SHared automation Operating models for Worldwide adoption

SHOW

Grant Agreement Number: 875530

D4.4: Open modular system architecture – third 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

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

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

Concluding the work started and progressing with D4.1, D4.2 and D4.3, in the current deliverable, the last issue of this series of Deliverables, we present the WP4 final updates. This year's updates included work by both WP4 teams on cybersecurity, connectivity, interoperability and SHOW data pipeline testing with sites as well as work performed by all local site technical teams in setting up their final technology ecosystem setup. The focus of this document is on presenting any updates with respect to the SHOW Mobility Data platform tools and updates or refinements of the local architecture solutions with respect to the previous version of the architecture deliverable, i.e. D4.3.

The following (twelve) active SHOW test sites are included in this reporting: Linköping, Gothenburg, Madrid, Graz, Salzburg, Carinthia, Karlsruhe (the other two German sites Monheim and Frankfurt are not yet formally integrated and thus not reported here), Tampere (Hervanta), Turin, Trikala, Brno and Brainport. Addiditonally, one new functional architecture for a French newcomer site expected to partially replacing Rouen, namely Les Mureaux site is also described.

Highlighting the results of WP4, lessons learnt from the reference architecture instantiation in each test site focusing on interoperability and cybersecurity aspects are included as part of Chapters five and six which are dedicated to the work conducted by the WP4 team. Additional WP4 work not directly related with SHOW reference architecture is hosted in Appendixes I and II while section 5.4 and Appendix III hosts a comparison with AVENUE project in the field of cybersecurity practices.

Finally, the findings of the third and final round of the risk assessment performed in the context of Activity A4.6 are provided in Chapter 7 (along with Appendix IV).

Document Control Sheet

Start date of project:	01 January 2020
Duration:	48 months
SHOW Del. ID & Title:	D4.3: Open modular system architecture- third 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), Nicolas Morael, Edgar Zanelato Contier (Transdev), Georgios Spanos, Evangelos Antypas, Alexandros Papadopoulos, Athanasios Sersemis, Iordanis Papoutsoglou, Konstantinos Giapantzis, Antonios Lalas (CERTH/ITI), Maria Gkemou, Matina Loukea (CERTH/HIT), Nico Lambing (FZI), Petra Schoiswohl (SURAAA), Markus Karnutsch (Salzburg Research), Tor Skoglund, Thanh Bui (RI.SE), Lucia Isasi, Ray Lattarulo (TECNALIA), Timo Mustonen (Sensible4), Pekka Eloranta (Sitowise), Jansen, S.T.H. (TNO), Anna Antonakopoulou (ICCS), Ioannis Gragopoulos (CERTH), Marek Vanzura (Brno), Katharina Karnahl (DLR)
Internal Reviewers:	Maria Gkemou – CERTH/HIT
External Reviewers:	N/A
Actual submission date:	01/03/2023
Status:	Final
File Name:	SHOW_D4.4_Open modular system architecture – third version_Final

Document Revision History

Version	Date	Reason	Editor
0.1	23/11/2022	ToC circulated by ICCS to WP4 and Demo sites	A. Bolovinou (ICCS)
0.2	23/12/2022	Integration of sites inputs	A. Bolovinou (ICCS)
0.3	23/01/2022	Integration of sites inputs	A. Bolovinou (ICCS)
1.0	27/02/2023	All contents integrated. Stable version sent for peer review	A. Bolovinou (ICCS)
2.0	01/03/2023	Final version, addressing peer review comments	A. Bolovinou (ICCS)

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
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
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
TMC	Traffic management centre
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)

Abbreviation	Definition
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 are the following:

a. To provide a reference architecture final updated diagram and its mapping to involved stakeholders for external audience (chapter 2).
b. To present the local sites architecture updates including the design of local Dashboard when applicable: this part is covered by chapter 4 applying the template proposed in chapter 3.
c. To present the cybersecurity tools specifications and deployment covering any updates with respect to SHOW deliverable D4.1 [1], D5.1 [2] and D4.3 [3]: this part, that also includes lessons learnt is covered by chapter 5 and Appendix II and Appendix III.
d. To present any updates on the SHOW interoperability mechanisms and lessons learnt: this part is covered by chapter 6.
e. To present the last risk assessment findings: this part is covered by chapter 7 and App. IV.
f. To present the research work performed as part of Activity A4.2 on V2X urban surfaces, please see Appendix I.

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 the near-future CCAM/PT landscape.

1.3 Interrelations within the project

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.

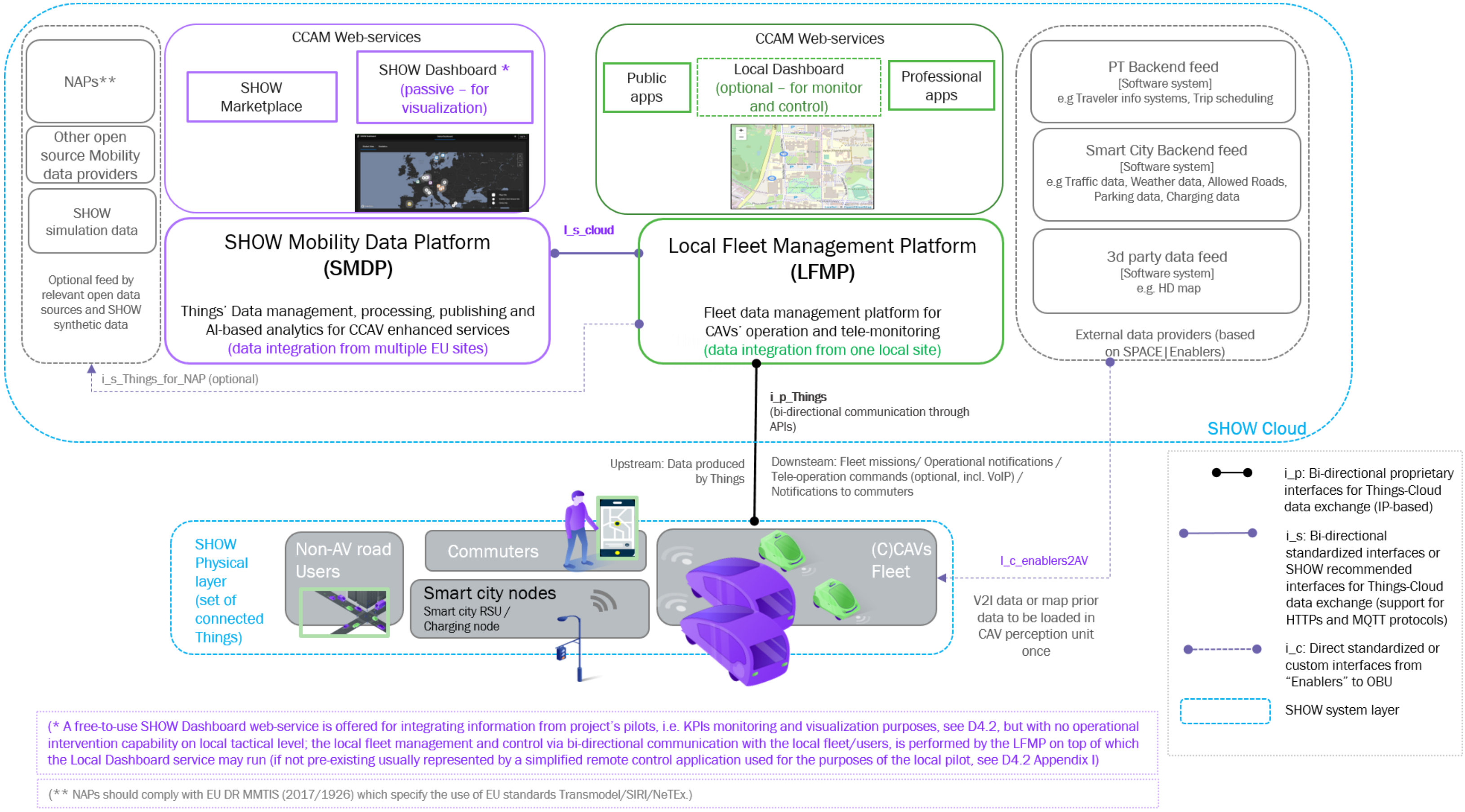
2 Recap as of D4.3

This year's updates included work by both WP4 teams on cybersecurity, connectivity, interoperability and SHOW data pipeline testing with sites as well as work performed by all local site technical teams in setting up their final technology ecosystem setup. More specifically, work items updated with respect to previous version of the architecture deliverable, D4.3 include:

- Updates in the local functional architecture of the following SHOW sites, namely: : Linköping, Gothenburg, Madrid, Graz, Salzburg, Carinthia, Karlsruhe (the other two german sites Monheim and Frankfurt are not yet integrated and thus not reported here), Tampere (Hervanta), Turin, Trikala, Brno and Brainport
  - New functional architecture for a newcomer sites (France/Les Mureaux site replacing former Rouen site)
  - Should be stressed that **only updated parts as of D4.3**, are provided in the current Del. If nothing has changed, D4.3 should serve as the reference.
- Updates on cybersecurity mechanisms in three directions: i) Network-based IDS development (and its deployment in SHOW DMP and in the local site of Madrid), ii) ML framework to enable explainable IDS and iii) generic cybersecurity and data-privacy framework.
- Updates on SHOW data interoperability mechanisms and lessons learnt.
- New research work on intelligent surfaces as an urban 6G applications enabler, as part of wp4-A4.2 (placed in App. I as it is not related with the SHOW reference architecture).
- Update of the Risk assessment report.

2.1 Mapping SHOW reference architecture to types of involved stakeholders

Based on the layers component-based SHOW reference architecture depicted in Figure 1, a new diagram is created in Figure 2, where each layer or main component of the proposed architecture is flagged with stakeholders possibly involved for its implementation/support/maintenance. With this alternative reference architecture view, we want to assist any future possible instantiation of the SHOW reference architecture for urban CCAM services deployment within the public transport domain that will essentially involve a set of national or European stakeholders.


CCAM Web-services
SHOW Marketplace
SHOW Dashboard *
(passive – for visualization)
NAPs**
Other open source Mobility data providers
SHOW simulation data
Optional feed by relevant open data sources and SHOW synthetic data
SHOW Mobility Data Platform (SMDP)
Things' Data management, processing, publishing and AI-based analytics for CCAV enhanced services
(data integration from multiple EU sites)
I_s_cloud
i_s_Things_for_NAP (optional)
CCAM Web-services
Public apps
Local Dashboard
(optional – for monitor and control)
Professional apps
Local Fleet Management Platform (LFMP)
Fleet data management platform for CAVs' operation and tele-monitoring
(data integration from one local site)
PT Backend feed
[Software system]
e.g Traveler info systems, Trip scheduling
Smart City Backend feed
[Software system]
e.g Traffic data, Weather data, Allowed Roads, Parking data, Charging data
3d party data feed
[Software system]
e.g. HD map
External data providers (based on SPACE|Enablers)
SHOW Cloud
i_p_Things
(bi-directional communication through APIs)
Upstream: Data produced by Things
Downsteam: Fleet missions/ Operational notifications / Tele-operation commands (optional, incl. VoIP) / Notifications to commuters
SHOW Physical layer (set of connected Things)
Non-AV road Users
Commuters
Smart city nodes
Smart city RSU / Charging node
(C)CAVs Fleet
I_c_enablers2AV
V2I data or map prior data to be loaded in CAV perception unit once
i_p: Bi-directional proprietary interfaces for Things-Cloud data exchange (IP-based)
i_s: Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange (support for HTTPs and MQTT protocols)
i_c: Direct standardized or custom interfaces from “Enablers” to OBU
SHOW system layer

(* A free-to-use SHOW Dashboard web-service is offered for integrating information from project's pilots, i.e. KPIs monitoring and visualization purposes, see D4.2, but with no operational intervention capability on local tactical level; the local fleet management and control via bi-directional communication with the local fleet/users, is performed by the LFMP on top of which the Local Dashboard service may run (if not pre-existing usually represented by a simplified remote control application used for the purposes of the local pilot, see D4.2 Appendix I)

(** NAPs should comply with EU DR MMTIS (2017/1926) which specify the use of EU standards Transmodel/SIRI/NeTEx.)

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

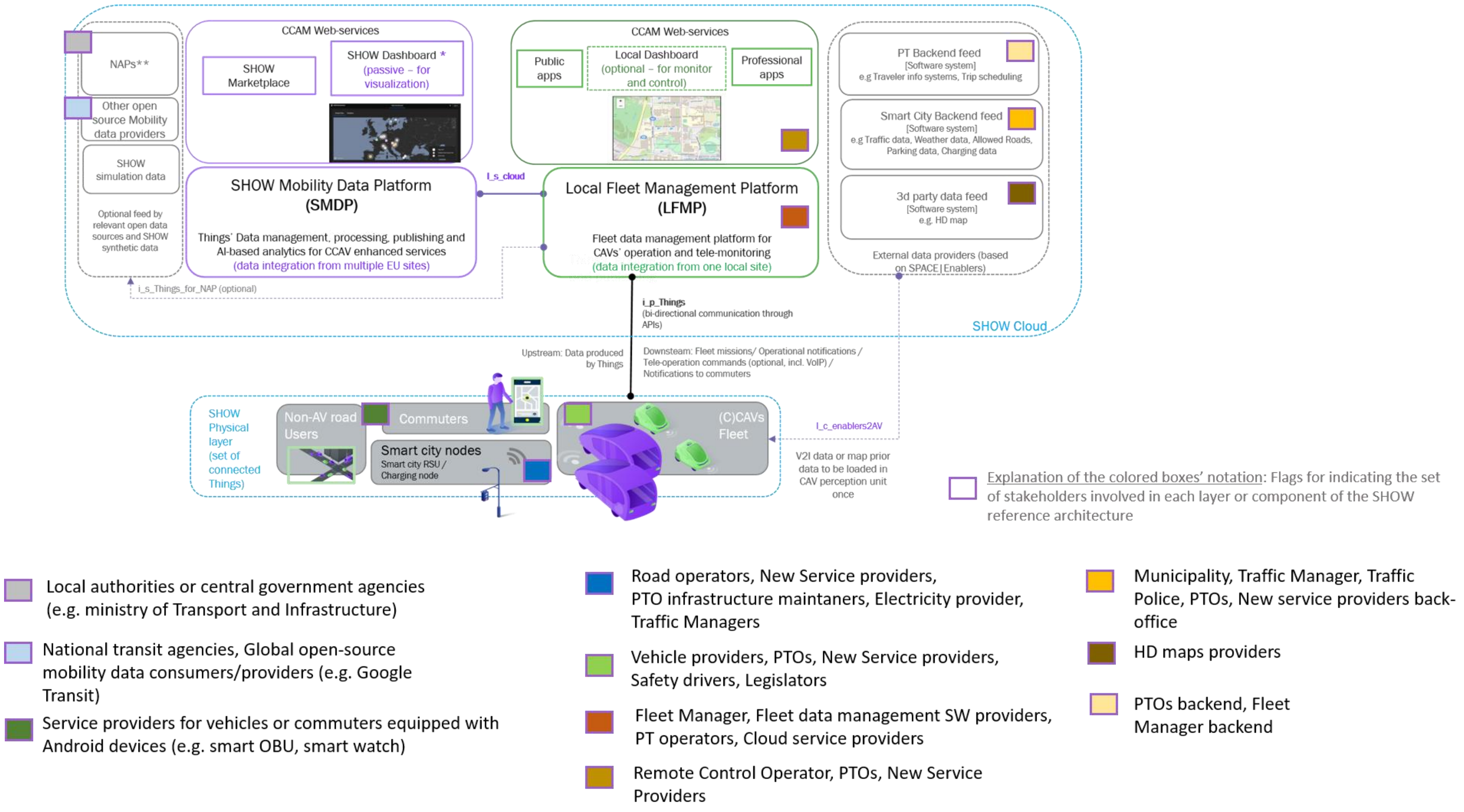

CCAM Web-services
SHOW Marketplace
SHOW Dashboard * (passive – for visualization)
NAPs**
Other open source Mobility data providers
SHOW simulation data
Optional feed by relevant open data sources and SHOW synthetic data
SHOW Mobility Data Platform (SMDP)
Things' Data management, processing, publishing and AI-based analytics for CCAV enhanced services (data integration from multiple EU sites)
I_s_cloud
i_s_Things_for_NAP (optional)
CCAM Web-services
Public apps
Local Dashboard (optional – for monitor and control)
Professional apps
Local Fleet Management Platform (LFMP)
Fleet data management platform for CAVs' operation and tele-monitoring (data integration from one local site)
PT Backend feed [Software system] e.g Traveler info systems, Trip scheduling
Smart City Backend feed [Software system] e.g Traffic data, Weather data, Allowed Roads, Parking data, Charging data
3d party data feed [Software system] e.g. HD map
External data providers (based on SPACE|Enablers)
SHOW Cloud
i_p_Things (bi-directional communication through APIs)
Upstream: Data produced by Things
Downsteam: Fleet missions/ Operational notifications / Tele-operation commands (optional, incl. VoIP) / Notifications to commuters
SHOW Physical layer (set of connected Things)
Non-AV road Users
Commuters
Smart city nodes
Smart city RSU / Charging node
(C)CAVs Fleet
I_c_enablers2AV
V2I data or map prior data to be loaded in CAV perception unit once
Explanation of the colored boxes' notation: Flags for indicating the set of stakeholders involved in each layer or component of the SHOW reference architecture
Local authorities or central government agencies (e.g. ministry of Transport and Infrastructure)
National transit agencies, Global open-source mobility data consumers/providers (e.g. Google Transit)
Service providers for vehicles or commuters equipped with Android devices (e.g. smart OBU, smart watch)
Road operators, New Service providers, PTO infrastructure maintaners, Electricity provider, Traffic Managers
Vehicle providers, PTOs, New Service providers, Safety drivers, Legislators
Fleet Manager, Fleet data management SW providers, PT operators, Cloud service providers
Remote Control Operator, PTOs, New Service Providers
Municipality, Traffic Manager, Traffic Police, PTOs, New service providers back-office
HD maps providers
PTOs backend, Fleet Manager backend

Figure 2: SHOW reference architecture main components mapped to stakeholders (better viewed in zoom-in mode)

3 Local architecture updates description: the template

To facilitate the reporting of each local architecture instantiation, the design adopted by each local site is described using a common template focusing on updates from D4.3. More specifically, filling in the following sub sections has been requested:

3.1 Template for general updates focusing on the LFMP side (diagram + textual description)

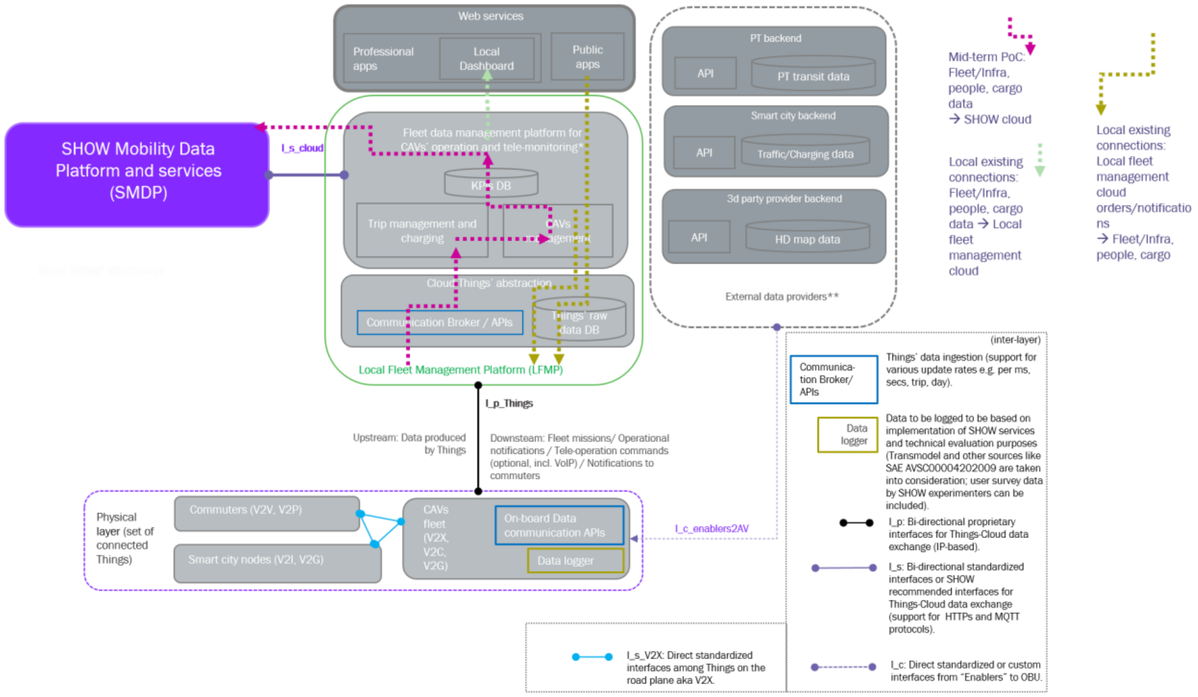

Web services
Professional apps
Local Dashboard
Public apps
SHOW Mobility Data Platform and services (SMDP)
I_s_cloud
Fleet data management platform for CAVs' operation and tele-monitoring*
KPIs DB
Trip management and charging
CAVs management
Cloud Things' abstraction
Communication Broker / APIs
Things' raw data DB
Local Fleet Management Platform (LFMP)
PT backend
API
PT transit data
Smart city backend
API
Traffic/Charging data
3d party provider backend
API
HD map data
External data providers**
Mid-term PoC: Fleet/Infra, people, cargo data → SHOW cloud
Local existing connections: Fleet/Infra, people, cargo data → Local fleet management cloud
Local existing connections: Local fleet management cloud orders/notifications → Fleet/Infra, people, cargo
I_p_Things
Upstream: Data produced by Things
Downsteam: Fleet missions/ Operational notifications / Tele-operation commands (optional, incl. VoIP) / Notifications to commuters
Physical layer (set of connected Things)
Commuters (V2V, V2P)
Smart city nodes (V2I, V2G)
CAVs fleet (V2X, V2C, V2G)
On-board Data communication APIs
Data logger
I_c_enablers2AV
(inter-layer)
Communica-tion Broker/ APIs
Things' data ingestion (support for various update rates e.g. per ms, secs, trip, day).
Data logger
Data to be logged to be based on implementation of SHOW services and technical evaluation purposes (Transmodel and other sources like SAE AVSC00004202009 are taken into consideration; user survey data by SHOW experimenters can be included).
I_p: Bi-directional proprietary interfaces for Things-Cloud data exchange (IP-based).
I_s: Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange (support for HTTPs and MQTT protocols).
I_s_V2X: Direct standardized interfaces among Things on the road plane aka V2X.
I_c: Direct standardized or custom interfaces from "Enablers" to OBU.

Figure 3: SHOW functional architecture and information flows (better viewed in zoom-in mode).

3.2 Template (diagram + textual description) focusing on the LFMP Dashboard/Remote-control centre (if applicable)

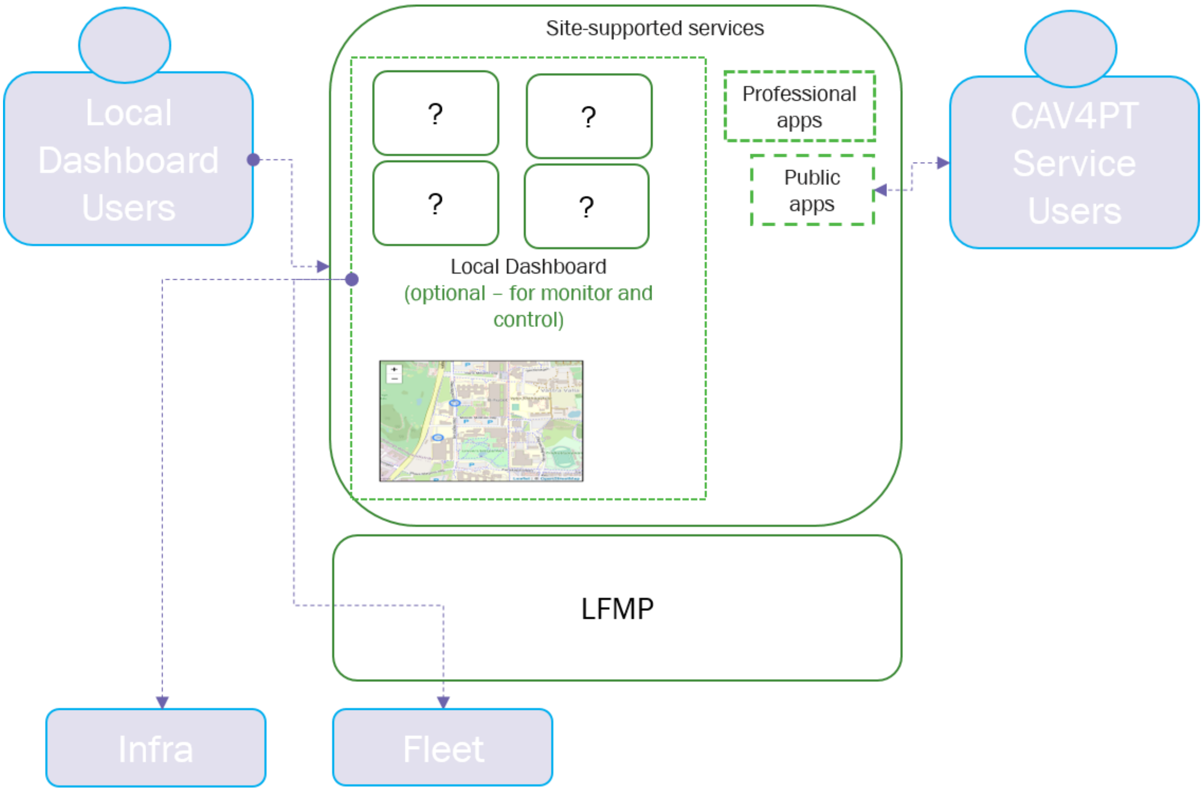


Figure 4: SHOW functional architecture and information flows (better viewed in zoom-in mode)

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.

3.3 Template for CAVs4PT Services information flow updates (diagram + textual description)

Description and detailed diagram of the local services information flow as in the example of Figure 5 focusing on updates from D4.3.

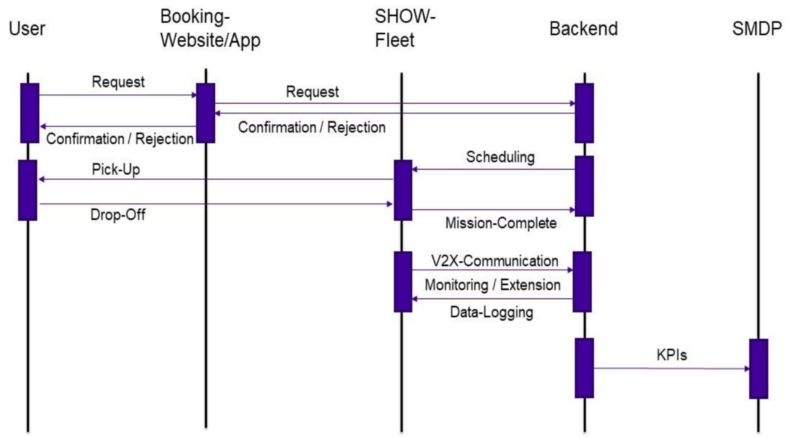


Figure 5: Example of service information flow diagram (UML sequence diagram)

3.4 Template for any updates on 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, will be presented. The information in each sub-chapter is structured in four sub-sections according to the template described in section 3.

4.1 Madrid local architecture

Madrid ecosystem includes Madrid's Local Data Management Platform (MLDMP), Madrid's fleet (a bus, two shuttles and two vehicles) and on-site digital infrastructure (C-ITS node, smart traffic light node). The architecture illustrated below is common for both sites in Madrid; Carabanchel and Villaverde. More details about the internal logical architecture of the MLDMP (technology ecosystem) are provided in Figure 8.

