs in PT

[1] https://itxpt.org/
[2] https://space.uitp.org/
[3] https://www.w3.org/
[4] https://data4pt-project.eu/
[5] https://eip.its-platform.eu/activities/monitoring-and-harmonisation-national-access-points
[6] https://h2020-avenue.eu/

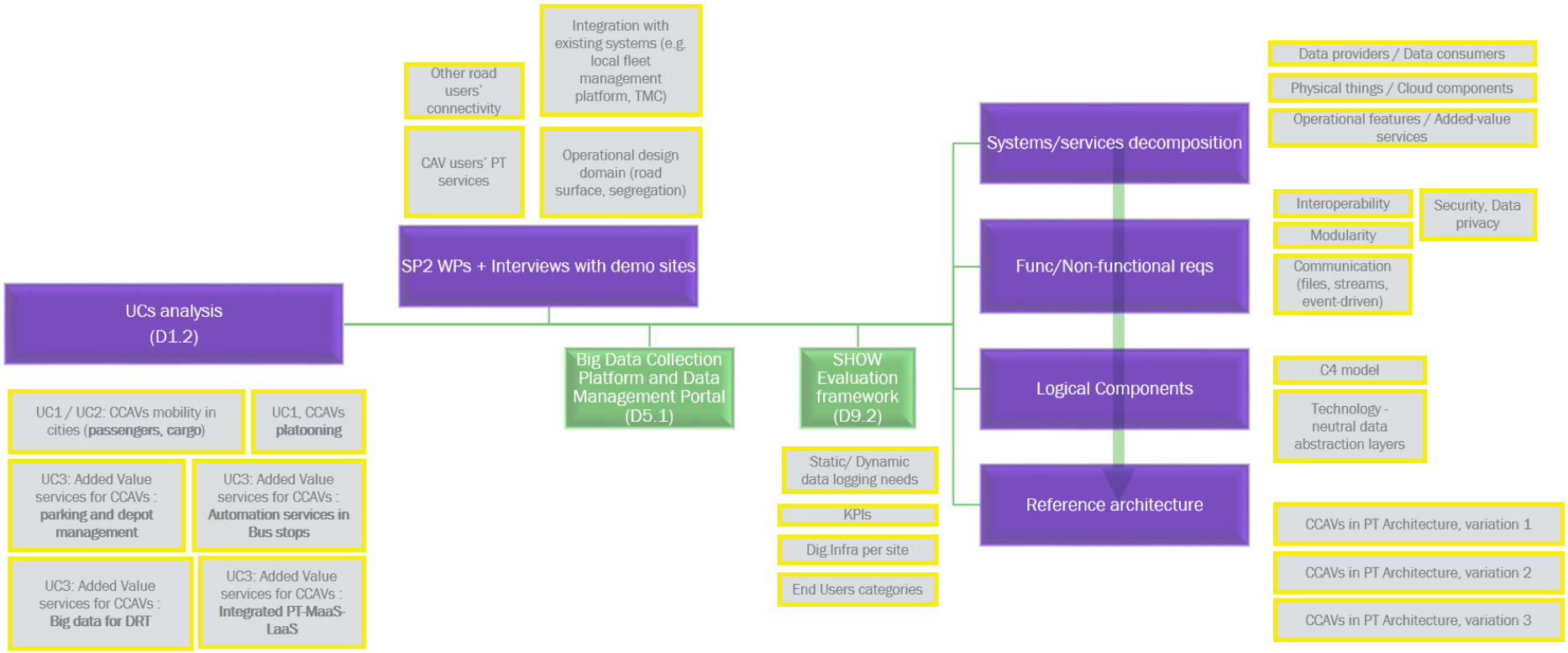

Figure 1 : D4.1 interrelations with other SHOW work items.

2 Relevant initiatives and standards

Public transport services rely increasingly on information systems to ensure reliable, efficient operation and widely accessible, accurate passenger information. These systems are used for a range of specific purposes: setting schedules and timetables, managing vehicle fleets, issuing tickets and receipts, providing real time information on service running, and so on.

In the following sections, we study the state-of-the-art and we structure its review in the following sub-sections:

- Architectures for CCAVs in PT
- CCAVs web-services and the WoTs paradigm
- C-ITS connectivity relevant aspects
- Data access for 3rd party service providers and NAPs
- Cyber-security relevant aspects

2.1 Architectures for CCAVs in PT

In this section, the main inspirations for designing the SHOW reference architecture are briefly presented.

2.1.1 SPACE reference architecture

The SPACE (Shared Personalised Automated Connected vEhicles) project[2] launched in 2018 with the aim of placing public transport at the centre of the automated vehicles (AVs) revolution. SPACE has developed a high-level reference architecture that aims at ensuring a comprehensive and seamless integration of driverless vehicles with other IT systems in the mobility ecosystem using a fleet orchestration platform (Figure 2). The SPACE architecture enables mixed fleet operation using both driven and automated vehicles using the same fleet orchestration software.

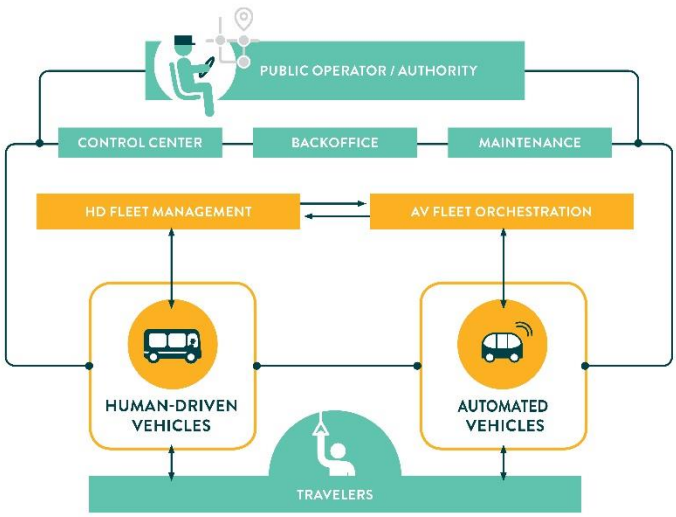

Figure 2: SPACE conceptual architecture (source: UITP).

To orchestrate efficiently the fleet (i.e. to send the right vehicle to the right place at the right time) the platform is interconnected with the existing public transport back-end

systems, the digital road infrastructure and the smart city data sources (e.g. Traffic Management Centres, smart parking, IoT platforms) as shown in Figure 3.

The platform also ensures a brand- and type-agnostic integration with the driverless vehicles and provides rich and open Application Program Interfaces (APIs) to develop professional and end users' applications. The high-level architecture identifies the main functions and components necessary to enable real-life operation of AVs in passenger service, while identifying the relationship between them.

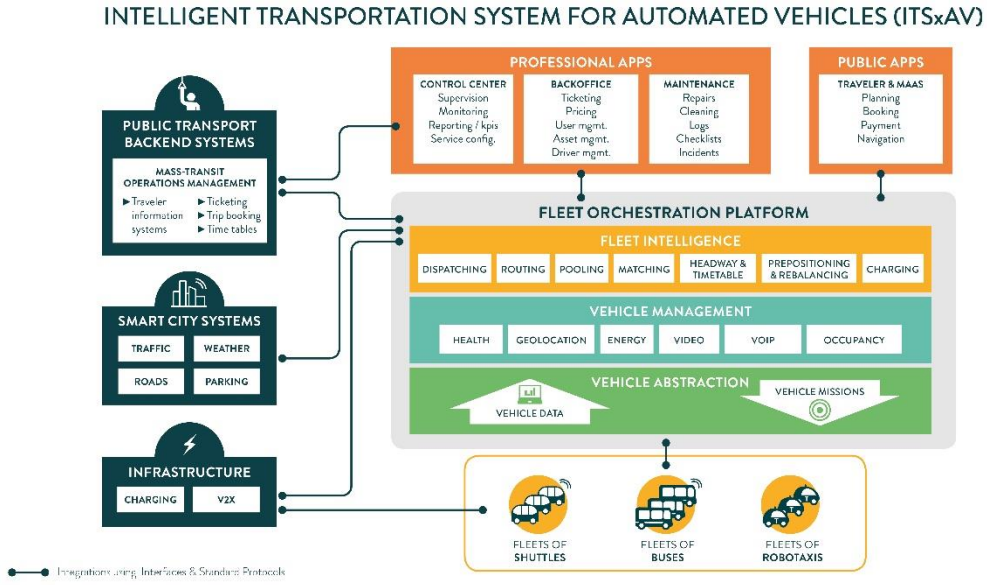

Figure 3: SPACE reference architecture (source: UITP).

The SHOW architecture uses the SPACE reference architecture as the basis of its system functional architecture for the parts that have to do with the CCAVs local orchestration by a cloud fleet management platform which is also connected to different external enablers. As it will be shown in ch.4, Figure 15, the SPACE architecture is integrated as the right part of the overall SHOW architecture representing the local existing systems with which the SHOW Mobility Data Platform subsystem has to interface with. As it will be explained in the relevant chapter (sec. 4.3), the SHOW system design approach led to a small differentiation with respect to the SPACE reference architecture, in the way integration of the SPACE enablers was applied: in the SHOW architectural approach, the physical layer includes not only CCAVs but also other road users and infrastructure nodes. Additionally, assigning components to either the physical layer or the cloud layer is desired, for that reason we need to include the "Infrastructure" (part of the SPACE enablers) in both layers; hence, infrastructure nodes are added as interacting with the CCAV fleet at the physical layer while "charging" data (part of SPACE Infrastructure enabler) is added as part of the SHOW smart city enabler (see Figure 13 – functional architecture abstraction).

2.1.2 Selection of standards for web services in PT

In transport organizations, the main stakeholders are:

- The National Organization Unit (NOU), dedicated to national area: the NOU gives directives to PTA and manages National and/or European regulations and decrees regarding PT.
- The Public Transport Authority (PTA), dedicated to regional geographical area (depending on the country: region, district, agglomeration…): the PTA is responsible for tenders and contracts with PTO.
- The Public Transport Operators (PTO) operating vehicles: the PTO is a PTA contract partner and can be present in several geographical areas as partner with different PTA.

Different configurations exist depending on the geographical organization and the roles of the stakeholders in PT. Geographical areas can be defined by nation, region, district, town or local council community. On a national scale, there are several PTA in the same organization. A PTA can operate vehicles either directly or through a subcontractor (PTO). Furthermore, a PTO can also use subcontractor operators.

Figure 4 illustrates the complexity of such organizations. It represents some combinations with different levels of complexity.

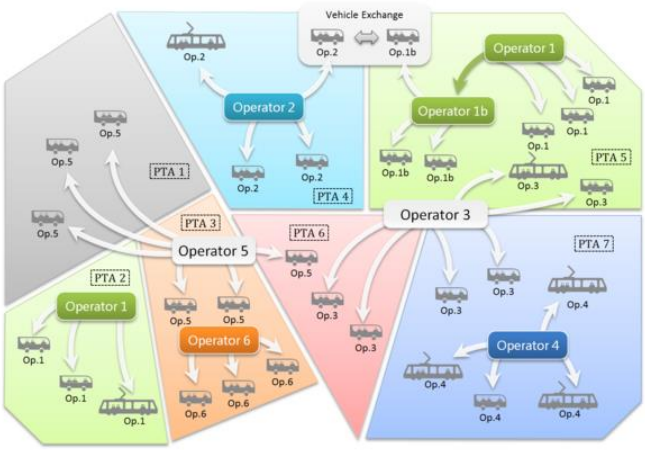

Figure 4: PTA/PTO interoperability (source: ITxPT)

In the following sub-sections, the work on relevant standards' review is outlined starting from the broader C-ITS domain and ending with the PT domain that is closer to the SHOW objectives.

2.1.2.1 Relevant C-ITS and CAVs standards

Whilst initially "silo-solutions" were predominantly developed and deployed for the different Intelligent Transport Systems (ITS) service domains (e.g. Electronic Fee Collection / Road Tolling, eCall, Public Transport, Traffic and Traveller Information), the last decade the concept of "Cooperative ITS" (C-ITS) that includes support for sharing of data, components and software (e.g. radio transceivers, localization equipment, software-based facilities) amongst service domains has gained consensus in EU leading to the development and release of numerous C-ITS standards by ISO,

CEN and ETSI working groups which promote hybrid communications, neutrality of technology where applicable, portability of ITS applications, security and privacy.

Returning to a CAV-centric perspective and under the auspices of the W3C automotive working group[7], Vehicle Data Interfaces Architecture is developed. This work is extended by the GENIVI cooperation[8] for the promotion of new secure vehicle-cloud interfaces. They proposed the Secure Vehicle Interface (SVI) as a ready-to-deploy technology, based on three CEN/ISO standards namely the TS 21177, TS 21185 and TS 21184. SVI enables safe, cyber-secure communication between the vehicle and service partners who have been chosen to obtain the data by the vehicle Owner/Users. SVI uses a standardised secure interface to connect recognised and authorised external systems to the network within a vehicle. SVI then converts the vehicle manufacturer's proprietary vehicle data into a common language, which enables broad interoperability for competitive services irrespective of the manufacturer or brand of the vehicle. On the more traditional side of the spectrum, the OEMs' view which is promoted by CLEPA position papers is represented by the work of ISO 20078 on Extended Vehicle (ExVe) specification[9].

Finally, many new technical reports are being currently generated targeting the new field of CAVs development and testing. Under The CAV umbrella the following sources of draft standards or technical documents have been proved useful for this deliverable:

- SAE MOBILUS Automated & Connected Content (incl. CCAVs)[10].

- BSI PAS standards for AVs (ODD, safety, security)[11].

2.1.2.2 Relevant urban C-ITS standards

The fast development of cooperative ITS technologies and the first ongoing inter-urban large-scale deployment of C-ITS have now raised attention to the urban environment. Since cooperative systems require a new way of communication and implementation processes, standards are crucial to ensure on the one hand interoperability and on the other hand to enable migration paths for the existing ITS infrastructure.

The European Commission takes a prominent role by establishing a cooperative framework of relevant C-ITS stakeholders including national road authorities (the C-ITS Platform) in order to create a common European C-ITS roadmap, also addressing standardization needs. From a standardization perspective, the previous and new European Mandates M/453 and M/546–issued on 6/10/2009 and 12/02/2016 respectively – together is a mechanism for requesting further standardization projects in support of ITS directive 2010/40/EU and the objective of single transport market at the strategic level [1]. The relevant standardization initiatives and activities have been reviewed in [3].

2.1.2.3 Relevant PT data exchange standards and data models

A review of available standards used in PT has been performed as part of this work and a list of all relevant standards along with our comments on their applicability is included in Table 46 of Appendix II. In this deliverable, protocols have been proposed

---

[7] https://www.w3.org/blog/auto/2017/01/04/vehicle-data-interfaces/
[8] https://www.genivi.org/about-genivi
[9]https://clepa.eu/mediaroom/clepa-position-paper-on-access-to-in-vehicle-data-and-resources/
[10] https://saemobilus.sae.org/automated-connected/publications/explore/
[11] https://www.bsigroup.com/en-GB/CAV/

for data exchange among Things and the cloud subsystems (see sec. 4.6.1.1) while the specification of the minimum set of data to be exchanged (data models) is still work in progress. However, a preliminary version of data description including a classification of the data into categories is provided in sec. 4.4.5 and it is aligned with the information on data provided in deliverable in D5.1 (*Big Data Collection Platform and Data Management Portal*) [19].

Moving towards a Single European Transport Area requires a digital layer interlinking all of the elements of transport. Building up this Digital Architecture involves open and common standards and interfaces and an efficient, but secure data ecosystem. This is why Member States are setting up their National Access Points[12]; to facilitate access, easy exchange and reuse of transport related data, in order to help support the provision of EU-wide interoperable travel and traffic services to end users. NAP is an European intermediary platform and it is part of EU ITS Directive 2010/40/EU specification. All delegated regulations supplementing the ITS Directive refer to certain standards to be used when exchanging information with NAPs. While DATEX II is prevalent, the NeTEx CEN/TS 16614 and SIRI CEN/TS 15531 standards are also stated. The EU common data model for services in PT: "Transmodel" is the short name for the European Standard "Public Transport Reference Data Model" (EN 12896). It contributes to improving a number of features of public transport information and service management: in particular, the standard facilitates interoperability between information processing systems of the transport operators and agencies. Transmodel has an important strategic role for European Public Transport data. Under the ITS Directive (Priority Action A), by 2019 all EC member states must make their data available under Transmodel based standard formats such as NeTEx and SIRI.

Additionally, the following are also relevant in the context of NAP data exchange:

- TAP–TSI technical specification for interoperability (TSI) for telematics applications for passenger services
- (TAP) Public transport Open API for distributed journey planning –CEN/TC 278
- GTFS-Google Transit Feed Specification and GTFS-RT (real time feed).

In the project's FRAME documentation, a brief description of these standards and the conclusions, mainly about DATEX II implementation, from the 2019 survey on the status of national NAP developments is provided.

2.1.2.4 The ITxPT technical specifications for services in PT

The implementation of C-ITS framework in urban road networks and in public transport is pursuit by the well-established CEN TC278 WG3 and it remains a challenging task due to the specificities of the urban context as argued in [3]. Traffic in an urban environment faces a complex road network topology and furthermore involves a variety of modes of transport. Traffic is volatile, with vehicles entering and leaving the network at every possible point. Network geography and topology are also volatile with many short-term, temporary modifications (road work, street work, special permissions) and being maintained by multiple organizations / authorities. This is very different to the well-controlled motorway environment and consequently requires high accuracy in positioning and granularity in location referencing to enable cooperative services.

The non-profit association ITxPT (Figure 5) enables an open architecture, data accessibility and interoperability between IT systems in PT. The members of ITxPT develop the IT architecture for public transport and other mobility services together, based on standards and best practices. ITxPT specifications are adopted worldwide

[12] [EC-ITS / NAPs] https://ec.europa.eu/transport/themes/its/road/action_plan/nap_en

and are included in main PT tenders among others in UK, France, Italy, Sweden, the Netherlands, Norway and Dubai. As ITxPT is a member of SHOW WP4 as subcontractor of UITP, close cooperation with ITXPT for reviewing D4.1 interoperability aspects has been built.

Figure 5: ITxPT laboratory (source: ITxPT).

ITxPT specification is based on standards from CEN / TC278 WG3. CEN / TC278 standardization body manages the preparation of standards in the field of Intelligent Transport Systems (ITS) in Europe. It serves as a platform for European stakeholder to exchange knowledge, information, best practices and experiences in ITS. WG3 defines ITS standard for Public Transport.

ITxPT specification covers the following scopes:

- S01: Installation Requirements

This is mainly related to “physical interface” onboard the vehicle (i.e., enclosure, wiring, connector, antenna, etc.). This is the first step to secure interoperability. It defines rules to prepare vehicles and onboard IT systems according to standard interfaces to avoid useless redundancies (e.g., multiple antennas, silo systems, proprietary interfaces).

- S02: Onboard Architecture

The Onboard Architecture deals with “software interface” onboard the vehicle around a Service Oriented Architecture. It covers communication protocol, data models and data format. It is key to secure interoperability offering standard interface to exchange data (e.g., single GNSS information can be published and shared on IP onboard network or MADT – Multi Application Driver terminal - to share single interface for all onboard application). S02 covers already a set of functional scope including vehicle monitoring (i.e., progress of vehicle on a journey according to timetable), passenger counting, time synchronization, GNSS data, etc.)

- S02 is based on standard TS13149 (from CEN TC278 WG3)
- S03: Backoffice Architecture

It covers backoffice interfaces (ie. outside the vehicle) based on existing standards:

- reference data model providing common public transport concepts and data structures: **TRANSMODEL** (from CEN TC278 WG3)
- network description including timetables, stops, fares: **NeTEx** (from CEN TC278 WG3)
- real-time information for exchanging information about real-time public transport operations: **SIRI** (from CEN TC278 WG3)

- vehicle data to share information from telematics with any third party: **TiGR** (from ITxPT)

2.2 CCAVs web services and the WoTs

The Web of Things (WoT) is an evolution of the contemporary Internet of Things as silos and fragmentation are some of the documented as described by Datta et al [6]**.** The WoT is proposed by the World Wide Web Consortium (W3C) as an extension of the Web. The architecture is composed of three main components which are the connected device called Thing, the Gateway and the Cloud level.

The basis of the architecture starts with the Things that could be physical or virtual. Things are exposed as software objects with APIs by communicating events, properties and actions enclosed in Thing Description [7]. There are three main building blocks of WoT [8] which are: Thing Description, Binding Templates and Scripting API with security mechanisms applied to all of them.

Blackstock et al [9] are presenting the contemporary WoT approach that is for Things, sensors and actuators, can be represented as resources and can be exposed using REST architecture. They documented that while it is intuitive that a single Things or small groups of Things could be given web presence via a lightweight web server in an embedded device, the growing trend is to aggregate the web presence of numerous Things with the deployment of WoT hubs and Sensor Webs.

A number of different technologies are enabling and driving the adoption of the WoT [10]. Web services, that are the cornerstone for establishing interoperable distributed systems, are allowing Things to be exposed. Two major classes are implemented to regulate the Web services, the REST-compliant Web services and the arbitrary Web service protocols stacks. Furthermore, embedded web servers would facilitate the communication of Things and the HTTP protocol enabling the long term adaptation of the WoT. Finally, stacks would facilitate the scalability and accessibility of the infrastructure. For instance, the 6LoWPAN protocol defines packets to be sent and received between devices.

The Automotive sector is adopting the WoT Architecture to produce interoperable implementations [11], [12]. The vehicle could act in the edge layer above the infrastructure and would be connected to the cloud [70]. This architecture calls for the installation of an On Board Unit (OBU) in the vehicle to run an agent to supply the measurements. The web services communication of the metadata and configuration information are encoded in JSON format. The OBU has the ITS-G5 stack implemented to enable software elements, written in C, to be deployed into Road Side Units (RSUs) (Figure 6).

The architecture for AVs is apparent in the development of a precision positioning service platform [12]. The platform consists of three layers: secure web services deployed in a Cloud infrastructure, highly autonomous cars with cloudlets at the edge layer and V2X communication with various infrastructure. The platform would make use of positional algorithms developed in project HIGHTS. A summary of the best practices would include: following the W3C Web of Things recommendations; using SenML and JSON based implementation for the real time aspect preservation; deploying MQTT for publishing type messages; developing the web services by using microservices; Things description to include events, properties and actions to support granular descriptions; using CoRE Resource Directory for Things repository; using a JSON based authentication for the connected cars and consumers in the Cloud system (Figure 7).

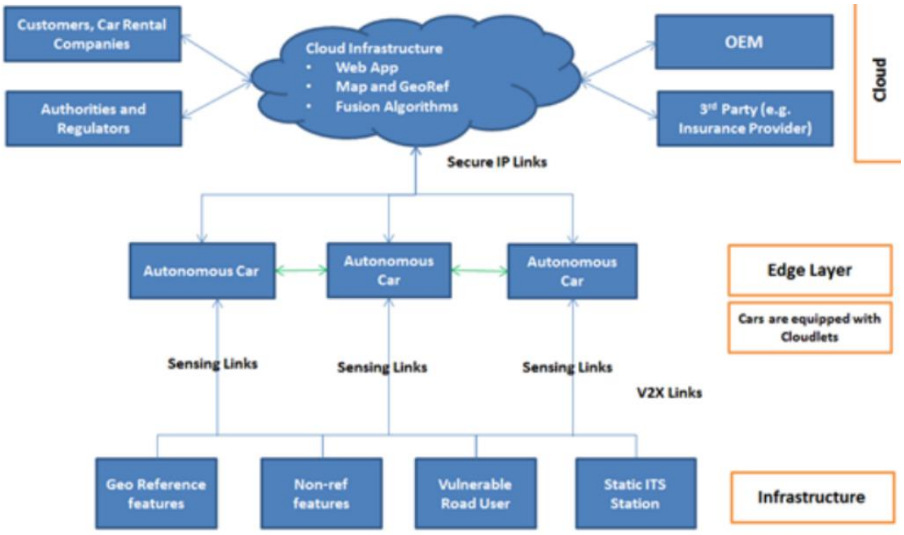

Figure 6: Platform Architecture for AVs [12].

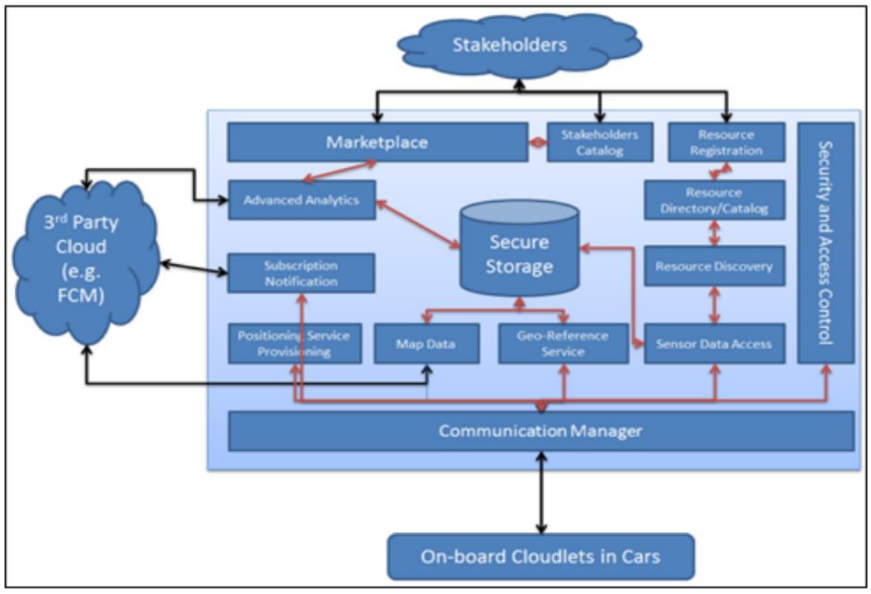

Figure 7: Services for AVs [12].

2.3 C-ITS Connectivity

2.3.1 General aspects

C-ITS typically involves communication between vehicles (V2V), between vehicles and infrastructure (V2I) and/or infrastructure-to-infrastructure (I2I). The benefits span a range of areas, including improving road safety, reducing congestion, optimizing transport efficiency, enhancing mobility, increasing service reliability, reducing energy use and environmental impacts, and supporting economic development. Over the past decade, there have been remarkable new developments in technologies that facilitate C-ITS. In recognition of the high potential of C-ITS, the Commission has set up a dedicated C-ITS Platform, bringing together representatives from a wide range of stakeholders.

From a vehicle-centric view, at the top of vehicular communication systems is the vehicle to everything (V2X) communication. The concept of a “connected car” is not new to the automotive industry, however, the technology to make it possible (as well as the necessary communication standards) were not available until a few years ago. V2X is the parent category of a broader set of communication technologies needed to achieve the goal of connecting vehicles with the world surrounding them.

V2X communications encompasses 7 types of vehicle connectivity listed below and as will be shown in Figure 12, all 7 types will be considered within SHOW:

- Vehicle to network (V2N)
- Vehicle to infrastructure (V2I)
- Vehicle to vehicle (V2V)
- Vehicle to cloud (V2C)
- Vehicle to pedestrian (V2P)
- Vehicle to device (V2D)
- Vehicle to grid (V2G)

As with any new field of technology, there are competing standards in play for V2X. ***IEEE 802.11p:*** The original V2X standard is based on a Wi-Fi offshoot, IEEE 802.11p (part of the IEEE's WAVE, or Wireless Access for Vehicular Environments program), running in the unlicensed 5.9GHz frequency band. IEEE 802.11p, which was finalised in 2012, underpins Dedicated Short-Range Communications (DSRC) in the US, and ITS-G5 in the European Cooperative Intelligent Transport Systems (C-ITS) initiative. V2X communication via 802.11p goes beyond line-of-sight-limited sensors such as cameras, radar and LIDAR, and covers V2V and V2I use cases such as collision warnings, speed limit alerts, and electronic parking and toll payments. Functional characteristics of 802.11p include short range (under 1km), low latency (~2ms) and high reliability -- according to the US Department of Transportation, it *"works in high vehicle speed mobility conditions and delivers performance immune to extreme weather conditions (e.g. rain, fog, snow etc* Essentially, 802.11p extends a vehicle's ability to 'see' the environment around it, even in adverse weather conditions. IEEE 802.11p is not dependent on the presence of cellular network coverage, and solutions for on-board units (OBUs) and road-side units (RSUs) are available now from various vendors.

Cellular V2X (C-V2X): A key advantage of C-V2X is that it has two operational modes depending on the use case: The first is low-latency C-V2X Direct Communications over the PC5 interface on the unlicensed 5.9GHz band, and is designed for active safety messages such as immediate road hazard warnings and other short-range V2V, V2I,

and V2P situations. This mode aligns closely with what's offered by the incumbent IEEE 802.11p technology, which also uses the 5.9GHz band.

The second mode is communications over the UMTS air **interface** or "**Uu interface**", which links User Equipment to the UMTS Terrestrial Radio Access Network, on the regular licensed-band cellular network, and can handle V2N use cases like infotainment and latency-tolerant safety messages concerning longer-range road hazards or traffic conditions. Because it doesn't use cellular connectivity, IEEE 802.11p can only match this mode by making ad hoc connections to roadside base stations.

Focus in SHOW: IEEE 802.11p has the advantage of earlier development and deployment, and therefore incumbency. On the other hand, C-V2X offers arguably better performance, the ability to employ both direct and network-assisted communication, and an evolutionary path to 5G. Depending on the availability and maturity of technology in SHOW sites, hybrid connectivity schemes will be deployed. This will allow for ensuring continuity and availability of service and more importantly AVs localization will be deployed, i.e. ITS-G5 together with LTE 4G or 5G.

2.3.2 Collaborative feature

As defined in SAE J3216 standard [5], cooperative driving automation technologies enable mobility applications that are not achievable by individual automated driving system (ADS)-operated vehicles operating independently. These technologies do so by sharing information that can be used to increase safety, efficiency, and reliability of the transportation system, and that may serve to accelerate the deployment of driving automation in on-road motor vehicles. Driving automation and connectivity present opportunities to deploy multiple cooperative automation strategies, but successful deployment of multiple cooperative automation strategies depends on coordination among diverse stakeholders. These include road operators, intelligent transportation system (ITS) technology providers, ADS and ADS-equipped vehicle manufacturers and suppliers, as well as ADS-dedicated vehicle (ADS-DV) fleet operators. These public and private sector stakeholders are preparing for and deploying different use cases at different temporal and spatial scales. These use cases may implement vehicle strategies, such as speed harmonization and/or transportation systems management and operations (TSMO) strategies, e.g., basic travel, traffic incident management, weather management, and work zone management data sharing. The United States Department of Transportation (U.S. DOT) highlighted the importance of cooperative situational awareness standards in its guideline document “Automated Vehicles 3.0: Preparing for the Future of Transportation.” To develop these strategies, stakeholders are engaging each other and would benefit from a common language and organization of complex technology concepts. Standardizing terms and definitions for cooperative automation and its components has already started as shown in [5].

Focus in SHOW: A dedicated activity A7.5: “Interaction between cooperative and non-cooperative traffic participants” is anticipated with the goal to develop VRU-targeted applications that extend the awareness of and about non-connected VRUs (pedestrians, bicycles, motorcycles, traffic participants with disabilities) in the neighbourhood of other traffic participants.

2.3.3 5G aspects

The prospect of 5G utilization in SHOW pilot sites activities could provide extremely upgraded capabilities for the envisioned systems in the communication and operational sections. Taking into account that data exchange is a critical challenge, an optimized utilization of 5G networks could efficiently facilitate this process. The Fifth-Generation Network employs wireless broadband connections and 360^{o} antennas, an aspect that

ensures fast connections and security [15].Therefore, it could prove to be more than useful for the Internet of Vehicles, which is defined as the integration of human, vehicle and thing and the exchange of data and application amongst them, but also support the V2X communications. The benefits of 5G are, briefly, presented in Table 2.

Table 2: Comparison between 4G and 5G

Basic Parameters	4G	5G
Latency	10-50ms	1ms
Density	100k connections per km^2	1 million connections per km^2
Throughput	2Gbps	20Gbps
Spectral efficiency	30bps/Hz	100bps/Hz
Traffic Capacity	10Mbps/m^2	1000Mbps/m^2
Network Energy Efficiency	Baseline	15% less

A characteristic example from the automotive perspective which depicts the superiority of 5G network in comparison with a 4G/LTE one is the following [16]: In a 4G network, it would take about 1.5m for a vehicle, after a detection of an obstacle, to apply its brakes. In 5G, vehicle would require less than 2.5cm. Moreover, 4G's performance deteriorates in areas with law coverage or very populated. These problems, theoretically, have been overpassed with a 5G network implementation.

2.3.4 5G in Smart Transportation Systems

The International Telecommunication Union divides 5G applications into three types: enhanced mobile broadband, massive machine type communications, and ultra-reliable low-latency communications. These three application scenarios outline a blueprint for the future ITS, that will greatly enhance the real-time reliability of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [17].

The combination of 5G and Artificial Intelligence could provide extra safety, higher productivity and efficiency in ITS [18]. The connection between the vehicles and the vehicles with RSUs guarantees the collision avoidance and consist a primary tool for the development of the majority of SHOW services, as they are described in D5.1 [19]. Moreover, 5G and AI could solve the vital problem of a mixture of autonomous and manual vehicles. In [17], a deep-learning traffic safety solution is presented.

The use cases in the automotive domain that are relevant for 5G include: **autonomous driving vehicles, vehicle platooning** and **traffic safety and control** [18]. Furthermore, the improvement of V2X communications which is a result of 5G use enables the AV ecosystem with the ability to avoid accidents and unpleasant situations which are caused by human errors. Autonomous vehicles need to process at least 1 Gbps of data rate to make smart decisions. Current technologies can tackle with this challenge taking as a fact that the fleet will remain small in pilot sites. However, current technologies cannot support the simultaneous transmission and reception at such a high data rate among hundreds or thousands of vehicles within a small area [18].

2.3.4.1 Main technologies

Millimeter Waves (mmWaves): A method in order to overcome the limitation in the provided bandwidth is the use of Millimeter Waves (mmWaves). Millimeter waves are broadcasted at frequencies between 30 and 300 GHz, beyond from frequencies that are used for other services such as mobile phones. Millimeter Waves could provide higher data capacity. But there is a major disadvantage of mmWaves. This is that mmWaves cannot easily travel through buildings or obstacles and can be absorbed by rain and foliage. This is why 5G networks are likely to increase traditional cellular

towers with another new technology, called small cells [1]. There are mainly two alternatives for V2X communications: dedicated short-range communications (DSRC), and Long-Term Evolution (LTE)-V2X. Unfortunately, both alternatives fall to provide the multi-gigabit-per-second capability required to exchange real-time sensor data. mmWaves are proposed as solution since there is a huge amount of available channel bandwidth at this frequency band. Millimeter Waves are a prime choice for short range, high speed connection. Therefore, mmWaves is a powerful tool in Device-to-Device (D2D) communication [20]. Due to limited transmission rate, an alternative for AVs has been searched. The multi-hop V2V communication is usually preferred as it can enhance the signal propagation with minimum or without aid of mobile communication infrastructure [21]. Lastly, a situation that must be analyzed with any detail is the Non-Line-of-Sight (NLOS). Channel propagation model combined with the implementation of powerful real-time safety application, such as “Bird’s Eye View” and “See Through”, could be the solution in this problem [22]. In [23], a whole analysis about propagation parameters, beamforming and blockage in mmWave V2X communication is presented. The main challenges in the implementation of mmWaves in V2X communications, according to [24], are the complexity of the transceiver and the lack of channel measurement campaign at mmWave in vehicular scenarios.

Small cells: Small cells are portable tiny base stations that require minimal operating power and can be installed every 250 meters or so throughout cities. To prevent signal drop, thousands of these stations can be installed in a city to form a dense network that acts as a relay team, receiving signals from other base stations and sending data to users at any location. While traditional cellular networks have also come to rely on an increasing number of base stations, achieving 5G performance will require even greater infrastructure. Fortunately, antennas in small cells can be much smaller than traditional antennas if they transmit mmWaves. This size difference makes it even easier to attach cells to bridges and traffic lights. Radio Access Network technology which can be used for the Autonomous Vehicles can be micro cell or small cell. Micro cell could be used with light poles on the side of the road. Small cells are currently being developed using sensor technology and light emitting diodes [25].

Massive MIMO: MIMO technology is known from the current 4G base stations. It means Multiple Input Multiple Output and, is referred in the simultaneously use of multiple antennas for transmitting and receiving data signals. A 4G base station can consist of 8 antennas. The corresponding 5G could consist of, at least, 100 antennas. The capacity of the system is 22 and more times greater and the needs of ITS could be meet. There are many types of configuration for massive MIMO systems. The most widespread are the spherical, the cylindrical and the square. However, installing such a large number of antennas to manage cellular traffic also causes more interference if these signals intersect. This is why 5G stations need to integrate beamforming techniques. Massive MIMO combined with full-duplex technique could guarantee a great enhanced capacity of the system and reliable communication connection [26]. An interesting implementation is presented in [27], where an architecture of 100-antennas at 20GHz achieves high throughput, low latency and flexible extension up to128 antennas. Massive MIMO at mmWave frequencies is also possible exploiting the large available bandwidth. A fundamental obstacle in massive MIMO systems is the complexity of signal processing. The solution is searched in the co-design of powerful algorithms, configurable of the hardware architecture and circuits [28]. In [29], five promising antennas arrays, Extremely large aperture arrays, Holographic Massive MIMO, Six-dimensional positioning, Large-scale MIMO radar, and Intelligent Massive MIMO, is discussed.

Beamforming: Beamforming is a traffic-signaling system for cellular base stations that identifies the most efficient data transmission path to a specific user and reduces interference for users in the surrounding area. Beamforming can help massive MIMO

arrays make more efficient use of the spectrum around them. The primary challenge for massive MIMO is to reduce interference while transmitting more information from many more antennas. On massive MIMO base stations, signal processing algorithms design the best over-the-air transmission path to each user. Then, they can send individual data packets in many different directions, avoiding buildings and other objects with a precisely coordinated pattern. In this way beamforming allows multiple users and antennas in a massive MIMO array to exchange much more information at the same time. Beamforming becomes more challenging in Autonomous Vehicles due to their speed. In [30], the basic indicators are defined. These are information loss due to collisions, number of possible re-transmissions after collision, net neighbors and probability of losing information. A very useful kind of beamforming is the hybrid one. This concept lies in hybrid transceivers which use a combination of analog beamformers in the RF domain, together with digital beamforming in the baseband, connected to the RF with a smaller number of up/down conversion chains. In [31], a survey about hybrid beamforming in massive MIMO systems is presented. Hybrid beamforming based on instantaneous CSI, Hybrid beamforming based on averaged CSI, Hybrid beamforming with selection and Hybrid beamforming at mmWave are the main techniques.

NOMA: Non-Orthogonal Multiple Access (NOMA) has been proposed for use in 5G networks, due to the fact that it provides service to multiple users in the same source block, such as a time slot, bandwidth or encoding, separating them energetically. So, it improves the transmission rate for users with weak channels and we have one more efficient utilization of the spectrum, which is not the case with conventional methods Orthogonal Multiple Access, such as TDMA, OFDMA. NOMA can be combined with mmWave and MIMO technology. NOMA enriches our tools with an extra powerful one in order to achieve the massive connectivity and avoid the collisions in a dense traffic environment. Moreover, NOMA reduces the latency in V2X communication. In [32], a NOMA-based mixed centralized/ distributed scheme for cellular V2X broadcasting is proposed. With NOMA, the signals for long range broadcast with major power and signals for short range neighbors with small power can be superposed in one transmission. Therefore, distributed V2V communication could support broadcast and multicast communications simultaneously [33]. A network architecture for Autonomous Vehicles based on NOMA is presented in [34]. The research investigates different and realistic traffic scenarios, mainly highways and intersection, and the simulation results are encouraging.

