SHared automation Operating models for Worldwide adoption

SHOW

Grant Agreement Number: 875530

D4.3: Open modular system architecture – second 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

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. In the case of SHOW ecosystem this includes automated cars, shuttles, buses, commuters with smart devices, AV fleet management providers, PTOs whose orchestration and needs for cloud data management motivated the work of D4.1.

The principle design target of D4.1 was to propose the main interfaces needed by a service-oriented architecture built on top of the on-road network of things that are involved when CAVs enter the public transport. For this purpose, D4.1 models the attributes of and the interaction among the SHOW system actors in an integrated system (AV operators, PT operators, passengers, other road users, public authorities, 3rd party services providers and vehicle vendors) and proposes interfaces which can be used by existing fleet management and PT backend systems to create local integrated systems for SHOW services deployment. Part of these services are supported by a central SHOW cloud infrastructure (SHOW Mobility Data Platform) developed in WP5 which also includes an in-SHOW developed custom Dashboard visualizing KPIs from the different collaborating test sites, for project monitoring purposes.

Continuing the work started with D4.1, in this deliverable, we show how SHOW flexible architecture proposed in D4.1, was adapted by each local test site integration/implementation team to the local ecosystem needs/pre-existing components in order to create the site's SHOW local architecture. Therefore, this document presents the local architecture solutions applied by each SHOW test site. Local CCAM solutions and integration with the central SHOW cloud subsystem were based on the three layers' generic architecture proposed and discussed in D4.1 where: i) different actors were connected to the local data management cloud (lower layer), ii) the local cloud was connected to the SHOW cloud (middle layer) and iii) on top of the local and central data management platforms, the various local or SHOW web-services were hosted (top layer). In this deliverable, the design adopted by each local site is described using a common reporting template. Thirteen SHOW test sites are included in this reporting, namely those of Madrid, Linkoping (Sweden Mega Site), Gothenburg (Sweden Mega Site), Rouen (French Mega Site), Karlsruhe (German Mega Site), Graz, Salzburg and Carinthia (Pörtschach area and the city of Klagenfurt) (Austrian Mega Site), Turin, Tampere, Brainport, Trikala and Brno. The deliverable also presents updates on the main SHOW cloud infrastructure subsystem (updates that took place after D5.1 submission) as well as cyber security and interoperability SMDP work performed as part of the project activity A4.4 (Cyber security mechanisms) and A4.5 (Interoperability mechanisms). Finally, the findings of the second round of the risk assessment performed in the project are also provided in this document.

Document Control Sheet

Start date of project:	01 January 2020
Duration:	48 months
SHOW Del. ID & Title:	D4.3: Open modular system architecture- second 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:	Emanuel de Verdale (ITxPT/UITP), Sam Lysons, Mihai Chirca (Transdev), Evangelos Antypas, Alexandros Papadopoulos, Athanasios Sersemis, Iordanis Papoutsoglou, Konstantinos Giapantzis, Georgios Spanos, Antonios Lalas, Konstantinos Votis (CERTH/ITI), Maria Gkemou, Matina Loukea (CERTH/HIT), Sven Salomon (Easymile), Emmanuel de Verdalle (ITxPT), Nico Lambing (FZI), Petra Schoiswohl (SURAAA), Markus Karnutsch (Salzburg Research), Tor Skoglund, Cilli Sobiech (RI.SE), Lucia Isasi, Ray Lattarulo (TECNALIA), Timo Mustonen (Sensible4), Pekka Eloranta (Sitowise), Jansen, S.T.H. (TNO), Anna Antonakopoulou (ICCS), Ioannis Gragopoulos (CERTH), Daniele Brevi (LINKS), Marek Vanzura (Brno), Katharina Karnahl (DLR)
Internal Reviewers:	Stefan Abendroth (Mobility Systems Engineering) – Robert Bosch GmbH Joachim Rentel (Cross Domain Computers) – Robert Bosch GmbH Maria Gkemou – CERTH/HIT Maciej Muehleisen (Ericsson)
External Reviewers:	N/A
Actual submission date:	17/02/2022
Status:	Final
File Name:	SHOW_D4.3_System_architecture - second Version_final

Document Revision History

Version	Date	Reason	Editor
0.1	27/08/2021	ToC circulated by ICCS to A4.1	A. Bolovinou (ICCS)
0.2	06/09/2020	Diagrams template for sites	A. Bolovinou (ICCS)
0.3	27/10/2020	Sections template to be followed by sites	A. Bolovinou (ICCS)
0.4	14/12/2020	Integration of sites inputs	A. Bolovinou (ICCS)
0.5	16.12.2020	Integration of sites updated inputs and wp4 inputs by CERTH-ITI	A. Bolovinou (ICCS), A. Lalas (CERTH/ITI)
1.0	30.12.2021	All contents integrated. Stable version sent for internal peer review.	A. Bolovinou (ICCS)
2.0	14.02.2021	Updates by ICCS based on internal wp4 review	A. Bolovinou (ICCS)
2.1	16.02. 2021	Final check from Technical Manager – sent for submission	M. Gkemou (CERTH/HIT)

Table of Contents

List of Tables

List of Figures

Abbreviation List

Abbreviation	Definition
AD	Automated Driving
ADS	Automated Driving System
AI	Artificial Intelligence
API	Application Programming Interface
AV	Autonomous Vehicles
AVxPT	AVs for PT (source UITP/ SPACE project)
CAV	Connected and (fully) automated vehicle
CCAV	Collaborative Connected Autonomous Vehicles
C-ITS	Co-operative Intelligent Transport Systems
CKAN	Comprehensive Knowledge Archive Network
CSRF	Cross-site Request Fraud
CSV	Comma Separated Values
DDoS	Distributed Denial of Service
DoS	Denial of Service
DRT	Demand-Responsive Transit
DSRC	Dedicated short-range communications
ETA	Estimated Time of Arrival
ETSI	European Telecommunications Standards Institute
EU	European Union
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPU	Graphics Processing Unit
GTT	Gruppo Torinese Trasporti
HD	High Definition

Abbreviation	Definition
HTTP	Hypertext Transfer Protocol
I2V	Infrastructure to Vehicle
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
KPI	Key Performance Indicator
LFMP	Local Fleet Management Platform
LiDAR	Light Detection and Ranging
M2M	Machine to Machine
MDP	Mobility Data Platform
MITM	Man In The Middle
MLDMP	Madrid's Local Data Management Platform
MQTT	Message Queuing Telemetry Transport
NAP	National Access Point
OBU	On Board Unit
OEM	Original Equipment Manufacturer
PT	Public Transport
PTA	Public Transport Authority
PTO	Public Transport Operators
REST	REpresentational State Transfer
RSU	Roadside unit
SMDP	SHOW Mobility Data Platform
SP#	Sub-Project number
SSL/TLS	Secure Socket Layer/Transport Layer Security
TCC	5T control center
TMC	Traffic management centre

Abbreviation	Definition
TSMO	Transportation Systems Management and Operations
UFW	Uncomplicated Firewall
UML	Unified Modeling Language
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)
vERPC	virtual Evolved Packet Core
VRU	Vulnerable Road User
WoT	Web of Things
WP	Work Package

1 Introduction

1.1 Purpose and structure of the document

The objectives of this deliverable and the corresponding structure hosting the work of each objective include:

a. to present the local sites architectures and discuss any interoperability aspects: this part is covered by chapter 4 applying the template proposed in ch. 3 and Appendix II.
b. to present the SHOW Mobility Data Platform (SMDP) architecture updates: this part is covered by chapter 4 and Appendix I.
c. to present the cybersecurity tools specifications and present updates on theoretical and implementation / testing work performed as part of WP4-A4.5: this part is covered by chapter 6 and Appendix III.
d. to present the SHOW data management interoperability tools specifications: this part is covered by chapter 7.
e. to present the updated risk management tracing table: this part is covered by chapter 8 and App. IV.

1.2 Intended Audience

The intended audience of this work includes:

- SHOW SP2 OEMs and vehicle owners responsible for the CCAV deployment/integration into the SHOW demo cities ecosystem;
- SHOW SP2 service designers and developers (WP5 and WP6) interested in the service information flow described in each of the local architecture instances.
- SHOW SP3 demo sites' technical teams responsible for
  - the technical verification of SHOW local system in each site (pre-demo activity)
  - the Real-life demonstrations and the
  - technical validation of SHOW local system in each site (demo activity)
- Stakeholders and research community outside SHOW dealing with CCAVs integration in future PT landscape: Interested in the design alternatives supported in each SHOW site.

1.3 Interrelations

Interactions with SP2 technical WPs and discussions with the sites to support them in developing the local SHOW system architecture took place this second year of the project focusing on aligning all sites with the SHOW data expectations format and exchange through the main SHOW cloud subsystem, namely the SHOW Mobility Data Platform (SMDP). In particular, interactions will all the following WPs are outlined:

- WP5: SMDP design and cloud cyber security mechanisms applied
- WP8: Digital infrastructure
- WP9-WP11: sites' demos setup, evaluation and impact assessment teams.

2 The role of SHOW reference architecture (D4.1 recap) and SHOW Dashboard web-service

In order to prepare for the integration of both mature and non-mature CAV fleet ecosystems, the work in D4.1 [1] provided an 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). This offers a harmonized and "supervised" design framework to be used by the SHOW sites for integration of their local subsystem, namely their fleet and the Local Fleet Management Platform (abbreviated as LFMP), with the SHOW Mobility Data Platform (abbreviated as SMDP).

In this way, while a big degree of flexibility is given to the local teams on how to design their local ecosystem for SHOW fleet piloting activity, a minimum set of design requirements is ensured to be followed by all, entailing the following aspects:

- 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 and integrated such mechanisms through SMDP.

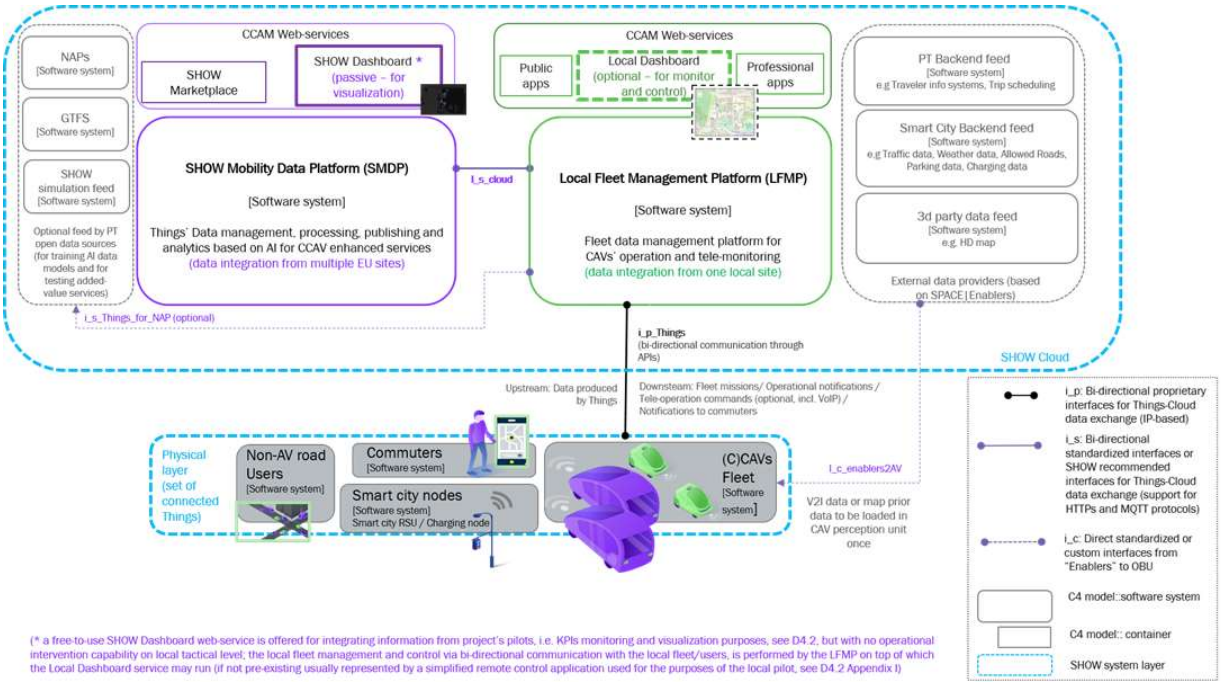


Figure 1: SHOW reference architecture (better viewed in zoom-in mode)

The proposed reference architecture implements integration of local fleet and connected commuters through the *i_p_things* interface while LFMP and SMDP subsystems cloud communication is implemented through the *I_s_cloud* interface. It also supports two discrete Dashboard services that can be enabled by the LFMP and SMDP cloud platforms respectively. Their discrete roles, the first may operate in a bi-directional mode with the fleet while the second may operate only in single-directional mode for project KPI data visualization, are specified in table 13 of the latest revised D4.1 deliverable [1]. In Figure 2 below, the new data architecture showing how SHOW Dashboard migrated to a SMDP based data channel for both batch processed KPI data over REST protocol and real-time sensor data over MQTT protocol is presented.

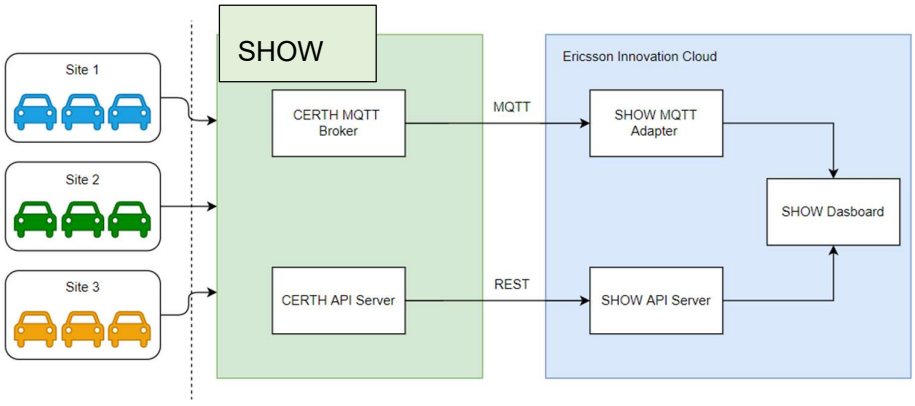
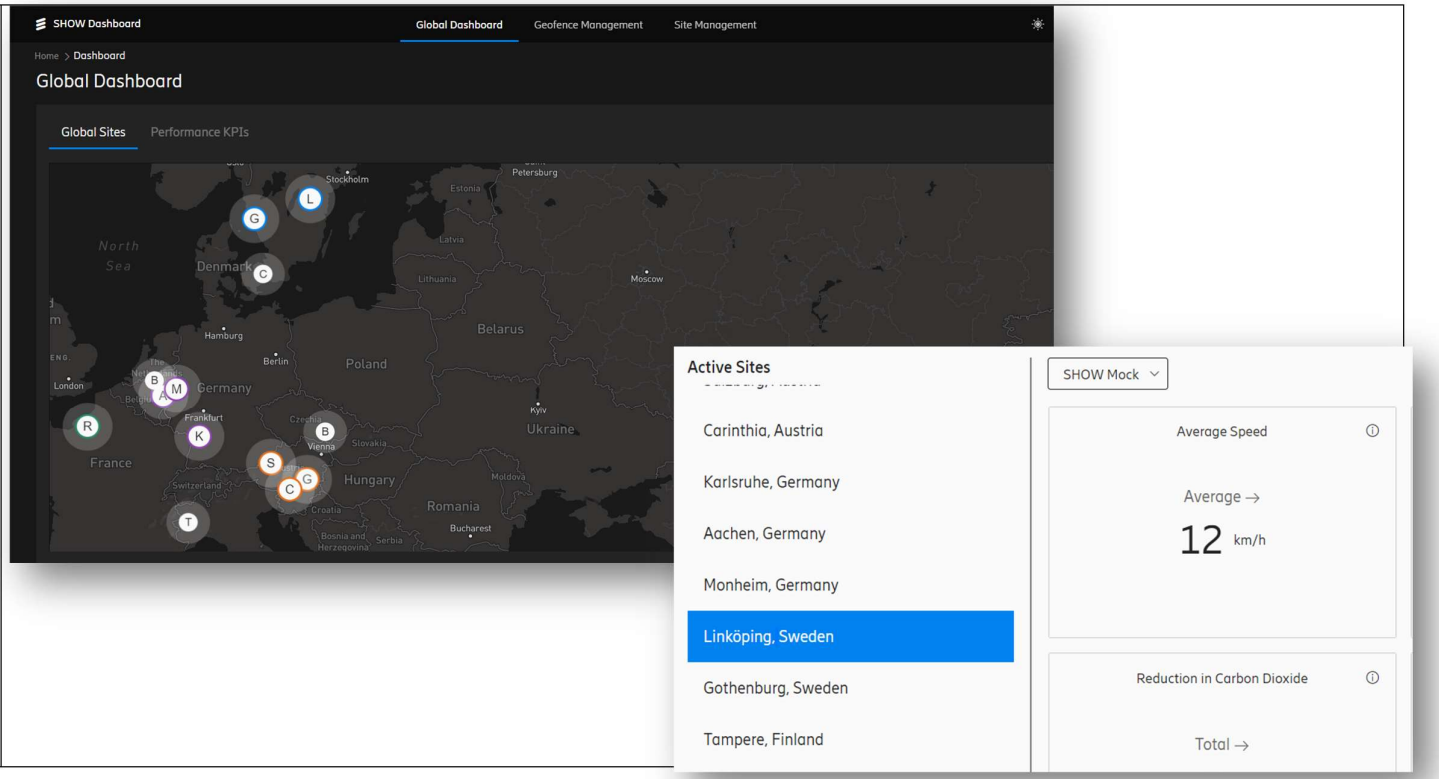


Figure 2: SHOW Dashboard data flow on top of SHOW MDP.

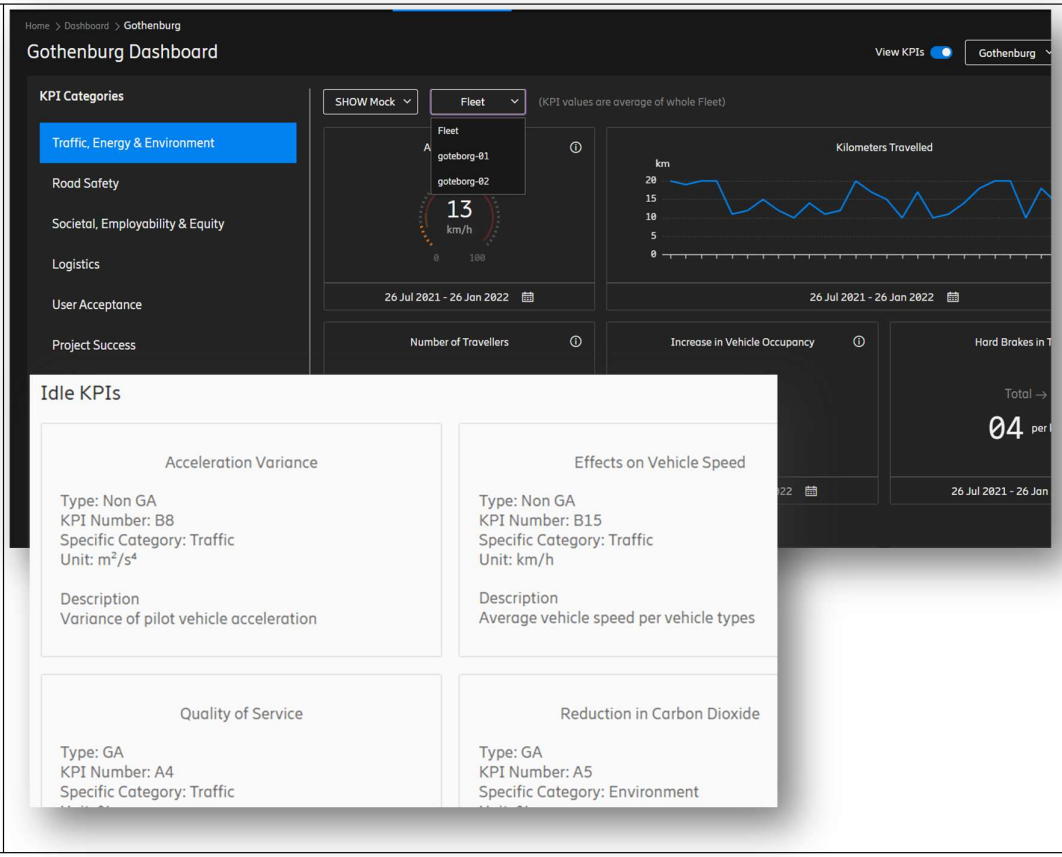
In addition, in the Table 1 below we present an update of D4.2, SHOW Dashboard design by providing snapshots of the current SHOW Dashboard sitting on top of SMSP.

Table 1: SHOW Dashboard features in snapshots.

Introduction of a Public Layer – Dashboard accessible to public – Public Layer link to be updated in https://show-project.eu/ – A set of agreed upon Site KPIs can be visualized in this dashboard	

KPIs

- Implementation and visualization of KPIs of a specific vehicle
- An entity dropdown enables users to toggle between Fleet and vehicle KPIs
- KPIs which are unavailable for a site can be visualized in a descriptive card.



3 Local architecture description: the template

In this deliverable, the target is to show how the D4.1 flexible architecture was adapted by each local demo site integration/implementation team to the local ecosystem needs/pre-existing components in order to create the site's SHOW local architecture.

To facilitate the reporting of each local architecture instantiation, the design adopted by each local site is described using a common diagrams/text/tabular template. This included the following sub sections:

a) The local technology actors

Description and diagram of the local ecosystem following the D4.1 conceptual architecture representation (as in Figure 3). Here, all actors that interact with the local fleet management platform and the SHOW Mobility Data Platform via specified interfaces are of interest (components internal to SMDP like the SHOW Dashboard that are common for all sites' architectures do not need to be described). Additional diagrams describing existing solutions in more details were considered complementary and were allowed to be added (e.g. Rouen case).

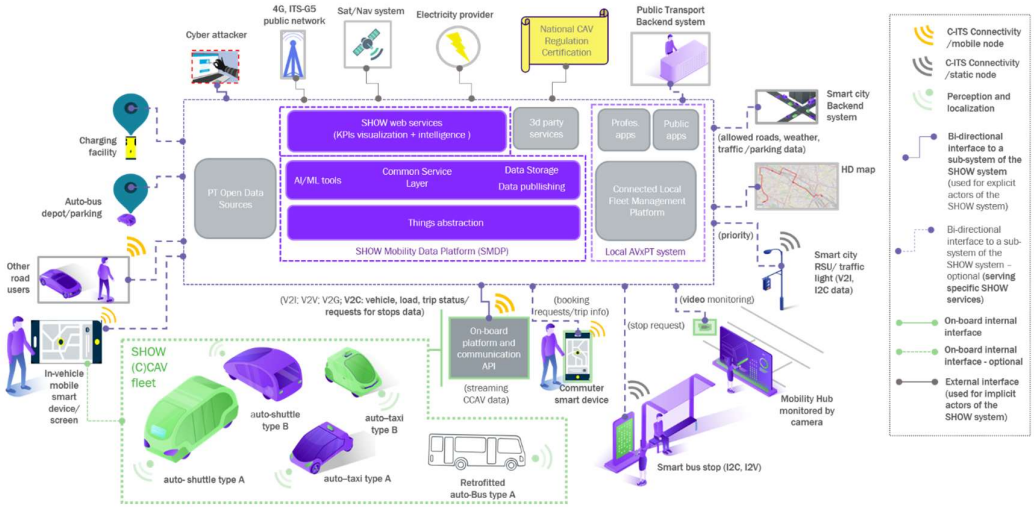


Figure 3: SHOW integrated system conceptual view (from D4.1)

b) Functional architecture

Description and diagram of the local functional architecture following the D4.1 functional architecture representation (as in Figure 4, grey part).

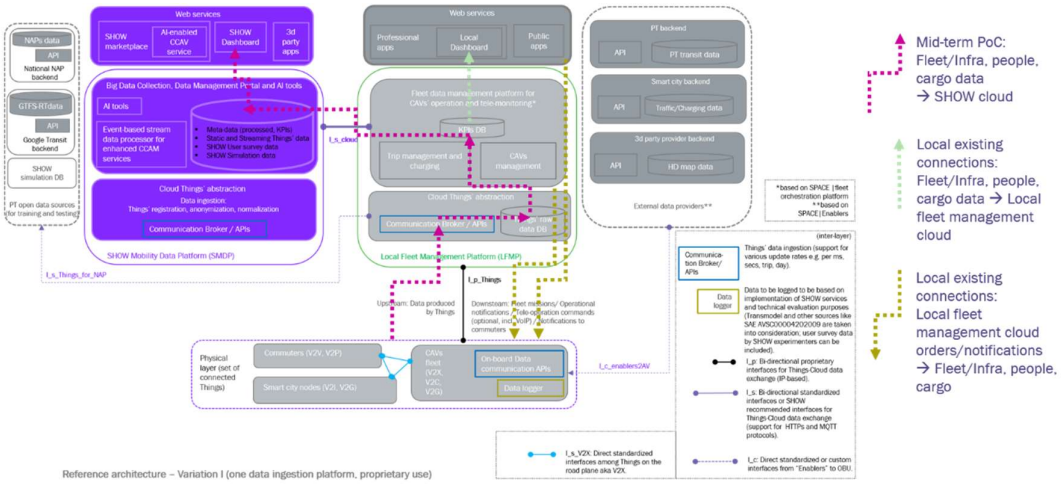


Figure 4: SHOW functional architecture and information flows (better viewed in zoom-in mode)

In this deliverable, we first cast our focus on the right grey-components part of the diagram presented in Figure 4, to present the local CAV ecosystem functional architecture. Each local architecture *detailed* diagram should include:

- the local low layer components (modules inside: fleet connected, infra nodes connected, IoT devices connected)
- the local internal LFMP components
- the local web services on top of LFMP
- the external components linked to LFMP (if any)
- ADDITIONALLY: inside the local Dashboard service add in bullets the Local Dashboard functionality (if a local dashboard service is supported
- the connections among the above.

Local architecture information flow paths to be described include:

- Connected fleet/passengers **to** local LFMP/Dashboard
- Local LFMP/Dashboard **to** connected fleet/passengers
- LFMP **to** SMDP.

c) Service information flow

Description and simplified diagram of the local services information flow following the D4.1 service information flow representation, as in the example of Figure 5.

NOTE: In this deliverable, preliminary information on services data flow is documented, final services will be detailed in the upcoming WP5 (D5.3) deliverable, see also Appendix II as well as in the final WP4 deliverable (D4.4).

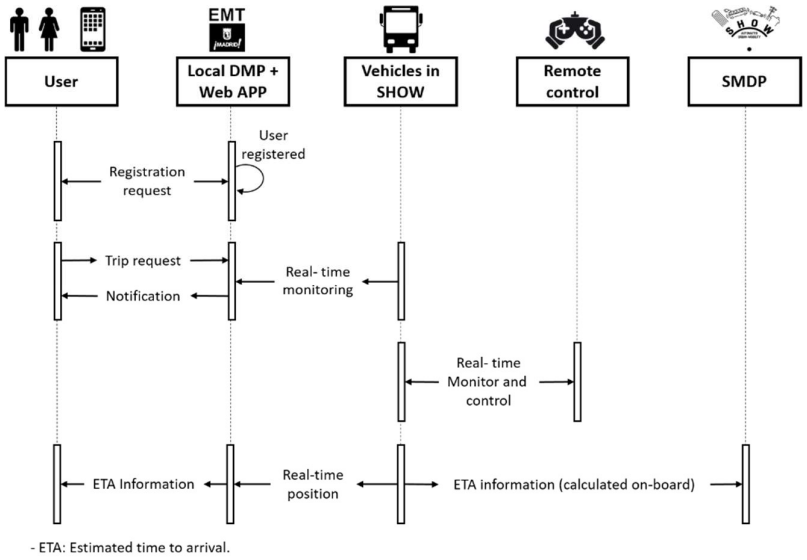


Figure 5: Example of service information flow diagram (UML sequence diagram)

d) [optional section] Special aspects: interoperability, connectivity, cybersecurity custom solutions (if any).

Description of interoperability, connectivity, cybersecurity challenges faced and custom solutions required not covered by SHOW architecture recommended interfaces.

4 Sites local architecture instances

In this chapter the local architecture in each of the active SHOW test sites, namely those of Madrid, Linkoping, Gothenburg, Rouen, Karlsruhe, Graz, Salzburg, Carinthia (Pörtschach area and the city of Klagenfurt) mega pilots and those of Turin, Tampere, Brainport, Trikala and Brno satellite pilots will be presented. The information is structured in four sub-sections according to the template described in section 3: a) conceptual architecture and actors' description b) functional architecture (components' level) c) services' information flow (where available) and d) special interoperability, cybersecurity, connectivity aspects (if applicable).

4.1 Madrid local architecture

4.1.1 The local technology actors

Madrid ecosystem includes the Madrid's Local Data Management Platform (MLDMP), the Madrid's fleet (a bus, two shuttles and two vehicles) and the Madrid's on-site digital infrastructure (C-ITS node, smart traffic light node). Interconnection among the technology actors is presented in the diagram of Figure 6.

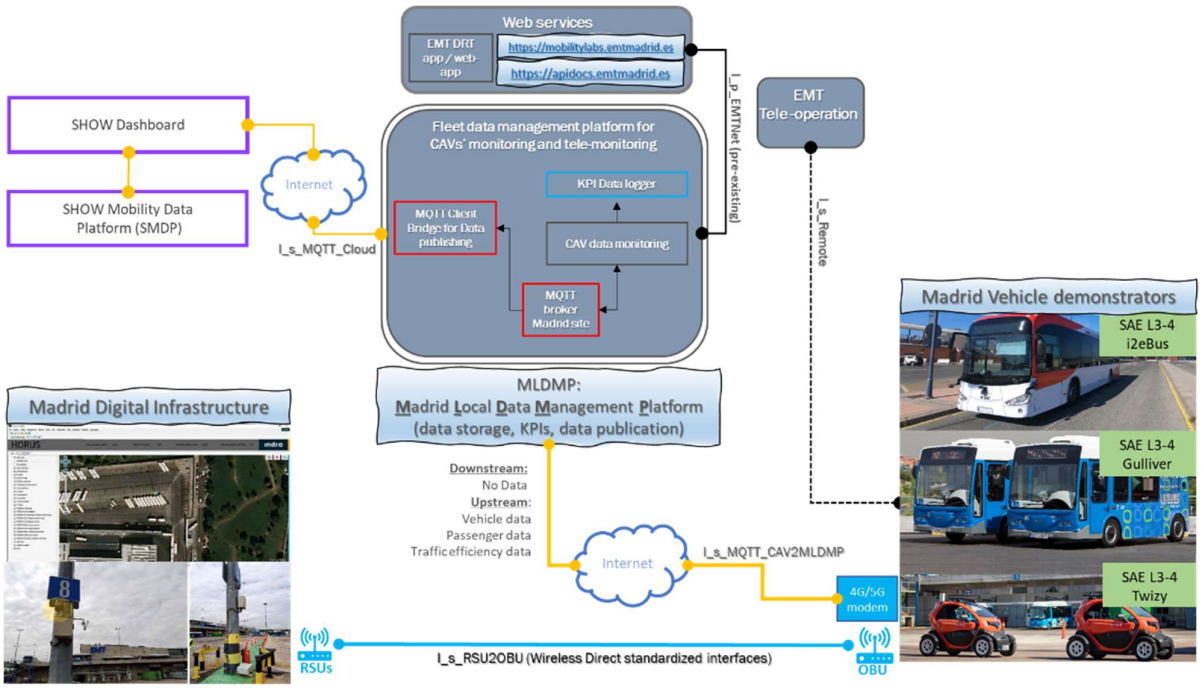


Figure 6: Madrid site local actors (better viewed in zoom-in mode).

Brief description of the actors' role and their connectivity profile is provided in Table 2.

Table 2: Local technology actors and their connectivity profile.

Actor	Role	Connectivity
Gulliver fleet	Provide Service for passengers, remote radio control and V2C connectivity	V2C, Radio Control[1]
Twizy fleet	Demonstrate technical advancements in cooperation maneuvers and connectivity with infrastructure	V2V, V2I and V2C
i2Bus	Demonstrate technical advancements in cooperation maneuvers (platooning) and connectivity with infrastructure	V2V, V2I and V2C
Madrid LDMP (MLDP)	Provide integration for all platforms, existing infrastructure, and SHOW MDP	Internet connectivity (C2V)
Madrid Digital Infrastructure	Provide connectivity for smart infrastructures through I2V communications	I2V
SHOW commuters	Users of the Madrid SHOW fleet	Cloud (Web app)

4.1.2 Functional architecture

Madrid functional architecture (component level) is presented in Figure **7** and the data exchange (single-directional) among the LFMP, SMDP and the fleet is described hereafter:

- Connected fleet/passengers **to** local LFMP/Dashboard: Vehicle/passenger/traffic efficiency real time data from connected fleet using MQTT on a local broker, for storage, monitoring and transfer to SMDP.
- Local LFMP/Dashboard **to** connected fleet/passengers : No downstream data.
- LFMP **to** SMDP: LFMP connects to SMDP through internet using MQTT, it forwards the real time data gathered from all vehicles in Madrid Site through its local broker, and sends it through a bridge.
- I_s_RSU2Fleet: Fleet supports V2I connectivity enabled by Horus C-ITS hub installed locally and communicating with both vehicles and smart traffic light node.

Note 1: Pre-existing local Dashboard service controlled by EMT communicates with MLDMP via the proprietary i_p_EMTNet interface.

Note 2: Two pre-existing interfaces for tele-operation (I_s_Remote) and for remote emergency braking (I_s_safety) are also supported by the fleet without being controlled by the MLDMP.

[1] Applicable only on Carabanchel scenario.