4.1.1 General updates focusing on the LFMP side

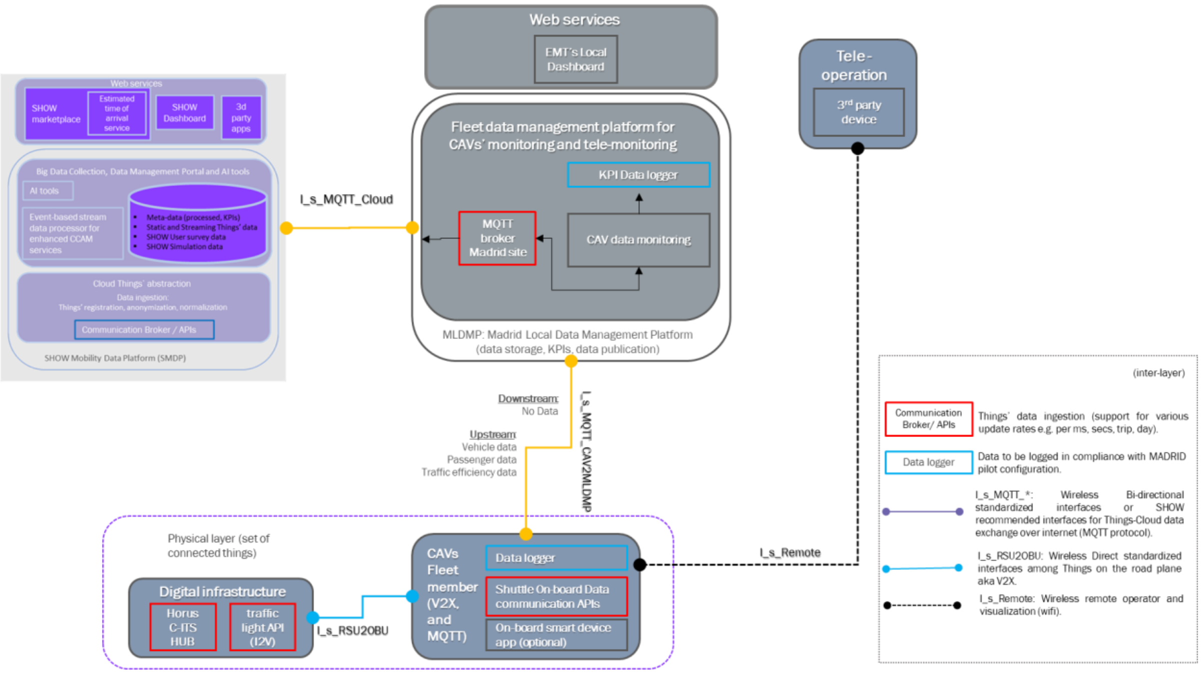

Web services
SHOW marketplace
Estimated time of arrival service
SHOW Dashboard
3d party apps
Big Data Collection, Data Management Portal and AI tools
AI tools
Event-based stream data processor for enhanced CCAM services
Meta-data (processed, KPIs)
Static and Streaming Things' data
SHOW User survey data
SHOW Simulation data
Cloud Things' abstraction
Data ingestion:
Things' registration, anonymization, normalization
Communication Broker / APIs
SHOW Mobility Data Platform (SMDP)
I_s_MQTT_Cloud
Web services
EMT's Local Dashboard
Fleet data management platform for CAVs' monitoring and tele-monitoring
KPI Data logger
MQTT broker Madrid site
CAV data monitoring
MLDMP: Madrid Local Data Management Platform
(data storage, KPIs, data publication)
Tele-operation
3rd party device
Downstream:
No Data
Upstream:
Vehicle data
Passenger data
Traffic efficiency data
I_s_MQTT_CAV2MLDMP
I_s_Remote
Physical layer (set of connected things)
Digital infrastructure
Horus C-ITS HUB
traffic light API (I2V)
I_s_RSU2OBU
CAVs Fleet member (V2X, and MQTT)
Data logger
Shuttle On-board Data communication APIs
On-board smart device app (optional)
(inter-layer)
Communication Broker/ APIs
Things' data ingestion (support for various update rates e.g. per ms, secs, trip, day).
Data logger
Data to be logged in compliance with MADRID pilot configuration.
I_s_MQTT_*: Wireless Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange over internet (MQTT protocol).
I_s_RSU2OBU: Wireless Direct standardized interfaces among Things on the road plane aka V2X.
I_s_Remote: Wireless remote operator and visualization (wifi).

Figure 6: Madrid Mega site: Updated local architecture diagram.

The main changes from Madrid's previous architecture are the removal of the "Remote Stop" emergency button, which was deem unnecessary given that a safety driver must be in the pilot seat for all fleet vehicles as required by regulation. And the simplification of the MLDMP, which removes the "MQTT Client Bridge for Data publishing", which functionality has been integrated into the MQTT broker itself, using the capabilities for bridge already available in the protocol.

4.1.2 Description focusing on the LFMP Dashboard/RC center (if applicable)

The full path of Madrid's CAV data, from the vehicle to the SMDP is visualized in **Figure 7**. The data is logged and uploaded (real time) in MLDMP, and simultaneously streamed to SHOW's DMP (CERTH), where relevant KPIs are calculated online.

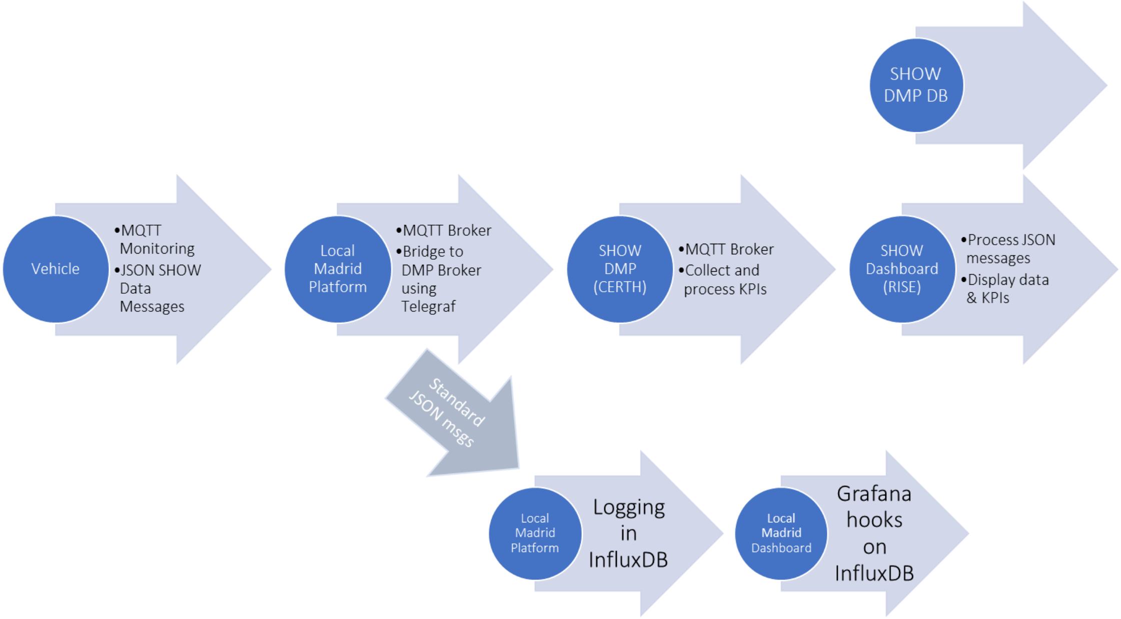


Figure 7: Madrid Mega site: CAV data path representation.

The vehicle data is collected for each vehicle making use of its sensors and the intelligence systems available on board. This data is aggregated into a series of JSON messages, and streamed via MQTT to the Madrid's Local DMP.

Madrid's Local DMP, handles the logging, dashboard and bridges the communication with SHOW's DMP, while also receiving continuous streamed data as shown in Figure 8 . A series of containerized environments are used for each task, an influx database, the mosquito broker itself, a Telegraf handle to capture data into the Influx DB, and Grafana as a Dashboard for monitoring.

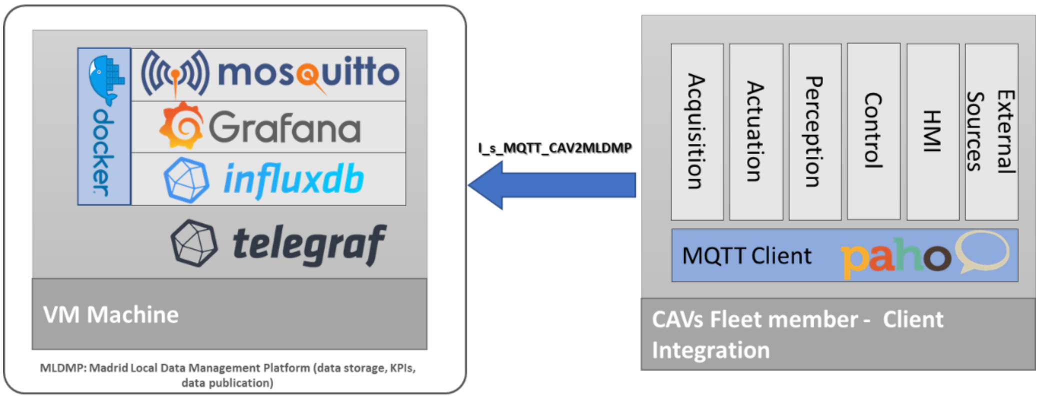


Figure 8: MLDMP logical architecture

4.1.3 CAVs4PT Services information flow (if applicable)

4.1.3.1 Carabanchel Scenario

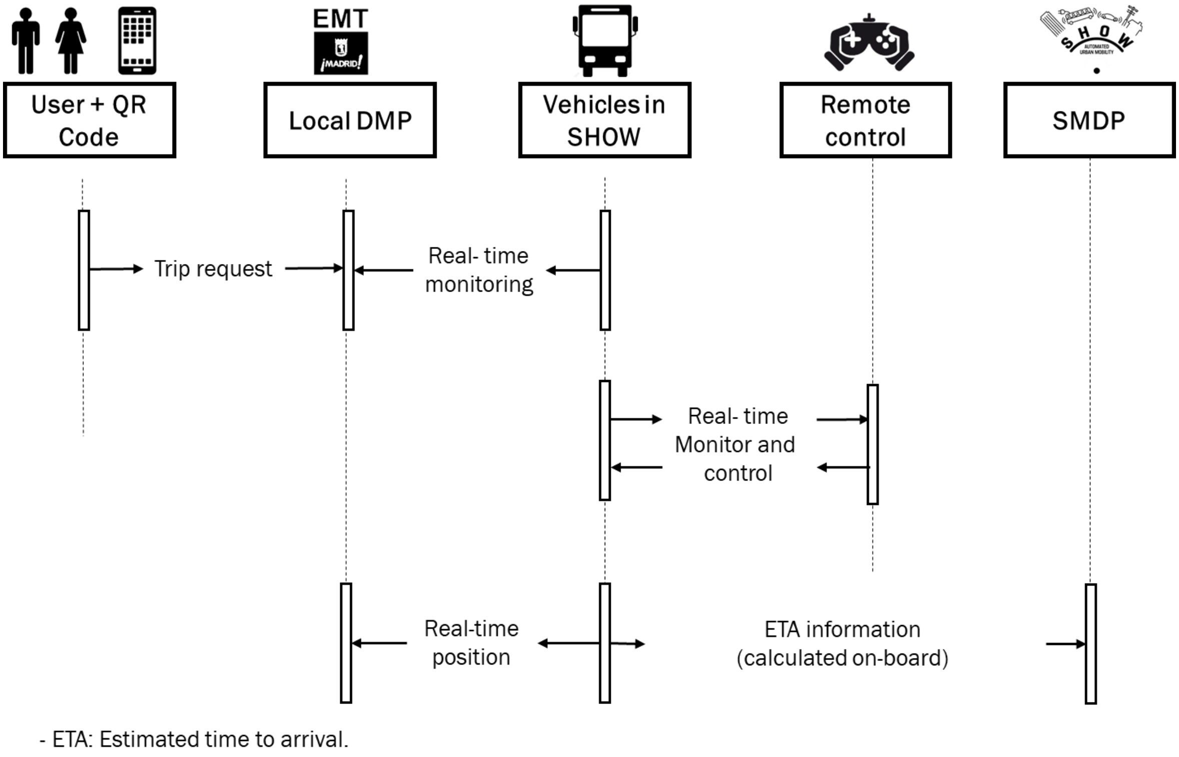


Figure 9: Madrid Mega site: services information flow diagram for Carabanchel Scenario

The local CAV monitoring service as well as user DRT (demand-responsive transit) information flow is presented in **Figure 9**. This service is focused on providing transportation to visitors and employees with access to the Carabanchel depot, and includes the remote teleoperation use case. Data exchange between the services is listed in Table 2 that follows.

Table 1: Local service actors and to/from data exchange summary in Carabanchel.

Local Service title	**Short description**	**Data used (coming from fleet, devices, infra)**
QR Request (User)	Trip request inside in Carabanchel.	User bus stop (location) inside the Carabanchel depot and timeframe.
Local DMP/ Web app	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 in 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	Remote operation of the vehicle	Feed of video perception, and control commands.

Local Service title	Short description	Data used (coming from fleet, devices, infra)
SMDP	KPI calculation and storage. Connectivity to Show Dashboard	Real time data received from Local DMP from all vehicles in Madrid Site.

4.1.3.2 Villaverde Scenario

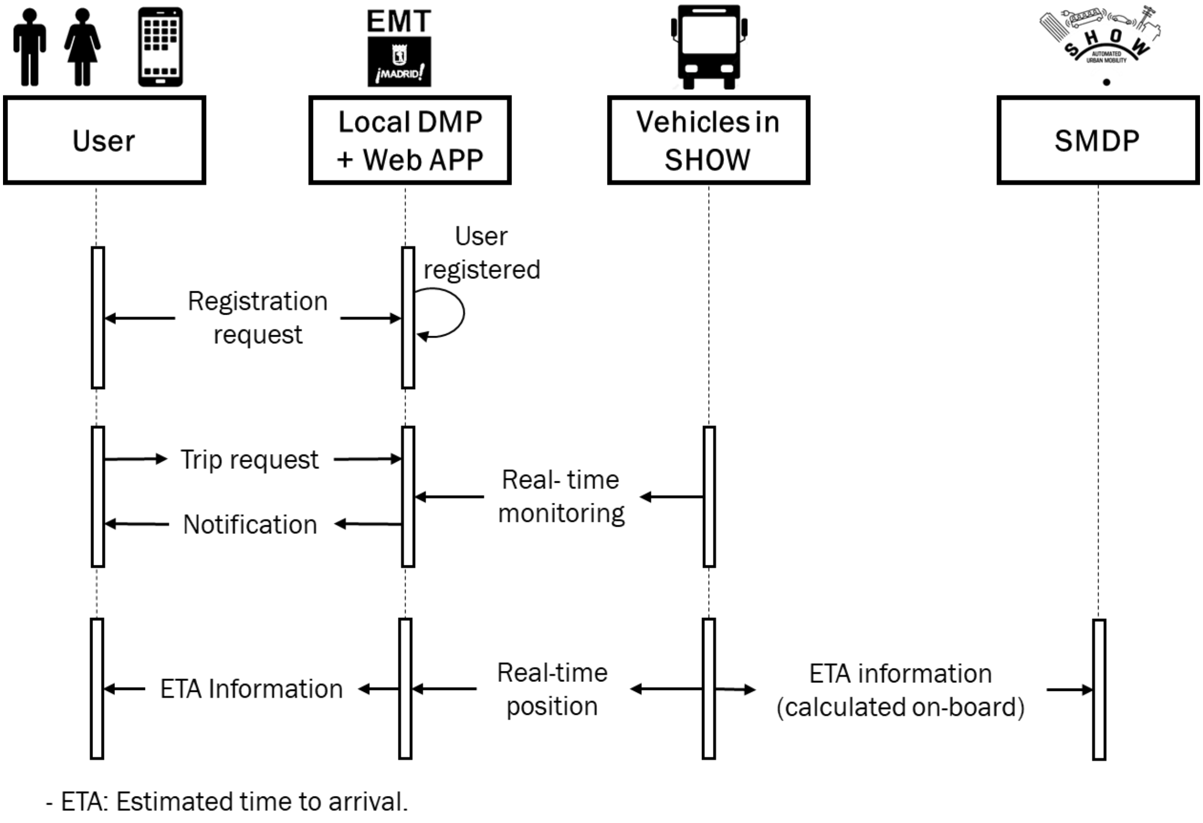


Figure 10: Madrid Mega site: services information flow diagram for Villaverde Scenario

The local CAV monitoring service and user DRT (demand-responsive transit) information flow is presented in Figure 10. This service is focused on providing public transportation in the Villaverde area. Data exchange between the services is listed in Table 2 that follows.

Table 2: Local service actors and to/from data exchange summary in Villaverde

Local Service title	Short description	Data used (coming from fleet, devices, infra)
User app	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	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.

Local Service title	Short description	Data used (coming from fleet, devices, infra)
Vehicles in 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).
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 applicable)

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. Additionally, in collaboration with CERTH-ITI team (leading cybersecurity work within WP4), a cloud-based cybersecurity monitoring solution was integrated and tested for Madrid local cloud DMP, please refer to section 5.1.4.

4.2 Swedish Pilot sites

4.2.1 Linköping local architecture

4.2.1.1 General updates focusing on the LFMP side

The digital infrastructure that was described in D4.3 still applies in Linköping. No major redesigns or updates has been made.

Two updates have been made to the digital infrastructure.

We have added 4G enabled tablets in the busses to enable the safety drivers to manually indicate when passengers step on resp. step off the bus. From the tablet dataset we get positional data on those events.

We have also installed additional IMU and accelerometer sensor on the busses. The original sensors did not have high enough quality and sampling frequency to be able to detect hard breaks in a reliable way.

4.2.1.2 Description focusing on the LFMP Dashboard/RC center (if applicable)

The local dashboard has not implemented any remote-control features. This effort has been stopped by both technical limitation of the vehicles and legal issues. Also, more rudimentary on-demand functionality has not been able to be tested due to limitation of the dynamic route planning capabilities of the vehicles at hand in Linköping.

4.2.1.3 CAVs4PT Services information flow (if applicable)

See previous chapter.

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

Cyber security 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.

4.2.2 Gothenburg local architecture

The architecture has not changed comparing to D4.3, however the diagram has been updated as illustrated in Figure 11 in order to present the data flow with respect to the SHOW reference architecture blueprint.

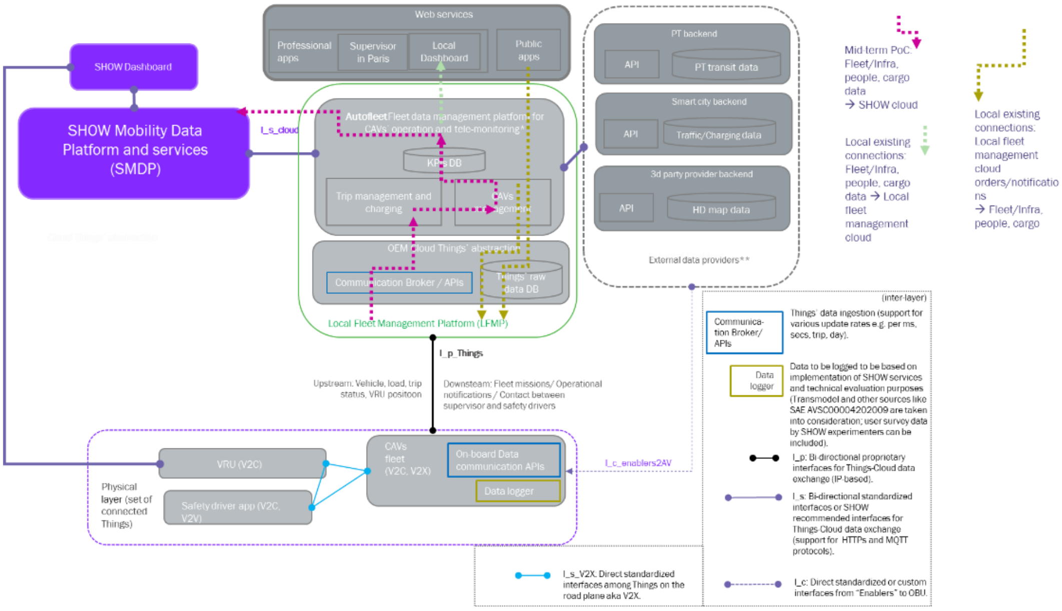

Web services
Professional apps
Supervisor in Paris
Local Dashboard
Public apps
SHOW Dashboard
SHOW Mobility Data Platform and services (SMDP)
I_s_cloud
Autofleet Fleet data management platform for CAVs' operation and tele-monitoring*
KPIs DB
Trip management and charging
CAVs management
OEM Cloud Things' abstraction
Communication Broker / APIs
Things' raw data DB
Local Fleet Management Platform (LFMP)
I_p_Things
Upstream: Vehicle, load, trip status, VRU positoon
Downsteam: Fleet missions/ Operational notifications / Contact between supervisor and safety drivers
PT backend
API
PT transit data
Smart city backend
API
Traffic/Charging data
3d party provider backend
API
HD map data
External data providers**
Mid-term PoC: Fleet/Infra, people, cargo data → SHOW cloud
Local existing connections: Fleet/Infra, people, cargo data → Local fleet management cloud
Local existing connections: Local fleet management cloud orders/notifications → Fleet/Infra, people, cargo
VRU (V2C)
Safety driver app (V2C, V2V)
Physical layer (set of connected Things)
CAVs fleet (V2C, V2X)
On-board Data communication APIs
Data logger
I_c_enablers2AV
(inter-layer)
Communica-tion Broker/ APIs
Things' data ingestion (support for various update rates e.g. per ms, secs, trip, day).
Data logger
Data to be logged to be based on implementation of SHOW services and technical evaluation purposes (Transmodel and other sources like SAE AVSC00004202009 are taken into consideration; user survey data by SHOW experimenters can be included).
I_p: Bi-directional proprietary interfaces for Things-Cloud data exchange (IP-based).
I_s: Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange (support for HTTPs and MQTT protocols).
I_s_V2X: Direct standardized interfaces among Things on the road plane aka V2X.
I_c: Direct standardized or custom interfaces from "Enablers" to OBU.

Figure 11: Gothenburg demo site functional architecture

4.3 France/Les Mureaux site (replaced Rouen-Vernon Mega site)

The Rouen-Vernon France Megasite which included the two sites located in the Normandy region was cancelled due to the Transdev R&D team shut-down in beginning of 2022. The Megasite was replaced by the Navetty project, which is located in the Parisian area, at the ArianeGroup private industrial plant (Les Mureaux, FR).

The Navetty project consists on a mobility service delivered for Ariane Group employees and visitors by up to three EasyMile EZ10 Gen3 shuttles running from 8AM to 7PM. The service is fully autonomous (without any on-board safety operator) since November 2022. By the 2nd semester 2023 a new feature is expected for the project: an on-demand app by which all passengers will be able to book their ride.

The shuttles are real-time monitored by a remote supervision operator using the Supervision system provided also by EasyMile. The system enables tracking of the correct functioning of vehicle, mission management, passenger assistance and remote interventions. The previous architecture is also replaced by a new one, as seen here below in Figure 12. The actors' roles and connectivity profile are described in Table 3.

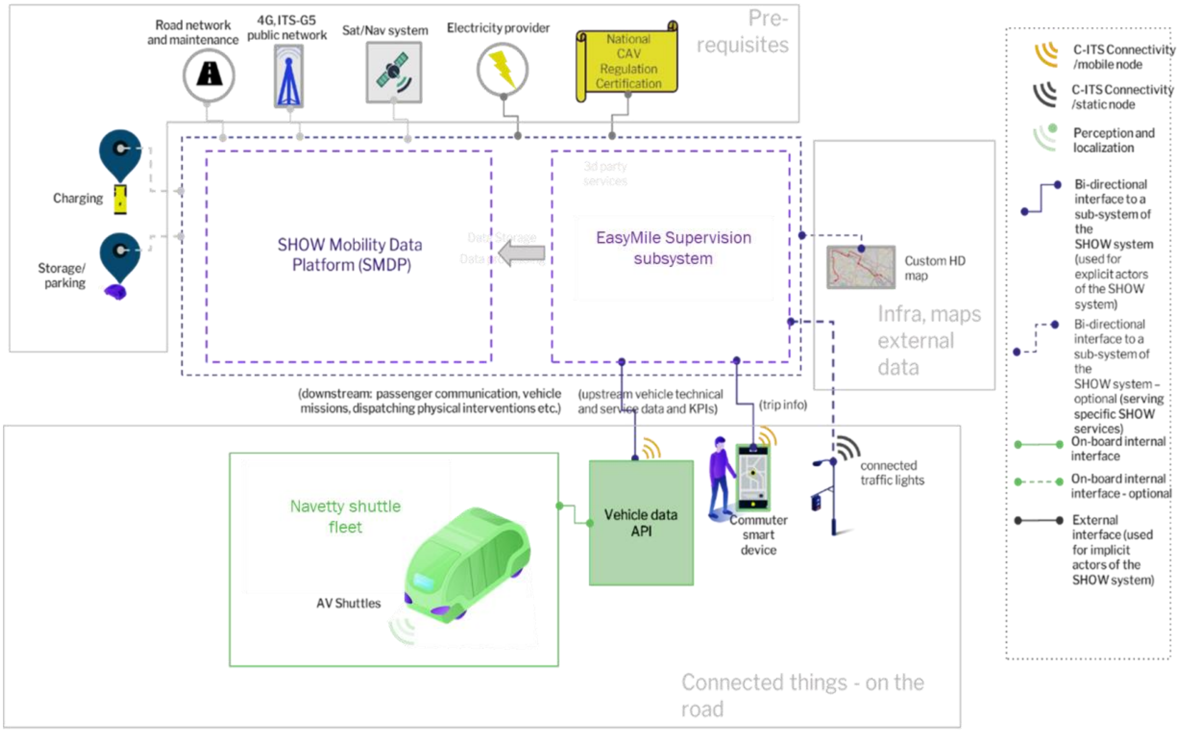

Road network and maintenance
4G, ITS-G5 public network
Sat/Nav system
Electricity provider
National CAV Regulation Certification
Pre-requisites
Charging
Storage/ parking
SHOW Mobility Data Platform (SMDP)
Data Storage
Data processing
3d party services
EasyMile Supervision subsystem
Custom HD map
Infra, maps external data
(downstream: passenger communication, vehicle missions, dispatching physical interventions etc.)
(upstream vehicle technical and service data and KPIs)
(trip info)
Navetty shuttle fleet
AV Shuttles
Vehicle data API
Commuter smart device
connected traffic lights
Connected things - on the road
C-ITS Connectivity /mobile node
C-ITS Connectivity /static node
Perception and localization
Bi-directional interface to a sub-system of the SHOW system (used for explicit actors of the SHOW system)
Bi-directional interface to a sub-system of the SHOW system – optional (serving specific SHOW services)
On-board internal interface
On-board internal interface - optional
External interface (used for implicit actors of the SHOW system)

Figure 12: Les Mureaux site local actors

Table 3: Local actors end their connectivity profile

Actor	**Role**	**Connectivity**
AV Shuttles	Part of shared transport service (regular bus line on a predefined route)	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 located directly inside the ArianneGroup plant	Cloud
Users	Booking and execution of a trips for "on-demand" transport, obtaining service and timetable information for regular shuttle service	App / website

4.3.1 General updates focusing on the LFMP side

Navetty’s functional architecture (component level) is presented in Figure 13 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 is connected to the EasyMile Local Supervision Platform and key data and KPIs are uploaded through API by the back-end terminal

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

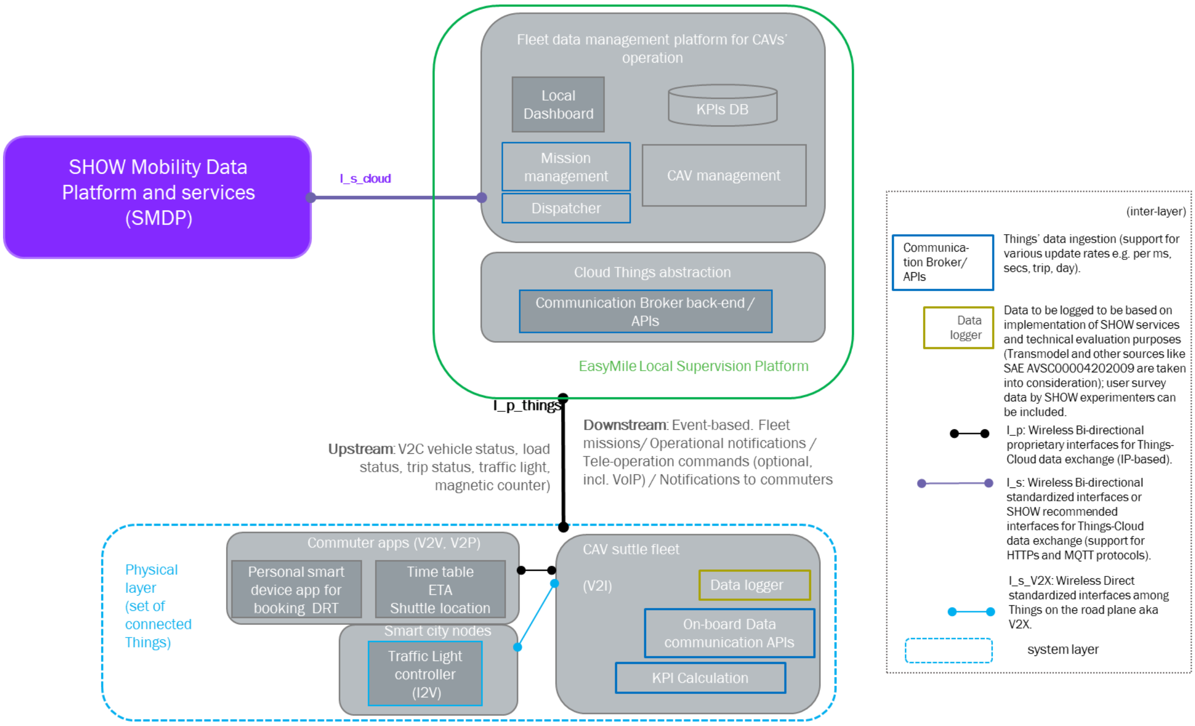

Fleet data management platform for CAVs' operation
Local Dashboard
KPIs DB
Mission management
CAV management
Dispatcher
Cloud Things abstraction
Communication Broker back-end / APIs
EasyMile Local Supervision Platform
SHOW Mobility Data Platform and services (SMDP)
I_s_cloud
I_p_things
Upstream: V2C vehicle status, load status, trip status, traffic light, magnetic counter)
Downstream: Event-based. Fleet missions/ Operational notifications / Tele-operation commands (optional, incl. VoIP) / Notifications to commuters
Physical layer (set of connected Things)
Commuter apps (V2V, V2P)
Personal smart device app for booking DRT
Time table ETA Shuttle location
Smart city nodes
Traffic Light controller (I2V)
CAV suttle fleet
(V2I)
Data logger
On-board Data communication APIs
KPI Calculation
(inter-layer)
Communica-tion Broker/ APIs
Things’ data ingestion (support for various update rates e.g. per ms, secs, trip, day).
Data logger
Data to be logged to be based on implementation of SHOW services and technical evaluation purposes (Transmodel and other sources like SAE AVSC00004202009 are taken into consideration); user survey data by SHOW experimenters can be included.
I_p: Wireless Bi-directional proprietary interfaces for Things-Cloud data exchange (IP-based).
I_s: Wireless Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange (support for HTTPs and MQTT protocols).
I_s_V2X: Wireless Direct standardized interfaces among Things on the road plane aka V2X.
system layer

Figure 13: Functional architecture diagram – focus on the LFMP (EasyMile Local Supervision Platform)

4.3.2 Transdev Local Supervision Platform to SMDP

Data and KPI extracts are being sent from the EasyMile Supervision Platform back-end to the SMDP. Description below focuses on the LFMP Dashboard/RC centre.