2.3.4.2 5G Slicing technique in V2X

A way in order to improve the performance of the network is the slicing method. The key downside of today's networks is that the same architecture serves multiple services, usually built without elasticity in mind, and is processed by the same network components in the Core Network and by sharing the same resources in the Radio Access Network [36]. Slicing the Core Network segment affects control plane functionalities, such as mobility management, session management, and authentication. Slicing the Radio Access Network is a less mature and challenging practice (mainly due to the shared nature of wireless resources) and encompasses various radio access technology parameter configurations, such as time/frequency resources [36]. A set of network functionalities that are selected from the shared network infrastructure are assigned to each slice. These functions can be virtualized using technologies like Software Defined Networking and Network Functions Virtualization [35]. 5G Slicing can take place in Core Network or Radio Access Network for each mode of V2X communication**.**

2.4 IP-based Connectivity to Cloud relevant aspects

Many protocols may be at play when data is sent across the web, but the main protocols for delivering the Web of Things and promoted also within this SHOW reference architecture are HTTP, Websockets, and MQTT. Main characteristics of these three protocols are provided hereafter:

HTTP: The Hypertext Transfer Protocol (HTTP)13 is an application layer protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser. Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989. Development of early HTTP Requests for Comments (RFCs) was a coordinated effort by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), with work later moving to the IETF.

- HTTP/1.1 was first documented in RFC 2068 in 1997. That specification was obsoleted by RFC 2616 in 1999, which was likewise replaced by the RFC 7230 family of RFCs in 2014.
- HTTP/2 is a more efficient expression of HTTP's semantics "on the wire", and was published in 2015, and is used by 50.0% of websites; it is now supported by virtually all web browsers and major web servers over Transport Layer Security (TLS) using an Application-Layer Protocol Negotiation (ALPN) extension[3] where TLS 1.2 or newer is required.
- HTTP/3 is the proposed successor to HTTP/2,[6][7] which is already in used by over 4% of websites; and is used by over 5% of desktop computers (enabled by default in latest macOS), using UDP instead of TCP for the underlying transport protocol. Like HTTP/2, it does not obsolete previous major versions of the protocol. Support for HTTP/3 was added to Cloudflare and Google Chrome in September 2019,[8][9] and can be enabled in the stable versions of Chrome and Firefox.[10]

Websockets: WebSocket is a network protocol that provides bi-directional communication between a browser and a web server. The protocol was standardized in 2011 and all modern browsers provide built-in support for it. Similar to MQTT, the WebSocket protocol is based on TCP.

- Websockets are protocols that act as a handshake between web browsers (or similar software) and web servers, which lowers overhead involved in two-way communications using HTTP. Unlike the request-response messaging used with HTTP/1, the bi-directional transactions used in websockets are ideal for monitoring systems and those that require quick and/or constant updates. Websockets are supported in any web browser.
- Since HTTP/2 now includes bi-directional or full-duplex messaging, the need for websockets will likely diminish as HTTP/2 becomes standard, at least for IoT.

MQTT: MQTT[14] as the name suggests, is a publisher subscriber protocol, in which clients connect to a broker and the remote devices publish messages to a shared queue. The protocol optimizes towards message size, for efficiency. It was invented by IBM to facilitate machine-to-machine communication. It works on the publish and

[13] HTTP on Wikipedia: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
[14] MQTT on Wikipedia: https://en.wikipedia.org/wiki/MQTT

subscribe model to ensure efficient communication across platforms, and also has a level system for message priority. Currently, this protocol is widely used for IoT and large-scale communication because of its small footprint and minimal bandwidth consumption.

The conclusion drawn from a google cloud experiment[15] is that when choosing MQTT over HTTP, it's really important to reuse the same connection as much as possible. If connections are set up and torn down frequently just to send individual messages, the efficiency gains are not significant compared to HTTP.

2.5 Data generation and access for 3rd party services

Data generated during CCAV deployment include:

- data broadcast from a CAV over open one-to-any channels
- data provided by a CAV over private wireless methods
- data that can be accessed only by physical connection into the vehicle.
- data that are created and stored in the cloud for the technical evaluation of CCAVs and the provision of CCAV services

During the increased testing and development phase of CCAV functionality taking place in the industry and the research community the last few years, the needs for next generation vehicle platforms and data sharing have started to be shaped based on the following two objectives:

i) To efficiently test newly-introduced L4 and L5 Automated Driving (AD) functions in real world conditions by creating parallel virtual testing sessions on simulation hosted on the cloud (digital twins). Additionally, even most importantly, in contrast to using proprietary platforms for data ingestion, an open-source platform that offers free APIs and real-field vehicle data to the researchers and developers in the community, would allow to a broader and faster deployment and evaluation of AD applications on the real environment.

ii) To fully harvest the potential in safety and comfort of the future connected and autonomous vehicles (CAVs) treated as a part of a network of sophisticated computer on wheels, with substantial on-board sensors as data sources and a variety of services running on top to support autonomous driving or other functions. That is however quite challenging due to the time-critical requirements present in vehicular networks where any machine learning-enabled deployed apps/services useful for situation awareness and prediction should respect real time data processing and streaming requirements so that each (cloud-based or edge based) service could be finished within an acceptable latency and limited bandwidth consumption [4].

The above considerations apply also in the PT domain where the PT services deployment on EU-wide level can strongly proliferate from national traffic and PT data sharing, avoiding vendor lock-in solutions with data management centres that can be remotely connected to their associated fleets and cooperating also in cross-border travelling scenarios. This is also linked with National Access Point (NAP) EU initiative as the forthcoming C-ITS Delegated Regulation, already considers efficient strategies

[15] Google cloud blog: https://cloud.google.com/blog/products/iot-devices/http-vs-mqtt-a-tale-of-two-iot-protocols

for EU-wide traffic and public transport data sharing especially for safety-critical applications. Based on the latest C-ITS directive the members states have now to deliver mobility data using CEN standards (including NeTEx, cf. EU regulation 2017/1926). NAP architecture and its local instantiations are supported by DATA4PT[4] and FRAME[16] projects.

SHOW focus: Data sharing considerations for time critical web-based applications are tackled by the SHOW reference architecture in its third variation (sec.4.4.4). Justification behind the conception of this third variation took also into account the FAIR data[17] principles promoted by the EU.

2.6 Cyber-security special aspects

Based on the ISACA glossary[18] an attack vector is a path or route used by the adversary to gain access to the target (asset). Focusing on the software, the attack surface of a software environment is the sum of the different points (the 'attack vectors') where an unauthorized user (the 'attacker') can try to enter data to or extract data from an environment. Generalizing the definition above to the operating environment of a fleet of CAVs (L4-L5 type of vehicles operated by a cloud control centre), i.e. that includes the AV SW and HW, other connected road users and road infrastructure nodes, the road context itself and the cloud backend, the objective of the SHOW cybersecurity mechanisms would be to minimize the connected system's attack surface.

In, one of the earliest analyses of cyber-attacks in the automotive field, the authors discuss attacks on automated vehicles and connected automated vehicles [48]. In [47], the authors have presented feasible attacks on different bus systems used in modern vehicles, including CAN, LIN, and FlexRay. Lately, the topic of security in vehicle-to-infrastructure and vehicle-to-vehicle communication has also been quite extensively researched [51],[52] and [53].

In SHOW ecosystem, the V2X feature is strongly present in most of the use cases while the whole fleet to cloud communication is built on top of an all-IP based communication assumption and therefore users' registration/authentication to the SHOW cloud, cloud internal components' cyber security and secure web-based services deployment is the focus of interest for the development of cyber security mechanisms. SHOW project targets to define mechanisms that make cyber security of automated processes efficient. In the current chapter, Cyber Security Module for SHOW will be presented from a state of the art point of view. More details concerned the tools and the methods which will be used to secure SHOW architecture can be found in D5.1: Big Data Collection Platform and Data Management Portal [19]. In this chapter, relevant and security-critical parameters that make cyber security efficient in automated vehicles transportation are described and the special characteristics of the driving functions and the provided infrastructure are given to take them under consideration. Main threats and vulnerabilities of the autonomous driving systems are presented. SHOW makes use of advanced mechanisms for detection of cyber-attacks through novel tools with the aim to cover wide aspects of cyber security anomaly detection and intrusion detection.

[16] https://frame-next.eu/
[17] https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_0.pdf
[18] https://www.isaca.org/Pages/Glossary.aspx?tid=2049&char=A

Relevant Projects:

The mechanisms and the systems which, if they are combined, are able to create a trustworthy, scalable and secure environment for autonomous vehicles are a subject of research in several H2020 projects. The Avenue [37] project is the predecessor of SHOW, exhibiting many similarities, and targets to validate the advantages of the autonomous vehicles to the public transport. The nIoVe [39] project is a project that aims to build a cyber-security interoperable solution for connected Autonomous Vehicles with the use of machine learning tools for threat analysis. In addition, the DIAS [38] project is a diagnostic anti-tampering solution for vehicles based on the Blockchain technology and Autosar/SECoc (Specification of Secure Onboard Communication).

EVITA [40] project is a relative to SHOW project that proposed an E/E (electrical/electronic) architecture and a Hardware Security Module for autonomous vehicles. EVITA targets to protect vehicles from tampering attacks and prevent leak of sensitive data. For this purpose, EVITA project works together with strong partners such as BMW Group Research and Technology [41] and BOSCH [42]. In addition, one more project that targets to design an IDS system for the European Industry of autonomous vehicles is CARAMEL [43]. Based on AI and ML techniques, the CARAMEL project tries to mitigate risks in the automotive environment by assessing vulnerabilities and possible cyber-attack impacts to the system.

The SAFERtec [65] project focuses on the electronic safety of autonomous vehicles, dividing it into two main points. Secure data exchange between vehicle and road and secure communication between vehicle and cloud application and smart devices. The SURE [66] project concerns the optimization of cyber-physical systems using a large amount of data, which are received from sensors in real time. For this reason, techniques related to the detection of abnormalities, the diagnosis and evaluation of errors and cyber-safe reconfigurable control are used. The goal of the NHTSA [67] project is to use practices implemented by the National Institute of Standards and Technology in Government Security Framework on issues related to cybersecurity. In this way technologies offered by the specific project such as driver assistance, front collision warning, automatic emergency braking and safe communication between vehicles are protected from attacks and security gaps. The E-CORRIDOR [68] project focuses on creating a secure framework for multiple transport systems that will manage cyber threats and prevent unauthorized access to the organization's platform. The European Union Cyber Security Agency, ENISA [69], aims to establish a common level of cyber security throughout Europe. It offers the community a safe and confident environment for secure data exchange.

Focus in SHOW: SHOW project targets to define mechanisms that make cyber security of CCAV services deployment for PT scenarios feasible. For this purpose, relevant security-critical parameters will be identified and the special characteristics of the driving functions and the provided infrastructure as well as the CCAV services deployed on top will be taken under consideration, mainly focusing on securing the SHOW core cloud components and the communication of the SHOW set of connected things to this cloud backend. At the level of the SHOW cloud data portal, the project makes use of advanced mechanisms for detection of cyber-attacks through novel tools with the aim to cover wide aspects of cyber security anomaly detection and intrusion detection. Current progress and planning of the cybersecurity implementation aspects have been described in D5.1.

SHOW cyber-security strategy is based on the following standards: ISO/SAE 21434, ISO 31000, ISO 26262, SAE J3061 and J3101 for cybersecurity risk management. The SHOW process for cyber security would be able to monitor the updates in the overall system and make sure that all the necessary provisioning and also supervision services as recommended by standards have taken place. SHOW strategy will deliver

lifecycle safety and security including scalability. In order for unrecognized vulnerabilities to have less effect in the system's performance SHOW comes with a strategy with different type of operations such as normal, attack or emergency modes. A system that relies on safety and security, which contains the different security operational modes, provides a fall-back possibility.

In order for cyber security to be effective, efforts from multiple parties along the value chain are required, for the entire lifecycle of automated vehicles. Security and privacy are crucial factors for every system and need to be carefully approached in order to guarantee system's stability and efficiency.

2.6.1 Threats and Vulnerabilities

Hackers can gain access to a system with a lot of different ways and they're trying to exploit all of them. A system's security is only as strong as the system's weakest spot. For secure data storage, in the cloud and generally on web, defence in-depth approach is a must. So, in order to prevent cyber-attacks and maximize protection, a multi-layered threat model must consider all threats as equally dangerous. To ensure that your data is fully protected; a security system with multiple layers of defence is needed. Cloud security can be increased by starting the machine with trusted hardware, to ensure security down to the BIOS. The infrastructure should include network virtualization, data encryption in end to end and machine to machine communication, enforcement of least privileged access management and restrict traffic to warranted paths and access patterns [52].

2.6.2 A Taxonomy of Attacks in autonomous vehicles

A variety of potential attacks can be identified in autonomous vehicles technological aspects. The most important of them are described next.

Non-invasive Attacks: This type of attacks happens when the exposed device is not well protected and the attacker can physically access the device. For example, sensors and communication systems which are in public view, such as traffic light sensors should be secured in an isolated environment in order to prevent hackers to physically access the device.

Side Channel Attacks: This type of attacks is used to gather information from the transmitted data. This includes packet sniffing and capturing, time analysis information, etc. Asynchronous processing architecture should be applied as a defence mechanism in this type of attacks.

Code Modification: Hackers can also exploit the OBD-II port in order to gain access and then control first a single ECU and then critical functions of a vehicle. For example, Code Modification can be carried out by a tool connected to the OBD-II port which has been previously modified with malicious code. For this kind of attacks, all the connections in the vehicle should be protected by password so only authorized staff can implement modifications.

Code Injection: Like code modification, code injection is an invasive attack that malicious programs like trojans, viruses and spyware spreaded by the network are trying to implement. Intrusion Detection Systems and Privileged Access Management are the best defenses against this type of attacks.

Packet Sniffing: An eavesdropper can sniff the packets that are transferred between two parties which communicate to each other. So, all transmitted data should be encrypted to ensure confidentiality.

Packet Fuzzing: Fuzzing is a clever way to trick the system by sending modified data to test the system behaviour. Tests with different inputs should be done on a regular basis and the errors that are discovered should be updated and fixed.

In vehicle spoofing: The hacker pretends to be a trusted user in order to replace the default components with modified spoofing devices. The system should be able to distinct a spoofed and an authentic module with resistant techniques.

GPS spoofing: GPS spoofing is a remote access attack. The hacker tries to trick the GPS receiver by interrupting the original signal and transmitting incorrect signals from another device. The power strength of the modified signal is stronger than the original and so the GPS receiver captures the wrong signal. Strong identity and authentication mechanisms should be used in order to protect from this type of attacks. One solution should be that the system should cross check the data with the data another vehicle received.

Jamming: In Jamming attacks also known as blinding attacks hackers use a jammer device that can block the sensors to receive the data. Near infrared filter in cameras or multiple frequency bands can be used to avoid this type of attacks.

2.6.3 A Taxonomy of defences in autonomous vehicles

A variety of potential defences can be also identified in autonomous vehicles to efficiently mitigate the risk of damage. The most important of them are described next.

Secure Communication: Secure Communication between different devices and different parties is a must for the overall security of the system. Encryption can assure confidentiality and authenticity. Message Authentication Code algorithms should be used to assure the integrity of the data transferred.

In Vehicle Device Authentication: Certificates can be used for the in-vehicle authentication process. Certificates are part of the preventive type of defence. The gateway for the inner vehicle parts stores all the public keys.

Nullification: Nullification is part of the attack response type of security. In this type of defence, the capabilities of the in-vehicle devices are extended in order to avoid external attacks. For example, GPS anti-jamming devices are used to protect the system from jamming devices.

Isolation: Isolation of the in-vehicle devices which have been maliciously affected, is a good practice to avoid affection of the critical parts of the system.

Continuous Security Monitoring: Cyber security is not only to prevent attacks and hackers but also to have full control of the system. Security monitoring provides snapshots from all selected parameters of the system. These parameters have to be carefully selected in order to secure the critical parts of the system.

Adaptive Security: Adaptive reconfiguration of parts of the system which are under attack and deception tactics should be applied in the system for better results during an attack.

Table 3: A Taxonomy of Attacks, source: Autonomous Vehicle Security [62]

Physical Access Attack	Remote Access Attacks
Non-invasive Attacks	GPS Spoofing
Side Channel Attacks	Jamming
Code Modification	
Code Injection	
Packet Sniffing	
Packet Fuzzing	
In Vehicle Spoofing	

Table 4: A Taxonomy of Defences – source: Autonomous Vehicle Security [62]

Preventive defence	Passive Defence	Active Defence	Collaborative Defence
Secure Communication	Nullification	Security Monitoring	Cloud Computing
Device Authentication	Isolation	Adaptive Security	
User Authentication	Attack Recovery		
Firewall			

Table 5: Cloud Security Tools for Security and Risks, source [52]

Tools	Risks General
Identity and Access Management	Loss of Visibility
Physical Security	Compliance Violations
Threat Intelligence, Monitoring, and Prevention	Lack of Cloud Security Strategy and Architecture
Encryption	Insider Threats
Cloud Vulnerability and Penetration Testing	Contractual Breaches
Micro-Segmentation	Insecure Application User Interface (API)
Next-Generation Firewalls	Misconfiguration of Cloud Services

Table 6: Types and Layers of Security for External Threats, source [52]

Types	Layers Of Security
Distributed Denial Of Service	DDOS Attack Protection
Infiltration	Bot Management & Mitigation
Data Breach	Web Application Security
	Managed DNS
	Credential Controls
	Endpoint Device Protection
	Identity Management

Table 7: Types and Layers of Security for Internal Threats, source [52]

Types	Layers Of Security
Social Engineering/Phishing	Encryption
Unauthorized Devices	Security training
Unapproved Applications	DNS Security Extensions (DNSSEC)
	Access Control & Authentication

2.6.4 Cyber Security and Artificial Intelligence

Focus in SHOW: Within activities of the SHOW system development, an intrusion detection system as well as an anomaly detection system will be developed based on novel artificial intelligence and deep learning aspects to meet the demanding challenges of AV cybersecurity defence. Various algorithms will be explored and final intrusion detection module and anomaly detection module will be integrated in selected parts of the SHOW system to strengthen defences. These modules will also be

integrated in selected pilot sites either at the operator site or even on-board and further assessed in real conditions.

2.6.4.1 Machine learning algorithms

Machine learning goes beyond the limits of classical programming, training models that enable them to learn and make decisions without simply executing predefined commands explicitly set by the programmer. One of the possibilities of a machine learning model is to derive predictions based on mathematical-type functions that serve to convert natural language into mathematics so that structures or paths can be found in them [63]. Artificial intelligence can be used to create a honeypot system. This application uses machine learning techniques to detect a possible intrusion that may occur. Depending on the body's security measures, an intrusion attempt can be detected by a firewall. Therefore, the firewall can be set up in such a way as to redirect the suspicious user to the honeypots, in order to gather information about the movements he makes and his behaviour in general. The data collected is subjected to machine learning algorithms to group the data into homogeneous classes and to create a profile related to user behaviour.

Another area of contribution of artificial intelligence is the detection of anomalies in a network. Signature anomaly detection methods monitor network mobility and compare incoming user packages with those in the database that have been identified as malicious. Then the comparison is made and if the incoming packages are identified with the malicious ones then the user is characterized as hostile. These systems, however, have limitations when it comes to zero-day attacks where no vulnerability has been previously detected, leaving no signature available to detect them [48]. For this reason, intrusion detection systems are used, taking advantage of the possibilities of artificial intelligence to detect patterns that are hostile even in packages that are used for the first time without existing in a database [64].

2.6.4.2 Intrusion Detection

The cyber threats have become more sophisticated and complex in our times; however, defence is still focused on previously recognized threats and external threat intelligence. When we are looking the hardware level threats, we are dealing with supply chain compromises, software/ firmware tampering, or more advanced attacks in the hardware root level. A system that uses only the default defences or blocking known threats cannot be considered reliable. Every system has different needs for security so different tools and processes have to be involved to boost security [52].

Intrusion detection is part of the general signal detection problem. Intrusion observations are considered to be the signal to be detected, while signals of normal operations are considered to be noise. In classical signal detection techniques, both the noise distributions and the signals are viewed as known, and the security system needs to decide if a given observation belongs to the signal-plus-noise distribution or to the noise distribution. Classical signal detectors use both distributions in order to make a decision, but intrusion detectors depend on either signal or noise characterization to make decisions [54].

In the era of AI, intrusion detection is leveraged to address the ongoing challenges of cyber threats. Specifically, “An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars” is an IDS (Intrusion Detection System) research work that compromises Artificial Neural Networks and uses data generated from the network behaviour to detect DoS attacks [56]. An additional IDS research work for AV’s named “Tree-based Intelligent Intrusion Detection System in

Internet of Vehicles", evaluates and compares machine learning algorithms such as random forest, decision tree, extra trees, XGBoost, stacking, SVM, KNN in order to detect BENIGN, DoS, Port-Scan and Brute-Force attacks with the use of CICIDS2017 [57] data set. It should be mentioned that according to the results of this work stacking algorithms and the XGBoost method combined with Feature Selection Techniques are the best algorithms in terms of accuracy [58].

2.6.4.3 Anomaly Detection

A full description of the noise distribution can be used as an anomaly-based detector. Any observation that is not included in the noise description it is considered to be an attack. The anomaly systems are based on the hypothesis that intrusive activities differentiate from system's normal activities at some level of observation [62]. In order for the anomaly detection system to work appropriately to cover SHOW needs there are some requirements which have to be satisfied: First, the anomaly detection system should provide real time detection, second, detection should not be based on the system's experience from previous attacks and finally anomaly detection should be automated and not relying on human operators.

The work from Van Wyk et al. [59] have acknowledged that AVs would heavily rely on information from other vehicles and sensors. So, they propose an anomaly detection approach to pinpoint malicious cyber-attacks and faulty sensors that can potentially lead to undesired scenarios. The proposed framework for the anomaly detection is based on the Kalman Filter and Convolutional Neural Network (CNN). The Kalman Filter is widely adopted in time-series data and an adaptive Kalman Filter with a x2-detector is implemented in the framework. The role of the Kalman Filter is to filter out the noise from the process and measurements. Furthermore, the CNN's input is a series of instances produced by the continuous feed of the sensor's raw data during a trip. The framework makes use of the models in a successive way. Initially, the data from sensors are fed to the CNN that flags the malicious sensors. Consequently, the remaining data after the exclusion of malicious sensors are fetched to the Kalman Filter for the same purpose. The framework is tested against data from a database from Safety Pilot Model Deployment program [59].

"Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle" is a relevant research which goes back to 2016 in the 15th International Conference on Ubiquitous Computing and Communications and in the 8th International Symposium on Cyberspace and Security. The researchers built an anomaly detection system using an autonomous - robotic vehicle to detect Replay Packet Injection and Rogue Node attacks with the use of supervised machine learning algorithms and GPS spoofing or sensor jamming taking into account the Received Signal Strength. Finally, a mechanism that applies weights in the different data sources was applied in [60], as shown in Figure 8.

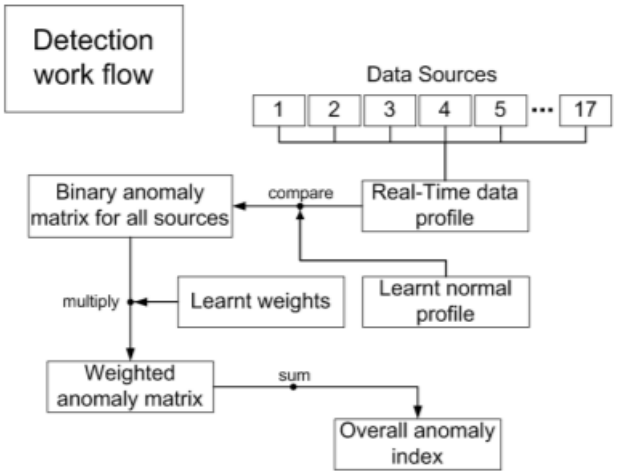

Figure 8: Intrusion Detection System [60].

Another work on anomaly detection has been done by Guo et al [61] who bridge the edge computing and anomaly detection in their framework named EVAD. The suggestion springs for the realization that the CAN bus protocol could be unable to meet the demands set from real-time scenarios due to constraints in resources. The acronym for the framework stands for *Edge Computing Based Vehicle Anomaly Detection* and pinpoints the anomalies based on time and frequency domain properties. The edge devices intervene between the vehicles and the cloud as intermediary devices. Four modules are composing the EVAD framework. The first module focuses on the data collection for EVAD as it links to the On-Board Diagnostic Interface. Next is the Model Generation module that is hosted to a separate cloud server from the other modules. This module generates a general model with the correlation ring for the selected sensors and their order, the preliminary threshold for anomalies, and the specific frequency range of PSD for a specific vehicle. The third module is the Anomaly Detection Module where the data from sensors are analyzed to decide on the existence of a vehicle anomaly. The final module objective is to notify the driver and push the result to the cloud server [55].

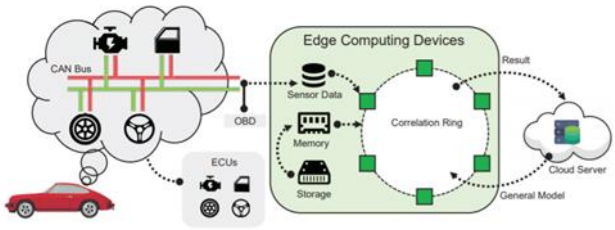

Figure 9: EVAD's System Overview, source [61].

3 Methodological Approach

The system architecture is a formal description of a system that enables reasoning about the structural properties of the system. It defines the system components or subsystems and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system. This may enable one to manage investment in a way that meets business needs. A C-ITS architecture is the conceptual design that defines the structure and/or behaviour of an integrated co-operative Intelligent Transport System (C-ITS). “Co-operative” C-ITS Architecture can be created at EU-wide, national, regional or city level, or relate to specific sectors or services.

The methodology that was followed in SHOW in order to derive the reference architecture is schematized in Figure 10 and includes the following steps:

1. Based on the project Use Cases (see Appendix I) and the knowledge acquired via the interviews with the majority of the local demo site technical boards, within project activity A4.1 and in conjunction with WP5 and WP6 of the project, the conceptual architecture (see sec. 4.2) as well as the internal and external sub systems of the SHOW system were defined (see sec. 4.3). In parallel, a preliminary service decomposition into cloud/on-board functions was made possible useful for step no. 4;
2. Based on the WoTs architecture paradigm, the SHOW four logical layers were derived (see sec. 4.4);
3. Based on the type of services and data/interfaces required for integration of SHOW platform with existing systems, non-functional cross-layers’ requirements w.r.t to interoperability, cyber-security and communications have been derived (see sec. 4.6);
4. Based on the C4 nested model, the work was split into providing four views of the system architecture, presented in Figure 11, in an iterative mode:
    a. System conceptual view (see sec. 4.2);
    b. System functional view (in three variations) (see sec. 4.4);
    c. System intra layer architecture focusing only on i) the SHOW CAV generic on-board architecture and ii) the SHOW cloud backend architecture (see sec. 4.5);
    d. Web-service deployment architecture including three prominent SHOW services, namely the SHOW Dashboard, the ETA service and the MTP service (see chapters 5 and 6).

3.1 Diagrams model

For the architecture documentation and visual diagrams’ provision the following methodology was followed:

- Inspired by the C4 model (outlined in the Appendix V) but not following it strictly, the following architecture views are derived adding details incrementally by using four levels of representation (Figure 11):
    - Conceptual view (the system, external systems interfaced with the system and their actors – either data providers or data consumers)
    - System functional view (layers)
    - Layers’ functional view
    - Web-service instantiation view (see chapters 5 and 6): types of data, components involved, types of interfaces, functional requirements for specific SHOW service

- For the creation of the diagrams' elements, we follow the C4 model when possible, where:
  a) The following C4 elements are used: User, SW system, Container, Database.
  b) In our implementation, a C4 Software System is denoted with a rounded rectangle while a C4 Container or a C4 Component are denoted with a normal (non-rounded) rectangle.
  c) Optional interfaces among C4 elements are denoted with dashed line.

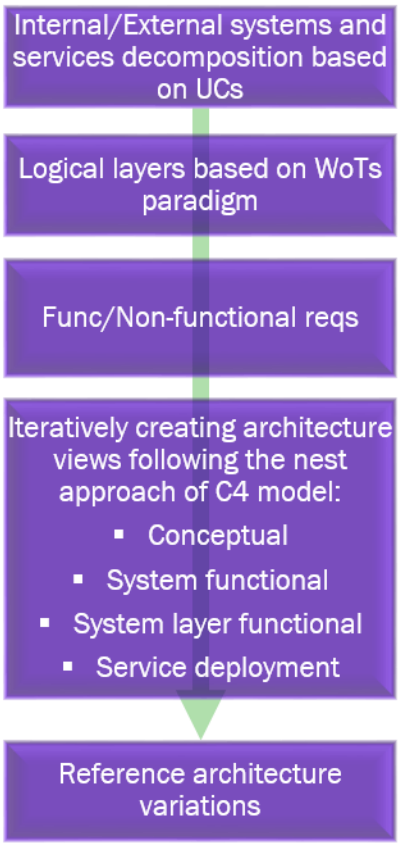

Figure 10: Methodological approach overview.

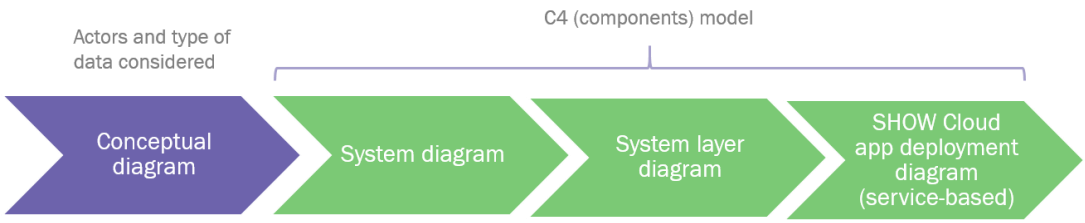

Figure 11: Discrete architecture views (4 levels of detail).

3.2 Modal verbs terminology

For the requirements' elicitation in the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described below. "must" and "must not" are NOT used in D4.1.

Table 8: Modal verbs terminology

Modal verb	Equivalent expression
shall / shall not	is to, is required to, it is required that, has to, only ... is permitted, it is necessary
	is not allowed [permitted] [acceptable] [permissible], is required to be not, in not to be
should / should not	it is recommended that, ought to
	it is not recommended that, ought not to
may / may not	is allowed, is permissible
	it is not required that
can / cannot	be able to, there is a possibility of it is possible to
	be unable to, there is no possibility of, it is not possible to

4 SHOW Architecture views

This chapter explains the motivation behind a reference design framework for CCAM services (sec.4.1) and then describes the SHOW architecture views produced by following the methodology described in sec. 3.1 (system conceptual view, system functional view, system layer view). Starting from the system conceptual view, the system functional and operational requirements (sec. 4.3) are derived and based on those, the functional architecture views are defined. Chapters 5 and 6 that follow complement this work by adding the deployment diagrams of the SHOW Dashboard service (chapter 5) and two of the SHOW advanced CCAM services (chapter 6) as an exercise to create a service-oriented deployment view.

4.1 Services for CCAM under a common design framework

The C-ITS domain for connected and collaborative driving services comprises widely spread systems like traffic management systems, road side unit controllers, and vehicle on-board units. Such complex and heterogeneous systems have independent uses but demand a strategy to facilitate their convergence. Looking at the C-ITS evolution in Europe, the reference C-ITS architecture proposed by ETSI[19] which is application and technology-agnostic (compatible with the ISO/IEC/IEEE 42010 international standard for architecture descriptions of systems), proved to be useful for the pan-European adoption of standardized data models and communication protocols.

Going beyond the C-ITS domain and embracing new AV functionality, the CCAM partnership SRIA[20] has identified three domains which are considered as enablers of new CCAM services, namely cybersecurity, data sharing and artificial intelligence (AI), all very relevant to the SHOW central concept of a big-data mobility cloud platform. Based on CCAM SRI agenda, “a harmonized approach to further develop these technologies can help to reduce market fragmentation, currently hindering EU companies to fully benefit and exploit new mobility business cases based on CCAM.” and “leading to maximized societal benefits of the technology application”. For SHOW big-data enabled services and project centralized monitoring purposes, following a joint and harmonised approach supporting a centralized data sharing and data storage platform development is essential to allow for seamless, continuous operation by multiple actors (both from the vehicle side and the infrastructure) across very different settings as these are defined by the local ecosystems deployed within SHOW. The required harmonised approach will need to incorporate aspects like standardized interfaces for maximizing interoperability, a common data format, a common ontology for defining the local architecture design in a harmonized way as well as service-specific and site-independent transversal non-functional aspects like quality of service (e.g. data delay tolerance), interoperability, data privacy and cybersecurity (complying with European regulation regarding privacy, data security and cybersecurity). Covering all these aspects and also caring for future SHOW services’ deployment, an abstract SHOW system architecture was decided to be produced with the main objective to guide all the integration, implementation and evaluation work of the project keeping the need for design and implementation effort by the sites at minimum and applying a service-oriented approach. Within the proposed architecture, three main

[19] https://www.itsstandards.eu/app/uploads/sites/14/2020/10/C-ITS-Brochure-2020-FINAL.pdf
[20] https://www.ertrac.org/uploads/images/CCAM%20Partnership%20SRIA%20v1.0%2002-11-2020.pdf

variations of system architecture for data sharing are identified (note that data sharing architectures is identified as important by CCAM SRIA).

In conclusion, to prepare for the integration of both mature and non-mature CAV fleet ecosystems, this work provides a unified multitier architecture that supports a set of service-oriented passenger, on-board and operational backend intelligent applications (i.e. the SHOW AI tools and services) offering a harmonized and "supervised" design framework to be used by the SHOW sites for integration of their local subsystem with the SHOW Mobility Data Platform (the role of this supervision is undertaken by WP4). This generic reference architecture will then be adapted by each local demo site integration/implementation team to the local ecosystem needs/pre-existing components in order to create the site's reference architecture instantiation that will be described for each site in next version of this deliverable, D4.3. In this way, a minimum set of design requirements is ensured to be followed by all:

- Service-oriented design principles following the WoTs paradigm
- Common data sharing design principles for both static and dynamic content (via standardized interfaces)
- Interoperable data exchange among heterogeneous data providers (maximizing standardized interfaces)
- Harmonized integration of external data sources through APIs
- Data privacy and cyber-security cross-layers mechanisms recommendations

4.2 System conceptual view

SHOW architecture has been conceived as an extended model of a C-ITS architecture for urban deployment with a service-oriented approach inspired by the Web of Things (WoTs). The system conceptual view, that is presented in Figure 12, models the attributes of and the interaction among the SHOW system actors in an integrated system: AV operators, PT operators, riders, other road users, public authorities, 3rd party data providers, 3rd party services providers, automakers and legislation. This view captures a preliminary version of the system where all the actors considered are either data providers and/or data consumers based on the WoTs paradigm.

The focus of the corresponding diagram, presented in Figure 12, is to describe the entities in the SHOW ecosystem based on a synthesis of actors present in the SHOW 16 demo sites' use cases' and services' description (see Appendix IV), along with the type of data they are expected to exchange with the SHOW cloud system: i.e. the SHOW Mobility Data Platform (SMDP) as well as any existing local AV fleet management platform (AVxPT local fleet management platform - LFMP), which together comprise the SHOW integrated cloud system. Please note, that i) for reasons of completeness, in this diagram, actors like the "Electricity provider" assumed implicitly present for the SHOW ecosystem implementation are also depicted although not part of the SHOW system ii) dashed connections denote an optional interface to the cloud present only to specific use cases iii) as also presented in the notation at the upright corner of the diagram, for nodes that belong to the physical layer of the road environment (like RSUs, CCAVs and connected road users) and which exhibit C-ITS connectivity a connectivity icon is added (in white for mobile nodes, in grey for static nodes.

Similar to the WoTs' architecture (see sec. 2.2), the cloud architecture is composed of four main layers, namely the connected devices layer called *Things* (not depicted as *layer* but as C-ITS nodes in the conceptual architecture), *the data ingestion and publishing layer,* called *Things' abstraction* (first layer inside the SHOW Mobility Data Platform system in the conceptual architecture), the *Cloud data processing layer* including the data and services management and finally, the *Web-services layer* which

is built on top of it. In this view, the cloud system is simplistically presented as more details on the internal and external components needed to implement this core part of the system will be given in the subsections 4.4 and 4.5.2 that follow.

As presented in Figure 12, the SHOW conceptual architecture encompasses the actors described in Table 9. Actors of the integrated system are also linked to UCs using as quick reference the Appendix I.