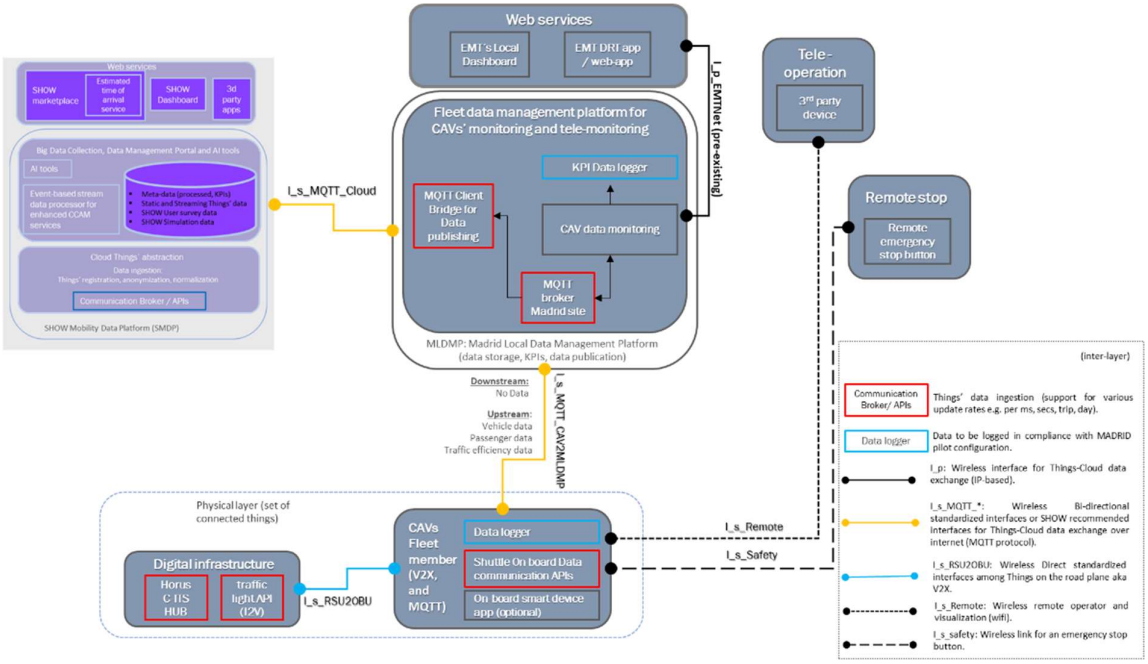


Figure 7: Madrid site functional architecture (better viewed in zoom-in mode)

4.1.3 Service information flow

The local CAV monitoring service as well as user DRT (demand-responsive transit) and ETA (Estimated Time of Arrival) service information flow is presented in Figure 8 and the Table 3 that follows.

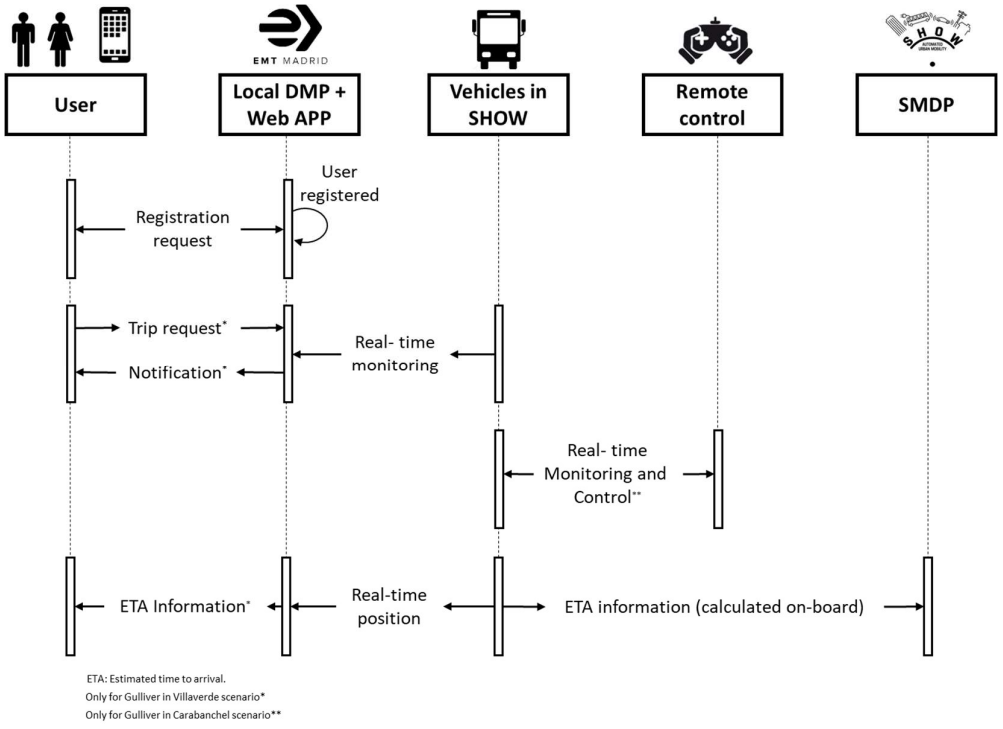


Figure 8: Information flow diagram

Table 3: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
User app[2]	Notifications to the user, and registration, as well as request at bus stop.	Location from the vehicle platform. User information and registration data.
Local DMP/ Web app[3]	Monitoring CAVs, storage of KPIs, connectivity with SHOW DMP. Integration with User app.	Real time data from vehicle fleets, received through MQTT. User data for interaction and registration.
Vehicles Show	Automated vehicles with connectivity through MQTT via Internet and V2X (DSRC)	Real time data from internal systems to be published through MQTT Real time data from other vehicles and infrastructure from V2X (DSRC).
Remote Control[4]	Remote operation of the vehicle	Feed of video perception, and control commands.
SMDP	KPI calculation and storage. Connectivity to Show Dashboard	Real time data received from Local DMP from all vehicles in Madrid Site.

4.1.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if any)

No custom developments. Connectivity and integration with SMDP followed cybersecurity guidelines provided, establishing an authenticated and encrypted connectivity between the Madrid LMDP and the SMDP for KPI data exchange.

4.2 Swedish Pilot sites

4.2.1 Linköping local architecture

4.2.1.1 Local technology actors

The Swedish site in Linköping site has a mixed approach where two different vehicle providers are deploying their fleet at the site with 3 automated vehicles in total.

The architecture below (Figure 9) describes the higher level of operators that are present directly or indirectly at the pilot site.

[2] User app functionality available only for Gulliver in Villaverde scenario.
[3] User registration and request functionality available only for Gulliver in Villaverde scenario.
[4] Remote operation available only for Gulliver in Carabanchel scenario.

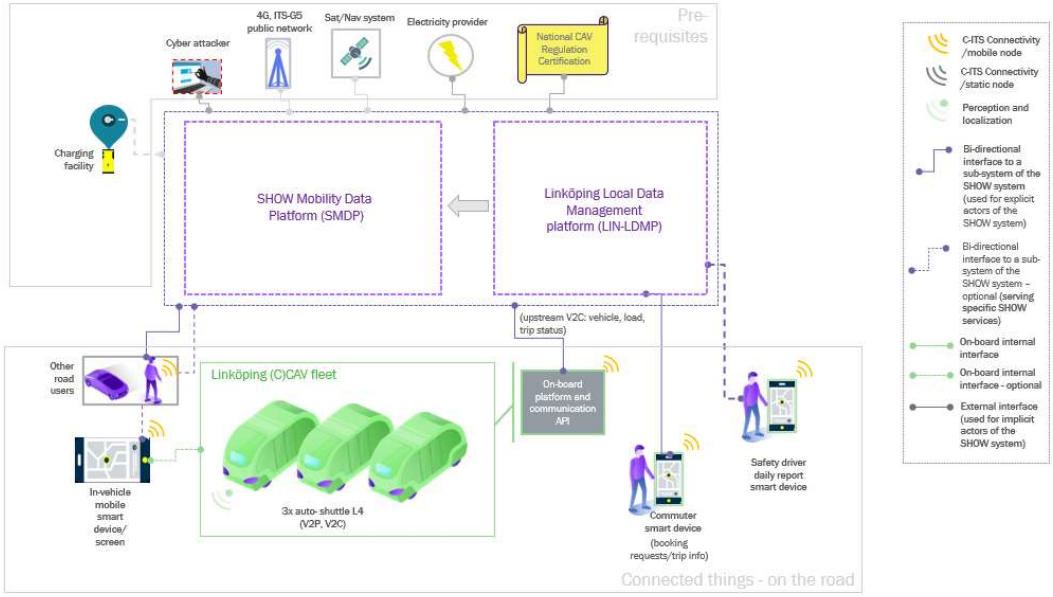


Figure 9: Linköping site local actors

The passenger will have the route information available at local operator's data service, but the vehicle will not directly integrate to it. Vehicle will provide real time and KPI data to the local data management platform, from where it is also sent to SHOW mobility data platform and dashboard.

Brief description of the actors' role and their connectivity profile is provided in Table 4.

Table 4: Local actors and their connectivity profile

Actor	Role	Connectivity
Web services by Transdev Sweden	Passenger transportation and vehicle operations	Connects to local data management platform
Cloud infra/LFMP by RISE	Digital Infrastructure Manage local data platform	Data collection from vehicles. Connects to local data management platform Connects to SHOW DMP
SHOW technical team, VTI	Management and Operational center of site	No direct integration between vehicle data and operator's passenger information service
Campus Site owner, Akademiska Hus	Property owner and landlord Keep the roads and the surroundings in operational conditions at the university campus.	No direct data connection.

Actor	Role	Connectivity
City of Linköping / Linköping Muncipality	Landlord. Keep the roads and the surroundings in operational conditions on city ground and roads.	No direct data connection.
Telecommunications (3rd party 4G/LTE/5G +GNSS connections)	Provide safe and reliable data connection and localization.	Between autonomated vehicle and data management platforms.
SHOW commuters	Users of the SHOW fleet	Cloud (Web app)

4.2.1.2 Functional architecture

Locally the data flows are as depicted below. Real time data is provided by the autonomous vehicles. Some of the KPI calculations are done in the local data management platform but Linköping relies on KPIs that will be calculated by the SHOW data management platform. The autonomated vehicle does not provide data directly to the central SHOW data platform. The communication is done via the local FMP using the standardized SHOW data management interface. The local fleet management platform is designed to support easy integration to other services like smart traffic or smart city solutions, route planners, etc. However, at the initial phase of the pilot these are omitted to reduce complexity and to ensure that operations can commence on time.

Linköping's functional architecture (component level) is presented in Figure 10and the data exchange (single-directional) among the LFMP, SMDP and the fleet is described hereafter:

- Connected fleet/passengers **to** local FMP/Dashboard:
  - Autonomous vehicles provide data produced by the sensors and technical equipment in the vehicle, such as speed, acceleration, location, etc.
  - A special passenger counting app is deployed on tablets in the autonomous vehicles.
  - A passenger web app can be used to indicate that you are waiting at a bus stop

- Local FMP/Dashboard **to** connected fleet/passengers : Local Data Management Platform sends number of waiting passengers to the safety driver.

- LFMP to SMDP: There is a data connection that sends real time upstream data to the SMDP. These include location of the autonomous vehicle, its occupancy, etc. (There is no downstream data connection enabled)

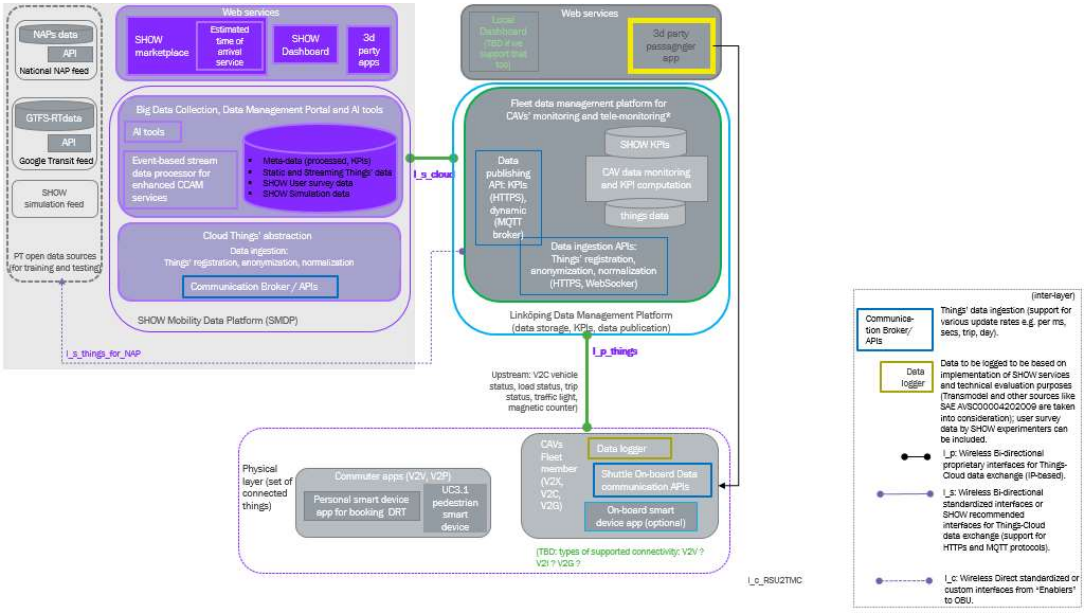


Figure 10: Linköping site functional architecture (better viewed in zoom-in mode)

4.2.1.3 Service information flow

The service information flow is as described in Figure 11 and the table Table 5 that follows. The autonomous vehicles in the pilot will not be directly connected to the existing passenger services by the local operator. The schedule and route information are provided from the sites own website and via the passenger web app. Automated vehicles communicate with LDMP, that in turn communicates with SMDP in providing real time data and KPI information. Operational data between vehicle and local fleet management is handled in real time. Safety drivers will be present inside the automated vehicle at the pilot site and the data for remote monitoring of the fleet is provided to the data management platform.

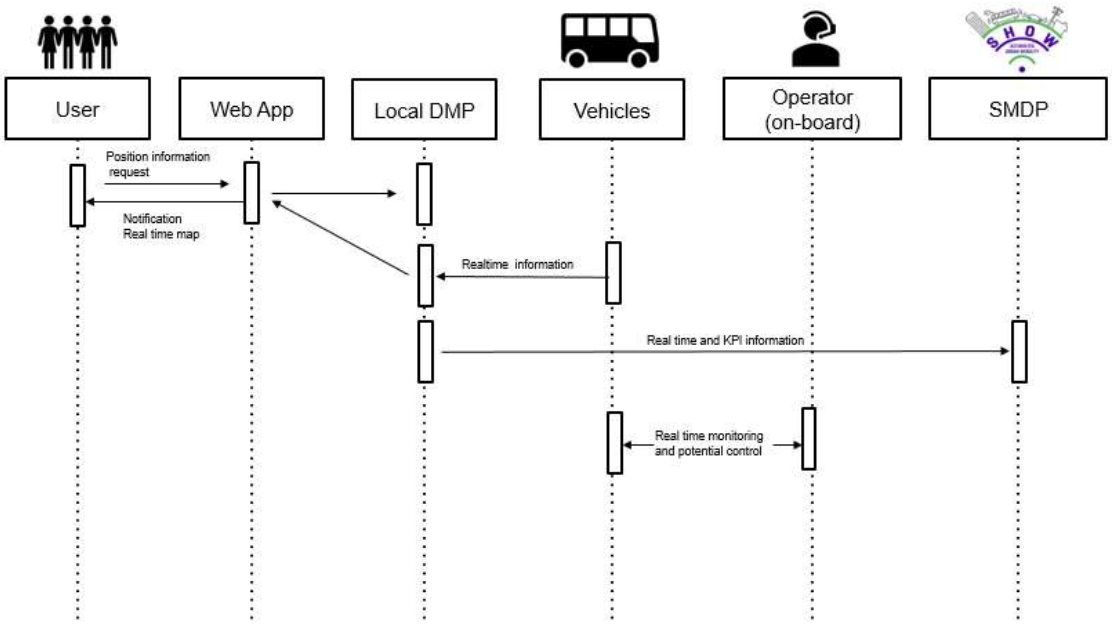


Figure 11: Information flow diagram

Table 5: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
Passenger web app	Passengers can get route and schedule information and real time vehicle position from the local operator web application	Static route and schedule data.
Local Data Management Platform	Vehicles provide real time data to LDMP, that in turn provides the real time and KPI data to SMDP.	KPIs: Vehicle location, acceleration, speed, occupancy, etc.
Operator/driver (in-vehicle)	Vehicle provides the operator/safety driver and LDMP with KPI data.	Updated routing data.

4.2.1.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if any)

The Linköping site will not have V2I connectivity at the site. The potential for connecting to the smart traffic lights on the route was investigated, but the traffic light operator did not allow any additional installations in their traffic system.

Cybersecurity follows vehicle manufacturer's standard security practices and there is no sensitive data transferred between the vehicle and the local fleet management platform.

The site will have safety drivers inside the vehicles. Under the current permits, we are not allowed to deviate from the programmed route.

4.2.2 Gothenburg local architecture

4.2.2.1 The local technology actors

The Gothenburg experiment has taken (in pre-demo phase) and will take also place in the final demo phase on the Chalmers campus. Between 2 and 3 (in the final demo phase) automated shuttles have operated/ will be operated on the site by Keolis. The architecture below (Figure 12) describes the technology actors that are present directly or indirectly at the pilot site interacting with the local fleet management platform ran by Autofleet. The actors are also described in Table 6.

A safety driver was/will be present in each shuttle. The safety driver will perform various functions:

- Report incidents that occur on road thanks to a safety driver app.
- Count get-on / off at each station thanks to the safety driver app too.
- Alert the supervision team in case of high incidents or accidents with his/her smartphone.
- Drive the vehicle in manual in the situations that the autonomous vehicle cannot manage.

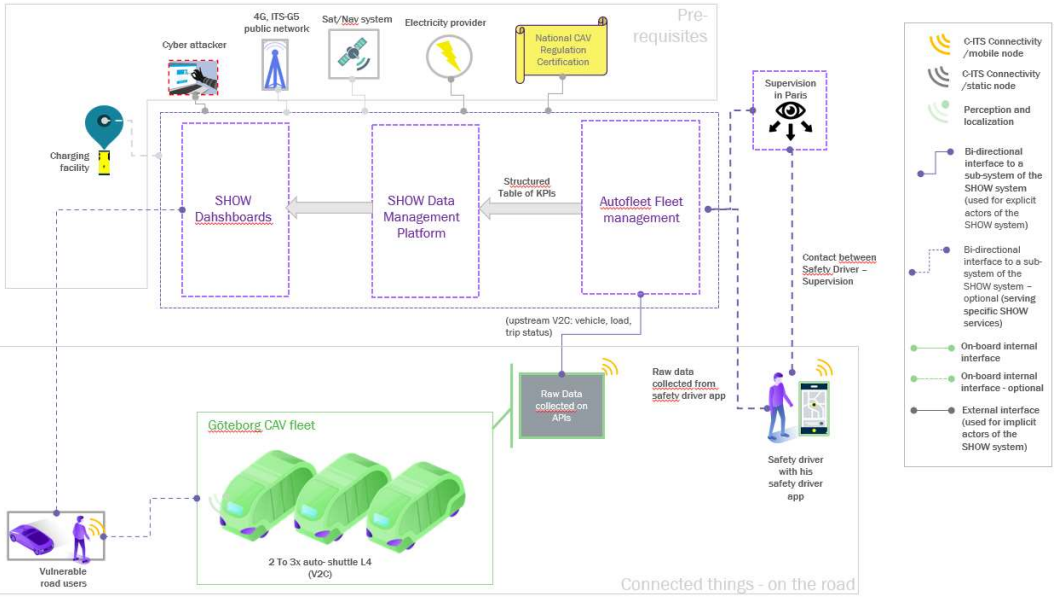


Figure 12: Gothenburg site local actors

A dedicated remote supervision team in Paris will monitor the experiment throughout the project. This supervision team will be able to monitor the location and status of the various automated vehicles in real time using the supervision tools provided by the manufacturer. It will be in permanent contact with the on-board safety drivers through a dedicated online conversation (via webRTC).

To supervise the performance of the experiment, Keolis is collaborating with the company Autofleet, which build dashboards of KPIs. To do this, Autofleet will take the raw data sent live by the automated vehicles on their APIs and by the Safety Driver application and transform it into key performance indicators that can be consulted on online dashboards. Access to these dashboards will be limited to Keolis and, for cybersecurity reasons, access

to live data from the manufacturer's API will be limited to Autofleet. However, structured KPI tables will be frequently uploaded throughout the project to the SHOW data management platform which will be linked to the SHOW dashboards. Thus, the KPIs produced by the Autofleet fleet management system will also be visible on the SHOW dashboards.

Finally, to assess the KPIs related to passenger perception, RISE will carry out on-site surveys and interviews.

Table 6: Local actors and their connectivity profile

Actor	Role	Connectivity
Service provider, Keolis Sweden	Passenger transportation and vehicle operations	Realtime connection between Autofleet and vehicles. Upload KPI extracted from Autofleet to SHOW SMDP
Cloud/connectivity infra, Ericsson	Dashboard 5G infrastructure	VRU connection to SMDP/SHOW Dashboard 5G onboard device MQTT data connection to SMDP/SHOW Dashboard
Chalmers campus	Site	No direct data connection.
Technical team on site, RISE	Interview, survey	Qualitative KPI to survey platform
SHOW commuters	Users of the SHOW fleet	No connectivity
Connected VRU	To limit the risk of collision with vulnerable road users, Keolis is planning to alert some selected VRUs when an automated vehicle passes in their surroundings. These selected VRUs will be alerted through their smartphones or a reflective vest equipped with sensor device that the selected VRUs will wear	Smartphone/smart vest
Safety driver app	On-board app providing vehicle info to the safety driver and to Autofleet cloud app.	Realtime connection between Autofleet and vehicles

4.2.2.2 Functional architecture

The local functional architecture is presented in Figure 13 while the data flows are as outlined in the Table 7 below. The automated vehicle does not provide data directly to the SHOW data platform, however real-time location data from auxiliary 5G equipped smart on-board device is provided directly to SMDP. Real time data are provided by the vehicle OEM clouds. KPI calculations are performed in the Autofleet fleet management platform: the KPI data are

extracted in the LFMP (managed by Autoflleet) and uploaded to the standardized SHOW SMDP interface. The Autofleet fleet management platform can be easily integrated to other services like smart traffic or smart city solutions, route planners, etc. However, at the initial phase of the pilot these are omitted to reduce complexity and to ensure that operations can commence on time.

Table 7: Fleet to LFMP to SDMP data flow summary

Information flow paths short description		
Connected fleets/VRUs **to** SMDP	Vehicle cloud, safety driver app **to** Autofleet	Autofleet **to** SMDP
Location data from 5G onboard device will be published to MQTT broker situated at SHOW SMDP and thus accessible from site dashboard (hosted in SHOW Dashboard).	Collect realtime vehicle data and safety driver app data, prepare the data for SHOW KPI's	Extract and upload KPI data to SMDP (via CKAN) to provide raw data for further KPI computations in SMDP and thus visualization in SHOW Dashboard

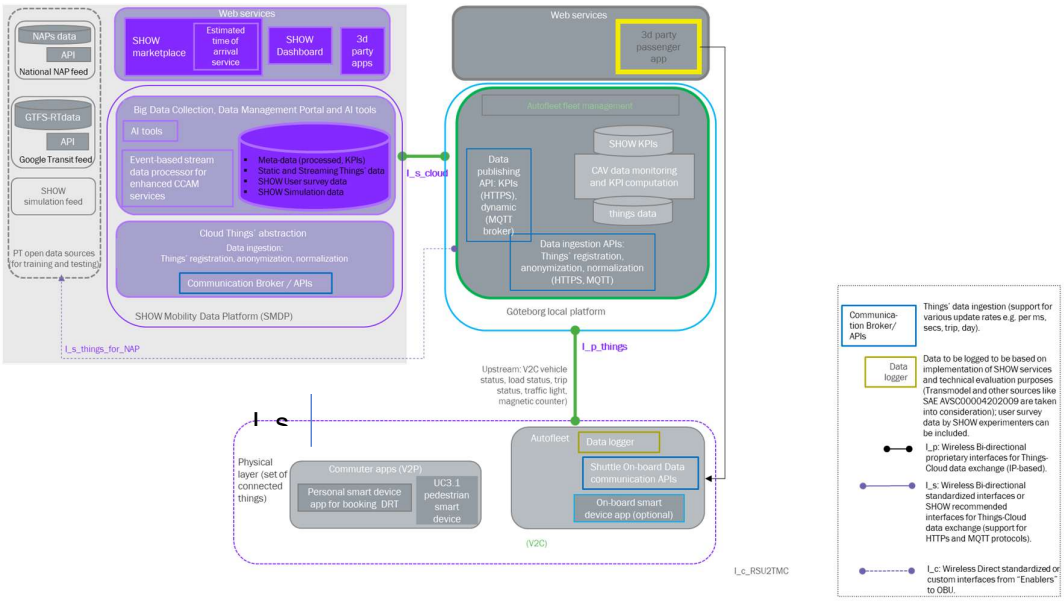


Figure 13: Gothenburg site functional architecture (better viewed in zoom-in mode)

Note: Here, reference architecture variation number 2 is assumed supporting both interface" I_s_things" and I_p_things (please refer to sec. 4.4.4 in revised D4.1 [1]).

4.2.2.2.1 Notes on Use Case 1.3

To limit the risk of collision with vulnerable road users, Keolis is planning to alert some selected VRUs when an automated vehicle passes in their surroundings. These selected VRUs will be alerted through their smartphones or a reflective vest equipped with sensor device that the selected VRUs will wear. To do that, the shuttles will be equipped with 5G

modem / router, as well as 5G antennas mounted on the roof of the shuttles. These 5G antennas will be directly connected to the 5G vEPC (virtual Evolved Packet Core) located in data center in Ericsson premises at Lindholmen.

Once a vehicle and a VRU geofence will be too close, an alert will be sent to the device (smartphone or reflective vest equipped with sensor) of the concerned VRU. Simultaneously, a notification will also be sent to the SHOW Dashboard.

Figure 14: Reflective vest equipped with sensor device + LED lights in front and back

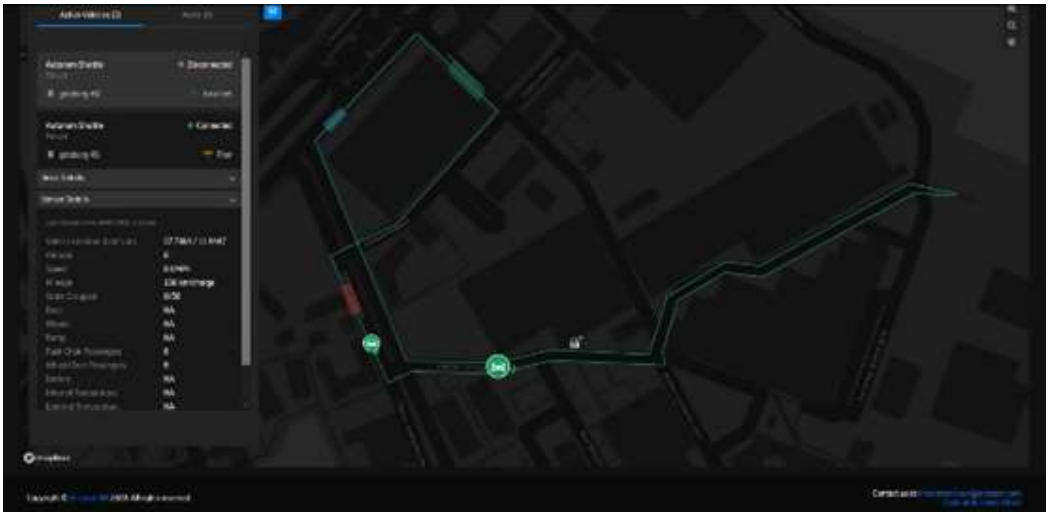


Figure 15: SHOW Dashboard making it possible to visualize location/heading of objects such as shuttles and Vulnerable Road Users (marked with vest icon in middle)

4.2.2.3 Service information flow

The service information flow is as described in Figure 16 and in the table that follows. The autonomous vehicles in the pilot will not be directly connected to the existing passenger services by the local operator. Autonomous vehicles communicate with Autofleet, that in turn supply SMDP with KPI related data in the form of CSV files. Autofleet also collects data from safety driver app. Operational data between vehicle cloud/safety driver app and Autofleet is handled in real time.

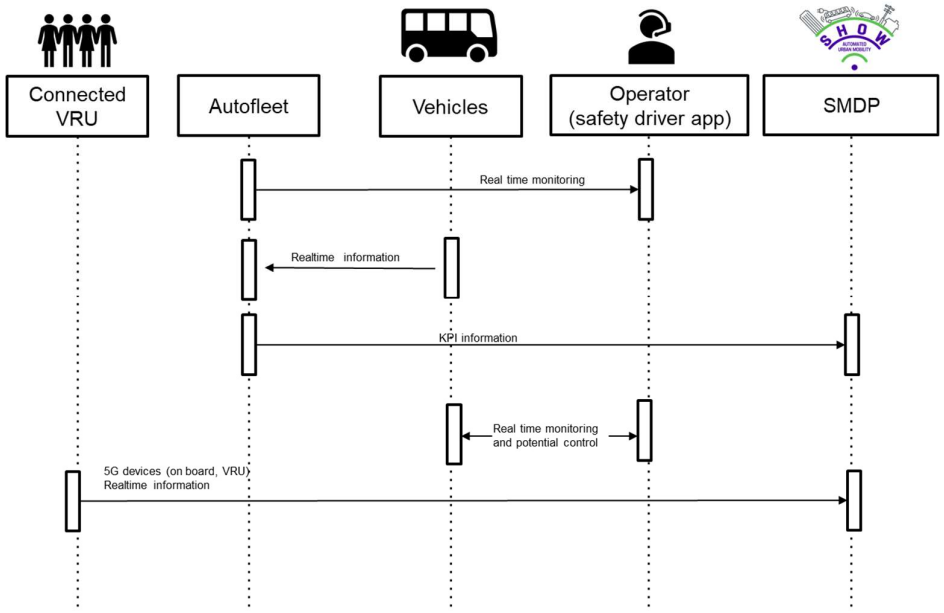


Figure 16: Services information flow diagrams

Table 8: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
Autofleet	Fleet management platform that will collect data from driver and vehicle and prepare KPI data to upload to SHOW SMDP. Connection with vehicle cloud and safety driver app	KPI data
Operator/driver (safety driver app)	Vehicle provides the operator/safety driver and Autofleet with operational data.	Updated routing data.

4.2.2.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if any)

There is no direct connection from any SHOW cloud subsystems to the vehicles (except connections from OEM systems if any). All data flows are one way (extraction of data and populate inside local data platform). All connections are secured with SSL.

Cybersecurity follows vehicle manufacturers standard security practices and there is no sensitive data transferred between the vehicle and the local fleet management platform.

The site will have safety drivers inside the vehicles. Under the current permits we are not allowed to deviate from the programmed route.

4.3 Rouen local architecture

4.3.1 The local technology actors

The **Rouen-Vernon France Megasite** includes two sites located in the Normandy region with two types of autonomous mobility services (Shared AV shuttles and on demand AV robotaxis). The services are open to members of the public including tourists, students and professionals (generally subscribed in panels). Both types of services are monitored by Transdev's remote supervision system which enables tracking of the correct functioning of vehicle and infrastructure systems, mission management, passenger interface and remote interventions.

In Figure 17 and Figure 18, we present the architecture diagrams depicting the pilot site actors that are implicitly or explicitly present. The actors' roles and connectivity profile is described in Table 9.

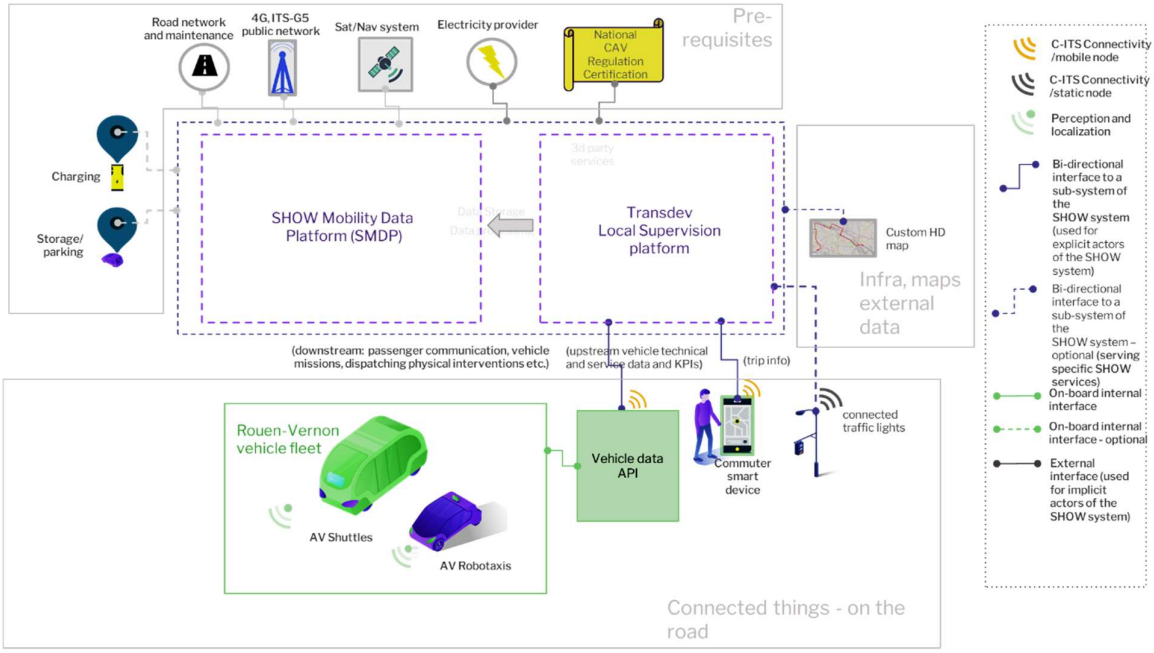


Figure 17: Rouen-Vernon site local actors

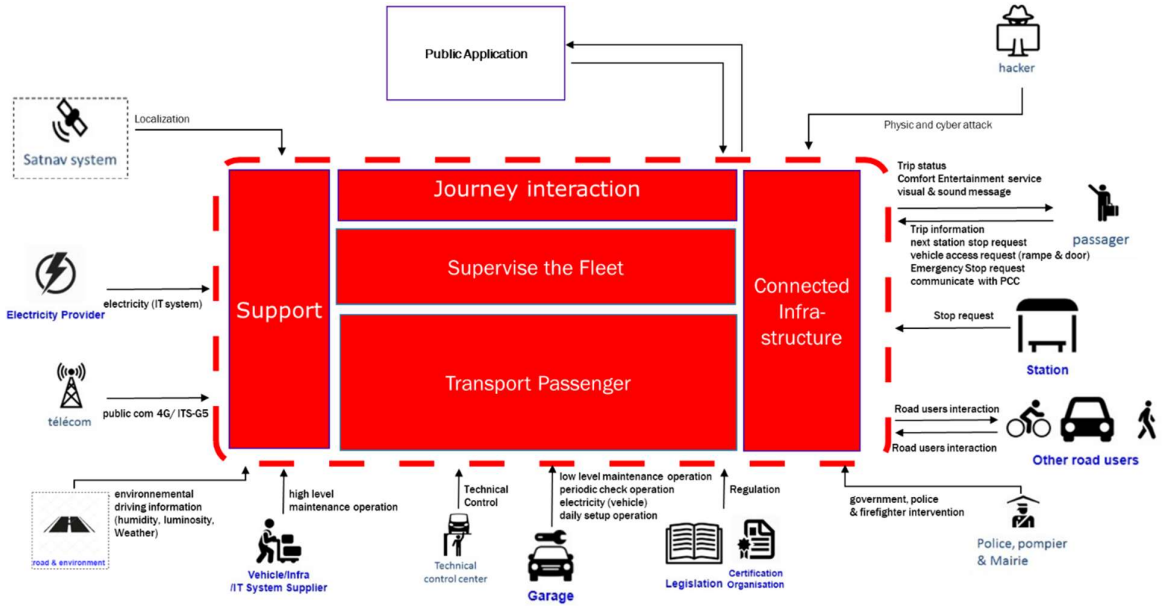


Figure 18: Rouen-Vernon site local actors (alternate view)

Table 9: Local actors and their connectivity profile

Actor	Role	Connectivity
AV Shuttles	Part of shared transport service (regular bus line on a predefined route)	V2C
AV Robotaxis	Part of on demand transport service	V2C
Infrastructure (connected traffic lights)	Smart traffic lights communicate with vehicles directly and can regulate traffic flow priorities	I2C
Supervision system	System enabling tracking of vehicle and infrastructure systems, mission management and remote interventions. A human is always in the loop in the local supervision centre, which is situated in the same control centre room as for the Rouen Public Transport system.	Cloud
Users	Booking and execution of a trips for “on-demand” transport, obtaining service and timetable information for regular shuttle service	App / website

4.3.2 Functional architecture

Rouen-Vernon' site functional architecture (component level) is presented in Figure 19 and the data exchange (single-directional) among the LFMP, SMDP and the fleet is described hereafter:

- Connected fleet/passengers **to** local LFMP/Dashboard:
  - Passengers interact with the service via a mobile app or website, where it is possible to obtain information relating to the service, or to book journeys in the case of on-demand transport.
  - The vehicle fleet and infrastructure are connected to the Transdev Local Supervision System and key data and KPIs are uploaded.