The Dashboard on the Supervision System as seen in the Figure 14 has a global vision of the health of the fleet and the system as well as other non-real time functions:

- Health of system includes all real time functions: alerts, KPI, controls, intercom (for passenger assistance), fleet position and metrics (for each shuttle)
- Other non-real time functions are: Line/itinerary definition and Shuttle assignment

The passenger app info is connected directly to the LFMP back-end.

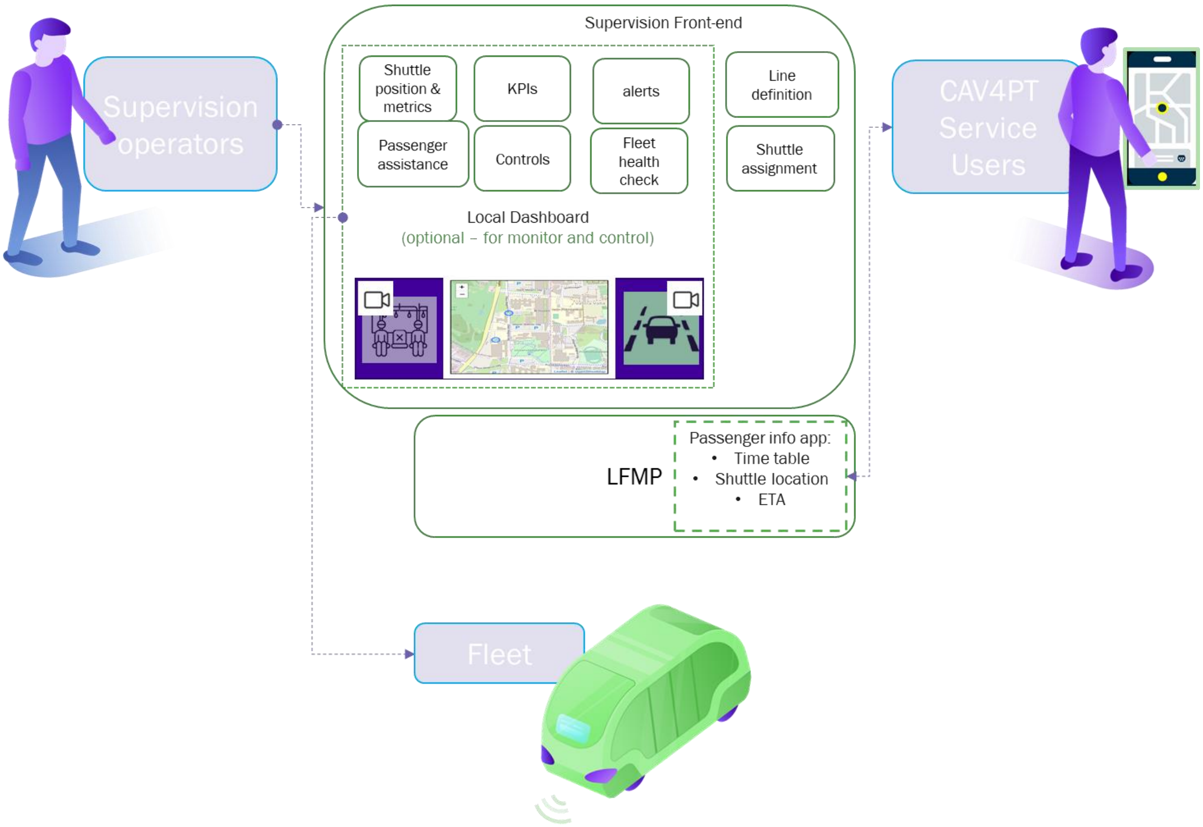


Figure 15: Dashboard of the EasyMile LFMP

4.3.3 CAVs4PT Services information flow

The service information flow is as described in Figure 16 and in Table 4 that follows.

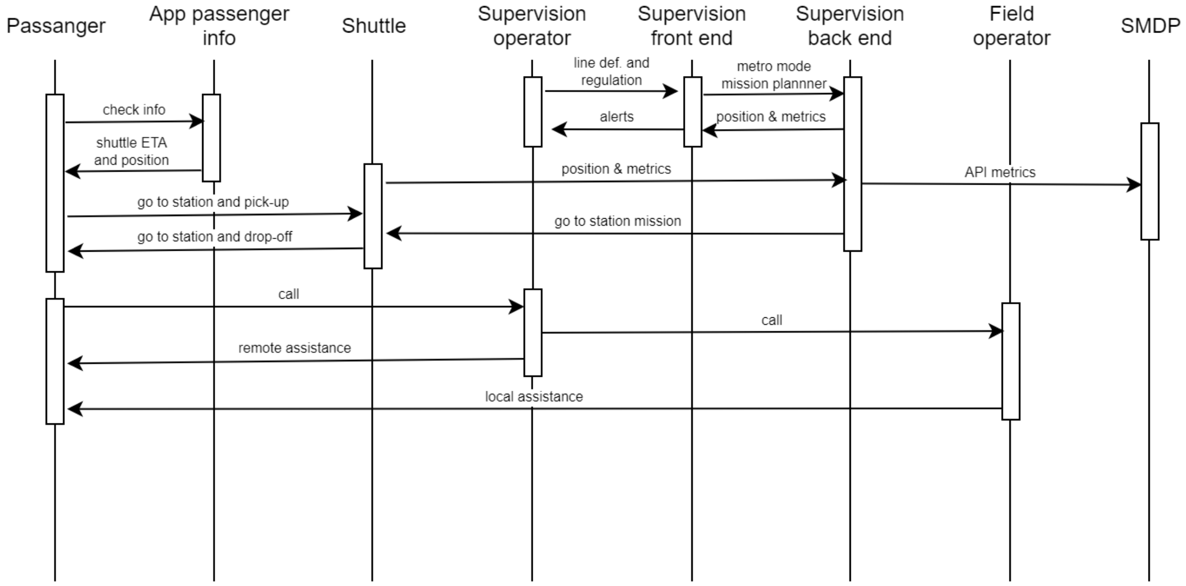


Figure 17: Service flow on the Les Mureaux site.

Table 4: Local service actors and to/from data exchange summary.

Local Service	**Short description**	**Data used (coming from fleet, devices, infra)**
Passanger and App passenger info	User of the mobility service (every ArianeGroup employee or visitor)	• 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
Shuttle	Vehicle fleet (shuttles)	• Key data and metrics are processed
Supervision front-end Supervision back-end Supervision operator	System provided by EasyMile enabling tracking of vehicle, mission management and remote interventions. A human is always in the loop in the local supervision centre, which is situated in the ArianeGroup dedicated control centre room.	• System monitoring ○ Vehicles ○ Infrastructure • Mission management ○ Timetables ○ Customer on demand journey requests • Passenger interface via HMI • Managing non-nominal situations (roadworks, accidents, public demonstrations, passenger illness…)
Field operator	"Human in the loop" – Field operators guarantee all the necessary local	• System monitoring and reception of alerts originating from the vehicle fleet • Assigning of journey missions for the vehicle (NB. This is NOT remote

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

Connectivity and integration with SMDP followed connectivity and cybersecurity guidelines provided, establishing an authenticated and encrypted connectivity between the Les Mureaux site LFDP and the SMDP for KPI data exchange through EasyMile's API.

4.4 Karlsruhe local architecture

4.4.1.1 General updates focusing on the LFMP side

Figure 18 shows a general overview off the local actors participating in the Karlsruhe pilot side. While the participants and their connections did no change in comparison to D4.3, their where minor adjustments regarding the role descriptions, what can be seen in Table 5.

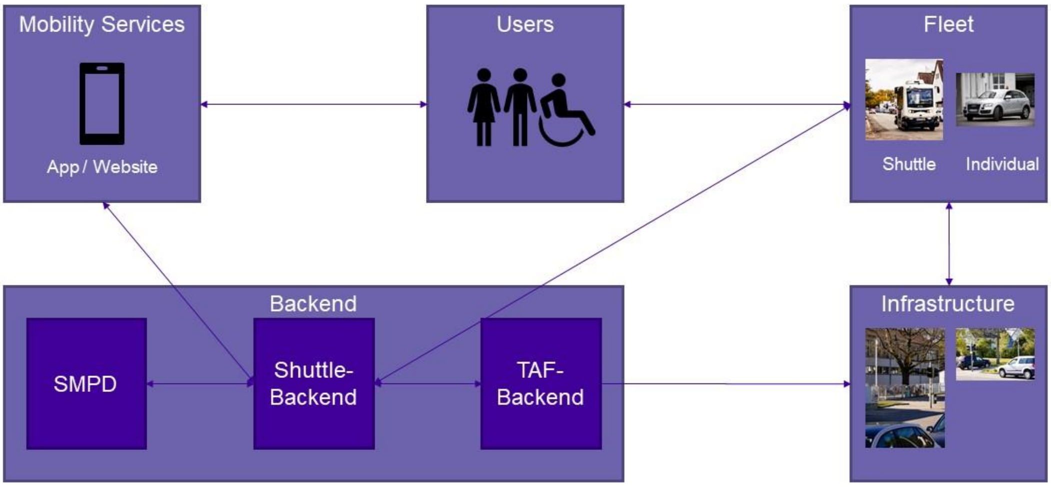


Figure 18: Local actors in Karlsruhe pilot side

Table 5: Local actors and their connectivity profile

Actor	Role	Connectivity
Shuttle	Part of DRT service for passengers and Cargo	V2X / LTE

Actor	Role	Connectivity
Retrofitted vehicle: Modified Q5	Part of DRT service for passengers and Cargo (platooning only)	V2X / LTE
Users	Booking and execution of a DRT service for passengers and/or cargo	App / website
Infrastructure (Light signals, RSUs)	Sending / Receiving SpaT, MAP, CAM, CPMs	V2X
Shuttle backend/TAF backend	Local fleet management platform	Webservice

4.4.1.1.1 Updates regarding the functional architecture

Figure 19 shows the functional architecture of the Karlsruhe pilot site. While the architecture itself did not change, the following connections have been refined:

- 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 for person or cargo transport by selecting a starting and end location from a predefined set of stations. 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.)
    - Furthermore, the backend is responsible for the cargo management, e.g. keeping track of the transported cargo and which compartments of the cargo hold are currently occupied.

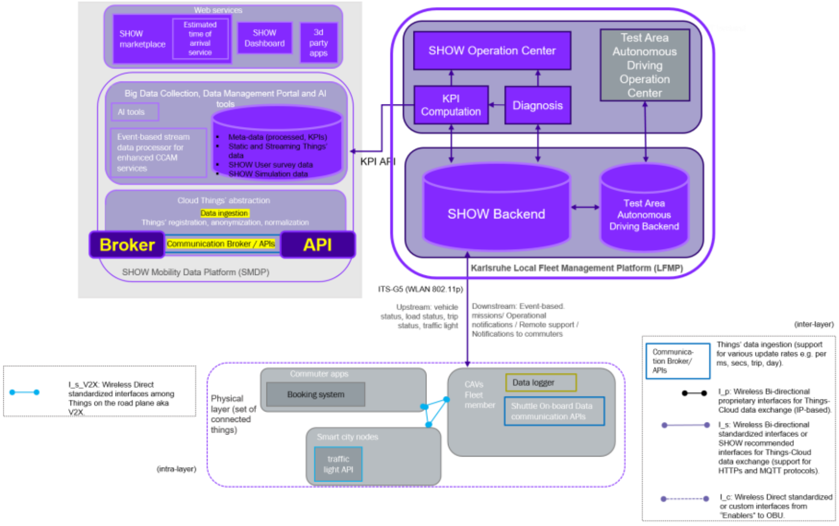

Web services
SHOW marketplace
Estimated time of arrival service
SHOW Dashboard
3d party apps
Big Data Collection, Data Management Portal and AI tools
AI tools
Event-based stream data processor for enhanced CCAM services
Meta-data (processed, KPIs)
Static and Streaming Things' data
SHOW User survey data
SHOW Simulation data
Cloud Things' abstraction
Data ingestion
Things' registration, anonymization, normalization
Broker
Communication Broker / APIs
API
SHOW Mobility Data Platform (SMDP)
KPI API
SHOW Operation Center
Test Area Autonomous Driving Operation Center
KPI Computation
Diagnosis
SHOW Backend
Test Area Autonomous Driving Backend
Karlsruhe Local Fleet Management Platform (LFMP)
ITS-G5 (WLAN 802.11p)
Upstream: vehicle status, load status, trip status, traffic light
Downstream: Event-based missions/ Operational notifications / Remote support / Notifications to commuters
(inter-layer)
Communication Broker/ APIs
Things' data ingestion (support for various update rates e.g. per ms, secs, trip, day).
I_p: Wireless Bi-directional proprietary interfaces for Things-Cloud data exchange (IP-based).
I_s: Wireless Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange (support for HTTPs and MQTT protocols).
I_c: Wireless Direct standardized or custom interfaces from "Enablers" to OBU.
I_s_V2X: Wireless Direct standardized interfaces among Things on the road plane aka V2X.
(intra-layer)
Physical layer (set of connected things)
Commuter apps
Booking system
Smart city nodes
traffic light API
CAVs Fleet member
Data logger
Shuttle On-board Data communication APIs

Figure 19: Karlsruhe pilot site functional architecture

4.4.1.1.2 Updates regarding the service information flow

While the service flow provided is still valid an additional service flow has been defined as shown in Figure 20. The figure shows the information flow when a user picks up cargo, that was send to them. To do so, the user receives a QR-Code from the sender. To start the process depicted in Figure 20, the user has to scan the QR-Code with a scanner, that is attached to the cargo hold. The corresponding ScannerApp extracts the compartment number from the QR-Code and contacts the Booking Management to check if the compartment is currently booked by the specific user. After that the Booking Management sends a request to open the specific compartment. The request gets translated into the ROS ecosystem in order to control the compartment locks. After a successful delivery the Booking Management gets updated accordingly.

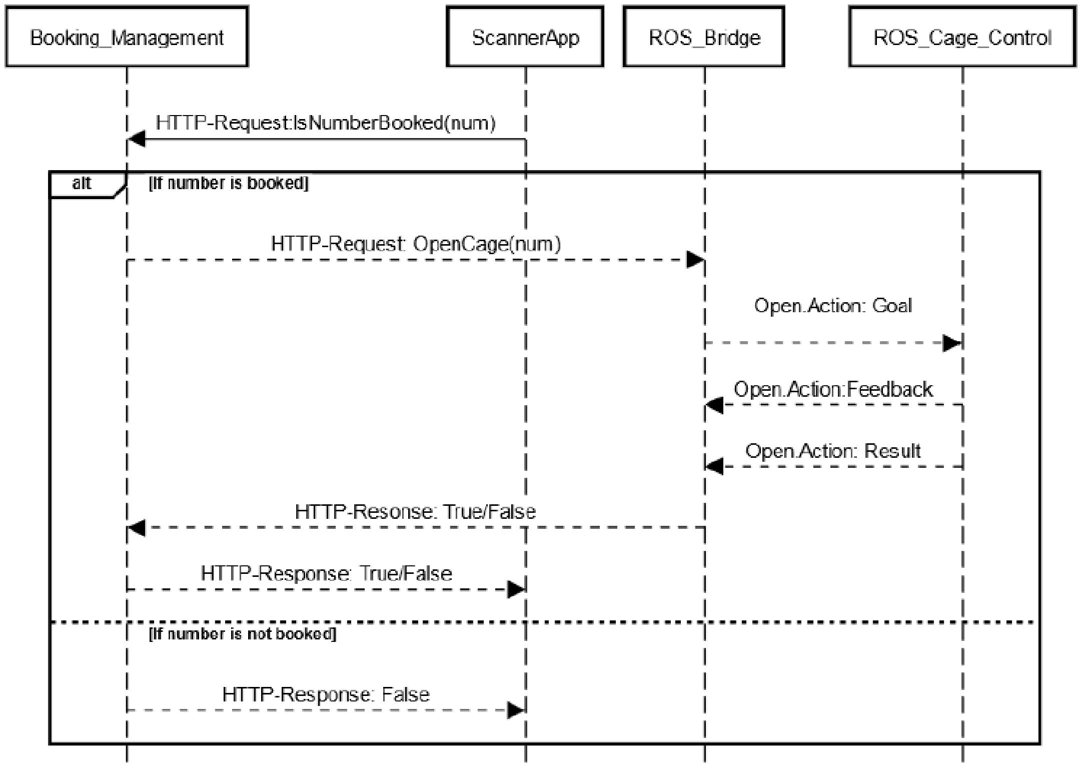


Figure 20: Service information flow for picking up cargo

4.5 The Austrian Pilot sites

4.5.1 Graz local architecture

4.5.1.1 General updates focusing on the LFMP side

Graz conceptual architecture including all technological components interacting with the SMDP are presented in the diagram of Figure 21 and the Table 6. 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.

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 bus terminal is monitored via a smart camera system. It detects the bounding boxes of the objects in its view, classifies them and provides corresponding information locally to the C-ITS Road Side Unit (RSU), which further sends out C-ITS messages to the vehicles. In addition, AVs need to cross a tram track after leaving and before entering the bus terminal. This information is also conveyed via C-ITS to the vehicles.

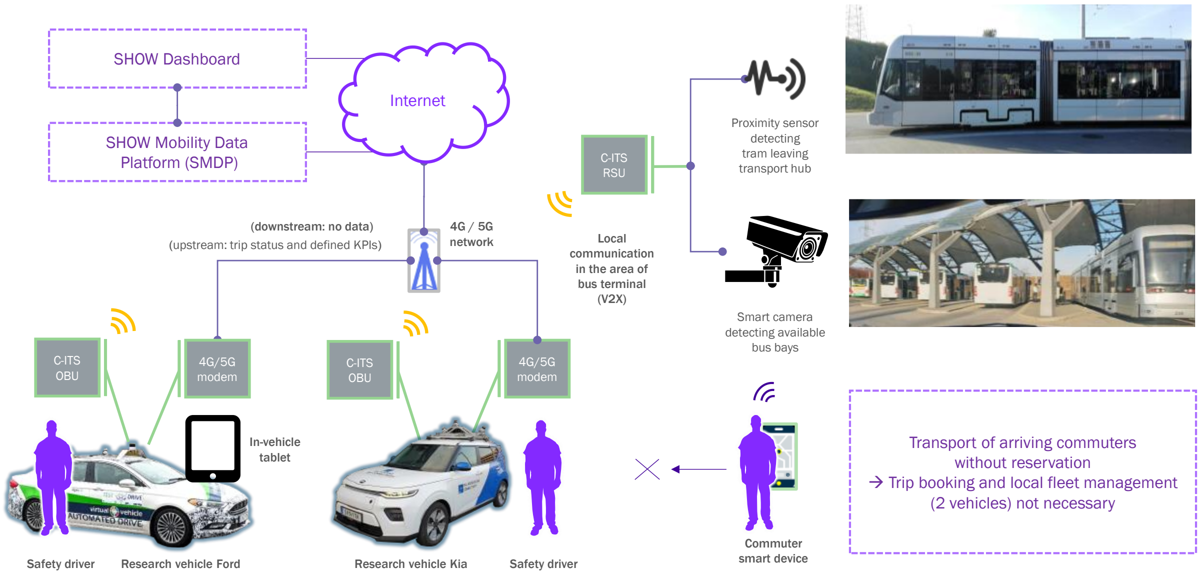

SHOW Dashboard
SHOW Mobility Data Platform (SMDP)
Internet
(downstream: no data)
(upstream: trip status and defined KPIs)
4G / 5G network
C-ITS RSU
Local communication in the area of bus terminal (V2X)
Proximity sensor detecting tram leaving transport hub
Smart camera detecting available bus bays
C-ITS OBU
4G/5G modem
In-vehicle tablet
C-ITS OBU
4G/5G modem
Safety driver
Research vehicle Ford
Research vehicle Kia
Safety driver
Commuter smart device
Transport of arriving commuters without reservation
→ Trip booking and local fleet management (2 vehicles) not necessary

Figure 21: 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 6: 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 V2X

Actor	Role	Connectivity
Public bus and tram	Public transport. Transfer connection from AV.	Proprietary connection to local city transport management. Not used in SHOW, since buses are detected directly when they enter the terminal.
Commuter / User	User of the service	No connectivity foreseen

4.5.1.2 Description focusing on the LFMP Dashboard/RC center (if applicable).

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" (i.e. the MQTT interface) 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 CAVs4PT Services information flow (if applicable).

In the following figure (Figure 22), 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 several potential stops in the targeted area.

After boarding the vehicle and confirming the stop, 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. In the same way, information exchange about the crossing of tram tracks is performed to give clearance to vehicle in these special zones.

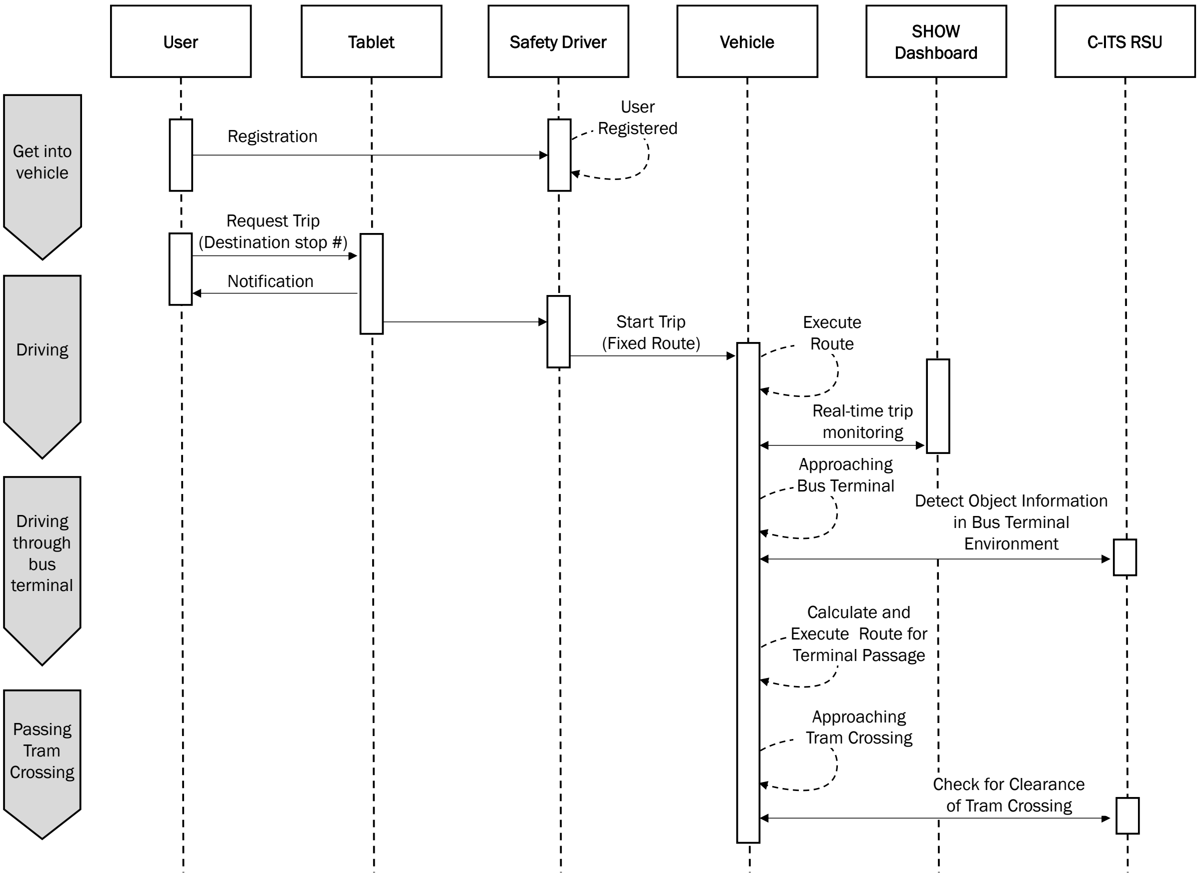

User
Tablet
Safety Driver
Vehicle
SHOW Dashboard
C-ITS RSU
Get into vehicle
Driving
Driving through bus terminal
Passing Tram Crossing
Registration
User Registered
Request Trip (Destination stop #)
Notification
Start Trip (Fixed Route)
Execute Route
Real-time trip monitoring
Approaching Bus Terminal
Detect Object Information in Bus Terminal Environment
Calculate and Execute Route for Terminal Passage
Approaching Tram Crossing
Check for Clearance of Tram Crossing

Figure 22: Information flow diagram for Graz

4.5.1.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if applicable)

4.5.2 Salzburg local architecture

Figure 23 describes the system conceptual view in the Pilot Site Salzburg. Table 7 adds textual description of the local actors, their role as well as their connectivity.