Table 9: Conceptual architecture actors

Architecture actors: (Data producer/ Data consumer per WoTs paradigm)	**Description**	**Relevant UCs**
(C)CAV	AV, member of the SHOW CAV fleet. It may be an Auto-shuttle, Auto-taxi, Retrofitted bus, Retrofitted vehicle. SHOW CAVs may be connected via their on-board communication API to all or part of the following entities: - the local cloud AVxPT system - SHOW cloud data portal and analytics platform (either directly or indirectly) - the V2I infrastructure nodes - the V2G infrastructure nodes - other AVs via V2V in SHOW platooning scenario (UC #3.1 for CCAVs) - other road users via M2M communication (UC #3.1)	All UCs
On-board smart device/screen	Device installed inside the CAV to present local fleet management platform notifications (trip or other info) to the users (acts as data consumer). It may also act as a data provider and transmit sensor or other data towards the SMDP.	All UCs (optional feature)
Other road users	This actor definition covers AV cooperative entities (that will coexist or interact with the AV) present in SHOW UC #3. It may include other vehicles with driving automation feature(s) engaged, shared road users (e.g., drivers of manually operated vehicles or pedestrians or cyclists carrying personal devices), or road operators (e.g., those who maintain or operate traffic signals or work-zones). As per SAE J3216 [/REF], Machine-to-machine (M2M) communication to enable cooperation between two or more participating entities or communication devices possessed or controlled by the previously referred entities is implied. The cooperation supports or enables performance of the dynamic driving task (DDT) for the AV under test.	UC 3.1
Auto-bus depot/parking	Physical infrastructure node representing a parking location. (Equipping this with digital infrastructure node to offer connectivity to local fleet management platform may be offered)	
Charging facility	Physical infrastructure node representing a charging position	UC 1.4
Cyber attacker	Cyber-attack threats are considered against SHOW's connected integrated system across all layers of the system	All UCs
4G, ITS-G5 public network	Available communication networks for AV's	All UCs
Sat/Nav system	GNSS positioning systems. Such as GPS, Galileo and more.	All UCs

Architecture actors: (Data producer/ Data consumer per WoTs paradigm)	Description	Relevant UCs
Electricity provider	[self-explained]	All UCs (when electric CAVs are involved)
National CAV Regulation – Certification	National regulations that SHOW CCAV fleet should respect for permits' acquisition	All UCs
Public Transport Backend system	Public Transport data provider (e.g., trip scheduling, transit data)	All UCs (when PT backend is integrated, see)
Smart city Backend system	Smart city data provider (e.g., parking data)	All UCs (optional feature)
HD map	Apriori HD map data provision for aiding CCAV perception	All UCs (optional feature)
Smart city RSU/traffic light (V2I, I2C data)	SHOW could send decisions to components such as e.g. traffic lights	All UCs (optional feature)
Mobility Hub monitored by camera	Auxiliary video monitoring node to assist decisions for CAVs passing a mobility hub	UC 1.x
Smart bus stop	Smart bus stops can provide to Public Transportations requests such as asking a bus/taxi to stop to this position	UC 3.4
Commuter smart device	Provides information to users such as the location of bus, the expected arrival time, proposed trips to access a specific location etc	All UC 1.x (optional feature)
On-board commun. API	Responsible to connect the CCAVs to the cloud or other road users	All UCs

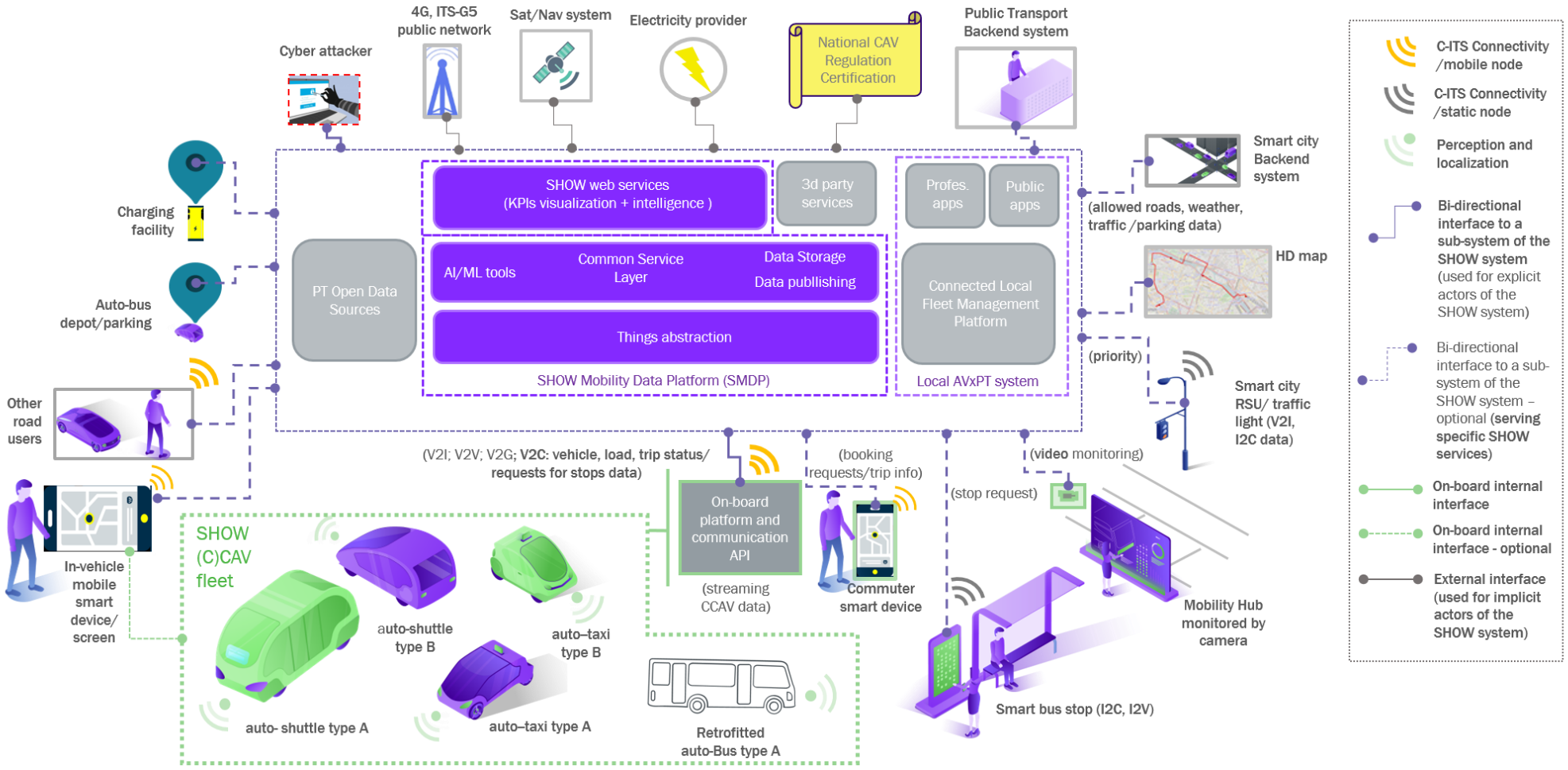

Figure 12: System conceptual view: actors and type of data exchanged among them and the SHOW integrated system.

4.3 From use cases to logical and SW architecture

In Table 10, the system's high-level functional, non-functional and operational requirements are presented. These were derived based on the demo sites' UCs analysis (last column of Table 10). Based on the conceptual architecture presented in Figure 12, each requirement is linked with the corresponding architecture entity involved in its satisfaction.

Based on an iterative system requirements' analysis within the WP4 team,

- First, the core entities of the three layers of the system have been conceived; the result is shown in the next section's architecture abstraction as Figure 13.
- Then, the core entities of the three layers of the system have been conceived leading to the more detailed architecture diagram of Figure 16 (multiple Things' data ingestion platforms).
- Finally, based on continuous discussion with the demo sites on CAVs data handling and envisioned data exchange among the local AVxPT system and the SHOW MDP as well as future proofing work based on the state of the art, two more architecture variations are created leading to the architecture diagrams of Figure 15 (single private Things' data ingestion platform) and Figure 17 (futuristic shared data ingestion platform).

Table 10: System Functional (FR), non-functional (NFR) and operational (OR) high-level requirements based on SHOW demo sites' UCs analysis and rough mapping to SHOW integrated system architecture elements

Identifier	Functional (FR), non-functional (NFR) and operational (OR) high-level requirements	Architecture elements	Relevant UCs
FR-01	Each SHOW Thing, member of the (C)CAV fleet, infrastructure nodes (includes SHOW smart bus stop node) and other connected road users, shall be connected via their on-board/device communication API to the following SHOW entity: .the local cloud AVxPT system. Both periodic exchange of vehicle/trip static data and close to real time vehicle/trip data shall be enabled.	Interface between ▪ SHOW Thing ▪ local cloud AVxPT system	All UCs/ UC 3.4 (smart bus stops) (only applicable for sites that do possess local cloud AVxPT system)
FR-02	Each SHOW Thing, member of the (C)CAV fleet, infrastructure nodes and other connected road users, may be connected via their on-board/device communication API to the following SHOW entity: .the SHOW cloud data portal. Both periodic exchange of vehicle/trip static data and close to real time vehicle/trip data shall be enabled.	Interface between ▪ SHOW Thing ▪ SHOW cloud data portal system	All UCs / UC 3.4 (optional feature)
FR-03	Each SHOW Thing (member of the (C)CAV fleet and other connected road users) may be connected via their on-board/device communication API to the following SHOW entity:	Interface between ▪ SHOW Thing ▪ SHOW Infrastructure node (e.g.	All UCs (optional feature)

Identifier	Functional (FR), non-functional (NFR) and operational (OR) high-level requirements	Architecture elements	Relevant UCs
	.the V2I infrastructure nodes.	smart traffic light)	
FR-05	Each SHOW (C)CAV fleet member, shall be connected via their on-board/device communication API to the following SHOW entity: .other AVs via V2V in SHOW platooning scenario.	V2V interface between CAVs	UC 1.9
FR-06	Each SHOW Thing (including the (C)CAV fleet members, the infrastructure nodes and other connected road users) shall be connected via its on-board/device communication API to the following SHOW entity: - other road users via M2M communication between and among traffic participants in SHOW cooperative AD scenario.	Short-range / wireless communication among SHOW Things	UC 3.1
FR-07	Things' data from the local AVxPT cloud platform shall be shared with SHOW cloud in close to real time updates and via standardized interfaces.	Interface between SHOW cloud data portal and local AVxPT platform	All UCs (only applicable for sites that do possess local cloud AVxPT system)
FR-08	Processed KPI data from the local AVxPT cloud platform shall be shared with SHOW cloud in regular intervals	Interface between SHOW cloud data portal and local AVxPT platform	All UCs (only applicable for sites that do possess local cloud AVxPT system)
FR-09	SHOW CCAV fleet member shall cooperate with another connected road user in the neighborhood. The cooperation supports or enables performance of the dynamic driving task (DDT) for the AV under test.	CCAV communication API	UC 3.1
FR-10	Local AVxPT system integration with external data providers like PT backend, TMC, smart city backend for traffic, transit and charging data retrieval	Local AVxPT system: Integration with external data providers	All UCs, especially 1.4, 1.5, 1.10 (optional feature)
FR-11	SHOW data portal integration with external PT data open sources like NAPs ot GTFS-RT via standardized interfaces may be established for collecting of additional data to be used in AI algorithms/ML models training. Bi-directional exchange by local AVxPT systems feeding the NAPs may be also considered for after SHOW implementation.	Local AVxPT system: Integration with external data providers	All UCs, especially 3.1, 3.2 (optional feature)
OR-01	Storage of Things' data including meta-data carrying data creation	SHOW cloud data portal DB	All UCs

Identifier	Functional (FR), non-functional (NFR) and operational (OR) high-level requirements	Architecture elements	Relevant UCs
OR-02	Storage of additional data like SHOW user surveys	SHOW cloud data portal DB	All UCs
OR-03	SHOW cloud data portal shall support communication between itself, the SHOW Dashboard and other service providers.	▪ SHOW cloud data portal ▪ SHOW Dashboard as a SHOW service ▪ SHOW Marketplace incl. 3rd party service providers.	All UCs
OR-04	Subscription of all connected Things to SMDP shall be possible in a secure and anonymized way	SHOW cloud data ingestion (IP-based protocols)	All UCs
OR-05	Event-based analysis and re-publishing of stream data shall be supported by SHOW cloud Mobility Data Platform for SHOW web services provision (incl. the SHOW Dashboard)	SHOW cloud Mobility Data Platform	All UCs and especially 3.1 and 3.2
OR-06	Storage of big data from continuous operation shall be supported	SHOW cloud data portal DB	All UCs and especially 3.1 and 3.2
OR-07	Smart AI-enabled tools shall be hosted inside the SHOW cloud Mobility Data Platform for providing of advanced CCAM services (e.g. estimated time of arrival service, multi-modal journey planner service)	▪ SHOW cloud Mobility Data Platform ▪ Web-based AI-enabled services	3.1 and 3.2
OR-08	SHOW marketplace to support DRT services for PT	SHOW cloud Mobility Data Platform	
OR-09	One-way event-based communication among the CCAV fleet and the LFMP shall be supported for tele-monitoring		All UCs
OR-10	Bi-directional event-based communication among the LFMP and the CCAV fleet shall be supported for tele-monitoring and tele-operation service (VoIP streaming may be included too)	AVxPT local system: Integration of local Operation Centre	UC1.7: Connection to Operation Centre for tele-operation and remote supervision.
NFR-01	Cyber security mechanisms present in all interfaces among systems and inside each layer and especially among CAV fleet members and the cloud.	Cyber security: cross-layer	All, especially UC1.7
NFR-01	Cyber security mechanisms present in all interfaces among systems and inside each layer and especially among CAV fleet members and other CAVs	Cyber security: V2V	UC 1.8 - Platooning

Identifier	Functional (FR), non-functional (NFR) and operational (OR) high-level requirements	Architecture elements	Relevant UCs
NFR-01	Precise localization aid via RSU auxiliary node may be offered	CCAV to RSU node for localization (e.g. via RFID)	UCs 1.2, 1.3 that pose higher safety concern (optional feature)
NFR-01	Hybrid communication scheme may be supported by the SHOW (C)CAV fleet member when available, for ensuring service continuity	CCAV (hybrid connectivity)	All UCs and especially UCs 1.2, 1.3 and 1.8 that pose higher safety concern.
NFR-01	Secure, low-latency M2M communication between SHOW CCAV fleet member and any other participating entity or communication device possessed or controlled by other road users or RSU.	V2P, V2V, V2I, V2C	UC 3.1
NFR-01	Unicast/broadcast C-ITS communication may be supported by the CCAV API	V2V, V2I	All UCs (optional feature)
NFR-01	Secure and private subscription of all connected Things to SHOW cloud data portal shall be managed via authentication, de-anonymization and other means	SHOW cloud data portal: Things' subscription mechanisms	All UCs (optional feature)

4.4 System functional view

First, an abstraction of the system functional architecture is provided in Figure 13. The SHOW cloud platform is named SHOW Mobility Data Platform (SMDP) and includes the cloud Things' abstraction, the Big Data Collection, the Data Management Portal and the AI tools suite. It is created using the SPACE reference architecture as a subsystem and extending it to support the role of the SHOW Mobility Data Platform (SMDP), under the following additional considerations:

- Two interfaces among the physical layer (incl. Things) and the data ingestion cloud platforms have been foreseen, namely the I_p_Things and the I_s_Things towards the LFMP and the SMDP respectively in order to cover cases where both LFMP and SMDP process subset of the Things' data. This is particular valid in cases where the LFMP focus only on CCAVs fleet integration ignoring other actors of the physical layer. It may be also the case that CCAV data includes auxiliary ad-hoc on-board equipment installed for the SHOW purposes and not initially considered in the local existing LFMP operation (e.g., on-board android tablet).

- SW blocks "Fleet Operational Platform" and "External Enablers" are borrowed from SPACE but in our architecture we have omitted the "V2X+charging" Enabler component as we consider this as part of the Smart City Enabler component;

- We add nodes interacting directly with AV fleet at the physical layer level. Those nodes include: Non-AV road users, commuters, infrastructure nodes.

  Important note: ALL nodes within the physical layer may be connected to the cloud via the I_p or I_s interfaces. Additionally, they are considered interconnected within the same layer they belong into, via short-range V2X ad-hoc networks. This is not depicted due to space limitation in the graph of Figure 13, but it becomes explicit in the functional views of Figure 15, Figure 16 and Figure 17 that follow. That includes a physical V2G interface provided for charging the electric CAVs.

- Direct interface between enablers and CAV fleet is also foreseen, this is the purpose of the interface I_c_enablers. This may include i) a wireless connection to a 3^{d} party data provider API or ii) stored data transfer to CAV on-board platform via a physical port (e.g., USB port), e.g. for offline transferring of HD maps;

- We added an optional new link to Open Mobility data sources (shared through GTFS, GTFS-RT or NAPs) to highlight the need for such open road traffic/PT data, especially in view of CCAV enhanced services' provision based on big data and AI as envisioned within SHOW.

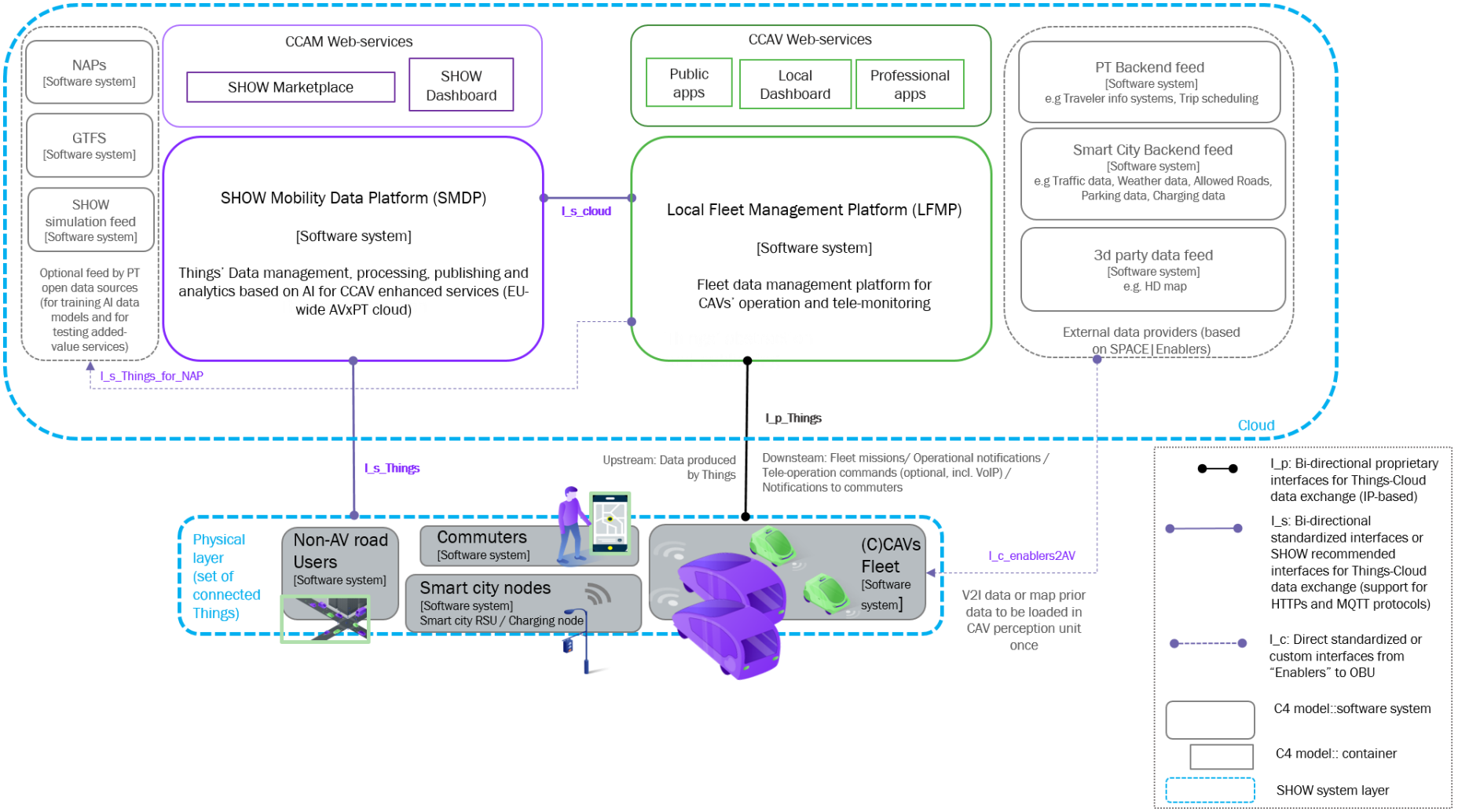

Figure 13: System functional architecture abstraction.

Main components/ SW systems involved shown in Figure 13 are described in detail in Table 11.

Table 11: SHOW integrated system main SW systems and sub-systems, shown in Figure 13, and data exchange mechanisms

Description	Codename	Data exchange mean
SHOW Mobility Data Platform (on top of which the SHOW and 3rd party web services are located)	SMDP	Event-driven big data management and analytics platform APIs
Local Fleet Management Platform for orchestration of AV fleet and deployment in PT connected to external city data providers (on top of which the professional operational and 3rd party web services are located)	LFMP	Integrated CAV data platform APIS
Non-AV road users includes traditional connected vehicles, pedestrians with smart devices, bicycles with smart devices, 2-wheelers with smart devices	Non-AV road users	Android device or other smart device
Passengers, commuters at home or at bus stops equipped with smart device	Commuters	Web interface or personal smart device
Connected AV fleet that includes AD-enabled taxis and shuttles. Being also "Collaborative" only for specific SHOW scenario (UC 3.1).	(C)CAV fleet	On-board communication API (support for proprietary V2C and standardized V2V, V2I and optionally V2P)
Urban infrastructure nodes equipped with sensors and C-ITS/LTE communication capability (e.g. smart traffic light, RSU)	Smart city nodes	RSU communication API
PT static and dynamic data: schedules, transit data, traveller info data	PT backend	PT backend APIs to LFMP and others
Smart city data including traffic, geofencing for AVs, weather, parking and charging related data	Smart city backend	Smart city backend API to LFMP and others
NAPs data feed	NAPs	NAP API
GTFS/GTFS-RT transit data feed	GTFS	GTFS APIs
SHOW simulation data feed	SHOW Simulation feed	SHOW A12 / offline or through SHOW defined API

The interfaces depicted in Figure 13, are described in Table 12.

Table 12: Interfaces of Figure 13

Description	Codename	Protocol if known/ Data examples
Bi-directional proprietary interfaces for data exchange between the THINGS and the Cloud	I_p_Things	Data produced by THINGS, Fleet missions, Operational notifications, Tele-operation commands (optional), Notifications to commuters
Bi-directional standardized interfaces or SHOW recommended interfaces for data exchange between the THINGS and the Cloud	I_s_fleet	Support for HTTPs and MQTT protocols / data from CCAV on-board smart devises

Description	Codename	Protocol if known/ Data examples
		Not only CAV data but also all other connected THINGS data
Bi-directional standardized interfaces for data exchange between cloud servers	I_s_cloud	Data managed by local fleet management platform and requested by SHOW DMP (CCAV data, operational data, data aggregates for KPIs computation) Bi-directional means that the LFMP can also subscribe to SHOW DMP services
Data exchange from LFMP to open data server (e.g. NAP)	I_s_Things_for_NAP	For EU, minimum set of data to be public according to new ITS directive for NAPs
Direct standardized or custom interfaces from "Enablers" to CAV OBU	I_c_enablers2AV	V2I data or map prior data to be loaded in CAV perception unit once
Direct standardized interfaces among THINGS on the road plane aka V2X	I_s_V2X (not incl. in Fig X but see Fig. Y-Z below)	It includes V2V among CAVs fleet e.g. for platooning. Relates also to UC 3.1 (interaction to other rod users)

4.4.1 The complementary role of a SHOW reference Dashboard service

As presented in the system functional overview of Figure 13, the proposed reference architecture supports two discrete Dashboard services that can be enabled by the LFMP and SMDP cloud platform respectively. Their discrete roles are specified in Table 13 hereafter. The Local Dashboard service was the first to be designed as part of the traditional Fleet Control Room on top of the LFMP used mainly for operational purposes by the LFMP owner. As in SHOW, maturity among multiple local sites varies (please refer to sec. 5.4), not all sites do support a fully functional LFMP and hence not all the local sites have the privilege to operate or plan to implement a Dashboard service for fleet monitoring and KPIs visualization purposes on top of their LFMP. Therefore, this service on top of LFMP is considered optional within the research/experimental purposes of the SHOW project.

This was the main motivation behind the design of a centralized SHOW Dashboard on top of the SHOW MDP since the projection of the local sites' fleet data on a map was considered an important project monitoring tool and the KPIs data from all local sites would already have been part of the big data SHOW Databases (stored inside SMDP, transferred through the I_s_cloud interface, see Figure 14). This reference Dashboard design was the basis for a site-agnostic PoC for LFMP data visualization (described in D4.2) that also proved very helpful during the deployment of SHOW architecture in the local demo sites that wanted to implement their own dashboard services on top of their LFMP (helped in early verification of data model, data interfaces/integration, KPI definitions/visualization paradigms).

The SHOW dashboard was designed as a web service that can be accessed freely by all partners in SHOW on top of SMDP and used for LFMP data monitoring purposes. The service, maintained in Sweden's cloud and run by RI.SE partners remotely, excludes any operational or tactical inteventions to the local things' ecosystem and it is primarily used for project's KPIs visualization purposes and multi-site fleet

visualization during the SHOW piloting activity (as also presented in Table 13), especially assisting the local sites that do not own their own local Dashboard service.

Functionality	**Local Dashboard service**	**SHOW Dashboard service**
Fleet data visualization on a map	(x)	x
Infrastructure data visualization	(x)	x
Commuters' data vosualization	(x)	x
Local LFMP KPIs	x	x
SHOW project KPIs	(x)	x
Map alerts' generation	(x)	x
Backward communication with the fleet (notifications, emergency stop message)	x	-
Bilateral VoIP communication with the fleet	(x)	-
Remote control functionality	x	-

Table 13: Functionality supported by the two Dashboard services part of the SHOW reference architecture ('x' means supported, '(x)' means optionally supported, '-' means not supported)

NOTE 1: There is no conflict in having both SHOW Dashboard and local dashboard running in parallel as their objectives are disentangled. The SHOW Dashboard is designed as a passive dashboard used for performance monitoring and visualization purposes and as such no operational intervention to site operation is allowed. The local fleet management and control via bi-directional communication with the local fleet/users, is performed by the LFMP (via the I_p_things generic interface, see Figure 13*) on top of which the Local Dashboard service may run (if not pre-existing usually represented by a simplified remote control application used for the purposes of the local pilot, see D4.2 Appendix I).*

Apart from the project-specific use described above, the design of a reference SHOW dashboard service may serve a broader audience, and in particular for future-wise use by AV4PT operators: the dashboard and its components can serve as inspiration and best practice reference for the designs of local dashboards and multi-site/multi-view

dashboard e.g. at European or national transport authority level.

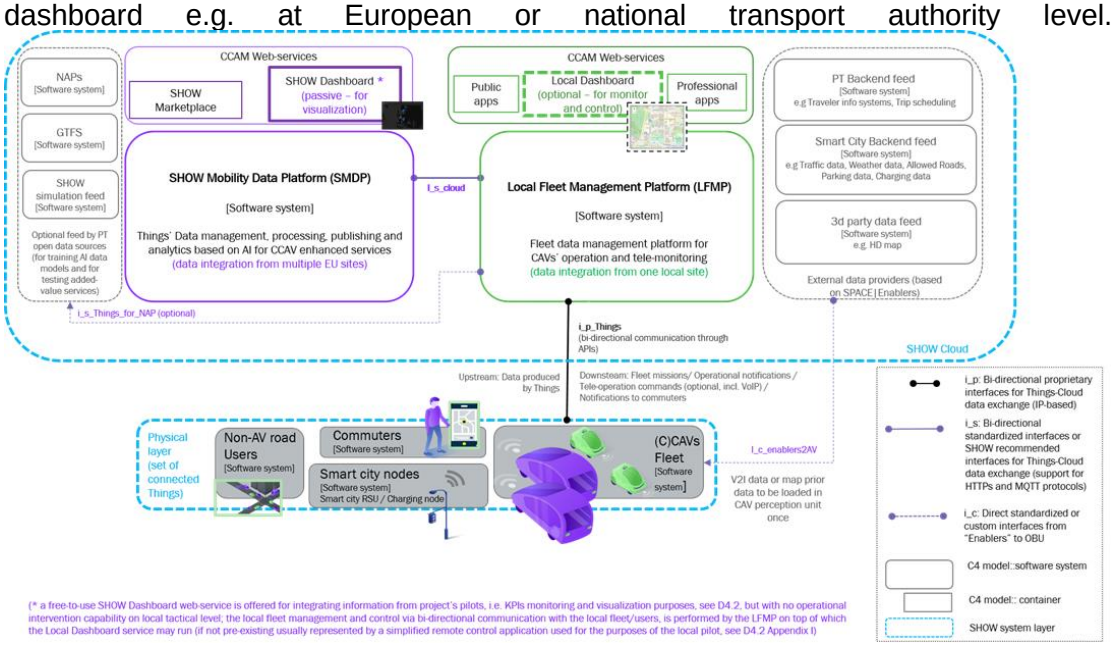

Figure 14: SHOW reference dashboard service and LFMP (demo site) dashboard service roles in the SHOW reference architecture (better viewed in zoom-in mode).

4.4.2 Discussion on multiple data ingestion platforms for services provision

For the creation of the SHOW functional architecture, two core design objectives have been considered and discussed:

a. The design of the SHOW service-oriented modular integrated system which supports efficient integration with existing local autonomous transportation systems, PT backend systems any other external data providers present in all SHOW demonstration sites, **represented by architecture variations I and II below**.

b. The design of a future-proof modular service-oriented "reference" architecture for EU-wide CCAM services' provision, **represented by architecture variations II and III**. Aspects of open data access for safety-critical in vehicle applications have been identified and solutions discussed although not inside the SHOW direct focus.

Both include the SHOW cloud Mobility Data Platform (SMDP) as their central subsystem.

As it can be seen in the diagram of Figure 13, two interfaces among Things and the data ingestion cloud platforms have been foreseen, namely the I_p_Things and the I_s_Things towards the LFMP and the SMDP respectively. This is not currently the typical case in reality where CAVs' safety and cyber-security unresolved aspects as well as the industry competitiveness imposes restrictions on accessing the data generated by CAVs and hence typically the CAV fleet data ingestion on the cloud is the sole responsibility of the CAV owners or the assigned fleet operator (via the I_p_Things) using secure wireless connections to the cloud and proprietary APIs. However, as the set of Things considered in SHOW include other connected entities apart from the CAV fleet, we have also included the I_s_Things interface to serve all the direct connections of SHOW Things to the SHOW MDP (e.g. from a commuter smart device to SHOW MDP). It is also foreseen to possibly equip some of the CAVs with auxiliary smart devices in order to log SHOW extra data like passengers' count

when this is not part of the existing list of vehicular data offered by a SHOW autonomous shuttle. In that case the I_s_Things interface will be used to connect to the SHOW MDP.

Depending on the availability of RT streaming data and the data integration path, three architecture variations are proposed:

- ***Variation - I***: Indirect access to THINGS' data, subset of data available via cloud- to cloud file transfers or ideally via pub/sub APIs (assumes an agreement with project CCAV data owners and operators); CCAVs non time critical services can be offered.
- ***Variation - II***: Both direct and indirect access to THINGS' data in multiple update rates via two data ingestion cloud platforms, namely the LFMP and SDMP cloud platforms respectively. CCAVs non time critical services can be offered.
- ***Variation - III***: (futuristic) Open data for equal access by service providers streamed real time via intermediary vendor-neutral server (CCAVs time critical services can be offered); NG AV on-board architecture is assumed that supports real-time communication from in-vehicle buses and ECUs. CCAVs time-critical services related to safety can be offered.

In all three variations the following considerations apply:

- The Things' data ingestion and data publisher is denoted as discrete layer (THINGS' abstraction) to unify various operations performed on raw data in modern cloud data sharing platforms like data normalization, filtering, anonymization, authentication e.t.c.
    - Support for various data feed rates e.g. per ms, secs, trip, day implies the support of IoT event-driven architectures
    - It is called "cloud" Things' abstraction to differentiate from the possibility of a similar layer located on the edge (of the physical layer), however in the future where 5G will be more widespread this could be indeed the case.
- *ALL nodes within the physical layer may be connected to the cloud via the I_p or I_s interfaces. Additionally, they are considered interconnected within the same layer they belong into, via short-range V2X ad-hoc networks. This is not depicted due to space limitation in the graph of Figure 13, but it becomes explicit in the functional views of Figure 15, Figure 16 and Figure 17 that follow. That includes* a physical V2G interface provided for charging the electric CAVs.

Based on the architecture abstraction of the diagram in Figure 13, the next objective is to fill in each Software system depicted there with functional components and identify the core relevant interfaces among layers and among the SHOW subsystems. Each variation defines its own solution for data integration with the SHOW central cloud platform and will be described in more detail in the three subsections that follow.

4.4.3 SHOW architecture - Variation I (CCAVs data ingestion cloud platform privately owned)

Data Flow Description: Things data are fed into privately owned local fleet management platform where they are processed for CCAV service provision and KPIs computation and visualization. Then, via a cloud-to-cloud standardized interface (I_s_cloud), a specific subset of Things' data is transmitted to the SHOW platform and then to SHOW Dashboard for centralized KPIs visualization and CCAV enhanced services' provision (Figure 15).

Applicability: CCAVs services deployment based on peer-to-peer agreements between CAVs' owners, CCAV operators and 3d party service providers.

Graph accompanying technical notes:

1. OEMs will provide via **I_s** to SHOW DMP minimum set of raw data needed for KPI computation, KPIs and additional raw data based on wp5-6 request (for enhanced CCAV services provision);
2. DMP Database includes static data, dynamic data and meta-data and will be stored using MongoDB as described in D5.1 [19];
3. Historical data retrieval from SHOW components or 3d party apps/ services will be possible from the SHOW DMP as described in D5.1 (DMP publisher);
4. Open data sources like NAP data could be retrieved and used for offline training of DMP AI algorithms for enhanced CCAV services;
5. Support for real time streaming is not offered;
6. Cloud to app communication is also included (tele-operation, on-board updates) as part of the local FMP default functionality;

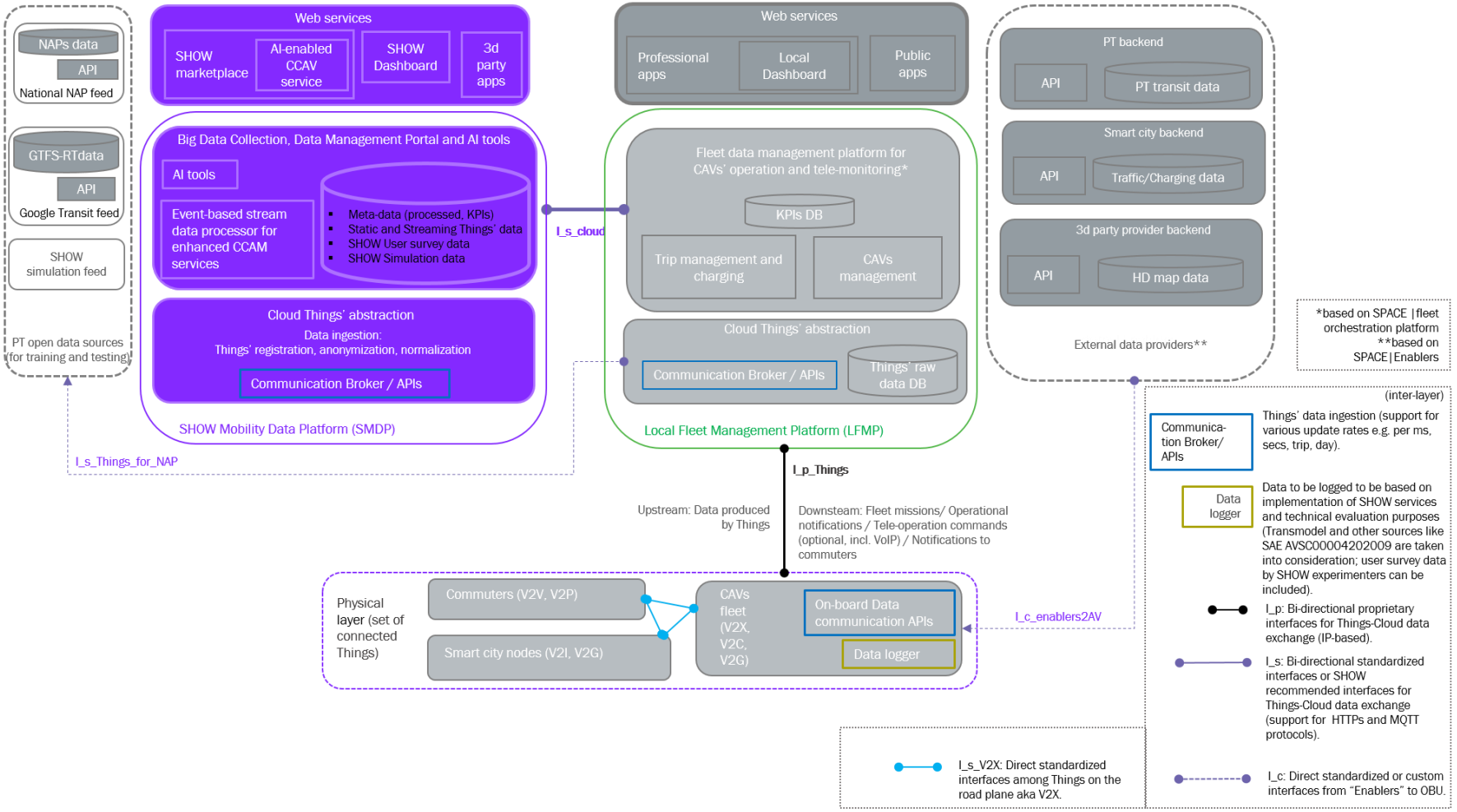

Figure 15: System functional view: Variation I.

4.4.4 SHOW architecture - Variation II (multiple data ingestion cloud platforms)

Data Flow Description: Things data are fed into proprietary local fleet management platform where they are processed for CCAV service provision and KPIs computation and visualization. In parallel, a specific subset of THINGS'' data are transmitted to the SHOW platform and Dashboard for centralized KPIs visualization and CCAV enhanced services' provision (Figure 16).

Applicability: CCAVs services deployment based on peer to peer agreements between CAVs' owners, CCAV operators and 3^{d} party service providers.

Graph accompanying technical notes:

*Note 1: Mobility data available from smart devices installed on-board (smart tablet for provision of info on passengers) will be directly transferred to SDMP via **I_s_Things** (e.g. trip data, kinematic data measured by smart devices sensors); This interface can be also used by experimental SHOW vehicles where SHOW on-board APIs can be implemented for CAV raw data real time access.*

Note 2: Data ingestion and publishing layer should follow an event-driven architecture that supports real time streaming of data. Similarly, to the Google Cloud Platform, it would offers Pub/Sub as an asynchronous messaging service that decouples services that produce events from services that process events. Basically, this allows the creation of topics and subscription channels without worrying about the data center infrastructure needed for storage and distribution. Communication can be one-to-many (fan-out), many-to-one (fan-in), and many-to-many. SHOW's approach on such a data ingestion mechanism and big data portal platform (using Kafka, CKAN and MongoDB) is described in D5.1 [19].

Using the "SHOW SDK" one can build the clients for the publication and consumption of subscriptions, counting on a native integration with the rest of the services of the SHOW platform, which evidently increases the potential of our system under the streaming model.