- Local LFMP/Dashboard **to** connected fleet/passengers :
  - The back end of the Transdev Local Supervision System manages vehicle missions and can send instructions to the fleet to perform given journeys or carry out key actions.
  - The Supervision system also enables a communication link to passengers (Human Machine Interface).
  - A human is always in the loop in the supervision centre.

- Transdev Local Supervision Platform to SMDP: Data and KPI extracts can be sent from the Transdev Local Supervision Platform to the SMDP.

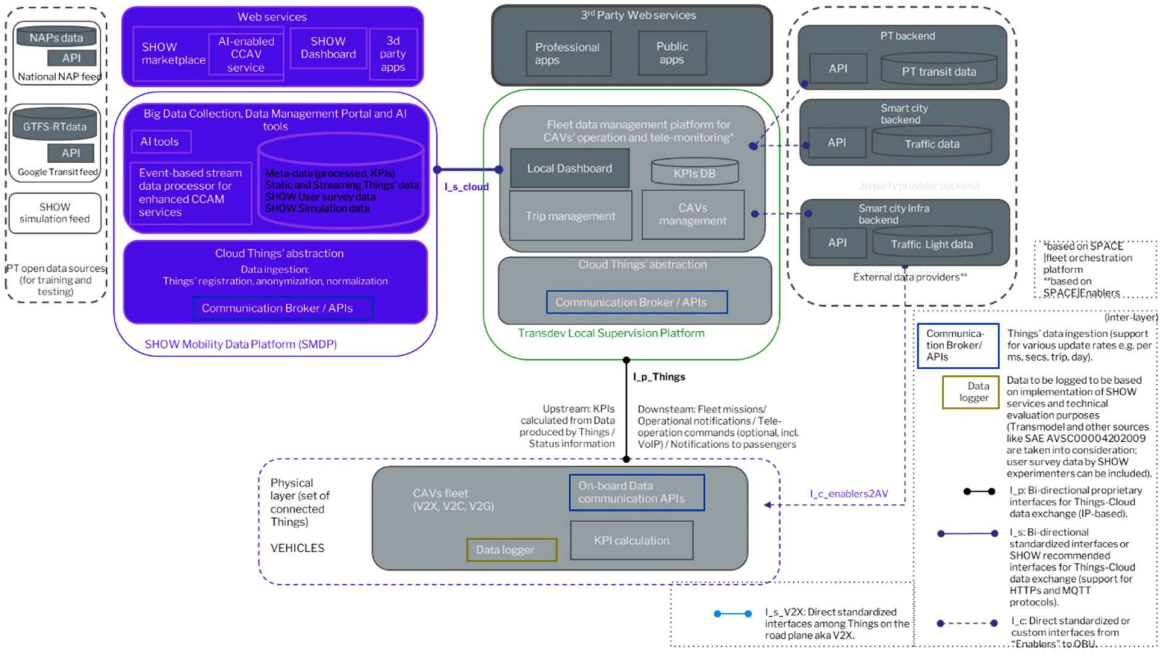


Figure 19: Functional architecture diagram (better viewed in zoom-in mode)

4.3.3 Service information flow

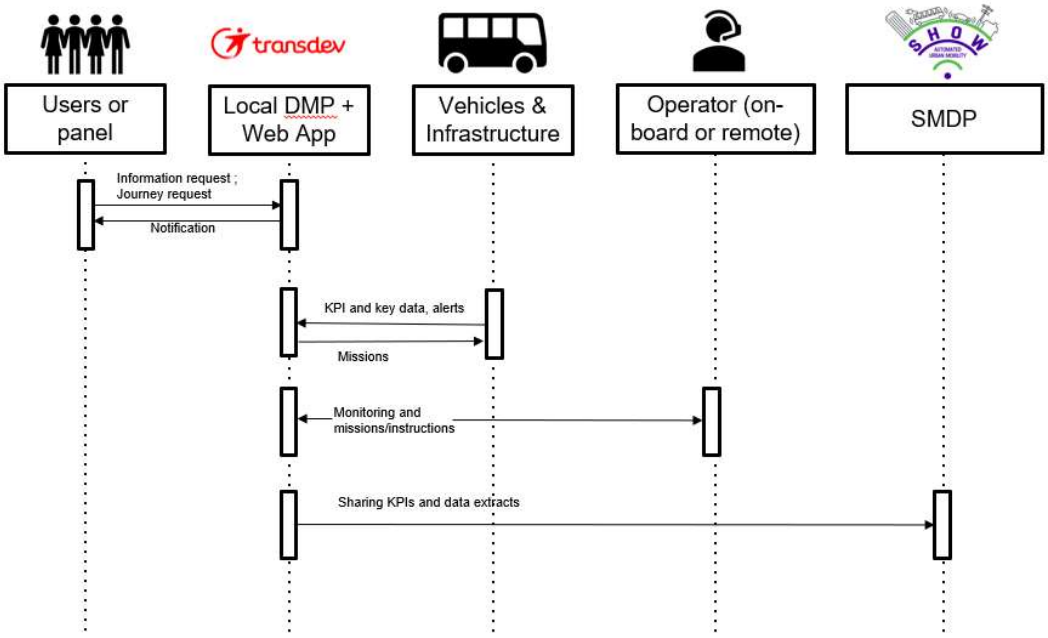


Figure 20: Service information flow in Rouen-Vernon pilot site

The service information flow is as described in Figure 20 and in the table Table 10 that follows.

Table 10: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)

Users / panel	User of the mobility service (normally part of a pre-selected panel for the purposes of the pilot)	• Users can access information relating to the service via app/website
		  ○ Timetables
		  ○ Alerts
		• Users can book journeys for the on-demand transport service
		  ○ Pick up/drop off location and timing

Vehicles and Infrastructure	Vehicle fleet (shuttles and robotaxis) and connected traffic lights	• Key data and KPIs sent to the Transdev Local Supervision Platform • Receive missions from Transdev Local Supervision Platform

Transdev Local Supervision System	System enabling tracking of vehicle and infrastructure systems, mission management and remote interventions.	• System monitoring
		  ○ Vehicles
		  ○ Infrastructure
		• Mission management
		  ○ Timetables

Local Service	Short description	Data used (coming from fleet, devices, infra)
	A human is always in the loop in the local supervision centre, which is situated in the same control centre room as for the Rouen Public Transport system.	○ Customer on demand journey requests • Passenger interface via HMI • Managing non-nominal situations (roadworks, accidents, public demonstrations, passenger illness…)
Operators (on board or remote)	"Human in the loop" – operators on board during pilot phase; remote supervisors in the Supervision Control Centre	• System monitoring and reception of alerts originating from the vehicle fleet or infrastructure • Assigning of journey missions for the vehicle (NB. This is NOT remote driving) or key actions (e.g. door opening) • Passenger interface • Interactions with law and order and emergency services

4.3.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if any)

Connectivity and integration with SMDP followed connectivity and cybersecurity guidelines provided, establishing an authenticated and encrypted connectivity between the Rouen LFDP and the SMDP for KPI data exchange.

4.4 Karlsruhe local architecture

4.4.1 The local technology actors

As presented in Figure 21, in the Karlsruhe pilot site the users interact with the Shuttles via the SHOW mobility service app / website, where a trip can be booked. The Shuttle backend (local fleet management platform) is then processing the request and deploys the request to the available fleet which returns the vehicle that is currently available. The selected vehicle is then conducting the trip by picking up and dropping off at the desired locations. During the ride, vehicles are supported via V2I communication enabled by intelligent and smart infrastructure for connected driving, which is supplied by the Test Area Autonomous Driving Baden-Württemberg (TAF-BW).

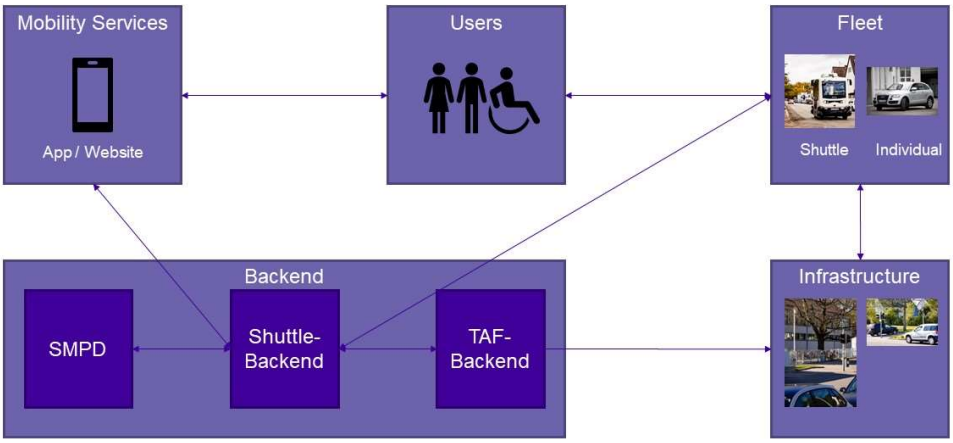


Figure 21: Local actors in Karlsruhe pilot site

The technology actors' roles and connectivity profile is described in Table 11.

Table 11: Local actors and their connectivity profile

Actor	Role	Connectivity
Mini-shuttle	Part of DRT service for passengers and Cargo	V2C
Retrofitted vehicle: Modified Q5	Part of DRT service for passengers and Cargo	V2C / LTE
Users	Booking and execution of a trip	App / website
Infrastructure (Light signals,..)	Sending / Receiving SpaT, MAP, CAM, CPMs	V2I
Shuttle backend/TAF backend	Local fleet management platform	Cloud

4.4.2 The functional architecture

Karlsruhe' site functional architecture (component level) is presented in Figure 22 and the data exchange (single-directional) among the LFMP, SMDP and the fleet is described hereafter:

- Connected fleet/passengers **to** local LFMP/Dashboard:
  - The users can interact with the mobility service through an app or the website, where they can book a trip by selecting a starting and end location. These locations are transformed into GPS positions, which then are processed and scheduled in the backend.
  - The backend also processes further incoming data from the individual vehicles (e.g. current state of charge, global position etc.)

- Local LFMP/Dashboard **to** connected fleet/passengers :
  - The backend processes the desired trips and assigns it to individual vehicles.
  - If there is a vehicle available, the users receive either a positive or negative feedback.
  - The backend provides additional information from the smart and intelligent infrastructure to the individual vehicles.

- LFMP to SMDP:
  - The logged data from the shuttles is processed and the KPIs are extracted from the recorded data of individual vehicles.
  - KPIs are then exported and sent to the SMDP

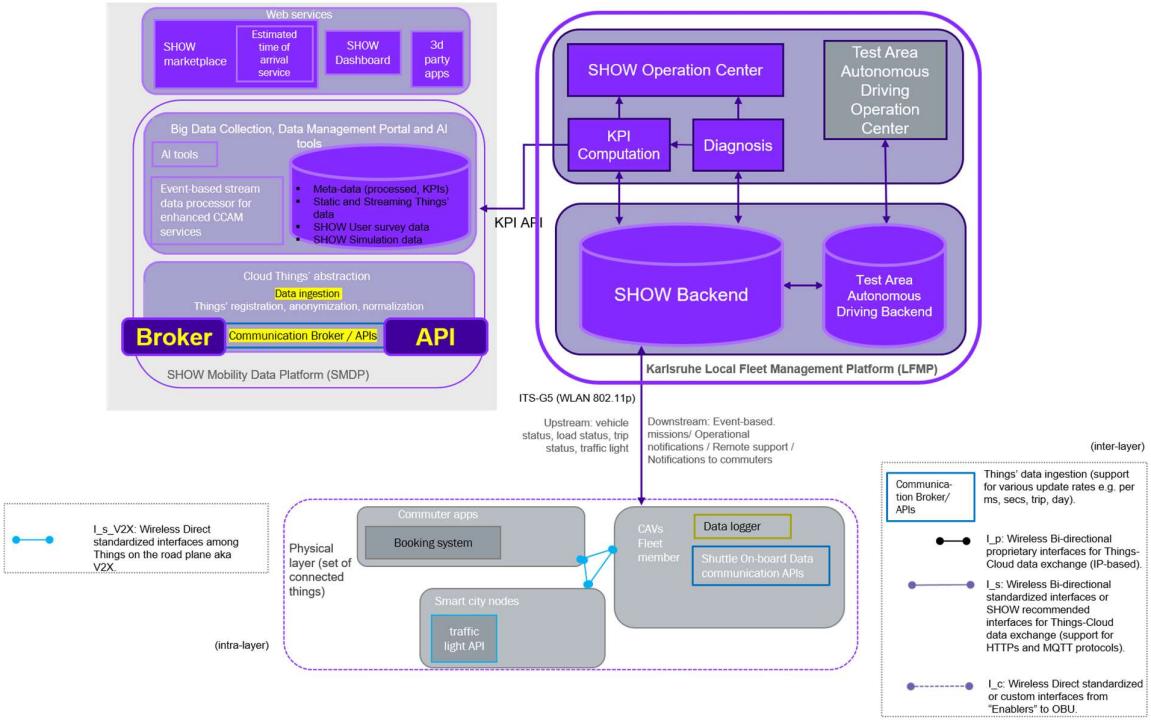


Figure 22: Karlsruhe Demo site functional architecture (better viewed in zoom-in mode)

4.4.3 Service information flow

The service information flow is as described in Figure 23 and in the Table 12 that follows.

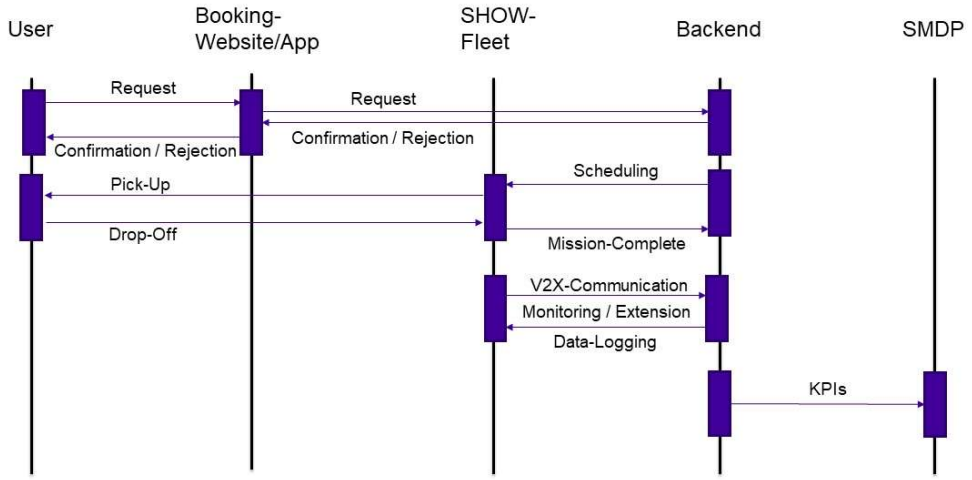


Figure 23: Service information flow

Table 12: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
User	User of the mobility service	• Using the app/website to request a trip sending GPS-positions • Pick-Up / Drop-off
Booking (App/Website)	Interface for Users	• Sending GPS-positions from start / endpoint of the desired trip • Sending Confirmation / Rejection to User
Backend	Intelligent backend, which is processing the incoming request, the infrastructure and shuttle data	• Scheduling of fleet • Processing of infrastructure data • Monitoring of shuttle status • Post-Processing of data logging data
Fleet	The individual vehicles (shuttle, modified Q5)	• Executing the incoming trips (Pick-Up and Drop-Off of passengers) • Receiving data from smart Infrastructure • Sending monitoring status

4.4.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if any)

No custom developments. Connectivity and integration with SMDP followed cybersecurity guidelines provided, establishing an authenticated and encrypted connectivity between the LFMP and the SMDP for fleet data/KPIs exchange.

4.5 The Austrian Pilot sites

4.5.1 Graz local architecture

4.5.1.1 The local technology actors

Graz conceptual architecture including all technological components interacting with the SMDP are presented in the diagram of Figure 24 and the Table 13. The vehicle fleet in Graz consists of two automated vehicles. Both cars are research passenger vehicles equipped with automated driving functionality. They can both be driven either manually or automatically. In automated mode, a safety driver must always be present and able to take over the vehicle at any time. The vehicles technically have 2 ways to communicate with the outside world, firstly traditional short range V2X for the local environment and secondly cellular V2N (4G/5G) to connect to the internet. At the time writing, it is not yet fully clear whether both vehicles will have the same capabilities or whether there will be a difference.

An essential task of the automated journey is to drive through a bus terminal. Here, it must be determined which bus bay is available, i.e. free of buses, and where few VRUs are at risk. For this reason, the bus terminal digital infrastructure must allow to detect presence of buses and acquire information of buses arriving soon. The buses transmit their GPS position to the local city public transport management to provide real-time data. This real-time data is then forwarded nationally to a country-wide traffic information system. The latter can be accessed via the internet using an API and can be queried by the vehicles. In addition, the bus terminal is monitored via a smart camera system, which includes a connected C-ITS Road Side Unit. The smart camera detects the bounding boxes of the objects in its view, classifies them and provides corresponding information locally to the C-ITS Road Side Unit, which further sends out C-ITS messages to the vehicles.

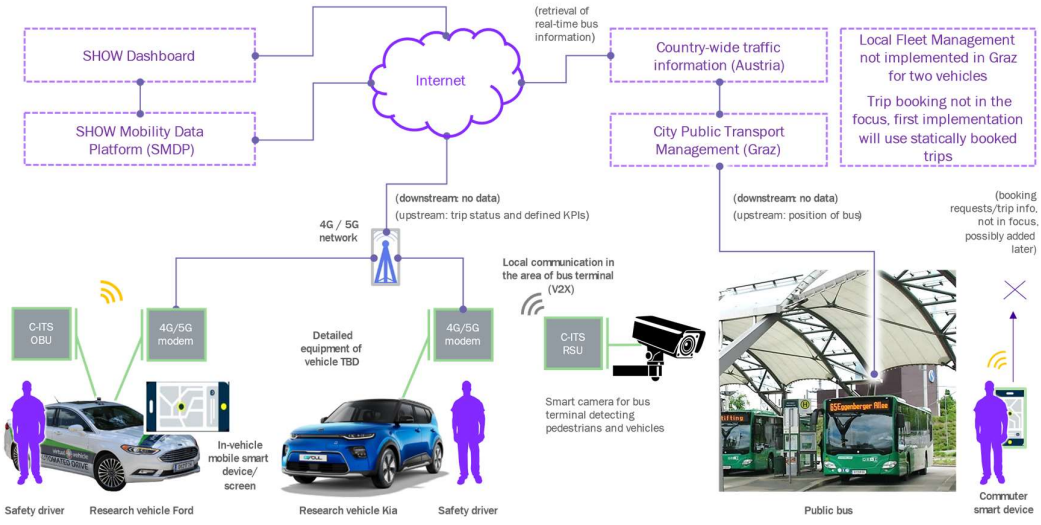


Figure 24: SHOW pilot architecture in Graz

The focus in the Graz Pilot Site is on the technical challenges of passing through the terminal, a trip booking by users is out of scope, as this can be successfully presented in other sites

independently. Therefore, local fleet management is not implemented, because trip bookings are not carried out here either. Users in Graz who want to use the service are attracted from the pool of people at the bus terminal on one side or at the shopping center on the other side. They do not have to order the ride in advance; they only need to approach the vehicle for a ride.

Table 13: Local actors and their connectivity profile

Actor	Role	Connectivity
Vehicle 1 / 2	Part of DRT service for passengers	Cellular V2C (4G/5G) and ETSI V2X
Safety Driver	Taking over in safety-critical situations; not needed for normal operation for driving; assisting passengers for getting into the vehicle	-
Smart camera system (including a C-ITS Road Side Unit)	Observing bus terminal for detecting empty spots and VRUs density	ETSI I2N
Public bus	Public transport. Transfer connection from AV.	Proprietary connection to local city transport management
Commuter / User	User of the service	No connectivity foreseen
City Public Transport Management	Overview of all public transport vehicles in the city	Proprietary connections
Country-wide traffic information	Information about all public transport vehicles in entire Austria	REST API over the Internet

4.5.1.2 Functional architecture

As explained above, there are no local LFMP, no local dashboard and other internal components in the Graz pilot site. Therefore, reference architecture variation number 2 supporting solely the interface" I_s_Things" is assumed *(please refer to sec. 4.4.4 in revised* [1]) and the reference SHOW Dashboard will be used for monitoring vehicles 'positions / KPIs (Fleet to SMDP is realized through REST API over the Internet).

4.5.1.3 Service information flow

In the following figure (Figure 25), the information flow for the Graz pilot site is illustrated. Since there is no booking process, a potential user of the service approaches the vehicle for a ride. In this initial process, the safety driver helps with the registration of the trip. The fixed route consists of three stops, whereby the middle stop is initially not scheduled for boarding. Typically, users requesting the service will do this one of the end stops and the destination

will be the other end stop. This means that a destination typically does not need to be given from the user to the vehicle service.

After boarding the vehicle, the automated trip starts along the route. During this time, regular information about the trip status and other SHOW KPIs is sent to the SHOW dashboard. This includes e.g. position, speed, acceleration etc. When approaching the bus terminal, the vehicle needs to determine the local path for a safe passage through the terminal. Therefore, it receives information about the bus terminal environment from the smart camera via C-ITS. This information already helps to see the current utilization of the bus bays. In addition, further busses might be just about to enter the terminal in the following seconds. To cover that information as well, a query of the real-time of bus arrivals is done via the countrywide traffic information service. This not only includes scheduled arrival times, but also delay information for busses.

Details on this information sequence are still being refined as the pre-demo phase progresses.

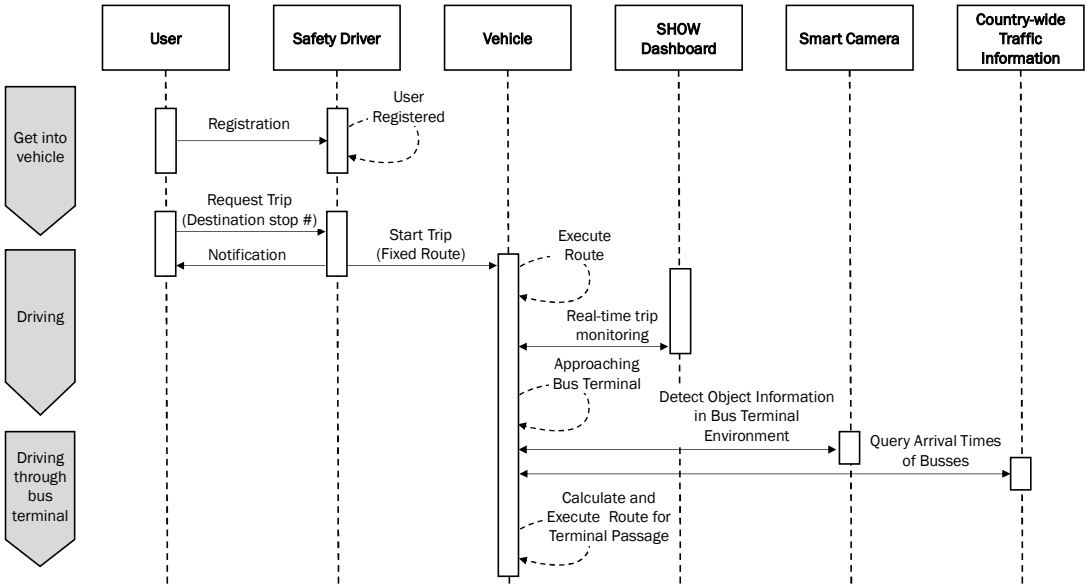


Figure 25: Information flow diagram for Graz

The local service is implemented in two phases:

- Phase a, support for a ride from bus terminal to shopping center and back: The ride itself can in principle be carried out completely independently of infrastructural data and is executed locally by the vehicle. Real-time trip monitoring to the SHOW dashboard is necessary for the functionality per se. Depending on the AV stop location at the bus terminal (before or after the bus bays), additional requests from smart camera and traffic information data is performed.
- Phase b, support for a ride to middle stop is added: Recognition of getting on/ getting off requests from passengers need to be added in a later stage.

4.5.1.4 Interoperability, Connectivity, Cybersecurity solutions applied (if any)

The Graz pilot site will initially start operation totally independent of infrastructural connectivity. After that, connectivity will be expanded step by step, first with 4G/5G and then with C-ITS. This expansion will only take place after the pre-demo phase due to the limited resources of the partners involved. Any challenges faced during implementation can therefore not be reported yet in this description and will be added in later documents. Connectivity and integration with SMDP followed cybersecurity guidelines provided, establishing an

authenticated and encrypted connectivity between the local fleet and the SMDP for fleet data exchange.

4.5.2 Salzburg local architecture

4.5.2.1 The local technology actors

Figure 26 describes the system conceptual view in the Pilot Site Salzburg. Table 14 adds textual description of the local actors, their role as well as their connectivity.

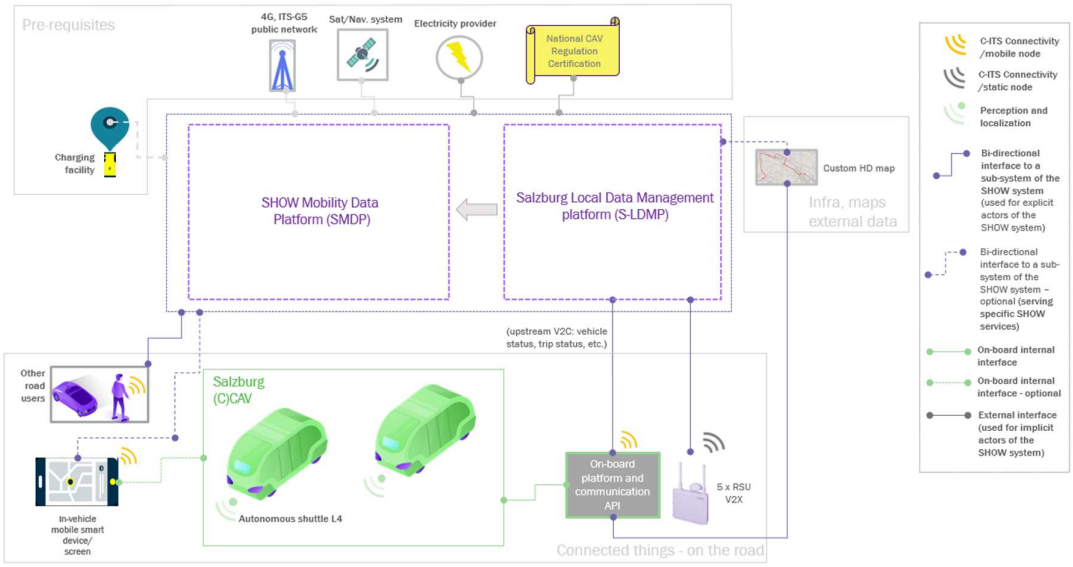


Figure 26: System conceptual view – Pilot Site Salzburg

Table 14: Local actors and their connectivity profile

Actor	Role	Connectivity
Automated shuttles L4	Part of AV DRT service for passengers	Vehicle to on-board platform and communication API
On-board platform and communication API	Data logger and V2C upstream to S-LDMP	V2C
Road Side Units	C-ITS data collection and broadcast of C-ITS Services (e.g. DENM)	V2I, I2V, I2C
Custom HD map	Provision of waypoints for navigational purpose; data cleansing (e.g. map-matching)	HTTP-APIs
In-vehicle smart-device/screen	Provision of information to passengers (e.g. next stop)	On-board platform

4.5.2.2 Functional architecture

In Table 15 the local architecture of the Salzburg pilot is described by explaining the three information flows depicted with the green, black and purple arrows in Figure 27.

Information flow paths short description		
S-LFMP Connections	S-LFMP internal dataflow	Mid-Term POC
Connection of Data logged by physical Things to S-LFMP. • CAVs Log Data locally, Onboard data communication transfers data via MQTT based Protocol to S-LFMP • V2X Devices submit data to RSU´s. RSU´s transfer data via AMQP based Protocol to S-LFMP • Local KPI Monitoring Dashboard access KPIs for Stream Data and KPIs Database to visualize and monitor State	• S-LFMP received data (MQTT/AMQP) is integrated using a streaming layer. • Data Cleaning and Validation is done using Device Metadata and HD Map Data (e.g. Map-Matching). • Data is streamed into KPI computated, results are pushed back to Stream Platform for further usage (e.g. Database Storage or Transfer to SHOW)	Show Connectivity Component transfers data (KPIs, Devices Data) accessible in Stream Layer via MQTT based Protocol to SMDP

Table 15: Description of information flow paths – Pilot Site Salzburg

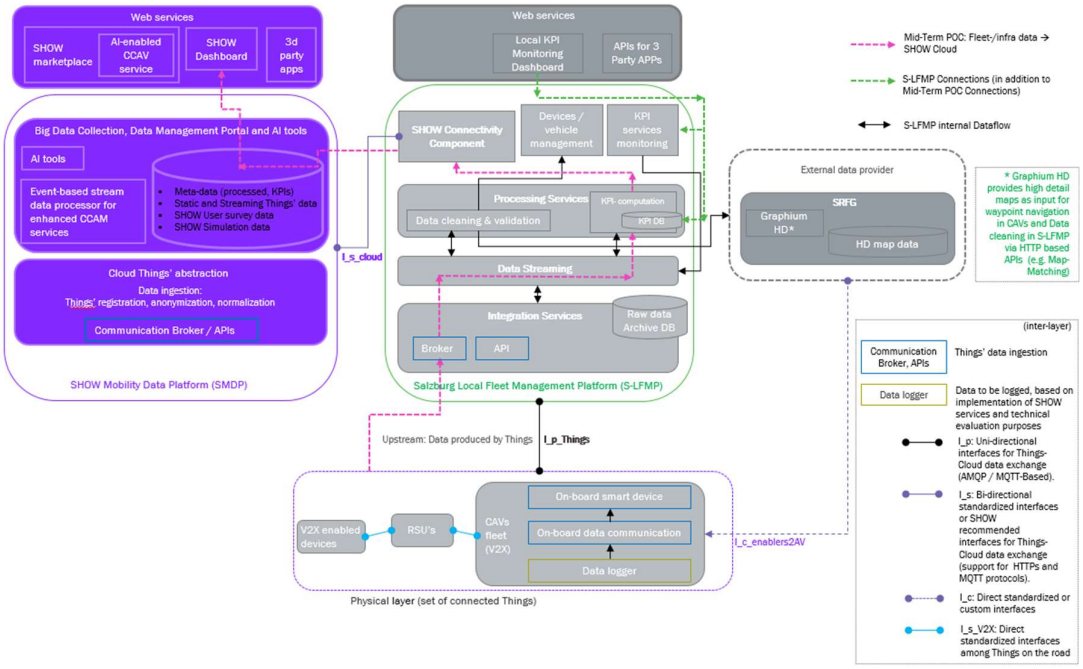


Figure 27: Local Architecture – Pilot Site Salzburg (better viewed in zoom-in mode)

4.5.2.3 Service information flow

Limited information. To be added in D4.4.

4.5.2.4 Interoperability, Connectivity, Cybersecurity solutions applied (if any)

Limited information. To be added in D4.4.

4.5.3 Carinthia local architecture

There are two test sites in Carinthia, one is in Pörtschach at the Lake Wörthersee and one is in the city of Klagenfurt (planning of the pre-demo phase for the latter is ongoing work). For both sites, information on the local architecture was not complete and therefore we report what it is available while what is missing will be provided in the next version of the deliverable.

4.5.3.1 Local technology actors

Klagenfurt: This is a site with a complex traffic situation. The route will include traffic lights, a roundabout and different and traffic barriers. There are three different route options, which will be implemented as level 1-3, the final route length will be 4.4 km. The route will connect the train station with a living area, restaurants, shops, the university and a business and science park. On this route we have a high variety of stakeholders: tourists, students, and commuters.