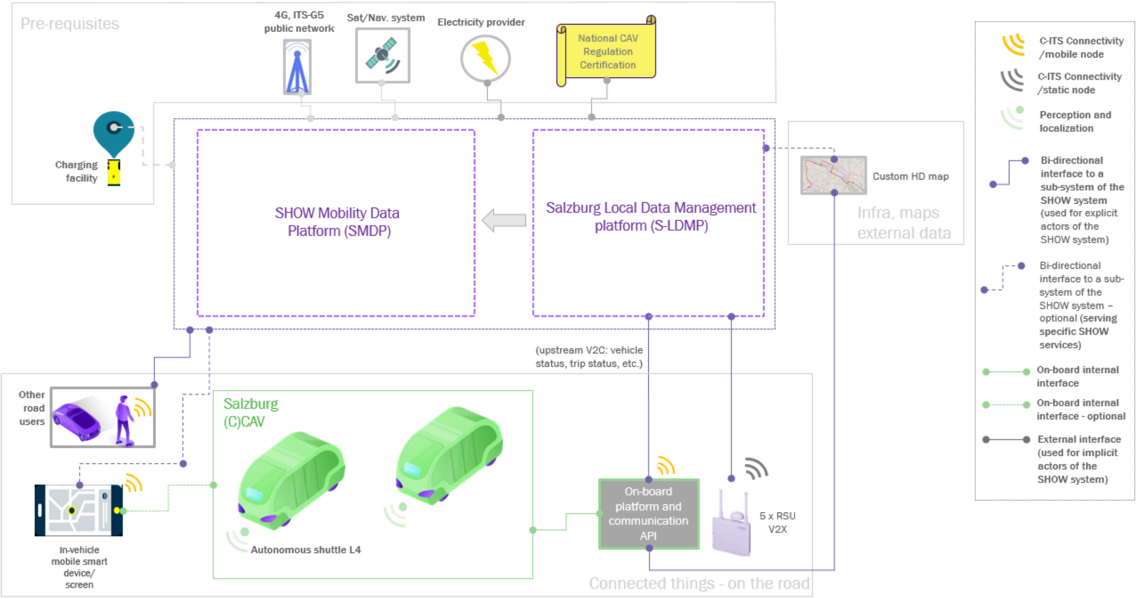

Pre-requisites
4G, ITS-G5 public network
Sat/Nav. system
Electricity provider
National CAV Regulation Certification
Charging facility
SHOW Mobility Data Platform (SMDP)
Salzburg Local Data Management platform (S-LDMP)
Custom HD map
Infra, maps external data
(upstream V2C: vehicle status, trip status, etc.)
Other road users
Salzburg (C)CAV
Autonomous shuttle L4
In-vehicle mobile smart device/ screen
On-board platform and communication API
5 x RSU V2X
Connected things - on the road
C-ITS Connectivity /mobile node
C-ITS Connectivity /static node
Perception and localization
Bi-directional interface to a sub-system of the SHOW system (used for explicit actors of the SHOW system)
Bi-directional interface to a sub-system of the SHOW system – optional (serving specific SHOW services)
On-board internal interface
On-board internal interface - optional
External interface (used for implicit actors of the SHOW system)

Figure 23: System conceptual view – Pilot Site Salzburg

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

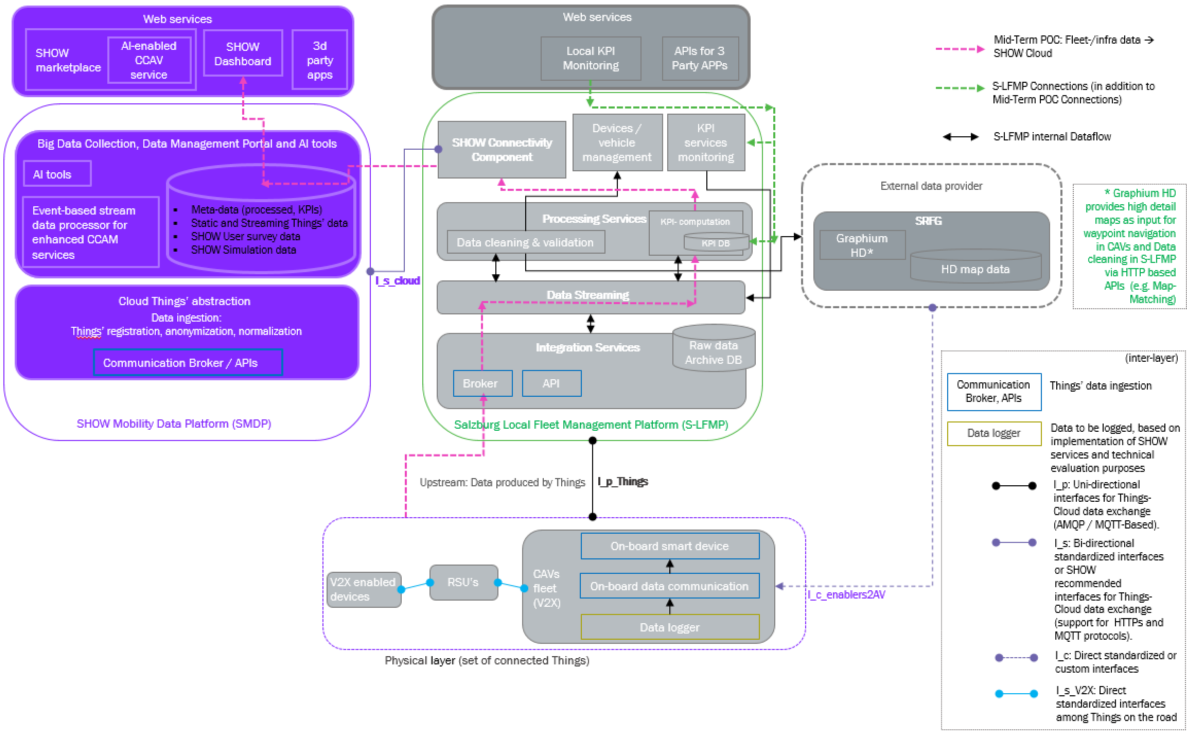
Table 7: Local actors and their connectivity profile – Pilot Site Salzburg

In Table 8, 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 24.

Table 8: Description of information flow paths – Pilot Site Salzburg

Information flow paths short description		
S-LFMP Connections	S-LFMP internal dataflow	Mid-Term POC

Information flow paths short description		
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 access KPIs for Stream Data and KPIs Database to monitor sLtate	• 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 computation, 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



Web services
SHOW marketplace
AI-enabled CCAV service
SHOW Dashboard
3d party apps
Big Data Collection, Data Management Portal and AI tools
AI tools
Event-based stream data processor for enhanced CCAM services
Meta-data (processed, KPIs)
Static and Streaming Things' data
SHOW User survey data
SHOW Simulation data
Cloud Things' abstraction
Data ingestion:
Things' registration, anonymization, normalization
Communication Broker / APIs
SHOW Mobility Data Platform (SMDP)
I_s_cloud
Web services
Local KPI Monitoring
APIs for 3 Party APPs
SHOW Connectivity Component
Devices / vehicle management
KPI services monitoring
Processing Services
KPI- computation
Data cleaning & validation
KPI DB
Data Streaming
Integration Services
Raw data Archive DB
Broker
API
Salzburg Local Fleet Management Platform (S-LFMP)
Upstream: Data produced by Things
I_p_Things
V2X enabled devices
RSU's
CAVs fleet (V2X)
On-board smart device
On-board data communication
Data logger
I_c_enablers2AV
Physical layer (set of connected Things)
Mid-Term POC: Fleet-/infra data → SHOW Cloud
S-LFMP Connections (in addition to Mid-Term POC Connections)
S-LFMP internal Dataflow
External data provider
SRFG
Graphium HD*
HD map data
* Graphium HD provides high detail maps as input for waypoint navigation in CAVs and Data cleaning in S-LFMP via HTTP based APIs (e.g. Map-Matching)
(inter-layer)
Communication Broker, APIs
Things' data ingestion
Data logger
Data to be logged, based on implementation of SHOW services and technical evaluation purposes
I_p: Uni-directional interfaces for Things-Cloud data exchange (AMQP / MQTT-Based).
I_s: Bi-directional standardized interfaces or SHOW recommended interfaces for Things-Cloud data exchange (support for HTTPs and MQTT protocols).
I_c: Direct standardized or custom interfaces
I_s_V2X: Direct standardized interfaces among Things on the road

Figure 24: Local Architecture – Pilot Site Salzburg

Internal data platform to connect AV and submit data has been setup. In a micro-service-based architecture, clearly separated components have been deployed to connect the AV Data to the streaming platform, process and bridge the data to the SHOW DMP and forward the data to a database-based storage solution for historical storage of the stream data. With this approach, data from AV is internally connected to a streaming platform and in addition historicized.

The bridge component to the SHOW DMP is processing the online data stream (locations and speed) and converting the data into the JSON based SHOW DMP MQTT message format.

4.5.2.1 General updates focusing on the LFMP side

Regarding the LFMP at the Pilot site Salzburg no significant updates have been realized. One aspect that has changed in comparison to the planned “Local architecture” reported in D4.3 is, that no Local KPI Monitoring Dashboard within the Web services will be deployed since SHOW Dashboard can be used instead.

4.5.2.2 Description focusing on the LFMP Dashboard/RC center (if applicable).

Not applicable.

4.5.2.3 CAVs4PT Services information flow

Figure 25 illustrates the service information (data) flow for the Pilot site Salzburg. The schedule of the AV is integrated into the service app of the local transport provider, from where a potential user retrieves the information. The potential user enters the AV at a predefined stop and the safety operator starts the trip on the fixed route, encompassing eight stops in total. The AV executes the route, including automated stop management (enter, stop and exit at designated stops) as well as intersection management (left turn at an unregulated intersection). V2X-communication between the AV and the C-ITS Road Side Units is established. ETSI-message used are CPM, DENM, RTCEM, which are transferred via AMQP based protocol to the S-LFMP. Dynamic driving data, such as GPS position, speed, acceleration etc. is logged locally within components of the AV. The on-board data communication transfers the data via MQTT protocol to the S-LFMP. Within the S-LFMP, the received data from the AV is integrated using a streaming layer. Data cleaning and validation is executed before being streamed into KPI computing and the SHOW DMP via MQTT based protocol.

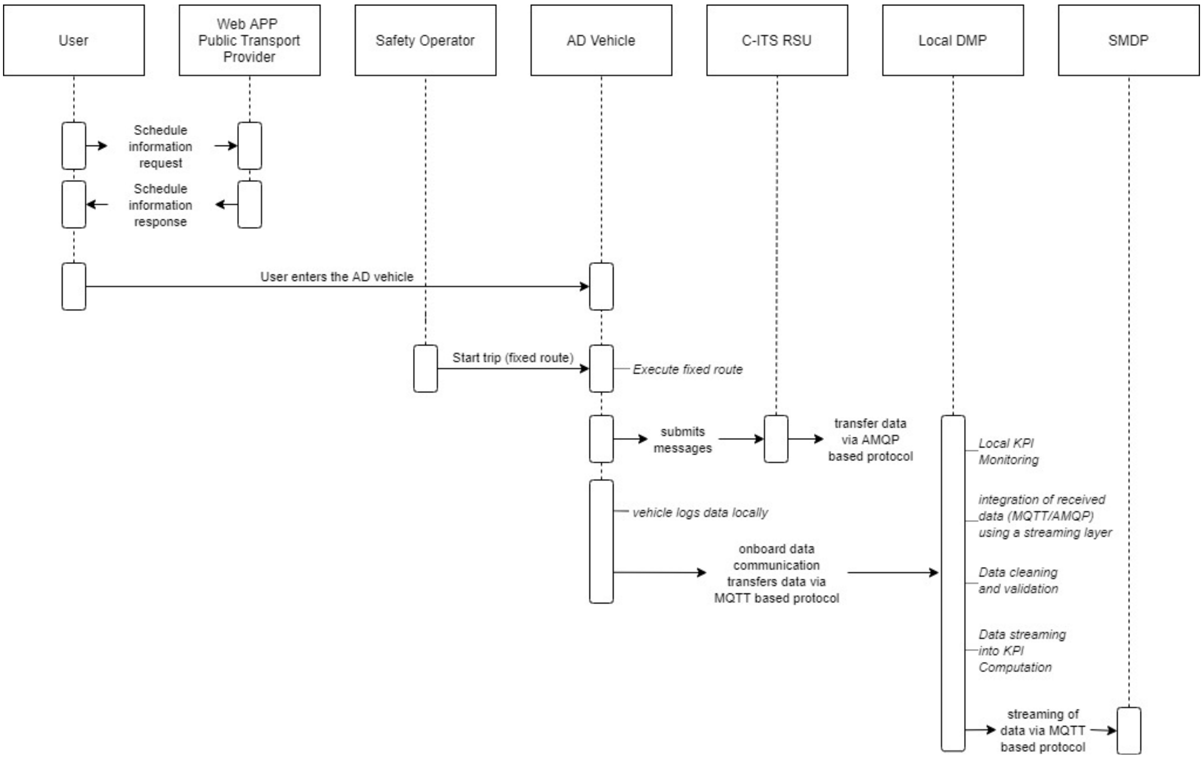


Figure 25: Service information flow diagram – Pilot Site Salzburg

4.5.2.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if applicable)

The AD-system in the vehicle ensures protection against unauthorized access. This is accomplished by the following measures:

- Software for automated functions is located on a physically separated Hardware (add-on units & measurement technology in the vehicle).
- Add-on & measurement technology has separate access authorizations & password protection.

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.

4.5.3.1 General updates focusing on the LFMP side

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).

Figure 26: Automated Shuttle at demo site Pörtschach (© SURAAA)

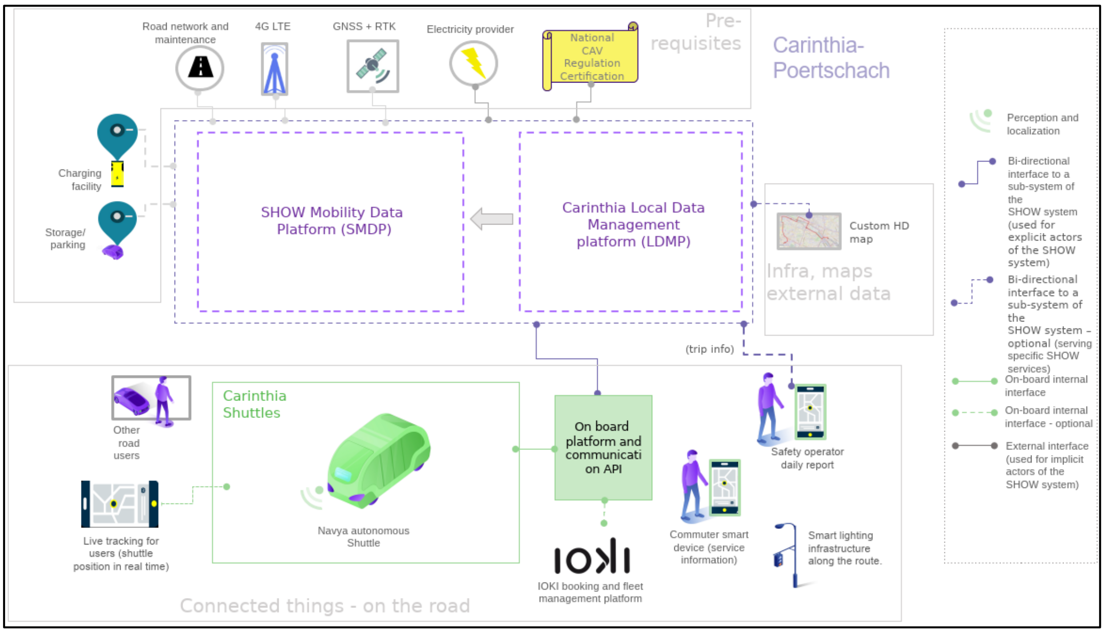
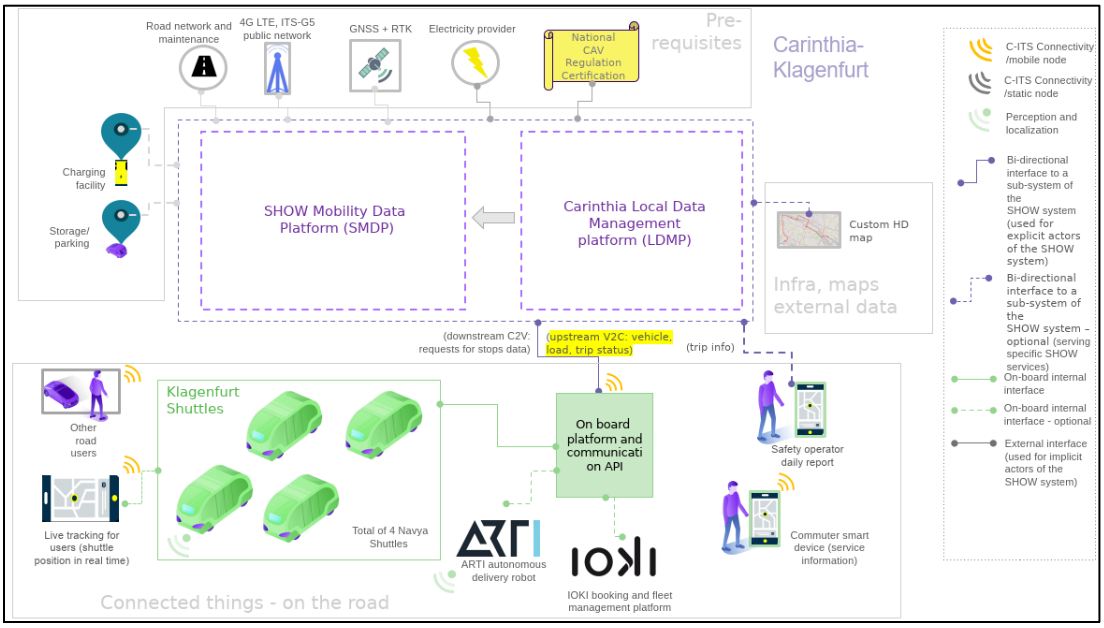

Road network and maintenance
4G LTE
GNSS + RTK
Electricity provider
National CAV Regulation Certification
Pre-requisites
Carinthia-Poertschach
Charging facility
Storage/ parking
SHOW Mobility Data Platform (SMDP)
Carinthia Local Data Management platform (LDMP)
Custom HD map
Infra, maps external data
(trip info)
Other road users
Carinthia Shuttles
Navya autonomous Shuttle
On board platform and communication API
Safety operator daily report
Commuter smart device (service information)
Smart lighting infrastructure along the route.
Live tracking for users (shuttle position in real time)
IOKI booking and fleet management platform
Connected things - on the road
Perception and localization
Bi-directional interface to a sub-system of the SHOW system (used for explicit actors of the SHOW system)
Bi-directional interface to a sub-system of the SHOW system - optional (serving specific SHOW services)
On-board internal interface
On-board internal interface - optional
External interface (used for implicit actors of the SHOW system)

Figure 27: Local actors at the pilot site Pörtschach Carinthia

Figure 27 shows the general overview of the architecture of the site Pörtschach in Carinthia. The IOKI booking and fleet management platform was added to the architecture in 2022. In Pörtschach IOKI will be used primarily for on-demand booking of the autonomous Navya shuttle. C-ITS was removed from the architecture for Pörtschach because there is no possibility to test/use C-ITS. At the pilot site in Pörtschach storage and parking is provided by the local community, together with the charging possibility. 4G/LTE is currently used in Pörtschach, 5G is ready to be used, but the shuttle does require a suitable 5G router. 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 can follow the location via the official website of SURAAA.

Klagenfurt: This is a site with a complex traffic situation. The route will include traffic lights, a roundabout and a traffic barrier. There are three different route options, which will be implemented as level 1-3, the final route length will be 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.



Road network and maintenance
4G LTE, ITS-G5 public network
GNSS + RTK
Electricity provider
National CAV Regulation Certification
Pre-requisites
Carinthia-Klagenfurt
Charging facility
Storage/ parking
SHOW Mobility Data Platform (SMDP)
Carinthia Local Data Management platform (LDMP)
Custom HD map
Infra, maps external data
(downstream C2V: requests for stops data)
(upstream V2C: vehicle, load, trip status)
(trip info)
Other road users
Klagenfurt Shuttles
Total of 4 Navya Shuttles
Live tracking for users (shuttle position in real time)
On board platform and communicati on API
ARTI
ARTI autonomous delivery robot
IOKI
IOKI booking and fleet management platform
Safety operator daily report
Commuter smart device (service information)
Connected things - on the road
C-ITS Connectivity /mobile node
C-ITS Connectivity /static node
Perception and localization
Bi-directional interface to a sub-system of the SHOW system (used for explicit actors of the SHOW system)
Bi-directional interface to a sub-system of the SHOW system – optional (serving specific SHOW services)
On-board internal interface
On-board internal interface - optional
External interface (used for implicit actors of the SHOW system)

Figure 28: Local actors at the pilot site Klagenfurt Carinthia

Figure 28 shows the general overview of the architecture of the site Klagenfurt in Carinthia. The participants and their connections did not change in comparison to D4.3, however two new participants were added. The IOKI booking and fleet management platform was added to the architecture in 2022. In Klagenfurt, IOKI will be used for on-demand booking of the automated shuttles as for the fleet management of the four deployed shuttles. The ARTI autonomous delivery robot was added as a new participant. The robot will transfer goods and is transported itself within the Navya shuttle. The ARTI robot is part of the LaaS UC.

4.5.3.2 CAVs4PT Services information flow

The diagram of Figure 29 shows the current situation at the demo site in Pörtschach.

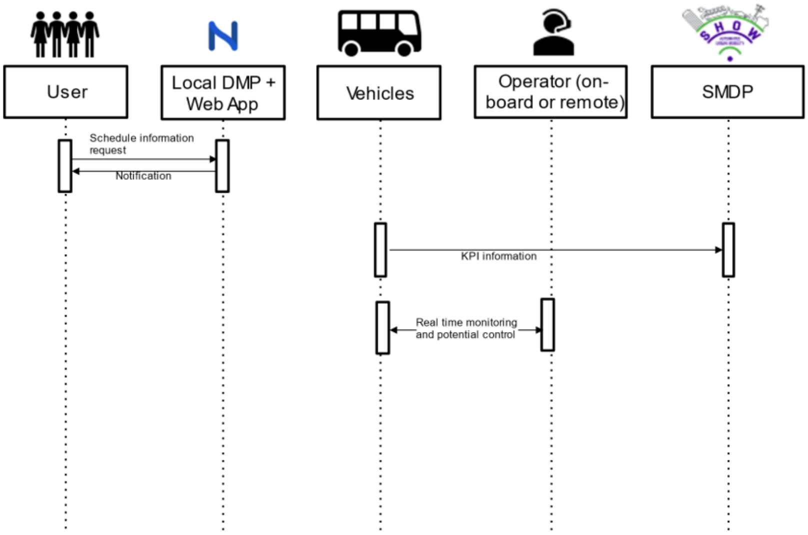
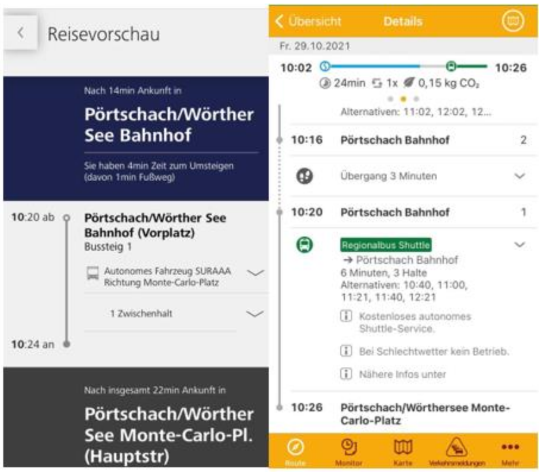

User
Local DMP + Web App
Vehicles
Operator (on-board or remote)
SMDP
Schedule information request
Notification
KPI information
Real time monitoring and potential control

Figure 29: CAVs4PT Services information flow at the demo site in Pörtschach

The following stakeholders are involved in Pörtschach:

- **Navya**: Shuttle provider
- **Local public transport providers**
    - External App provider already list the shuttle in the official public service schedule:



Nach 14min Ankunft in

Pörtschach/Wörther See Bahnhof

Sie haben 4min Zeit zum Umsteigen (davon 1min Fußweg)

10:20 ab Pörtschach/Wörther See Bahnhof (Vorplatz)
Bussteig 1
Autonomes Fahrzeug SURAAA Richtung Monte-Carlo-Platz
1 Zwischenhalt
10:24 an

Nach insgesamt 22min Ankunft in

Pörtschach/Wörther See Monte-Carlo-Pl. (Hauptstr)

Fr. 29.10.2021

10:02 — 10:26
24min 1x 0,15 kg CO₂
Alternativen: 11:02, 12:02, 12...

10:16	Pörtschach Bahnhof	2
	Übergang 3 Minuten	
10:20	Pörtschach Bahnhof	1

Regionalbus Shuttle
→ Pörtschach Bahnhof
6 Minuten, 3 Halte
Alternativen: 10:40, 11:00, 11:21, 11:40, 12:21

Kostenloses autonomes Shuttle-Service.

Bei Schlechtwetter kein Betrieb.

Nähere Infos unter

10:26 Pörtschach/Wörthersee Monte-Carlo-Platz

Figure 30: Public transport booking platforms OEBB and Kaerntner Linien

4.5.3.3 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if applicable)

The booking will be managed by the on-demand app from IOKI. As described above, the shuttle is currently using a 4G/LTE network. Cybersecurity aspects are handled by the shuttle OEM, i.e. Navya.

4.6 Turin local architecture

4.6.1 General updates focusing on the LFMP side

Turin architecture was described in detail in D4.3, no applicable updates.

4.7 Tampere (Hervanta) local architecture

This site comprises two sub-sites, namely “Hervanta” and “Lehti” which share similar architecture setup. Updates below correspond to Hervanta deployment since Lehti has not yet started.

4.7.1 General updates focusing on the LFMP side

Tampere functional architecture was described in detail in D4.3. Sensible 4 vehicles handle a big part of the KPI calculations on-board and the vehicle systems will provide the calculated KPI data to the Sensible 4 data management platform that acts as a local platform for the purposes of data logging (no additional functions within SHOW were utilised and therefore the local dashboard in these cases is a "black box”). It is a proprietary platform of Sensible 4 and is not connected to local service providers. It is connected to the SHOW platform, to which also the Sensible 4 vehicle provides the KPI data. VTT’s shuttle provides data directly to the SHOW data platform, but keeps a local backup of transmitted data.

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.

4.7.2 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if applicable)

VTT demonstrated I2V connection, where a roadside station positioned at a pedestrian crossing transmitted information about pedestrian occupancy to the automated vehicle(s).

Cyber- security follows SHOW D4.1 recommendation and adheres to the vehicle providers’ (Sensible 4, VTT & Remoted) 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 vehicles. Interoperability between vehicles to local actors, where needed, is to be done using predefined APIs. For its vehicles, Sensible 4 manage both the vehicle and the LDMP, as well as the connectivity to SDMP.

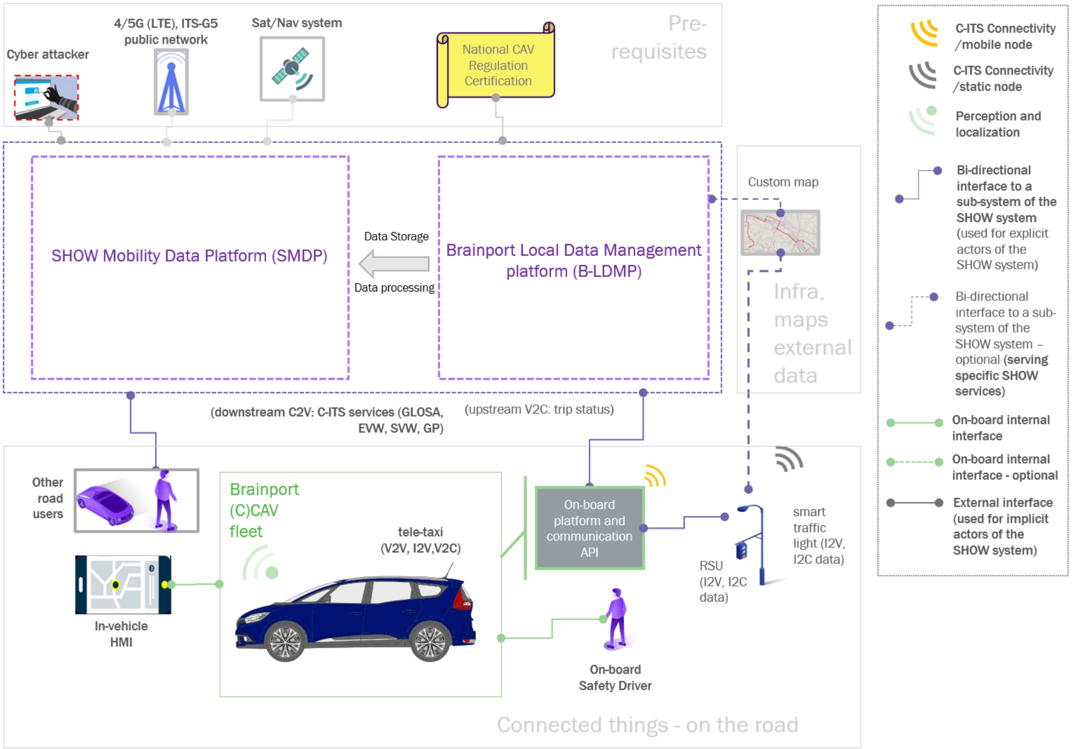
4.8 Brainport local architecture

The vehicle fleet in the Brainport satellite site consists of 3 Renault Scenic passenger cars. Additionally, a demonstrator might be executed using an AV shuttle or E-Bus, provided by a third party.