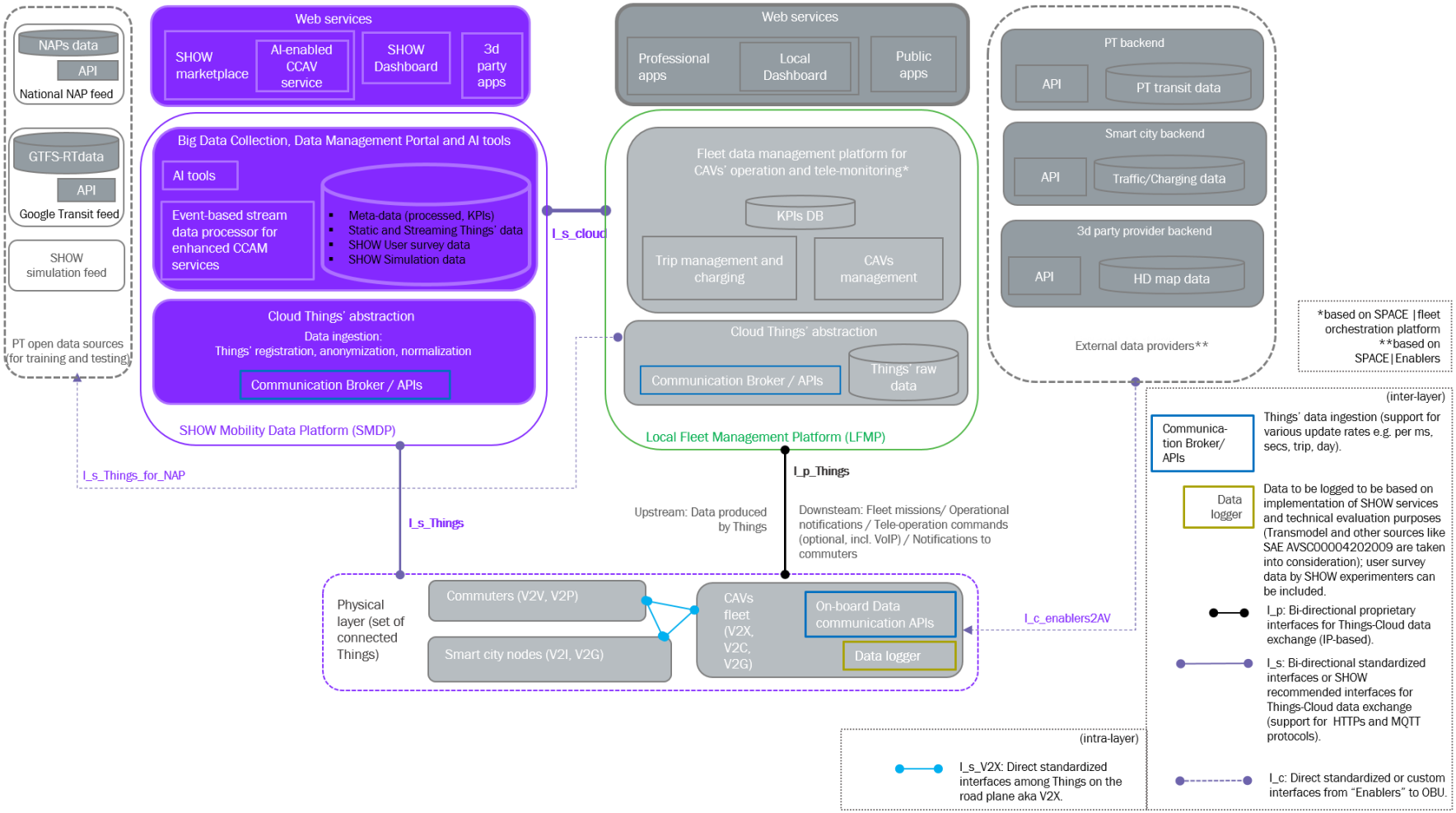

Figure 16: System functional view: Variation II.

4.4.5 SHOW architecture - Variation III (multiple data ingestion cloud platforms plus shared data ingestion platform for open real-time data publication)

Intro: SHOW MDP may be seen as an EU-wide platform for CCAM services of the future, promoting cross-border interoperability based on PT and CCAV data integration and hosting. Towards the vision of an open vehicular streaming data analytics platform for promoting safety-related services provision, a third future-oriented variation, at the edge of the SHOW demonstration objectives, has been negotiated and approved by WP4 team as a valuable addition in SHOW reference architecture. This variation assumes adopting an equal data access approach for 3rd party service providers (similar to B2B approach) on both national- and EU- level for an agreed minimum set of CAV data. It also assumes, that in few years from now the next generation of CAV on-board platforms will replace the current automotive in-vehicle platforms towards a new secure in-vehicle platform offering high computing and real time communications capabilities not only inside the vehicle but also to the external edge or cloud. The bespoke design considerations have taken into account the EU regulation "National Access Points (NAPs) for the provision of EU-wide real-time traffic information services"[21] which applies from 13 July 2017 as well as recent information about the undergoing ITS directive update (source: Data4PT first stakeholders' workshop[22]).

Data Flow Description: Data ingestion is conditionally decoupled from the local proprietary fleet orchestration platform and replaced by an open vehicular data platform for promoting open access of safety critical data that can be used by 3rd party service providers on EU-wide level and beyond (Figure 17). In parallel, the local fleet management platform (where data are processed for CCAV operational service provision and KPIs computation and visualization) may be fed directly with Things data via the I_p_Things interface or subscribe to the open platform to get data safety-critical data updates via the I_s_Things interface.

Applicability: Safety critical CCAVs services deployment based on minimum set of shared CCAV data on European union-wide scale.

Graph accompanying technical notes:

Note 1: This is in alignment with EU undergoing ITS-directive update and especially the part promoting NAPs for PT and beyond. A high level Data Task Force has been set up, designed to improve road safety by sharing data generated by vehicles and infrastructure between countries and manufacturers. A 12-month proof of concept started in June 2019. In 2020 WG NAP will carry out research on how the data sets that are published in the NAPs can be accessed and used, from both the publisher and consumer perspectives. The findings of this exercise will be shared in the upcoming Annual NAP Report.

Note 2: Data ingestion and publishing layer should follow an event-driven architecture that supports real time streaming of data. Similar to the Google Cloud Platform, it would offer Pub/Sub as an asynchronous messaging service that decouples services that produce events from services that process events. Basically, this allows the creation of topics and subscription channels without worrying about the data centre infrastructure needed for storage and distribution. Communication can be one-to-many

[21] "NAP for RTTI". Delegated Regulation (EU) 2015/962, was adopted in 2015; it applies from 13 July 2017.
[22] https://data4pt-project.eu/data4pt-first-stakeholders-workshop-5-november-2020/

(fan-out), many-to-one (fan-in), and many-to-many. SHOW approach on data ingestion mechanism and big data portal platform implementation is described in D5.1.

Note 3: Today's AVs' on-board architecture is a synthesis of a complex network of sensors and ECUs focused on autonomy and giving little room for connected features which are now allowed only for specific purposes not usually connected to the driving task and hence not optimized for the concept of the vehicle as a mobile sensor. Next Generation CAV on-board architecture is expected to support real time streaming of vehicle generated data in a secure and efficient way that does not affect the AVs' internal communication channels (an isolation-supported and security & privacy-preserved vehicle operation system).

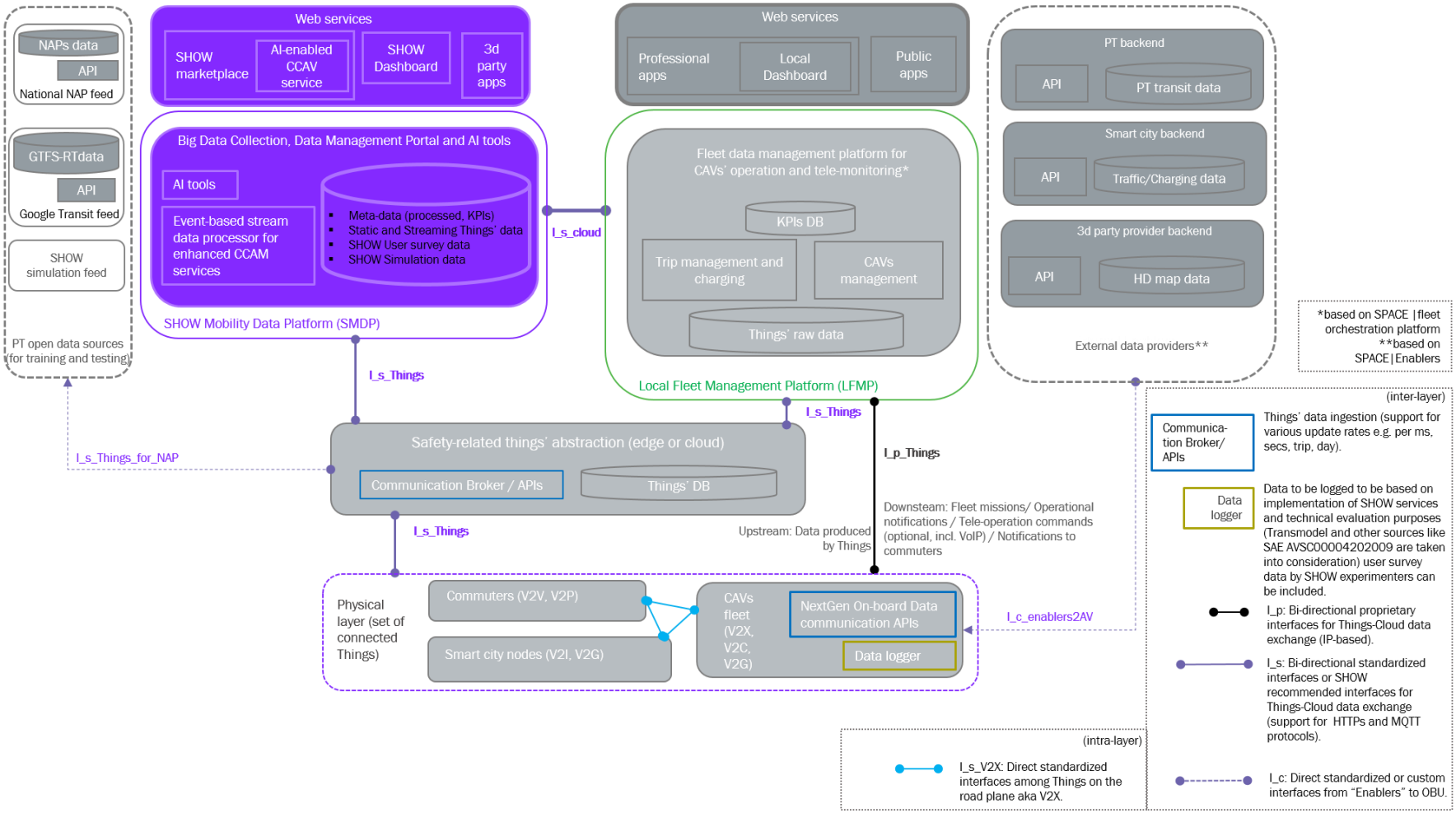

Figure 17: System functional view: Variation III.

4.4.6 Types of data to be exchanged for SHOW services

The groups, the data types and the analysis of their definition are presented in Section 5 of D5.1 [19]In this procedure, Use Cases, KPIs, data for Dashboard, services, data list from other partners and relevant research from other projects, such as AVENUE [37] and nIoVe [39], were taken into account. The whole data list is and will remain aligned with Transmodel in order to keep a common data format for all the pilot sites and partners. More details for the criteria of Transmodel's choice and for its components are included in the Section 4 of D5.1 [19].

In summary, the data groups and types are clustered in the following classes:

- **Static Data** that include all the features of the fleet which will be useful in a variety of activities and they remain constant.
  Such data variables are: Name, Manufacturer, Vehicle Type, Model, Seating capacity, Standing capacity, Energy Type, Vehicle function, Special place capacity, Push chair capacity, Wheelchair capacity, Max Payload.
- Dynamic Data that describe information that, by its nature, is varying with time. The frequency of the change depends on each data type. The main source of dynamic data are the vehicles' sensors.
  Dynamic data variables includes: Connection Status, Location, Door Status, Energy level, Odometer, State of Charge, Speed, Occupancy, Payload, Prams on board, Wheelchair on board, Passengers with special needs, Dispatch status, Orientation, Heading, Acceleration, Navigation Mode, GNSS connection, Communication protocol, Signal strength, Bandwidth, Latency, Operating Mode, CO2 emissions, Energy consumption, Travelled kilometres, Traffic in Vehicle's route.
- Traffic situation and its behaviour is a very challenging issue. There are many reasons which could affect the time of arrival of a vehicle, the best route from one place to another and so on. In order to achieve better supervision and prediction of the traffic situation, we define **Event-based data which** includes: Event, Type of event, Located event, Situation, Situation cause, Situation Reason, Incident, Alarm, Emergency notification time, Emergency notification location, Vehicle is driving in reverse, Vehicle is braking, Break light, Strong braking, Severe braking, Shuttle switched to manual mode, DUI: klaxon triggered, DUI: buzzer triggered
- Service data include all the information about the standard movements of a Public Transport vehicle. We integrated data types which can justify any deviation.
  Service data are: Stop places, Routes, Lines, Service area, Passing time, Delay, Timetable planned, Timetable actual, Operating Day, Day Type
- Taking into account that a crucial part of the project is DRT services, we create a data group with all the appropriate data types for this application.
  Booking/ride data: Load, Vehicle availability, Desired pickup location, Desired pickup time, Desired drop off location, Desired drop off time, Planned pickup location, Planned pickup time, Planned drop off location, Plan ned drop off time, Actual pickup location, Actual pickup time, Actual drop off location, Actual drop off time, Planned booking route, Actual booking route, Direct ride distance, Direct ride duration, Actual ride distance, Actual ride duration, Trip reason, Passenger Location, Passenger Destination, Timestamp.
- The data which originates from third parties is grouped in External data class.
  Externa data includes: Temperature, Feels like, Min Temperature, Max Temperature, Pressure, Humidity, Wind deg, Wind speed, Weather main, Weather description, City traffic, Maps, Noise levels, Parking, Parking Bay, Parking capacity, Parking Properties

- An important source of data is the given infrastructure that each pilot site supports. The infrastructure data also include information which originates from elements of the vehicles, except the sensors, as cameras.
  Infrastructure data includes: Internal temperature, Video-internal cameras, Video-external cameras, Magnetic loops, Lidar Sensor, Radar Sensor, Camera installed on traffic lights or bridge, Radio frequency sensor, Sensors for capturing wireless internet traffic, Vehicle traffic camera.
- Finally, we define a cluster of Other data that will prove to be useful but they cannot be sorted in the other groups.
  Other data may include: Bluetooth Sensor data, Network traffic metadata, Simulation data.

A note that must be taken into account is that some of these data types are personalized. Therefore, they demand special care according to Privacy Policy which is described in D5.1 [19]. Data which can be considered as personal are Booking/ride data, data from the internal and external cameras, Network traffic data, Bluetooth sensor data, Wheelchair on board and Passengers with special needs captured data. Network traffic data include Username, Password, IP address, MAC address, session and, maybe, cookies. These data and their management must be compatible with the GDPR regulation.

In chapter 6, as an exercise, the exact data required for two SHOW services' deployment is presented.

4.4.7 SHOW Demo sites subsystems and actors (current picture)

A summary of the local system actors including V2X infra nodes, the local cloud components per site and the user apps to be deployed (based on the SP2 Architects' TF interviews, project's horizontal data super spreadsheet, A7.5 material and D9.2) is provided in Table 48 of the Appendix III (*Note: Although this information is considered important, the table is placed in the appendix due to its size*).

4.5 System Layers functional view

4.5.1 On-board CAV architecture

A generic functional architecture of a CAV on-board platform is represented in the diagram of Figure 18: On the right side of the diagram, there is the mechanical chassis which enables the CAV to drive, brake, steer and the Car Body with the interior equipment to welcome passengers. On the left side of the diagram, there is the HW and SW needed to pilot the CAV which is here called "Virtual Driver". The virtual driver is composed of all the basic systems needed in a CAV: perception, localization systems, Obstacle detection and the decision and control systems. The virtual driver takes into account the apriori information given by MAPS (mapping of the site) and combines it with the online GNSS position (GNSS antenna communicating with base GNSS station). The HMI System enables displaying messages on the Driver User Interface from the CAV platform and also messages coming from the cloud through the Remote Communication System.

Intra-layer communications: The ECUs communicate mainly via CAN. The protocol used on the CAN device is extended, and there are 2 to 3 CAN channels with different frequencies for the CAN messages (BaudRate = 250 kb/s and 500 kb / s)

Bi-directional data exchanges between the CAV and other entities

The data that are typically being transferred from the CAV to the OEM cloud (in SHOW integrated with LFMP) via private wireless connection include:

- Events (when they occur)
- Telemetry (frequency :1 Hz)
- (Optionally) Views from the perception sensors (radar and lidar)
- Calls and video calls (when needed)

Communication from the CAV to infrastructure nodes or other AVs in the neighbourhood include:

- The traffic lights that communicate with the Virtual Driver via V2X.
- It is also possible to communicate with other AVs (V2V) but the technology is not yet developed in all shuttles.

NOTE 1: In SHOW, all the technologies described in sec. 2.3 (C-ITS Connectivity relevant aspects) are relevant to the CAVs fleet, but not always developed yet.

NOTE 2: As part of SHOW A7.3 optimised on-board HMIs for operator-less operations to improve passenger comfort and safety feeling will be studied.

NOTE 2: As part of SHOW A7.4, handovers between the L4 CCAV and the remote supervisor/controller will be studied in case of an automation abort situation. Specifically, the type of information that needs to be communicated to the driver or remote operator in each case, the timing and the mode of communication of the information, to enable smooth operation, avoid errors and enhance safety. External systems involved from Figure 18: Remote support system / Supervision system.

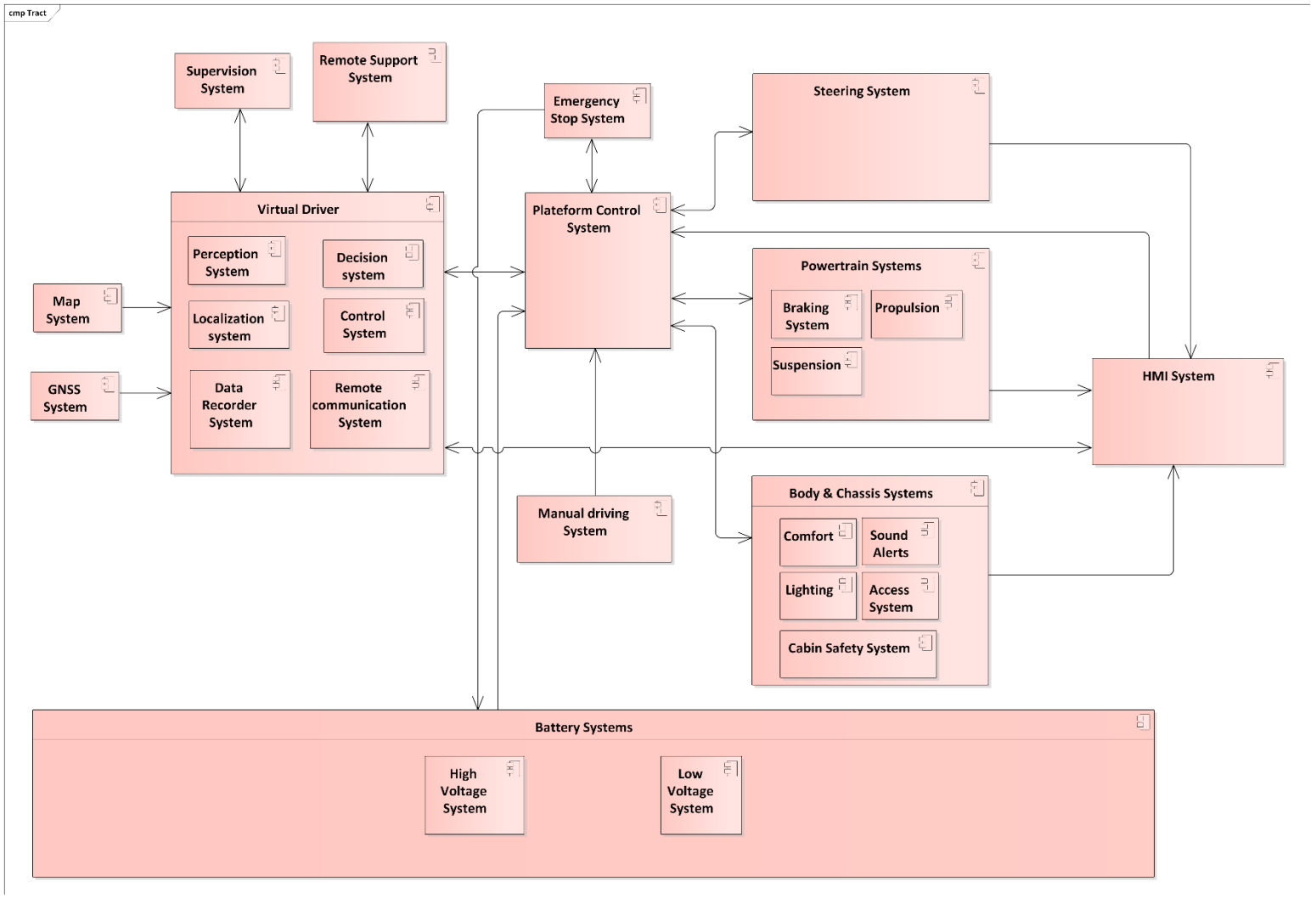

Figure 18: SHOW CAV generic functional on-board architecture.

4.5.2 SMDP Cloud server architecture

As the SHOW project constitutes the first EU-wide piloting effort focusing on CCAM services continuous operation deployment built on top of local C-ITS and fleet management systems, the data to be handled by the SHOW DPMP are classified as Big data. Similar to the Google Cloud Platform, the SHOW DPMP offers Pub/Sub as an asynchronous messaging service that decouples services that produce events from services that process events. Basically, this allows the creation of topics and subscription channels without worrying about the data centre infrastructure needed for storage and distribution. Communication can be one-to-many (fan-out), many-to-one (fan-in), and many-to-many. SHOW's approach on such a data ingestion mechanism regarding its Big Data Collection platform and Data Management Portal (using Kafka Spark, CKAN[23] and MongoDB is detailed in D5.1 [19]. A high level overview of the data collection and management mechanism of the DPMP system includes sub-components such as the Data Manager Portal that handles both the real time streams of processed data through Kafka and the asynchronous data publishing through the CKAN open data portal. It also includes the Data Collector Platform that is responsible for retrieving, processing, and saving data received from multiple sources, as well as the Big Data & AI toolboxes that handle the further data processing and inferencing mechanisms. The intra-layer SHOW DPMP architecture is part of the cloud infrastructure that will receive and store data and provide the applications and dashboards with data. As an extract from D5.1, the intra-layer SHOW DPMP architecture can be found in Figure 19. This figure visualizes the components of DPMP and their technical connection with the rest of the SHOW services. More information about the back-end are available in SHOW D5.1 subsection 3.2.

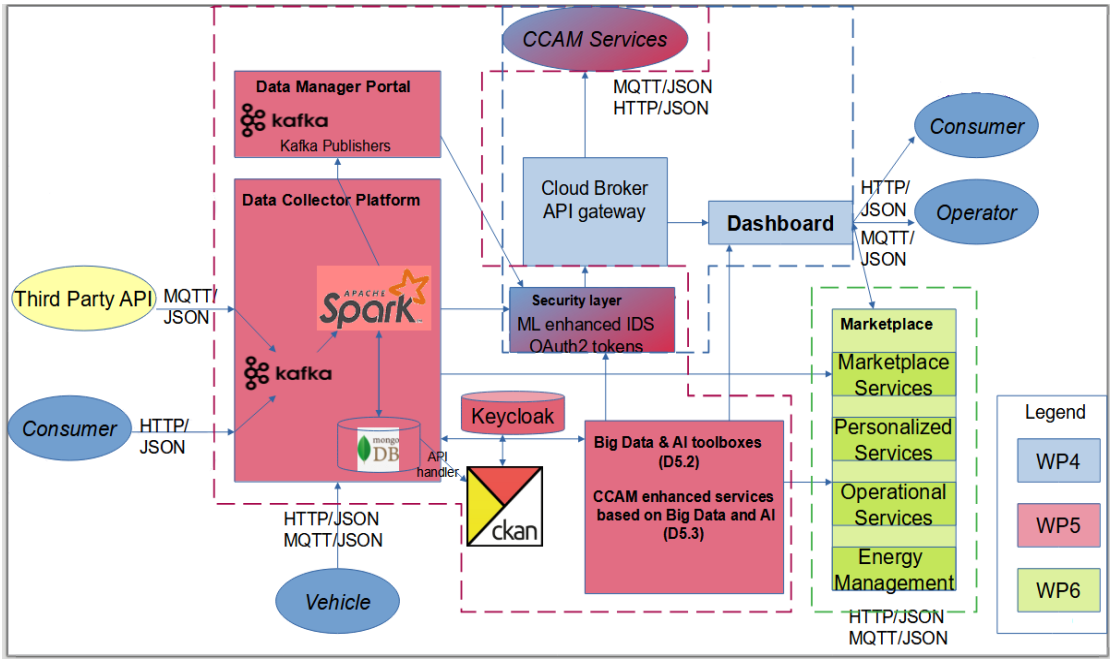

Figure 19: Inter-component relations of Data Portal and Big Data collection platform and their connection to SHOW web-services (source D5.1 [14]).

[23] CKAN is a powerful data management system that makes data accessible – by providing tools to streamline publishing, sharing, finding and using data.

Using the “SHOW SDK” one can build the clients for the publication and consumption of subscriptions, counting on a native integration with the rest of the services of the SHOW platform.

4.6 Cross-layer mechanisms for interoperability, cyber security and data communication

The main use of the proposed system architecture is i) the subsequent SHOW system integration work including the cloud to cloud communication between LFMP and SMDP. ii) the ongoing SMDP and SHOW services implementation. Both tasks heavily rely on agreed communication APIs and data models, maximizing the use of open and standardized interfaces and assuring cyber security which remains a critical aspect for the CCAV integration success especially for PT where services are addressing a mass audience.

4.6.1.1 On web communication protocols

Based on D5.1, the protocol for communication among the variety of components in SHOW MDP could be either HyperText Transfer Protocol (HTTP) or Message Queuing Telemetry Transport (MQTT), depending on the task. Both these protocols usually run over TCP/IP and can consume JSON formatted APIs. The HTTP client – server protocol is the basis on which RESTful APIs [79] are developed, which, although not obligatory, are usually the norm for Web of Things (WoT) applications [80]. The basic functions for persistent storage are Create, Read, Update, Delete (CRUD), or POST, GET, PUT, DELETE in this case. RESTful architecture is best utilized for implementing the services. On the other hand, the MQTT publish – subscribe model is an important tool [82], [83] for inter-component communication, as message exchange is applied when necessary. This helps improve efficiency considering energy, bandwidth and data usage. A message broker is needed for this function, in order to retain, store and forward messages to clients subscribed to specific topics [81]. Regarding security, OAuth2.0 is a very important tool designed to work with HTTP scheme [84] and MQTT relies on SSL/TLS for transport security [85]. SHOW D5.1 Appendix IV contains a comparison table of MQTT and REST APIs technical differences.

4.6.1.2 Notes on Local fleet management platform integration

For data exchange between the LFMP (when present) and the SDMP, the following mechanisms are foreseen:

- ad-hoc file transfer e.g. sharing the corresponding data as CSV/XLS data on frequent basis. [appropriate for historic data recordings]
- asynchronous message queuing (pub/sub) model via cloud Broker/APIs for sharing streams of AV data (such as AV current speed and location), appropriate for real-time data updates – see D5.1 [19] and chapter 5.

4.6.1.3 On Cyber-security aspects

SHOW is a multi-type, multi-tier connected THINGS’ system depending on many external actors (treated as black boxes from the SHOW architecture viewpoint). Although cyber security remains a transversal non-functional requirement applying equally to all layers of a WoTs ecosystem, the focus of security work will be mainly cast on the secure cloud platform side. In the SHOW platform, the data ingestion layer is a core component responsible for data normalization, de-identification and storage. As part of an all-IP based platform, SHOW allows the support of different types of application protocols popular in the internet world which already handle cybersecurity by design (e.g. HTTP(S)). A set of security features such as secure channel protocols,

access control and secure storage are considered and their preliminary specification has been included in D5.1 [19].

4.6.1.3.1 SMDP Cyber security aspects

In D5.1 section 6.4, (*Big Data Collection Platform and Data Management Portal*) [19], a set of basic Cyber Security mechanisms to be implemented (currently in demo stage) for the SHOW Data Portal are described. Cyber Security is not only to protect the system from suspicious users and attacks but also to have full control of the system, real-time monitoring and effective incident response. SHOW offers Privileged Access to resources with the use of roles but also restrict network access with the use of firewalls and Defence in Depth strategy. SHOW project uses OAUTH2 protocol for user authentication and user authorization. In order to fulfil these necessities, SHOW makes use of Google Cloud and Cloudflare Services for network monitoring, incident response, and virtual firewalls and metrics visualization. Cloudflare is also used for DDos protection and mitigation. Keycloak software is used for OAUTH2 and for Privileged Access Management to resources along with the features of CKAN DMP which are related to organizations and roles. Finally, to establish SSL/Secure connection a certificate and a private key were created with Python. In the next stage SHOW will deliver an Intrusion Detection System based on Machine Learning, Deep Learning and A.I. techniques.

4.6.1.3.2 LFMP Cyber security aspects

Although LFMP is treated as “black-box” from the SHOW implementation perspective, cybersecurity & data protection measures taken by Bestmile around its platform are provided hereafter as a baseline.

- Access to the Dashboard:
    - The Dashboard supports a role-based access control. Upon login to the platform, the API Gateway generates a short validity access token that is then used in every call to the platform to enable access to dedicated functionalities.
    - The communication is protected by HTTPS
- Access to Booking APIs:
    - The booking API is a standard REST API, secured by API key and SSL (HTTPS).
    - A different API Key is provided to each operator (Operator segmented). This API key is embedded in the applications and protected by the HTTPS connection. It authenticates the Operator. This API key can be managed by the operator (e.g. revoked if compromised). Secure storage and handling of this API key is the responsibility of the operator.
- 2-way communication with the vehicles:
    - A cloud to cloud connection between Bestmile and the OEM is secured by API key and SSL (HTTPS). Security mechanisms for this connection are under the responsibility of the OEM, Bestmile complies with the best practices requested by each OEM.
    - Mission management is not sending any safety-critical information to the vehicle. It only specifies a destination and route; path planning remains the responsibility of the automatic driving functionality of the vehicle.
- Data protection:

- The platform shall limit to the minimum the personal information collected, shall anonymize it whenever possible, and shall conform to GDPR rules.
    - Traveller data is managed between the Public Transport Operators and the Traveller App.
    - Traveller sensitive data is not shared with Bestmile in the platform: only anonymized user IDs are transmitted.

4.6.1.4 On data models for interoperability

Securing interoperability of SHOW architecture with CEN TC278 WG3/ITxPT implies introducing CAVs also in this context. Public Transport is quite advanced regarding standards adoption as this is key for day-to-day operation considering that Public Transport vehicles fleets are heterogeneous (multi-brand / multi-model / multi-energy), equipped with multiple IT systems from various IT suppliers and operated in multiple stakeholders' context (multi Public Transport Operator and Public Transport Authorities).

SHOW promoted data models for Urban C-ITS generated data in SHOW PT scenarios include Transmodel and SHOW custom data structures based on [89]. See D5.1-chapter 4 [19].

5 Functional preview of the SHOW Dashboard: SHOW operational Dashboard

This section describes in high level the SHOW Dashboard service. Further details of this service (and its discrete role from a potentially existing local site Dashboard service)are provided in D4.2.

5.1 Service descriptions

SHOW Dashboard service (Figure 13 – SHOW CCAV web services' layer) is based on Ericsson's Innovation Cloud platform, with container and micro service architecture. The service is designed to visualize in real time / near-real time SHOW vehicle operations at all connected demo sites up to availability of the data from the sites. The information in the Dashboard include project's defined KPIs, as can be derived from the following elementary data (though the final list of elements to be visualized is not yet determined):

- Vehicle related information
  - Vehicle profiles: Technical specification of vehicle
  - Operation modes: Manual/Automated Driving/Idle
  - Energy usage: Fuel or battery status
  - Passenger load: Number of passengers on board (upon data availability)
  - Geo-position (geospatial data-based rule engines)
  - Connectivity
- Trip related information (upon data availability)
  - Timetable (AV and/or PT)
  - Origin, destination, stops
  - Route segment
- Other KPIs (Energy, safety, service quality from surveys)

5.2 List of functionalities/features

- Provision of SHOW automated vehicles, assets, actors and relationships
- Collect and visualize real-time, near real-time data from vehicles and connected traffic infrastructure objects
- Analyze telemetry messages and trigger alarms
- Workflow with life-cycle events
- Data visualization: Dashboard with multiple views per actor roles to illustrate the real-time operations of AVs and project KPIs. This includes map-based real-time view of SHOW's vehicle positions (upon integration and data availability).
- Data collectors: Realtime telemetry, REST messages and batch data collection
- Data API for external systems
- Dashboard customization ability (only for the developer team).

5.3 Architecture review

5.3.1 Interfaces and system context

SHOW Dashboard will have the following interfaces to external systems (with regards to this component):

- Input data API interfaces: Collect site raw and aggregated data from SHOW's DMP platform with the following protocols:

    - HTTP/TLS
    - MQTT
    - Other messaging protocols
- Output data API interfaces: The Dashboard can establish API's to make Dashboard related information (e.g. geospatial queries) available for external access via REST, with regards to the data security requirements.

Figure 20 depicts the SHOW Dashboard in system context. The SHOW Dashboard collects its KPI data (both realtime and historical) from the central DMP, facilitated by the input API interfaces. The interface can also be used to collect additional data from third party systems (e.g. Smart city systems that provide traffic situations, weather, network statuses etc. that can later be visualized in Dashboard map). In a special situation where direct connection to local Dashboard(s) at sites is required, this interface can also be re-used with the same mechanism to collect KPI related data.

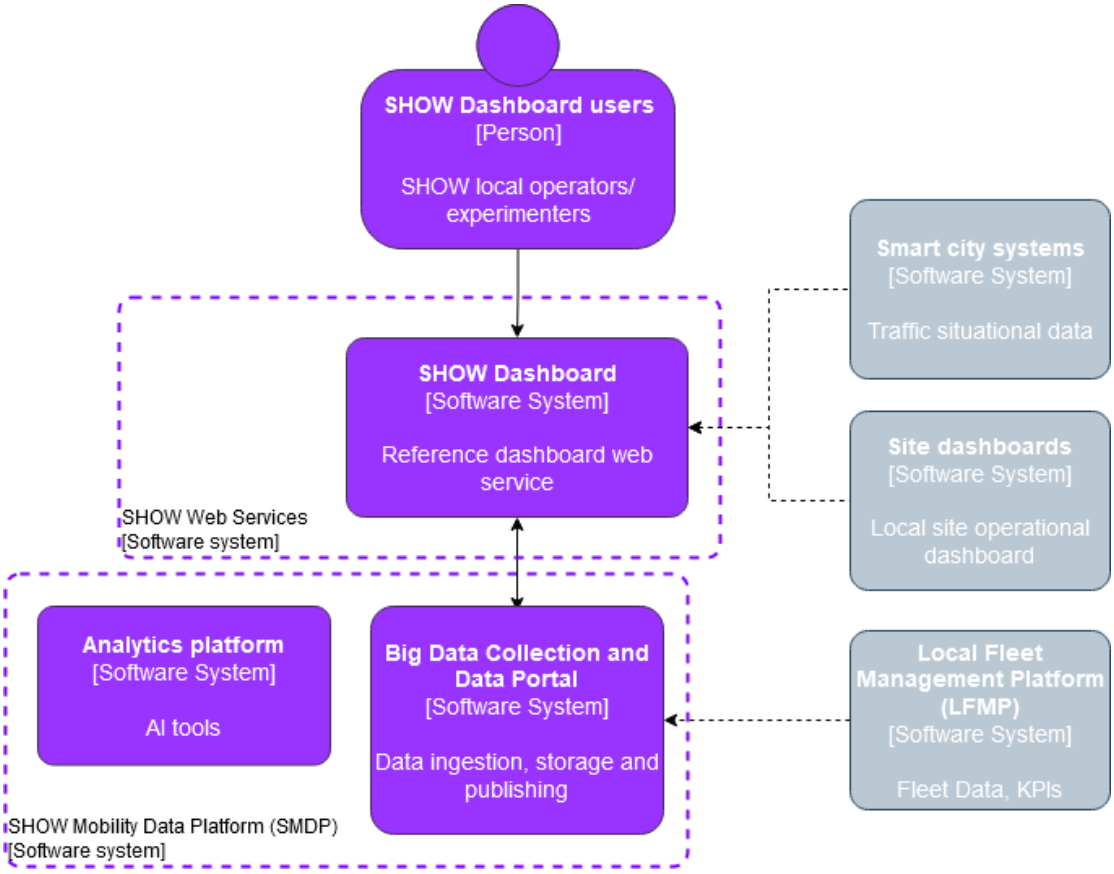

Figure 20: Show Dashboard component and its interfaces to external components/systems

5.3.2 Component diagram

The C4 component diagram of SHOW Dashboard is illustrated Figure 21. The system interfaces to external systems via Data sink and Data source layers. The API Server and API Manager components will manage all the data and other micro-service APIs. Telemetry Data Processor/Server are the components to perform real-time assessments of telemetry data collected from the vehicles with pre-defined rules, this component will generate real-time alerts (e.g. Geo-fencing violations).

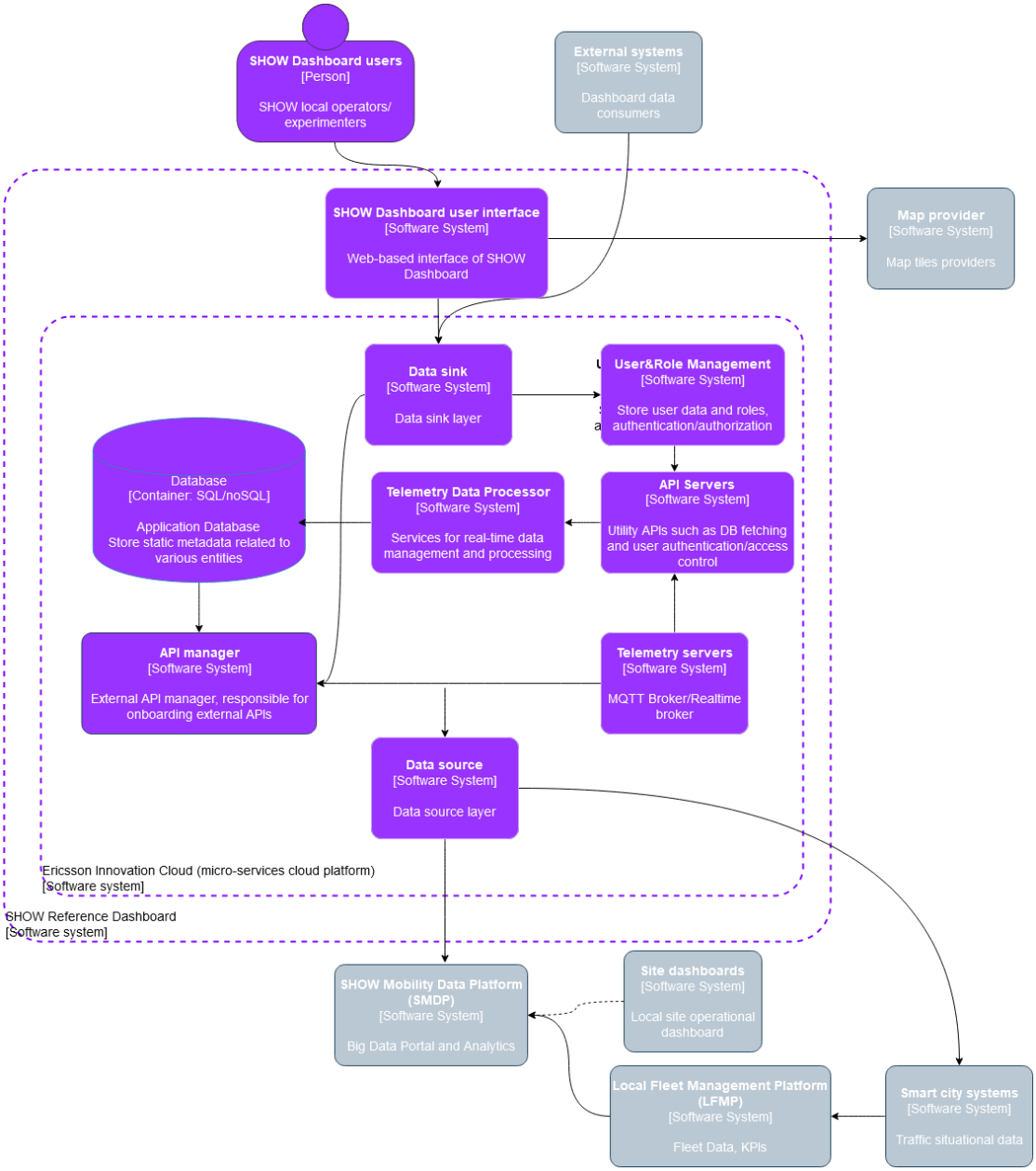

Figure 21: SHOW Dashboard architecture diagram (Component level)

5.3.3 Component descriptions

The descriptions of interconnected components in Figure 21 are provided below in Table 14. SHOW Dashboard is built on top of the Ericsson Innovation Cloud technology, leveraging its components and utilities and micro-service architecture. The components are interconnected via internal API interfaces.