Pörtschach: The demo site of Pörtschach is a site with a length of 2.7 km and 8 bus stops. Pörtschach is situated directly at the Lake Wörthersee and therefore a typical Austrian tourist area. The route is connecting the train station with the lake, hotels, shops, and the town center. End users and stakeholders on this site are mainly tourists, younger students, senior citizens, and public interest groups (tourist organizations, hotel owners, public authorities).

The pre-demo in Pörtschach started at the end of September and was running until end of November 2021.

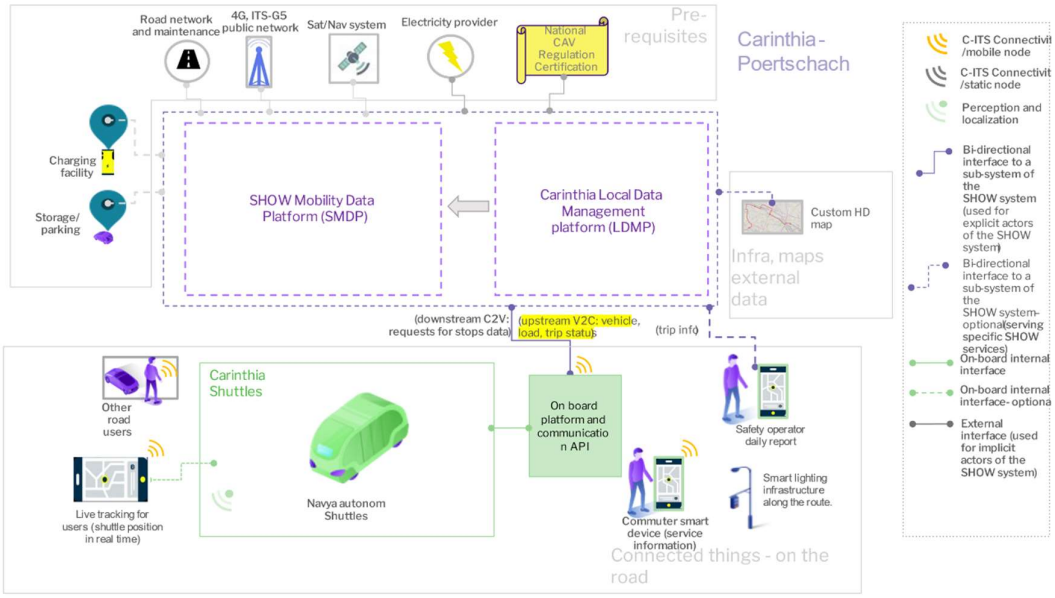


Figure 28: Local actors in the pilot site of Pörtschach (Carinthia)

The conceptual architecture for the SHOW system in Pörtschach is provided in Figure 28. On site, storage and parking is provided by the local community, together with the charging possibility. 4G/LTE is currently used in Pörtschach, 5G is under development. Along the route, there is smart lighting infrastructure implemented. The data is not processed in the LDMP. Live tracking is possible over an external device inside the shuttle. Users are able to follow the location via the official website of SURAAA.

Figure 29: Autonomous Shuttle at demo site Pörtschach (© SURAAA)

The following actors are involved in Pörtschach:

- **Navya**: Shuttle provider (see Figure 29)
- Local public transport providers
  - External App provider already list the shuttle in the official public service schedule (see Figure 30)

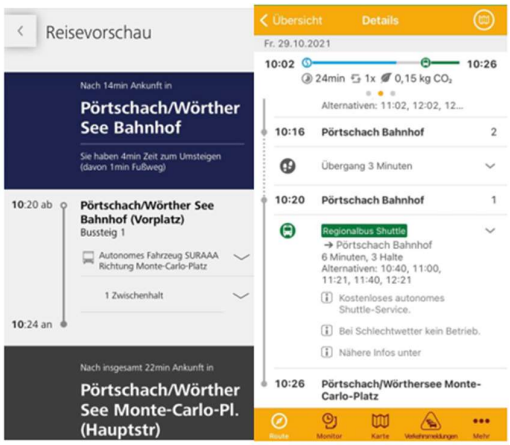


Figure 30: Public transport booking platforms OEBB and Kaerntner Linien

4.5.3.2 Functional architecture

At this point it is not possible to provide a diagram for the demo sites, because the current state of the API negotiations is still in progress. The missing information will be added in the next version of the deliverable.

4.5.3.3 Service information flow

The diagram of Figure 31 shows the current situation at the demo site in Pörtschach. More information to be added in the next version of the deliverable.

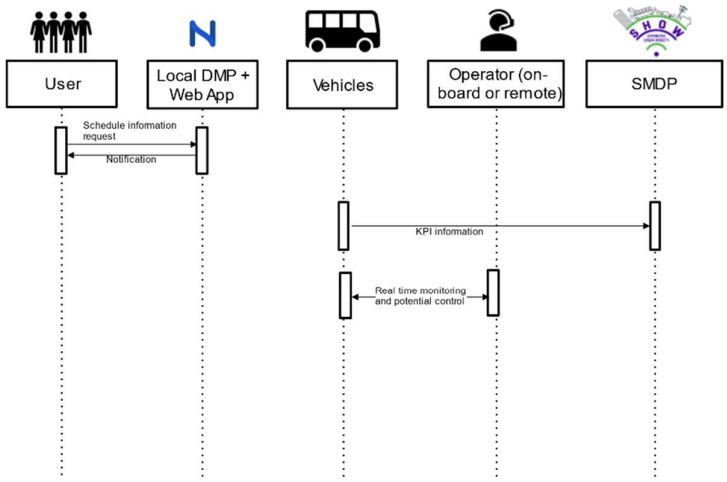


Figure 31: Service information flow at Pörtschach pilot site

4.5.3.4 Interoperability, Connectivity, Cybersecurity solutions applied (if any)

No custom implementations were expected for the test site in Pörtschach. For Klagenfurt test site, information will be added when the new demo site design and implementation is finalized.

4.6 Turin local architecture

4.6.1 The local technology actors

The Turin pilot site will demonstrate the use of two automated shuttles with on demand reservation. Moreover, an RSU will be dedicated to test a VRU warning service while the connection with the Turin Traffic Control Center will enable the validation of TLF/TLA[5] applications.

In the Turin pilot site the following actors are involved:

- LINKS: Pilot site leader. Installation of **RSUs for VRU warning** and TLA/TLF services
- Navya: Automated shuttles provider
- Swarco and 5T: Responsible of the **traffic control center**. Managing of TLA/TLF messages and of the **control of traffic lights**
- **IOKI**: provider of the on-demand reservation application and **backend**. Managing of the connection with the **SHOW Data Management platform**
- GTT: **Turin public transport operator (PTO)**, providing the safety drivers and responsible for the daily operations of the shuttles.

The high-level architecture is depicted in Figure 32.

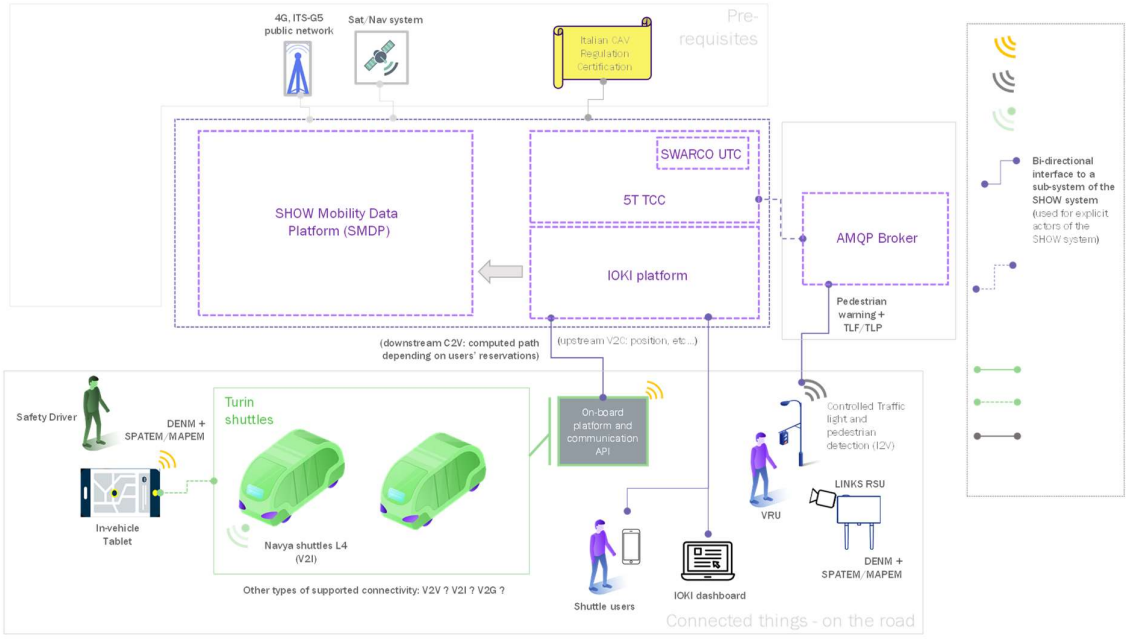


Figure 32: High-level architecture in Turin

Two automated Navya shuttles (Figure 33) will carry on and drop out people on a pre-computed path depending on the on-demand requests. The shuttle is equipped with a V2I short-range communication platform using ETSI ITS G5 and exchanging ETSI compliant messages (e.g CAM [1]). The shuttle can also rely on V2C connectivity towards IOKI backend through 4G connectivity.

[5] Traffic Light Forecast and Assistance

Moreover, the safety driver will receive notifications about VRUs and the status of traffic lights through an on-board smartphone connected in LTE to the 5T control center (TCC) that will act as a concentrator for this type of information.

Figure 33: Navya Shuttle

Two LINKS RSUs (Figure 34) will be installed, the first one will be equipped with camera and LiDAR sensors while the second only with a camera. Besides, the RSUs will mount short and long-range radio connectivity respectively based on ETSI ITS G5 and LTE/5G communications. Finally, the RSUs are equipped with an NVIDIA GPU in order to timely detect VRUs crossing the street and generate a warning on the smartphone for the safety driver.

Figure 34: Example of LINKS RSU with camera

All the ETSI messages coming from the street will be collected by a broker hosted in 5T TCC and the connectivity through the traffic lights will be managed by a SWARCO SW component.

The information used to book the shuttle by the users are managed by IOKI app and backend. The IOKI travellers' app will allow users to book their passage on the shuttles. The backend application will pre-compute the best shuttles path based on all the received reservations and send them to the GTT safety drivers (IOKI drivers' app) and to the shuttle itself. Moreover, the backend will collect information from the vehicle that will then be used to compute the project KPIs (thanks to the connection to the SHOW Data Management Platform) and other useful indicators useful for the PTO (shown in the IOKI operator dashboard).

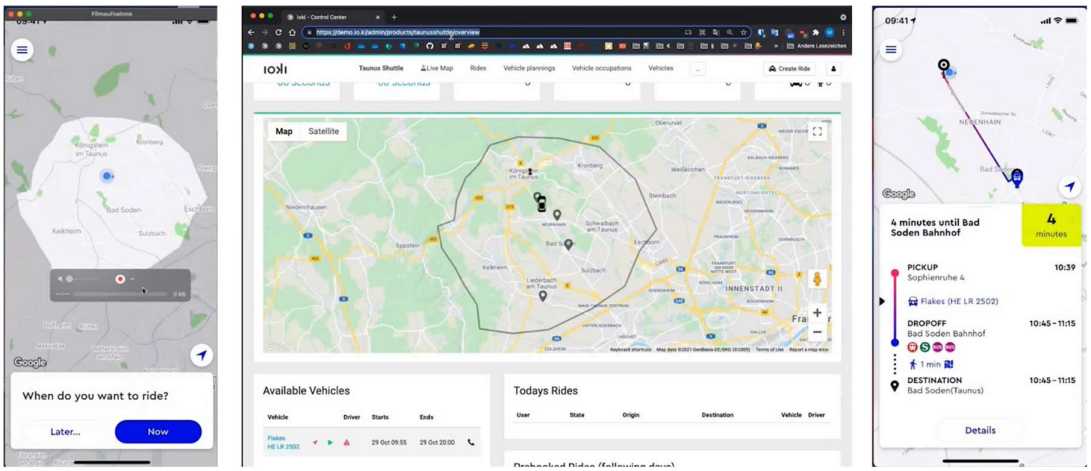


Figure 35: Example of IOKI web platform and app

4.6.2 Functional architecture

The detailed block diagram of the Turin Pilot Site is shown in Figure 36.

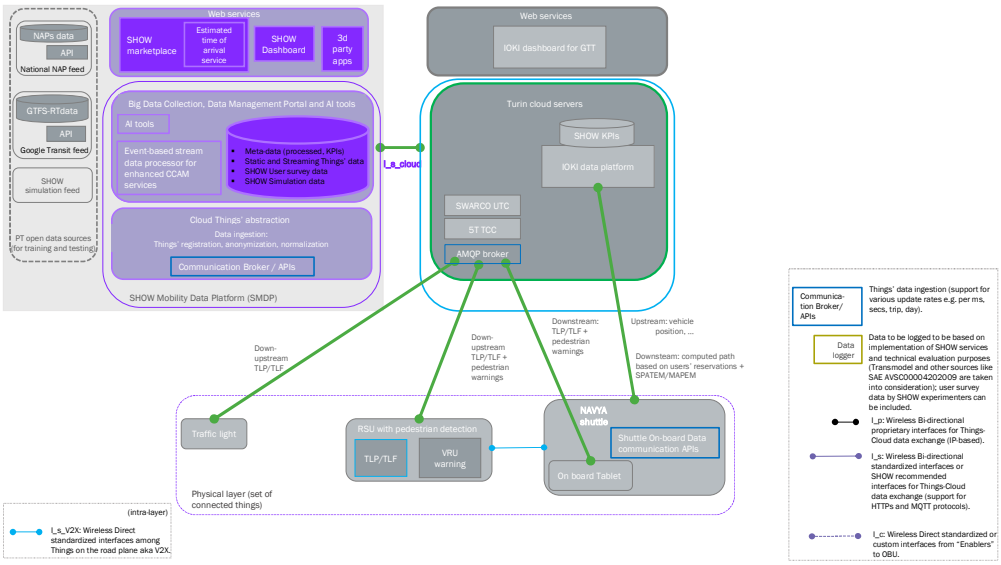


Figure 36: Turin demo site functional architecture diagram (better viewed in zoom-in mode)

In Turin there are two main data flows, namely:

- Shuttle's data and reservation: this data flow is directly managed by the IOKI application with a direct link to the shuttles.
- VRU and traffic light: this flow is managed using ETSI ITS compliant messages. Moreover, the data exchanged on the cellular network are transported using AMPQ 1.0 with an approach fully compliant with the C-ROADS [2] specifications

More in detail, the IOKI platform will retrieve real-time data from the shuttles using Navya proprietary APIs through a cellular connection. The users of the shuttle service can book their reservations thanks to a smartphone. The IOKI application computes the best path and makes it available through an app that can be used by GTT safety drivers. All the data coming from the shuttles will be used to compute the project KPIs and will be shared with the SHOW MDP.

The VRU service starts on the RSU where an AI-based real-time algorithm is able to detect pedestrians crossing the street. This information is coded as an ETSI ITS DENM [3] message and is sent by the RSU through a 5G modem to an AMQP 1.0 [4] broker hosted in the 5T TCC. The warning is then retrieved by the safety driver smartphone (via 4G network) if and when the shuttle is near the involved crossroad. This warning is useful to raise the attention of the safety driver in a possibly dangerous situation. Moreover, it is important to notice that the RSU sensors (LiDAR and camera) will detect the VRU even in a situation where the shuttle sensor could fail (e.g. due to some obstruction).

For what concern the TLA/TLF service, it starts when the shuttle is approaching a junction equipped with an RSU. The RSU receives the shuttle CAM and consequently sends a priority request to the traffic control center (again sending it to the TCC broker). This request is coded like a Signal Request Extended Message (SREM). The TCC, towards some SWARCO proprietary components, will interact with the traffic lights infrastructure and, if the priority can be granted, a Signal Response Message (SSEM) is published over the broker and can be retrieved by the on-board smartphone. Moreover, the RSU will read from the broker information about the phases of the traffic light (SPATEM/MAPEM messages) and will broadcast them over the ETSI ITS G5 short-range channel. The same information can be read by the smartphone over LTE.

4.6.3 Service information flow

In Figure 37, the service information flow diagrams (shuttle's data monitoring and reservation) are presented.

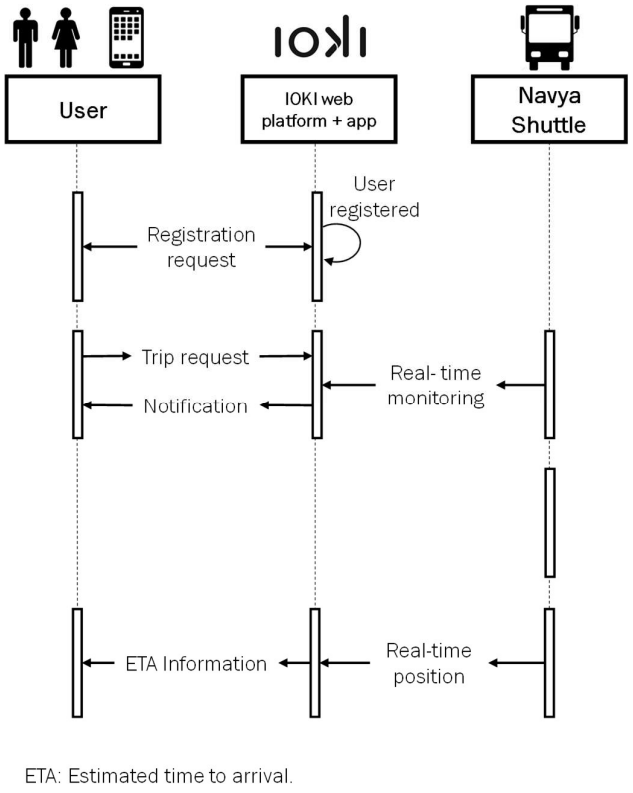


Figure 37: Service information flow in Turin pilot site

4.6.4 Special aspects: custom interoperability, cybersecurity and connectivity solutions applied

Connectivity solutions applied are described in previous sections making use of C-ITS standardized interfaces. Moreover, integration with SMDP followed connectivity and cybersecurity guidelines provided, establishing an authenticated and encrypted connectivity between the Turin Ioki LFMP and the SMDP for KPI data exchange.

4.7 Tampere local architecture

4.7.1 The local technology actors

Tampere, Finland site has a mixed approach with respect to its fleet deployment in the long term, where different vehicle providers are utilized throughout the duration of the piloting activities. The architecture diagram of Figure 38 describes the integrated system actors that are present directly or indirectly at the pilot site.

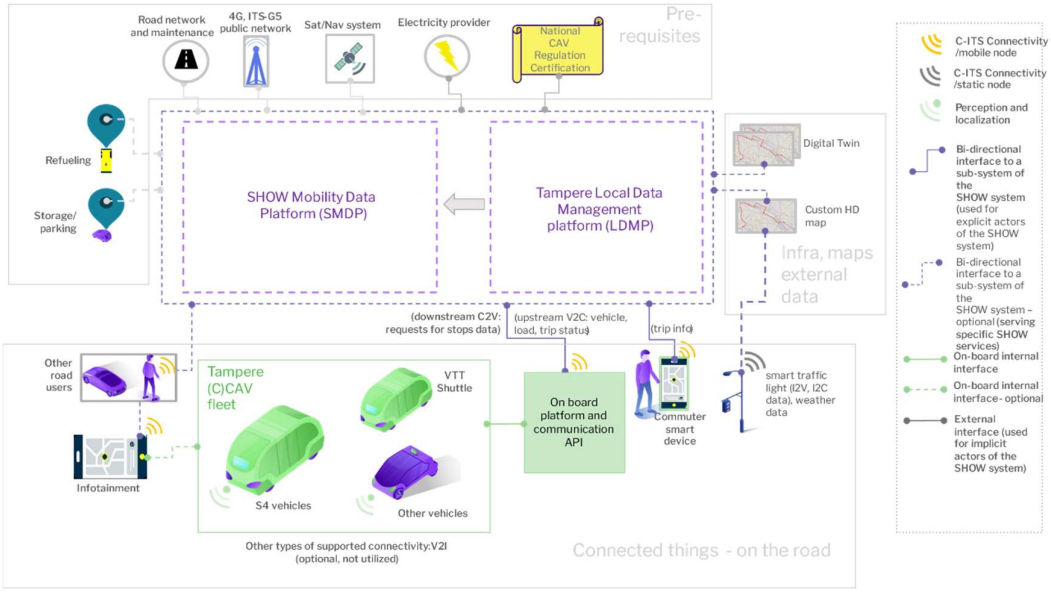


Figure 38: Local actors in Tampere pilot site

The passenger will have the route information available through the local operator's data service, however the vehicle will not interface to this latter service. Vehicle will provide mobility and KPI data to the local data management platform, from where it is also sent to SHOW data platform and dashboard.

The actors' roles and connectivity profile is described in Table 16.

Table 16: Local actors and their connectivity profile

Actor	Role	Connectivity
Sensible 4 vehicles	Passenger transportation and vehicle operations	Connects to local data management platform
VTT Shuttle	Passenger transportation and vehicle operations	Connects to local data management platform
Additional 3 vehicles targeted in 2022	Passenger transportation and vehicle operations	Connects to local data management platform

Actor	Role	Connectivity
Sensible 4 dashboard/management platform	Tampere LFMP	Connects to the fleet and to the SMDP via cellular/cloud connections repsectively
Local public transport operator	Passenger information and route schedule data.	No direct integration between vehicle data and operator's passenger information service
Infrastructure (City of Tampere and 3rd parties)	Keep the road and the surroundings in operational conditions.	No direct data connection.
Digital twin	Simulations of e.g. connectivity, conditions and weather.	No direct connectivity to pilot.
Telecommunications (3rd party 4G/LTE/5G + GNSS connections)	Provide safe and reliable data connection and localization.	Between vehicle and data management platforms.

4.7.2 Functional architecture

Tampere functional architecture is depicted in Figure 39 while the local data flows are as described in Table 17. Big part of the KPI calculations are performed on-board and the vehicle systems will provide the calculated KPI data to the local data management platform (Sensible 4 dashboard/management platform). The vehicle also provides the KPI data to SHOW data platform. The local fleet management platform can be easily integrated later to other services like smart traffic or smart city solutions, route planners, etc. However, at the initial phase of the pilot these are omitted to reduce complexity and to ensure that operations are able to commence on time.

Table 17: Fleet to LFMP to SMDP data flow summary

Information flow paths short description		
Connected fleet/passengers to local LFMP/Dashboard	local LFMP/Dashboard to connected fleet/passengers	LFMP to SMDP
Vehicles provide upstream the KPIs calculated from data produced by the sensors in the vehicle, such as speed, acceleration, location, etc. Vehicle can also provide data beyond metadata in case of e.g. incident verification. (requires manual	Local Fleet Management Platform sends downstream to the vehicles their fleet missions, operational notifications and potential information notifications to commuters (infotainment). In case of remote operations, teleoperation commands	There is a data connection, which sends upstream local KPI data to the SMDP. These include location of vehicle, occupancy, etc. There is downstream data connection enabled. Data from LFMP to SMDP is purely calculated KPI data

Information flow paths short description		
verification by safety driver).	are also sent by the remote operator to the vehicle via this link.	and related required metadata.

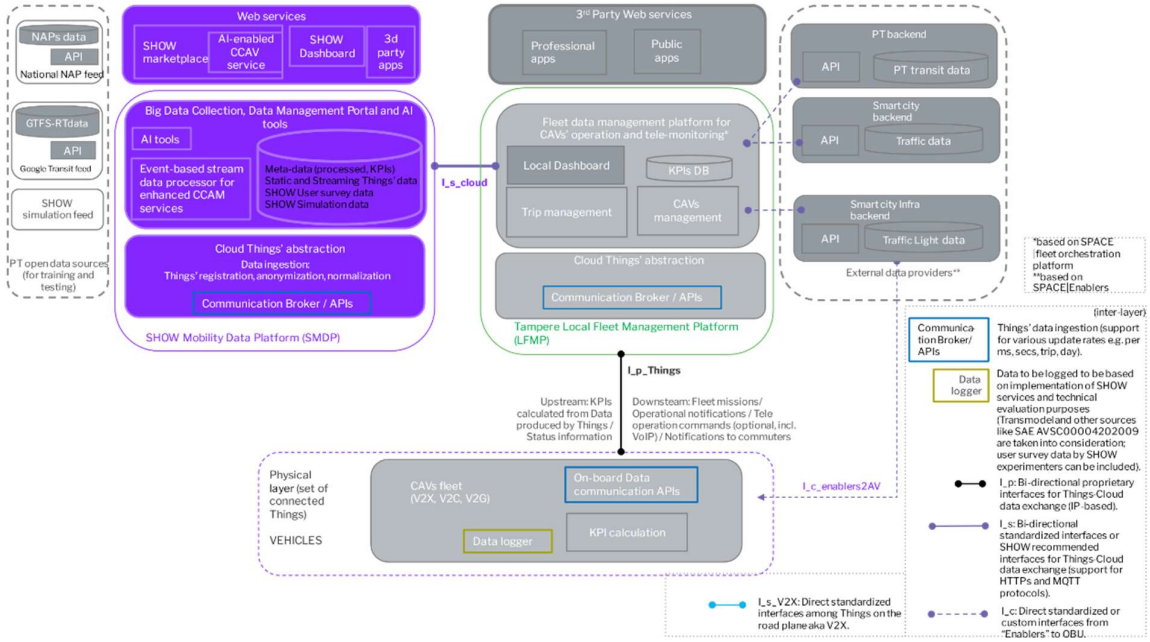


Figure 39: Tampere Site functional architecture (better viewed in zoom-in mode)

4.7.3 Service information flow

The service flow is as described in Figure 40. The vehicles in the pilot will not be directly connected to the existing passenger services by the local operator, but the schedule and route information is provided through their service. Vehicles communicate with LDMP, that in turn communicates with SMDP in providing KPI information. Operational data between vehicle and local fleet management is handled in real time. Safety drivers will be present inside the vehicle at the pilot, but the data for remote monitoring of the fleet is provided to the fleet management platform that serves also as Local Data Management Platform.

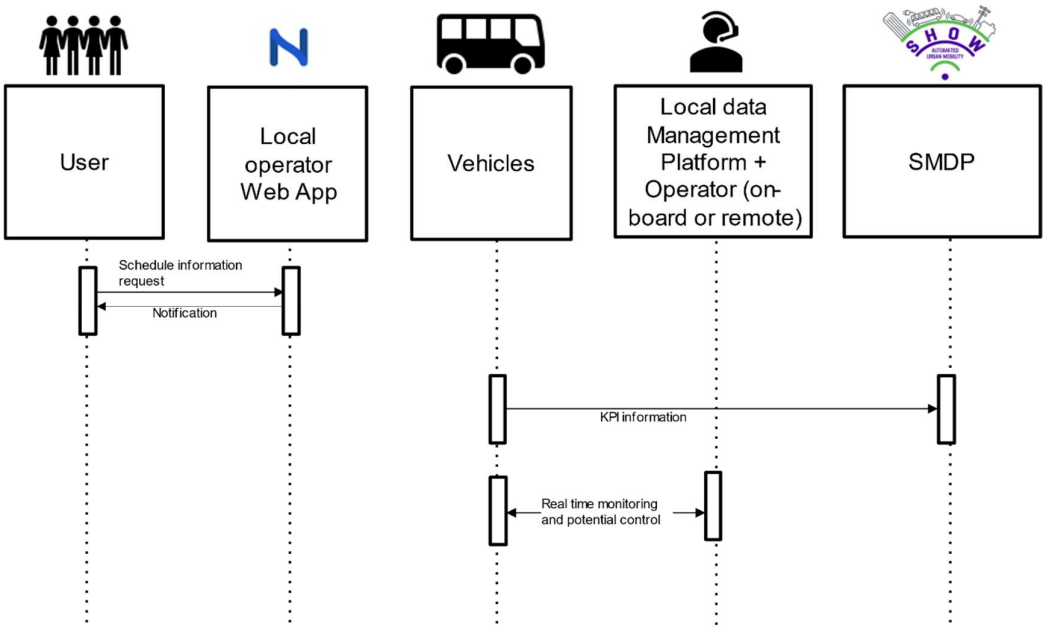


Figure 40: Service information flow in Tampere

Table 18: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
Local operator web app	Passengers can get route and schedule information (not real-time) from the local operator web application	Static route and schedule data.
Local Data Management Platform	Vehicles provide KPI data to LDMP, that in turn provides the KPI data to SMDP.	KPIs: Vehicle location, acceleration, speed, occupancy, etc.
Vehicle route data	LDMP provides the vehicle its mission, notifications, updates, etc.	Vehicle status data. Updated route and mission data.
Operator/driver (in-vehicle or remote)	Vehicle provides the operator/safety driver and LDMP with KPI data.	Updated routing data.

4.7.4 Interoperability, Connectivity, Cybersecurity solutions applied (if any)

The Tampere, Finland site initially will not have V2I connectivity at the site. The potential for connecting to the smart traffic lights on the route was researched, but the traffic light operator will change mid-pilot. Therefore, the possible connection will be reopened later in the pilot. Cyber- security follows SHOW D4.1 recommendation and adheres to the vehicle provider's (Sensible 4) standard security practices and there is no sensitive data transferred between the vehicle and the local fleet management platform. The pilot starts with safety drivers inside the vehicle. Interoperability between Sensible 4 vehicles to local actors, where needed, is to be done using predefined APIs. For its vehicles, Sensible 4 will manage both the vehicle and the LDMP, as well as the connectivity to SDMP.

4.8 Brainport local architecture

The vehicle fleet in the Brainport satellite site consists of 3 Renault Scenic passenger cars. Additionally a demonstrator is planned using an AV shuttle or E-Bus (brand tbd), provided by a third party. The current documentation of the Brainport site architecture focuses on the architecture that is in place during the pre-demo phase, which may be subject to change during the course of the project.

4.8.1 The local technology actors

The vehicles available in the Brainport site can be driving either manually or automatically. In automated mode, a safety driver will be present for take-overs. The automated vehicles are connected to the outside world using a hybrid mix of communication technologies including ITS G5 and cellular. The vehicles are connected with C-ITS services and benefit from full 4G coverage, early 5G deployment and IoT service networks. A high level schematic overview of the Brainport site architecture is depicted in Figure 41.

The Brainport site focuses on demonstration of the following use cases; UC1.1: Intersection crossing at normal operational speed, UC1.3: Safety for VRU at intersections, UC1.8: Vehicle relocation for automated mobility using platooning. In order to realize these use-cases, the demonstrators rely on a smart traffic light, VRU and road side unit for VRU detection. Further details on the actors and connectivity profile follow in the Table 19 below.

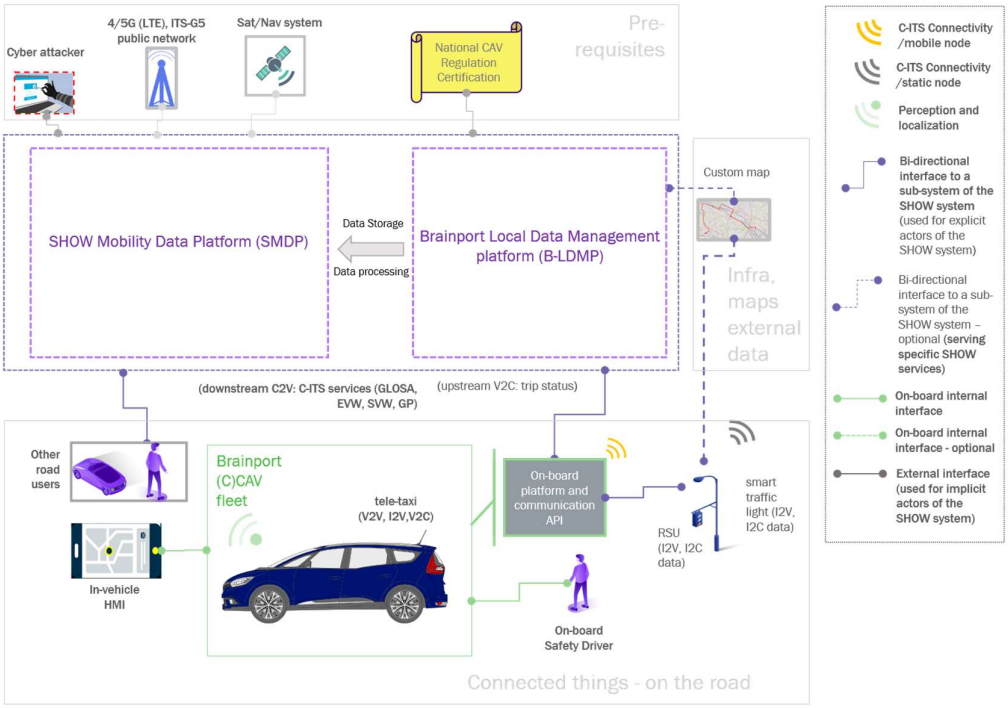


Figure 41: Brainport High Level Architecture

Table 19: Local actors and their connectivity profile

Actor	Role	Connectivity
AV Vehicles	Vehicle carrying out demonstrator UCs	V2C, V2I, V2V
On-board safety driver	System supervisor	N.A.
Commuter/user	User of system	No connectivity foreseen
Pedestrian	Actor in UC1.3: Safety for VRU at intersections	None (detected by RSU)
Smart Traffic Light	GLOSA service for UC1.1: Intersection crossing at normal operational speed	V2I
Smart Road Side Unit	Detection of VRU in UC1.3: Safety for VRU at intersections	V2I
Vehicle (2) equipped with V2V	Vehicle ready for platooning in UC1.8: Vehicle relocation for automated mobility using platooning.	V2V

4.8.2 Functional architecture

The interfaces between the Brainport Local Data Management Platform (B-LDMP), the Brainport vehicle fleet and the SHOW Mobility Data Platform (SMDP) are summarized in the Table Table 20below.

Table 20: Fleet to LFMP to SMDP information data flow summary

Information flow paths short description		
Connected fleet/passengers to local B-LDMP	Local B-LDMP to connected fleet/passengers	B-LDMP to SMDP
Real time data from the connected fleet on the vehicle and trip status. Offline data from connected fleet for storage and KPI calculation.	Downstream data features C-ITS services required in order to carry out the appropriate use-cases.	B-LDMP connects to SMDP through internet. It forwards the ready KPI computed on the B-LDMP.