4.8.1 General updates focusing on the LFMP side

The vehicles available in the Brainport site can be driving either manually or automatically. In automated mode, a safety driver must be present and take over the vehicle at any time. 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 31.

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. See D9.2 for a more elaborative description of these use-cases. In order to realize these use-cases, the demonstrators rely on a smart traffic light, VRU and road side unit for VRU detection. Please find further details on the actors and roles in the table below.



Cyber attacker
4/5G (LTE), ITS-G5 public network
Sat/Nav system
National CAV Regulation Certification
Pre-requisites
C-ITS Connectivity /mobile node
C-ITS Connectivity /static node
Perception and localization
Bi-directional interface to a sub-system of the SHOW system (used for explicit actors of the SHOW system)
Bi-directional interface to a sub-system of the SHOW system – optional (serving specific SHOW services)
On-board internal interface
On-board internal interface - optional
External interface (used for implicit actors of the SHOW system)
SHOW Mobility Data Platform (SMDP)
Data Storage
Data processing
Brainport Local Data Management platform (B-LDMP)
Custom map
Infra, maps external data
(downstream C2V: C-ITS services (GLOSA, EVW, SVW, GP)
(upstream V2C: trip status)
Other road users
In-vehicle HMI
Brainport (C)CAV fleet
tele-taxi (V2V, I2V,V2C)
On-board platform and communication API
RSU (I2V, I2C data)
smart traffic light (I2V, I2C data)
On-board Safety Driver
Connected things - on the road

Figure 31: Local actors diagram for Brainport pilot site

Table 9: Local actors' role and connectivity enabled (when applicable)

Actor	Role	Connectivity
Brainport 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

Actor	Role	Connectivity
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	I2V
Smart Road Side Unit	Detection of VRU in UC1.3: Safety for VRU at intersections	I2V
Vehicle (2) equipped with V2V	Vehicle ready for platooning in UC1.8: Vehicle relocation for automated mobility using platooning.	V2V

4.8.2 CAVs4PT Services information flow (if applicable).

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 run, the recorded data are bein stored on the Brainport Local Data Management Platform (B-LDMP), where KPIs are calculated. Ready KPI are exchanged with the SHOW Mobility Data Platform (SMDP) from where KPI can be visualized on the SHOW dashboard. The information flow in the Brainport site is summarized in Figure 32 and service entities are briefly described in the table below.

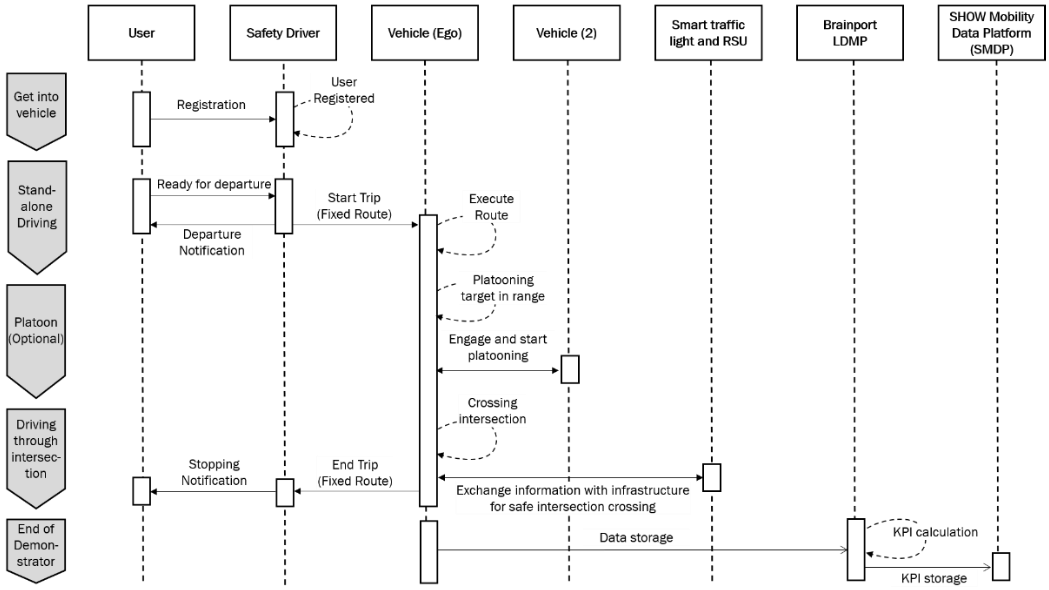


Figure 32: Brainport information flow diagram

Local Service title	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.

4.8.3 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if applicable)

No custom solution applied. The Brainport Pilot satellite site follows SHOW integration guidelines 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 General updates focusing on the LFMP side

SHOW local architecture instantiation for Trikala site was described in detail in the previous version, i.e. in D4.3. In this round of updates, we will focus on Remote Control Center updated functionality for increased safety and service information flow diagrams' update.

4.9.2 Description focusing on the LFMP Dashboard/RC center (if applicable).

In the updated vehicle-to-LFMP architecture illustrated in Figure 33, one important vehicle data management module has been acquired and installed on the shuttles for the DRT service implementation (real-time alerts functionality offered by the module provided by Heex). With this module, it is possible not only to transfer in real-time vehicle data to the LFMP but also to generate, record and manage events' triggers during runtime (real time sensor and vehicle data processing and events' annotation) so that the remote control centre is always aware of any safety-critical events on the road. This functionality combined with maintaining a bilateral connectivity channel between each AV and the remote control centre, which is responsible for the remote safety monitoring of the unmanned AV (as depicted in Figure 34), makes the deployment of unmanned shuttles possible in Trikala. This is in alignment with the Greek legislation that permits a remote safety operator only if certain functionalities and uninterrupted connectivity with the web-based RC center is guaranteed.

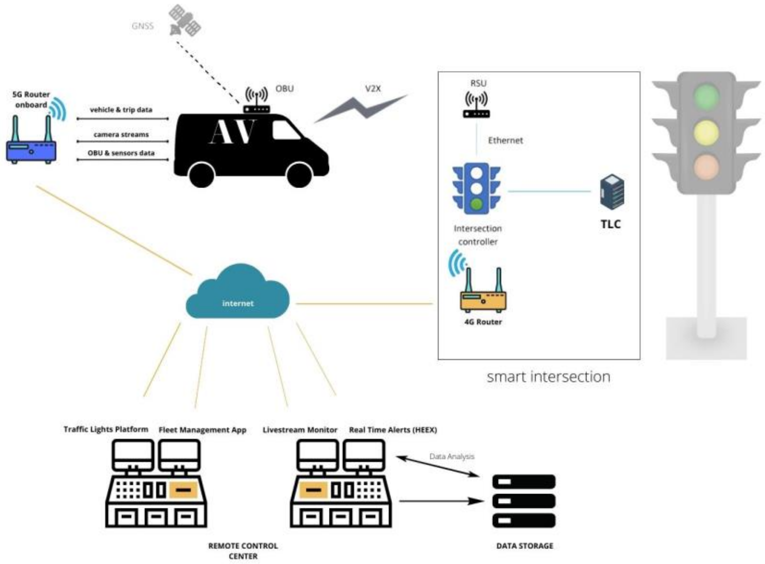


Figure 33: Components of the local architecture

4.9.3 CAVs4PT Services information flow (if applicable).

Three main use cases that correspond to three discrete services are offered in Trikala:

a. Passengers on demand transport (fixed route)
b. Logistics service with robots
c. Robo-taxis for passengers' last mile

Service flow diagrams for each of the three types of services are provided in the subsections that follow.

4.9.3.1 Updated DRT service data flow

In Figure 34, the updated service flow diagram for the on demand-responsive transport (DRT) service is provided. Booking system is now integrated and functionality of the Remote Control centre is better specified with respect to D4.3.

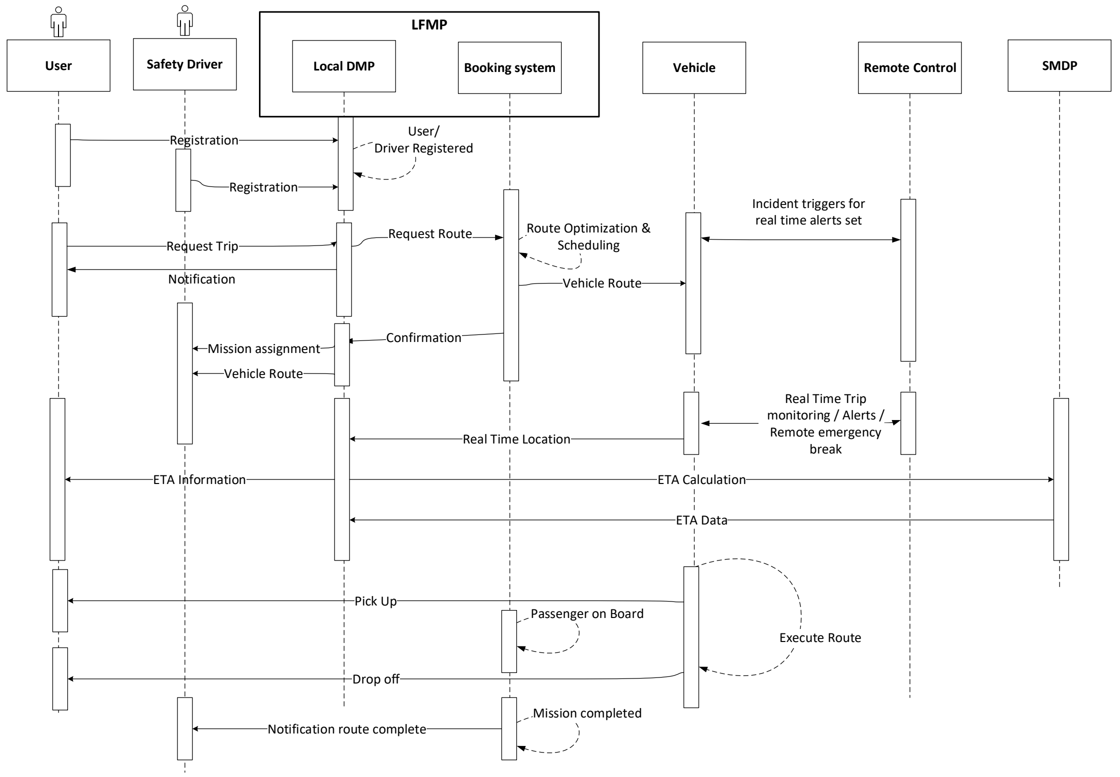


Figure 34: Trikala DRT service data flow

4.9.3.2 Logistics service with droids (small on-road robots)

In Trikala, for the logistics services, the Control Room laptop is connected through Wi-Fi or Ethernet to the network. The droids are connected through their internal modem to 4G network. In this setup, the 4G coverage must be guaranteed on the whole area where the droids are navigating.

A fiber-optic connection with a minimum speed of 100Mbps is preferred for the Control Room laptop. A 4G SIM card must be provided for each droid. Port forwarding is needed on the Control Room router towards the laptop IP on the UDP ports from 65000 to 65011 included.

Three different logistics services have been provided:

1. In the Christmas Park, the autonomous droid (Yape) collected Christmas letters from the post Office and delivered them to Santa’s house. The elves were in charge of putting the letter bags in the Yape at the post office and taking the bags from the Yape at the stop at Santa's house. The booking website was not used. The service was not by reservation but had been planned in advance using the Control Room (LFMP). The opening and closing of the Yape lid define the beginning and end of a delivery trip. Data about the delivery trips and KPI were downloaded at the end of each day.
2. In the pedestrian area in the Trikala city centre, a fleet of Yapes delivered newspapers to the shopkeepers in the area, starting from the deport/control room. The operator in the control room loads a certain number of newspapers into each Yape, the Yapes make multi-stop round trips. At each stop a shopkeeper opens the lid of the Yape, picks up a newspaper, closes the lid and the Yape continues to the next stop. The Yape then returns to the control room. Trips are planned in advance and were not by reservation. The booking website was not use. When the Yape arrives at a stop near a shop, Yape emits a sound

‘Arrived’ or a Lound music to signal its presence to the shopkeeper. The start of a delivery trip is defined by the instant the Yape lid is opened and ends the next instant it is closed. Data about the delivery trips and KPI were downloaded at the end of each day.

3. In the pedestrian area in the Trikala city centre, a fleet of Yapes collected coffee residuals from the coffee shops in the area and delivered them in the deport/control room. This is a demand-responsive service. Coffee shop owners use the special reservation system through the Yape booking website. The service request is processed and scheduled. When the order is accepted the Yape moves from the control room to the café shop. It arrives in the vicinity of the shop. It makes a sound. The shop owner opens the lid of the Yape, loads the coffee residue, closes the lid and the Yape returns to the deport/control room. Here the operator unloads the Yape. The Yape is then available for a new service. In the following figure, this service information flow diagram is shown.

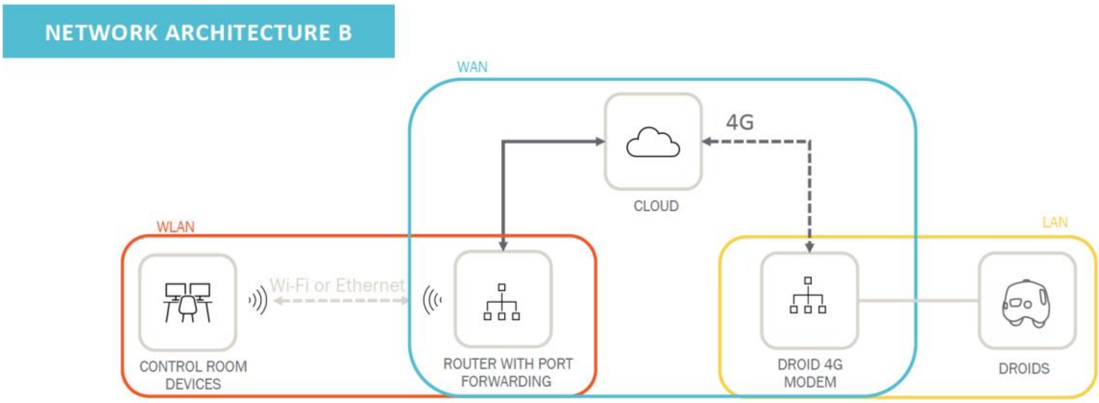


Figure 35: Network architecture zoom-in

As illustrated in Figure 35, the Control Room laptop is connected through Wi-Fi or Ethernet to the network. The droids are connected through their internal modem to 4G network. In this setup, the 4G coverage must be guaranteed on the whole area where the droids are navigating. A fiber-optic connection with a minimum speed of 100Mbps is preferred for the Control Room laptop. A 4G SIM card must be provided for each droid. Port forwarding is needed on the Control Room router towards the laptop IP on the UDP ports from 65000 to 65011 included.

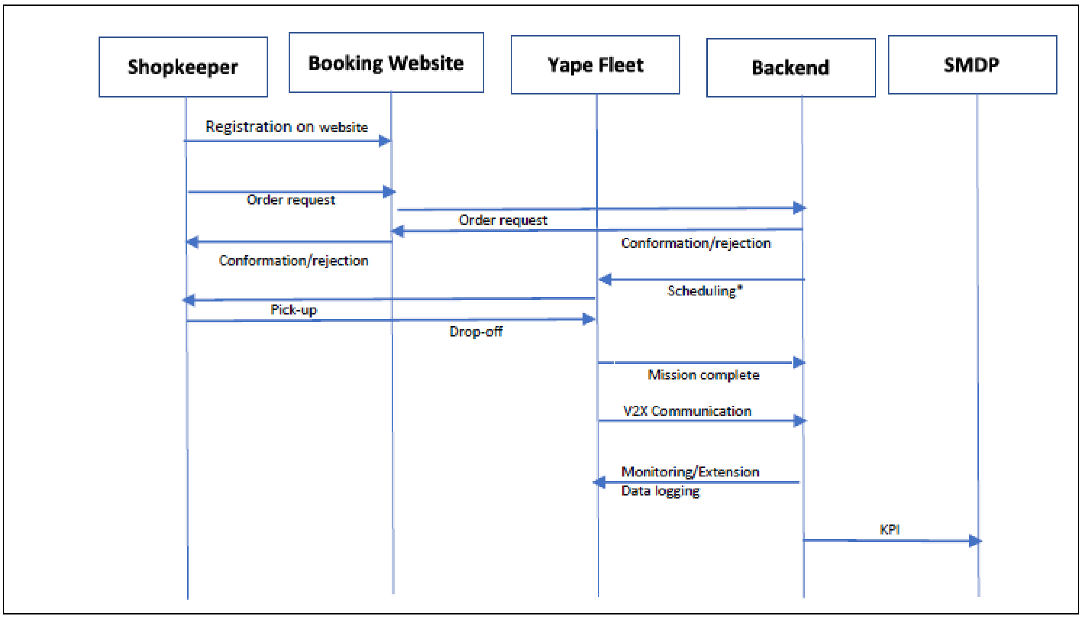


Figure 36: Logistics service information flow (*During scheduling, MapPoint of the shop is selected and Yape fleet automatically selects the shortest path (in predefined Yape path) from control room to the shopkeeper)

In the following three diagrams (Figure 37, Figure 38, Figure 39) more details for each step of the logistics' process is provided, namely about Delivery process creation, Parcel loading and Parcel delivery.

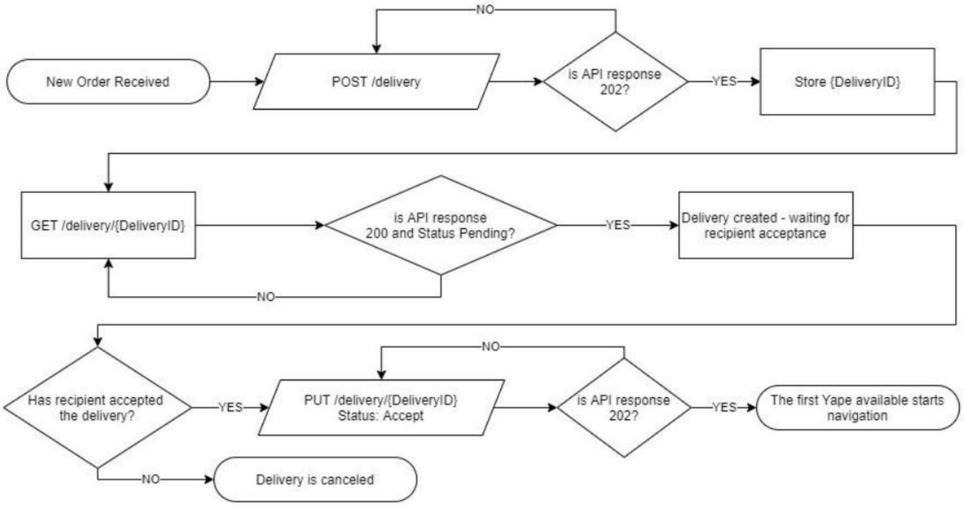

New Order Received
POST /delivery
NO
is API response 202?
YES
Store {DeliveryID}
GET /delivery/{DeliveryID}
is API response 200 and Status Pending?
YES
NO
Delivery created - waiting for recipient acceptance
Has recipient accepted the delivery?
YES
PUT /delivery/{DeliveryID} Status: Accept
NO
is API response 202?
YES
The first Yape available starts navigation
NO
Delivery is canceled

Figure 37: Delivery creation

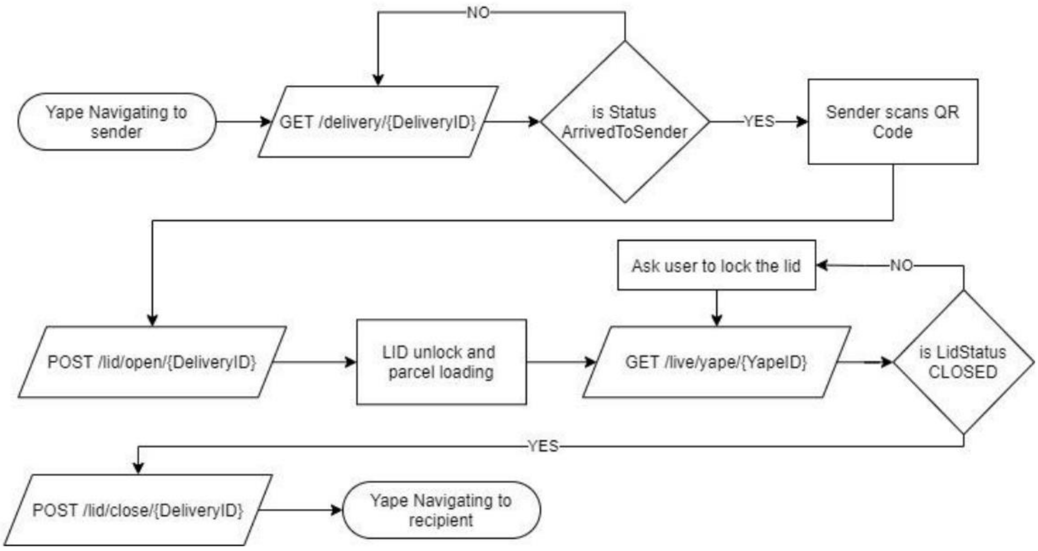

NO
Yape Navigating to sender
GET /delivery/{DeliveryID}
is Status ArrivedToSender
YES
Sender scans QR Code
Ask user to lock the lid
NO
POST /lid/open/{DeliveryID}
LID unlock and parcel loading
GET /live/yape/{YapeID}
is LidStatus CLOSED
YES
POST /lid/close/{DeliveryID}
Yape Navigating to recipient

Figure 38: Parcel loading

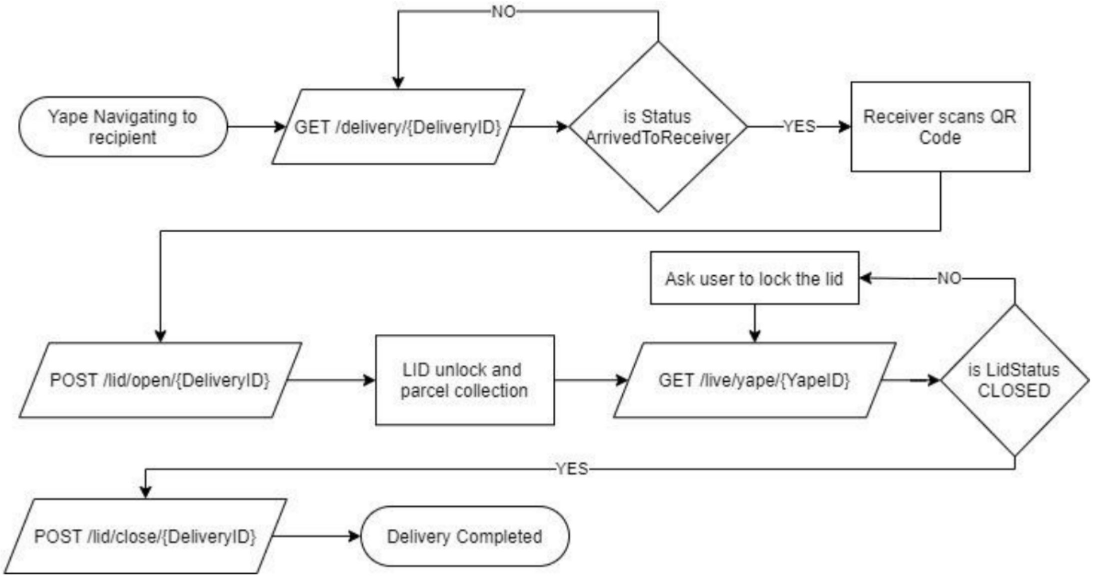

NO
Yape Navigating to recipient
GET /delivery/{DeliveryID}
is Status ArrivedToReceiver
YES
Receiver scans QR Code
Ask user to lock the lid
NO
POST /lid/open/{DeliveryID}
LID unlock and parcel collection
GET /live/yape/{YapeID}
is LidStatus CLOSED
YES
POST /lid/close/{DeliveryID}
Delivery Completed

Figure 39: Parcel Delivery

4.9.3.3 Last mile service (focus on VRU interaction)

In Trikala site, two solutions for the interaction of CAVs with VRUs will be evaluated. One solution where a VRU (in this case a pedestrian) is being detected via the infrastructure in a signalized pedestrian crossing and this information is then conveyed to all nearby connected vehicles using G5 DSRC communications. The detector sensor is a camera attached to an RSU and when a pedestrian is detected crossing the road a relative DENM message is transmitted, increasing the surrounding awareness of all connected vehicles in the area. The information flow of this solution is presented in Figure 40.

The second solution regarding VRU interaction with CAVs involves direct communication between them. An update on D4.3 is that this solution will not be evaluated with a pedestrian VRU carrying a special handheld device, but with rider on an electric scooter. The device is installed to the scooter, so it essentially plays the role of an OBU in this case servicing a VRU actor. In this particular e-scooter in addition to the conventional audio and visual warnings to the rider in dangerous situations, there is also the possibility of automated emergency brake. The modification to the initial solution plan with a connected pedestrian, was made in order to cover a different VRU group than with the first solution and to explore the benefits of automated functions even in VRU cases. Also, it is more realistic that a VRU vehicle (bicycle, e-scooter etc.) is fitted with such a special device than a pedestrian carrying it. The information flow of this solution is presented in Figure 41.

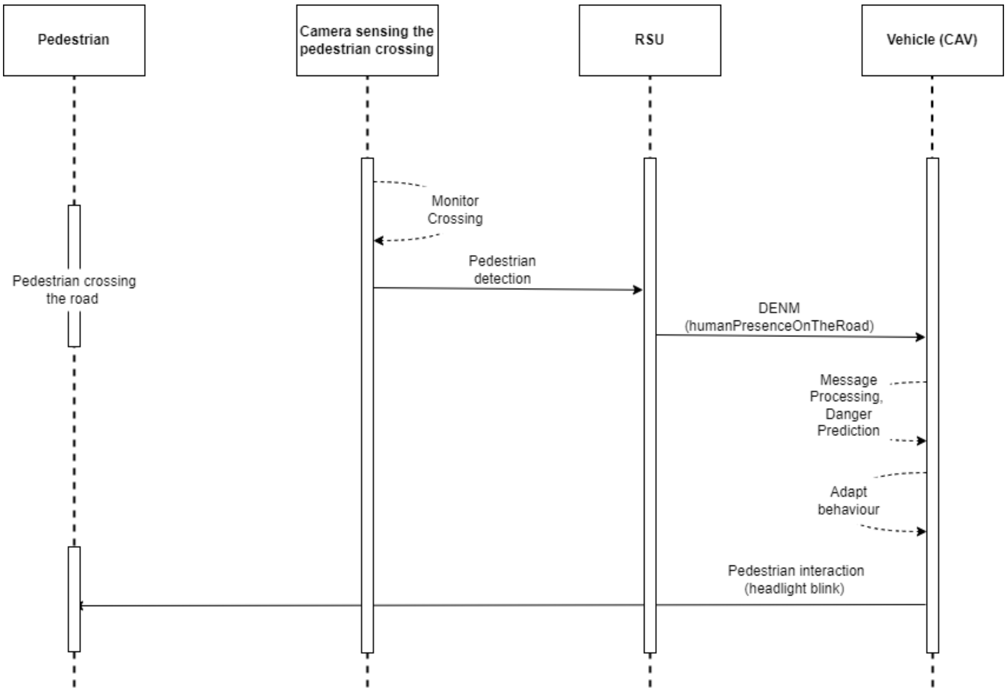

Pedestrian
Camera sensing the pedestrian crossing
RSU
Vehicle (CAV)
Monitor Crossing
Pedestrian detection
Pedestrian crossing the road
DENM (humanPresenceOnTheRoad)
Message Processing, Danger Prediction
Adapt behaviour
Pedestrian interaction (headlight blink)

Figure 40: Service information flow (VRU pedestrian crossing, sensed by infrastructure)

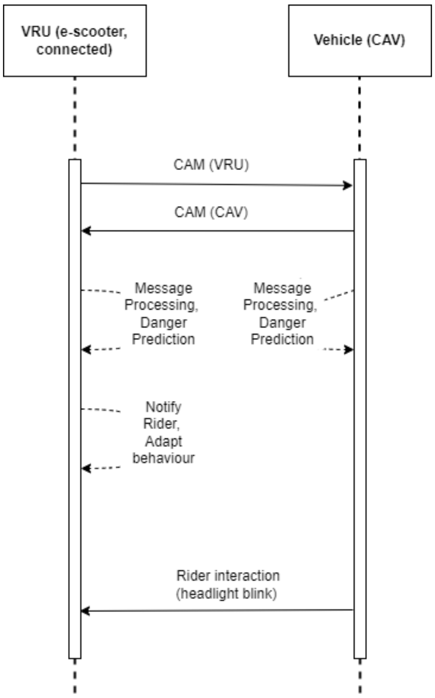

VRU (e-scooter, connected)
Vehicle (CAV)
CAM (VRU)
CAM (CAV)
Message Processing, Danger Prediction
Message Processing, Danger Prediction
Notify Rider, Adapt behaviour
Rider interaction (headlight blink)

Figure 41: Service information flow (VRU e-scooter interaction)

4.9.4 Special aspects: Custom Interoperability, Connectivity, Cybersecurity solutions applied (if applicable)

Bilateral continous communication between the AVs and the RC center that supports real time alerts' monitoring by the RC center has been already described in sec. 4.12.2 above.