Table 14: Component Descriptions.

Component	Description
SHOW Dashboard user interface	Web-based Dashboard interface to user with SHOW's KPI gadgets including map-based multi-layer real-time visualization of vehicle/fleet geospatial positions. Each layer represents a specific group of objects to be visualized on the map gadget. Depending on the integration and data availability, traffic situations can also be configured as a layer.
Data sink	Broker/gateway service to communicate with Dashboard user interface and Dashboard external data API for external parties to access the geospatial KPIs upon some security schemes. The data-sink services rely on the User & Role Management and API Manager for supporting secure access to the API data.
Data source	Broker/gateway service to facilitate communication with data sources e.g. SHOW DMP cloud platform, optional vehicles/sites/IoT devices in both synchronous (HTTP/TLS) and asynchronous (MQTT) modes, and possibly conversion between these modes. This component can facilitate both raw and aggregated data from sites for KPI's via SMDP- Big Data Collector and Data Portal.
Application Database	Scalable and secure storage to store all required data needed for SHOW Dashboard, diverse data types, e.g. detailed vehicle data (metadata and payloads) and KPI data retrieved from SMDP. This database stores the snapshot of data for visualization and real-time computations. Historical data is retrieved from SMDP- Big Data Collector and Data Portal via API interface.
Telemetry Data Processor	Application micro-service to facilitate transformation and broadcast of real-time messages (MQTT based payloads) into a format that is accessible and usable in the different micro-services deployed as a part of SHOW Dashboard Application.
Telemetry Server	Internal Application Server to facilitate the exchange of telemetry data between DMP with the SHOW Dashboard micro-services. This can also be connected with third party data source systems. Examples include a traffic-system sharing traffic notifications to the SHOW Dashboard directly, using the Telemetry Server as the single point of contact to SHOW Dashboard.
API Manager	Internal API management tools that help developers to on-board new API (Swagger specification), govern API usage, deploy and coordinate API lifecycle, and additionally allow users to access site KPI / geospatial data onboarded on the API Manager. This application allows creation of 'data-subscription' workflows for users to easily connect to for fetching data out of the SHOW Dashboard.
API Server	An internal API gateway/broker server that receive/orchestrate API requests, enforces security policies, route requests to the related services and handle responses to requesters.
User & Role Management	Keep and maintain user profiles. Access to different resources is based on role-based privileges. The anticipated roles and users will be in sync with the SHOW Cloud platform if possible. Users will be grouped by sites, partners, OEM, and project team role.

5.3.4 Data Source interfaces

The mappings between data source systems and the suggested Dashboard integration interfaces are provided in the below Table 15.

Table 15: Data sources interfaces

Interface	Source system	Description
Vehicle/IoT telemetry	DMP, Vehicle cloud	MQTT interface <fleet-id>/<vehicle-id>/<DMP-attribute>
Map	Map provider such as Mapbox	Map tiles, map objects (traffic road network…)
Traffic situation	Smart city systems	Weather, traffic situation (roadworks, accidents…)
Trip information	DMP, Operator fleet management	REST API
KPI information	DMP, Site dashboards	REST API

5.4 SHOW Dashboard integration and development

The status of the local Dashboards at pilot sites as well as the data interfaces is depicted in Table 16 and Table 17 for all SHOW demo sites. It is observed that amongst the 16 SHOW demo cities various approaches exist depending on the maturity of the existing LFMP subsystems and their planning with respect to exchanging data other than the precomputed KPIs to the SHOW DMP.

Table 16: Local Dashboards VS. SHOW reference Dashboard current status (the Mega sites)

ID	The Mega Sites	City	Local dashboard status	TRL (1-9)	Beneficiary operating local dashboard	Dashboard URL, press release	Short description of key operations of the local dashboard	Readiness to connect to SHOW Dashboard	Remarks
1	France	Rouen	WIll build one	6	Transdev	Data depository to be defined	Fleet monitoring & fleet management	Will provide only pre-computed KPI	We will provide pre computed KPIs and some batch data on a regular basis (frequency TBC)
2	France	Rennes	Existing	N/A	Keolis	N/A	fleet monitoring & fleet management	Others, please describe in Remark column	We did not plan to get a dashboard outside the one(s) dedicated to fleet monitoring by the shuttles providers
3	Spain	Madrid	Using SHOW Dashboard	N/A	EMT, IRIZAR, TECNALIA	N/A	Fleet monitoring, route visualisation, KPIs for user (driver/passenger)	Others, please describe in Remark column	Madrid mega pilot site fleet/KPI data are still under investigation based on all types of considered vehicles, both real time and batch data integration for feeding the SHOW Dashboard are considered.
4	Austria	Graz	Using SHOW Dashboard	6	VIF, AVL	N/A	N/A	Will provide "near realtime" data	N/A
5	Austria	Salzburg	Using SHOW Dashboard	N/A	N/A	N/A	N/A	Others, please describe in Remark column	"The Salzburg Pilot is using the fleet management API “EZ-Fleet” provided by the OEM. Connection to the SHOW Dashboard is possible only under the following prerequisites: data sharing with SHOW cloud platform can be achieved either via OEM-private cloud (OEM to allow) or via SFRG cloud storage (OEM to agree) or directly via communication with the fleet (only if OEM recommends this for some reason). It was agreed that the Task Force clarifies the position of the OEM on how data can be shared for SHOW purposes."
6	Austria	Carinthia (pending Amendment)	Using SHOW Dashboard	6	n/a	n/a	Route visualisation	Will provide daily batch data	Will provide KPIs on a regular basis. The frequency is not clear yet. In the past, the operator provided a Dashboard only including route visualisation. Use of SHOW Dashboard must be clarified.

ID	The Mega Sites	City	Local dashboard status	TRL (1-9)	Beneficiary operating local dashboard	Dashboard URL, press release	Short description of key operations of the local dashboard	Readiness to connect to SHOW Dashboard	Remarks
7	Germany	Karlsruhe	Using SHOW Dashboard	N/A	FZI	-	aggregated/realtime KPIs will be provided via interfaces and can be used by WP4 to be presented in SHOW dashboard	Others, please describe in Remark column	Will provide KPIs on a regular basis. The frequency is not clear yet.
8	Germany	Braunschweig (pending amendment)	Others, please describe in the remark column	N/A	n.a.	n.a.	N/A	Will provide only pre-computed KPI	no local dashboard planned, connection to SHOW dashboard tbd
9	Germany	Aachen	Others, please describe in the remark column	N/A	n.a.	n.a.	N/A	Will provide "near realtime" data	no local dashboard planned, connection to SHOW dashboard tbd
10	Sweden	Linköping	Will build one	8	Transdev	SAFE	Fleet monitoring and limited teleoperation	Will provide "near realtime" data	N/A
11	Sweden	Kista	Using SHOW Dashboard	7	Keolis	N/A	N/A	Will provide "near realtime" data	The interface is based on a number of defined and agreed API's between SHOW Dashboard and the Public Transport provider. Keolis are using IT systems from Hogia. Message transfer is done by using MQTT as a mechanism. This is tested and working since early November 2020. The same data collector solution as deployed in Linköping site will be used for integration with SHOW Dashboard.

Table 17: Local Dashboards VS. SHOW reference Dashboard current status (the Satellite sites)

ID	The Satellites sites	City	Local dashboard status	TRL	Beneficiary operating local dashboard	URL, press release, description of local dashboard	Short description of key operations of the local dashboard	Readiness to connect to SHOW Dashboard	Remarks
12	Finland	Tampere	WIll build one	6	Sensible 4	N/A	Fleet monitoring, route visualisation, KPIs for traveler and vehicle efficiency	Others, please describe in Remark column	Will provide some of the KPIs pre-computed. APIs can be made available. Data to be exchanged to be confirmed. Possibility to utilise SHOW dashboard fully is studied.
13	Greece	Trikala	Using SHOW Dashboard	7	(e-Trikala)	N/A	"Local existing system is a local remote control center (no tele-operation): Parameterization and provision of known C-ITS services necessary for pilot operations. Remote control center operations are fleet real time monitoring as driver's view via screens and emergency breaking and immobilisation."	Will provide "near realtime" data	Data from the AVs are not identified yet. we will be possibly able to share close-to -real time data. Yet to be confirmed when the fleet arrives.
14	Netherlands	Eindhoven (Brainport)	Others, please describe in the remark column	1	N/A	N/A	N/A	Will provide only pre-computed KPI	The activity in Brainport concerns a technology demonstrator. No operational service will be deployed, therefor no use for a dashboard
15	Italy	Torino	Existing	9	Bestmile	Fleet Orchestration Platform Overview and Dashboard User Flow documents can be provided upon request in PDF format	"• Observe bookings, automated matching of rides and dispatching of trips, and manage exceptions • Visualize real-time service and vehicle information • Receive, create and edit field logs and incident reports • Design service areas, lines, timetables and frequencies • Set parameters for service constraints and objectives • Plan vehicle, fleet and driver availabilities • Provide traveler, vehicle and fleet efficiency KPIs "	Others, please describe in Remark column	Will provide some of the KPIs pre-computed, extracted on a monthly basis. APIs also available to connect directly with our backend platform. Data to be exchanged to be confirmed.

ID	The Satellites sites	City	Local dashboard status	TRL	Beneficiary operating local dashboard	URL, press release, description of local dashboard	Short description of key operations of the local dashboard	Readiness to connect to SHOW Dashboard	Remarks
16	Czech Republic	Brno	WIll build one	6	ARTIN	Currently under development	Fleet monitoring and fleet management and teleoperation	Will provide only pre-computed KPI	Will provide KPIs on a regular basis. The frequency will be determined later.

6 Additional deployment views: description of two added-value SHOW services design

This section presents how the SHOW functional architecture may be deployed for two of the SHOW envisioned advanced CCAM services and introduces the related data requirements that support those services' provision. This is an exercise that will help reviewing the D4.1 proposed architecture and bind it with the work in WP5 and WP6. For this purpose, the component diagrams and information flow diagrams for two selected services are derived based on the functional architecture – Variation II derived in chapter4. The two services are:

- **Service A: Estimated time of arrival**

  The most fundamental element for a real time bus information service for passengers is accurate Expected Time of Arrival (ETA) prediction. SHOW's real time prediction engine is based on multi-dimensional statistics that provide stable ETA prediction and addresses variables such as day, time of the day, route type, schedule type, dwell time, travel time, etc. ETA Data may be available through standard SIRI and GTFS Real Time formats.

- **Service B: Multimodal planner**
  Optimal routing for a vehicle or a fleet of vehicles. Multiple modes of route/trip selection for both Scheduled Trips as well as Dynamic (ad-hoc) trips are supported.

Both services description included here are based on the SoA and remain to be renegotiated and yet to be developed later within WP5 and WP6.

As described in section 4.5.1.1, MQTT and REST are the two methods that will enable inter-component communication in SHOW.

6.1 Estimated Time of Arrival service architecture

6.1.1 Description of the service

The Estimated Time of Arrival (ETA) is one of the services to be implemented for SHOW. The main function of this service is to alert the customer about the estimated time for their request to be fulfilled. It is especially helpful in the case of Public Transport (PT), as well as in Demand Responsive Transport (DRT). This service can also be used to track the transport time of cargo, hence can be used in mixed passenger/cargo transport as well. More information about this service can be found in SHOW D5.1 subsection 7.2.3 paragraph 2, as a wider Bus arrival time / travel-time prediction service.

During this service operation, a consumer sends their location and their intended destination, while timestamping the specific request. In return, the cloud service collects that data and the data from the vehicles and the city traffic, calculates ETA and then notifies the consumer about their request, while being able to send frequent updates to the consumer. The cloud service is able to collect data from the vehicles, such as the vehicle's ID, location, speed, the traffic flow in its route and other data it may find useful (e.g., acceleration, next stop, internal temperature, battery status for electric vehicles, mileage, occupancy et al.), transmits the data to the SHOW data collector platform where ETA is calculated, converts UTC to DD/MM/YYYY format and sends messages to the consumer. The cloud platform database could also be able to

save the calculated ETA for self-learning and better performance purposes. The cloud platform should also be able to collect data considering topics relevant to ETA calculation (weather, overall city traffic, the status of the traffic lights and maps) from external providers (Third Party APIs and city infrastructure). The consumers' interface could be either an HTML page or a dashboard UI, from which they will be able to login and create a new request.

6.1.2 Functional Requirements

In this Section, the functional requirements of the Estimated Time of Arrival service are presented. These requirements describe the main functionalities of this service, taking into account the whole SHOW architecture, in order to address the needs of this specific service.

Table 18: Functional Requirements for ETA service

Req_Id	Description
Req_ETA_001	The passenger shall be able to log in the SHOW **Dashboard**
Req_ETA_002	The passenger shall be able to send information about their **location.**
Req_ETA_003	The passenger shall be able to to send information about their **destination.**
Req_ETA_004	The passenger shall be able to send information about their **current time.**
Req_ETA_005	The passenger shall to be able to send **IP / MAC address.**
Req_ETA_006	The passenger shall be able to create a **new session.**
Req_ETA_007	The passenger shall be able to choose **pickup/drop-off locations.**
Req_ETA_008	The passenger shall be able to **delete a request.**
Req_ETA_009	The passenger shall be able to **receive** pickup and drop-off **time** from the cloud platform via the SHOW Dashboard.
Req_ETA_010	The vehicle shall be able to send its **vehicle ID** to the cloud platform.
Req_ETA_011	The vehicle shall be able to send **IP/MAC address.**
Req_ETA_012	The vehicle shall be able to create a **new session.**
Req_ETA_013	The vehicle shall be able to send and update information about its **location.**
Req_ETA_014	The vehicle should be able to send and update information about its **speed.**
Req_ETA_015	The vehicle should be able to send and update information about the **traffic** in its route.
Req_ETA_016	The vehicle can be able to send and update **sensor data** about its current status.
Req_ETA_017	The cloud platform shall be able to **collect all data** sent by passenger/vehicle.
Req_ETA_018	The cloud platform shall be able to **send messages** to the SHOW Dashboard.
Req_ETA_019	The cloud platform should be able to **collect information** from **third party APIs.**
Req_ETA_020	The cloud platform (data manager) shall be able to **calculate ETA**.
Req_ETA_021	The cloud platform (data manager) shall be able to **convert UTC to DD/MM/YYYY**.
Req_ETA_022	The cloud platform can be able to **save ETA** for better performance.
Req_ETA_0	The third-party APIs should be able to send information about **relevant topics.**

Req_Id	Description
23	

6.1.3 Estimated Time of Arrival Message flows

In Figure 22, the overall message exchange flow for Estimated Time of Arrival is found. A consumer logs in the HTML page or the SHOW dashboard, in order to create a request. Both MQTT and REST APIs are used in this scope, according to the nature of the data. The API Gateway and the MQTT broker collect the data and forward it to the Data Management Portal, in order to calculate ETA and in turn store data in databases for future reference. The following figures provide a visualization of each message exchange protocol, as collected from each data source (passenger, vehicle fleet or infrastructure). More detail is provided in SHOW D5.1.

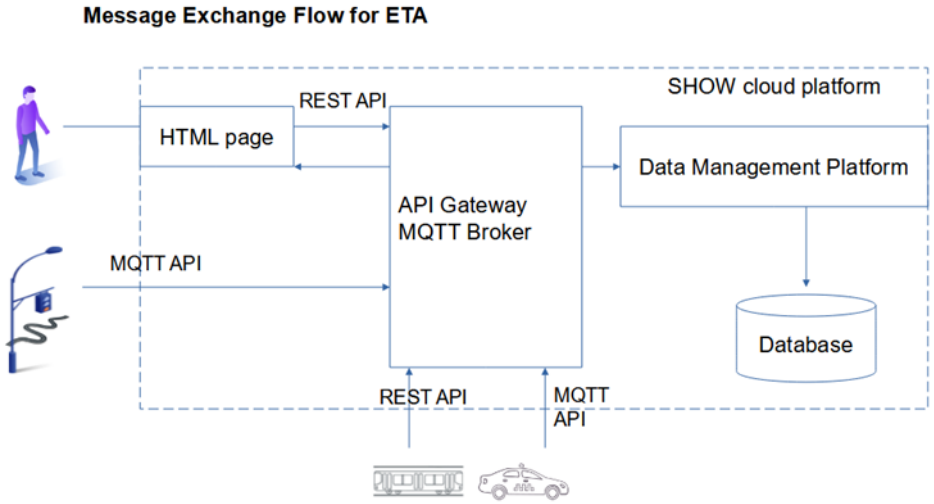

Figure 22: Overall message exchange for ETA service

Figure 22 presents the overall message exchange for ETA service. The passenger logs in an HTML page, which in turn transmits messages to the API Gateway and MQTT Broker, along with Third Party APIs and the vehicle fleet. These messages get sent to SHOW Data Management Platform, in order to calculate ETA and notify the passenger. ETA and data from the vehicle fleet is also stored in a database.

Figure 24 shows the REST APIs utilized in this service. Data transmitted in this scope mainly focus on passengers' personal data, in order to create a request, as well as data about the vehicle that will be used in this itinerary. Figure 23 on the other hand presents the data collection accomplished via MQTT APIs. Third Party APIs and vehicles publish on respective topics, for the SHOW cloud platform to be able to calculate the Estimated Time of Arrival concurrently and efficiently.

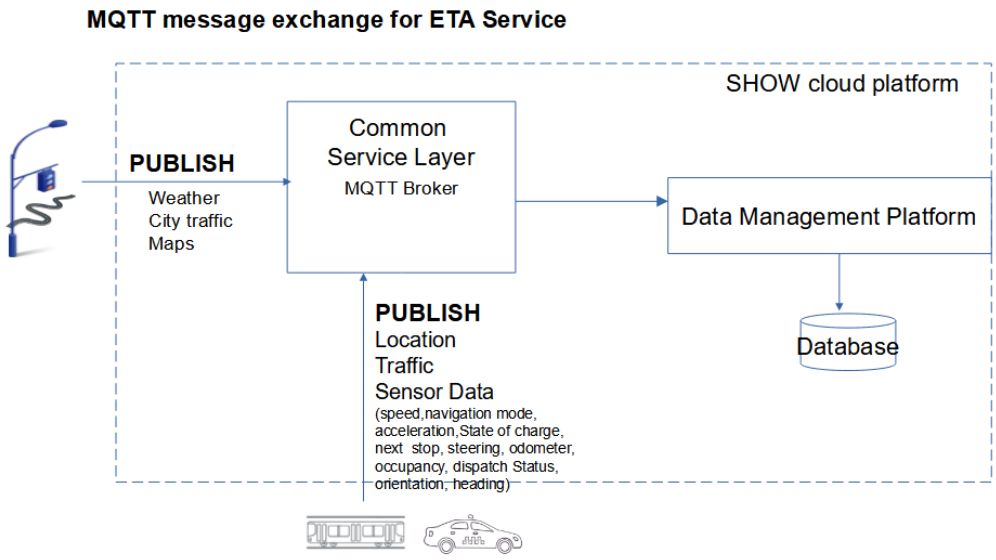

Figure 23: MQTT APIs for ETA service

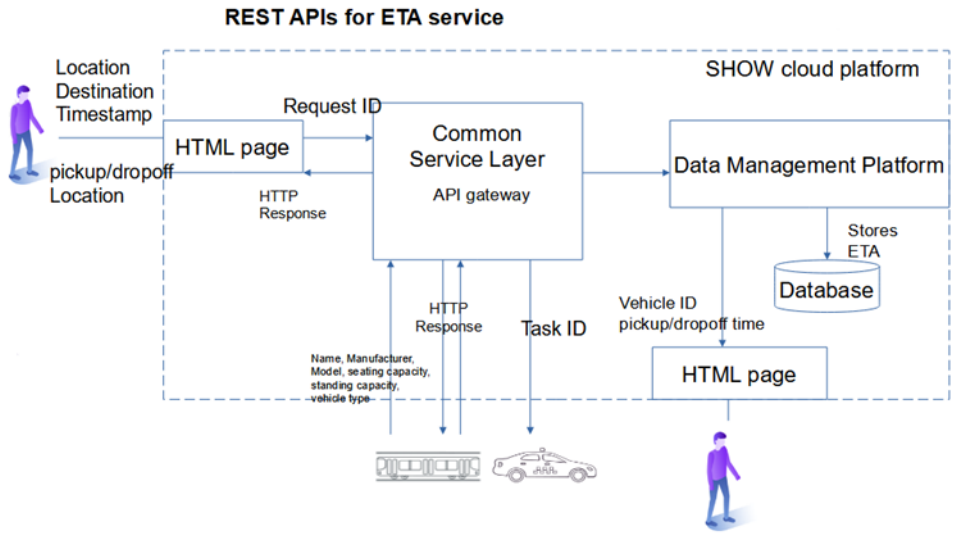

Figure 24: REST APIs for ETA service

6.2 Multimodal Planner service architecture

6.2.1 Description of the service

Multimodal Planner is one of the services to be implemented for SHOW. A Public Transport Trip (PT) in an urban public transport system usually involves the combined use of the available public transport services. Each passenger may require usage of multiple vehicles in the same fleet in order to reach their destination, as different mobility needs are defined by a different sequence of stops and a specified schedule. In this context, any PT trip may be realized by a path that consists of alternate interconnected route segments of the underlying public transport services. It is evident that a PT trip may be realized by several alternative itineraries. A major decision that emerges for the passengers relates to the selection of the itinerary that complies with their preferences and requirements. More information about this service can be found

in SHOW D5.1 (*Big Data Collection Platform and Data Management Portal*) [19] chapter 7.2.3 paragraph 8.

6.2.2 Functional Requirements

This Section describes the functional requirements of the Multimodal Planner service. The requirements which are presented address the needs of this specific service, taking into account the whole SHOW architecture. In an attempt to deploy a State-of-the-Art service, all possible requirements were attempted to be included.

Table 19: Functional Requirements for Multimodal Planner service

Req_Id	Description
Req_MP_001	The passenger shall be able to **log in** the SHOW dashboard
Req_MP_002	The passenger shall be able to send information about their **location.**
Req_MP_003	The passenger shall be able to send information about their **destination.**
Req_MP_004	The passenger shall be able to send information about their **current time.**
Req_MP_005	The passenger shall be able to send **IP / MAC address.**
Req_MP_006	The passenger shall to be able to create a **new session.**
Req_MP_007	The passenger shall be able to choose **pickup/drop-off locations.**
Req_MP_008	The passenger shall be able to **delete a request.**
Req_MP_009	The passenger shall be able to **receive** pickup and drop-off **time** from the cloud platform **via the SHOW Dashboard**.
Req_MP_010	The passenger shall be able to get data about the **vehicles they will embark** from cloud platform **via the SHOW Dashboard**.
Req_MP_011	The vehicle shall be able to send its **vehicle ID** to the cloud platform.
Req_MP_012	The vehicle shall be able to send **IP/MAC address.**
Req_MP_013	The vehicle shall be able to create a **new session.**
Req_MP_014	The vehicle shall be able to send and update information about its **location.**
Req_MP_015	The vehicle should be able to send and update information about its **speed.**
Req_MP_016	The vehicle can be able to send and update information about the **traffic** in its route.
Req_MP_017	The vehicle should be able to send and update **sensor data** about its current status.
Req_MP_018	The vehicle shall be able to send its **availability status** to the cloud platform.
Req_MP_019	The cloud platform shall be able to **collect all data** sent by passenger/vehicle.
Req_MP_020	The cloud platform shall be able to **send messages** to the SHOW Dashboard.
Req_MP_021	The cloud platform should be able to **collect information** from **third party APIs.**
Req_MP_022	The cloud platform shall be able to retrieve **vehicle availability.**
Req_MP_023	The cloud platform shall be able to **send data** (e.g., ID) to the SHOW Dashboard about the vehicles passengers will embark.
Req_MP_024	The cloud platform shall be able to **assign tasks** to vehicles.
Req_MP_025	The cloud platform shall be able to decide **optimal vehicle usage.**
Req_MP_026	The third party APIs should be able to send information about **relevant topics.**

6.2.3 Multimodal Planner Service message flow

In Figure 25, the overall message exchange flow for Multimodal Planner is depicted. A consumer logs in the HTML page or the SHOW dashboard, in order to create a request. The SHOW cloud platform utilizes AI algorithms to decide the passengers' itinerary and then returns its ID and other information back to the Passenger, via the HTML page. Both MQTT and REST APIs are used in this scope, according to the nature of the data. The API Gateway and the MQTT broker collect the data and forward it to the Data Management Platform, in order to decide optimal itinerary and vehicle usage. Figure 25 and Figure 26 provide a visualization of each message exchange protocol, as collected from each data source (passenger, vehicle fleet or infrastructure). More detail is provided in SHOW D5.1.

Figure 26 lower part shows the REST APIs utilized in this service. Data transmitted in this scope mainly focus on passengers' personal data, in order to create a request, as well as data about the vehicle that will be used in this itinerary. It is important to note that, since more than one vehicle will be used in this service, the concurrent data transmission is essential for the SHOW cloud platform to calculate optimal vehicle usage and task assignment for each itinerary.

Figure 26 upper part presents the data transmitted via MQTT APIs. Third Party APIs and vehicles publish on respective topics, for the SHOW cloud platform to be able to assign specific tasks to corresponding vehicles, according to the passengers' itineraries.

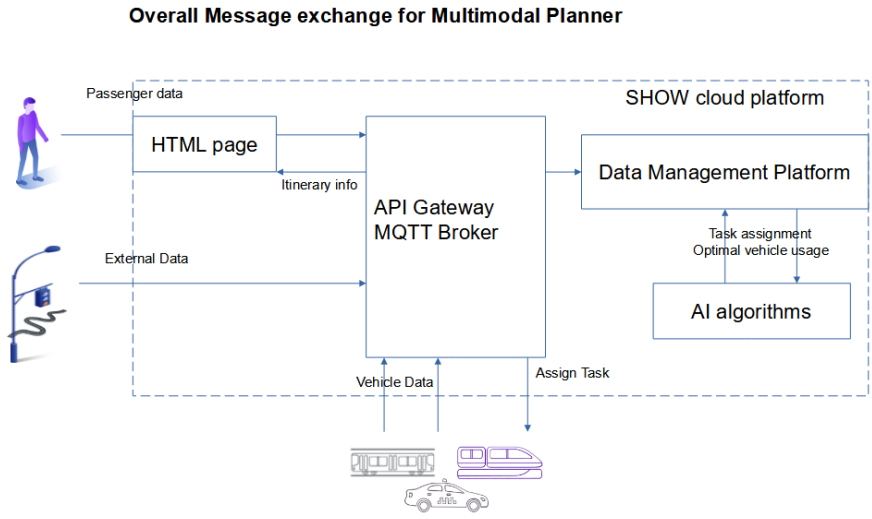

Figure 25: Overall message exchange for Multimodal Planner service

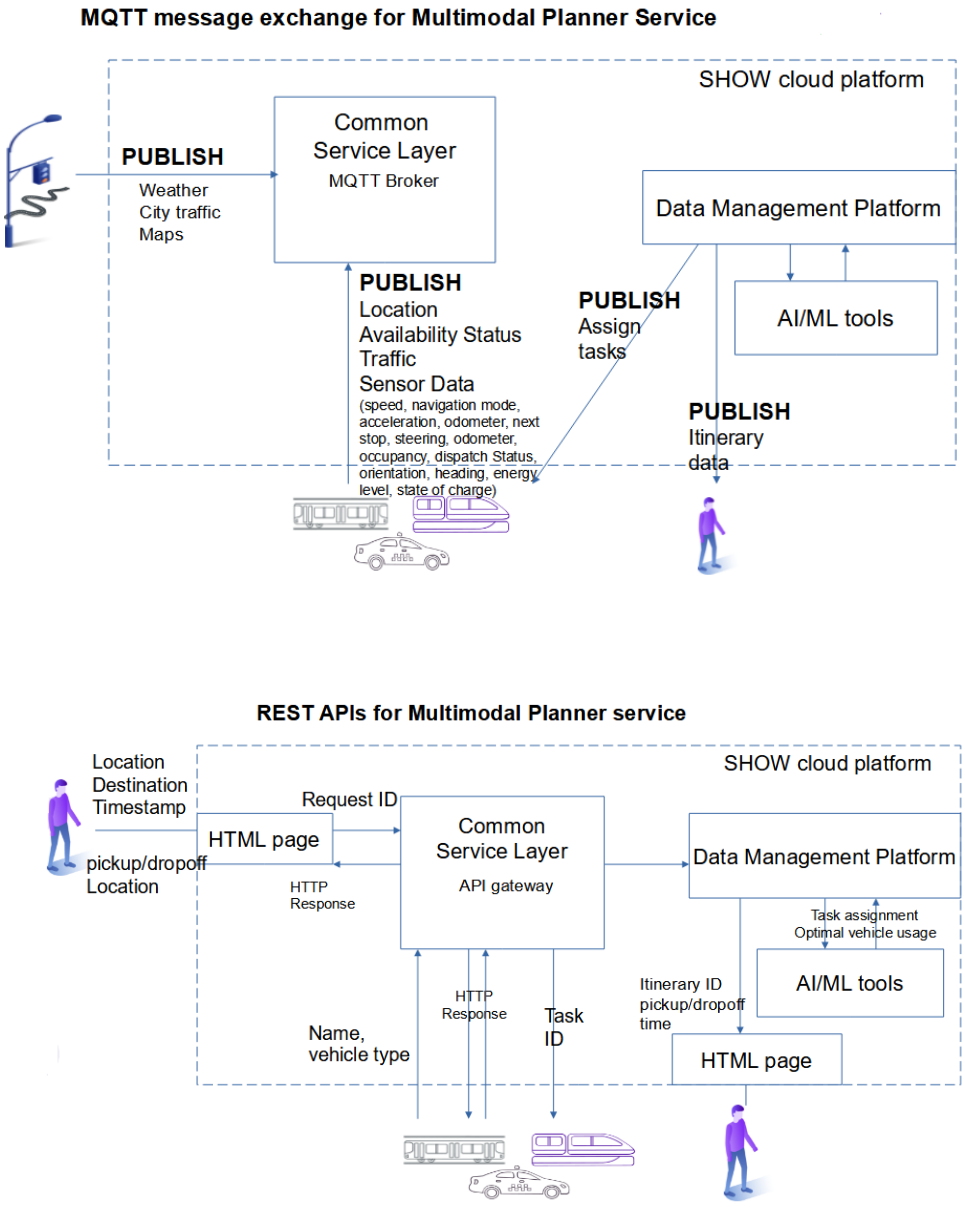

Figure 26: Message exchange for Multimodal Planner service via REST APIs and MQTT

6.3 Data for SHOW CCAM services

6.3.1 Data exchange for Estimated Time of Arrival service

Data sources inside the vehicle

For the estimated time of arrival (ETA) and travel time prediction applications, the minimum requirement of input features are geospatial data usually in the form of timestamped coordinates recorded by Automatic Vehicle Location (AVL) systems [70]. The simplest way to obtain such data is to equip the vehicle with a GPS sensor and transmit its location at frequent time intervals (typically ranging 20-60 seconds). An example of GPS sensor data type is presented in Table 27. Simple ETA prediction methods based only on timestamped coordinates use the average speed (which can be easily calculated) to predict the arrival time at a point of a predefined route [71].

However, more sophisticated methods such as Kalman Filters [72] and Neural Networks [73] can show better prediction accuracy.

Another way to accurately predict the time of arrival of a vehicle is to use information about the traffic flow. For that reason, camera and Lidar sensors could be installed on the vehicle so as to calculate the number and the speed of vehicles in front of it. This information can then be fused and utilized alongside the AVL data to train a predictive model.

Furthermore, as the AV's purpose is to carry passengers towards a destination with the potential of many intermediate stops, the passengers themselves affect the progress of the vehicle. Therefore, the number of persons on-board the vehicle as well as the frequency of the requested stops will influence the arrival time at any point on the route. This information can be acquired through camera sensors employing AI techniques for object detection to count the exact number of passengers. Moreover, the vehicle itself can obtain vehicle stop requests information and send them to the processing unit that employs the predictive algorithms. The data types of such information are described in Table 22.

External Data

It is widely known that progress in traffic also depends on external sources such as traffic volume and weather. A non-intuitive approach [74] used cameras installed on top of bridges that counted bus traffic and the velocity of taxis. The research found that the speed of buses and taxis is the same in heavy traffic. They also found that the predictions based only on data from the static cameras identifying the busses were more accurate than using GPS data alone. Moreover, weather can also affect the traffic; therefore, data acquired through the internet regarding the weather in the vehicle's area can be also utilized in the predictive algorithm. Such data can be acquired through an external API (i.e., https://openweathermap.org/) where a client can send requests every 10-20 minutes.

6.3.2 Data exchange for Optimal Routing

In [75] the authors introduce a method for dynamic vehicle routing for a network of autonomous taxis that minimizes the costs of travel requests, both current and future ones. The method first computes a probability distribution of future requests based on historical data and then solves an integer linear program to calculate the assignments to trips.

Data needed for these kinds of methods are:

- The current state of the fleet.
- A set of the current requests for vehicles.
- The future demand, which can be predicted and is consisted of destinations and origins.

Below there is a better formulation of the required data for the aforementioned algorithm. The state of the fleet can be expressed by a set of vehicles where each vehicle can be described by this tuple {*current vehicle position, current vehicle time, passengers*} where each passenger is a fulfilled request. Each of the current requests can be expressed by a tuple {*origin, destination, time, latest acceptable pickup time, earliest possible time to reach the destination*} where origin is the starting point from where the passenger is to be picked up from, destination is the final point the passenger needs to visit and time is the time of the request. There should also be saved the *actual pick-up time* of the person by the vehicle and the expected *drop off*

time. Moreover, there should be a way to compute travel times between an origin and a destination. Ideally, this information can be precomputed and saved in a database in the case of predefined stop stations or it can be calculated on the go in a scenario where we try to solve the same problem with requests originated by arbitrary points in the map. However, the second approach is more difficult and it probably requires an online API such as google maps. Additionally, a single vehicle can combine and serve more than one requests. We can save this information representing a trip in the database too. Each vehicle may execute many trips where each trip may be consisted of many requests. In that way and based on the characteristics of each request, machine learning algorithms may be trained to give different solutions on this problem once adequate number of data has been captured.

Another similar approach is shown in [76] where the authors present a real time ride sharing solution for big fleets in urban environments and customer requests utilizing the NYC Taxi and Limousine Commission dataset [77]The service in this solution is expressed as an optimization engine, which runs at periodic time instants (i.e every second). It processes the requests that arrive at those instants and proposes an optimal vehicle-costumer assignment and the related matching routes. Again, for this problem there is the concept of trip which is consisted of the origin coordinates, the destination coordinates and the time window constraints for pick-up and delivery. A representation of all the aforementioned data and their forms need for the optimal routing problem is depicted in Table 20 and Table 21.

Table 20: Vehicle related data

Name	Length	Type	Description
Vehicle ID	-	DOUBLE	Id of the vehicle
Vehicle Position	-	DOUBLE	Current position of the vehicle (longitude, latitude)
Timestamp	-	DOUBLE	Current vehicle time
Passengers	-	STRING	Tuple containing requests that have been picked up by the vehicle. (Pv = {p1,..,pn})
Available seats	-	INT	The number of available seats

Table 21: Customer Request

Name	Length	Type	Description
Request ID	-	DOUBLE	The id of the request
Origin	-	DOUBLE	Origin of the request (longitude, latitude)
Destination	-	DOUBLE	Destination of the request (longitude, latitude)
Timestamp	-	DOUBLE	The time the request was made
Pick-up time	-	DOUBLE	The latest acceptable pickup time
Destination time	-	DOUBLE	Earliest possible time to reach the destination

Table 22: Booking/Ride Data

Name	Length	Type	Description
Load	-	INT	Number of travelers contained in the booking/ride
Desired pickup location	-	FLOAT	Desired pickup location(latitute/longitude)
Desired pickup time	-	Date and time in UTC according to ISO 8601	Desired pickup time
Desired dropoff location	-	FLOAT	Desired dropoff location(latitute/longitude)

Name	Length	Type	Description
Desired dropoff time	-	Date and time in UTC according to ISO 8601	Desired dropoff time
Planned pickup location	-	FLOAT	Planned pickup location
Planned pickuup time	-	Date and time in UTC according to ISO 8601	Planned pickuup time
Planned dropoff location	-	FLOAT	Planned dropoff location
Planned dropoff time	-	Date and time in UTC according to ISO 8601	Planned dropoff time
Actual pickup location	-	FLOAT	Actual pickup location
Actual pickup time	-	Date and time in UTC according to ISO 8601	Actual pickup time
Actual dropoff Location	-	FLOAT	Actual dropoff location
Actual dropoff time	-	ISO 8601 duration	Actual dropoff time
Planned booking route	-	GeoJSON	Planned vehicle route between pickup and dropoff location
Actual booking route	-	GeoJSON	Actual vehicle route between pickup and dropoff location
Direct ride distance	-	FLOAT	Length of the fastest direct route between pickup and dropoff location
Direct ride duration	-	ISO 8601 duration	Duration of the fastest direct route between pickup and dropoff location
Actual ride distance	-	FLOAT	Length of the actual route between the actual pickup location and the actual dropoff location
Actual ride duration	-	ISO 8601 duration	Duration between the actual pickup time and the actual dropoff time

General data format

In the following tables data that can be collected from an AV and its sensors are presented. Frequent collection of information such as the data presented in Table 20-Table 26 can aid artificial intelligence algorithms give solutions in problems that concern WP5 such as AV's arrival and travel time, fleet and traffic management as well as mobility patterns identification and prediction while problems such as demand prediction and optimal routing can be addressed by the data descriptions presented in section 2 and specifically in Table 20 and Table 21.

In Table 23 various variables are presented that can be collected from an AV that can be stored by the Big Data Collection platform in the system's storage.

Table 23: Vehicle Sensor Variables

Name	Length	Type	Description
Localization (GNSS)	-	DOUBLE	Get (Longitude, latitude)
Connection status		BOOLEAN	Offline or Online
Real-time speed	-	DOUBLE	-
Navigation mode	-	STRING	(Autonomous/Manual)
Real-time Acceleration	-	DOUBLE	-
Type of service	-	STRING	(Metro/bus/On-demand)
Defined next station/stop	-	DOUBLE	Get Next station (Longitude,Latitude)
Internal passenger compartment temperature	-	DOUBLE	Internal temperature
Battery status	-	DOUBLE	Battery status of the vehicle
Mileage	-	DOUBLE	Mileage of the vehicle
Steering angle of two axes	-	DOUBLE	-
Hit ratio	-	DOUBLE	(recorded lidar impacts vs detected lidar impacts)
Cellular network connection	-	STRING	(3G/4G)
Odometer	-	INT	Current odometer reading of the vehicle
Occupancy	-	INT	Current occupancy of the vehicle
Dispatch status	-	STRING	Type of mission the vehicle is dispatched to serve
Orientation	-	FLOAT	Direction where the front of the vehicle is pointing to
Heading	-	FLOAT	Angle between the direction in which the vehicle's front is pointing and the true north
Door status	-	BOOLEAN	Whether doors are open or closed
GNSS connection	-	BOOLEAN	Whether GNSS is connected or not
Emergency notifications time	-	FLOAT	Vehicle location at the time of the emergency notification
Incident	-	STRING	An unexpected event.
Alarm	-	BOOLEAN	A dysfunctionality of the system
Type of Event	-	STRING	Emergency or incident
Located Event		FLOAT/TIME	Time and location of an existing event
Vehicle is braking	-	BOOLEAN	Whether vehicle is braking or not
Strong braking	-	BOOLEAN	-
Severe braking	-	BOOLEAN	-

The following tables present example data forms received from different sensors. A general schema of sensor data is presented in Table 25 and examples of IDPS, CP, GPS and camera sensors' data format is presented in Table 28.