A deeper zoom into the main Brainport architecture of Figure 41, yields Figure 42 which presents the functional architecture including the main components in each layer.

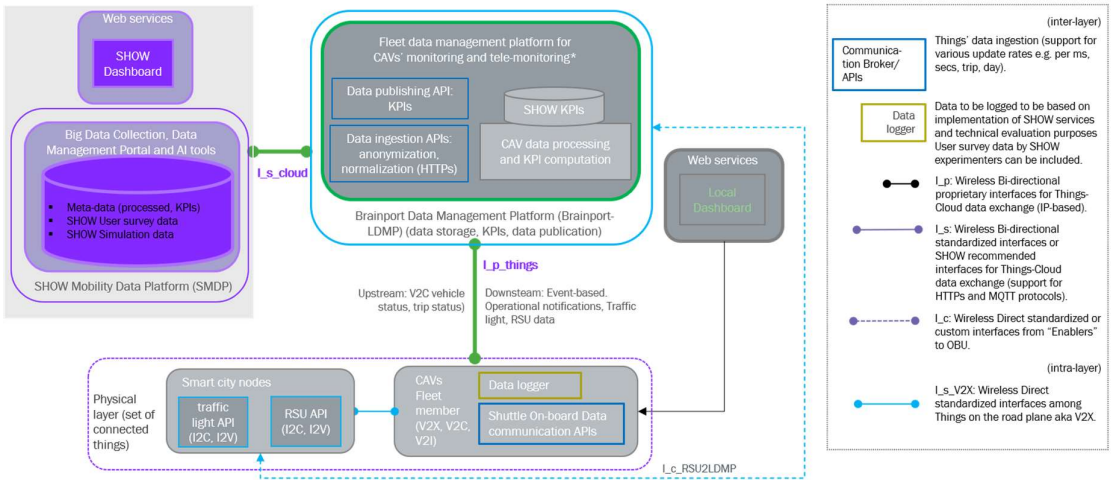


Figure 42: Brainport Functional architecture (component level)

4.8.3 Service information flow

For the Brainport site, the safety driver is in charge of starting and stopping an automated trip. During the trip, the vehicle will exchange information with the infrastructure in order to exploit the available C-ITS services foreseen to support the vehicle in its use cases. At the end of a demonstrator ruTable 21n, the recorded data will be stored on the Brainport Local Data Management Platform (B-LDMP), where KPI will be calculated. Available KPIs will be exchanged with the SHOW Mobility Data Platform (SMDP) from where KPIs can be visualized on the SHOW dashboard. The information flow in the Brainport site is summarized in

Figure 43 and service entities are briefly described in the following figure.

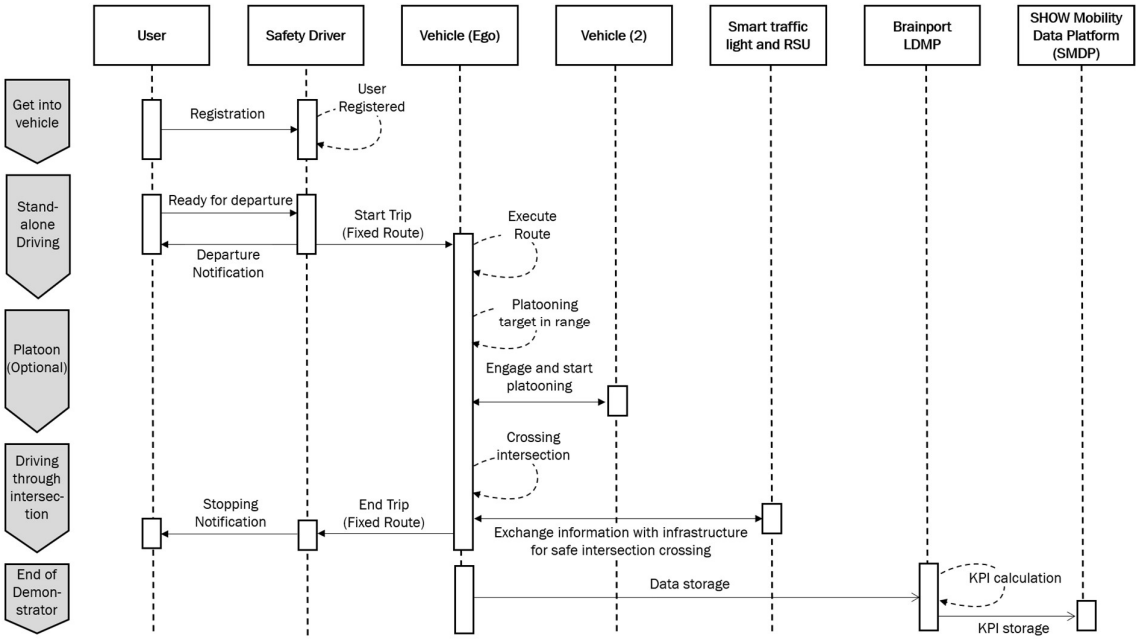


Figure 43: Brainport information flow diagram

Table 21: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
Brainport Vehicles (Vehicle (Ego) and Vehicle (2))	Automated vehicles with connectivity through ITS G5 and cellular (4/5G)*.	Real time data from other vehicles and infrastructure from ITS G5 and cellular (4/5G).
B-LDMP	Data storage, KPI calculation.	Data received from vehicles in Brainport site, Carrying out KPI calculations.
SMDP	KPI storage. Connectivity to SHOW Dashboard	KPI storage of data from Brainport site.

* the vehicles are also equipped with C-V2x communication, but this is not used in the SHOW use cases.

4.8.4 Interoperability, Connectivity, Cybersecurity solutions applied (if any)

No custom implementation. The Brainport Pilot satellite site realizes connectivity and integration with SMDP exploiting authenticated and encrypted connectivity between the Brainport LDMP and the SMDP in order to realize secure KPI data exchange.

4.9 Trikala local architecture

4.9.1 The local technology actors

The almost 6,7km long route for the automated shuttles runs between the city center and the intercity bus station covering also specific points of interest of the citizens such as Hospital, Milk Factory, major suburbs and villages. In summary, the ODD related requirements for the specific route include:

- support for mixed traffic with passenger and heavy vehicles on the lanes,
- support for signalized intersections, roundabouts, adjacent bicycle and pedestrian routes and street side parking and pedestrian crossings.

The integrated Trikala pilot site CAV ecosystem is depicted in Figure 44. In the physical layer and the cloud layer of the local SHOW integrated system, the actors presented in Table 22 are involved.

Table 22: Local actors and their connectivity profile

Actor	Role	Connectivity
CAV nodes	AV shuttles, retrofitted robot taxis and delivery robots realizing the Trikala UCs	V2C, V2I, V2V
On-board safety driver	System supervisor	V2C
Commuter/user	Shuttle/ robo-taxi commuter	Web app
Pedestrian	Pedestrian road user equipped with custom smart device compatible with V2P (actor in UC1.3: Safety for VRU at intersections)	V2P
Smart Road Side Unit	Detection of VRU in UC1.3: Safety for VRU at intersections	I2C, I2P
Smart Traffic Light / Road sensors for traffic monitoring	RSU node and sensors for implementing the Green Light service	V2I, I2C
Vehicle (2) equipped with V2V	Robo-taxis for platooning in UC1.8	V2V
Trikala FMP	Local fleet management platform incl. a remote control center and a traffic light management web app.	V2C, Cloud
Trikala TMC	Cloud external data provider: Traffic management center	Cloud
HD map	Custom static HD map created during the CAV piloting activity	N.A.

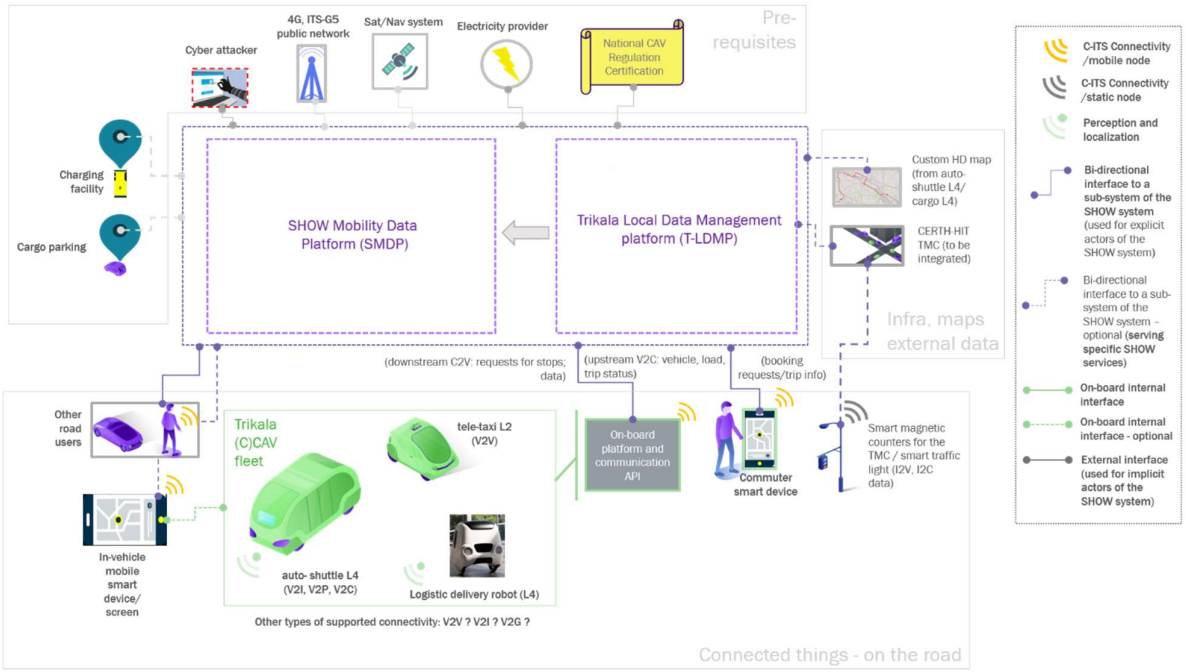


Figure 44: Local actors diagram for Trikala pilot site

4.9.2 Functional architecture

The Trikala Fleet Management Platform (TFMP) functional architecture is detailed in Figure 45 and includes apart from the main cloud data management system responsible for SHOW data collection and KPIs computation, the interface to an external cloud data provider, i.e .the Traffic Management Center (TMC). On top of the TFMP, apart from the SHOW AV DTR app to be developed, two other services will be integrated: the Traffic Light Signaling Monitoring, Control and Management (TLSMCM) service and the Remote Control Center (RCC) service.

Note: Traffic lights green wave for the shuttles can be implemented as standalone function in which case no integration with TFMP is needed.

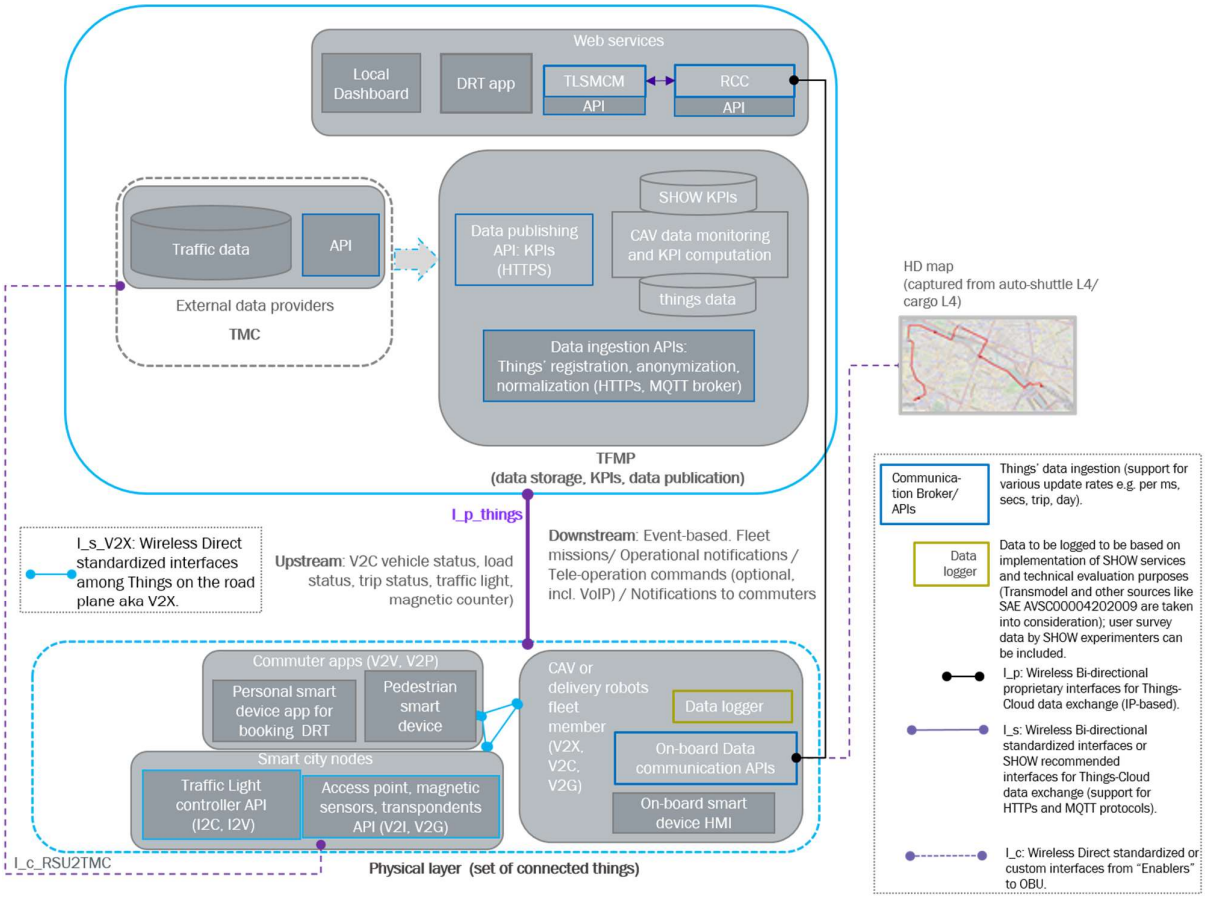


Figure 45: Trikala local Fleet Management Platform architecture: in light blue solid border line the cloud components, in light blue dashed border line the on-road components (better viewed in zoom-in mode).

The interfaces between the Trikala Data Management Platform (TDMP), the Trikala vehicle fleet and the SHOW Mobility Data Platform (SMDP) are summarized in the text of i_p_things interface of Figure 45.

4.9.3 Service information flow

The service information flow is as described in Figure 46. Note that information on local services is incomplete and will be added in the next iteration of this deliverable.

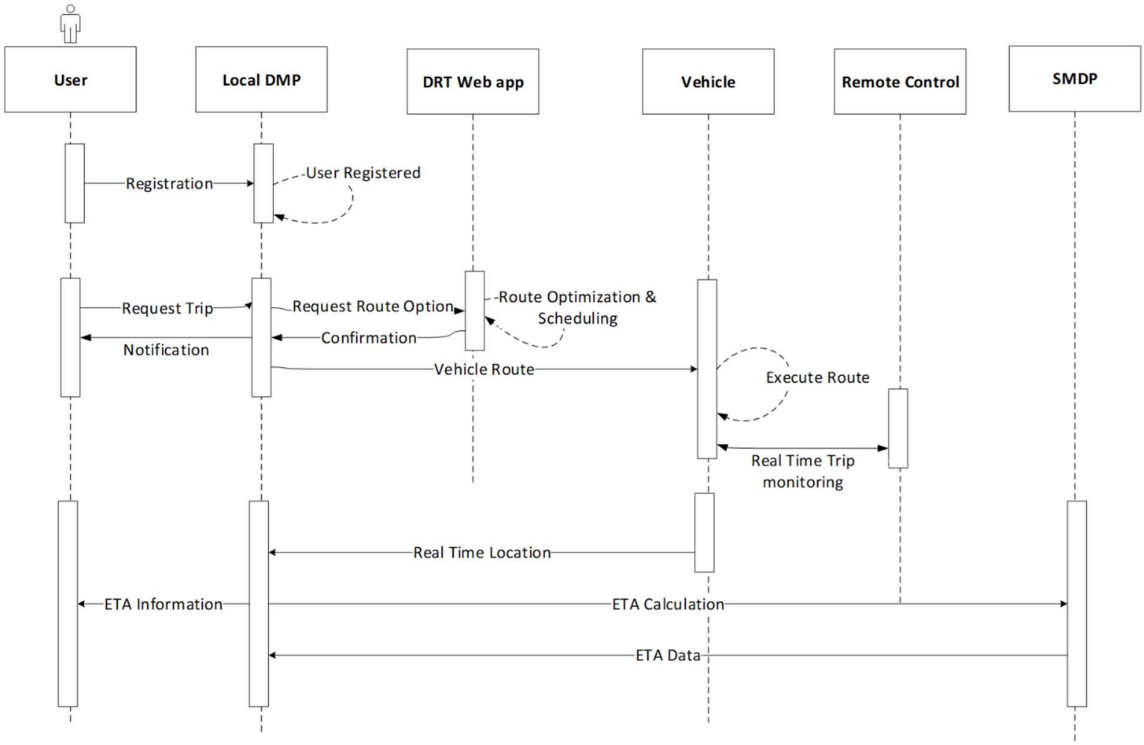


Figure 46: Service information flow

The **TFMP** provides the remote operator with comprehensive real-time monitoring of bus position as well as events, traffic and route-related reports with the cooperation of the TMC. Specifically, the remote operator can monitor in real time the current geographical location of a bus on a digital map and receive information about its position, speed, direction, and other statuses of the bus, such as starting, stopping, speed, low battery, door opening. Also, the remote operator will be able to create itinerary reports with the above data for specific periods of his choice, so that it is possible also to monitor and assess the movement of the fleet in the past.

The **TFMP** consists of three subsystems:

1. The Vehicle Fleet Service which is the main system responsible for pumping GPS data from the manufacturer's external subsystem (GPS Device Service that undertakes the communication with the devices) through API (Application Programming Interface), their processing and the synthesis of the generated information based on business logic, its storage in the System Database and finally the dissemination of information and communication with the applications used by remote operators.
2. The Fleet Vehicle Client Application (installed on the operator’s computers (PCs), which offers the overall supervision of the application and constitutes the user interface with the system.
3. The Vehicle Fleet Database, in which all the necessary data for the operation of the above two applications are stored.

Remote control functionality (RCC web service): The shuttles serving the specific route at Trikala are capable of independent navigation and locomotion in an urban environment, within real traffic conditions in mixed traffic. The automated vehicles actual driving is executed mostly without human intervention. Human intervention is mandatory from the Greek Legislation to be executed remotely in order to go over limited number of unforeseen, escalated, or difficult driving conditions. In addition, physical human intervention is expected

in case of an impending accident, daily maintenance like charging, and other similar limited number of events that stop the actual service and cannot be fulfilled remotely.

Additional types of data transmitted from the vehicle to the RCC via custom network connection are:

A. Raw data that will come from the telematics device and will include GPS coordinates of the bus position, speed, direction, odometer & events of interest for the vehicles on a digital map (e.g. start, stop, engine start-up, peripheral status if the corresponding information is received from the vehicles, etc.) which are sent by the vehicle via TCP/IP to a central server at the RCC, within a certain period of a few seconds. For this type of data, the GPRS service is considered sufficient for transmission.
B. VoIP communication through a network telephone device.
C. Video data from the 5 cameras placed on the vehicle in order provide to the RCC a complete view mainly of the external but also of the internal environment of the vehicle, as according to the regulation.

4.9.4 Interoperability, Connectivity, Cybersecurity solutions applied (if any)

With respect to connectivity for seamless operation of the autonomous vehicles the following specification of adequate 4G/5G network coverage along the entire length of the route has been agreed: high data throughput for video data transmission and low latency to support video streaming service, VoIP and exchange of data between the Remote Control Center and the vehicle. Full base station (BS) coverage is also provided for the entire route of the vehicle, ensuring minimum latencies during the network handover when moving from a BS to a neighbouring BS.

Trikala TMC functionality for implementing traffic lights green wave is described in D8.2.

In Trikala pilot site one RSU will be installed in one signalized intersection to monitor the pedestrian crossing area in order to detect possible dangerous situations (Figure 48). The RSU device will be placed on a traffic light pole, or in a suitable location with clear view to the zebra crossing. This device integrates many communication technologies and it has the following capabilities:

- G5 radio
- PC5 side link
- 5G/LTE/4G/3G
- WiFi/BLE
- Gigabit Ethernet
- GNSS with RTK base station
- Optical Camera,
- RF mmWave RADAR
- ETSI C-ITS full V2X software stack

Additionally, in Trikala site a special prototype handheld device that has been designed and developed by CERTH/HIT will be used to increase the interaction between VRUs and AVs. This device uses G5 direct communications with vehicles and infrastructure in order to exchange awareness and notification messages with other connected actors. It evaluates dangerous situations by itself and it uses audio and visual warning alerts via HMI when a risky situation is predicted (Figure 47). More details on interaction with VRUs can be found in Deliverable D7.3.

Figure 47: VRU interactions with V2X and handheld device

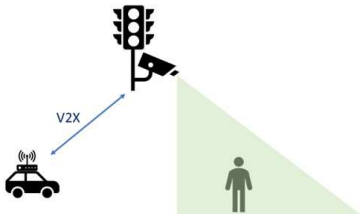


Figure 48: VRU interactions with V2X and camera

4.10 Brno local architecture

4.10.1 The local technology actors

The vehicle fleet in Brno (Czechia) consists of three automated vehicles, two shuttles and one robotaxi. Both shuttles are based on the same electric vehicle Esagono Energia Grifo, equipped with automated driving functionality, and able to accommodate up to five passengers in the rear passenger section. Robotaxi is a research passenger vehicle equipped with automated driving functionality, able to accommodate up to three passengers. They can all be driven either automatically or manually and also remotely. In automated mode, a safety driver must always be present and able to take over the vehicle at any time. Because the safety driver is there, s/he can also take over some of the activities of interacting with the passengers, but not at the expense of safety, which means this interaction will be restricted only to the bus stops. However, the driving itself is completely automated. The vehicles technically have one way of communicating with the external environment, in this case through a wireless 4G and/or 5G networks.

The vehicles will move together with other traffic and vulnerable road users in mixed operation. For a safe conduct of a trip, all vehicles are equipped with an abundance of sensors that detect every object in the driving trajectory. There is no direct communication link with other road users.

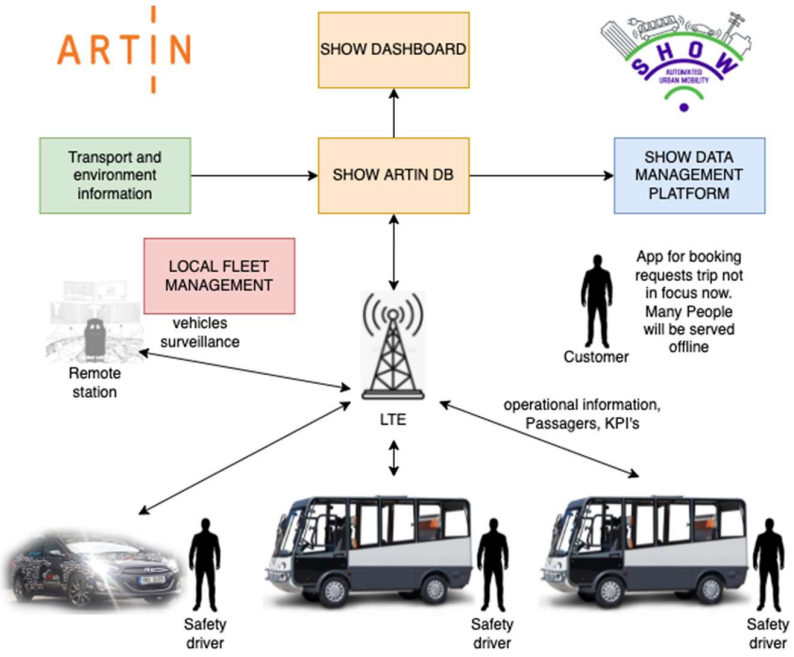


Figure 49: SHOW pilot architecture in Brno

The focus in the Brno Pilot Site is on the technical challenges of operating automated vehicles in the environment that has never seen this kind of transport before. Consequently, social challenges will be investigated in detail as well. Our service will be available on the first come first served basis, but there will be also a possibility to book a ride in advance. For this purpose, a dedicated booking system will be developed and deployed.

High-level architecture including the main actors of the pilot site is presented in Figure 49 while the actors' roles and their connectivity profile is described in Table 23 hereafter.

Table 23: Local actors and their connectivity profile

Actor	Role	Connectivity
Vehicle 1 / 2 /3	Passenger service	LTE (4G/5G)
Safety Driver	Taking over in safety-critical situations; not needed for normal operation for driving; assisting passengers for getting into the vehicle	-
Teleoperation station	Remotely assisting all vehicles	LTE (4G/5G)
Local mass public services	Local public transport operations including buses, electric buses, and trams.	Proprietary connection to local city transport management allowing real-time monitoring of all deployed vehicles
Users	Users of the automated service	No connectivity foreseen

Actor	Role	Connectivity
ARTIN Fleet management platform	Local data management platform (LFMP) used a gateway to the SMDP. Internal DB also storing traffic/weather info from external data provider	V2C, Cloud

4.10.2 Functional architecture

Locally, the data streams are shown in Figure 50. The vehicle sends data to a central database that provides KPI data to the SHOW data platform. All vehicles are monitored from control stations, which are able to intervene in the same way as the safety driver, if necessary.

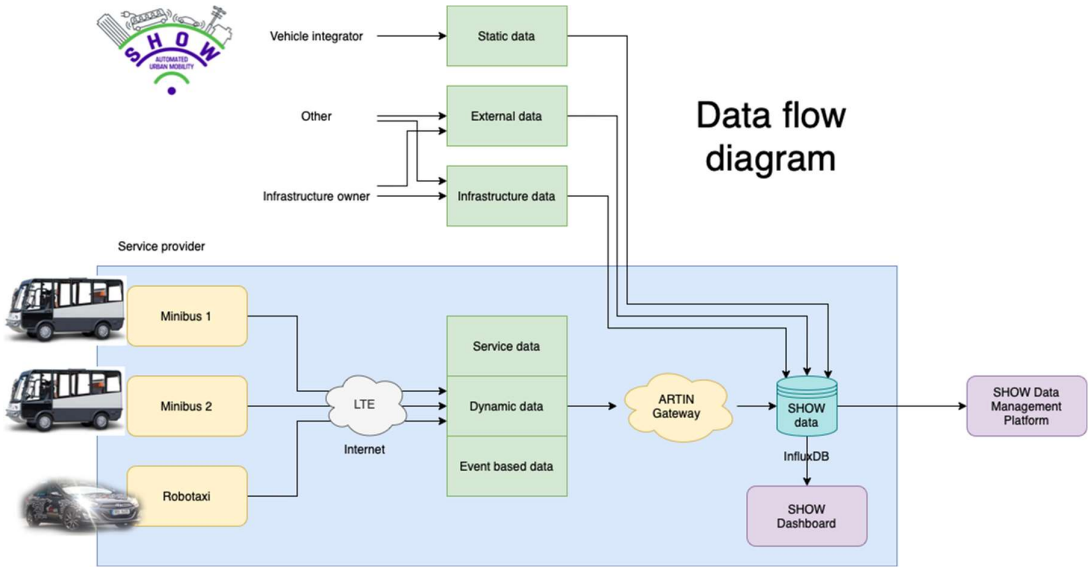


Figure 50: Functional architecture at Brno pilot site

4.10.3 Service information flow

In the following figure (Figure 51) and the table that follows, the information flow for the Brno pilot site is illustrated. The service can be used directly by boarding our automated vehicles at the bus stop. Potential users therefore can wait at the bus stop and get on board as the vehicle arrives. A safety driver will be there available to assist. The fixed route will consist of five stops, users can get on board on each of them. For a robotaxi service, there will be a booking platform that will allow users to hail a ride.

After boarding the vehicle, the automated trip starts along the route. During this time, regular information about the trip status and other SHOW KPI is sent to the SHOW dashboard. This includes e.g. position, speed, acceleration etc.

Details on this information sequence are still being refined as the pre-demo phase progresses. Final service list will be provided in the next iteration of the deliverable.

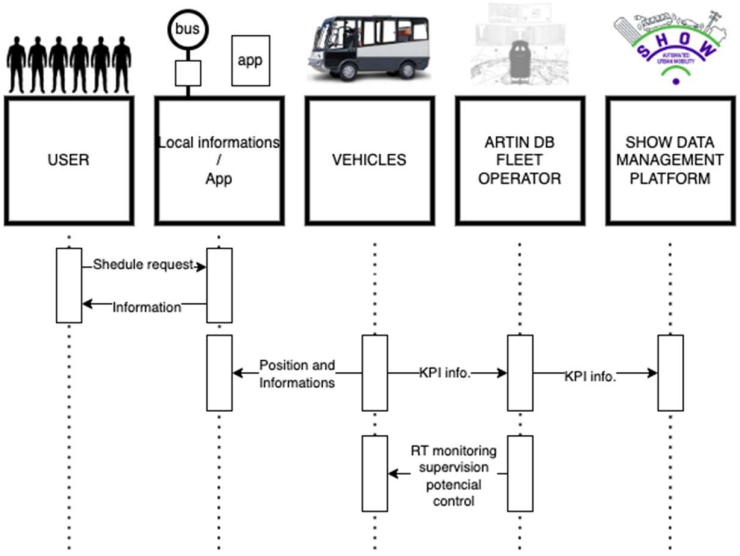


Figure 51: Information flow diagram for Brno pilot site

Table 24: Local service actors and to/from data exchange summary

Local Service	Short description	Data used (coming from fleet, devices, infra)
City center shuttle service	A user can take a ride in an automated shuttle through the city center.	The ride itself can in principle be carried out completely independently of infrastructural data and is executed locally by the vehicle. However, a real-time monitoring will be done through our remote-control station.
Technology Park shuttle service	A user can take a ride in an automated shuttle around one of the local technology parks and university buildings.	
Robotaxi service	A user can take a ride in a robotaxi that will function as an auxiliary service to the shuttles.	Recognition of getting on/ getting off requests from passengers needs to be added in a later stage.

4.10.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if any)

The Brno pilot site will not utilize any C-ITS functionality because there is no such equipment. However, there will be a remote monitoring station that will allow teleoperation, i.e., remote driving, remote assistance, and remote management. This functionality will rely on 4G and 5G networks operated by two independent mobile carriers (T-Mobile and Vodafone). The wireless networks cover all anticipated deployment areas. Cybersecurity solutions are inherent to the teleoperation system developed by the respective partner.

5 SHOW Mobility Data Platform (updates)

Whereas, Section 4 focused on the implementation of the architecture in each local pilot site, mainly describing the local fleet management platform implementation and abstracting the central SHOW cloud platform, Sections 5, 6 and 7 will focus on design aspects and mechanisms implemented for the centralized cloud SHOW Platform. As explained in Section 2, each local fleet connects to the SHOW MDP and provides the required data defined for measuring project KPIs using a common data model and KPIs format for all sites. The connection is realized in two ways: The first method is a real-time connection utilising MQTT messaging protocol, while the second one exploits the CKAN platform for historical data provision. Therefore, the SHOW Mobility Data Platform unifies the seemingly unrelated local architectures, with an underlying common message definition and data acquisition protocol allowing for project KPIs monitoring on a cross-European level (see central Dashboard versus local Dashboard discussion in Section 2 and D4.2). The final list of KPI IDs and categories that form the SHOW common data model can be found in Appendix I.

5.1 SHOW DPMP first version summary

SHOW integrated system, as presented in D4.1 (Open modular system architecture and tools) [1], is the first (considering public transport) EU-wide piloting platform that focuses on CCAM services. SHOW CCAM services are built on top of local fleet management and data from each pilot site is transferred to the SHOW Mobility Data Platform (SMDP) responsible for data management and publication to available web-services sitting on top of it. The SHOW MDP then becomes responsible for data management and KPIs calculation, in order to present KPIs subsets from each local site on the SHOW Dashboard. The first version of SHOW MDP was proposed to contain five main components. **The Data Collector Platform** was presented as a conglomeration of Apache Kafka[6].

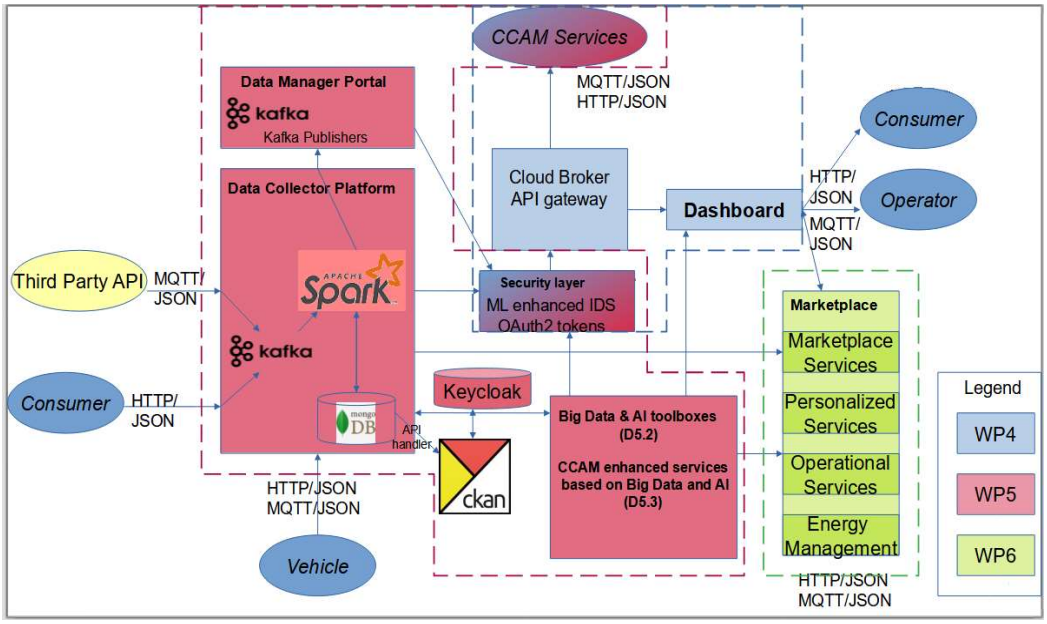


Figure 52: First version of SHOW DPMP (inside red dashed polygon), highlighting the inter-component interrelation with other SHOW WPs. (source: D4.1 [1])

6 https://kafka.apache.org/intro

Apache Spark[7] /MongoDB[8]. The **Data Manager Portal** consisted of Apache Kafka Publishers. The other three components are the **CKAN platform**[9], for historical data provision, the **Security layer** (for both WP4 and WP5 purposes) and **Keycloak**[10] for authentication and access management. The first version of SHOW DPMP, as proposed in D4.1 [1] and D5.1 [2], is presented in **Error! Reference source not found.**, inside the red dashed polygon.