4.10 Brno local architecture

4.10.1 General updates focusing on the LFMP side

The vehicle fleet in Brno consists of three automated vehicles. One of them is a retrofitted Hyundai i40 sedan equipped with autonomous driving technology stack, two other ones are autonomous shuttles. All of these vehicles can be driven manually if necessary. The safety driver is always present behind the steering wheel and ready to take over the vehicle if needed. All vehicles are connected via LTE (4G or 5G) network to a remote centre from which a supervisor can monitor each vehicle. The remote centre also has a capability to remotely steer the vehicles. There is no other communication between the vehicles and external infrastructure.

The vehicles operate in a mixed traffic consisting of other vehicles, pedestrians, and cyclists. There is a variable number of stops, ranging from two to five stops, depending on the route. The service runs based on a timetable, therefore there is no option to book the vehicles in advance, it is a first come, first served mode. If the demand increases, vehicles can operate in pairs, effectively doubling the capacity. Otherwise, the vehicles run on their own separately. Passengers can approach the vehicle at each stop and board it. If needed, a safety driver can assist with the boarding process (for example, helping with a baby stroller).

Information about the local actors and their connectivity profile is summarized in Table 10.

Table 10: Local actors and their connectivity profile

Actor	Role	Connectivity
Vehicle 1, 2, 3	Part of DRT service for passengers	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	-
Passengers	Users of the service	No connectivity

4.10.2 Description focusing on the LFMP Dashboard/RC center (if applicable)

Local Fleet Management Platform or Remote Center allows a remote supervisor to assess the driving condition of each vehicle. If needed, the Center allows to steer the vehicle remotely. This functionality helps to deal with situations that are challenging for autonomy. In the future, when it becomes legal to operate autonomous vehicles without safety drivers onboard, this remote center can be foreseen as a possible substitute for safety drivers in the vehicle.

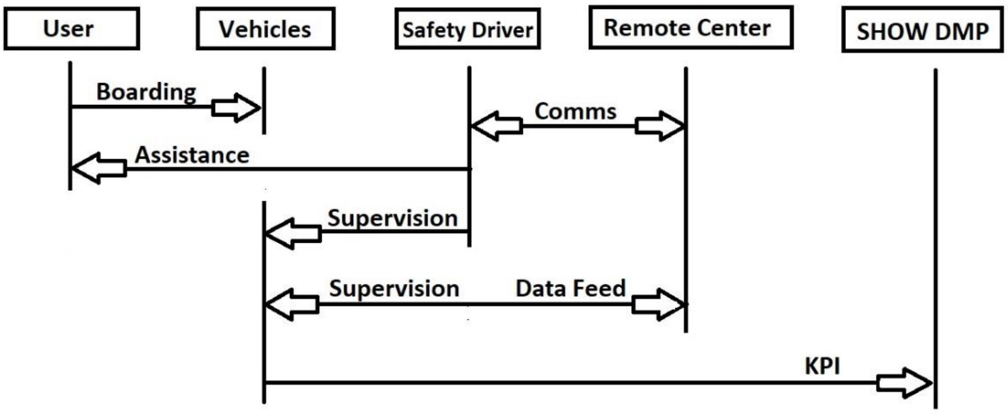


Figure 42: Information flow diagram for Brno

5 Cybersecurity updates and lessons learnt (CERTH-ITI, UNIGE, RI.SE, ICCS)

In this Chapter the updates of the last year with respect to cybersecurity are presented. More specifically, one of the main outcomes of the aforementioned period is the formulation and circulation of a cybersecurity best practices document related to automotive applications (more information in APPENDIX II). Moreover, in the next subsections the three cybersecurity defence frameworks (network-based IDS, Machine Learning Framework for Explainable and Generalized Automotive Intrusion Detection System, Cybersecurity and Data Privacy Assessment Framework) are described and particularly for the network-based IDS (also analyzed in more details), the respective deployment to the SHOW cloud infrastructure and to two pilot sites is also described. Finally, in the last subsection, a summarizing analysis upon a specific cybersecurity questionnaire (APPENDIX III) based on a similar questionnaire from Avenue project, which was shared to the SHOW pilot sites, is performed along with a comparison with the Avenue project.

5.1 Network-based IDS

An intrusion detection system (IDS) is a security tool that monitors network systems against malicious activity. It is designed to detect and alert in case of unauthorized access, misuse, and other malicious actions that may threaten organization's assets. There are two main types of IDS: network-based IDS (NIDS) and host-based IDS (HIDS).

A network-based IDS (NIDS) monitors network traffic and analyzes it for signs of malicious activity. It is typically deployed at strategic points within a network, such as a gateway or a firewall, and aims to monitor traffic for all devices existing in the network. A host-based IDS (HIDS) is installed on individual hosts or devices and monitors activity on that specific host. It is designed to protect against attacks such as malware or unauthorized access by a user. Both NIDS and HIDS use various techniques to detect threats, such as examining network traffic for patterns that indicate a potential attack, analyzing system log files for unusual activity, and comparing activity against a set of rules or signatures that define normal behavior. When a threat detected, the IDS can alert security personnel and take action to prevent or mitigate the threat.

Within activity A4.4, an Intrusion Detection System (IDS) that utilizes the predictions generated by a neural network has been developed. The proposed IDS receives data from network traffic in real-time, providing a dynamic and efficient method of detecting potential security threats. The suggested methodology involves the selection of a suitable dataset for training the neural network model, the design and implementation of the experimental procedure, and finally, the evaluation of the performance of different models. The process used to generate predictions of network activity along with the methodology to evaluate the performance of the final model are outlined. The research and development of this IDS system was carried out with a rigorous scientific approach, ensuring the integrity and robustness of the system.

5.1.1 Methodology

In this section, the methodology followed for the creation of the Artificial Intelligence based IDS is presented. One of the main features taken into consideration is the planning phase. This is a very crucial step for the deployment considering factors such as the network architecture, the types of threats that the IDS will need to detect, and the resources available for the IDS. Additionally, it is important to decide the AI technology used to ensure that the necessary hardware and software resources were available to support it.

A key aspect of an AI-based IDS is the ability to analyze large amounts of data in real-time to identify patterns and anomalies that may indicate a threat. Therefore, it is important to ensure that the IDS has access to a sufficient amount of data and these data are properly formatted and prepared for analysis. Next step of the methodology refers to the way in which the artificial intelligence model will be trained. This procedure includes the decision to use among three machine learning types, namely supervised learning, unsupervised learning, or semi-supervised learning. The optimal way to classify different types of attacks is by using supervised learning and for this reason the appropriate data set was used. Following the common practices in machine learning problems, the data set was divided into training data and testing.

The next step is of utmost importance, since this is the validation and fine-tuning of the AI models to ensure that they are functioning according to their purpose achieving accurate predictions. This may involve also adjusting the parameters of the AI model or adding more epochs during training process (in case of deep learning model which is also the proposed case). Once the AI model has been fine-tuned, the IDS can be deployed and configured to monitor the network for threats. This may involve setting up rules, signatures, and thresholds for the IDS. Lastly it is important to continuously monitor the IDS's performance and to have an incident response plan against possible threats.

5.1.2 Dataset

The CSE-CIC-IDS2018 dataset [9][9] is a collection of network traffic data having been captured during a simulated cyberattack on a computer network. It was created by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick as part of a research project to study the effectiveness of intrusion detection systems (IDS). The dataset includes both normal and malicious traffic and is intended to be used for evaluating the performance of IDS algorithms.

The CSE-CIC-IDS2018 dataset consists of approximately 7.9 million network traffic flows, each of which contains information about the source and destination IP addresses, port numbers, and protocol used. The training set includes normal and malicious traffic data that can be used to train an IDS algorithm, while the testing set includes traffic data both normal and malicious in similar distribution with training set that can be used to evaluate the performance of the trained IDS algorithm. The dataset is designed to be representative of real-world network traffic and includes a variety of different attack types.

Before splitting the dataset into training and testing, a tool for cleaning the data was created. Specifically, this tool removed records with invalid values, managing to delete approximately 59.000 records. From the total number of 7.89 million data a random sample of 13.500 were used representing 1.7% of the dataset, due to hardware resources constraints. Of the 13.500 data, 88.9% were used for model training and 11.1% for testing. Below is the table displaying the corresponding percentages of each class.

Table 11: Types of attack in the dataset

Class	Training Dataset (%)	Testing Dataset (%)
Benign	11.0	10.53
Bot	11.05	10.07

Class	Training Dataset (%)	Testing Dataset (%)
DoS attacks-Hulk	11.1	9.67
Brute Force -Web	8.21	7.53
Brute Force -XSS	3.01	3.53
SQL Injection	1.17	1.07
Infilteration	10.96	10.93
DoS attacks-Slowloris	10.97	10.08
FTP-BruteForce	10.87	11.73
SSH-Bruteforce	10.9	11.43
DDOS attack-HOIC	10.76	12.67

As observed from Table 11, the data between the different classes were balanced so that the prediction of the model is as objective as possible. The 2 types of attacks Brute Force-XSS and SQL Injection present deviation approximately 8.5% from the mean of the training set and 8.2% from the mean of the testing set. This happens because these two types of attacks rarely appear in a modern infrastructure, and it is more difficult for someone to represent them in order to create the necessary data. For this reason, the distribution of the classes should be balanced between the training and the testing set so that the predictions of the model are accurate and representative.

5.1.3 Experimentation

This section describes the experimental procedure followed, the algorithms chosen, the equipment for the experiments and the model comparison. The model architecture chosen in order to create the proposed IDS is Transformer due to its excellent performance in many contemporary and complex problems [10]. Transformer neural networks are a type of deep learning model that has been very successful in natural language processing tasks. The architecture of transformer neural networks is based on self-attention mechanisms and multi-headed attention. These mechanisms allow the model to effectively process input sequences and capture dependencies between different elements of the input.

The architecture of a transformer model consists of an encoder and a decoder. The encoder processes the input sequence and generates a set of hidden states, which are then used by the decoder to generate the output sequence. The encoder consists of a stack of identical layers, each of which includes a self-attention mechanism and a feedforward neural network. The self-attention mechanism allows each element of the input sequence to attend to all other elements, weighting them based on their relevance. This allows the model to capture long-range dependencies in the input.

The feedforward neural network processes the weighted input and generates a set of intermediate hidden states. The decoder also consists of a stack of identical layers, each of which includes a self-attention mechanism and a feedforward neural network. Additionally, the decoder also takes as input the hidden states generated by the encoder. This allows the decoder to incorporate information from the entire input sequence when generating the output. Five different transformer models are tested, and their corresponding results are presented in the following subsections. These transformer models are: GPT-2[11], XLNet [12], BERT [13][13], Roberta [14][14], XLM-Roberta [15][15] and their results are listed in both prediction accuracy and execution time.

5.1.3.1 Training Phase

The goal of the training phase is to find a set of parameters for the Transformer model that minimizes the difference between the model's predictions and the ground truth labels for a given dataset of network traffic records. This is achieved through the optimization of an objective function, which measures the model's performance according to a chosen metric. In this case, the objective function is chosen to be the prediction accuracy of the model.

During training, the model receives a batch of input data, and its output is compared to the corresponding labels using a loss function. The loss is then backpropagated through the model, and the model's parameters are updated in a way that reduces the loss. This process is repeated for multiple epochs, until the model reaches a satisfactory level of performance (is in convergence). In addition to minimizing the loss, the model may also be trained to optimize other metrics, such as accuracy, precision, or recall. The choice of loss function and optimization metrics depends on the specific task for which the model is being trained for, as well as the characteristics of the dataset and the desired performance of the model.

The training process begins by initializing the model's parameters randomly. Each model then receives a batch of input data and its corresponding labels, and the model's predictions are compared to the ground truth labels using the chosen loss function. The results of the comparisons between the various Transformer models used are presented in Figure 43 & Figure 44. The accuracy of the models per epoch, is displayed in Figure 43. Similarly, Figure 44 illustrates the loss function, also by epoch.

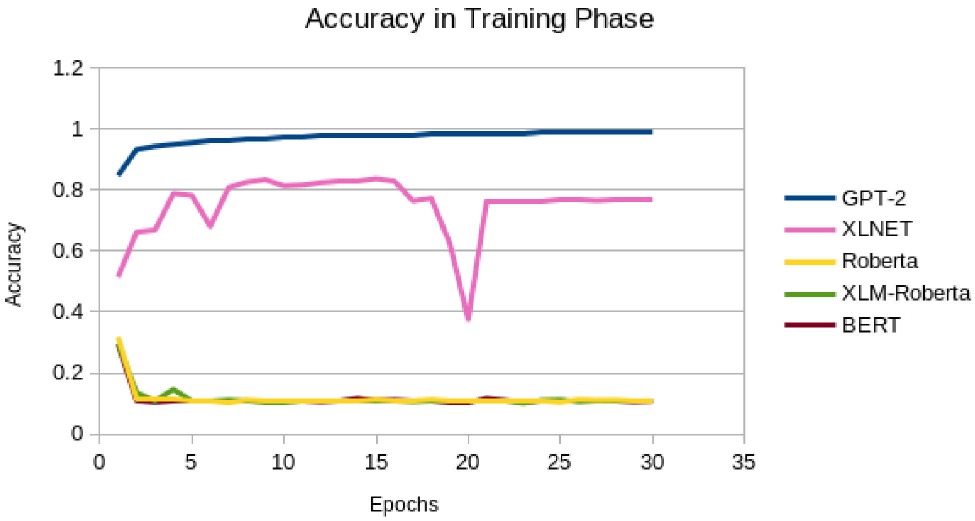


Figure 43: Accuracy per Epoch in training phase

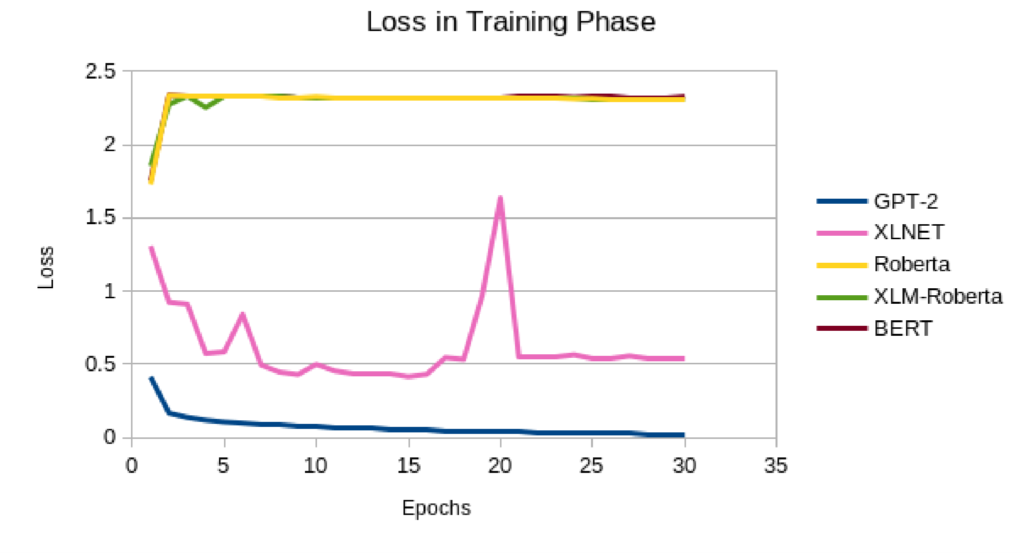


Figure 44: Loss per Epoch in training phase

The Transformer models were trained for 30 seasons, a period of time that is considered to be sufficient for 13,500 data so that the classification could be done effectively. As can be seen from the figures, GPT-2 is the one with the highest learning stability and the highest degree of effectiveness. XLNET presents a relatively high accuracy but with large variations in its accuracy. The rest of the models seem to have worse performance since they have a high loss rate with an extremely low prediction rate.

5.1.3.2 Testing

Throughout the training process, the model's performance is regularly evaluated on a testing set, in order to track its progress and identify possible overfitting or underfitting. When the model's performance on the testing set has reached a satisfactory level, the model can be considered trained and is ready for deployment. Figure 45 shows the accuracy of the models by epoch, while Figure 46 shows the loss in relation to epochs.

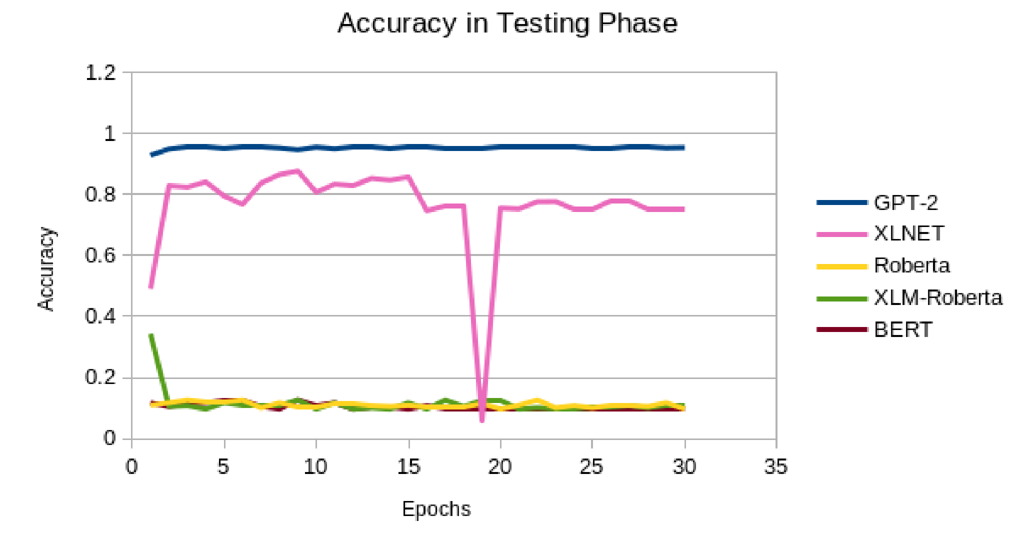


Figure 45: Accuracy per Epoch in testing phase

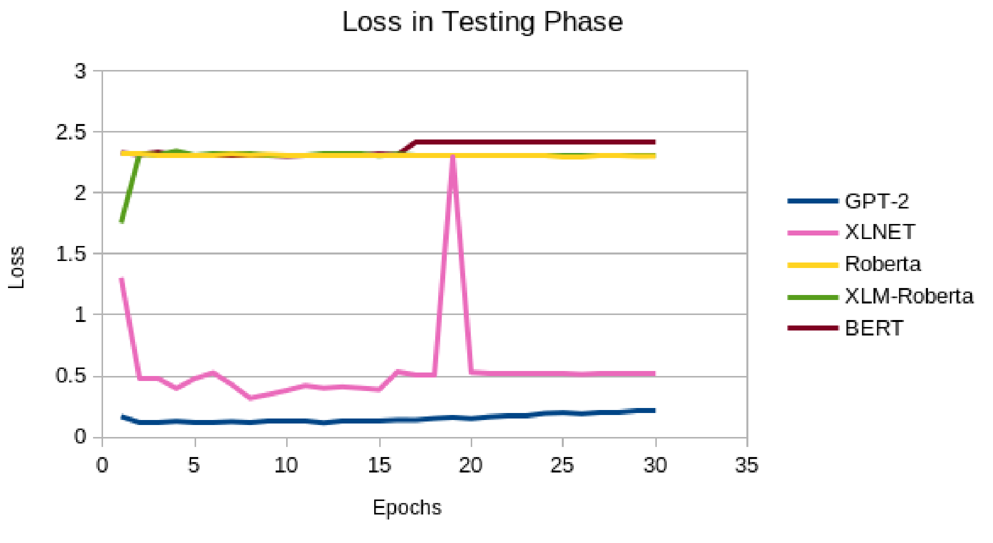


Figure 46: Loss per Epoch in testing phase

5.1.3.3 Comparison

The table below presents the results from the comparisons between the models. Specifically, the maximum prediction accuracy of each model in testing, the epoch it was achieved and the time it took to train are presented.

Table 12: Comparison of efficiency and training time between the models

Model	Accuracy (%)	Loss	Epoch	Training Time (hour:min:sec)
GPT-2	95.93	0.1274	15	07:00:08
XLNET	87.73	0.3484	9	08:09:24
Roberta	12.66	2.3101	6	05:41:16
XLM-Roberta	34.33	1.7759	1	05:40:19
BERT	12.67	2.3151	5	05:15:08

From Table 12 it is clear that the most effective model for the classification of network traffic is GPT-2. Although the training time is one of the longest, the efficiency is a factor that makes it the optimal choice for the application in the IDS.

5.1.4 Deployment

The following section provides a detailed description of the Intrusion Detection System (IDS) having been developed within SHOW and how it can be deployed. More specifically, the process of capturing packets in real-time, the tools utilized for this purpose, and the development of the corresponding custom software that incorporates all of the above-mentioned functions are presented. Finally, this section explains briefly the methodology for network-based intrusion detection, as well as the whole procedure needed to be performed (communication, system requirements and installation) for the deployment of this solution to pilot sites. The procedure of deployment has been performed in SHOW cloud infrastructure and communication with pilot sites of Madrid and Trikala has been performed for the respective deployment.

5.1.4.1 Network monitoring

Regarding network monitoring performed by the proposed IDS, initially, the user has the option to specify the: a) network interface, b) IP address, and c) port or range of ports that will be inspected from the IDS. However, the default configuration of the proposed solution is to automatically detect these parameters. Specifically, if a network interface is not specified, it will be automatically detected by the system. Similarly, if the IP address or the ports to be monitored are not defined, the IDS will detect the public IP and scan it for open ports. If none of the ports are open to a public network, the default range of 1-1024 will be automatically set as the ports to be monitored. Subsequently, real-time monitoring of the network commences. Through the utilization of the open-source tool cicflowmeter, related features are extracted from network packets, which serve as inputs for the neural network in order to detect intrusions.

5.1.4.2 Network packets assessment

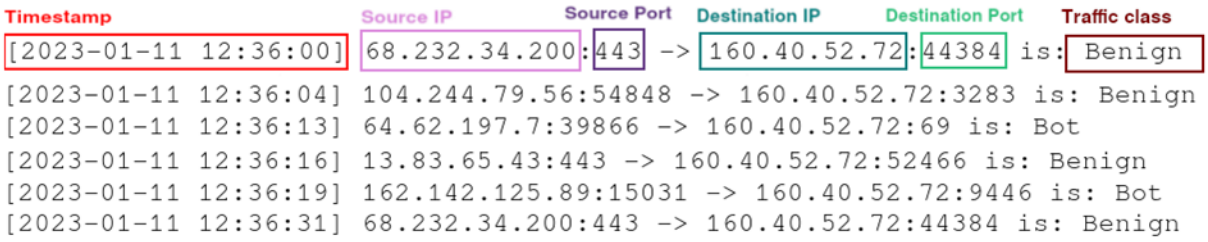
The suggested experimental procedure involves a comprehensive evaluation of various Transformer models in order to identify the model that exhibits the highest prediction accuracy. This model is then selected as the primary component for generating predictions of the network activity. The selection process is conducted using a controlled experimental design and statistical analysis, ensuring that the chosen model is robust and reliable for the intended purpose. To apply the desired model as the core of the proposed IDS this was saved as a pre-trained model. A pre-trained Transformer is a machine learning model that has been trained on a large dataset prior to being used for a specific task, in this case the network intrusion detection. The pre-training process involves learning the underlying patterns in the network packets and building a representation of it, which can be used to make predictions or decisions with respect to network security.

Upon the capture of network packets, these are transformed into tensors through a tokenization process, allowing them to be input into the neural network. This transformation necessitates the utilization of complex mathematical operations, not only for the conversion of the data into tensors, but also for the subsequent inverse process. The prediction result is derived from the data patterns and is one of the 11 following classes (one safe, one neutral and nine types of attacks): Benign, Infiltration, Bot, DoS attacks-Slowloris, DoS Attacks-Hulk, FTP-Brute Force, Brute Force-Web, SSH-Brute force, Brute Force-XSS, DDOS attack-HOIC, SQL Injection.

5.1.4.3 Log files and Alerts

After the model has completed its assessment, the user's console will display a variety of information about the network traffic. The timestamp of the event is prominently displayed, allowing the user to easily understand when the event occurred. Additionally, the type of network traffic is also displayed, allowing the administrator to quickly identify whether the traffic is benign or malicious and to determine the situation severity.

The IP address and port from which the data is sent, as well as the IP address and port that receives the data, is also displayed on the console output. This information is crucial in identifying the source and destination of the network traffic, which can aid in determining the intent of the traffic. As an example, the IDS console output may show:



```
[2023-01-11 12:36:00] 68.232.34.200:443 -> 160.40.52.72:44384 is: Benign
[2023-01-11 12:36:04] 104.244.79.56:54848 -> 160.40.52.72:3283 is: Benign
[2023-01-11 12:36:13] 64.62.197.7:39866 -> 160.40.52.72:69 is: Bot
[2023-01-11 12:36:16] 13.83.65.43:443 -> 160.40.52.72:52466 is: Benign
[2023-01-11 12:36:19] 162.142.125.89:15031 -> 160.40.52.72:9446 is: Bot
[2023-01-11 12:36:31] 68.232.34.200:443 -> 160.40.52.72:44384 is: Benign
```

Figure 47: Intrusion Detection System console output

This output allows the user to check the traffic, in real time, and take actions if necessary, or review past traffic. The user has the capability of filtering or searching specific records, which could be useful in identifying patterns or anomalies. It is important to note that this output is generated by the IDS system based on the predictions made by the model and is intended for use by authorized personnel with the necessary cybersecurity knowledge and training to properly interpret and act upon the information.

After the threat detection (network traffic classified not as "Benign" category), a CSV file is generated and stored for the purpose of further analysis and investigation of the traffic data. This measure is implemented as a means to safeguard the system and network from potential cyber threats. The CSV file will provide a detailed record of the network activity, allowing for in-depth analysis of the incident and any necessary follow-up actions.

In addition to the network traffic data, the CSV file also documents and records the IP address associated with the detected malicious activity. This information is crucial in identifying the source of the attack, and assists in the determination of the appropriate measures to be taken in response. The specific request or action that was deemed hostile will also be recorded in the CSV file, allowing for better understanding of the nature of the attack and the methods used.

Moreover, this information will be useful for ongoing monitoring and continuous security improvements, and could be shared with relevant authorities, law enforcement agencies and other teams in charge of incident response, in order to coordinate and mitigate security breaches.