Table 24: General form of expected data

Name	Length	Type	Description
sensor_id	4 Bytes	UINT32	The ID of the sensor
creation_timestamp	8 Bytes	UINT64	The timestamp on which this PSD(Processed Sensor Data) has been created. Unix time (UTC) in milliseconds since epoch.
sensor_specific_variable	-	-	Variables depending on the type of sensor

Table 25: IDPS sensor data fields

Name	Length	Type	Description
sensor_id	4 Bytes	UINT32	The ID of the sensor
creation_timestamp	8 Bytes	UINT64	The timestamp on which this PSD has been created. Unix time (UTC) in milliseconds since epoch.
timestamp	8 bytes	UINT64	The timestamp on which the anomaly has been detected. Time (in seconds) from the uptime of the system.
segment	1 bytes	UINT8	The port number of the IDPS.
sample_param	2 bytes	UINT16	Identification of the anomaly type.
msg_id	4 bytes	UINT32	The CAN message ID.
data	8 bytes	UINT8	The CAN frame payload.

Table 26: CP sensor data fields

Name	Length	Type	Description
sensor_id	4 Bytes	UINT32	The ID of the sensor
creation_timestamp	8 Bytes	UINT64	The timestamp on which this PSD has been created. Unix time (UTC) in milliseconds since epoch.
timestamp	8 bytes	UINT64	The timestamp of the alert
msgnum	8 bytes	UINT64	Index
truncate	1 bytes	CHAR	Whether the message is truncated or not (happens when msg is too long).
vin	17 bytes	STRING	Vehicle number
phase	8 Bytes	UINT64	Vehicle state, one of of the following: normal, suspend, teardown
version	unlimited	STRING	The version of the log format.
path	indeterminate	STRING	The path of violating the process.
pid	4 bytes	UINT32	The violating process ID.
uid	4 bytes	UINT32	
action	unlimited	STRING	The action type that CP performed as a response.
category	unlimited	STRING	The identifier of the heuristic that was triggered.
text	unlimited	STRING	Depends on the heuristic - detail about the anomaly detected.

Table 27: GPS sensor data fields

Name	Length	Type	Description
sensor_id	4 Bytes	UINT32	The ID of the sensor
creation_timestamp	8 Bytes	UINT64	The timestamp on which this PSD has been created. Unix time (UTC) in milliseconds since epoch.
timestamp	8 bytes	UINT64	The timestamp of the alert
latitude	8 bytes	FLOAT64	The latitude in the DDMM.MMMMM format. Decimal places are variables.
longitude	8 bytes	FLOAT64	The longitude in the

Name	Length	Type	Description
			DDMM.MMMMM format. Decimal places are variables.

Table 28: Camera Sensor data fields

Name	Length	Type	Description
sensor_id	4 Bytes	UINT32	The ID of the sensor
creation_timestamp	8 Bytes	UINT64	The timestamp on which this PSD has been created. Unix time (UTC) in milliseconds since epoch.
timestamp	8 bytes	UINT64	The timestamp of the alert
camera data	-	OBJECT	Specific frame corresponding to a timestamp

Additionally, data captured from the traffic between the vehicles network can be acquired for analysis. In particular, these kinds of data can be logs referring to metadata showing the traffic between the sensors and the cloud servers (which sensor data are sent to which cloud server, at which time etc). Example of such data (Table 29) can be found in CAV cyber-attacks dataset which is derived from KDD'99 [78].

Table 29: Network traffic metadata

Name	Length	Type	Description
Protocol_type	4 Bytes	STRING	The protocol type (tcp, udp etc)
Service	8 Bytes	UINT64	Protocol type used for the service (i.e http)
Src_bytes	8 Bytes	UINT64	Source bytes
Dst_bytes	8 Bytes	UINT64	Destination Bytes
duration	4 Bytes	INT	Duration of the request

The overview of the SHOW MDP architecture, based on D5.1, was provided in 4.5.2. Communication protocols selected have been discussed in 4.6.1.1

7 Technical Risks' management

7.1 Risk assessment in SHOW

A risk assessment is planned to be performed **prior to any technical validation and evaluation phase** on all SHOW layers using an extended FMEA methodology within *A4.6: Risk assessment* (apart from the project management layer that is addressed in the context of *A14.3: Quality & Risk Management*, in the context of which a continuous process is being performed with its results being reported on annual basis in the project progress reports).

The starting point has been the risks identified in the Grant Agreement of the project (Section 1.3.5), which have been preserved in the final risk registry, while additional risks have been added on top. Not only **technical**, but also **behavioural, legal/regulatory, operational** or **demonstration/evaluation** risks have been considered (following the methodology described in the following section), while COVID-19 related effects have been also addressed.

The risk assessment process will take place in 3 iterations in total in SHOW project, in order to early identify risks but also potential corrective and mitigation actions prior to each evaluation phase (technical, pre-demo, final demo phase). This first round reported herein corresponds to the risks recognized in view of the technical validation of the project that is anticipated to be completed in the first semester of 2021.

7.2 The extended FMEA methodology in SHOW

Failure Mode and Effects Analysis (FMEA) is a methodology designed to:

- Identify potential failure modes for a product or process;
- Assess the risk associated with those failure modes and prioritise issues for corrective actions;
- Identify and carry out (in advance) corrective actions to address the most serious concerns.

The FMEA procedure is a well-known tool that has been adapted in many different ways for many different purposes. It can contribute to improved designs for products and processes, resulting in higher reliability, better quality, increased safety, enhanced customer satisfaction and reduced costs. The tool can also be used to establish and optimise maintenance plans for repairable systems and/ or contribute to control plans and other quality assurance procedures. It provides a knowledge base of failure mode and corrective action information that can be used as a resource in future troubleshooting efforts and as a training tool for new engineers. In addition, a FMEA is often required to comply with safety and quality requirements, such as ISO 9001, Six Sigma, FDA Good Manufacturing Practices (GMPs), Process Safety Management Act (PSM), etc.

In SHOW an **extended FMEA** will be used that has been developed at ADVISORS project [88]. The findings, solutions and processes to be applied and/or developed in SHOW project will undergo a thorough assessment in an iterative manner using the extended FMEA methodology adjusted – as explained below – in a way to fit the needs of the project.

The early recognition of risks and potential (and also alternative) corrective and mitigation actions will allow the smoothest possible adoption of SHOW solutions and processes and fulfilment of the project objectives.

The **extended FMEA** methodology adjusted for SHOW, is based on the classical FMEA methodology, which by default includes the indicators of *hazard consequence severity, occurrence probability, detectability* and *recoverability*, but extends it, covering not only technical risks, as done in the classical FMEA methodology, but including also *behavioural*, *legal and operational* and *demonstration/ evaluation*–related ones. The significance of a risk, overall, depends both on its consequences and the probability of its occurrence, but also on how easily the developing risk can be detected. In general, a risk assessment process consists of an analysis of the risk (e.g., the identification of potential hazards and some estimation of their magnitude) and an evaluation of the tolerability of that risk in its anticipated context. The steps followed for the calculation of the risk according to the **extended FMEA methodology**, and as applied in SHOW project, are depicted in Figure 27 and in Figure 28 respectively (identical to the original FMEA process steps).

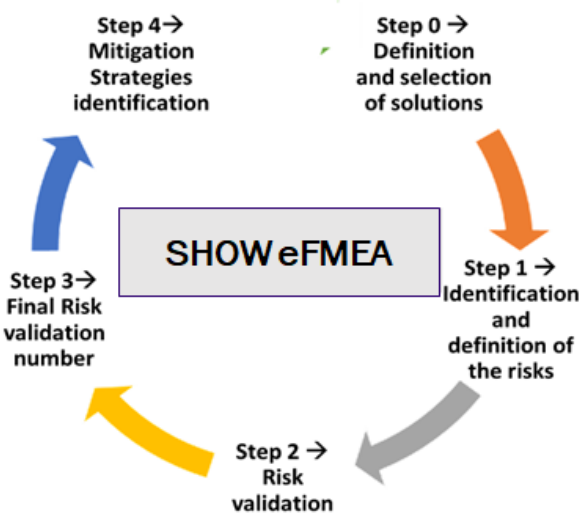

Figure 27: FMEA methodology steps

Risks identification is a living process in the project and for their identification all beneficiaries have been involved with a specific emphasis to the beneficiaries involved in the pilot sites of the project. Still, the ranking of every risk across severity, occurrence probability, detectability and recoverability has been given by the SHOW Core Group, and after being averaged for each parameter, it has led to one overall risk level for each risk listed. All the consolidation work has been done by CERTH/HIT who is the risk assessment issuer in the project.

The first round of the A4.6 risk assessment has been already completed and relevant risks have been identified in view of the technical validation phase of the project. For every risk identified, the risk **severity, occurrence probability, detectability and recoverability** has been calculated to allow, finally, the calculation of the **overall risk level** per each.

For this first round of risk assessment, a common registry of risks has been compiled, utilising the feedback by all Partners, recognising, every time, the applicability of the risks to the project sites. In the future versions, risk assessment will be performed in two discrete levels; one horizontal level and one site specific level for the Mega and Satellite sites.

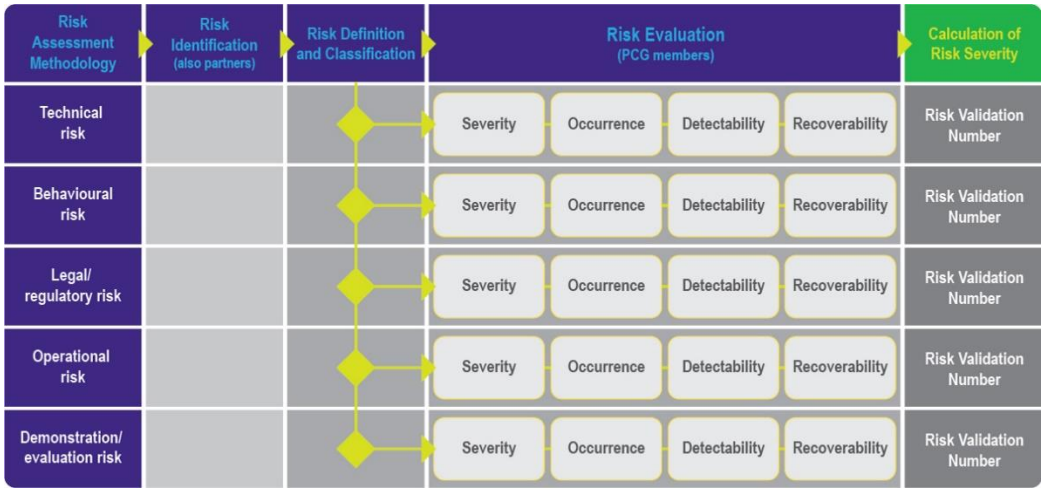

Figure 28: eFMEA Methodology in SHOW.

In the next sections, the **extended FMEA** methodology implemented in SHOW, is being described, step by step, as it has been realised in the project in the context of Activity 4.6. Additionally, all the parameters used in the **extended FMEA methodology** analysis are being explained and a reference table for each parameter that helps in understanding the meaning of such parameters and the criteria utilised for the value assignment, is also included.

7.3 SHOW eFMEA registry template & step-wise approach

For the realisation of the extended FMEA methodology, a template (Table 1) has been filled in from all the beneficiaries of the Consortium. Each cell of the table corresponds to each individual step of the methodology, as explained in the following sections.

Table 30: Risks assessment methodology template.

Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WP(s)	Specific site(s) this risk is associated (if applicable)	S	O*	D*	R*	Risk Number	Problem severity	Risk Mitigation Measures
	❑Technical ❑Behavioural ❑Legal/ Regulatory ❑Operational ❑Demonstration/Evaluation												

7.3.1 Step 0: Definition and selection of solutions

In this step, the objective of the risk assessment has been defined, which is namely the SHOW solutions (meaning the technological solutions on infrastructure and vehicle side as well as the services to be deployed) and processes (target evaluation activities with all associated to them activities) as those will be piloted in the different sites of the project according to the workplan of the project.

7.3.2 Step 1: Identification and definition of risks

The first step encompasses the as much as more accurate short description of the risk ("definition of Risk" column), its clustering in the defined types of risks for SHOW ("Type of Risk" cluster), and, in turn, the definition of the accompanying attributes of the risk ("Risk Effect", "Risk Cause", "Risk Detection" columns) that assist with the understanding of the risk anticipated. In turn, the "Relevant WP(s)" this risk is associated with is necessary to identify (for the later mitigation of the risk through concrete actions by specific task forces of the project). Also, and for SHOW in

specific, the correspondence of the risk to all or specific sites of the project is defined ("Specific site(s) this risk is associated (if applicable)") column.

Based on various criteria (e.g., significance of solution and/or of SHOW process, society readiness, technical aspects of pilots realisation, etc.), all SHOW partners have been asked to identify risks according to their understanding, expertise and their so far experience in the project.

Risks clusters in SHOW were pre-defined to be either **technical** (e.g. related to potential future technological limitations and challenges), **behavioural** (e.g. related to user and stakeholder engagement and acceptance), **legal/ regulatory** (e.g. related to legal and regulatory barriers especially with regard to demonstration), **operational** (e.g. shift of authority, processes, logistics, etc.) and **demonstration/evaluation** (associated with any demonstration/evaluation aspect of the project).

7.3.3 Step 2: Risk Validation

For each one of the risks identified, a specific validation has been made across the different interrelated aspects, as explained below.

Table 31: Extended risks assessment methodology template, Step 2.

Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WP(s)	Specific site(s) this risk is associated (if applicable).	S*	O*	D*	R*	Risk Number	Problem severity	Risk Mitigation Measures
	❑Technical ❑Behavioural ❑Legal/ Regulatory ❑Operational												

7.3.3.1 Risk Severity (S)

Technical Risks Analysis

Technical assessment considers technical (hardware and software) failures or risks that are related to the technical maturity, readiness and limitations of the under assessment solution. In general, technical issues are considered as barriers to SHOW anticipated outcomes if one or more of the following applies:

1. A technical solution or part of it, is not available or mature enough, needs further investigation, or is highly complicated.
2. Cost of the technical solution or part of it would be prohibitive.
3. Technical limitations are anticipated to significantly prohibit the target functionality and/or the benefits gained from the functionality of the solution are uncertain.

On this basis, the severity levels (S) for technical failure are described below.

Table 32: Definition of unmitigated severity levels for technical risks.

Severity of unmitigated risk	Rate	Definition
Extremely severe	9-10	The failure could put user safety at risk.
Severe	7-8	The failure implies total loss of the solution availability causing major user's dissatisfaction.
Moderate	5-6	Failure implies the partial loss of the solutions' function causing user's dissatisfaction.
Slight	3-4	The failure implies slight dissatisfaction to the user.
Insignificant	1-2	The failure does not imply perceptible effects to the system function and to the user's satisfaction.

Mitigation strategies could involve implementing one of the alternative provisions identified in the FMEA or restricting the scope or function of the solution.

Behavioural Risks Analysis

Behavioural risks are mainly associated with the behaviour of users and entities that may have a negative impact on the society and the SHOW outcomes. In general, in this cluster, human error and behaviour effects but also engagement and acceptance issues are tackled, as follows:

1. A change to human behaviour is required before the solution can be fully deployed or accepted.
2. The expected cost (training, design changes, time availability) of the deployment of the solution is significant.
3. The benefits gained from changed human behaviour due to the deployment of the solution are uncertain.

The severity levels (S) for behavioural risk are described below.

Table 33: Definition of unmitigated severity levels for behavioural risks.

Severity of unmitigated risk	Rate	Definition
Extremely severe	9-10	The user error in operating the solution could lead to an incident worseness (i.e. safety effects).
Severe	7-8	User behavioural error may abort the solution's benefits (i.e. safety effects due to changes in ways of acquiring info).
Moderate	5-6	User's behavioural changes (including engagement and acceptance) may significantly reduce the positive effects of the solution.
Slight	3-4	User's behavioural changes (including engagement and acceptance) may somehow influence the positive effects of the solution.
Insignificant	1-2	User's behaviour (including engagement and acceptance) is not expected to reduce the solution's benefits significantly, or may even further enhance them.

Note that Table 33 (and subsequent tables) develops their broad risk categorisations – "severe", "moderate" etc. – to allow a broad strategic overview of risk even though the nature of the risk can arise in different ways. This means that classification of risk severity is a process that requires the application of experts' judgement.

Legal/ Regulatory Risks Analysis

In a similar way, legal/regulatory issues will be a barrier to SHOW deployment if one or more of the following applies:

1. A change to existing law is required before the solution can be fully deployed.
2. The expected legal cost of deployment (including fees and damages) is significant.
3. There is uncertainty about where large potential liabilities will fall.

The severity levels (S) for liability failure are described below.

Table 34: Definition of unmitigated severity levels for legal/regulatory risks.

Severity of unmitigated risk	Rate	Definition
Extremely severe	9-10	Are there laws in each country that do not allow the solution to be implemented?
Severe	7-8	New laws are required for solution's implementation and no relevant work has been performed yet.
Moderate	5-6	New laws are required for solution's implementation and work required has already been performed.
Slight	3-4	New laws are required for solution's implementation but consensus on them exist.
Insignificant	1-2	No new laws are required for implementation.

Operational Risks Analysis

The regulatory pressures for improved risk assessment and reporting on internal control is of high importance before implementing and, even more, deploying a specific solution, since operational risks like unexpected changes in business routines, frauds, internal control breaches, and governance failures may occur.

It is necessary to relate the attributes of the SHOW outcomes, to the actors involved in their design, evaluation and use. Application of the risk assessment methodology in this area is difficult but operational issues can be subject to analysis by management and political consultants by considering actors, roles and responsibilities, processes and communications. Problems can occur when there is a lack of communication and reporting structures between actors.

The severity levels (S) for Operational risks are described below.

Table 35: Definition of unmitigated severity levels for operational risks.

Severity of unmitigated risk	Rate	Definition
Extremely severe	9-10	Wide and different operational framework is needed, that is completely missing (e.g. services, business roles and models, even infrastructure and communication framework that define operation).
Severe	7-8	Operational framework adaptation is needed (some initial actions have been taken on this domain).

Severity of unmitigated risk	Rate	Definition
Moderate	5-6	Operational framework adaptation is needed which has already started being realised.
Slight	3-4	There is a need for limited and easily realised operational changes.
Insignificant	1-2	There is no need at all for operational changes.

Demonstration/Evaluation Risks Analysis

This risks' category includes the issues that are likely to emerge in the SHOW pilot sites (on an individual basis mainly) and affect either the process to be followed for their proper and expected realisation or their success in terms of collected data (e.g., making them inappropriate for evaluation).

The demonstration/evaluation risks are highly connected to the successful realisation of the Use cases that are to be piloted in each site.

The severity levels (S) for Demonstration/Evaluation risks are described below.

Table 36: Definition of unmitigated severity levels for demonstration/evaluation risks.

Severity of unmitigated risk	Rate	Definition
Extremely severe	9-10	Full adaptation/ change of the demonstration/evaluation framework of the site is needed (≥80% of the Use Cases to be addressed are in danger of failing for any reason).
Severe	7-8	High adaptation of the site's demonstration/evaluation framework is needed (60-80% of the Use Cases to be addressed are in danger of failing for any reason).
Moderate	5-6	Adaptation of the site's demonstration/evaluation framework is needed which has already been organised by the site (30-60% of the Use Cases to be addressed are in danger of failing for any reason).
Slight	3-4	Limited adaptation of the site's demonstration/evaluation framework is needed (≤30% of the Use Cases to be addressed are in danger of failing for any reason).
Insignificant	1-2	Any threat to the realisation of the pilots of the specific site is very unlikely to happen and/or the consequences would be insignificant.

7.3.3.2 Risk Occurrence Probability (O)

The **Occurrence Probability (O)** is the probability that all the risk causes related to the risk modes described in the analysis can occur. This is often a qualitative index especially when new technologies are concerned because of the few reliability data available.

Table 37: Occurrence indicator scale of risk analysis methodology.

Occurrence Probability (O)	Technical issue	Behavioural issue	Legal/ Regulatory issue	Operational issue	Demonstration/ Evaluation issue
9 – 10 (HIGH)	It is certain that some failures will sometimes occur.	It is certain that some behavioural effects will occur (by the users).	It is certain that some legal problems will occur.	It is certain that there will be a need for operational restructuring.	It is certain that there will be a need for adaptation/ change of the demonstration/ evaluation framework to avoid failure in the UCs anticipated.
6 - 7 – 8 (MEDIUM)	A failure could occasionally occur.	Some behavioural effects could occasionally occur.	Some legal problems could occasionally occur.	A need for operational restructuring could occasionally occur (depending on the needs of the solution that will arise).	A need for adaptation/ change of the demonstration/ evaluation framework could occasionally occur.
3 - 4 – 5 (SLIGHT)	There is only a slight probability that an error/failure will occur.	There is only a slight probability that some behavioural effects will occur.	There is only a slight probability that some legal problems will occur.	There is only a slight probability that a need for operational restructuring will occur.	There is only a slight probability that a need for adaptation/ change of the demonstration/ evaluation framework will occur.
1 – 2 (IMPROBABLE)	It is unlikely that a fault will occur.	It is unlikely that some behavioural effects will occur.	It is unlikely that some legal problems will occur.	It is unlikely that a need for operational restructuring will occur.	It is unlikely that a need for adaptation/ change of the demonstration/ evaluation framework will occur.

7.3.3.3 Risk Detectability (D)

Detectability (D) is the probability to detect the occurrence of a risk mode identified in Step 1 of the methodology. Detection of a developing risk is an important aspect of overall risk management, as early detection is a prerequisite for the application of mitigation strategies. In the technical, and to some extent behavioural, domains, detection can be facilitated by additional sensors and processing. In all the other domains, physical monitoring and feedback are the key mechanisms.

Detectability is assigned a value between 1 and 10 (1 means that it is always perfectly detectable and 10 that it is always undetectable).

Table 38: Detectability indicator scale of risk analysis methodology.

Detectability (D)	Technical issue	Behavioural issue	Legal/ Regulatory issue	Operational issue	Demonstration/ Evaluation issue
9 – 10 (IMPROBABLE)	It is impossible or improbable that a problematic area will be detected.	It is impossible or improbable that a user's behavioural effect will be detected.	It is impossible or improbable that a legal problem will be detected.	It is impossible or improbable that an operational problem will be detected.	It is impossible or improbable that a problem connected to the demonstration/ evaluation framework and process will be detected.
7 – 8 (SLIGHT)	The problematic area is detected only in particular cases.	The user's behavioural effect is detected only in particular cases.	The legal problem is detected only in particular cases.	The operational problem is detected only in particular cases.	The demonstration/ evaluation problem is detected only in particular cases.
5 – 6 (MODERATE)	It is probable that the problem will be detected (depending on the situation).	It is probable that the user's behavioural effect will be detected.	It is probable that the legal problem will be detected.	It is probable that the operational problem will be detected.	It is probable that the demonstration/ evaluation problem will be detected.
3 – 4 (HIGH)	It is very probable that a problem will be detected.	It is very probable that the user's behavioural effect will be detected.	It is very probable that the legal problem will be detected.	It is very probable that the operational problem will be detected.	It is very probable that the demonstration/ evaluation problem will be detected.

Detectability (D)	Technical issue	Behavioural issue	Legal/ Regulatory issue	Operational issue	Demonstration/ Evaluation issue
1 – 2 (VERY HIGH)	It is certain that a problem will be detected.	It is certain that the user's behavioural effect will be detected.	It is certain that the legal problem will be detected.	It is certain that the operational problem will be detected.	It is certain that the demonstration/ evaluation problem will be detected.

7.3.3.4 Risk Recoverability (R)

Recoverability (R) is an efficacy index of the possible recovery action performed by the risk management procedures implemented. It estimates the ability of the solution to tolerate the risk. The effectiveness is valued in terms of recoverability which is assigned a value between 1 and 10 (10 represents not recoverable and 1 always perfectly recoverable).

Table 39: Recoverability indicator scale of risk analysis methodology.

Recover-ability (R)	Technical issue	Behavioural issue	Legal/ Regulatory issue	Operational issue	Demonstration/ Evaluation issue
9 – 10 (NULL)	No recovery action is provided.	System is inflexible to user's behavioural effects.	System is either accepted or rejected by the legal framework.	System requires a fixed operational environment to operate.	No recovery action is provided.
6 - 7 – 8 (LOW)	The user is only advised on the failure.	Behavioural effects are taken into account by the solution.	System may be slightly adapted to meet legal restrictions.	System requires a fixed operational framework with limited adaptations.	Solution requires a fixed demonstration/ evaluation framework with limited adaptations.
3 - 4 – 5 (HIGH)	Effective recovery actions are provided.	System customisation might compensate for user's behavioural effects.	System encompasses different versions to meet particular legal demands.	System may operate within various operational frameworks.	Effective recovery actions are provided within the demonstration/ evaluation framework.

Recover-ability (R)	Technical issue	Behavioural issue	Legal/ Regulatory issue	Operational issue	Demonstration/ Evaluation issue
1 – 2 (TOTAL)	The failure effect is completely avoided by the recovery action.	System does not allow user's behavioural effects.	System is easily reconfigurable to meet legal demands.	System does not require operational changes.	System does not require changes of the demonstration/ evaluation framework.

7.3.4 Step 3- Final risk validation number

After collecting the feedback of all beneficiaries, the issuer and consolidator of the risk assessment, CERTH/HIT in this case, consolidates all individual feedbacks aiming at a consistent presentation of risks, covering all different items identified, but at the same time achieving the same level of detail in the risks (and their characteristics) description, avoiding also overlappings.

After that, the consolidated risk registry has been provided to the SHOW Core Group members to give their individual rankings across each index above (Severity, Occurrence Probability, Detectability, Recoverability). Those are collected by each contributor by the issuer (CERTH/HIT) and are averaged so that the overall risk number (RN) will be calculated. The latest aims to give an overall relative indication of risk that is the final tangible outcome of the assessment (together of course with the mitigation actions below) and is calculated as depicted in the following formula.

$$\text{Risk Number} = S * O * \left\lceil \frac{D + R}{2} \right\rceil \quad (1)$$

The results of this equation may vary from 0 to1000 depending on the validity of the risk each failure mode has. Normally, organisations select a pre-defined range for the RN, i.e. above 500 in the 0-1000 scale for which risks a mitigation strategy should be implemented. This is done in order to optimise use of resources and minimise cost.

The results of the risk number can be translated using the following table, which has been established by the FMEA methodology.

Table 40: Results of the Risk number.

Severity Level	Risk Number	Mitigation Possibility	Colour
I – Extremely Severe	513-1000	Very High	Red
II - Severe	217-512	High	Orange
III – Moderate	65-216	Medium	Yellow
IV – Slight	9-64	Low	Green
V – Insignificant	1-8	Improbable	Blue

The overall Risk Number helps in recognising the most critical risks. A critical risk mode is a risk which is very dangerous in their effects, which occurs rather often, is not detected by the internal diagnosis and there is no recovery action performed over its effects.

Table 41: Extended risks assessment methodology template, Step 3.

Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WP(s)	Specific site(s) this risk is associated (if applicable).	S*	O*	D*	R*	Risk Number	Problem severity	Risk Mitigation Measures
	❑Technical ❑Behavioural ❑Legal/ Regulatory ❑Operational												

7.3.5 Step 4- Mitigation strategies identification

At the stage of risk identification, beneficiaries have been asked to provide also potential mitigations strategies. Those, were also consolidated by CERTH/HIT in order to reflect at the end all perspectives in a homologated and compact way. In specific, in terms of mitigation strategies, risk can be reduced in a number of generic ways:

1. reducing the probability of the hazard occurring;
2. increasing failure detection speed and probability;
3. reducing the magnitude (severity) of the consequences of the potential hazard;
4. protecting against the risk - mitigating strategies to compensate for a failure (e.g. back-ups).

One advantage of this approach is its consistency between the different domains (Technical, Legal/Regulatory, Operational, Behavioural and Demonstration/Evaluation).

Table 42: Extended risks assessment methodology template, Step 4.

Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WP(s)	Specific site(s) this risk is associated (if applicable).	S*	O*	D*	R*	Risk Number	Problem severity	Risk Mitigation Measures
	❑Technical ❑Behavioural ❑Legal/ Regulatory ❑Operational												

7.4 1st SHOW Risk Assessment Round results

The analytical outcomes of the first risk assessment round in SHOW are provided below. Going through the outcomes, one can see that **40 risks have been identified in total** at this phase of the project, 5 of them being of double risk type (e.g. having technical but also operational aspects) and 25 pre-existing as of the Grant Agreement preserved all of them as being still valid (noted as pre-existing, if it is the case, at the beginning of each risk description).

In total (and considering the above-mentioned double type of risks), **12 technical, 15 operational, 4 behavioural, 6 legal/ regulatory** and **8 demonstration/evaluation** related risks have been identified and analysed.

It becomes apparent that, while the potential risks identified are many, there **is no risk identified as Extremely Severe and only one risk is ranked with a Level II Severity** (risk number 22, indicated in orange) and it is the one dealing with the impact of **COVID-19** in a cross-cutting way of the project associated mainly with issues related to vehicle procurements and type approvals, permit processes, etc., that is very frequently and commonly recognised in the majority of the SHOW sites as one would expect.

Moreover, **4 risks of the identified ones have been evaluated to be of low severity** and the rest **35 have been validated as of moderate severity**. The Consortium will ensure that the SHOW solutions and services are well protected against the less serious risks (Overall Severity Levels III, IV marked in yellow and green, accordingly – see Table 43), while the already identified mitigation strategies will be applied, if needed.

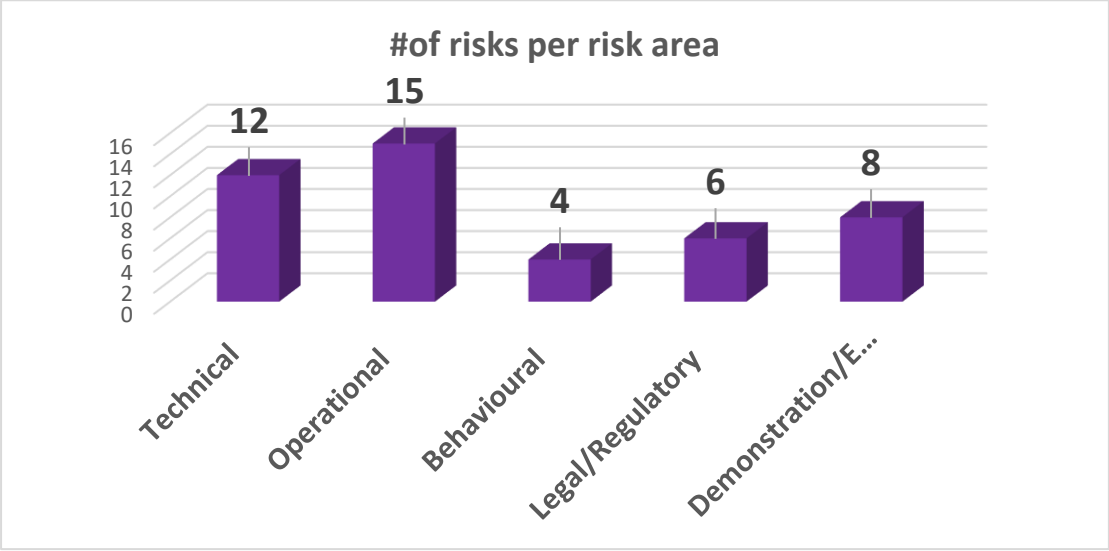

Figure 29: SHOW 1st Risk Assessment Round – Clustering of risks (40 in total; 5 are doubled in clusters).

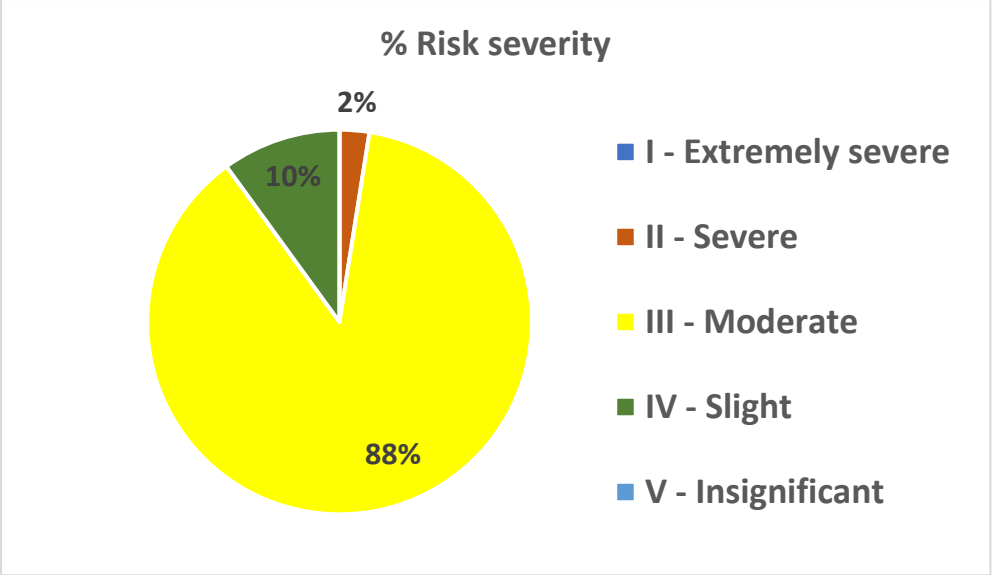

Figure 30: SHOW 1st Risk Assessment Round – Risk Severity Classification.

Table 43: 1st SHOW Risk Assessment Round results.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
1.	[pre-existing] Data platforms: risk related to the lack of openness between the systems, reducing the capability to provide data having a relevant coverage.	Technical	No interoperability reached and able to be proved.	"Closed systems" by OEMs, infrastructure operators and other industrial partners.	During iterative development and integration.	SP2 (WP4-WP8)	All	6	6	4	5	162	This risk shall be mitigated by relying on open standards, such as Fiware and through the development of a common dashboard (A4.3) and a data collection platform (A5.1) with interfaces built to several site dashboards and databases.
2.	[pre-existing]	Technical	Interoperability on	• Highly specific	Self-evident mainly		All	4	3	2,5	4	45	Establish a sound system architecture to enable

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	Lack of transferability of solutions.	Operational	operational level cannot be proved. Replication activities may be limited.	requirements / legacy systems per site. • Local business models and stakeholder's relationships may vary highly from site to site.	during final demonstration phase.	WP2; WP4; WP12							interoperability / transferability of solutions as far as reasonably possible. The various pilot sites of SHOW with different properties, sizes, etc. allow to test shared CCAVs in very different environments, covering a wide range of situations and implementations. This will also allow the establishment of basic models for similar locations (cities, municipalities, regions) that are not directly involved in the project and are considering the introduction of shared CCAVs in the future. Stakeholders engagement in local demo communities from the project beginning and common gathering events will aim at early

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
													alignment and collaboration.
3.	[pre-existing] Closed vendor systems whether these refer to OEM or PTOs.	Technical Operational	Some of the functions and services left out during validation phase. In consequence might cause malfunctions during pre-pilot/pilot phase.	Inevitable "silos"; trust issue; lack of common vision on interoperable CCAM.	During iterative development and integration.	SP2 (WP4-WP8)	All	5	5	4	5	112, 5	This will be solved by the upper layer API manager that will orchestrate all flow of information between different modules as well with the definition of minimum set of data that will be requested by all sites.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
4.	[pre-existing] Cost explosion in the high-tech sector for system development (vehicle sensor implementation, infrastructure).	Technical	Under budgeted tasks in SHOW regarding vehicle and infrastructure upgrades.	Evolving competitive market.	During development and digital/physical adaptations.	WP7, WP8	All	5	4	3	6	90	Contact automotive and suppliers' industry for availability regarding AV technical requirements and PT specifications; look for examples of international go-to-market and product deployment in Asia and US.
5.	[pre-existing] Technical readiness of vehicles for safe operation on public roads not given in due time of the project pilots.	Technical Operational	Smaller fleets; limited value added and impact.	Insufficient planning in combination with COVID-19 effects. Delay in type approvals.	During technical validation and pre-demo phases (within 2021).	WP7	Potentially all	7	5	3	4,5	131,25	Replace vehicles or perform field trials with some of them being ready, perform some complex and high speed UCs in controlled environment (i.e. in JRC) or joining later the plan, transfer of know-how and products from external sites, including the extra European twinning ones.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
6.	[pre-existing] Parallelisation of simulation models: risks related to capability for massive parallelisation of the simulation models. Further, risks related to the challenge for proper configuration (e.g., vehicle segment, environmental condition, proper	Technical	Unsuccessful projection of results or projection under assumptions.	Technical inevitable difficulties; lack of data; lack of necessary effort by adequate Partners in the respective tasks.	During construction of the simulation environments and as revealed in first data feeding pool from the sites.	WP10	Potentially all. Greater danger for French and Spanish site lacking Partners with effort on simulation.	3,5	4	4	3	49	Clear reporting of underlying hypothesis and limitations. Use of several complementary models and work on models iteratively during the project (using pilot data from pre-pilot and early pilot results) to gradually achieve improved model accuracy. Exploration of additional data feeding pools external to the project (i.e. from AVENUE project on DRT).