5.2 SHOW MDP second version description and implementation

In the second version of SHOW MDP, while the main components remained as they were in the first version (i.e. *Data Collector Platform, Data Manager Portal, CKAN, Keycloak, Security*), the final implementation of some of these components introduced some modifications. The Data Collector Platform currently supports a bridged Kafka/MQTT broker. Moreover, pilot sites and their vehicles are able to connect to SHOW MDP MQTT Broker and publish the available data to the corresponding MQTT topics. Apache Kafka is then responsible to stream the accumulated data to a Lenses docker, which replaces Apache Spark. According to SMDP technical team conclusions after extensive elaboration, only the data visualization aspect of Spark is required. Therefore, another powerful tool was selected for this scope, which is LensesIO. LensesIO is a tool that connects to Kafka streams, while being able to visualize MQTT connections and data transferred via MQTT. Furthermore, it provides both UI and APIs for data handling, as it enables to store the vehicle data from the MQTT/Kafka broker directly to the SMDP Database (which is MongoDB, as proposed in the first version). Based on the data stored, KPI calculation algorithms are implemented, depending on the nature of the data and the contextual KPIs. KPI calculation is implemented in Python3, drawing data from MongoDB using corresponding queries. The main sets of KPIs can be summed up as calculation of **Average**, calculation of **Percentage**, calculation of **Cumulative** (total values), as well as API exposure of **Units per kilometer** and **Numbers**, which are provided directly from pilot sites.

Figure 53: Message transmitted from an AV via MQTT.

The agreed format of message transmission is as follows. For MQTT real time transmission, Pilot Sites must use a JSON formatted message to the respective MQTT topic that includes the value of the transmitted metric, the ID and the acquisition timestamp.

In the next phase of the Data Flow, an application was developed in Python, using the Flask Library [11]. This was implemented in order to create the REST APIs, based on HTTP communication protocol and to transmit the calculated values directly to the SHOW Dashboard (with the help of a security layer consisting of OAuth2.0 and tokenization/email authentication). It is important to note that, in this context, REST APIs are utilized for the communication between the SHOW DPMP and the SHOW Dashboard, in order to follow the WoT protocol [12] as described by W3C. However, HTTP communication between the Data

7 https://spark.apache.org/docs/latest/quick-start.html
8 https://docs.mongodb.com/
9 https://ckan.org/?s=cachlambep.net
10 https://www.keycloak.org/

Collector Platform and the Vehicles is omitted, while MQTT was chosen as the only one supported communication protocol. This change was performed for both consistency reasons, in order to establish a robust communication method with Pilot Sites and Vehicles, as well as to harness as less data bandwidth as possible for better communication performance. For a comparison between REST and MQTT communication protocols, the reader can refer to D5.1 [2] chapter 7.2.5 and Appendix V.

The calculated KPIs follow a format that includes two sections. The first section is related to information about the message sender, i.e. the vehicle, vehicle ID, the fleet ID and the site ID along with the corresponding names. The second section contains the KPI ID, KPI value, KPI unit, the requested frequency (daily, weekly, monthly), KPI category, and the corresponding dates for which the calculation is applied along with the KPI values for these dates. Figure 54 displays a message example of the calculated KPIs. More information about KPI IDs and categories can be found in Appendix I.


```
{
    "Timestamp": "2021-06-03T08:52:44Z",
    "Entity": "Vehicle",
    "Entityid": {
        "Site": {
            "Site ID": "b1c75b3b-af83-4a5a-a67b-86be75bc5329",
            "Name": "Thermi, Greece"
        },
        "Fleet": {
            "Fleet ID": "ac40f3da-c47d-40a8-af1a-7e5950a67e94",
            "Name": "CERTH Fleet"
        },
        "Vehicleid": {
            "Model": "Vehicle 1",
            "Vehicle ID": "certh-vehicle-1"
        }
    },
    "Kpiid": "1",
    "Kpivalue": "50.75",
    "KpiUnit": "KMPH",
    "Frequency": "daily",
    "Category": "traffic-efficiency",
    "FromDate": "2021-06-01T21:09:09Z",
    "ToDate": "2021-06-03T21:09:09Z",
    "Kpivalues": [
        {
            "value": "23.28301886792453",
            "time": "2021-06-01"
        },
        {
            "value": "50.75",
            "time": "2021-06-02"
        }
    ]
```


Figure 54: Message of calculated KPIs in JSON format

Additionally, the direct communication of commuters and SHOW DPMP was removed, since no pilot sites provide this capability. Therefore, the commuters are going to communicate with each pilot site's local dashboard. However, as CCAM services will be developed and implemented within the SHOW ecosystem, direct communication will be added in future versions. It is obvious from the aforementioned analysis that the SHOW Data Management Portal has been developed in a different method than the previous one proposed in D4.1 [1] and D5.1 [2], as Kafka Publishers have been replaced by REST APIs using Python/Flask.

The remaining SHOW MDP components remained stable and as proposed in the previous version. CKAN was developed as a data platform in order to support historical data provision. The pilot sites are able to create an account and upload a file (csv extension or a compressed one) containing the historical and demo data. When the data are made available, the CKAN platform utilizes API handlers in order to store the collected data to the DPMP Database.

From there, the data flow remains the same as with real-time accumulated data, i.e KPIs are calculated and exposed to the SHOW Dashboard using REST APIs created in Python3/Flask. Finally, the Keycloak tool was exploited for authentication and access management issues, namely in the communication between SHOW MDP and SHOW Dashboard.

The new SMDP architecture, along with the revisited inter-component interrelation is provided in Figure 55, while Figure 56 displays a general data flow visualization within the SHOW MDP, from the vehicle data provision to the SHOW Dashboard.

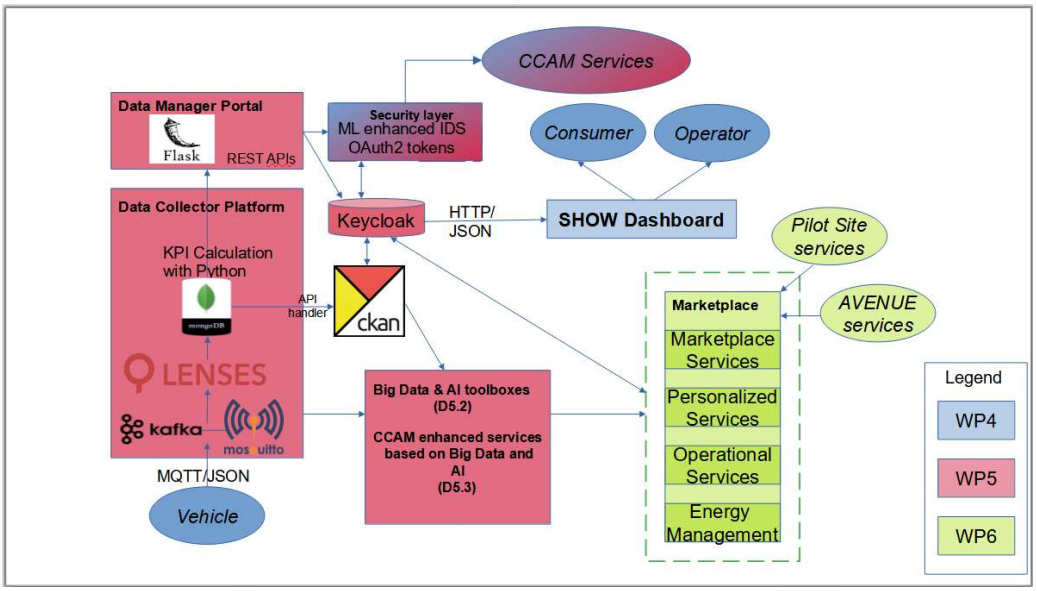


Figure 55: Second Version of SMDP and revisited inter-component interrelation with other SHOW WPs.

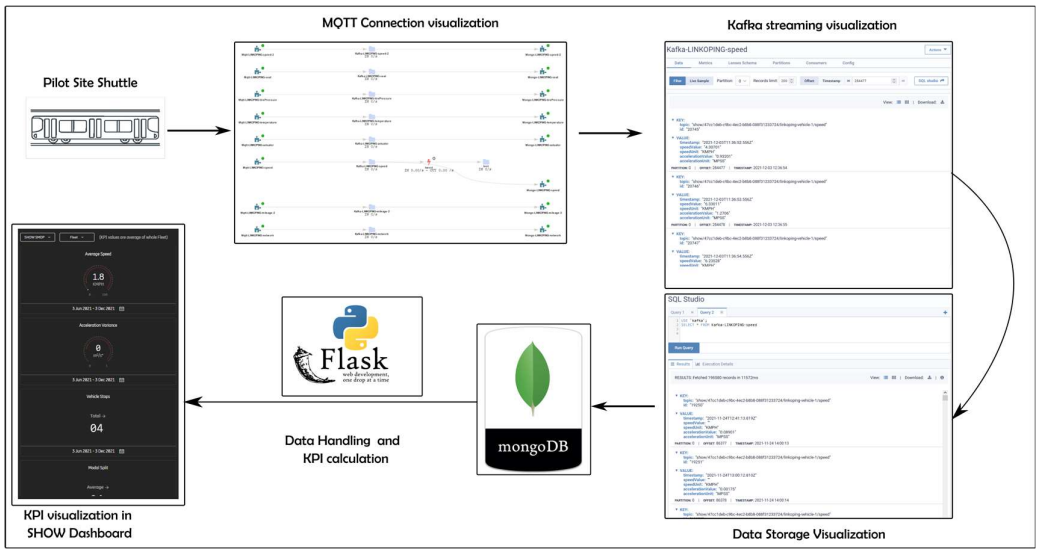


Figure 56: Data flow visualization diagram within SHOW MDP.

In conclusion, the initial goal of SHOW DPMP was accomplished. More specifically, Publish/Subscribe asynchronous messaging services offered decouple the ones which produce events from the others that process events [1]. Channels and topics are created

seamlessly, allowing operators to connect to the Platform without worrying about the data center infrastructure needed for storage and distribution. Connection of the SHOW MDP and Pilot Sites as well as the SHOW Dashboard is well established, utilizing the methods explained in this chapter. A list of the SHOW KPIs visualized in the SHOW Dashboard, along with their data inputs and outputs is presented in Appendix I.

6 Cyber security

Section 2 of SHOW D4.1 [1] mainly described a State-of-the-Art analysis of the main cyber security aspects applied in European projects and in the contemporary literature. This deliverable focuses on the defence mechanisms applied on the SHOW Mobility Data Platform (i.e. the central cloud infrastructure of the project linked to all local sites cloud infrastructure).

The cloud SMDP cyber security architecture, which includes a number of mechanisms to counter the most frequent manner of cyber-attacks, is presented in section 6.1. This section is further structured depending on the type of the main defense mechanisms into the following sub-sections: ***Intrusion Detection System***, ***Firewall***, ***Cryptography*** and ***Software Vulnerability Management***. In complement of the implementation details, section 6.2 presents real-life cyber-attack experiments that were conducted by the SMDP technical team against known attacks, part of WP4.4 work. Finally, the synopsis of cyber security work in SHOW along with the challenges and future directions is presented in the last two subchapters (namely sections 6.3 and 6.4 respectively).

It is important to note that the defence mechanisms described in subsection 6.1 are designed for and apply on the SHOW MDP part of the SHOW integrated system. In each pilot site additional cyber security mechanisms may apply depending on the cybersecurity protocols of the vehicle owners and the existing cloud infrastructure components/APIs. These are omitted from the presentation here as they represent elements that are pre-existing and conceived outside SHOW and moreover confidentiality issues may apply. Details on the implementation of the fleet can be found in SHOW deliverable D7.4.

6.1 Defence Mechanisms

This methodology makes the overall SHOW project more robust to cyber-attacks, as each component adopts a unique cyber security measure preventing a single point of failure that could endanger SHOW's cyber security as a whole. Moreover, thorough cyber security measures have been implemented for the pilot sites' communication and message sharing with the SHOW MDP, both for real-time messaging and historical data provision, while different cyber security mechanisms were developed for the SDMP – Dashboard connection.

Cyber security in terms of the SHOW project concerns the platform and its underlying components developed in the project. Pilot sites can independently apply their own cyber security strategy as a way not to disturb their business operations. However, a list of best practices has been circulated by the SHOW cyber security team in order not to change each pilot site's architecture but to enhance the overall cyber security against known and unknown threats.

6.1.1 Intrusion Detection System

The basic defence mechanism for detecting network attacks applied to the SHOW applications' server (Data management portal and marketplace) and consequently to the SHOW whole system is Snort [9]. Snort is an intrusion detection software relied on signature-based detection method. The tracking method is based on incoming network packets from any source, which are compared to a set of features stored in the database. The type of attack is determined depending on the attributes of the incoming packets [10]. The benefits of tracking signatures are reliability and easiness in the implementation. Figure 57 shows the architecture that Snort follows.

As observed from Figure 57, SNORT initially accepts network packets as input and, through its decoder, specifies which protocols are used in the package (such as Ethernet, IP, TCP, etc.). It then stores this data along with the location of the payload / application data contained within the package and the size of this payload to use this information [10]. According to the

available rules stored in the database of SNORT, the packages are classified. This classification concerns the type of attack, a brief description of it but also the priority, as shown in Appendix III: Cyber Security, and more specifically in Table 26: Snort Default Classifications. Finally, an instance of SNORT running in SHOW applications' server is displayed in Figure 58.

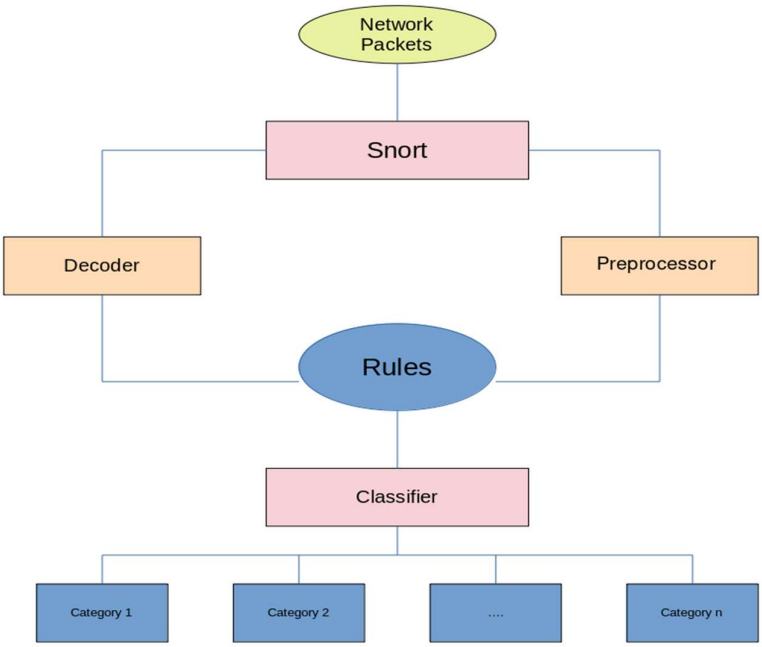


Figure 57: Snort IDS architecture

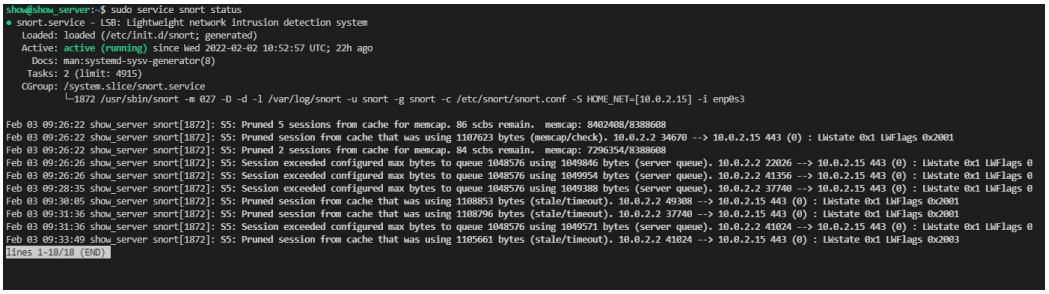


Figure 58: An instance of SNORT

As already mentioned, Snort is a signature-based IDS for network security, but in the future, this IDS will be accompanied by an anomaly-based IDS based on artificial intelligence. The deep learning algorithms on which the IDS will be based, as well as the data with which the neural networks will be trained, are under consideration. Figure 59 displays a concept for the architecture of the future AI-based IDS.

Initially, the model that will be chosen consists of two separate phases. The first one concerns the training process, and the second one the testing process. In more detail, the first phase involves the model training, where input is given as predefined data. Consequently, the data are initially normalized and then encoded in the form of tensors. After the training process's execution, the neural network's effectiveness is examined in data that were not included in the training data set. If the model's performance is considered satisfactory, then real-time

network monitoring is performed, taking all the network packages as input. These packets are then categorized into predefined categories to detect possible attacks.

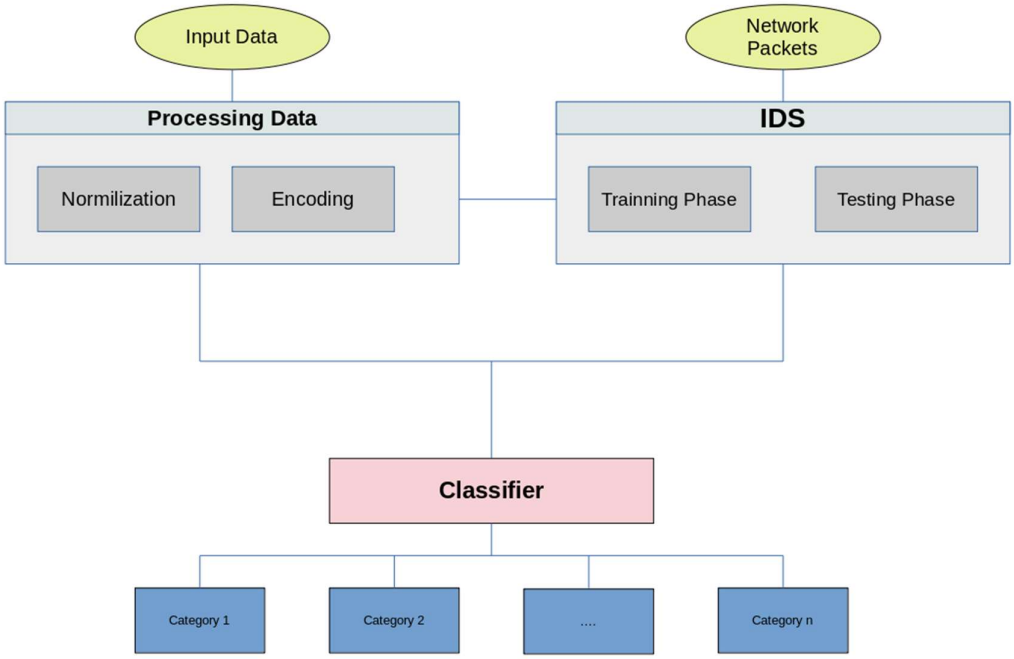


Figure 59: Artificial Intelligence based IDS architecture.

6.1.2 Firewall

The firewall applied to the server is UFW (Uncomplicated Firewall) [11]. This is a network protection software that uses IP tables to interrupt or mitigate unauthorized access to private networks connected to the Internet. The set of firewall policies defines the allowed traffic since any other attempt to gain access to the network is excluded. As shown in Figure 60, the UFW was placed on the first line of a network to function as a communication link between internal and external devices.

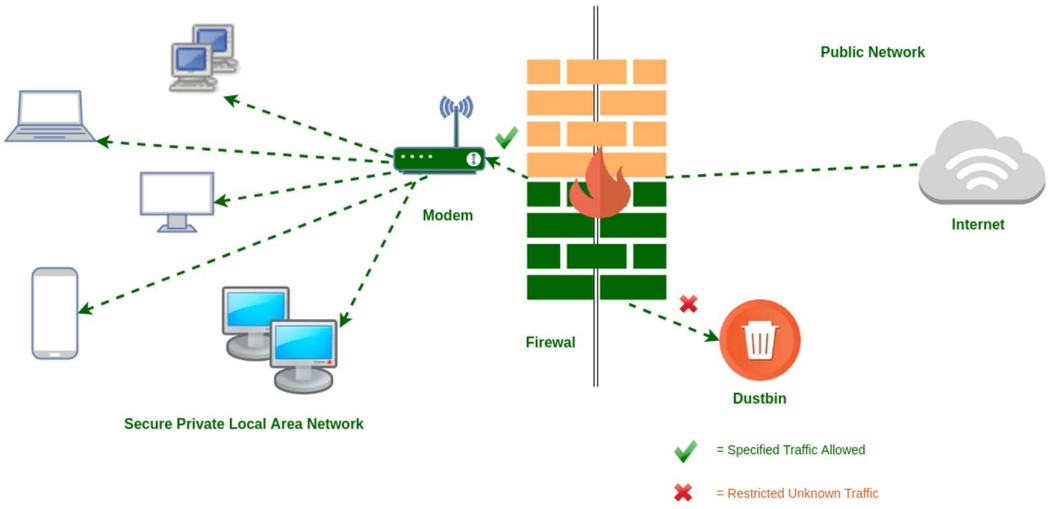


Figure 60: SHOW Server Firewall [14]

6.1.3 Cryptography

Regarding the users' registration procedure on any of the available software platforms, the passwords are not stored as plain text in the Mongo database. Priority is given to the protection of critical data, and for this reason, all passwords are hashed. The hash process is something different from the encryption process. In the first case, there is a one-way function that does not allow the reversal of the hashed password, while in the case of encryption there is a way to recover the plain text if the secret key is available. So even in the case of a password breach, it is extremely difficult to retrieve the original text.

6.1.4 Software vulnerability management

6.1.4.1 Cross site scripting (XSS) protection

One of the security measures implemented for data protection is the protection against Cross Site Scripting (XSS) attacks. XSS exploits occur when an unreliable source manages to import data into a web application without being granted the appropriate permissions. This type of attack takes place in the client's browser and the malicious content is usually in the form of JavaScript code or flash media code [3].

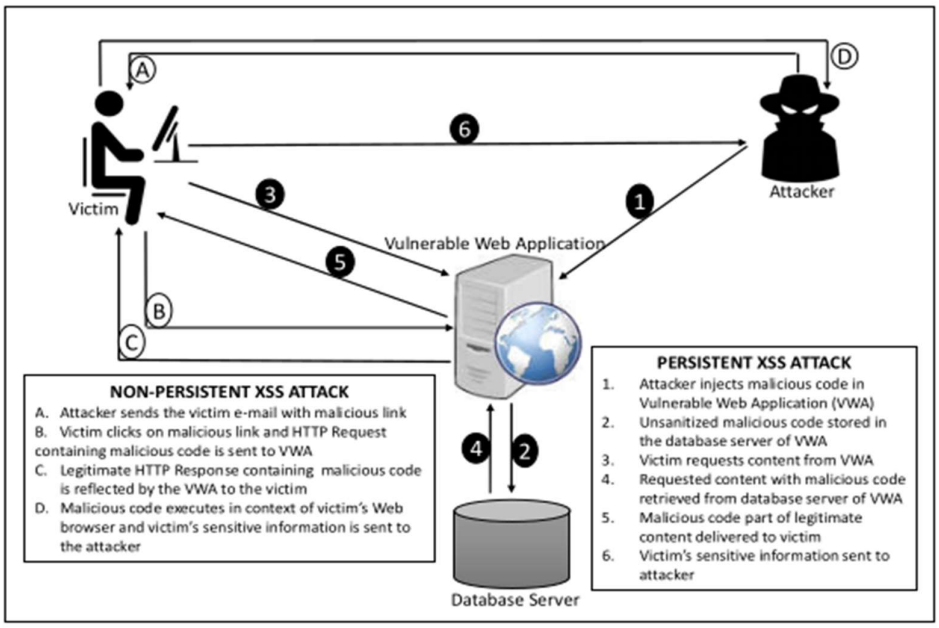


Figure 61: Types of XSS Attacks [4]

As shown in Figure 61, there are 2 basic types of attacks [4]:

- Non-persistent XSS attack or Reflected attack
- Persistent XSS attack or Stored attack

For both of these types of attacks the necessary measures have been taken to make these attacks impossible.

6.1.4.2 Cross site request forgery (CSRF) protection

Cross-site Request Fraud (CSRF) is a well-known web attack that allows a malicious user to perform actions on the website using another user's credentials [5]. On the CSRF exploit, malicious requests are routed to the web application through the user's browser, without the need of using a malicious piece of JavaScript. Usually, this results in the malicious requests

not being distinguished from the upcoming benign requests that were actually authorized by the user [6].

CSRF protection works by checking for a secret token on every POST request made by the user on the website. This feature makes it impossible for a malicious user to "reproduce" a POST form submitted by a licensed user. In order for such an attack to be possible despite the security mechanism, the malicious user must somehow know the secret token, which is distinct for each user (using a cookie).

6.1.4.3 SQL Injection Protection

SQL injection occurs when a malicious user attempts to insert malicious T-SQL into the parameters used in Dynamic SQL [7]. It is one of the most dangerous attacks on a website, since a malicious user can extract critical information about another user's credentials such as email address, username, and even password. The SHOW database is protected from such attacks, as query sets are protected by SQL injection, because all queries are generated using query parameterization. It is important to note that the SQL query is used to define the query parameters separately. Since the parameters coming from the user may not be secure, they escape from the underlying database driver.

6.1.4.4 Clickjacking protection

Clickjacking is a common type of attack where a malicious site crawls onto another site in the form of a frame, with no visible difference to the user. This operation follows 4 steps to become successful. The first step involves misleading the user of the attractiveness of the frame. The second step involves performing some user action such as filling out a form or pressing a button. The third and most difficult step is the introduction of the content by the attacker in the form of JavaScript or HTML and at the same time zeroing the visibility of the frame through deception of the users leading them to press the button. Finally, without the user being notified or aware of it, user’s click has been captured and made the attacker capable of utilizing it for malicious purposes [8]. SHOW project contains protection against clickjacking exploits in the form of the X-Frame-Options middleware, which in a supporting browser that can prevent a site from being rendered inside a frame.

6.1.4.5 Host header validation

SHOW server uses the Host Header provided by the client to construct URLs in certain cases. Host Header is responsible for preventing XSS attacks, cache poisoning attacks, CSRF attacks and poisoning links in emails.

6.1.4.6 Session security

The implementation of security measures for the session ensures that a malicious user will not be able to access subdomains. Also, after the user's 20 minutes of inactivity, users will automatically log out so that no one has unauthorized access to his information.

6.2 Cyber Security Tests

Some attacks were performed to test the efficiency of Cyber Security Tools, which have been applied to both the SHOW DPMP and Marketplace platform. A variety of tools and mechanisms have been utilized to protect SHOW resources. These mechanisms and tools are described in deliverable D5.1 (Big Data Collection Platform and Data Management Portal) [2]. The current subchapter is a brief presentation of cyber security checks to test the SHOW infrastructure. Initially, the first attacks described are: Denial of Service (DOS) and Distributed DOS (DDOS) and were performed targeting the SHOW URL endpoints e.g., https://show-data-portal.eu (the URL endpoint for SHOW CKAN data management platform for historical data). Next, the popular data capture analyzer program WIRESHARK [15] was used to

capture the MQTT network traffic in transit in two different cases. First when no SSL/TLS encryption was utilized for MQTT connections and then with SSL/TLS enabled with the use of self-signed certificates. Moreover, Network Mapper tools are some of the most important and critical tools for hackers. Hence, the way forward and proxy servers can hide the real IP from a hacker is presented. Finally, unauthorized access to resources can be avoided with the Keycloak server, which is a tool that supports OAuth2 and Role Access Management services.

6.2.1 Denial of Service (DOS) and Distributed DOS (DDOS) Attack mitigation with CLOUDFLARE

Different Python Libraries were used to perform DOS and DDOS attacks. The DOS python scripts that were used to test the SHOW infrastructure can be found in Appendix III: Cyber Security and more precisely in Table 27: DOS/DDOS Python Libraries.

All the attacks were performed simultaneously from Virtual Machines (VMs) which were installed on Google Cloud Platform [16]. Also, a VM was used to ping the targeted URL to inspect the response server times. CLOUDFLARE was configured in under attack mode. A slight increase in the server response times was observed for the first seconds of the attack. The normal response time was about 11-12ms and the maximum response time during the attack was 200ms. CLOUDFLARE was able to find, manage and cut the connections from the attackers. CLOUDFLARE also classified and visualized the attacks in the CLOUDFLARE dashboard as shown in Figure 62.

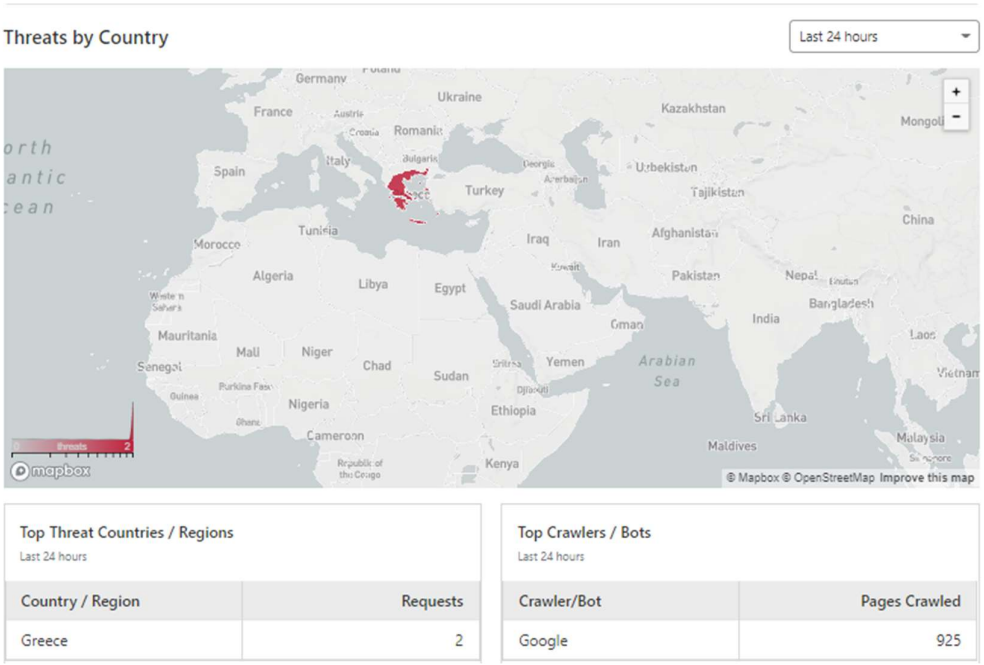


Figure 62: Threats visualized in CLOUDFLARE

6.2.2 Man in the middle attack mitigation (MITM) and message spoofing with SSL/TLS

MITM attack or message spoofing was performed with WIRESHARK, which is probably the most used packet tracing and packet network analyser tool. WIRESHARK was filtered to capture the MQTT messages in the network in two different use cases. First, with no SSL/TLS encryption. In this case, WIRESHARK was able to capture the payload of the messages and

translate them to raw text. So, a malicious user could sniff the MQTT messages which are in transit and use them to gain privileged access to the system or perform different attacks that may find the system vulnerable. In the second case, self-signed certificates were used to encrypt the message that is transferred from the vehicle to the SHOW DPMP. In this case, the hacker was unable to read the message in transit.

An indicative message as it was captured in WIRESHARK with no SSL/TLS configuration is presented in Appendix III: Cyber Security. In Appendix III, it is shown the message payload as it was captured with WIRESHARK when SSL/TLS configuration was applied to the vehicle – SHOW DPMP communication. In this case, the hacker needs the certificate in order to decrypt and read the message payload.

Regarding encryption, SSL/TLS x.509 certificates are based in key pairs and asymmetric encryption and an example of one public key which was used to test the connection in the pre-demo phase is presented in Appendix III: Cyber Security.

6.2.3 Avoid Network Discovery Tools/ Network Mappers with NGINX and CLOUDFLARE

NMAP [17] is a Network Mapper discovery tool that may reveal vulnerable system points. NMAP was applied to the SHOW DPMP URL https://show-data-portal.eu, and the results are presented in Appendix III: Cyber Security.

As observed in the specific snip, the mapper was unable to find any weak spots. This is because of the SHOW architecture, which employs two proxy servers: NGINX and CLOUDFLARE. NGINX is used as a forward proxy server, namely it forwards all the traffic from localhost to specific secured ports. NGINX has been configured to apply strict encryption from origin server to client alongside with CLOUDFLARE. CLOUDFLARE is used to secure the traffic to specific ports to the server and captures the traffic coming from and to these ports. CLOUDFLARE can be thought of as a private network that handles all the traffic and exposes the data from NGINX ports to the internet using its own network. So, its real and practical function is to hide the real IP and act as a VPN. In addition, it is worth mentioning that only the ports of the system that are managed through CLOUDFLARE should be publicly exposed to the internet. All the other services and ports should also be closed and protected with simple firewall rules, for example cut all inbound and outbound traffic to specific ports.

Figure 63: NGINX and CLOUDFLARE as Proxy servers

In Figure 63, a synopsis of the overall architecture of how the SHOW resources become publicly available on the internet is displayed.

6.3 SHOW Cyber Security Synopsis

In SHOW ecosystem, a variety of different cyber security tools and concepts have been applied, as depicted in Figure 64. The architecture, alongside the defence-in-depth approach, can guarantee a resilient and secure system that fulfils the most important cyber security requirements: Confidentiality, Availability and Integrity (CIA). Defence in depth is a concept that takes advantage of the different security enhancements each security component provides. These security components could be physical or virtual equipment and for even better protection it can be both. For example, a physical firewall can be used together with a virtual firewall in case a hacker is able to bypass one of them. So, the concept is to develop as many as possible obstacles to the intruder. All defence mechanisms mentioned in section

6 are applied to the SHOW Platform and provide an extensive cyber security architecture against the most commonly listed cyber-attacks. The system can guarantee the fulfilment of the most critical requirements regarding Cyber Security: Confidentiality, Integrity and Availability (CIA). SSL/TLS protocol alongside with authentication and authorization have been applied to all connections and entities to ensure Confidentiality. Integrity is fulfilled by utilizing hash algorithms and Availability is based on firewalls, load balancers and proxy servers such as NGINX, IDS such as SNORT and Content Delivery Network (CDN) platforms such as CLOUDFLARE.