5.1.4.4 REST API

The proposed system offers the capability of identifying malicious network traffic as a RESTful API service. The data collected from the computer whose network is monitored will be securely transmitted using the HTTP protocol to the server running the aforementioned pre-trained Transformer model. After the transmission, the model existing in the server processes the input and generates a prediction as the response. The prediction will be returned in a standardized format such as JSON, allowing for easy integration with other systems. The REST API also includes authentication and authorization mechanism to ensure the secure transmission of data.

Given that the communication with the server responsible for assessing network traffic will be conducted via API call, the standard ports utilized by the HTTP protocol are needed. Consequently, as long as ports 80 and 443 remain open, communication will proceed without any problem.

5.1.4.5 System Requirements

To ensure successful installation of the application to the computer, the Python 3.9 version or later is needed. In order for the designated service to operate effectively, one of the following operating systems should be pre-installed in the computer: Ubuntu 20.10, Ubuntu 22.10, Ubuntu 24.10, Debian10, Debian 11, Arch x86_64.

5.1.4.6 Installation

For the installation of the proposed IDS a python setup script has been created to automatically detect the operating system and to install the relevant application. Subsequently, this script creates a systemd service within the directory /etc/systemd/system and activates it automatically. This service will be run automatically upon system startup and will not necessitate any additional actions. It is important to note that the user must have administrator privileges when running this script in order for the IDS to successfully be installed.

5.2 Machine Learning Framework for Explainable and Generalized Automotive Intrusion Detection System

5.2.1 Methodology description

The current in-vehicle networks (IVNs) are vulnerable to various external attacks due to the lack of security features, mandating the need for a robust intrusion detection system (IDS). Although many machine learning (ML) solutions have been proposed in the literature for intelligent Intrusion Detection Systems (IDS), the same deployment rate of ML-based IDS solutions in the automotive industry is still in progress. Moreover, the advances in ML techniques, such as random forest (RF), artificial neural networks, support vector machine (SVM), ensemble learning, and clustering techniques, have increased the popularity of such solutions for use in IDS. Still, the current state-of-the-art ML models for automotive IDS lack generalizability across different vehicle vendors. Figure 48 illustrates the contrast between deploying a traditional ML-based IDS and a generalized ML-based IDS.

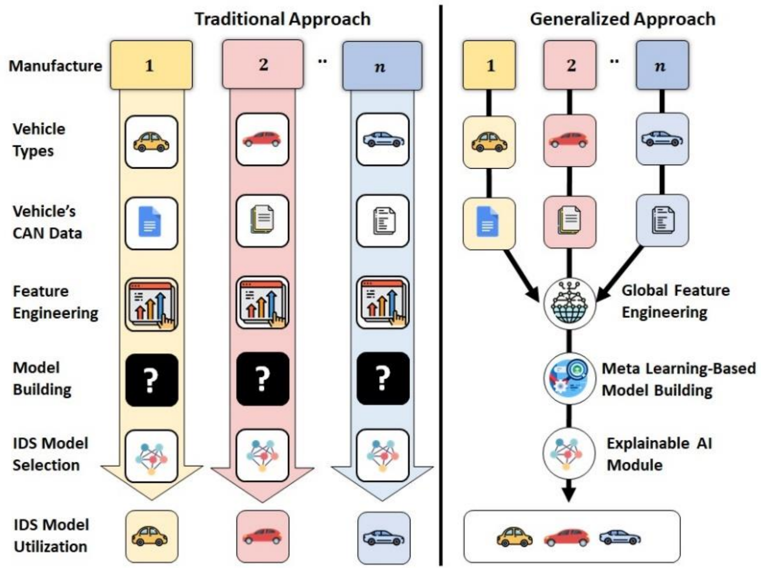


Figure 48: Proposed framework

Based on Figure 48, the key aspects of the traditional ML-based IDS and generalized ML-based IDS are as follows,

- In traditional ML-based IDS, the feature engineering operation occurs stand-alone, and the respective ML-based IDS systems are built separately to generate vehicle manufacturer-specific IDS design. As a result, such IDS solutions suffer from low scalability as the ML model cannot be generalized across all the datasets of different vehicle manufacturers. Although machine learning/artificial intelligence-based solutions give effective management solutions, the algorithms' "black box" character makes it difficult to gain enough trust in their use.
- For both the traditional and generalized IDS solutions, researchers/engineers need to better understand the ML models' optimization process i.e., how, why, and when the learning model made certain decisions in a given environment. More specifically, the deep learning (DL)-based automotive IDS systems' or pipelines' decisions should be trustworthy and justified. Nevertheless, in the case of traditional ML-based automotive IDS, the explainability feature is missing as compatible to the generalized ML-based automotive IDS due to the lack of generalizability.

Under the above circumstances, the current research work focuses on developing generalized explainable AI solutions for the automotive IDS:

- A combination of cloud and on-vehicle machine learning framework for explainable and generalized automotive IDS is proposed. The proposed framework facilitates explainability by applying SHapley Additive exPlanations (SHAP) to identify model parameters and feature importance. This approach is leveraged in the proposed model generalization of automotive IDS.
- A cloud-based meta-learning scheme is proposed to autonomously construct and choose the most suitable IDS model configurations among many possible configurations. The suitable model is then deployed in the vehicle's on-board unit (OBU) for on-vehicle attack detection.

Using two publicly available standard datasets, extensive experimental analysis is in progress to generate generalized input features and detect anomalies. The efficacy of the proposed approach is prevalent because different datasets across different vehicle manufacturers share a standard set of learning features as a part of the feature engineering process to detect the malicious behavior of heterogeneous vehicles.

5.3 Cybersecurity and Data Privacy Assessment Framework

5.3.1 Research Motivation

The Cybersecurity and Data Privacy Assessment Framework investigates ways to answer to the following research questions:

- How to efficiently mitigate cybersecurity and data privacy threats related to CAVs according to a holistic view of all eventual risks?
- What are the key technical tools recommended by legal policies to countermeasure data leakage risk?
- How risk assessment, vulnerability analysis and penetration testing are conducted to certify the deployed CAVs?
- By being compliant to the existing standards, how robust the CAV would be from both security and data protection perspectives?
- How the existing standards and regulations can be upgraded to cope with the CAV technological evolution and legal requirements?

- How to build the most adequate security certification model with respect to the CAV landscape?

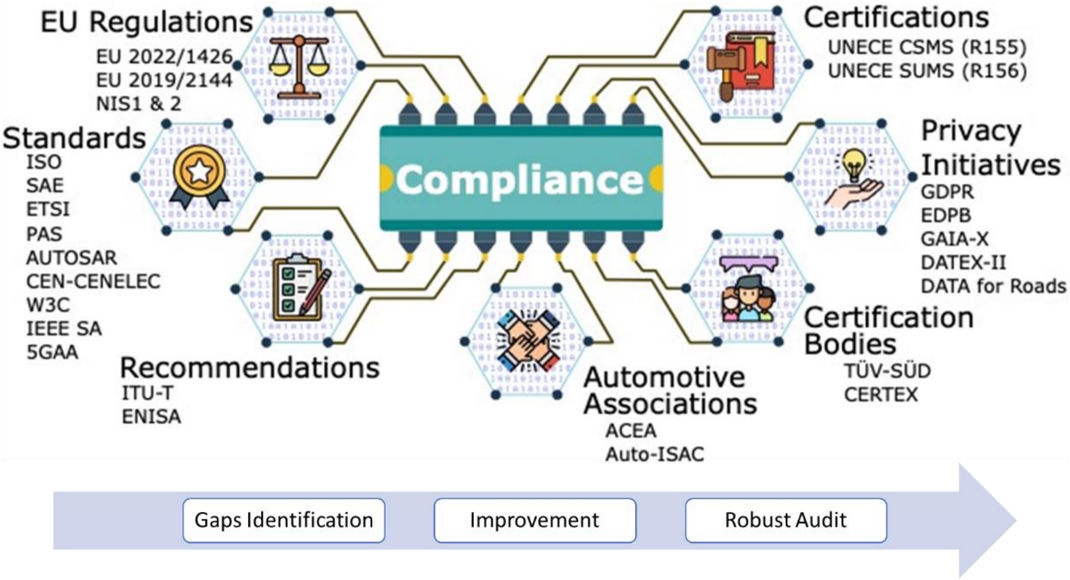


Figure 49: Research motivation

5.3.2 Methodology

The proposed work (Figure 50) aims to provide a holistic view of all the existing cybersecurity and data privacy threats and map them to efficient legal and technical mitigation strategies. Providing in-depth analysis on how the GDPR should be implemented into the driverless environment. Inspired from the PCI-DSS process, interfaces and components that should be audited, will be identified. The motivation is to come up with an innovative set of security & privacy attributes and recommendation model with respect to the cyber security and personal data protection through all the CAV's lifecycle.

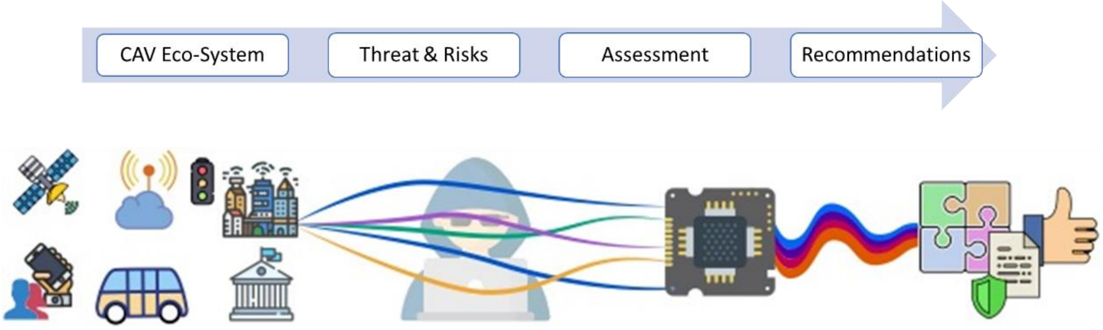


Figure 50: Cybersecurity and Data Privacy Assessment Framework

5.3.3 Continuous efforts

The aforementioned cybersecurity and data privacy assessment framework is an ongoing effort that tries to:

- Investigate gaps and shortcomings of existing standards, regulations and certification schemes (with a main focus on Europe) on cyber security and data privacy.
- Joining regulation committees on (and related to) Connected Automated Vehicles (CAVs) (eg ISO/VSS).

- Enhancing the recommendations based on the most recent technologies to keep pace with the CAV's evolutions.
- Combining and upgrading the most specific standards and regulations to develop a comprehensive compliance and recommendation tool.

Finally, the continuity of these efforts with respect to cybersecurity and privacy is depicted by the various collaboration with other European projects (ENFLATE [5], ULITMO [6], AVENUE [4] , nIoVe [7], GHOST [8][8]).

5.4 Cybersecurity survey analysis and comparison with Avenue

In this subsection, a summary of the pilot sties' answers to the cybersecurity and privacy questionnaire (APPENDIX III Cybersecurity & Privacy Questionnaire) is provided in order to get insights and extract general conclusions regarding these critical issues for each complex system such as the autonomous vehicles. At the end of this subsection, a comparison with the cybersecurity and privacy in the Avenue project as extracted by a similar questionnaire is provided.

First of all, all the pilot sites include dedicated software for autonomous driving in various situations (passenger car, minibus etc.). Therefore, aggregated information from the sites about software security can highlight best practices, research gaps and possible future directions. Regarding source code vulnerabilities, various countermeasures are followed in the pilot sites including source code auditing, and best programming practices. Continuing with penetration testing and adoption of the CVSS [16] for vulnerability scoring, it is clear from the answers that the vast majority of the pilot sites do not use them, since there is no specific need. Another prominent question to be answered is how to face Jamming and Spoofing attack at the GNNS receiver, and for these types of attacks many pilot sites use complementary lidar sensors as a countermeasure. With respect to the existence of regular vulnerability reports and the coordination with the partners, most of the pilots have answered negatively. On the other hand, the cybersecurity training of the corresponding personnel of the autonomous vehicles is of utmost importance for all the pilot sites. Finally, the results in the questionnaire with regard to the cybersecurity standards, regulations and certifications are ambiguous, since some pilots take into consideration them, and several do not.

The analysis of the pilot sites' answers continues with privacy related issues. Hence, the majority of the sites do not use personal data. Moreover, regarding location data, the majority of the pilots do not use encryption, however they use secure communication protocols for the data transmission (SLL, TLS). Moreover, the vast majority of the pilot sites do not share data with Location Based Services except for SHOW Data Management Platform. Additionally, regarding the GDPR and the Federal Data Protection and Information Commissioner (FDIC) compliance, all the pilot sites respect the aforementioned acts adopting where required techniques such as video processing. Finally, in case of data breaches, the majority of the sites have a clear and well-defined procedure and in several cases this procedure is in accordance with the standard ISO27001 and GDPR regulation.

From the analysis of the cybersecurity and privacy questionnaire, it is clear that there is not a common cybersecurity and privacy strategy for all the pilot sites, however they all respect the GDPR & FDIC acts obeying to the obligations coming from these regarding personal data, most of the pilot sites utilize secure communication protocols for data transmission and also have various cybersecurity countermeasures in order be protected against crucial cyber-attacks such as Jamming and Spoofing.

A comparative analysis between the SHOW and the Avenue cybersecurity & privacy architecture is performed below. Before comparing the answers from a similar questionnaire answered by the service providers in Avenue, a brief overview of the Avenue architecture in terms of cybersecurity is provided below. First of all, regarding communication security, the main defense mechanisms to shield it by applying restrictive authentication are the TLS certificates and the cyphered Virtual Private Network (VPN). Furthermore, an important aspect with respect to the in-vehicle security is that the Secure Onboard Communication (SeOc) is the main mitigation tool against common attacks (either in sensor or in the in-vehicle communication) such as Jamming, Spoofing, Sniffing and Man in the Middle attack.

Continuing with the answers of the Avenue service providers in the questionnaire, as in the SHOW project, not all the service providers use the CVVS standard for vulnerability scoring. Moreover, a similar approach with the SHOW project is followed in the Avenue project regarding penetration testing, standards, and certification adoption and thus, there are providers that utilize them and others that do not. Additionally, regarding the privacy issues, the majority of the service providers in the Avenue project hold personal data (since this is inevitable in order to offer in-vehicle services) obeying however to the GDPR standards by utilizing respective encryption technologies. The previous point of personal data holding is the main difference between the two projects, since as mentioned previously, the vast majority of the partners in the SHOW project do not use personal data. However, there is accordance between the two projects in the GDPR compliance where required.

To sum up, it is obvious from the aforementioned that in both projects the indispensable need for cybersecurity and privacy mechanisms is satisfied by powerful and well-established solutions, but there is not a unified and universal cybersecurity strategy that each service provider and respectively each partner follows, either in the SHOW or in the Avenue project.

6 Interoperability aspects and lessons learnt (ITxPT, CERTH-ITI)

Interoperability is a crucial component of the SHOW project, as enables the seamless transfer and exchange of data among the various entities composing the SHOW ecosystem. This ecosystem comprises of 18 pilot sites and a pipeline of different tools and mechanisms that should be able to communicate with each other. To facilitate this communication, it is necessary to establish a common language.

Based on this work of reporting the local sites functional architecture and on discussions with sites, few general remarks can be drawn:

1) Adoption of EU formats, as proposed by ITxPT specifications reviewed in SHOW deliverable D4.1, varied per site, mainly based on CCAM services maturity.
2) Local Fleet Data Management is often the responsibility of the OEMs (i.e. shuttles' providers) and hence the fleet to cloud data format and protocols are proprietary.
3) When connected mobility is deployed via connectivity to infrastructure or other vehicles (V2X), ETSI C-ITS standards are used.
4) At the level of the SHOW **cloud** infrastructure, SHOW could have more control since all data had to be eventually transferred (historic and close to real time) to the SHOW MDP and hence in the communication with SHOW MDP, interoperable data format, standardized interfaces and cloud cybersecurity mechanisms were adopted as proposed by the project.
5) At the level of the local sites' **cloud** infrastructure, a big variety exists among the architectures deployed in the SHOW sites, based on their maturity and commercial components' integration as well as the CCAM use cases under focus. There is no one architecture that fits all solutions.
6) There is a standardization gap for newly emerging use cases including remote fleet monitoring and bilateral communication with the fleet in case of an emergency, for both CAVs equipped with safety drivers and unmanned vehicles and therefore SHOW deployment should be considered as experimental.

Towards the future standardization of CCAM deployment for Public Transport we would make these two additional notes:

- Vehicle data: It is important that the access to vehicle data through EU standards based on PTA/PTO requirements data is supported. If such data are requested by PT operator shall then be made available by OEM either as historic data or real-time feed. This is part of ongoing discussion in the frame of EU data act[1] :
- Mobility data: this is related to NAP (National Access Point) and MMTIS delegated regulation[2] which request to publish mobility data (static one today and dynamic one in coming revision of MMTIS) using EU standards.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

[2] multimodal travel information services : https://eur-lex.europa.eu/eli/reg_del/2017/1926/oj)

6.1 SHOW Data interoperability

Interoperability in the SHOW project enables efficient data transfer between different participants, and for this reason a common readable format for all project participants is of utmost importance. The obstacle of interoperability can be overcome through the development and implementation of data converters, which have been installed within the various components of the SHOW system. The interoperability mechanisms are dedicated in two different classes requiring notable treatment and cautious management:

- **Historical data provision and**
- **Real-time connection**

6.1.1 Historical data provision

The SHOW project includes several pilot sites for which a real-time connection with the SHOW DMP is not the preferred way of data transmission. To address this, an online repository has been deployed as a means for these partners to share their data. The SHOW pilots upload files to the aforementioned repository on a regular basis, typically on a weekly basis. Historical data provision is also available through the SHOW CKAN data management platform uploading CSV files in a specified format. The SHOW online repository can be accessed through the following link: https://show-data-portal.eu/

Due to frequent inconsistency reasons in the data format more effort to achieve interoperability is needed. A representative example is in the LABEL TIMESTAMP where there are various methods by which TIMESTAMP can be represented. The official SHOW TIMESTAMP format is the universal format for time and has the structure: 2023-02-01T14:35:13.

To address these inconsistencies in the uploaded CSV files, **convertors** have been designed for seven pilot sites with the following objectives:

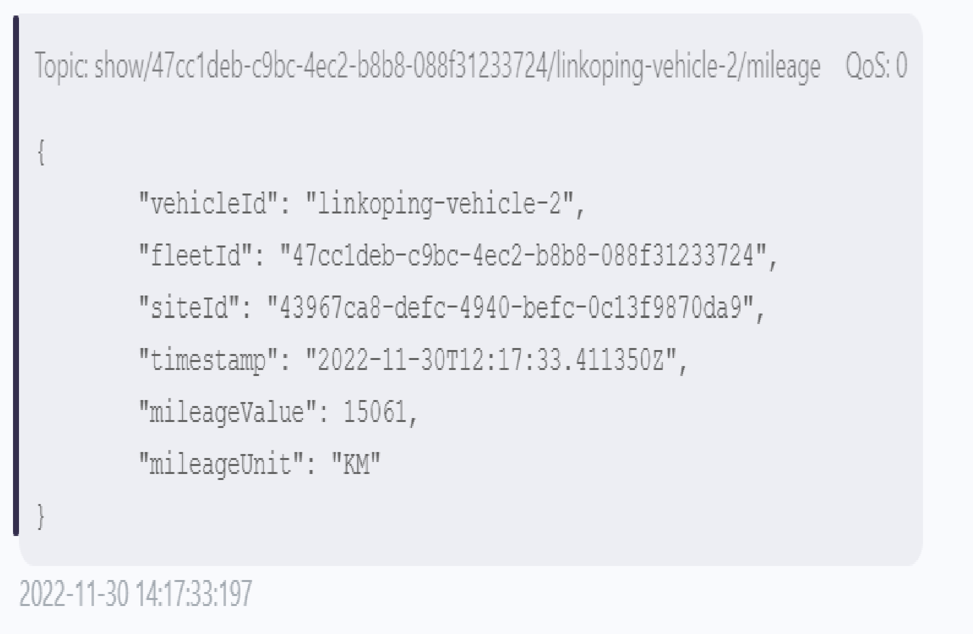
- Adaption to common definitions
- Alignment with the time format of the SHOW DMP
- Utilizing valuable information

6.1.2 Real-time connection

For the realization of the real time connection between SHOW DMP and the pilot site supporting this type of connection, two different mechanisms have been developed in the SHOW project:

- **MQTT**
- **WebSocket**

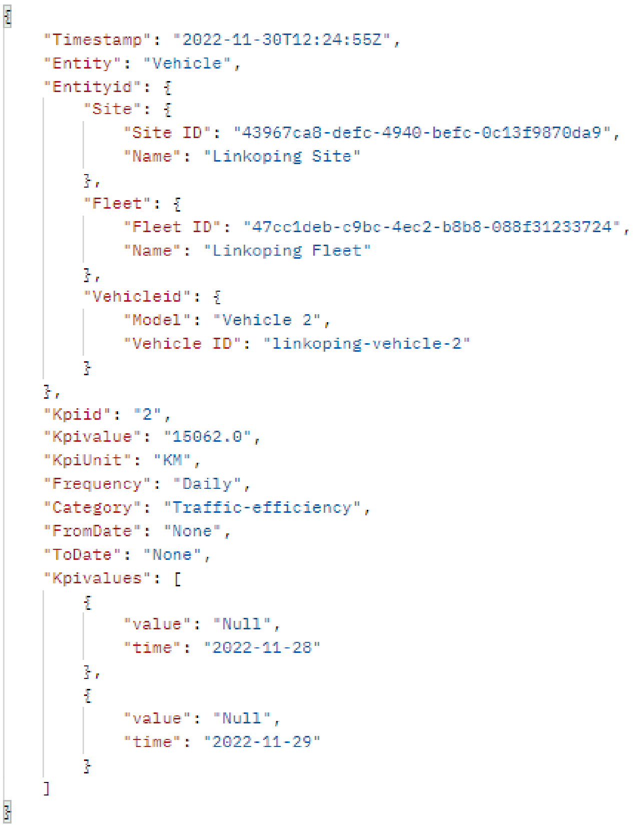
In terms of interoperability, the management of the two methods is similar. As previously mentioned, convertors have been developed to transform the structure of the data into a common format universally understandable among all partners. This indispensable transformation is more urgent in the case of the SHOW dashboard that accepts certain types of data formats in order to display the incoming data and KPIs. For instance, in the following images (Figure 51 and Figure 52), the transformation of the mileage attribute format is displayed in order to meet the desired format required by the SHOW dashboard, allowing for the creation of the "kilometers traveled" KPI.



```
Topic: show/47cc1deb-c9bc-4ec2-b8b8-088f31233724/linkoping-vehicle-2/mileage   QoS: 0

{
        "vehicleId": "linkoping-vehicle-2",
        "fleetId": "47cc1deb-c9bc-4ec2-b8b8-088f31233724",
        "siteId": "43967ca8-defc-4940-befc-0c13f9870da9",
        "timestamp": "2022-11-30T12:17:33.411350Z",
        "mileageValue": 15061,
        "mileageUnit": "KM"
}
2022-11-30 14:17:33:197
```

Figure 51: JSON MQTT Input (mileage attribute)



```
{
    "Timestamp": "2022-11-30T12:24:55Z",
    "Entity": "Vehicle",
    "Entityid": {
        "Site": {
            "Site ID": "43967ca8-defc-4940-befc-0c13f9870da9",
            "Name": "Linkoping Site"
        },
        "Fleet": {
            "Fleet ID": "47cc1deb-c9bc-4ec2-b8b8-088f31233724",
            "Name": "Linkoping Fleet"
        },
        "Vehicleid": {
            "Model": "Vehicle 2",
            "Vehicle ID": "linkoping-vehicle-2"
        }
    },
    "Kpiid": "2",
    "Kpivalue": "15062.0",
    "KpiUnit": "KM",
    "Frequency": "Daily",
    "Category": "Traffic-efficiency",
    "FromDate": "None",
    "ToDate": "None",
    "Kpivalues": [
        {
            "value": "Null",
            "time": "2022-11-28"
        },
        {
            "value": "Null",
            "time": "2022-11-29"
        }
    ]
}
```

Figure 52: JSON API Output (kilometres-travelled API)

6.1.3 Lessons Learned

Figure 52 summarizes all the work with respect to data interoperability and presents all the types of convertors having been developed for the SHOW project so far. The development of interoperability mechanisms is crucial for any project that involves data transfer generated from multiple entities, such as vehicles or fleets, similar to the

SHOW project. Without such mechanisms, communication among the various tools and frameworks in large-scale projects like SHOW cannot be guaranteed. It is not feasible to rely on the use of a common language by default, as there are cases where inconsistencies between partners arise. Therefore, interoperability is an indispensable part of any big data system to facilitate communication between different entities, such as vehicles, APIs, and dashboards.

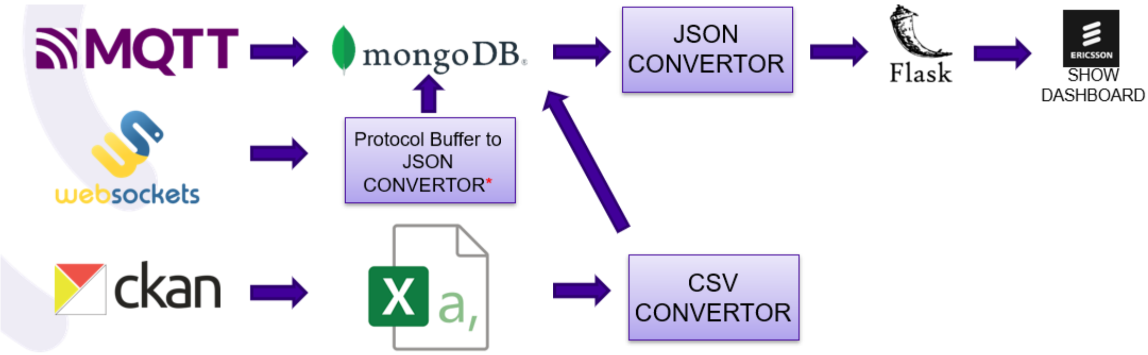


Figure 53: SHOW convertors

7 SHOW Risk Assessment – 3rd Round (CERTH-HIT)

7.1 Introduction

A cross-cutting multi-layered risk assessment is being performed in SHOW **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.

The full methodology has been presented in D4.1: Open modular system architecture and tools - first version and is not repeated herein. Overall, 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** are 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/business** and **demonstration/evaluation** risks are considered, whereas apart from the **horizontal risks, risks associated with specific pilot sites and/or SHOW beneficiaries** are also recognised if and when applicable.

The first 2 rounds of risk assessment and the emerging results have been already presented in D4.1: Open modular system architecture and tools - first version (ICCS, M12) and D4.3: Open modular system architecture - second version (ICCS, M24). The first round corresponded to the risks recognised in view of the technical validation phase of the project, while the 2nd iteration, focused on the identification of the risks in view of the "pre-demonstration" phase.

The third and final iteration of the SHOW risk assessment, reported herein, has been implemented with respect to the final real life pilot phase of the project and the following section presents its results.

7.2 3rd SHOW Risk Assessment Round results

The analytical outcomes of the third risk assessment round in SHOW are provided below. Going through the outcomes, one can see that **40 risks have been identified in total at this phase of the project**, **5 of them being of double risk type (e.g. dealing with technical but also operational aspects)**, while **39 are pre-existing as of the Grant Agreement and the previous risk assessment iterations** (shaded in different colours, in grey the ones from the GA phase and in light blue the ones from the first and second rounds). However, all risks has been revisited during this phase, reclarified when needed, and re-assessed from the beginning so that they reflect accurately the status of the project.

In addition, for all, their so far materialisation status has been assessed and clearly declared. Whenever there are specificities to either test sites and/or specific project beneficiaries, it has been clearly declared (the relevance and the proactive or mitigation measure both).

A final internal revision of the materialisation status will be conducted towards the end of the project and the final status will be updated in the participant portal.

In total (and considering the above-mentioned double type of risks), **11 technical**, **17 operational/business**, **4 behavioural**, **5 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** **at this phase of the project** and **only three risks are ranked with a Level II Severity (risks numbered 1, 2 and 11, indicated in orange)**. Those are namely:

- Lack of will of PTAs/PTOs to create common business models for automated PT and non-automated PT mobility services disrupting the current state of art/ business.
- Data platforms: risk related to the lack of openness between the systems, reducing the capability to provide data of a sufficient coverage.
- Lack of endorsement for the regulatory and operational guidance and recommendations.