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	velocity), thus reducing accuracy of the results.												
7.	[pre-existing] Security issues related to data transfer and use.	Technical	Security threats; liability issues; safety hazards; all creating further trust issues.	Insufficient specification and/or implementation of cybersecurity mechanisms.	During technical validation phase (it is one of the distinct layers of technical validation).	WP4	All	7	5	5	3	140	Through the standard compliant cybersecurity mechanisms of WP4.
8.	[pre-existing] AI algorithms not leading to improved or acceptable operational schemes.	Technical	No enhanced services emerging as an outcome of SHOW.	Technical fact. May be due to several reasons; insufficient basis provided by the sites; insufficient data, etc.	During development phase.	WP5	Potentially all.	6	5	4	4	120	Several algorithms will be employed within WP5 and the best will undergo iterative optimization. Nevertheless, the optimized/standard services will be used as default in case of suboptimal algorithmic performance.
9.	[pre-existing] Not enough	Technical	No enhanced services	Actual data missing (due to	During development phase.	WP5, WP10	Potentially all	7	6	3	3	126	The relevant activities (WP5 and W10) will use pre-Pilot data (from

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	or compatible data from previous research to develop AI algorithms and/or train simulation tools.		emerging as an outcome of SHOW.	insufficient recording mechanisms, etc.) and/or unwillingness to share them.									WP11) and intermediate sets of data from real-life tests. The Gantt Chart allows for such a delay; since the duration of the WPs extends to Month 40 and 46 respectively; to allow pre-Pilot and intermediate real-life demo results to be integrated/used before final application. In addition, external to SHOW, data pools will be explored from other initiative, taking advantage also of the twinning sites.
10	Insufficient localization on the test route.	Technical	High degree of localization uncertainty potentially creating safety risks and services	Poor GNSS-RTK localization.	Intention to be detected throughout the validation phase, before starting the actual field trials and	WP11, WP12	Austrian site; potentially all.	5	5	3	3	75	Adaptation of the used method; exploration of other possible localisation methods exploiting the cooperative context.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
			insufficient operation.		apply corrective actions in time.								
11	Insufficient 4G coverage on the test route.	Technical	High degree of localization uncertainty potentially creating safety risks and services insufficient operation.	Poor 4G coverage.	Intention to be detected throughout the validation phase, before starting the actual field trials and apply corrective actions in time.	WP11, WP12	German site; potentially all.	6	5	3	4	105	Identification of factors that lead to poor 4G coverage; review of measurements which lead to a better 4G coverage.
12	[pre-existing] Lack of will of PTAs/PTOs to create common business models for PT and non	Operational	Endangered real life deployment - decreased impact brought by the project.	Benefits and value added have not been made evident or are not enough. Promotion and	Progressively, during the entire project lifespan, throughout physical and virtual events, surveys	WP2	All	5	5	5	4,5	118,75	Analyse power and interests of relevant stakeholders to classify them into roles of Latent, Promoter, Apathetic or Defender towards certain business models and solutions and set up an adequate communication strategy. If not yet

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	PT mobility services disrupting the current state of art/ business.			awareness strategies have not been adequate.	and interviews. Still, more evidently, during demonstration phases.								available, create a comprehensive integrated mobility strategy for each of the participating cities, regions and stakeholder eco-systems in the course of the project.
13	[pre-existing] The Marketplace fails to integrate the services and systems under the common SHOW approach.	Operational	Individual decentralised deployment of services instead	Different, not aligned service definition.	During development/integration.	WP6	All	5	4	4	5	90	Through iterative and agile-like approaches, SHOW will adopt standardized and widely accepted technologies for the common APIs, protocols to be used in order to allow different systems to connect to the Marketplace. Moreover, the necessary documentation and SDKs will be provided to allow external stakeholders to seamlessly integrate with the SHOW solution.
14	[pre-existing] Lack of	Operational	Barriers to wide deployment	Current practice proving	During preparation phase in	WP12, WP14, WP17	Potentially all, slightly	6	6	4	4	144	Establishment of a competence group within the framework of SHOW

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	adoption of the guidelines / lack of implementation resources & competence in the public sector or other stakeholders.		, exploitation and replication.	stronger; delayed digestion of changed and harmonised processes; resources issues; COVID-19 effects.	view of pre-demonstration phase but also and mainly during replication phase towards the end of the project.		more probably for satellite non-commercial sites.						(possibly led by UITP in the context of WP14/WP17), which will be also available after the end of the project. Tight coordination of local demo communities
15	[pre-existing] Lack of endorsement for the regulatory and operational guidance and recommendations.	Operational	Lack of interoperability; limited impact of SHOW in Europe and beyond; lessons learned remaining unused.	Insufficient engagement strategies and mechanisms; not useful enough DSS tools; market and society unreadiness to CCAV encompassing also	During replication and exploitation phase of the project.	WP17	Potentially all, but also external to SHOW sites aiming to host replication of its solutio	7	5	3	4	122,5	This can be averted by combining different quantitative and qualitative research methodologies (online consultation, interviews, focus group meetings), by involving and engaging all relevant stakeholders (operators, industries, research) and by presenting and debating draft conclusions at SHOW

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
				changing policies respectively.			ns and lessons learned.						stakeholder forum meetings.
16	[pre-existing] Lack of data and info exchange between different Partners in the value chain may prevent integrated shared mobility services (PT and non-PT).	Operational	Limited impact and value added; limited demonstration of shared CCAV with subsequent effects in data.	Not well advanced and tight local ecosystems and business models.	During pre-demonstration phase.	WP2, WP9, WP11	Potentially all	6	5	4	4	120	Pre-agreed data exchange through local sites Partnerships with all key actors (private and public) linked by contracts and MoU's in the context of A9.1: Plans for pilot evaluation and A9.3: Users engagement and co-creation initiatives. Possibility to integrate new actions or transfer Pilot site UCs in case of local suboptimal integration (to be reported and decided within WP9 – A9.1). Tight coordination of local demonstration boards. Identification of tight ecosystems and adequate business models for them.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
17	[pre-existing] Non compatible operation plans of mixed passenger cargo UC's	Operational	Failure to fully demonstrate the specific Use Case.	Technical and operational difficulties. Low interest on behlaf of the City..	During pre-demonstration phase (for the first time).	WP11, WP12	Karlsruhe, Rennes.	6	6	4	4	144	The ability to combine it will be demonstrated. If needed, everyday operation will be decoupled and the common vehicle will be used either for passenger or for cargo transportation, at different timeframes of the Pilot.
18	[pre-existing] Lack of sufficient traffic demand for platooning UC.	Operational	Limited demonstration, and, consequently relevant results availability and impact shown.	Inherent to the ecosystem, traffic and mobility context and culture of each City.	During pre-demonstration phase (for the first time).	WP11, WP12	Karlsruhe, Madrid, Brainport, Trikala	5	4	4	4	80	The ability of this functionality will be demonstrated; even if used not frequently/ regularly at everyday operations during the Pilot.
19	[pre-existing] Operators of PT at Pilot sites not ready to apply safely and	Operational	Unsuccessful demonstration of use cases and selected business and	Lack of awareness and skills required.	During pre-demonstration phase (for the first time).	WP15	Potentially all.	6	4	3	3	72	To be resolved through appropriate training session (WP15).

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	efficiently the new AV-based operational schemes.		operational business models.										
20	[pre-existing] Business models influenced and challenged by unexpected emerging competing services by third parties.	Operational	Disturbance in field trials process and local ecosystems functioning.	Competitive market by nature.	During pre-demonstration phase (for the first time).	WP4, WP6	Potentially all	5	4	4	3	70	Relevant activities range over the whole project duration and will be open to external stakeholders; ready to establish local alliances to emerging services (through the open architecture and API's of WP4 and WP6). That is also why the final Architecture is delayed until Month 36 of the project; to allow integration of emerging key services/ business models during project execution.
21	Exceeding the capacity of JRC to test the vehicles during	Operational	Delays in or incomplete vehicle validation.	The capacity of JRC for testing vehicles is limited by	Depending on the time needed for validation. Ideally, the risk should	WP11	JRC	6	4	3	3	72	Maintaining clarity among the partners regarding available testing time slots, for example by using a scheduling calendar

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	technical validation phase.			the available infrastructure and timeslots. In case of multiple requests to test vehicles in the same period this capacity might be exceeded. In addition, the specific infrastructure deemed necessary for some specific validation purposes might not be present at JRC site.	be detected and resolved before the start of actual validation phase (A11.1)								available openly to everyone. Keeping a buffer timeslot for emergency cases, e.g. when some extra testing is needed. Providing a clear list of available tests and infrastructure by JRC. Obliging the partners to provide at least a draft list of the planned validation activities before reserving the testing timeslot.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
22	Covid-19 related cross-cutting effects.	Operational	Delays in vehicle procurements and type approvals, permit processes, development and validation phases' execution. Changes in demo sites creating further delays. Economic crisis affecting demo sites resulting in even more further delays. Constraints regarding	Due to mobility restrictions it might be not allowed to move vehicles or the vehicle operators to the test site. Field trials themselves may be hindered. Working routines, development and permit processes may be delayed. Logistics affecting development and trials are also hindered.	Monitored continuously, depending on the evolution of pandemic situation and related restrictions.	All, specifically SP2 and SP3 WPs.	Potentially all.	7	8	4	5	252	For vehicle operators, it might be possible to organise some part of the training remotely. For vehicle validation, possible to determine some emergency testing sites in case moving the vehicle to JRC is not possible. Vice versa, JRC site may serve as a back-up site for pre-demo activities. Ad-hoc solutions depending the specific site challenges emerging. If those fail and depending the size of pandemic evolution, short extension of the project duration should be considered.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
			transport of passengers (allowed number of passengers).										
			Delay in the start of pre-demo and demonstrations	No demonstration or restricted driving period	Delayed evaluation of services/vehicle	WP1, WP9, WP12	All	6	7	4	5	189	
23	[pre-existing] Liability and ownership of data produced as well as liability of services that are built based on these data.	Legal/ Regulatory	Barriers to deployment and exploitation	Common "global" challenge regarding data. Regulatory and IPR issues not clarified in advance.	During Data Management Plan and Data Protection Impact Assessment subsequent versions issue. Also through deployment of data for several purposes in	WP3, WP11, WP12, WP13, WP14	All	4	4	4,5	4	68	The specific issue will be tackled through the recently awarded EASME tender on Big Data, whose results will be capitalised also in SHOW. In addition legal and liability issues will be dealt thoroughly and across countries within SHOW in the context of WP3 and WP14 primarily. Progressive clarification will emerge in Data Management Plan and Data Privacy

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
					the project different phases (demonstration, evaluation, impact assessment).								Impact Assessment subsequent versions.
24	[pre=existing] Policy Regulation for vehicle approval is not harmonized throughout the different countries.	Legal/ Regulatory	Not direct effect in SHOW as demonstration is not cross-border. May affect only fleet parts that may travel and deployed to more than one countries which will be rare cases, if	New sector with inevitable gaps in regulations.	During permit authorisation phase prior to pre-demonstration.	WP3, WP11, WP12	All	5	5	3	5	100	Align with national and international initiatives for Automated Driving regulatory frameworks, e.g. Vienna Agreement updates, EU, ECE, etc. The strong support of many national authorities in the project facilitates the emergence of national regulations. One of the concrete tasks in the project is exactly the issue of recommendations on harmonised regulations in near future that is tackled by

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
			any. Other than that, it constitute a serious challenge for CCAV deployment overall across Europe..										AUSTRIATECH and EUROCITIES in A3.1 and A3.3 respectively. In the meanwhile in the project, an attempt is being made for each demo site to align and fulfil primarily the national requirements in order to proceed with demonstration; still, learning from other sites. This process is being handled in A3.1.
25	[pre-existing] Sentiment analysis (of A1.2) not possible to be legally performed in third party social media.	Legal/ Regulatory	Not the broadest possible impact that could be achieved.	IPR	During second year of the project that the tools will start being deployed.	WP1	N/A	4	4,5	2,5	3	49,5	To be performed in project's own social media.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
26	Lack of a clear governance on mobility data encompassing lack of level playing field in data sharing (the user of the data should share back the enriched data).	Legal/ Regulatory Technical	Unsuccessful utilisation of data for feeding all the different tasks (services and modules operation, evaluation, simulation and impact assessment).	Not clear picture on all the data types and the feasibility to get them. IPR issues. Unwillingness to share and abide to centralised principles of the project.	During development phase (in first place).	SP2 (WP4-WP8)	All	6	6	3,5	4	135	A unified data requirements list is being already constructed in the project under the auspices of the Technical Manager in order to allow a consistent operation during the project. Ad hoc solutions will be sought whenever specific problems are emerging.
27	Lack of consumer protection.	Legal/ Regulatory	Low penetration and user acceptance - complaints and problems in field trials execution.	Some pilot sites are not mature enough to have already established mechanisms to address this part.	During development phase (in first place).	WP11, WP12	Potentially all	5	4	3	4	70	Regulatory bodies will be defined as part of pre-commercial deployment in the pilot sites. This is upon the responsibility of the local demo communities.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
28	Test permits are not issued in time.	Legal/ Regulatory	Delay in the start of pre-demo and/or demonstration phases or shortened pre-demo and/or demonstration phases or no pilot demonstrations possible at all at specific sites.	The requirements to be met for issuing the test authorisation are not met (or are not met in time). COVID-19 related effects in combination with cumbersome national regulations.	From the first year of the project when the permit processes have started.	WP3, WP11, WP12	Eindhoven/Brainport; Copenhagen sites; potentially more.	6	5	2,5	4	97,5	Ongoing exchange with the authorities from the very beginning of the project that provide the test authorisation. Continuous monitoring and support of the test sites under WP3 (A3.1) of the project.
29	[pre-existing] Low traveller acceptance and trust issues, services underuse	Behavioural	Insufficient data availability for robust SHOW evaluation and impact assessment. Barriers	Ineffective user and stakeholder engagement strategies for SHOW demonstration; ineffective	During pre-demonstration phase for the first time in the project.	WP7, WP9, WP11, WP12	All	6	5	3	4	105	Emphasis is put within WP7 to enhance user experience inside the vehicle as well as the interface towards other travellers and the vehicles; to alleviate safety and security fears. The control tower

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	and non-sustainable operation.		to deployment, exploitation and replication.	engagement of local demonstration boards in SHOW; insufficient level of solutions offered; generic challenges regarding CCAV trust beyond SHOW.									concept and the direct link to teleoperation centre (including "driver" avatars on board) are expected to help. Also, citizen engagement strategies of A9.3 and the tight coordination of demo communities in the context of WP12 aim to help in this direction.
30	[pre-existing] Contradicting needs and wants of AV's HMI between different vendors and Pilot sites.	Behavioural Operational	No serious risk - there is room for alternative strategies among different vendors.	Alternative strategies among vendors.	During development phase.	WP7	Potentially all.	3	6	2	4	54	Different ones will be applied and then benchmarked between then and with SoA. WP7 (A7.4: HMI & Control/Handover strategies) will provide just the framework, some recommended elements, principles and guidelines but will allow each vendor/site to follow its own "look and feel".

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
31	[pre-existing] Different user clusters require fundamentally different HMI's.	Behavioural	Greater effort than planned for addressing all potential user clusters.	Wide spectrum of user needs and preferences.	During development phase (in first place).	WP7	Potentially all	5	6	3	3	90	Partially covered through A7.4 HMI adaptability and personalisation.
32	Misunderstandings due to lack of common vision, definitions and terminology.	Behavioural	Inefficient team work resulting in delays and insufficient results.	Unforeseen critically safety events.	During pre-demo phase in first place.	All	Potentially all.	6	5	5	4	135	Regular technical (virtual) meetings, daily monitoring and technical management constantly creating and maintaining liaisons and synergies, common glossaries (A1.1) and cross-cutting reference documentation (e.g. unified data list), etc.
33	[pre-existing] Characteristics of each Pilot site must be critically reviewed in advance in	Demonstration/Evaluation	Inconsistency in results.	Inconsistent evaluation framework.	During the first year of the project while the evaluation framework is being prepared.	WP9	Potentially all	5	5	4	4	100	Through the common parametric evaluation framework of D9.1.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	order to ensure results compatibility.												
34	Validation and commissioning framework unsuitable for specific pilot sites.	Demonstration/Evaluation	Some of the functions and services left out during validation phase. In consequence, this might cause malfunctions during pre-pilot/pilot phase.	WP11 assumes developing a single generic validation and commissioning framework to be applied to all pilot sites, which brings potential risk of not covering certain site-specific aspects.	Before the approval of the final version of the technical validation framework.	WP11	Not yet known which ones.	5	5	3	3	75	Strong involvement of all the pilot sites in preparation and revision of the validation framework, peer-reviews.
35.	Accidents (e.g.	Demonstrati	Decommissioning of	Unforeseen critically	During pre-demo	WP11, WP12	Potentially all.	6	5	3	5	120	Robust and as complete as possible technical

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	incidents with specific type of vehicle) having a negative popularity impact for the project overall and on other sites as well.	on/Evaluation	certain type/brand of vehicles or specific use cases execution at all sites for a period of time.	safety events.	phase in first place								validation. Lessons learned exchanged from one site to another from the beginning. Rehearsal and in-depth walk through with professionals prior to pre-demo phase in each site.
36	Test routes are not available as planned or cannot be equipped with C-ITS and other infrastructure as planned.	Demonstration/Evaluation	Delay in the start of pre-demo and/or demonstration phases or shortened pre-demo and/or demonstration phases.	Lack of cooperation from the authorities, infrastructure along the route not operational; Limited financial resources available.	Continuous monitoring and negotiations since the very beginning of the project.	WP11, WP12	Potentially all.	6	5	2	4	90	Search for alternative test routes. Continuous discussions and flexibility in procurement. Smarter utilisation of infrastructure equipment.
37	Insufficient numbers of	Demonstrati	Delay in the start of pre-	Limited financial	Continuous monitoring	WP11, WP12	Potentially all.	6	4,5	3	4	94,5	Early awareness and engagement campaigns

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
	safety operators can be recruited.	on/Evaluation	demo and/or demonstration phases or shortened pre-demo and/or demonstration phases.	and time resources available.	and negotiations since the very beginning of the project.								in each site to recruit safety operators, comprehensively advertising of the vacant positions.
38	The target duration of demonstration phases cannot be reached.	Demonstration/Evaluation	The targets of the GA cannot be met. The tests are not carried out in full.	Shuttles are only available for a shorter period than planned, test permit is issued for a limited time period, weather conditions do not allow for continuous testing. COVID-19	Made evident during the second year of the project.	WP11, WP12	Potentially all.	6	6,5	3	4	136,5	Flexibility in the conduction of the field trials; short extension of the project; identification of further metrics for success of demonstration activities (e.g. number of trips conducted).

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
				related effects.									
39	Low number of passengers	Demonstration/Evaluation	Cannot reach the number of passengers stated in the GA; no effect on the technical performance, however, proved impact will be less significant.	COVID-19 related effects in combination with ineffective awareness and engagement strategies in local sites.	During pre-demo phase in first place.	WP9, WP11, WP12, WP15	Potentially all.	6	6	3,5	4	135	Effective awareness and engagement campaigns. More intense engagement of fewer users as a back-up plan. Recruitment of users from the extended SHOW Consortium.
40	Critical changes in vehicles or demo sites plans - unavailability of vehicles, cities segments, etc.	Demonstration/Evaluation	Risk of need to change a part of the pilot.	COVID-19 related effects mainly.	Continuous monitoring since the very beginning of the project.	WP11, WP12	Eindhoven/Brainport; Copenhagen sites; Austrian site; potenti	6	7	3	5	168	Recognition of mitigation actions ad-hoc depending the case.

#	Definition of Risk	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Relevant site(s)	(Averaged) Risk Severity	(Averaged) Risk Occurrence Probability	(Averaged) Risk Detectability	(Averaged) Risk Recoverability	Consolidated Overall RN	Risk Mitigation Measures
							ally more.						

7.5 Future steps

As mentioned, the risk assessment in SHOW project across all applicable aspects, is a living process. While the first one, reported in this Deliverable, compiles the results of the one held in 2020 in view of the technical validation phase, its next iteration will take place within 2021 in view of the pre-demonstration phase that will be launched in all the sites, with the aim to pre-identify potential risks and apply in advance corrective actions prior to their materialisation to the maximum possible degree.

While in this first round of the risk assessment, the risks encountered were more generic and common across the pilot sites of the project, while the project progresses and the implementation and site preparation phases are intensified, the site-specific technicalities and details will be become more evident and will most probably differentiate to each other. As such, and while expecting the first pilot phase of the project, the next round of the risk assessment will be applied on horizontal level for the common to all issues (e.g., central digital infrastructure of the project, communication and visualisation) but also on Mega and Satellite site level in order to reveal and mitigate the specific to each context risks.

In addition, future risk assessment rounds may reveal the need for identifying more materialisation areas, for example, business and exploitation related risks will be definitely added in a more targeted way at some point in the process, though this is a rather early stage for this and as such they are included in the general operational risks category. Finally, in the next risk assessment rounds, the consolidated results will be acknowledged to the Advisory Board of the project in order to get their insight, in specific about the mitigation strategies recognised.

Future reporting, and depending on the time evolution of the pilots in the project, will follow in the upcoming *D4.3: Open modular system architecture - second version (ICCS, M24)* and *D4.4: Open modular system architecture - third version (ICCS, M36)*.

8 Conclusions and outlook

The dual target of this work was:

a. to design a modular inclusive architecture which can efficiently integrate with existing local autonomous transportation systems and PT backend systems and provides the implementation framework that supports the design of the SHOW integrated system **represented by architecture variations I and II**. this work focused on the SHOW central service-oriented cloud subsystem, i.e. the SHOW cloud Mobility Data Platform (SMDP). This included:
    i. the SMDP high-level design (detailed design is provided in SHOW D5.1 [19])
    ii. designing the secure integration of SHOW demonstration sites' connected Things (SHOW set of Things include CAVs fleet, smart city RSU nodes, commuters and other road users with the ability to connect to the SHOW integrated system);
    iii. designing the secure integration with the local CAV fleet management system that monitors the fleet and offers PT services for CAVs;
    iv. designing the layer of novel CCAM services on top of the SMDP. This includes a central reference Dashboard designed as SHOW web-service and described in a dedicated chapter of this deliverable (chapter5)
    v. designing the integration of relevant open data sources as well as SHOW generated data from simulations and user surveys

b. the design of a future-proof modular service-oriented architecture for EU-wide CCAM services' provision, **represented by architecture variations II and III**. Aspects of open data access for safety-critical in vehicle applications have been identified and solutions discussed.

In this deliverable, the SHOW reference architecture representing the high level functional requirements of the system is presented while communication, interoperability and cyber-security mechanisms addressing non-functional horizontal requirements are derived (chapters 3 and 4). In addition, a dedicated chapter is devoted to the SHOW reference Dashboard implementation (chapter5) while another chapter is reserved for adding two architecture deployment views corresponding to two of the SHOW CCAM envisioned services as a means of projecting the reference architecture on a service-oriented implementation level which also allowed to define the required data to be exchanged (chapter6).

The work of D4.1 will be continued and refined during the next two years of the project mainly focusing on the local implementations in the SHOW demonstration sites by:

- providing architecture deployment views based on a selected use case or service
- monitoring and supporting the implementation of communication protocols (MQTT and HTTPS are the main mechanisms proposed by D4.1)
- monitoring and supporting the implementation of cross-layers' cybersecurity and interoperability mechanisms applied
- contributing to the SHOW data content and format specification work (work in progress in collaboration with SP2 and SP3 of the SHOW project)
- monitoring all technical risks stemming from the implementation of the integrated SHOW system in all SHOW demo sites.

Future results will be reported in the upcoming *D4.3: Open modular system architecture - second version (ICCS, M24)* and *D4.4: Open modular system architecture - third version (ICCS, M36)*.

References

[1] SHOW (2020) D1.2: SHOW Use Cases. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

[2] EC, White paper, Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system, 2011.

[3] Osama Al-Gazali, Josef Kaltwasser, D2.5 (public), C-ITS standardization requirements for the urban environment, CIMEC EU project, 2016.

[4] Q. Zhang *et al*., "OpenVDAP: An Open Vehicular Data Analytics Platform for CAVs," *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, 2018, pp. 1310-1320, doi: 10.1109/ICDCS.2018.00131.

[5] Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles, SAE J3216, May 2020.

[6] Datta, S. K., & Bonnet, C. (2018, May). Advances in web of things for IoT interoperability. In 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW) (pp. 1-2). IEEE

[7] Daoud, Alaa. "Semantic Web Environments for Multi-Agent Systems: Enabling agents to use Web of Things via semantic web." arXiv preprint arXiv:2003.02054 (2020).

[8] Kovatsch, M., Matsukura, R., Lagally, M., Kawaguchi, T., Toumura, K., & Kajimoto, K. (2020). Web of Things (WoT) Architecture, W3C Recommendation 9 April 2020. W3C Recommendation. World Wide Web Consortium (W3C), Apr.

[9] Blackstock, M., & Lea, R. (2013, September). Toward interoperability in a web of things. In Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication (pp. 1565-1574)

[10] Mathew, S. S., Atif, Y., Sheng, Q. Z., & Maamar, Z. (2013). The web of things-challenges and enabling technologies. In Internet of things and inter-cooperative computational technologies for collective intelligence (pp. 1-23). Springer, Berlin, Heidelberg.

[11] Patel, P., Ali, M. I., & Sheth, A. (2018). From raw data to smart manufacturing: AI and semantic web of things for industry 4.0. IEEE Intelligent Systems, 33(4), 79-86.

[12] Sciullo, L., Aguzzi, C., Di Felice, M., & Cinotti, T. S. (2019, January). WoT store: Enabling things and applications discovery for the W3C Web of Things. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-8). IEEE.

[13] Datta, S. K., Da Costa, R. P. F., Bonnet, C., & Härri, J. (2016). Web of things for connected vehicles. In International world wide web conference (pp. 1-3).

[14] Datta, S. K., Härri, J., & Bonnet, C. (2018, November). IoT platform for precision positioning service for highly autonomous vehicles. In 2018 22nd International Computer Science and Engineering Conference (ICSEC) (pp. 1-6). IEEE.

[15] Storck, C. R., & Duarte-Figueiredo, F. (2020). A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles. IEEE Access, 8, 117593-117614.

[16] Guevara, L., & Auat Cheein, F. (2020). The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. Sustainability, 12(16), 6469.

[17] Yu, K., Lin, L., Alazab, M., Tan, L., & Gu, B. (2020). Deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in a 5G-enabled intelligent transportation system. IEEE Transactions on Intelligent Transportation Systems.

[18] Yu, H., Lee, H., & Jeon, H. (2017). What is 5G? Emerging 5G mobile services and network requirements. Sustainability, 9(10), 1848.
[19] SHOW (2021). D5.1: Big Data Collection Platform and Data Management Portal. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.
[20] Kaur, A., Kaushik, S., Bajpai, R., & Gupta, N. (2020, October). Performance Analysis of Millimeter-Wave Based Device-to-Device Communications System. In 2020 27th International Conference on Telecommunications (ICT) (pp. 1-4). IEEE.
[21] Li, Z., Xiang, L., Ge, X., Mao, G., & Chao, H. C. (2020). Latency and Reliability of mmWave Multi-Hop V2V Communications Under Relay Selections. IEEE Transactions on Vehicular Technology, 69(9), 9807-9821.
[22] Antonescu, B., Moayyed, M. T., & Basagni, S. (2017, October). mmWave channel propagation modeling for V2X communication systems. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-6). IEEE.
[23] Anjinappa, C. K., & Guvenc, I. (2018, August). Millimeter-wave V2X channels: Propagation statistics, beamforming, and blockage. In 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall) (pp. 1-6). IEEE.
[24] Martin-Vega, F. J., Aguayo-Torres, M. C., Gomez, G., Entrambasaguas, J. T., & Duong, T. Q. (2018). Key technologies, modeling approaches, and challenges for millimeter-wave vehicular communications. IEEE Communications Magazine, 56(10), 28-35.
[25] Mustakim, H. U. (2020). 5G Vehicular Network for Smart Vehicles in Smart City: A Review. Journal of Computer, Electronic, and Telecommunication, 1(1).
[26] Feng, J., Shi, Z., & Ma, S. (2016, December). Sum rate of full-duplex two-way massive MIMO relay systems with channel aging. In 2016 IEEE International Conference on Communication Systems (ICCS) (pp. 1-6). IEEE.
[27] Vieira, J., Malkowsky, S., Nieman, K., Miers, Z., Kundargi, N., Liu, L., ... & Tufvesson, F. (2014, December). A flexible 100-antenna testbed for massive MIMO. In 2014 IEEE Globecom Workshops (GC Wkshps) (pp. 287-293). IEEE.
[28] Van der Perre, L., Liu, L., & Larsson, E. G. (2018). Efficient DSP and circuit architectures for massive MIMO: State of the art and future directions. IEEE Transactions on Signal Processing, 66(18), 4717-4736.
[29] Björnson, E., Sanguinetti, L., Wymeersch, H., Hoydis, J., & Marzetta, T. L. (2019). Massive MIMO is a reality—What is next?: Five promising research directions for antenna arrays. Digital Signal Processing, 94, 3-20.
[30] Kang, H., Montejo-Sánchez, S., Azurdia-Meza, C. A., & Céspedes, S. (2019, August). Beamforming for Beaconing in V2V Communications. In 2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON) (pp. 1-4). IEEE.
[31] Molisch, A. F., Ratnam, V. V., Han, S., Li, Z., Nguyen, S. L. H., Li, L., & Haneda, K. (2017). Hybrid beamforming for massive MIMO: A survey. IEEE Communications Magazine, 55(9), 134-141.
[32] Di, B., Song, L., Li, Y., & Li, G. Y. (2017, December). NOMA-based low-latency and high-reliable broadcast communications for 5G V2X services. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.
[33] Tang, Z., & He, J. (2020, September). NOMA enhanced 5G distributed vehicle to vehicle communication for connected autonomous vehicles. In Proceedings of the ACM MobiArch 2020 The 15th Workshop on Mobility in the Evolving Internet Architecture (pp. 42-47).
[34] Liu, Y., Zhang, H., Long, K., Nallanathan, A., & Leung, V. C. (2019). Energy-efficient subchannel matching and power allocation in NOMA autonomous driving vehicular networks. IEEE Wireless Communications, 26(4), 88-93.
[35] Chekired, D. A., Togou, M. A., Khoukhi, L., & Ksentini, A. (2019). 5G-slicing-enabled scalable SDN core network: Toward an ultra-low latency of autonomous

driving service. IEEE Journal on Selected Areas in Communications, 37(8), 1769-1782.
[36] Campolo, C., Molinaro, A., Iera, A., & Menichella, F. (2017). 5G network slicing for vehicle-to-everything services. IEEE Wireless Communications, 24(6), 38-45.
[37] H2020. (2020). The Avenue Project. The Avenue Consortium. https://h2020-avenue.eu/.
[38] H2020. (2020). The DIAS Project. The DIAS Consortium. https://cordis.europa.eu/project/id/814951
[39] H2020. (2020). A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles. https://cordis.europa.eu/project/id/833742
[40] EVITA. (2020). Henniger, Olaf. EVITA, evita-project.org/.
[41] BMW. (2020). Innovation, www.bmwgroup.com/en/innovation.html.
[42] BOSCH. (2020). Automated Mobility, www.bosch-mobility-solutions.com/en/highlights/automated-mobility/.
[43] H2020. (2020). The CARAMEL project. “Artificial Intelligence Based Cybersecurity for Connected and Automated Vehicles.”. www.h2020caramel.eu/.
[44] Check Point Software technologies LTD. (2020). Cyber Security Report. https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf
[45] Luke Irwin. (2020). List of data breaches and cyber-attacks in July 2020 – 77 million records breached. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-july-2020
[46] Lily Hay Newman. (2020). The Worst Hacks and Breaches of 2020 So Far. Wired. https://www.wired.com/story/worst-hacks-breaches-2020-so-far/
[47] National Security Agency. (2020). Mitigating Cloud Vulnerabilities .https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
[48] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546-556, April 2015, doi: 10.1109/TITS.2014.2342271.
[49] Edward Jones. (2020). A Comprehensive Guide to Cloud Security in 2020 (Risks, Best Practices, Certifications).Kinsta. https://kinsta.com/blog/cloud-security/
[50] Eric Knorr. (2020). Cyber security in 2020: From secure code to defence in depth. https://www.csoonline.com/article/3519913/cybersecurity-in-2020-from-secure-code-to-defense-in-depth.html
[51] Oracle.(2020).MODERN-Defense-In-Depth.-Oracle. https://www.oracle.com/a/ocom/docs/security/modern-defense-in-depth.pdf
[52] McKinsey and Company. (2020). Cyber security in automotive. https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf
[53] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy (Vol. 99). Technical report.
[54] Bace, R. G., & Mell, P. (2001). Intrusion detection systems.
[55] Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124.
[56] Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. D. (2015, January). An intrusion detection system against malicious attacks on the communication network of driverless cars. In 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC) (pp. 916-921). IEEE.
[57] Panigrahi, R., & Borah, S. (2018). A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. *International Journal of Engineering & Technology*, *7*(3.24), 479-482.
[58] Yang, L., Moubayed, A., Hamieh, I., & Shami, A. (2019, December). Tree-based intelligent intrusion detection system in internet of vehicles. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[59] Van Wyk, F., Wang, Y., Khojandi, A., & Masoud, N. (2019). Real-time sensor anomaly detection and identification in automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 21(3), 1264-1276. Source to be deleted
[60] Bezemskij, A., Loukas, G., Anthony, R. J., & Gan, D. (2016, December). Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle. In 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS) (pp. 61-68). IEEE.
[61] Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M., & Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. Information Sciences, 513, 386-396.
[62] Thing, V. L., & Wu, J. (2016, December). Autonomous vehicle security: A taxonomy of attacks and defences. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 164-170). IEEE.
[63] El Kamel, N., Eddabbah, M., Lmoumen, Y., & Touahni, R. (2020). A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning. Security and Communication Networks, 2020.
[64] Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020, June). Evaluation of machine learning algorithms for anomaly detection. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.
[65] H2020. (2020). SAFERtec project. Security Assurance FramEwoRk for neTworked vEhicular technology. https://www.safertec-project.eu/
[66] H2020. (2020). SURE project. Safe Unmanned Robotic Ensembles. https://www.tudelft.nl/en/3me/about/departments/delft-center-for-systems-and-control/
[67] United States Department of Transportation. (2020). NHTSA project. National Highway Traffic Safety Administration. https://www.nhtsa.gov/
[68] H2020. (2020). E-CORRIDOR project. Edge enabled Privacy and Security Platform for Multi Modal Transport. https://e-corridor.eu/
[69] European Union Agency For Cybersecurity. (2020). ENISA project. https://www.enisa.europa.eu/
[70] Reich, T., Budka, M., Robbins, D., & Hulbert, D. (2019). Survey of ETA prediction methods in public transport networks. arXiv preprint arXiv:1904.05037.
[71] Lin, W. H., & Zeng, J. (1999). Experimental study of real-time bus arrival time prediction with GPS data. Transportation Research Record, 1666(1), 101-109.
[72] Kumar, B. A., Kumar, V., Vanajakshi, L., & Subramanian, S. C. (2017). Performance comparison of data driven and less data demanding techniques for bus travel time prediction. EUROPEAN TRANSPORT-TRASPORTI EUROPEI, (65).
[73] Maiti, S., Pal, A., Pal, A., Chattopadhyay, T., & Mukherjee, A. (2014, October). Historical data based real time prediction of vehicle arrival time. In 17th International IEEE Conference on Intelligent Transportation Systems (ITSC) (pp. 1837-1842). IEEE.
[74] Xinghao, S., Jing, T., Guojun, C., & Qichong, S. (2013). Predicting bus real-time travel time basing on both GPS and RFID data. Procedia-Social and Behavioral Sciences, 96, 2287-2299.
[75] Alonso-Mora, J., Wallar, A., & Rus, D. (2017, September). Predictive routing for autonomous mobility-on-demand systems with ride-sharing. In 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (pp. 3583-3590). IEEE.
[76] Simonetto, A., Monteil, J., & Gambella, C. (2019). Real-time city-scale ridesharing via linear assignment problems. Transportation Research Part C: Emerging Technologies, 101, 208-232.

[77] NYC Taxi and Limousine Commission dataset: https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page
[78] Cyber Security for Connected and Autonomous Vehicles: https://sites.google.com/view/cav-cyber-sec
[79] RESTful API team, (last access 19 November 2020). What is REST. Available online. https://restfulapi.net/
[80] M. Kovatsch, R. Matsukura, M. Lagally, T. Kawaguchi, K. Toumura, K. Kajimoto. (9 April 2020). Web of Things (WoT) Architecture. Available online: https://www.w3.org/TR/wot-architecture/
[81] MQTT Version 5.0. Edited by Andrew Banks, Ed Briggs, Ken Borgendale, and Rahul Gupta. (07 March 2019). OASIS Standard. https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html. Latest version: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html.
[82] Ian Skerret. (2020, 29 October). Why MQTT has become the De Facto Sandard for the Connected Car. https://www.hivemq.com/blog/mqtt-standard-for-connected-car/
[83] HiveMQ Team (last access 2021, 15 January). Enabling the Connected Car with HiveMQ. https://www.hivemq.com/solutions/iot/enabling-the-connected-car/
[84] D. Hardt Ed. (2012). The OAuth 2.0 Authorization Framework. https://tools.ietf.org/pdf/rfc6749.pdf
[85] TheHiveMQ Team. (20 April 2015). HiveMQ – MQTT security fundamentals. https://www.hivemq.com/blog/introducing-the-mqtt-security-fundamentals
[86] S. Brown. (last access 11 January 2021). The C4 model for visualizing software architectrure. Available online: https://c4model.com/
[87] K. G. Zografos and K. N. Androutsopoulos, "Algorithms for Itinerary Planning in Multimodal Transportation Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 9, no. 1, pp. 175-184, March 2008, doi: 10.1109/TITS.2008.915650.
[88] Bekiaris, E., Stevens, A. (2005), "Common risk assessment methodology for advanced driver assistance systems", Transport Reviews, Vol. 25, No. 3, p. 283-292, May 2005.
[89] Best Practice for In-Vehicle Fallback Test Driver Selection, Training, and Oversight Procedures for Automated Vehicles Under Test, SAE Automated Vehicle Safety ConsortiumTM (AVSC), AVSC00001201911, 2019.

Appendix I: Mapping of pilot sites to SHOW Use Cases and UCs' prioritization (D1.2 extract)

Extracts from D1.2 SHOW Use Cases [1] included here for reasons of document's self-consistency.

Table 44: Prioritisation of SHOW single UCs

Essential	• UC1.1: Automated passengers/cargo mobility in Cities under normal traffic & environmental conditions. • UC1.2: Automated passengers/cargo mobility in Cities under complex traffic & environmental conditions. • UC1.6: Mixed traffic flows. • UC1.10: Seamless autonomous transport chains of Automated PT, DRT, MaaS, LaaS. • UC3.1: Self-learning Demand Response Passengers/Cargo mobility. • UC3.2: Big data/AI based added value services for Passengers/ Cargo mobility.
Secondary	• UC1.3: Interfacing non automated vehicles/ travellers (VRU). • UC1.4: Energy sustainable automated passengers/cargo mobility in Cities. • UC1.5: Actual integration to city TMC. • UC2.2: Automated mixed temporal mobility. • UC3.4: Automated services at bus stops.
Additional	• UC1.7: Connection to Operation Centre for tele-operation and remote supervision. • UC1.8: Platooning for higher speed connectors in people transport. • UC1.9: Cargo platooning for efficiency. • UC2.1: Automated mixed spatial mobility. • UC3.3: Automated parking applications. • UC3.5: Depot management of automated buses.