As it has been already described in the section 6.2 of the current document, different checks have been performed to test the requirements of the SMDP cyber security system. These specific attacks are managed to be mitigated with the proper security mechanisms. Moreover, it is worth mentioning that the concept of privileged access management can boost the system overall security. This means that in case a malicious user has gained access to the system they should not be escalated to a more privileged role and access the important resources of the project. In addition, segmentation of services to different machines can guarantee that there is not a single point of failure for the system. Finally, all the SHOW members, especially the users in the SHOW project who have elevated privileged access to the SMDP's resources (spear-phishing attack), have to be informed of the current cyber security threats. Plenty of phishing attacks are performed each year and can cause critical damage to the overall cyber security system. Cyber security awareness is the most important countermeasure for SHOW cyber security ecosystem.

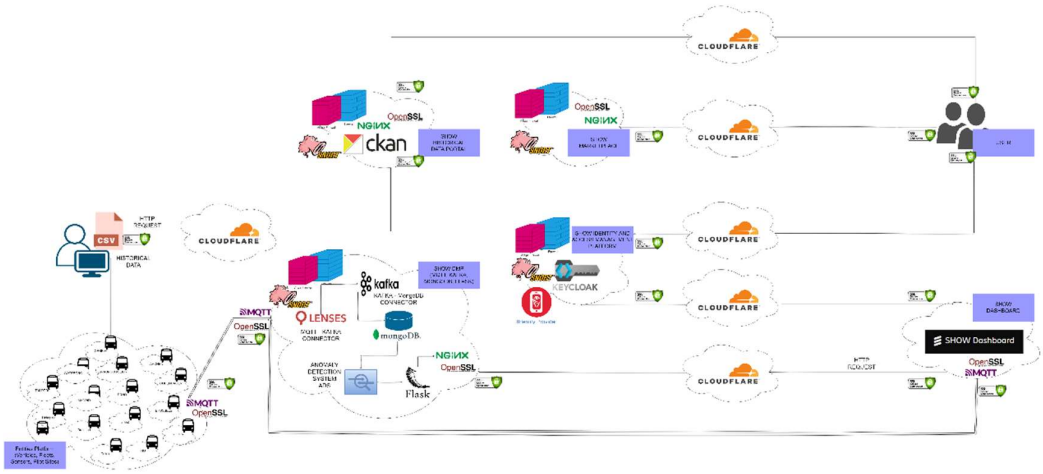


Figure 64: SHOW Ecosystem Cyber Security Synopsis

6.4 AI-based automotive cyber security challenges and future directions

Taking into account the different perspectives of AI-based cyber security mechanisms presented earlier, along with the formulated SHOW ecosystem, a set of challenges are revealed which may pave the way towards real-world realizations. These challenges are described in more detail next, accompanied by future directions.

6.4.1 Privacy and anonymization

AI-based cyber security solutions face privacy issues particularly if the data has to be sent to a centralized cloud system for computation. According to a recent research, addressing privacy concerns through data anonymization or noise injection is significantly difficult. Moreover, even when appropriately implemented, the required privacy budget might

significantly reduce the system's accuracy [18]. This demonstrates that concepts like differential privacy are not necessarily the ultimate solution for privacy issues. Another approach is federated learning, which enables privacy-preserving local learning implemented in the vehicles by taking the global weight updates from a global model deployed in a centralized system such as the cloud [19]. In order to properly address such issues, AI and automotive cyber security researchers would need to come together to study the trade-offs between privacy and performance.

6.4.2 Data issues

AI-based cyber security solutions rely heavily on data. Some of these issues seem to be related to dataset bias and coverage problems, where the dataset is not a reliable representation of reality due to skewed sampling. Sometimes there is a significant size difference among classes in a dataset. For example, an intrusion detection dataset for automotive systems may have a more significant proportion of benign instances and only a few attack instances leading to a dataset imbalance that can negatively impact the performance of machine learning-based solutions. Unfortunately, the class imbalance is prevalent in security applications where normal data is observed more than malicious data. Over-sampling from the minority class, under-sampling from the majority class, or a hybrid strategy like SMOTE [20] can be used to address data balance difficulties. Another method is to give to the minority classes higher weight by assigning each class a specific score/loss multiplier [21]. Also, performance metric different from accuracy, such as the F-1 score and Matthew's correlation coefficient (MCC) are better suited to evaluate performance when working with imbalanced datasets [22].

6.4.3 Explainability and generalizability of AI-based automotive IDS

Over the years, many machine learning-based automotive intrusion detection methods have been developed in the research community. However, a major percentage of this field's academic research has yet to be translated into practical applications [23]. The lack of accountability of the models utilized, in essence, they are black boxes in their current condition with outputs that are difficult or impossible to explain, is a major barrier to the widespread use of AI algorithms in real-world applications such as automotive IDS. These characteristics are essential for gaining user trust, and additional research is needed to figure out how these systems can provide consistent and effective explanations for their decisions. Another factor is that the designed models are tested and perfected on one dataset that may not perform well when applied to other datasets coming from different vendors. This is particularly important if an automotive IDS is supported by a centralized detection system such as the cloud that needs to work on a wider variety of datasets. Current research in this field focus on exploring suitable feature formats allowing detecting attacks in different datasets, thereby allowing the designed model's generalizability for practical use [23][24].

7 Interoperability

Interoperability is considered the concept that will boost data sharing among all involved stakeholders in SHOW ecosystem. An interoperable architecture should provide a series of functionalities:

- Ensure a secure and stable background architecture across the participating systems.
- Maximize real-time data transfer and real-time information.
- Enable continuous deviation information across involved parties.
- Boost competitiveness between operators.

In D4.1 interoperability was approached as part of the design of the integrated system point of view foreseeing interfaces (of both standardized and proprietary nature) among system internal layers as well as system and external data providers. Specifically, from the fleet point of view, different C-ITS data protocols applying to CCAM vehicles and smart infrastructure have been reviewed in order to provide technical recommendations to the local site teams. In this deliverable, the interoperability achieved by applying common data models and interfaces for a cross-sites harmonized LFMP to SMDP data exchange will be described. In each pilot site additional interoperability mechanisms may apply depending on the interoperability protocols agreed between the vehicle owners and the existing cloud infrastructure components/APIs, these have been already reported in sub-sections 4.x.4.

7.1 Data Interoperability

The SHOW project aims to maximize data sharing from twenty different pilot sites across Europe and especially, to significantly enhance travel information sharing conducted using Public Transport. Data interoperability poses a crucial role in SHOW project, since each pilot site possesses different groups of vehicles transmitting data from a variety of sensors. Interoperability allows the identification and the indexing of data transmitted from and to the SHOW ecosystem. Specifically, within the SHOW MDP, a variety of mechanisms have been developed to guarantee interoperability between all the entities and operators participating in data sharing activities.

Firstly, a standard data schema (represented in JSON format) has been adopted when formulating each message. This approach guarantees that the message format the sender is using is aligned with the receiver's message format, thus diminishing incompatibilities. An example of a schema value is presented in Figure 65:

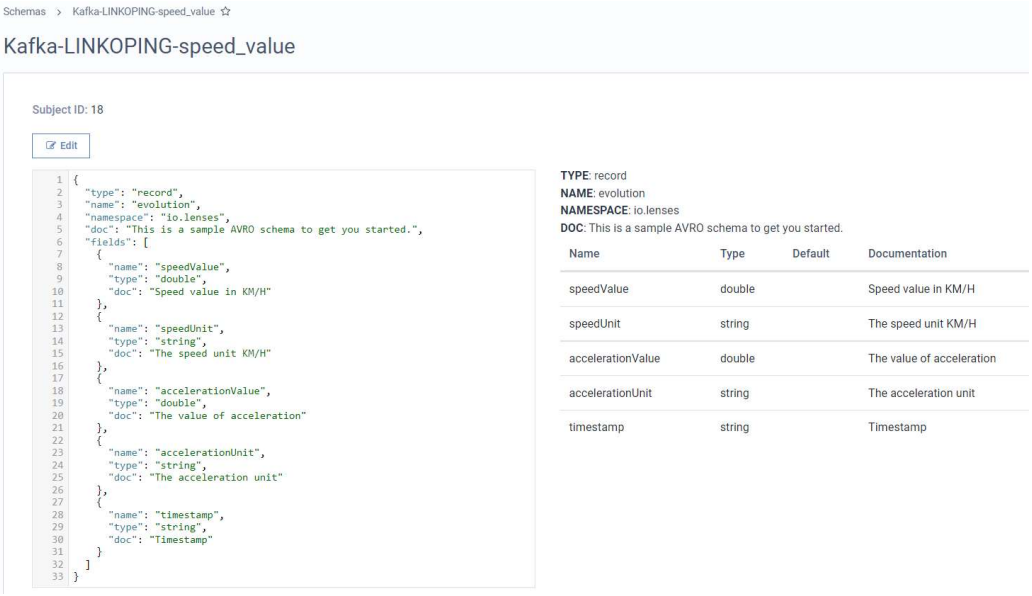


Figure 65: Message schema - speed value Linkoping

In addition to the default schema for messages, a communication schema has been applied. This means that each entity has been assigned to a unique Identification Number (ID). Within SHOW project, there are three main IDs:

- Site ID
- Fleet ID
- Vehicle ID

This is extremely important in order for the communication to be established among all pilot sites and all vehicles, since each Site ID is used as topic name in MQTT and KAFKA protocols utilized in the project. The Madrid site IDs are presented in the Figure 66 as an indicative example.

Madrid Site (Spain)

- Site ID: 359f2b37-7fc9-4d07-b957-7a3e87c60f1f
  - Fleet 1:
    - Fleet ID: 7de70f04-5d50-4374-9656-7f80828ad824
    - Fleet Name: IRIZAR Fleet
    - Routes: La Nave, Villaverde
      - Vehicles:
        - Vehicle 1:
          - ID: irizar-vehicle-1
  - Fleet 2:
    - Fleet ID: f9beae21-5866-4b8a-bc2b-501e61ec938d
    - Fleet Name: EMT Fleet
    - Routes: La Nave, Villaverde
      - Vehicles:
        - Vehicle 1:
          - ID: emt-vehicle-1
        - Vehicle 2:
          - ID: emt-vehicle-2
  - Fleet 3:
    - Fleet ID: 2ae2ed0c-84cf-442f-8ba8-1fd01a49acc3
    - Fleet Name: Tecnalia Fleet
    - Routes: La Nave, Villaverde
      - Vehicles:
        - Vehicle 1:
          - ID: tecnalia-vehicle-1
        - Vehicle 2:
          - ID: tecnalia-vehicle-2

Figure 66: Communication Schema – Madrid

Finally, a group of data converters has been developed in the SHOW MDP infrastructure to tackle data inconsistencies between stakeholders when necessary. These converters aim to apply data transformations and then push the data to the proper database table with the appropriate format, thus facilitating data provision in an interoperable way. Next, these data are used to calculate corresponding KPIs, which are visualised through the SHOW Dashboard. The consistent format of the data is very critical for the SHOW MDP – SHOW Dashboard connection, since the current connection is based on APIs (HTTP requests) with a standard payload. The HTTP responses to the SMDP API have to follow a specific format in order for the dashboard to be able to receive and visualize these data. The response as described in the SHOW documentation is presented in Figure 67.

• Response:


```
{
    "entity": <"site","fleet","vehicle">,
    "entityId": "<siteId/fleetId/VehicleId>",
    "kpiId": "1",
    "kpiValue": 0,
    "kpiUnit": "",
    "frequency": <"daily","weekly","monthly">,
    "category": "travel-and-passenger-patterns",
    "fromDate":"",
    "toDate":"",
    "kpiValues":
        [
            {
                "value": 0,
                "time":"<day,week,month>"
            },
            {
                "value": 0,
                "time":"<day,week,month>"
            }
        ]
}
```


Figure 67: HTTP response for SHOW MDP - Dashboard connection

8 SHOW Risk Assessment – 2nd Round

8.1 Introduction

A cross-cutting multi-layered risk assessment is planned to be performed prior to all distinct evaluation phases in SHOW (technical validation; "pre-demo" phase – 1st pilot round with end-users; "final demo" phase – 2nd pilot round with end users), using an extended FMEA methodology, within the context of Activity 4.6.

For every risk identified through a process involving all the WP leaders and test sites leaders of the project, the risk **severity, occurrence probability, detectability and recoverability** is being ranked **by the SHOW Core Group** to allow, finally, the calculation of the **overall risk level** per each. As a starting point the risks identified in the project's proposal phase are used and are being updated during each risk assessment phase. Not only **technical,** but also **behavioural**, **legal/regulatory, operational** and **demonstration/evaluation** risks are considered, whereas apart from the **horizontal risks, risks associated with specific test sites** are also recognised if and when applicable, while COVID-19 related effects have been also addressed.

The first round of risk assessment and the emerging results have been already presented in *D4.1: Open modular system architecture and tools - first version (ICCS, M12).* The first round corresponded to the risks recognised in view of the technical validation phase of the project (that is now closing for the SHOW sites).

The 2nd iteration reported herein, focused on the identification of the risks in view of the "pre-demonstration" phase that has started since some months to be progressively launched at the SHOW sites, aiming at:

1. Checking if the formerly recognised risks as of the 1st round have been indeed materialized and how in specific.
2. If the formerly recognised risks as of the 1st round are still applicable and, if yes, if they remain equally significant.
3. Which are the new risks that have been recognised on top of the ones of the 1st iteration, and, finally,
4. Which are the mitigation and corrective actions that can be applied in order to minimise their chance of occurrence or at least their degree of severity.

The third and final iteration of the SHOW risk assessment will be implemented prior to the final real life pilot phase of the project and its results will be reported in *D4.4: Open modular system architecture - third version (ICCS, M36).*

The extended FMEA methodology, upon which the risk assessment in SHOW is conducted, has been already presented in D4.1. As such, it is not repeated herein. The following section presents the results of the 2nd risk assessment iteration, whereas

8.2 2nd SHOW Risk Assessment Round results

The analytical outcomes of the second risk assessment round in SHOW are provided below. Going through the outcomes, one can see that **45 risks have been identified in total at this phase of the project**, **5 of them being of double risk type (e.g. dealing with technical but also operational aspects)**, while **39 are pre-existing as of the Grant Agreement and the first risk assessment iteration** (shaded in different colours, in grey the ones from the GA phase and in light blue the ones from the first round).

In total (and considering the above-mentioned double type of risks), **11 technical**, **19 operational**, **4 behavioural**, **7 legal/ regulatory** and **8 demonstration/evaluation related risks** have been identified and analysed.

It also 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 29, indicated in orange), being the one dealing with the impact of COVID-19 in a cross-cutting way in the project, associated mainly with issues related to delays noticed in 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, 20 risks of the identified ones have been evaluated to be of low severity (slight and insignificant), while the rest 24 have been validated as of moderate severity.

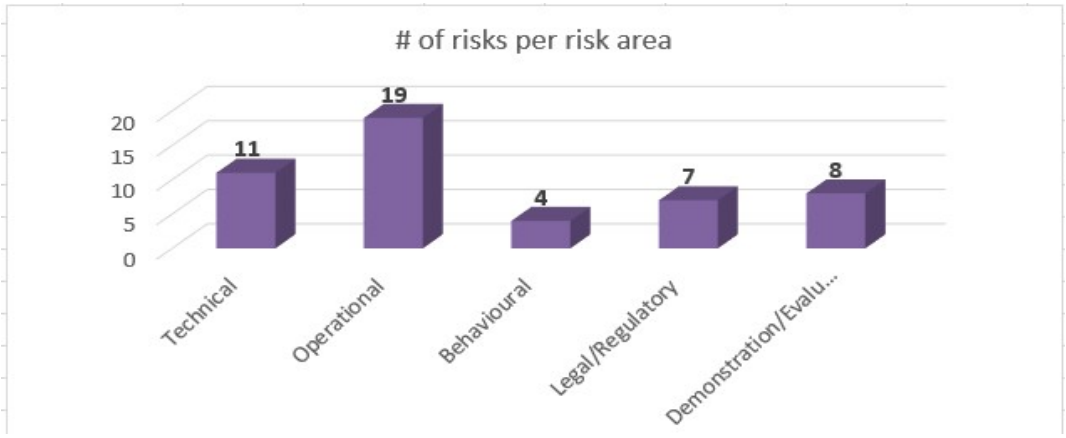


Figure 68: SHOW 2nd Risk Assessment Round – Clustering of risks (45 in total; 5 are doubled in clusters).

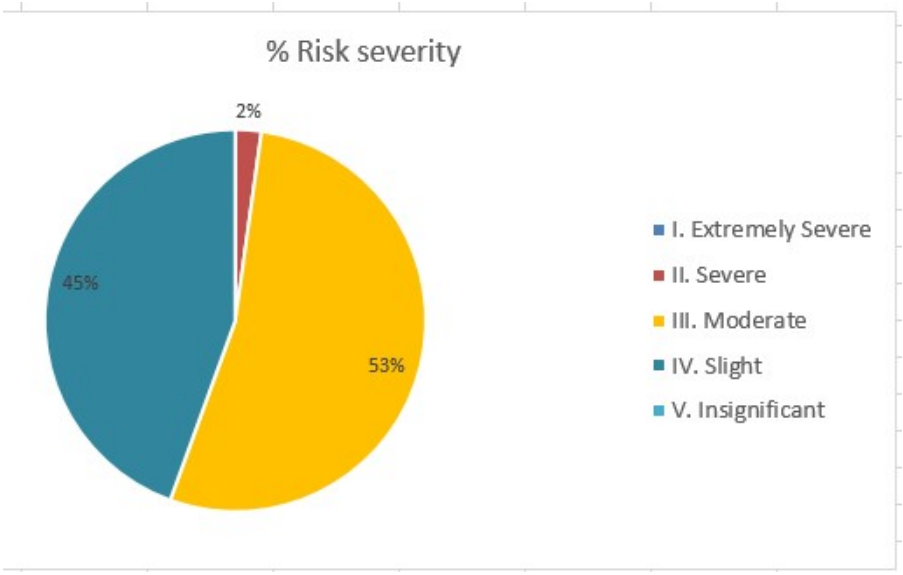


Figure 69: SHOW 2nd Risk Assessment Round – Risk Severity Classification.

Comparing to the first risk assessment round, the risks overall number **has increased by 5 risks**, which, given that the intermediate period between the two risk assessment iterations was considered the most challenging for the project, is not considered a significant increase.

The current derived allocation across the different potential nature of risks (technical, operational, behavioural, legal/regulatory, demonstration/ evaluation) is similar to the 1st risk

assessment round (where, correspondingly, **12 technical, 15 operational, 4 behavioural, 6 legal/ regulatory** and **8 demonstration/evaluation** risks had been identified). It is specifically operational risks that have been increased, which is justified by the fact that the project is getting close to the actual real life experience of the field trials.

It is also worth stressing that it is again the same (sole) risk that is characterised with Level II Severity, which is namely the pandemic related risk. Finally, it is optimistic for the project that the number of low severity risks has increased from 4 (in the first risk assessment round) to 20, while, rationally, the number of moderate severity has decreased from 35 to 24. This finding reveals that progressively risks are mitigated or not even materialized due to the corrective actions taken (which is also evident through the materialization last columns of the table below), which further reveals the significance of the risk assessment process itself for the project. It is also worth notable that most risks are applicable to all the test sites of SHOW, having a cross-site nature, while a few of them (i.e. adverse weather conditions) are naturally associated to the specificities of some test sites.

The full results of the 2nd Risk Assessment round are provided in the table 1 of Appendix IV. If there are specific test sites associated with the risk, those are mentioned per se. The calculated Risk Number is also colour coded: Yellow stands for Medium Severity; Green stands for Low Severity, and Orange for High Severity. The risk mitigation measures and the so far materialization, if any, of each risk is also discussed.

Risks rows are shaded in different colours: in grey are the ones – pre-existing and still considered applicable from the Proposal/ GA phase; in light blue the ones from the first risk assessment round; in yellow the additional ones recognised on top in the 2nd risk assessment round.

Due to high length the averaged risk severity, risk occurrence probability, risk detectability and risk recoverability numbers that lead, upon the FMEA formula (see D4.1), to the consolidated overall Risk Number (RN) are not included in the Appendix IV table (they are fully available upon request).

9 Conclusions and outlook

The targets of this deliverable and ways used to achieve it were:

a. to present the local sites architectures and discuss any interoperability aspects: this part is covered by chapter 4 applying the template proposed in chapter 3. Not all sites' diagrams follow strictly the template but the overall language and objectives of the architecture description is harmonized across all sites.

b. to present the SHOW Mobility Data Platform (SMDP) architecture updates: this part is covered by chapter 4 in close collaboration with the SMDP technical team (wp4+5, CERTH-ITI)

c. to present the cybersecurity tools specifications and present updates on theoretical and implementation / testing work performed as part of WP4-A4.5: this part is covered by chapter 6.

d. to present the SHOW data management interoperability tools specifications: this part is covered by chapter 7.

e. to present the updated risk management tracing table: this part is covered by chapter 8 and App. IV.

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

- Local sites architectures' refinements covering especially the sites that presented incomplete information in this version as well as local sites added recently replacing other SHOW sites. Furthermore, incomplete information on services deployed will be added where updates are needed.
- SMPD cybersecurity updates covering also feedback from sites' demo phase.
- SHOW sites' connectivity/interoperability updates based on feedback from sites' demo phase.
- Updated risk management tracing table based on experience gathered from pre-demo and demo phase of the project.

References

[1] SHOW (2021). D4.1: Open modular system architecture and tools (November 2021 revision). Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

[2] SHOW (2021). D5.1: Big Data Collection Platform and Data Management Portal. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

[3] Singh, M., Singh, P., & Kumar, P. (2020, March). An Analytical Study on Cross-Site Scripting. In *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)* (pp. 1-6). IEEE.

[4] Sarmah, U., Bhattacharyya, D. K., & Kalita, J. K. (2018). XSSD: A Cross-site Scripting Attack Dataset and its Evaluation. In *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)* (pp. 21-30). IEEE.

[5] Sudhodanan, A., Carbone, R., Compagna, L., Dolgin, N., Armando, A., & Morelli, U. (2017, April). Large-scale analysis & detection of authentication cross-site request forgeries. In *2017 IEEE European symposium on security and privacy (EuroS&P)* (pp. 350-365). IEEE.

[6] Calzavara, S., Conti, M., Focardi, R., Rabitti, A., & Tolomei, G. (2020). Machine learning for web vulnerability detection: the case of cross-site request forgery. *IEEE Security & Privacy*, *18*(3), 8-16.

[7] Pollack, E. (2019). Protecting Against SQL Injection. In *Dynamic SQL* (pp. 31-60). Apress, Berkeley, CA.

[8] Jyotiyana, P., & Maheshwari, S. (2018). Techniques to Detect Clickjacking Vulnerability in Web Pages. In *Optical and Wireless Technologies* (pp. 615-624). Springer, Singapore.

[9] Snort. (2021, January 4). New to Snort?. https://www.snort.org/

[10] Hendrawan, H., Sukarno, P., & Nugroho, M. A. (2019, July). Quality of Service (QoS) Comparison Analysis of Snort IDS and Bro IDS Application in Software Define Network (SDN) Architecture. In 2019 7th International Conference on Information and Communication Technology (ICoICT) (pp. 1-7). IEEE.

[11] Flask. Retrieved December 15, 2021, from https://flask.palletsprojects.com/en/2.0.x/.

[12] Koster M (2018, April). Web of Things (WoT) Protocol Binding Templates. https://www.w3.org/TR/2018/NOTE-wot-binding-templates-20180405/.

[13] UFW. Retrieved December 15, 2021, from https://help.ubuntu.com/community/UFW.

[14] How Does a Firewall Work?. Retrieved December 15, 2021, from https://hackonology.com/courses/computer-networking/lesson/firewall/. Last accessed 15/12/2021

[15] Wireshark · Go Deep. Retrieved December 15, 2021, from https://www.wireshark.org/.

[16] Google Cloud. Retrieved December 15, 2021, from https://cloud.google.com/.

[17] Nmap. Retrieved December 15, 2021, from https://nmap.org/.

[18] Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., & Ristenpart, T. (2014). Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 17-32).

[19] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

[20] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique. Journal of artificial intelligence research, 16, 321-357.

[21] Pazzani, M., Merz, C., Murphy, P., Ali, K., Hume, T., & Brunk, C. (1994). Reducing misclassification costs. In Machine Learning Proceedings 1994 (pp. 217-225). Morgan Kaufmann.
[22] Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC genomics, 21(1), 1-13.
[23] Sarhan*, M., Layeghy, S., & Portmann, M. (2021). Evaluating Standard Feature Sets Towards Increased Generalisability and Explainability of ML-based Network Intrusion Detection.* arXiv preprint arXiv:2104.07183
[24] Sarhan, M., Layeghy, S., & Portmann, M. (2021). An Explainable Machine Learning-based Network Intrusion Detection System for Enabling Generalisability in Securing IoT Networks. arXiv preprint arXiv:2104.07183.

Appendix I: Data Collection and KPI Calculation

The highlighted KPIs compose the subset of which will be visualized in the SHOW Dashboard. Each site should provide the corresponding data, relevant to the contributing use cases. The provision of data required for the rest of the KPIs remains mandatory. This data would be utilized for the needs of service implementations, for the calculation of metrics within other WPs and for the complete and overall evaluation of the project.

Table 25: SHOW Data Collection and KPI Calculation

KPI ID	Data Input	KPI calculation Output	KPI Grouping
1.1	Passengers in vehicle	Average Passengers Transported (daily, weekly, monthly)	Society, Employability, Equity
1.2	Vehicle availability Vehicle utilization	Average Vehicle Utilization Rate (daily, weekly, monthly)	Society, Employability, Equity
1.3	Operative cost (once demo is concluded)	Operative Cost (once, monthly)	Society, Employability, Equity
1.4	Operative cost + Vehicle utilization	Operative Revenue (weekly, monthly)	Society, Employability, Equity
1.5	Passenger location Passenger destination Willingness to share	Shared Mobility Rate (weekly, monthly)	Society, Employability, Equity
1.6	Mileage, Occupancy, Kilometers traveled with passengers	Distance Traveled with Passengers (daily, weekly, monthly)	Society, Employability, Equity
1.7	Mileage, Occupancy, Kilometers traveled without passengers	Distance Traveled without Passengers (daily, weekly, monthly)	Society, Employability, Equity
1.8	Jobs lost	Job Loss (monthly)	Society, Employability, Equity
1.9	Jobs gained	Job Gain (monthly)	Society, Employability, Equity
2.1	Current speed of the vehicle	Average Speed (daily, weekly, monthly)	Traffic, Energy and Environment
2.2	Current acceleration of the vehicle	Acceleration Variance (daily, weekly, monthly)	Traffic, Energy and Environment
2.3	Direct ride distance	Total Distance Traveled (daily, weekly, monthly)	Traffic, Energy and Environment
2.4	Energy consumption	Average Energy Usage (daily, weekly, monthly)	Traffic, Energy and Environment
2.5	Occupancy	Increase in Vehicle Occupancy (daily, weekly, monthly)	Traffic, Energy and Environment
2.6	QoS	Quality of Service (daily, weekly, monthly)	Traffic, Energy and Environment
2.7	CO2 emissions	Reduction in Carbon Dioxide (daily, weekly, monthly)	Traffic, Energy and Environment
2.8	Noise level of the city	Reduction in Noise level (daily, weekly, monthly)	Traffic, Energy and Environment
2.9	Current energy consumption	Reduction in Energy consumed (daily, weekly, monthly)	Traffic, Energy and Environment

KPI ID	Data Input	KPI calculation Output	KPI Grouping
2.10	Strong braking	Hard Brakes (daily, weekly, monthly)	Traffic, Energy and Environment
2.11	Reliability of the service	Service Reliability (daily, weekly, monthly)	Traffic, Energy and Environment
2.12	Number of stops Timetable	Scheduled Stops (daily, weekly, monthly)	Traffic, Energy and Environment
2.13	Number of stops Timetable	Non Scheduled Stops (daily, weekly, monthly)	Traffic, Energy and Environment
2.14	Delay, deviation from timetable	Vehicle Delay (daily, weekly, monthly)	Traffic, Energy and Environment
2.15	Delay, deviation from timetable	Interchapter Delay (daily, weekly, monthly)	Traffic, Energy and Environment
2.16	Network traffic metadata	Network Travel Time (daily, weekly, monthly)	Traffic, Energy and Environment
2.17	Traveled Kilometers	Total Mileage (daily, weekly, monthly)	Traffic, Energy and Environment
2.18	Network traffic metadata	Total Network Delay (daily, weekly, monthly)	Traffic, Energy and Environment
2.19	Network traffic metadata	Network Speed (daily, weekly, monthly)	Traffic, Energy and Environment
2.20	Timetable planned, timetable actual	Trips (daily, weekly, monthly)	Traffic, Energy and Environment
2.21	Emissions daily	CO2, PM and NOx Emissions (daily, weekly, monthly)	Traffic, Energy and Environment
2.22	Air pollution	Air Quality (daily, weekly, monthly)	Traffic, Energy and Environment
2.23	Noise pollution	Noise (daily, weekly, monthly)	Traffic, Energy and Environment
3.1	Number of accidents	Road Accidents (weekly, monthly)	Road Safety
3.2	Pilot site feedback	Safety Enhancement (weekly, monthly)	Road Safety
3.3	Pilot site feedback	Conflicts (weekly, monthly)	Road Safety
3.4	Shuttle camera	Illegal Overtaking (weekly, monthly)	Road Safety
4.1	Payload (cargo weight)	Number of Cargo transported (daily, weekly, monthly)	Logistics
4.2	Payload (cargo weight)	Average Load Ratio (daily, weekly, monthly)	Logistics
4.3	Timetable planned Timetable actual	Delivery Punctuality (daily, weekly, monthly)	Logistics
4.4	Timetable planned Timetable actual	Delivery Precision (daily, weekly, monthly)	Logistics
4.5	Customer satisfaction	Customer Satisfaction (daily, weekly, monthly)	Logistics
4.6	Unit cost of delivery	Unit Cost of Delivery	Logistics

KPI ID	Data Input	KPI calculation Output	KPI Grouping
		(daily, weekly, monthly)	
4.7	Load factor patterns	Load Factor Patterns (daily, weekly, monthly)	Logistics
4.8	Public acceptance	Public Acceptance (daily, weekly, monthly)	Logistics
4.9	Willingness to pay	Willingness to Pay (daily, weekly, monthly)	Logistics
4.10	Number of accidents	Accidents on Site (daily, weekly, monthly)	Logistics
4.11	Number of accidents	Accidents in AV UFT Facility (daily, weekly, monthly)	Logistics
4.12	Number of crimes	Crimes in AV UFT Facility (daily, weekly, monthly)	Logistics
4.13	Number of vandalism	Vandalism in AV UFT Facility (daily, weekly, monthly)	Logistics
4.14	Lost and damaged packets	Loss & Damage to Parcels in AV UFT Facility (daily, weekly, monthly)	Logistics
4.15	User feedback	Fair & Equal Access in AV UFT Facility (daily, weekly, monthly)	Logistics
5.1	Service acceptance user feedback	Traveler Acceptance (daily, weekly, monthly)	User Acceptance
5.2	Service reliability user feedback	User Reliability Perception (daily, weekly, monthly)	User Acceptance
5.3	Service safety user feedback	User Safety Perception (daily, weekly, monthly)	User Acceptance
5.4	User feedback	Travel Comfort (daily, weekly, monthly)	User Acceptance
5.5	Service usefulness user feedback	Perceived Usefulness (daily, weekly, monthly)	User Acceptance
5.6	User feedback	Willingness to Pay (daily, weekly, monthly)	User Acceptance
5.7	Service ridesharing user feedback	Willingness for Shared Ride (daily, weekly, monthly)	User Acceptance
5.8	User feedback	Use of Autonomous Driving (daily, weekly, monthly)	User Acceptance
6.1	User feedback	User Cases (daily, weekly, monthly)	Project Success
6.2	User feedback	User Case Realization (daily, weekly, monthly)	Project Success
6.3	Operator feedback	SMEs using SHOW Marketplace (daily, weekly, monthly)	Project Success
6.4	Operator feedback	Business Models (daily, weekly, monthly)	Project Success
6.5	Operator feedback	Local Synergy Business Models (daily, weekly, monthly)	Project Success

KPI ID	Data Input	KPI calculation Output	KPI Grouping
6.6	Operator feedback	MoUs for Service Sustainability (daily, weekly, monthly)	Project Success
6.7	Pilot Site feedback	Deployed Fleets (daily, weekly, monthly)	Project Success
6.8	Pilot Site feedback	Future AV Fleets (daily, weekly, monthly)	Project Success
6.9	Pilot Site feedback	Alternate Infrastructure Schemes (daily, weekly, monthly)	Project Success

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

The services shown in the following table are derived from the latest one to one interviews contacted with the demo site leaders that expressed their interest in the initial interviews.

Service	Brno	Turin	Gothenburg	Tampere	Linköping	Salzburg	Graz	Trikala	Carinthia
Fleet Management	X	X							
Demand prediction	X	X*	X	X	X				
Mobility patterns	X	X*	X	X	X				
ETA	X	X*		X		X	X		
C-ITS & Traffic Management		X						X	
Safety services & passenger counting			X						
Freight vehicle / cargo services	X*							X*	X*

*Tentative.

The above table summarises the results of interviews contacted with the leaders of each demo site. Services marked with *denote an optional service that might be supported in the final phase of the pilot (e.g. the service will be implemented by the provider). The services will be described in detail in the upcoming deliverable D5.3: CCAM enhanced services based on Big Data and AI (M30).

Appendix III: Cyber Security

A variety of information related to cyber security is presented within this Appendix.