Table 45: Mapping of pilot sites to SHOW Use Cases

	UC 1.1	UC 1.2	UC 1.3	UC 1.4	UC 1.5	UC 1.6	UC 1.7	UC 1.8	UC 1.9	UC 1.10	UC 2.1	UC 2.2	UC 3.1	UC 3.2	UC 3.3	UC 3.4	UC 3.5
Mega Demonstration Sites																	
Rouen Pilot site	×	×	×	×	×	×	×			×			×			×	
Rennes Pilot site	×		×	×						×		×					
Linköping Pilot site	×		×			×	×						×	×		×	
Kista Pilot site	×	×	×			×	×									×	
Madrid Pilot site	×	×	×			×	×	×		×					×		×
Graz Pilot site		×	×													×	
Salzburg Pilot site		×	×		×	×							×				
Karlsruhe Pilot site	×	×	×			×	×		×		×	×					
Aachen Pilot site	×			×		×				×							
Braunschweig Pilot site (pending amendment)	×					×		×									
Satellite Demonstration Sites																	
Turin Satellite site		×	×		×		×			×							
Trikala Satellite site	×	×	×		×	×	×	×		×							
Tampere Satellite site	×	×		×			×						×				
Brainport Satellite site	×		×					×									
Brno Satellite site	×	×	×			×	×										
Copenhagen Satellite site	×	×	×	×	×	×	×						×	×		×	

Appendix II: IT standards used in PT tabulated

Table 46: Relevant standards used in PT focusing on road transport

Name	Status	Reference	Scope	Comment
NeTEx	European CEN norm	CEN/TS 16614-1 Network description CEN/TS 16614-2 Timing information CEN/TS 16614-3 Fare description	Public transport : network, timetables and fares Exchange protocol Reference data	Exchange of Public Transport scheduled information. Based on Transmodel 6 (integrating IFOPT)
SIRI	European CEN norm	EN 15531-1 - Business case EN 15531-2 - Communication EN 15531-3 - Services TS 15531-4 - Facility monitoring service TS 15531-5 - Situation exchange service	Public transport real-time information Exchange protocol Real-Time (and a bit of control)	Exchange of real-time information about PT services, vehicles, events and facilities.
Transmodel	European CEN norm	ENV12896	Covers most of the data domains of public transport Data Model all categories	Reference data model for public transport (base for NeTEx and SIRI, but also for a lot of national standards like TransXChange, NEPTUNE, TRIDENT, NOPTIS, etc.). Version 6 of Transmodel Part 1-2-3 (integrations IFOPT) has been published 2017. Transmodel 4 to 8 will be submitted to vote mid-2018.

Name	Status	Reference	Scope	Comment
INSPIRE	EU Directive	Directive 2007/2/EC http://inspire.ec.europa.eu/	Geographic features, maps related information and associated metadata Exchange protocol Reference data	It covers a wide range of information. It contains a set of transport dedicated layers (road, rail, water, cable), which are mainly focused on infrastructure description and their related geographic information.
IFOPT	European CEN norm	EN 28701 (DEPRECATED)	Stop Place description Logical data model	Identification of Fixed Objects in Public Transport IFOPT is now deprecated and has been embedded in Transmodel 6 (Part 1 and 2 published 2017)
DATEX II	European CEN norm	EN 16157 part 1 to 5 & 7 ongoing CEN/TS 16157 part 6	Data Model and Dictionary for traffic data exchange Real-time data	Part 1: context and framework (the modelling methodology) Part 2: location referencing Part 3: situation publication (for traffic information messages) Part 4 : VMS (variable message signs) publication Part 5 : Measured and elaborated data Part 6 : Parking publication Part 7 : Common data elements The current published version is Datex II version 2.3 whereas version 3.0 is being finalised.
	CEN ISO and ISO standards	ISO 14827-1 & -2 Projects: CEN ISO/TS 19468 & EN ISO 14827-3	Exchange protocols for real-time traffic data between centres Exchange protocol	Part 1 : Message definition requirements Part 2 : DATEX-ASN Part 3 : Data interfaces between centres for ITS using XML TS 19468 : Platform independent model specifications

Name	Status	Reference	Scope	Comment
RDS-TMC	ISO-CEN standard	EN ISO 14819 series	Traffic and travel information Exchange protocol Real-time data	Delivering of traffic and travel information to vehicle drivers over Radio Data System (mainly conventional FM radio broadcasts). Now managed by TISA (with TPEG, its successor)
TPEG	ISO standard (via TISA)	ISO TS 21219 part 1 to 251	Traffic and travel information Exchange protocol Real-time data	TPGEG Generation 2 covers the following information services: LRC - Location referencing container, (used in conjunction with applications and encapsulating different location referencing systems like Alert-C, OpenLR, Geographic Location references, …) PKI - Parking Information TFP – Traffic flow and prediction TEC - Traffic Event Compact WEA - Weather information for travellers FPI – Fuel price information and availability RMR – Roads and multimodal routes EMI – Electromobility charging infrastructure VLI – Vigilance location information Note: Some services defined for generation 1 have currently no equivalent in generation. It may be due to the lack of interest from the main contributors in TISA.
GDF	ISO-CEN standard	EN ISO14825:2011	Road network and all navigation related data Conceptual Data Model Exchange protocol Reference data	GDF (Geographic Data Files) aimed to provide reference data to in-vehicle or portable navigation systems, traffic management centres, or services linked with road management systems, including the public transport systems. Current version: GDF 5.0. is being updated, split into GDF 5.1-Part 1 (corresponds to GDF 5.0 except for the Public Transport feature theme) and GDF 5.1-Part 2 with integration of extensions (see below). Part 2 soon to be published.

Name	Status	Reference	Scope	Comment
ISO 17572-Location referencing for geographic databases	ISO Standard	ISO 17572 series	Location referencing Data Model/ methodology	Specifies Location Referencing Methods (LRM) that describe locations in the context of geographic databases and will be used to locate transport-related features.
ISO 19157:2013	ISO Standard	ISO 19101 series	Geographic information : Data model / geographic imagery	It defines the reference model for standardization in the field of geographic information. This reference model describes the notion of interoperability and sets forth the fundamentals by which this standardization takes place. The second part of this document provides a reference model for processing of geographic imagery which is frequently done in open distributed manners.
ISO 19148	ISO Standard	ISO 19101 series	Geographic information : Data quality	specifies a conceptual schema for locations relative to a one-dimensional object as measurement along (and optionally offset from) that object. It defines a description of the data and operations required to use and support linear referencing. ISO 19148:2012 is applicable to transportation, utilities, location-based services and other applications which define locations relative to linear objects.

Name	Status	Reference	Scope	Comment
GML	ISO Standard (via Open GIS Consortium)	ISO 19136	Geographic data set Exchange protocol Reference data	Defined by the Open Geospatial Consortium (OGC) to express geographical features, covering: Feature Geometry Coordinate reference system Topology Time Dynamic feature Coverage (including geographic images) Unit of measure Directions Observations Map presentation styling rules
CityGML	Open GIS Consortium and ISO	OGC Open standard (OGC 12-019)	Geographic data set Exchange protocol Reference data	Description and exchange of the representation of sets of 3D urban objects. Based on GML
Open Street Map (OSM)	de facto open standard	http://www.openstreetmap.org/about	Geographic features, maps related information and associated metadata Data set Reference data	OpenStreetMap (OSM) is a collaborative project to create a free editable map of the world. OSM is covering a wide range of objects, including public transport (http://wiki.openstreetmap.org/wiki/Public_transport), road network (http://wiki.openstreetmap.org/wiki/Highways)
ADASIS	Private	http://adasis.org/	Map data ahead of the vehicle	Member of Open Autodrive Forum (OADF)

Name	Status	Reference	Scope	Comment
SENSORIS	Private	http://sensor-is.org/homepage/	Data from vehicle sensors (stored in and available from cloud)	Member of Open Autodrive Forum (OADF)
NDS	Private	https://www.nds-association.org	Map database supporting incremental updates	Member of Open Autodrive Forum (OADF)
TN-ITS	CEN	tn-its.eu	TN-ITS is concerned with the exchange of information on changes in static road attributes.	Managed by ERTICO

Table 47: SVI related ongoing standardization activity

Standard Identifier/ Title	Description	Comment
SVI (by AutoCARE association)	The Secure Vehicle Interface (SVI) is a ready-to-deploy technology, based on three CEN/ISO standards: TS 21177, TS 21185 and TS 21184. SVI enables safe, cybersecure communication between the vehicle and service partners who have been chosen to obtain the data by the vehicle Owner/Users. SVI uses a standardised secure interface to connect recognised and authorised external systems to the network within a vehicle. SVI then converts the vehicle manufacturer's proprietary vehicle data into a common language, which enables broad interoperability for competitive services irrespective of the manufacturer or brand of the vehicle.	Supported by GENIVI. Related to variation III of SHOW reference architecture.
CEN/TS 21177: Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices	This document contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities: devices operated as bounded secured managed entities, i.e. "ITS Station Communication Units" (ITS-SCU) and "ITS station units" (ITS-SU) specified in ISO21217 between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks	Relevant to SHOW cyber-security work (published in 2019).

	These services include authentication and secure session establishment which are required to exchange information in a trusted and secure manner. These services are essential for many ITS applications and services including time-critical safety applications, automated driving, remote management of ITS stations (ISO 24102-2), and roadside / infrastructure related services. This document is complemented by guidelines (contained in CEN/TR 21186-3) on how security for C-ITS can work in general for all communication types (broadcast information dissemination and unicast sessions), considering especially what is needed in the infrastructure in addition to the technical features implemented in ITS station units.	
CEN/TS 21184: Cooperative intelligent transport systems,Global transportand data management (GTDM) framework	This document specifies a "Global Transport Data Management" (GTDM) framework composed of a global transport basic data model, a global transport function monitor data model, a global transport access control data model to support data exchange between ITS-S application processes and correct interpretation of these data. This document defines standardized data classes in a "Global Transport DataFormat" (GTDF) and means for managing them. The format of the data part is specified by a globally unique identifier pointing to a configuration including instructions for correct interpretation of the data part. Application and role-based access control to GTDF resources are specified in conformance with IEEE 1609.2 certificates. The set of ITS-S facility layer services is described as an ITS-S capability conformant with ISO24102-6, which is an optional feature.	Relevant to SHOW architecture conceptualization work and proposed data models / IP-based interfaces (unpublished, work in progress).
CEN/TS 21185 Cooperative intelligent transport systems - Communication profiles	This document specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices. These profiles enable information exchange between such trusted devices, including secure low-latency information exchange, in different configurations. This document also normatively specifies some ITS-SCPs based on the methodology, yet without the intent of covering all possible cases, in order to exemplify the methodology. Configurations of trusted devices for which this document defines ITS-SCP's include the following units according to ISO 21217: • ITS station communication units (ITS-SCU) of the same ITS station unit (ITS-SU), i.e. station-internal communications specified e.g. in ISO 24102-4 • an ITS-SU and an external entity such as a sensor and control network, or a service in the Internet • ITS-Sus The specifications given in this document can also be applied to unsecured communications and can be applied to groupcast communications as well	Relevant to SHOW communication layer work (published in 2019).

Note: A detailed list of all C-ITS relevant standards can be found here: http://its-standards.info/Guidelines/References.html

Appendix III: Actors and components present in demo sites

A summary of the local system actors including V2X infra nodes, the local cloud components per site and the user apps to be deployed (based on the SP2 Architects' TF interviews, project's horizontal data super spreadsheet, A7.5 material and D9.2) is provided in Table 48 below.

Table 48: Architectural components and passenger / AVs' on-board apps per demo site

Site (city)	Physical layer	Cloud components			Others	
	V2X infra	Local fleet management/ supervision/ tele-operation	Cloud interface to local PT service / TMCs	Passenger/ on-board apps	Interaction with other road users	Preferred architecture variation (I or II)
Rouen	ITS-G5, 5G networks: 8 V2X intersections, 2 linked to traffic lights controllers (incl. lidars, connected cameras)	Fleet supervision centre integrated in the PT control room	.PT Operations Control Centre	User app for DRT	-	I
Rennes	ITS-G5, 5G networks (under validation: V2X intersections (incl. lidars, connected cameras)	-	. STAR metropolitan information system . University Hospital Centre (CHU) information system . CHU ticketing system/ CHU parking's ticketing system	-	. VRUs . Ambulances	I
Madrid – Villaverde + Carabanchel (EMT depot)	C- ITS : Hybrid communication (RSU-ETSI ITS G5 – 5G), V2V, V2I, Lidars ,radar, camera, DGP	- (EMT's local FMP, dashboard and cloud service is private and no interface to the project is foreseen)	- (only through V2I, indirectly)	-	. Trajectory re-planning .Occluded VRUs at crossings	II
Graz	ITS-G5, smart camera at mobHub	-	-	-	. Detection of VRUs @ bus stops	II
Salzburg	Road side units: ETSI-G5, 3GPP 4G Buses in scenario 2 (C-ITS enhanced bus corridor) will be equipped with OBU's and RSU's connected to the TMC of Salzburg are planned to be installed.	-	PT: Service is planned to be integrated in PT TMC: OBU on buses are planned to be connected via RSU's (V2I short range communication) to TMC. TMC shares event messages (i.e. Road works warning) and signal information of traffic lights with RSU's.	DRT Service for automated shuttle is planned to be integrated into a Maas App	-	I

Site (city)	Physical layer	Cloud components			Others	
	V2X infra	**Local fleet management/ supervision/ tele-operation**	**Cloud interface to local PT service / TMCs**	**Passenger/ on-board apps**	**Interaction with other road users**	**Preferred architecture variation (I or II)**
Carinthia (pending amendment)	4G to 5G, Wi-Fi, C-ITS (connected traffic lights, smart lighting systems or cameras)	-	- .Integrate automated & connected fleets into the existing mobility systems (e.g., DRT, PT). .Enable MaaS platforms & frameworks	-	-	I
Karlsruhe	Local traffic information via Roadside units (WLAN 802.11p ITS-G5), e.g. CAM, DENMs, SPaT and MAP messages. --> Platooning functionality via V2V	Supervision of autonomous vehicle and decision aid (no teleoperation of the vehicle) (Vehicle APIs available but backend still to be developed)	-	- (custom user app for DRT booking)	-	I
Aachen	Public 4G and 5G mobile network. Restricted 5G Campus Mobile Networks are also available.	Interfacing to an intelligent DRT/MaaS cloud application in discussion	Interfacing to an intelligent DRT/MaaS cloud application in discussion	DRT/MaaS application	-	I
Braunschweig (pending amendment)	Demonstrate platooning through a Roadside Infrastructure at Tostmannplatz, .demonstrating AGLOSA (Adaptive Green Light Optimal Speed Advisory using V2X to platoon (ITSG5 MAPEM and SPATEM messages).	No remote operation planned	- (only through V2I, indirectly)	User app for DRT (AR, booking, planning)	-	I

Site (city)	Physical layer	Cloud components			Others	
	V2X infra	**Local fleet management/ supervision/ tele-operation**	**Cloud interface to local PT service / TMCs**	**Passenger/ on-board apps**	**Interaction with other road users**	**Preferred architecture variation (I or II)**
Linköping	4G network. Buttons (LoRaWAN) will be installed at shuttle stops (to support on demand DRT service) No traffic lights integration	Connected Traffic Tower with remote monitoring & limited teleoperation (stop on demand) Local ELIN operational Dashboard, SAFE platform Central dashboard based on Ericsson Innovation Cloud	Integration of AV first/last mile with PT service No direct TMC integration but based on Linköping MaaS data, optimal embarking/disembarking options through app.	On-board app for tablets. Smart phone passenger app optimised for ELIN and SHOW	Info for the passengers to a smart device connected in the shuttle. Reservation capabilities for the elderly and the disabled (through a passenger app)	II
Kista	5G network Assistance systems will help the vehicle at the bus stops (TBD)	Scalable 5G Connected Traffic Tower with remote monitoring & tele-operation (The Control Tower can also send a request for additional information to the vehicles APIs. If the connection to the Control Tower is lost, the vehicle brakes)	-	-	.the Control Tower can connect to VRUs in the surroundings of the shuttle.	II
Tampere	LTE/5G and ITS G5. 5G & 4G network, intelligent lighting systems LoRaWAN. 10 5G base stations in Heravanta suburb	Operation Centre • Remote control • Tele-operated manoeuvres	Integration with PT (and MaaS)	User app for DRT service (TBD)	-	II

Site (city)	Physical layer	Cloud components			Others	
	V2X infra	**Local fleet management/ supervision/ tele-operation**	**Cloud interface to local PT service / TMCs**	**Passenger/ on-board apps**	**Interaction with other road users**	**Preferred architecture variation (I or II)**
Copenhagen	C-ITS infrastructure and traffic control centre. Road signs will be prepared to communicate with automated buses. Also a 5G network will be utilized. +bus stops to be adjusted to AVs	Custom AV Supervision centre (TBD)	full cooperation with the existing PT service, using an upcoming BRT infrastructure linking efficiently to the nearby multi-modal PT hub (S-train, high-speed buses, local busses and shared e-bikes)	(web/ on-board?) App for real time planning and information offered to passengers	. Presence of vulnerable road users in intersections .VRUs inside AV (UC to be discussed)	I
Turin	Traffic sensors, Intelligent Traffic Light Systems (51Centralised TLs; 39 TLSwith PT Priority; 7 existing TLA-Traffic Light Assistant Enabled; 10 planned TLA Enabled), PMVs and 5G to be deployed completely by 2021.	Control tower – teleoperated vehicles	improving PT system, integrating it with the metropolitan, the railway, and ITS infrastructure and services TM system (operated by 5T)	Web app for DRT service booking	RSU to AV: Presence of VRU on smart crossing equipped with C-ITS capabilities	II
Trikala	4G, 5G, optic fibers network, Proximity sensors on traffic lights	Local Operational Tower (+ SHOW platform)	-	Web app for DRT service booking from SHOW	.Crossings with C-ITS (?). Signalized and not-signalized. In lane cyclist detection, illegal stop. .AV in pedestrian road, stops on pedestrian detection.	II
Brainport, Eindhoven	Hybrid ITS G5/cellular. Connected with C-ITS services, full 4G coverage, early 5G deployment and IoT service networks.	-	-	-	(In case VRU violates the traffic light at intersections, the vehicle will be capable to react to that)	I

Site (city)	Physical layer	Cloud components			Others	
	V2X infra	**Local fleet management/ supervision/ tele-operation**	**Cloud interface to local PT service / TMCs**	**Passenger/ on-board apps**	**Interaction with other road users**	**Preferred architecture variation (I or II)**
Brno	4G network, gradually increasing number of areas covered by 5G, several C-ITS road side units throughout the city, but not necessarily on selected routes	Remote control – teleoperation for long distance travel (200km)	interface with an existing PT service	User app for ride bookings	- (No direct interaction/communication with surroundings, but vehicles will continuously respond to their environment)	I

Appendix IV: Overview of services to be evaluated at different sites (D9.2 extract)

Extract from SHOW deliverable D9.2: The SHOW Demonstrations will address the operation of motorised transportation means and fleets by bringing automated operation to all levels of city mobility from fixed route Public Transportation (PT) to Demand response transportation (DRT), connected Mobility as a Service (MaaS) and Logistic as a Service (LaaS).

Table 49: Overview of services to be evaluated at different sites

Country	City/Site	Service					
		PT	MaaS	DRT	LaaS	TMC	Other
France	Rouen	x		x		x	
France	Rennes	x	x	x			
Spain	Madrid - Villaverde	x	x				
Spain	Madrid - EMT depot					x	Platooning Automated parking
Austria	Graz			x			
Austria	Salzburg	x	x	x		x	
Austria	Carinthia (amendment pending)	x	x	x	x		Covid adjusted services
Germany	Karlsruhe					x	Supervision
Germany	Aachen	x	x	x			Cooperative automated driving
Germany	Braunschweig (amendment pending)			x			Platooning
Sweden	Linköping	x	x	x			Trunklines
Sweden	Kista			x		x	Control tower
Finland	Tampere	x	x	(x)			Sump
Denmark	Copenhagen	X (BRT)	x	x		x	
Italy	Turin			x		x	Control tower for teleoperated vehicles.
Greece	Trikala		x	x	x		Prioritisation at traffic light
Netherlands	Brainport, Eindhoven						Prioritisation at traffic light Red light violation warning Platooning
Czechia	Brno			x	x	x	Long distance Remote control - teleoperation

Appendix V: C4 model main logic

How C4[24] model hierarchy works is outlined in the two Figures below.

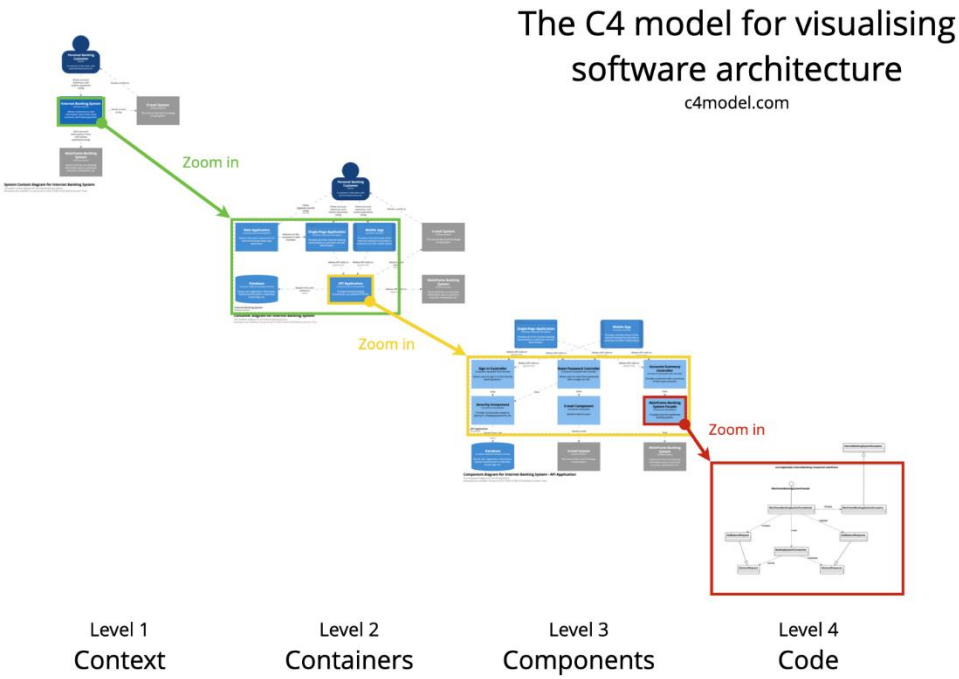

Figure 31: C4 model levels of SW representation (source: https://c4model.com/)

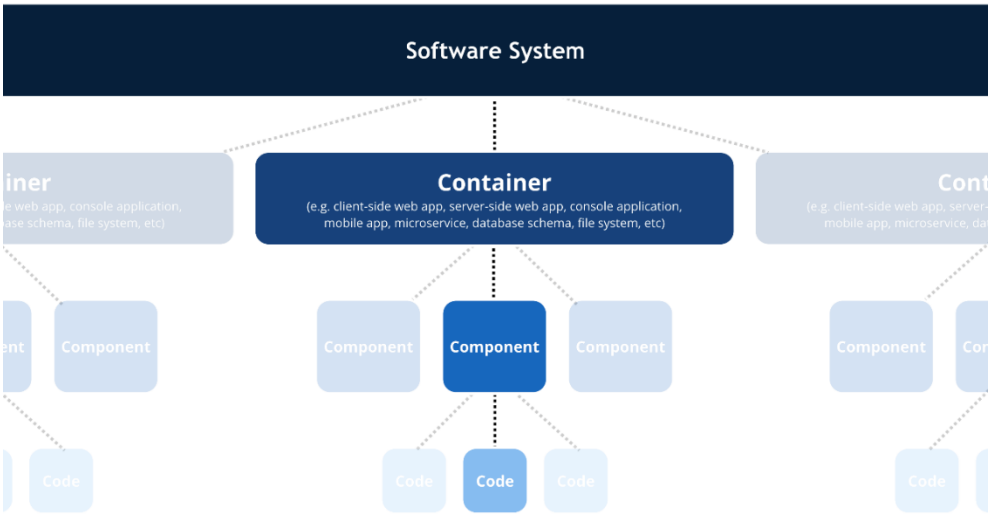

Figure 32: C4 model main blocks' hierarchy (source: https://c4model.com/)

[24] https://c4model.com/

Appendix VI: APIs for chapter 6 services (exercise)

APIs and functions used in Estimated Time of Arrival service.

CONSUMER		
Description: Consumer Login		
POST	URI: /consumer/{consumerLogin}	
consumerLogin(string, string): string		
Input	Username	String
	Password	String
Output	Web token	String
	Session	HTTP response
Description	Consumer Sends address	
POST	URI: /consumer/{consumerAddress}	
consumerAddress(string, string): HTTPresponse		
Input	IP address	String
	MAC address	String
Output	200: OK 401: unauthorized	HTTP response
Description	Consumer Actions	
createRequest(object, object, string): int		
POST	URI: /consumer/{request}/{requestID}	
INPUT	sendLocation(double, double): HTTP response	
	Input: Location Latitude: double Longitude: double	Output: HTTP response 200: OK 401: unauthorized 404: not found
	chooseDestination(double, double): HTTP response	
	Input: Destination Latitude: double Longitude: double	Output: HTTP response 200: OK 401: unauthorized 404: not found
	sendTimestamp(UTC ISO 8601): HTTP response	
	Input: time: UTC ISO 8601	Output: HTTP response 200: OK 401: unauthorized
OUTPUT	RequestID	Int
deleteRequest(int/double): HTTPresponse		
DELETE	URI: /consumer/{request}/{requestID}	
INPUT	RequestID	Int
OUTPUT	200: OK 401: unauthorized 404: not found	HTTP response
getPickupTime(int/double): time		
GET	URI: /consumer/{request}/{requestID}/{pickupTime}	
INPUT	RequestID	Int
OUTPUT	PickupTime	Time (mm:ss)
getDropoffTime(int/double): time		
GET	URI: /consumer/{request}/{requestID}/{dropoffTime}	
INPUT	RequestID	Int
OUTPUT	DropoffTime	Time (mm:ss)
getServiceData(object): HTTPresponse		
GET	URI: /cloud/{taskID}/{service}	
Input	Stops stopPlaces lines lineRoute ServiceArea Timetable operationHours operationDay dayType	Int Double, Double Int String String UTC time UTC time UTC time String
Output	200: OK	HTTP response

	404: Not found	
VEHICLE		
Description	Vehicle sends address	
vehicleAddress(string, string): HTTPresponse		
POST	URI: /vehicle/{vehicleAddress}	
Input	IP address	String
	MAC address	String
Output	200: OK 401: unauthorized	HTTP response
Description	Vehicle Actions	
PUBLISH	URI: /vehicle/{vehicleID}/{vehicleLocation}	
Msg.payload	Location: Latitude Longitude	 Double Double
postVehicleData(object): HTTPResponse		
POST	URI: /vehicle/{vehicleID}	
Input	VehicleID Name Manufacurer Model Seating Capacity Standing Capacity Vehicle Type	Int String String String Double Double String
Output	200: OK 401: Unauthorized 404: Not found	HTTP response
publishVehicleSpeed		
PUBLISH	URI: /vehicle/{vehicleID}/{vehicleSpeed}	
msg.payload	Speed	Double
Description	publishVehicleTraffic	
PUBLISH	Topic: /vehicle/{vehicleID}/{traffic}	
Msg.payload	Traffic	String
Description	publishSensorData	
PUBLISH	Topic: /vehicle/{vehicleID}/{sensors}/{sensorData}	
Msg.payload	navigationMode	String
	Acceleration	Double
	NextStop: Latitude Longitude	 Double Double
	Temperature	Double
	batteryStatus	Double
	Mileage	Double
	Steering	Double
	Odometer error	Int Boolean
	Occupancy	Int
	DispatchStatus	String
	Orientation	Float
	Heading	Float
getTaskID(object): HTTPresponse		
GET	URI: /cloud/{taskID}	
Input	Object	
Output	200: OK 401: unauthorized 404: not found	HTTP response
postEventID(object): HTTPresponse		
POST	URI: /cloud/{event}/{eventID}	
Input	Event eventType eventLocation Incident	Boolean String Double String

Output	200: OK 401: unauthorized	HTTP response
getEventID(object):HTTPresponse		
GET	URI: /cloud/{event}/{eventID}	
Input	Event eventType eventLocation Incident	Boolean String Double String
Output	200: OK 404: not found	HTTP response
CLOUD PLATFORM		
createTaskID(ojbect): int		
POST	URI: /cloud/{taskID}	
Input	getPassengerLocation(string, string): HTTPresponse	
	INPUT: Latitude: double Longitude: double	OUTPUT: HTTP response 200: OK 404: not fount
	getPassengerDestination(string, string): HTTPresponse	
	INPUT: Latitude: double Longitude: double	OUTPUT: HTTP response 200: OK 404: not fount
	getPassengerTimestamp(string): HTTPresponse	
	Input: time: UTC	Output: HTTP response 200: OK 401: unauthorized
Output	TaskID	Int
subscribeVehicleLocation		
SUBSCRIBE	URI: /vehicle/{vehicleID}/{vehicleLocation}	
Input	Latitude Longitude	Double Double
subscribeVehicleSpeed		
SUBSCRIBE	URI: /vehicle/{vehicleID}/{vehicleSpeed}	
Input	Speed	Double
getVehicleData(object): HTTPResponse		
GET	URI: /vehicle/{vehicleID}	
Input	VehicleID Name Manufacurer Model Seating Capacity Standing Capacity Vehicle Type	Int String String String Double Double String
Output	200: OK 404: Not found	HTTP response
subscribeVehicleTraffic()		
SUBSCRIBE	Topic: /vehicle/{vehicleID}/{traffic}	
Msg.payload	Traffic	String
subscribeSensorData()		
SUBSCRIBE	URI: /vehicle/{vehicleID}/{sensors}/{sensorData}	
Msg.payload	NavigationMode	String
	Acceleration	Double
	typeOfService	String
	NextStop: “Latitude” “Longitude”	 Double Double
	Temperature	Double
	batteryStatus	Double
	Mileage	Double
	Steering	Double
	Odometer error	Int Boolean
	Occupancy	Int
	dispatchStatus	String
	Orientation	Float
	Heading	Float

subscribeExternalData()		
SUBSCRIBE	Topic: /externalAPI/{externalAPIdata}	
Msg.payload	Weather: “weatherType” “humidity” “wind”	 String Double String
	cityTraffic	String
	maps	Object
postResponse(int): string, string		
POST	URI:/request/{requestID}/{pickupTime}, /request/{requestID}/{dropoffTime}	
POST	postPickupTime(int): time (mm:ss)	
	URI: /request/{requestID}/{pickupTime}	
Input	requestID	Int
Output	pickupTime	Time (mm:ss)
PUT	putPickupTime(int): time (mm:ss)	
	URI: /request/{requestID}/{pickupTime}	
Input	requestID	Int
Output	pickupTime	Time (mm:ss)
POST	postDropoffTime(int): time (mm:ss)	
	URI: /request/{requestID}/{dropoffTime}	
Input	requestID	Int
Output	dropoffTime	Time (mm:ss)
PUT	putDropoffTime(int): time (mm:ss)	
	URI: /request/{requestID}/{dropoffTime}	
Input	requestID	Int
Output	dropoffTime	Time (mm:ss)
postEventID(object): HTTPresponse		
POST	URI: /cloud/{event}/{eventID}	
Input	Event eventType eventLocation Incident	Boolean String Double String
Output	200: OK 401: unauthorized	HTTP response
getEventID(object):HTTPresponse		
GET	URI: /cloud/{event}/{eventID}	
Input	Event eventType eventLocation Incident	Boolean String Double String
Output	200: OK 404: not found	HTTP response
postServiceData(object): HTTPresponse		
POST	URI: /cloud/{taskID}/{service}	
Input	Stops stopPlaces lines lineRoute ServiceArea Timetable operationHours operationDay dayType	Int Double, Double Int String String UTC time UTC time UTC time String
Output	200: OK 404: Not found	HTTP response
SECURITY LAYER		
GET	URI: consumer/{consumerLogin}	
GET	URI: consumer/{consumerAddress}	
GET	URI: vehicle/{vehicleAddress}	
POST	URI: /DataRegister	
Input	authToken	String
Output	Certificate	File
THIRD PARTY PROVIDERS		
publishExternalData()		

PUBLISH	Topic: /externalAPI/{externalAPIdata}	
Msg.payload	Weather “weatherType” “humidity” “wind deg” Wind speed	 String Double Double Double
	Temperature temperatureMin TemperatureMax feelLike	Double Double Double Double
	Pressure	Double
	cityTraffic	String
	trafficLights	Double
	maps	Object

APIs and functions used in Multimodal Planner Service

PASSENGER		
Description: Consumer Login		
POST	URI: /consumer/{consumerLogin}	
consumerLogin(string, string): string		
Input	Username	String
	Password	String
Output	Web token	String
	Session	HTTP response
Description	Consumer Sends address	
POST	URI: /consumer/{consumerAddress}	
consumerAddress(string, string): HTTPresponse		
Input	IP address	String
	MAC address	String
Output	200: OK 401: unauthorized	HTTP response
Description	Consumer Actions	
createRequest(object, object, string): int		
POST	URI: /consumer/{request}/{requestID}	
INPUT	sendLocation(double, double): HTTP response	
	Input: Location Latitude: double Longitude: double	Output: HTTP response 200: OK 401: unauthorized 404: not found
	chooseDestination(double, double): HTTP response	
	Input: Destination Latitude: double Longitude: double	Output: HTTP response 200: OK 401: unauthorized 404: not found
	sendTimestamp(UTC ISO 8601): HTTP response	
	Input: time: UTC ISO 8601	Output: HTTP response 200: OK 401: unauthorized
OUTPUT	RequestID	Int
deleteRequest(int/double): HTTPresponse		
DELETE	URI: /consumer/{request}/{requestID}	
INPUT	RequestID	Int

OUTPUT	200: OK 401: unauthorized 404: not found	HTTP response
getPickupTime(int/double): time		
GET	URI: /consumer/{request}/{requestID}/{pickupTime}	
INPUT	RequestID	Int
OUTPUT	PickupTime	Time (mm:ss)
getDropoffTime(int/double): time		
GET	URI: /consumer/{request}/{requestID}/{dropoffTime}	
INPUT	RequestID	Int
OUTPUT	DropoffTime	Time (mm:ss)
subscribeItineraryID(int): int		
SUBCRIBE	URI: /consumer/{request}/{requestID}/ItineraryID	
INPUT	RequestID	Int
OUTPUT	ItineraryID	Int
getServiceData(object): HTTPresponse		
GET	URI: /cloud/{taskID}/{service}	
Input	Stops stopPlaces lines lineRoute ServiceArea Timetable operationHours operationDay dayType	Int Double, Double Int String String UTC time UTC time UTC time String
Output	200: OK 404: Not found	HTTP response
VEHICLE		
Description	Vehicle sends address	
vehicleAddress(string, string): HTTPresponse		
POST	URI: /vehicle/{vehicleAddress}	
Input	IP address	String
	MAC address	String
Output	200: OK 401: unauthorized	HTTP response
Description	Vehicle Actions	
PublishVehicleLocation		
PUBLISH	URI: /vehicle/{vehicleID}/{vehicleLocation}	
msg.Payload	Location: Latitude Longitude	 Double Double
PublishVehicleSpeed		
PUBLISH	URI: /vehicle/{vehicleID}/{vehicleSpeed}	
msg.payload	Speed	Double
Description	publishVehicleID	
PUBLISH	Topic: /vehicle/{vehicleID}	
Msg.payload	VehicleID Name vehicleType	Int String String
Description	publishVehicleTraffic	
PUBLISH	Topic: /vehicle/{vehicleID}/{traffic}	
Msg.payload	Traffic	String
Description	publishSensorData	

PUBLISH	Topic: /vehicle/{vehicleID}/{sensors}/{sensorData}	
Msg.payload	navigationMode	String
	Acceleration	Double
	NextStop: Latitude Longitude	Double Double
	Temperature	Double
	batteryStatus	Double
	Mileage	Double
	Steering	Double
	Odometer error	Int Boolean
	Occupancy	Int
	DispatchStatus	String
	Orientation	Float
	Heading	Float
	GNSSconnection	String
Description	Vehicle Availability Status	
PUBLISH	Topic: /vehicle/{vehicleID}/{availability}	
Msg.Payload	AvailabilityStatus	String
getTaskID(object): HTTPresponse		
GET	URI: /cloud/{taskID}	
Input	Object	
Output	200: OK 401: unauthorized 404: not found	HTTP response
CLOUD PLATFORM		
createTaskID(ojbect): int		
POST	URI: /cloud/{taskID}	
Input	getPassengerLocation(string, string): HTTPresponse	
	INPUT: Latitude: double Longitude: double	OUTPUT: HTTP response 200: OK 404: not fount
	getPassengerDestination(string, string): HTTPresponse	
	INPUT: Latitude: double Longitude: double	OUTPUT: HTTP response 200: OK 404: not fount
	getPassengerTimestamp(string): HTTPresponse	
	Input: time: UTC	Output: HTTP response 200: OK 401: unauthorized
Output	TaskID	Int
subscribeVehicleLocation		
SUBSCRIBE	URI: /vehicle/{vehicleID}/{vehicleLocation}	
msg.Payload	Latitude Longitude	Double Double
subscribeVehicleSpeed		
SUBSCRIBE	URI: /vehicle/{vehicleID}/{vehicleSpeed}	
msg.Payload	Speed	Double
subscribeVehicleTraffic()		
SUBSCRIBE	Topic: /vehicle/{vehicleID}/{traffic}	

Msg.payload	Traffic	String
subscribeAvailabilityStatus()		
SUBSCRIBE	Topic: /vehicle/{vehicleID}/{availability}	
Msg.payload	AvailabilityStatus	String
subscribeSensorData()		
SUBSCRIBE	URI: /vehicle/{vehicleID}/{sensors}/{sensorData}	
Msg.payload	NavigationMode	String
	Acceleration	Double
	typeOfService	String
	NextStop: “Latitude” “Longitude”	 Double Double
	Temperature	Double
	batteryStatus	Double
	Mileage	Double
	Steering	Double
	Odometer “error”	Int Boolean
	Occupancy	Int
	dispatchStatus	String
	Orientation	Float
	Heading	Float
	GNSSconnection	String
postServiceData(object): HTTPresponse		
POST	URI: /cloud/{taskID}/{service}	
Input	Stops stopPlaces lines lineRoute ServiceArea Timetable operationHours operationDay dayType	Int Double, Double Int String String UTC time UTC time UTC time String
Output	200: OK 404: Not found	HTTP response
subscribeExternalData()		
SUBSCRIBE	Topic: /externalAPI/{externalAPIdata}	
Msg.payload	Weather: “weatherType” “humidity” Temperature “wind”	 String Double Double String
	cityTraffic	String
	maps	Object
	parkingSpot	Double
postResponse(int): string, string		
POST	URI:/request/{requestID}/{pickupTime}, /request/{requestID}/{dropoffTime}	
POST	postPickupTime(int): time (mm:ss)	
	URI: /request/{requestID}/{pickupTime}	
Input	requestID	Int
Output	pickupTime	Time (mm:ss)
PUT	putPickupTime(int): time (mm:ss)	

	URI: /request/{requestID}/{pickupTime}	
Input	requestID	Int
Output	pickupTime	Time (mm:ss)
POST	postDropoffTime(int): time (mm:ss)	
	URI: /request/{requestID}/{dropoffTime}	
Input	requestID	Int
Output	dropoffTime	Time (mm:ss)
PUT	putDropoffTime(int): time (mm:ss)	
	URI: /request/{requestID}/{dropoffTime}	
Input	requestID	Int
Output	dropoffTime	Time (mm:ss)
publishItineraryID(int): int		
PUBLISH	URI: /consumer/{request}/{requestID}/ItineraryID	
INPUT	RequestID	Int
OUTPUT	ItineraryID	Int
SECURITY LAYER		
GET	URI: consumer/{consumerLogin}	
GET	URI: consumer/{consumerAddress}	
GET	URI: vehicle/{vehicleAddress}	
POST	URI: /DataRegister	
Input	authToken	String
Output	Certificate	File
Third Party Providers		
publishExternalData()		
PUBLISH	Topic: /externalAPI/{externalAPIdata}	
Msg.payload	Weather “weatherType” “humidity” “wind”	 String Double String
	cityTraffic	String
	trafficLights	Double
	maps	Object