Table 26: Snort Default Classifications

Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium
misc-attack	Misc Attack	medium
non-standard-protocol	Detection of a non-standard protocol or event	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious username was detected	medium
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web application	medium
icmp-event	Generic ICMP event	low
misc-activity	Misc activity	low
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low

Classtype	Description	Priority
tcp-connection	A TCP connection was detected	very low
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium
misc-attack	Misc Attack	medium
non-standard-protocol	Detection of a non-standard protocol or event	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious username was detected	medium
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web application	medium
icmp-event	Generic ICMP event	low
misc-activity	Misc activity	low
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low
tcp-connection	A TCP connection was detected	very low

Table 27: DOS/DDOS Python Libraries

Library Name	Source
Ha3MrX	https://github.com/Ha3MrX/DDos-Attack
ufonet	https://github.com/epsylon/ufonet
MHProDev/MHDDoS	https://github.com/MHProDev/MHDDoS
CC-attack	https://github.com/Leeon123/CC-attack
Pyflooder	https://github.com/D4Vinci/PyFlooder

Figure 70: MQTT message with no SSL/TLS encryption

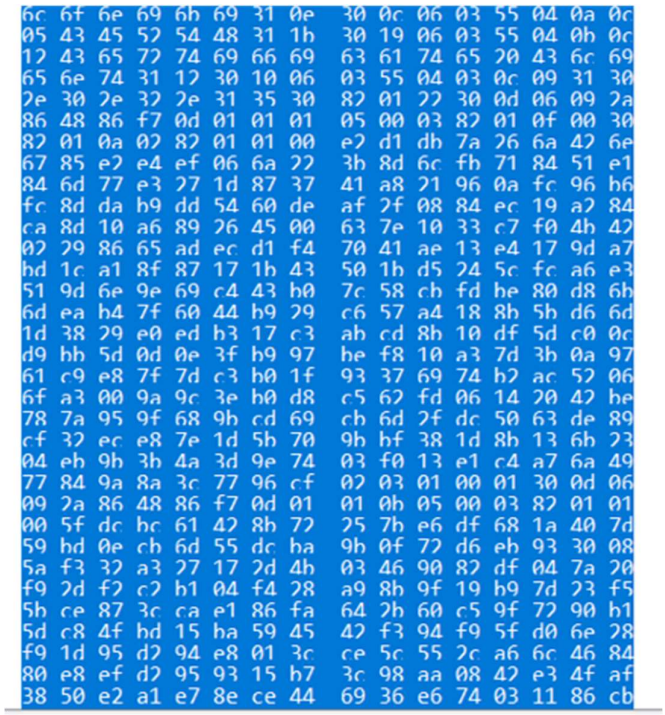


Figure 71: MQTT message with SSL/TLS encryption

Figure 72: Public Key for SSL/TLS MQTT communication

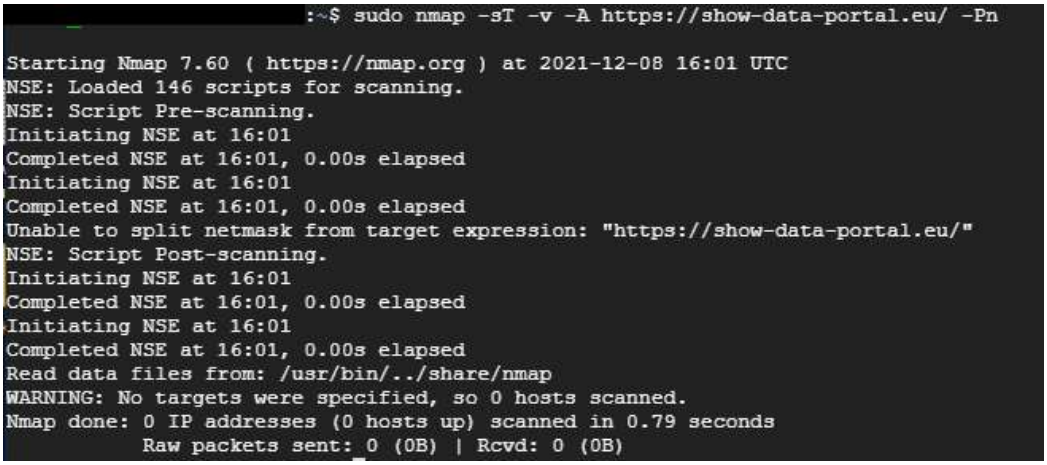


Figure 73: Application of Nmap to SHOW MDP URL (indicative results)

Appendix IV: SHOW Risk Assessment results (second round)

Table 28: 2nd SHOW Risk Assessment Round results.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
1	Lack of will of PTAs/PTOs to create common business models for PT and non PT mobility services disrupting the current state of art/ business.	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 awareness strategies have not been adequate.	Progressively, during the entire project lifespan, throughout physical and virtual events, surveys and interviews. Still, more evidently, during demonstration phases.	WP2	All	81	Medium	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			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										not yet available, create a comprehensive integrated mobility strategy for each of the participating cities, regions and stakeholder eco-systems in the course of the project.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
2	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	108	Medium	This risk is being 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			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										and databases.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
3	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 the project different phases	WP3, WP11, WP12, WP13, WP14	All	78,2	Medium	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 are being dealt thoroughly and across countries within SHOW			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
					(demonstration, evaluation, impact assessment).					in the context of WP3 and WP14 primarily. Progressive clarification has emerged in Data Management Plan and Data Privacy Impact Assessment subsequent versions, two of them already released in the project.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
4	Lack of transferability of solutions.	Technical	Interoperablity on operational level cannot	• Highly specific requirements / legacy systems per site.	Self-evident mainly during final	WP2; WP4; WP12	All	126,9	Medium	Establish a sound system architecture to enable interoperability /			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
		Operational	be proved. Replication activities may be limited.	• Local business models and stakeholder's relationships may vary highly from site to site.	demonstration phase.					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			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										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			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										communities from the project beginning and common gathering events will aim at early alignment and collaboration.			
5	Low traveller acceptance and trust issues, services underuse and	Behavioural	Insufficient data availability for robust SHOW	Ineffective user and stakeholder engagement	During pre-demonstration phase for the first	WP7, WP9, WP11,	All	99	Medium	Emphasis is put within WP7 to enhance user experience inside the			The final demo phase that is expecte

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
	non-sustainable operation.		evaluation and impact assessment. Barriers to deployment, exploitation and replication.	strategies for SHOW demonstration; ineffective engagement of local demonstration boards in SHOW; insufficient level of solutions offered; generic challenges regarding CCAV trust beyond SHOW.	time in the project.	WP12				vehicle as well as the interface towards other travellers and the vehicles; to alleviate safety and security fears. The control tower concept and the direct link to teleoperation centre (including "driver" avatars on board) are expected to help. Also,			d to be open to public and involve real life passengers has not started yet in any test site. Still, the few pre-demo activities that have been done (in Goethe

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										citizen engagement strategies of A9.3 and the tight coordination of demo communities in the context of WP12 aim to help in this direction.			nburg, Turin, Linkoeping, Tampere) have revealed great interest which imply that the risk of low engagement at least will not be materialised. Still, COVID-

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
													19 inferred restrictions are not positively affecting engagement.

6	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 any. Other than that, it constitute a	New mobility sector/paradigm with inevitable gaps in regulations.	During permit authorisation phase prior to pre-demonstration phase launch.	WP3, WP11, WP12	All	138	Medium	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			

			serious challenge for CCAV deployment overall across Europe.							near future that is tackled by 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.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
7	Closed vendor systems whether these refer to OEM or PTOs.	Technical Operational	Some of the functions and services will not be fully assessed in the post-validation phase.	Inevitable "silos"; trust issue; lack of common vision on interoperable CCAM.	During iterative development and integration.	SP2 (WP4 - WP8)	All	113,568	Medium	This is being tackled via the mechansims applied in the project by the Data Management Platform (A5.1) that orchestrates all flow of information between different ends of all test sites, defining and collecting the minimum set of data that is			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										mandatory by all sites towards the fulfillment of the project KPIs.			
8	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 and reluctancy to share services/products.	During development/integration.	WP6	All	61,523	Low	SHOW has built (in D6.1) a parametric infrastructure that allows different types of products, of also different maturity to be shared through it, and across different			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										access levels.			
9	Cost explosion in the high-tech sector for system development (vehicle sensor implementation, infrastructure).	Operational	Not able to fully meet the original project commitment.	Under budgeted tasks in SHOW regarding vehicle and infrastructure upgrades; at least in relation to	During development and digital/physical adaptations.	WP7, WP8	All	101,752	Medium	National initiatives and funding sources to be exploited as much as possible.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				the market reality.									
10	Technical readiness of vehicles for safe operation on	Technical	Smaller fleets; limited value added	Insufficient project planning or inevitable/ uncontrolla	During technical validation and pre-demo	WP7; WP11	Potentially all.	63,6	Low	Full technical validation performed in the project, prior to the	Turin site	Luxoft was not able to develo	Luxoft withdrew from the project,

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
	public roads not given in due time of the project pilots.	Operational	and impact.	ble technical issues in combination with COVID-19 effects. Delay in type approvals. Technical validation proving insufficient readiness.	phases (within 2021).					pre-demo phase launch (A11.2), revealing readiness for moving on to the next phase. 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		p their vehicle on time and in a way to meet the legal requirements.	and the missing vehicle will be replaced by one extra vehicle to be provided by the another project provider (solution, upon PO acceptance).

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										later the plan, transfer of know-how and products from other sites, also external to the project.			
11	Lack of adoption of the guidelines / lack of implementation resources & competence in the public sector or other stakeholders.	Operational	Barriers to wide deployment, exploitation and replication.	Current practice proving stronger; delayed digestion of changed and harmonised processes; resources	During preparation phase in view of pre-demonstration phase but also and mainly during replication phase towards	WP12, WP14, WP17	Potentially all, slightly more probably	91,805	Medium	Establishment of a competence group within the framework of SHOW (possibly led by UITP in the context of WP14/WP17), which will be			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				issues; COVID-19 effects.	the end of the project.		for satellite non-commercial sites.			also available after the end of the project. Tight coordination of local demo communities.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
12	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 changing policies respectively.	During replication and exploitation phase of the project.	WP17	Potentially all, but also external to SHOW sites willing to rep	57,276	Low	This will be averted by a series of project mechanisms, both technical and operational. Through the interoperability principles and mechanisms of the project (WP4), through specific customised engagement plans of the test sites			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							licate its solutions and lessons learned.			(WP9) as well as through the replication mechanisms that have already started in the project through engagement of network channels of EUROCITIES and the rest of the Partners as well as through the launch of the Open Call for Follower			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										Sites (launched in December 2021).			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
13	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, WP11	Potentially all.	84,315	Medium	Through the standard compliant cybersecurity mechanisms of WP4 that will be assessed through the technical validation of WP11.			
14	Characteristics of each Pilot site must be critically reviewed in	Demonstration /Evaluation	Incosistency in results.	Incosistent evaluation framework and	During the first period of the project while the	WP9	Potentiall	44,4	Low	Tight monitoring of the WP9 evaluation task force;			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
	advance in order to ensure results compatibility.			experimental plans.	evaluation framework and experimental plans are being prepared and updated.		y all.			carefull planning in terms of D9.1, D9.2 and D9.3.			
15	Lack of data shared and info exchange between different Partners in the value chain but also from each local	Operational	Limited impact and value added proven. Also, jeopardising the integration of the	Not well advanced and tight local ecosystems and business models. Conflict of interests between	During the technical validation phase and, more evidently, during the preparation of the pre-	WP2, WP5, WP9, WP11, WP12	Potentially all.	67,8405	Medium	Pre-agreed data exchange in the context of WP5 and mapping to project KPIs. Specific mechanisms established for the data	Carinthia site; SUARA & NAVYA, WP11	There is an issue of sharing data between NAVYA and the	Discussions with NAVYA and Carinthia to solve the specific issue

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
	ecosystem to SHOW, in the context of pilot field trials, may prohibit integrated shared mobility services and valuable impact assessment		planned automated services in the current PT paradigm (on site level).	stakeholders. Financial reasons. Unwilllingness to share data.	demonstration phase.					sharing. Tight daily (literally) monitoring of the process. Revision and strengthening of business and operational models on test site level that will allow the smooth collaboration between different stakeholders.		Carinthia site in specific (due to the different models and agreements followed in other test sites, this is not valid for other	arisen. Minimum data sharing has been requested in the context of the data management platform of WP5 in order to ensure the fulfillment of the basic

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
												sites). So far, no other similar issues have been recognised.	KPIs of the project. Iterative daily collaboration with all sites to address ad hoc all data sharing issues.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
16	Non compatible operation plans of mixed passenger cargo UC's.	Operational	Failure to fully demonstrate the specific Use Cases.	Technical and operational difficulties. Low interest on behalf of the City.	During pre-demonstration phase planning (for the first time).	WP9, WP11, WP12	Carinthia, Karlsruhe	50,54	Low	A specific task force, under the leadership of CTL, has been formulated to oversee all the cargo related plans across the sites. The best possible and most viable solutions from the operational and business point of view are being			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										configured for each site. In the worst case, in the sites that mixed transport is planned, the ability to combine it will be demonstrated and, if nothing more is possible, for the everyday operation the mixed case will be decoupled and the			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										common vehicle will be used either for passenger or for cargo transportation, at different timeframes of the Pilot.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
17	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 (in first place).	WP11, WP12	Karlsruhe, Madrid, Brainport, Trikala (more may come de pe	64,124	Low	The ability of this functionality will be demonstrated; even if used not frequently/ regularly at everyday operations during the Pilot. Traffic demand is definitely an aspect that the project cannot control.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							ndi ng on the am en dm ent s un der rev isio n)						
18	Contradicting needs and	Behavioural	No serious	Alternative strategies		WP7	Pot ent	64,35	Low	Different ones			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
	wants of AV's HMI between different vendors and Pilot sites.	Operational	risk - there is room for alternative strategies among different vendors.	among vendors.	During development phase.		iall y all.			(multivendor approach) 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			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										vendor/site to follow its own "look and feel".			
19	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.	58,432	Low	Several alternative and complementary algorithms for services will be employed within WP5 to be offered to the test sites. The AI services to be			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										offered through WP5 are not blocking any operation; they are value added services provided on top of the existing planned services in each test site.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
20	Operators of PT at Pilot sites not ready to apply safely and efficiently the new AV-based operational schemes.	Operational	Unsuccessful or no demonstration of planned use cases and selected business and operational models.	Lack of awareness and skills required. Change in priorities. Unexpected changes in sites local ecosystem structure. Several reasons (bureuocratic, operational, etc.) for delay.	During pre-demonstration phase (in first place).	WP11, WP15	Potentially all.	72	Medium	To be resolved through tight monitoring of the test sites plans (WP9), the demo sites communities (WP11, WP12) and appropriate training sessions (WP15).			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
21	Not enough or compatible data from previous research to develop AI algorithms and/or train simulation tools.	Technical	No enhanced services emerging as an outcome of SHOW.	Actual data missing (due to insufficient recording mechanisms, etc.) and/or unwillingness to share them.	During development phase.	WP5, WP10	Potentially all.	71,76	Medium	The relevant activities (WP5 and W10) will use pre-Pilot data (from 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;			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										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.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
22	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 (in first place).	WP5, WP6	Potentially all.	25,875	Low	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 WP5 and WP6). That is			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										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.			
23	Sentiment analysis (of A1.2) not possible to be legally	Legal/Regulatory	Not the broadest possible impact that	IPR.	During the actual use of the tools from the first period	WP1	Not applicable.	18	Low	To be performed in project's own social media.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
	performed in third party social media.		could be achieved.		of the project.								
24	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.	50,653	Low	Partially covered through A7.4 HMI adaptability and personalisation.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
25	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	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).	WP5	All	76,23	Medium	A unified data registry has been constructed in WP5 to support data sharing, 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			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
			assessment).							problems are emerging.			
26	Lack of consumer protection.	Legal/Regulatory	Low participation in trials and user acceptance - complaints and problems in field trials execution.	Unclear or insuffiently communicated data privacy policy.	During pre-demonstration phase (in first place).	WP3, WP9, WP11, WP12	Potentially all	67,08	Medium	Specific data privacy and ethics policy and evaluation protocols defined in the project to be applied by all sites.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
27	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-	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-	Before the approval of the final version of the technical validation framework.	WP11	Not yet known which ones.	55,44	Low	Strong involvement of all the pilot sites in preparation and revision of the validation framework, iterative peer-review; pursuing at a common but still parametric framework able to cover all site specific aspects.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
			pilot/pilot phase.	specific aspects.									
28	Exceeding the capacity of JRC to test the vehicles during technical validation phase.	Operational	Delays in or incomplete vehicle technical validation.	The capacity of JRC for testing vehicles is limited by the available infrastructure and timeslots. In case of multiple requests to	The risk to be detected during the technical validation phase (A11.2)	WP11	JRC; test sites	33,6	Low	Tight monitoring and scheduling of technical validation. Keeping a buffer timeslot for emergency cases, e.g. when some extra testing is needed.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				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.						Providing a clear list of available tests and infrastructure by JRC. Obliging the partners to "book" in time JRC for testing.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
29	Covid-19 related cross-cutting effects.	Operational	Delays in vehicle procurements and type approvals, permit processes, development and validation phases' execution. Changes in demo	Mobility restrictions due to COVID affect technical work on field as well as the actual operation. Passengers engagement is also prohibited. Working routines, development and permit	Monitored continuously, depending on the evolution of pandemic situation and related restrictions.	WP11, WP12	Potentially all.	228,532	HIGH	Continuous tight monitoring and mitigation solutions ad hoc and depending the specific local challenges. JRC site may serve as a back-up site for pre-demo activities. If all those fail and depending the size and duration of the	Several sites have acknowledged multiple types of problems.	Covid-19 has caused challenges in vehicle procurement. The expenses and costs of CAV's are higher than	Intensification of communication efforts and engagement strategies. Rescheduling of planned itineraries to make them denser. Intensification of local

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
			sites creating further delays. Economic crisis affecting demo sites resulting in even more further delays. Constraints regarding transport of passengers	processes may be delayed not only due to the general delay in processes but also due to the change of priorities. Local takeholders to be involved also affected making challenging the operation						pandemic, short extension of the project duration will be considered.		expected. In a lot of cases, Covid-19 has delayed considerably the actions and measures to be taken. ALso, due to Covid meas	ecosystem efforts for eliminating as much as possible the delays.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
			(allowed number of passengers). Finally, delay in the start of pre-demo and final demo phase.	of real life scenarios. Operation routines of scheduled trials inevitably affected as well.								ures the amount of passengers allowed on the shuttles have to be reduced in all European countries, which puts in dange	

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
												r the fulfillment of the initial commitment and target regarding transport of passengers and cargo.	

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
30	Misunderstandings due to lack of common vision, definitions and terminology.	Behavioural	Inefficient team work resulting in delays and insufficient results.	Failure to reach a common understanding in the project.	Continuous.	All.	All.	47,652	Low	Regular technical (virtual) meetings at all levels, daily monitoring and technical management constantly creating and maintaining liaisons and synergies, several management mechanisms applied.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
31	Accidents/ Incidents during field trials.	Demonstration /Evaluation	Negatively affecting the full operation of the site in all possible layers at which such events will occur as well as its future evolution.	Unforeseen critically safety events.	During pre-demo phase.	WP11	Potentially all.	62,604	Low	Robust and as complete as possible technical 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. Safety	Three incidents have been recorded in Linköping pre-demo phase trials (WP11), as reported by VTI, one of which is not related to the AV function. The other two were associated to hard braking events of the shuttles.		Direct acknowledgement and reporting to the vehicle provider; recording for optimisation in view of the next iteration.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
										analyses performed. Pre-demo conducted in purpose with internal to the project entities participants. Optimisation round following the pre-demo and before final demo to eliminate as much as possible such events occurence.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
32	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 and/or dropping some of the planned Use Cases.	Lack of cooperation from the authorities or change of their local plans, infrastructure along the route not operational; Limited financial resources available.	Continuous monitoring of the test site plans since the very beginning of the project.	WP11, WP12	Potentially all.	62,475	Low	Seek for alternative test routes. Smarter utilisation of infrastructure equipment and/or use of alternative technologies. In the case of Mega Sites, shift some Use Cases to other sites of the Mega Site.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
33	Insufficient numbers of safety operators recruited.	Demonstration /Evaluation	Delay in the start of pre-demo and/or demonstration phases or shortened pre-demo and/or demonstration phases.	Limited financial and time resources available. COVID related effects.	Continuous monitoring and recruitment process since the very beginning of the project.	WP11, WP12	Potentially all.	52,164	Low	Early awareness and engagement campaigns in each site to recruit safety operators (among other; such as passengers).			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
34	The target duration of demonstration/evaluation phases cannot be reached.	Demonstration /Evaluation	The targets of the GA concerning transport of passengers and cargo cannot be met.	Shuttles are only available for a shorter period than planned, test permit is issued for a narrower time period, weather conditions do not allow for continuous testing, financial resources	Continous monitoring; first evidence since the first year of the project.	WP11, WP12	Potentially all.	121,8	Medium	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).		Several sites have acknowledged such a risk. Still, the exact deviation will be evident in the context of D9.3, begin	All possible efforts are being made from all possible ends in order to eliminate the risk as much as possible.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				are not enough for longer testing, COVID-19 related effects.								ning of 2022.	

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
35	Insufficient localization on the test route.	Technical	High degree of localization uncertainty is expected to be potentially creating safety risks and services insufficient operation.	Poor GNSS-RTK localization.	To be detected throughout the technical validation phase, before starting the actual field trials and apply corrective actions in time.	WP11, WP12	Austrian site; potentially all.	52,038	Low	Adaptation of the used method; exploration of other possible localisation methods exploiting the cooperative context; optimisation of the placement of GNSS antennas.	Gothenburg	Planned routes could not be run in auto-mode.	Changed place of antennas and used combined transmitters.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
36	Insufficient 4G coverage on the test route.	Technical	High degree of localization uncertainty is expected to be potentially creating safety risks and services insufficient operation.	Poor 4G coverage.	To be detected throughout the technical validation phase, before starting the actual field trials and apply corrective actions in time.	WP11, WP12	Potentially all.	37,26	Low	Identification of factors that lead to poor 4G coverage and in-time technical mitigation.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
37	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.	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 or evolving national	Since the first year of the project when the permit processes have started.	WP3, WP11, WP12	Copenhagen, Turin & Graz sites.	110,166	Medium	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.	MOVIA (Copengagen site), LINKS (Turin site) and VIF (Graz site)	In Copengagen the usual process is very long and cumbersome. In Turin, the current legislation does not	Continuous attempts on site level, in each case, to tackle with the national peculiarities in order to override the difficulties. In some cases (i.e. Graz),

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				regulations.								cover SHOW plans; thus an exemption has been asked. In Graz, there is a gap for passenger Avs and as such a	the legislation was put under revision in order to allow the SHOW planned field trials and in another case (Turin), due to the very binding regulation that

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
												new legislation text is on-going to be released in early 2022.	cannot change overall, a specific permit to carry out an experiment by derogation, justified by the importance of testing innovative solutions, has been

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
													granted to the Turin site of SHOW.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
38	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	COVID-19 related effects in combination with ineffective awareness and engagement strategies in local sites.	During the first months of the final demo phase.	WP9, WP12	Potentially all.	78,4125	Medium	Effective awareness and engagement campaigns. More intense engagement of fewer users as a back-up plan. Recruitment of users from the extended SHOW Consortium.			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
			significant.										

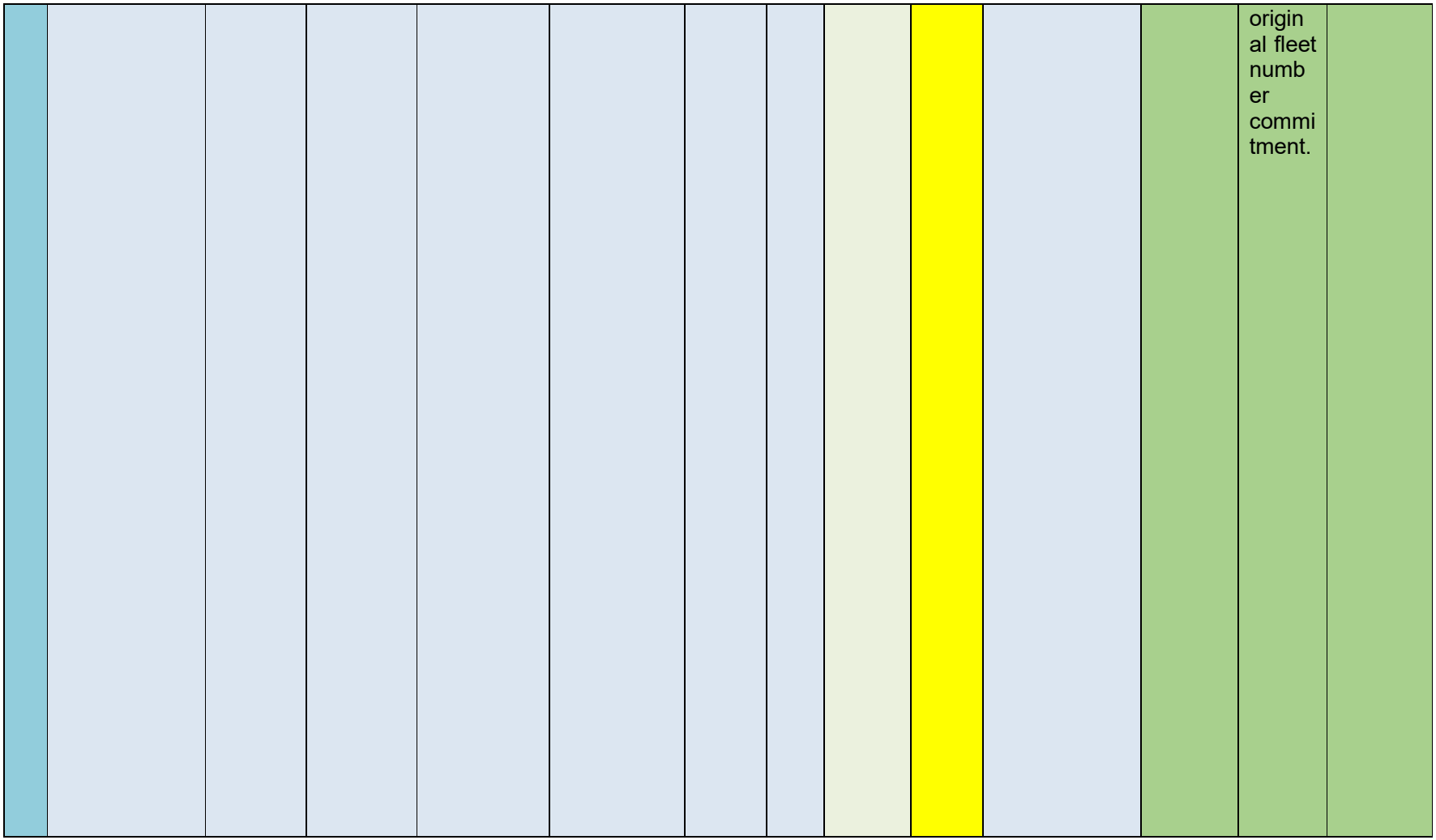
39	Critical changes in vehicles or demo sites plans - unavailability of vehicles, cities segments, etc.	Demonstration /Evaluation	Risk of need to change a part of the pilot or totally replace it.	COVID-19 related effects (related also to financial crisis) mainly.	Continuous monitoring since the very beginning of the project through numerous technical management mechanisms.	WP11, WP12	Eindhoven/Brainport; Copenhagen site; Aachen site; Rennes site; Turin site	108,054	Medium	Recognition of mitigation actions ad-hoc depending the case. On-going amendment processes to tackle with each issue separately. At the time of writing, the replacement of Aachen and the tackling of issues related to the Brainport operations seem to be the most challenging cases, as for the rest of the cases, solutions have been proposed and are subject to	Eindhoven/Brainport; Copenhagen site; Aachen site; Rennes site; Turin site	In Turin, Luxoft, being one of the OEMs (responsible for delivering 1 of the 2 vehicles foreseen for the Turin site) withdrew from the SHOW project, due to the inability of	In Turin, the risk was mitigating by the replacement of the former Luxoft vehicle by a shuttle to be provided by another provider of the project. The request is under revision by the PO. For Copenhagen, in case no viable solution

										acceptance by the PO and formal GA amendment.		developing the vehicle on time. Brainport is having difficulties in addressing the real life operation as expected by the rest of the test sites due to the lack of a complete ecosy	is identified very soon, a replacement has been already identified to be proposed to the PO. Rennes site replacement by another site in France is close to be finalised. Brainport and Aachen cases are still under

												stem and, mainly, due to the lack of the bus provider. In Aachen, the withdrawal of eGo and ASEAG has resulted in the need for the replacement of Aachen site and the identification	exploration.

												- together with the new site - of a new AV provider. In the case of Copenhagen, the available funds in combination with the challenging bureaucracy are turning the	

												fulfillment of the original commitment very challenging. Rennes site replacement was urged due to change of plans by the area in combination with the inability of KEOLIS to fulfill the	


original fleet number commitment.

40	Gap/Undergoing revisions in the national legislation for SHOW targeted use cases.	Legal/Regulatory	Test permit (risk #38) cannot be prepared, because the corresponding law text for CAVs in urban areasas planned in SHOW is not yet available or is not fully covering SHOW plans.	In some cases, the Ministries have not approved the original permit request. Specific precautions to address the SHOW use cases need to be reflected in the law. For example, the Austrian ministry did not approve original permit request for Graz as the available legislation was not	Rejection or acknowledment of possible revision of original permit requests, when those were done (for the specific sites).	WP3, WP11, WP12	Graz site in Austria, Madrid site, Turin site	161,9415	Medium	Communication with contact points (ongoing). The involvement of key stakeholders in the local sites ecosystem (e.g. AUSTRIATECH, EMT, etc.) is expected to speed up with the resolution of those matters.	Graz site, Madrid site, Turin site	Worst case would be that pilot cannot be performed in the manner it was planned because of missing law. In Graz, the Austrian Partners have contributed to the new law	In Austria, the involved Partners, under the auspices of AUSTRIATECH, have resubmitted the application permits, creating a safety analysis that covers all potential problems along the area. They have also

				addressing at the time passenger AVs circulation (that are planned in Graz) in urban areas. In another way around, there are some cases (i.e. in Madrid), that the relevant regulation is undergoing revisions and the new one is possible to affect the SHOW plans in the area.							text to ensure that all planned operation will move without problems, as soon as the permit will be provided. In Madrid, there are no problems encountered so far. However, the	contributed to new legal texts to close the legal gap. In Madrid, there is a on-going tight follow up with lobbying spanish stakeholders in order to ensure that planned revisions will not affect negatively SHOW plans.

												National Traffic Authority is planning to modify the current regulation on AV, which may affect the project (unsure yet). In Turin, the Italian legal requirements were not in line	In Turin, there is a decree regulating the circulation of automated vehicles in Italy, but it was not mature enough to consider the case proposed by the Turin pilot. In order to proceed with the authorisation to circulate, it was therefor

												with what was proposed in the SHOW field trials in the area; still with the exemption provided (see next column), any relevant risk has been lowered.	e necessary to ask the Ministry to make an exception to the legislation in force, in particular with regard to certain regulatory elements blocking the experiment. Discussions for Aachen and Brainport are

													on-going.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
41	Worldwide chip and component shortage may impact SHOW pilots.	Technical	Significant delays possible	Specific electronic components like V2X chips, GPUs, automotive semiconductors have delivery times up to one year due to international shortages and hoarding of component	The chip crisis became more visible on the markets at the beginning of 2021 and is accelerating.	WP7, WP8, WP11, WP12	Potentiall all, as it previously touches upon the supplying ve	136,4	Medium	Earlier requiry for h/w and s/w components from the suppliers. Purchase components in stock. Consideration of backup plan with different components or components utilised by affiliated entities and projects	Graz site, Madrid site	Delivery of some components for the automatization of vehicles are delayed affecting inevitably the development /	As already mentioned. In Madrid for example, the pending components are currently being borrowed by a research institute which coopera

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				s in the market			ndors, but more specifically it has been so far reported by Graz			(whenever possible).		integration process, especially in research based sites.	tes with EMT.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							site in Austria and Madrid site in Spain.						
42	Software problems on the vehicle.	Technical	Pause of operation.	Software problems/ malfunctions of	Experiencing the problems in real life	WP11, WP12	Potentially, tima	90,72	Medium	Continuous exchange with OEM and supervision.	Carinthia, Madrid site, Brainp	Encountered several types	Continuous exchange with OEMs;

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				several types.	pre-demo phase.		y be applicable for all sites, but, so far, it has been reported by			Optimisation or full replacement for final demo phase.	ort site, Turin site, Gothenburg, Turin sites	of problems during operation.	Replacement of vehicles, if needed.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							Carinthia, Madrid site, Braincport site, Turin and Gothenburg						

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							test sites and, also, as a high potenial for Graz test						

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							site.						
43	Adverse weather conditions jeopardising the operation.	Operational	Delays in field trials and mainly not seamless operation as planned.	Cold temperatures, affecting batteries. Snow and heavy rain are changing the environment and the lidars are having problems	Experiencing the problems in real life pre-demo phase.	WP11, WP12	Gothenburg (Sweden), Tampere (Finland) and Turin (Italy) sites	72,9	Medium	Identifying in the pre-demo phase which are the safe conditions boundaries that Avs can operate without problems. Optimising as much as possible vehicles technology	Gothenburg (Sweden), Tampere (Finland) and Turin (Italy) sites	Running of Avs under heavy rain, snow or temperatures around - 10-25 degre	Avoid adverse weather conditions in cases that safety is jeorpadised; pursue the maximum possible

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				to detect the route.			d Turin (Italy) sites. It has been reported also as a high potent			on the basis of the pre-demo phase outcomes.		es C is creating a series of technical problems, most of which cannot be overridden through the current vehicle	optimisation of vehicles' technology to tackle with such issues.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							ial for the future trials in Graz site in Austria.					technology in place.	
44	Wrongly parked vehicles during field trials	Operational	Cannot run in auto mode	Inappropriate parked vehicles along the	Experiencing the problems in real life	WP11, WP12	This is highly ap	54,096	Low	Plan for routes with margin from the parking lots. Manual	Gothenburg site	Parked cars along the route	Replan routes with margin from the

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
				route of AVs.	pre-demo phase		plicable to all test sites.			overtaking for specific parts of the route.		of the AV necessitating manual overtaking.	parking lots.
45	Spare parts for AVs not at hand	Operational	Cannot run a vehicle needing spare parts	Lacking of spare parts by OEM	Spareparts not continuously at stock at the warehouse.	WP11, WP12	This is highly applicable to all tes	114,68	Medium	Communication and continuous exchange with OEMs.	Gothenburg site	Could not run the broken vehicle.	Make a spare part plan with OEM (lesson learned for next phase).

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	(So far) materialisation		
											Pilot site/ Partner/ WP	Description of problem/ challenge	Taken/ planned Mitigation Measure(s)
							t sites.						