As it is evident, and along with the detailed documentation provided in Appendix IV, all of them are related to after the project broader deployment of shared CCAM. The within the project relevant to those risks topics have been resolved through project specific mechanisms. For this reason, those will be the first risks that will be priority reassessed towards the end of the project.

It is worth stressing, however, that the risk dealing with the impact of COVID-19 in the project, is currently considered to be of low severity, stressing out the fact that the corrective actions that have been adopted by the Consortium have delivered positive results and it is deemed that the inferred impact has been minimised.

Moreover, **16 risks** of the identified ones **have been evaluated to be of low severity**, while **the rest 21 have been validated as of moderate severity**.

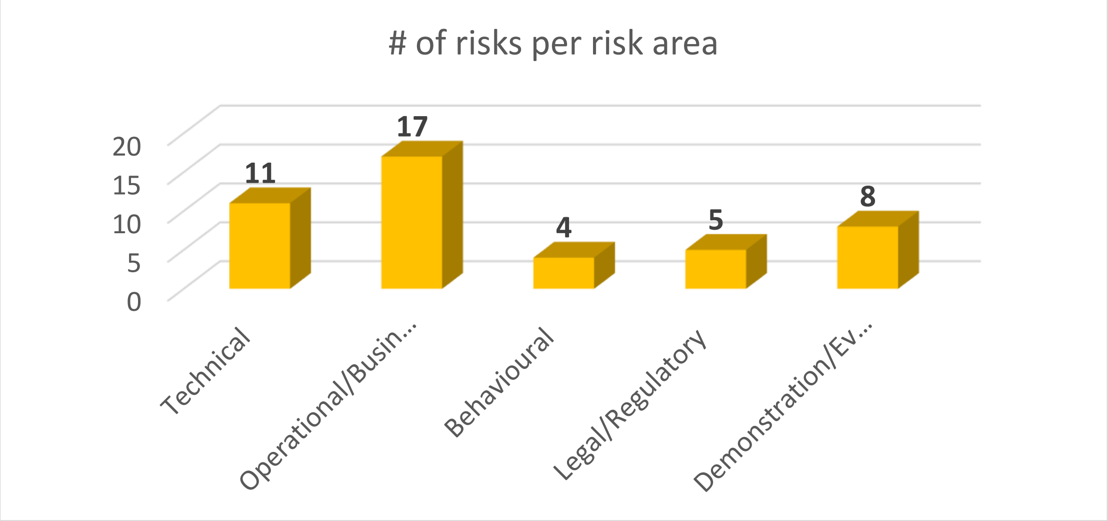


Figure 54: SHOW 3rd Risk Assessment Round – Clustering of risks (40 in total; 5 are doubled in clusters).

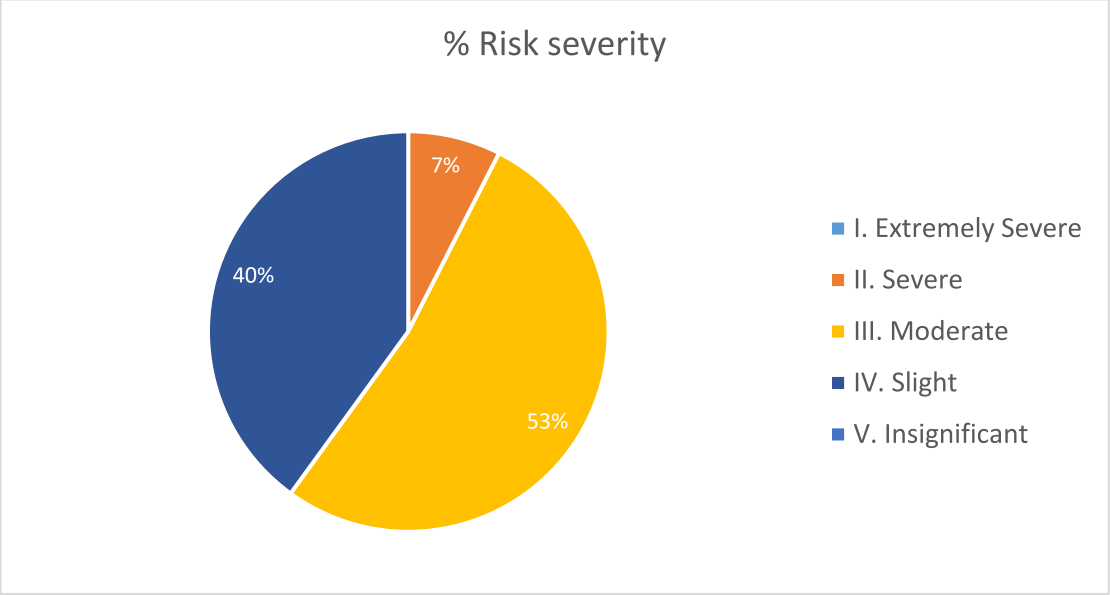


Figure 55: SHOW 3rd Risk Assessment Round – Risk Severity Classification.

Comparing to the previous (second) risk assessment round, the risks overall number **has decreased by 5 risks**, returning to the original number of risks of the first risk assessment round, proving that the intermediate period between is considered to be the most challenging for the project and that the project is back in track.

More particular, the risks that have been removed from the current risk assessment round are as follows:

1. **Policy Regulation for vehicle approval is not harmonized throughout the different countries.** This risk does not hold any longer (EU Regulation 2022/1426 concerning the type-approval of ADSs has been adopted last year). For SHOW and in general for ADSs the main risk is related to the fragmented legislations for deployment (both for testing and for actual services). This is a risk that will persist in the years to come for all the projects involving the deployment of ADSs (other risks are referring to this). In SHOW, WP3 is dealing with that having recognised the differentiations and gaps in national legislations and regulatory frameworks, having already proposed recommendations on harmonising them across Europe (D3.1 & D3.3).

2. **Characteristics of each Pilot site must be critically reviewed in advance in order to ensure results compatibility.** This no longer applies as a risk. It is no longer applicable for the project as this phase has been concluded for SHOW since some years ago. All test sites are conforming to their original use cases commitments; with some of them being tested in a context specific manner in more than one sites, anticipating to provide valuable insights corresponding to different configurations.

3. **Gap/Undergoing revisions in the national legislation for SHOW targeted use cases.** This is not applicable for SHOW since some years. All this process has been concluded and all the relevant work and experience acquired, apart from the fact that has been resolved operationally in the project, has led to recommendations to share beyond SHOW (D3.1 & D3.3).

4. **Spare parts for AVs not at hand.** This has been merged in a broader risk cluster.

5. **Adverse weather conditions jeopardising the operation.** This has been merged in a broader risk cluster.

Overall, the current derived allocation across the different potential nature of risks (technical, operational/business, behavioural, legal/regulatory, demonstration/ evaluation) is similar to the previous risk assessment rounds, while the overall decrease of the risks total number is being related specifically to the operational/business and the legal/regulatory risks.

The full results of the 3rd Risk Assessment round are provided in 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 2 previous risk assessment rounds; with no shading is the additional one recognised on top in the current risk assessment round, related to the logistics operations that have been emerging as a key topic the last period.

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 following table (they are fully available upon request).

8 Conclusions

With this report, the WP4 work is concluded. In chapter 2, a new extended view of the reference SHOW architecture is provided by integrating information concerning the involved stakeholders, which we believe it can assist future deployments of CCAM services in the European cities that want to start their work from the SHOW reference architecture blueprint.

Updates with respect to the previous architecture deliverable, D4.3, were presented in detail including:

- Local sites architectures' refinements covering especially the sites that presented incomplete information in the previous version as well as local sites added recently replacing other SHOW sites.
- SMPD cybersecurity updates and lessons learnt from SHOW SMDP cybersecurity tools deployed; work performed within the context of Activities 4.2 & 4.5.
- SHOW sites' connectivity/interoperability updates based on feedback from sites' CCAM services' demonstration phase; work performed within the context of Activities 4.2 & 4.5.
- Final updated risk management tracing based on experience gathered from pre-demo and demo phase of the project by applying an extended FMEA methodology, performed within the context of Activity 4.6.

In chapters five and six, lessons learnt based on SHOW reference architecture deployment covering interoperability and cybersecurity aspects were drawn which can serve as technical and theoretical hints for any SHOW work follow-up efforts. Hints also include aspects of standardization gaps related with remote fleet monitoring and control as well as cloud data management/abstraction layer hosting mobility data which is an important CCAM service enabler.

WP4 leading team will remain of service in case any newcomer site needs help to be integrated in the SHOW data pipeline but no other task will be performed.

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] SHOW (2021). D4.3: Open modular system architecture and tools –second version. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

[4] H2020 Avenue project. Autonomous Vehicles to Evolve to a New Urban Experience. Grant agreement ID: 769033. https://h2020-avenue.eu/

[5] Horizon Europe ENFLATE project. ENabling FLexibility provision by all Actors and sectors through markets and digital Technologies. Grant agreement ID: 101075783.

[6] Horizon Europe ULITMO project. Advancing Sustainable User-centric Mobility with Automated Vehicles. Grant agreement ID: 101077587. https://ultimo-he.eu/

[7] H2020 nIoVe project. A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles. Grant agreement ID: 833742. https://niove.eu/

[8] H2020 GHOST project. Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control. Grant agreement ID 740923.

[9] CSE-CIC-IDS2018 on AWS (17/02/2023). https://www.unb.ca/cic/datasets/ids-2018.html

[10] Wolf, T., Debut, L., Sanh, V., Chaumond, J., Delangue, C., Moi, A., ... & Rush, A. M. (2020, October). Transformers: State-of-the-art natural language processing. In Proceedings of the 2020 conference on empirical methods in natural language processing: system demonstrations (pp. 38-45).

[11] Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. OpenAI blog, 1(8), 9.

[12] Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R. R., & Le, Q. V. (2019). Xlnet: Generalized autoregressive pretraining for language understanding. Advances in neural information processing systems, 32.

[13] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. arXiv preprint arXiv:1810.04805.

[14] Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., ... & Stoyanov, V. (2019). Roberta: A robustly optimized bert pretraining approach. arXiv preprint arXiv:1907.11692.

[15] Conneau, A., Khandelwal, K., Goyal, N., Chaudhary, V., Wenzek, G., Guzmán, F., ... & Stoyanov, V. (2019). Unsupervised cross-lingual representation learning at scale. arXiv preprint arXiv:1911.02116.

[16] Scarfone, K., & Mell, P. (2009, October). An analysis of CVSS version 2 vulnerability scoring. In 2009 3rd International Symposium on Empirical Software Engineering and Measurement (pp. 516-525). IEEE.

APPENDIX I Reconfigurable Intelligent Surfaces

Introduction

In the next decade, the 6G networks will gather research and industrial interest and all the abilities that have been described in the 5th Generation will be a reality. However, the 6G networks should not be considered simply as a complementary technology to the 5G. The coming of 6G will equip the current communication systems with extraordinary properties. The extremely low latency, the enhancement of the peak data rate and area traffic capacity, and the increase of Quality of Service and connectivity density[3] will lead to new potential use cases such as Holographic Communication, Pervasive Intelligent, and Intelligent Transport[4].

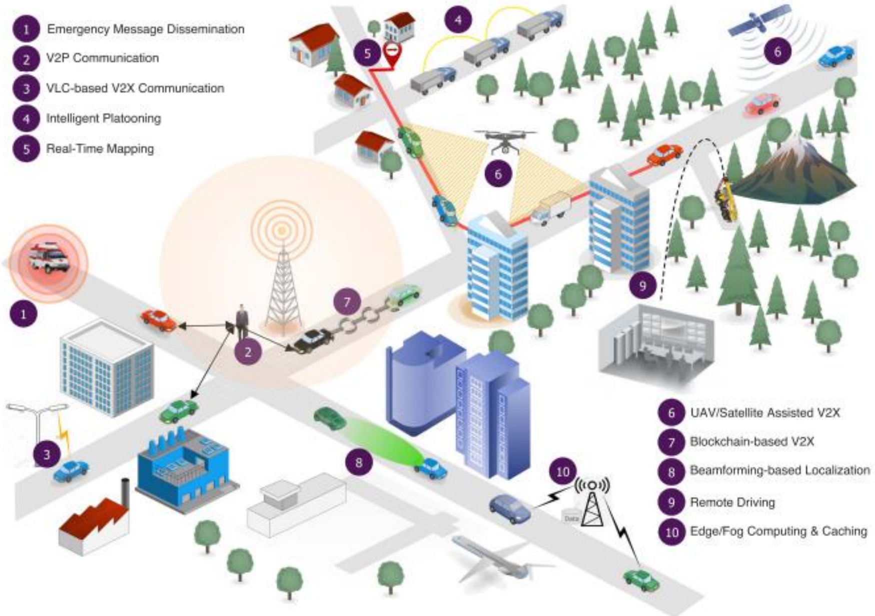

1 Emergency Message Dissemination
2 V2P Communication
3 VLC-based V2X Communication
4 Intelligent Platooning
5 Real-Time Mapping
6 UAV/Satellite Assisted V2X
7 Blockchain-based V2X
8 Beamforming-based Localization
9 Remote Driving
10 Edge/Fog Computing & Caching
Data

Figure 56: V2X communication environment

In Intelligent Transport Systems, the Vehicle-to-Everything (V2X) term is the key indicator. V2X communication encompasses a variety of connections such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) and Vehicle-to-Cloud Networks (V2N). The usage of the 5G technology enforced the ability of the cities' communication networks in order for the V2X to be feasible. However, the rising of the 6G networks will inaugurate a new age in which hundreds of automated vehicles will dominate the roads.

If there was only one difference between 6G networks and all the previous ones, it would be the perception of the communication environment. This perception, in contrast with the already known approaches, is realized as a programmable resource in which the reflection, scattering, and fading stop to be considered as uncontrollable

[3] Khiadani, N. (2020, December). Vision, requirements and challenges of sixth generation (6G) networks. In 2020 6th Iranian conference on signal processing and intelligent systems (ICSPIS) (pp. 1-4). IEEE.

[4] Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. IEEE Open Journal of the Communications Society, 2, 334-366.

phenomena. Now, they compose parameters of the system that could be optimized. Reconfigurable Intelligent Surfaces (RIS) is the main technology that gathers interest in order for the manipulation of the communication environment to be established in the real world[5].

Main RISs use cases in V2X

RIS particularly is a two-dimensional metasurface consisting of massive elements (unit cells) positioned in sub-wavelength distance among them[6]. The physical properties of the RIS, and mainly its electric permittivity and permeability, could be reconfigured in real time in order a specific, macroscopic electromagnetic response to be achieved. The outlook of a RIS is depicted in Figure 57.

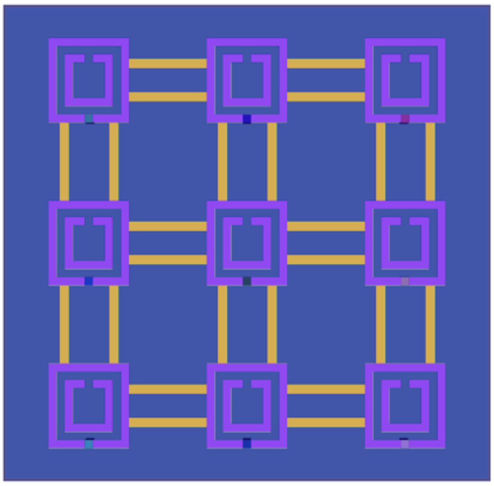


Figure 57: A Reconfigurable Intelligent Surface outlook

The basic goal of the RIS is the creation, the blockage, and the reconstruction of the communication links between the receiver and the transmitter. The most widespread use cases are:

- **Recovery** of **Non-Line-of-Sight** connection between the transmitter and the receiver. The existence of obstacles or buildings could block the Line-of-of-Sight (LoS) between the antennas. RIS is able to re-direct the electromagnetic signals in order for the deterioration of the network performance to be alleviated. In this way the dealing of the dark zones' existence is achieved.
- **Optimization** of the **Quality of Service** (QoS) of the users. The QoS refers to the overall performance of the network in respect to both the requirements of vehicles and the needs of passengers. The reconfigurability of the RIS ensures that their utilization could lead to the enhancement of different networks simultaneously.
- **Minimization** of the **cross-reference among the multiple antennas**. The current networks are composed of numerous transmitting and

[5] Liaskos, C., Tsioliaridou, A., Pitsillides, A., Ioannidis, S., & Akyildiz, I. (2018). Using any surface to realize a new paradigm for wireless communications. Communications of the ACM, 61(11), 30-33.

[6] Huang, J., Wang, C. X., Sun, Y., Feng, R., Huang, J., Guo, B., ... & Cui, T. J. (2022). Reconfigurable intelligent surfaces: Channel characterization and modeling. arXiv preprint arXiv:2206.02308.

receiving antennas. RISs can diminish the transmission energy of the antennas that are not mandatory to communicate.

- **Minimization** of the **latency.** A main goal for the deployment of more sophisticated networks with extra abilities is the minimization of the time in which the information is created and the time in which is available to the end-user. The achievement of lower latency values, apart from the impact in the QoS, would be the key for the domination of the AVs in Europe's roads.

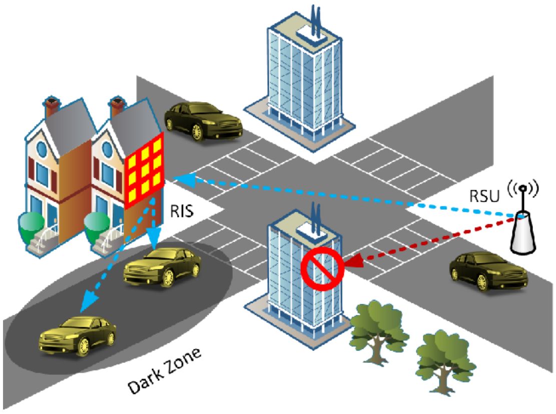


Figure 58: RIS in V2X networks

Tunability of RISs

The main functionalities that the RIS technology is able to support are the beam focusing and splitting, the change of polarization and the filtering. Furthermore, the appropriate configuration of the RIS could make possible its function in different frequency bands.

The ability of the RIS to obtain the desired functionality in the desired frequency is called tunability. There are many ways in order the tunability to be achieved such as mechanic, optical and thermal mechanisms[7]. The majority of these mechanisms are able to offer global tunability, namely that all the unit cells of the RIS are configured with the same way. The behavior of the RIS, in this case, could not ensure the full manipulation of the communication links. The most challenging case is the local tunability in which the elements are configured differently in order for exotic functionalities to be feasible. The main local tunability mechanism is the introducing of the lumped elements in each RIS's unit cell. The lumped elements can offer updatable impedance and reactance enabling the RIS unit to be adapted in its electromagnetic environment and respective needs.

[7] Liu, F., Pitilakis, A., Mirmoosa, M. S., Tsilipakos, O., Wang, X., Tasolamprou, A. C., ... & Tretyakov, S. (2018, May). Programmable metasurfaces: State of the art and prospects. In 2018 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.

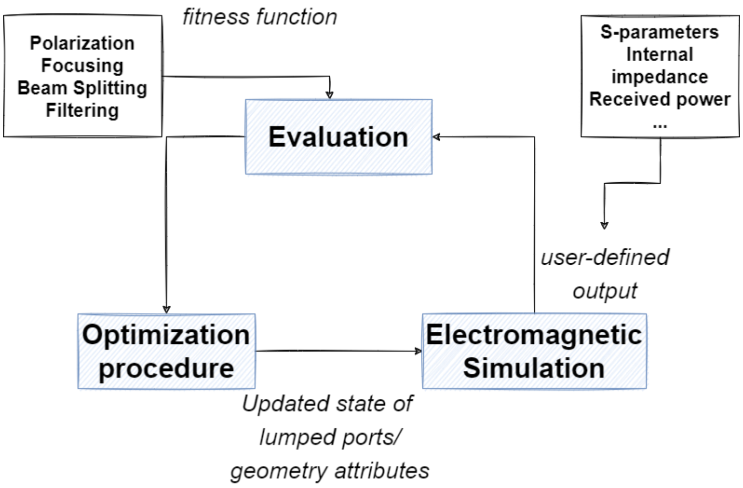


Figure 59: Optimization Workflow

Figure 59 depicts the main optimization workflow that aims to the detection of the optimal RIS configuration for a given desired functionality. Each functionality is described through a fitness function. In the first phase, the electromagnetic simulation defines the geometry attributes for the RIS to be designed and fabricated. Once this procedure is finished, the hardware of RIS is mentioned as unchangeable. In the next phase, the state of the unit cells' lumped ports, via their impedance and reactance, is updated until the user-defined output is matched with the fitness function of the desired functionality. Any already known optimization method, e.g., a Genetic Algorithm, a Differential Evolution, or a Particle Swarm Optimization, can be used. The workflow is completed once the level of fitness is deemed satisfactory or the maximum available amount of time is devoted.

6G-Open platform and V2X

The advantages of the RIS utilization can be enriched via their multiple positioning within the communication ecosystem. The usage of multiple RISs leads to cascaded links whose behavior should be investigated more deeply. The platform described in[8] could compose a very helpful tool in this study. The proposed platform offers an accurate description of the electromagnetic propagation between two RIS units. The platform is able to simulate sufficiently different communication links such as RIS-RIS, transmitter-RIS, RIS-receiver, and transmitter-RIS-RIS-receiver. This platform composes a state-of-the-art analysis performed within SHOW project and will be deployed within ULTIMO project.

The platform, mainly, simulates an RIS pair in any composition, and dimension and at varying distances between them. Furthermore, it pinpoints the resonating frequency of the defined RIS pair. It could be used for the optimization of the energy flow from one

[8] Papadopoulos, A., Lalas, A., Votis, K., Tyrovolas, D., Karagiannidis, G., Ioannidis, S., & Liaskos, C. (2022, October). An open platform for simulating the physical layer of 6g communication systems with multiple intelligent surfaces. In 2022 18th International Conference on Network and Service Management (CNSM) (pp. 359-363). IEEE.

RIS to another via the investigation of S-parameters. Figure 60 depicts the RIS pair simulated by the platform and the S-parameters of the RISs' ports.

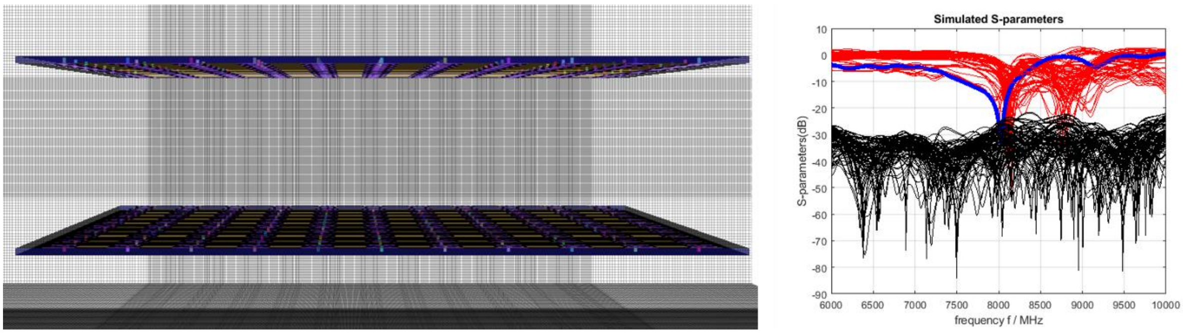


Figure 60: RIS pair with the respective S-parameters

The platform, apart from the basic usage, could be utilized as the basis for more sophisticated scenarios. In Figure 61, multiple RIS pairs have been placed across a road. This setup could handle the Doppler effect, which deteriorates the performance of V2X network phenomenon. The Doppler effect is introduced due to the velocity of the vehicles relevant to the transmitting antennas. There are numerous analyses of the Doppler effect impact in V2X networks[9][10][11][12]. The investigation of the electromagnetic propagation and the possible enhancement because of the multiple RIS pairs' existence could lead to new, realistic solutions.

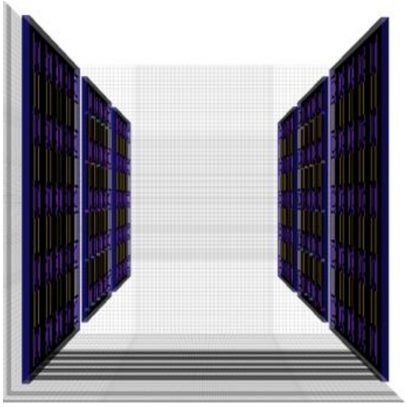


Figure 61: Multiple RISs for Doppler effect mitigation

As mentioned above, one of the most well-known use cases of the RIS technology is related to the LoS. Indeed, the LoS connection between the vehicle and the transmitter antenna could be lost in a cross of surrounding buildings. The positioning of RIS in the

[9] Huang, Z., Zheng, B., & Zhang, R. (2021, June). Transforming fading channel from fast to slow: IRS-assisted high-mobility communication. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[10] Wang, K., Lam, C. T., & Ng, B. K. (2021, December). Doppler effect mitigation using reconfigurable intelligent surfaces with hardware impairments. In 2021 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[11] Sun, S., & Yan, H. (2020). Channel estimation for reconfigurable intelligent surface-assisted wireless communications considering doppler effect. IEEE Wireless Communications Letters, 10(4), 790-794.

[12] Noh, S. K., Kim, P. J., & Yoon, J. H. (2016, October). Doppler effect on V2I path loss and V2V channel models. In 2016 international conference on information and communication technology convergence (ICTC) (pp. 898-902). IEEE.

corner of the building is suggested in order to avoid a no-signal hole in this area. In Figure 62, the simulation of this scenario is displayed.

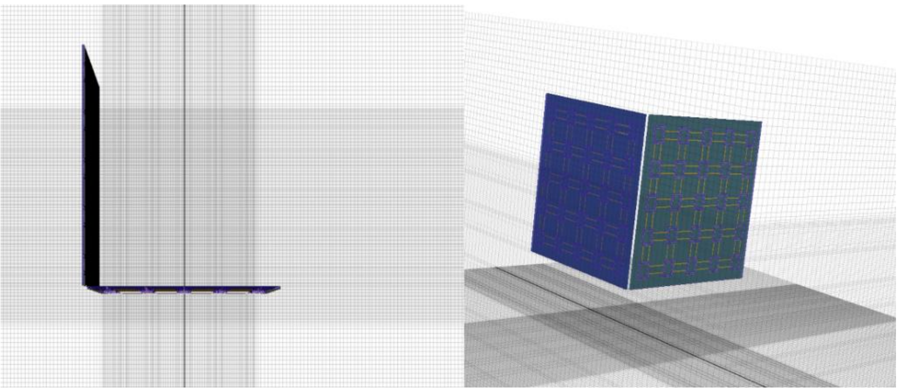


Figure 62: RISs in corner of buildings

APPENDIX II Cybersecurity Best Practices

Introduction

Cybersecurity testing in the automotive field has been a critical issue concerning the research community and cybersecurity specialists in recent years. The subject gains traction as the automotive field is promising for growth and is a field for implementing different technologies. In essence, the numerous novel technologies are vulnerable to threats that should be alleviated to achieve adoption in real-life scenarios like transportation of citizens and products.

The current status of the developed automotive systems is complex and fragmented at times. In more detail, the automotive systems consist of a variety of complex protocols, a significant number of electronic devices communicating with each other and systems analysing and visualising information. The various protocols, devices, and systems demand meticulous effort and specific knowledge to guarantee overall security. For example, AVs can be vulnerable to attacks or manipulation, and the specific aspects of modern vehicles have to be identified in order to be well protected.

Establishing common rules and best practices is important and valuable for the CCAM community as they permit the creation of reusable and easily modifiable systems for automotive professionals. Consequently, projects can be less costly, and developers can focus on specific functionalities in the system. Acknowledging the value of a coherent document for the automotive field, this guide presents a summary of potential best practices identified and analysed to address cyber threats.

In particular, the best practices cover organisational and technical aspects of vehicle cybersecurity, which can be classified into the 10 following major topics: 1) **incident response**, 2) **collaboration and engagement with third parties**, 3) **governance, risk assessment and management**, 4) **awareness and training**, 5) **threat detection, monitoring and analysis**, 6) **security by design**, 7) **access control**, 8) **protection of networks and protocols**, 9) **software security** and 10) **data management**.

Incident Response

Incident response can be described as the plan in case the system has been compromised and presents the steps that have to be followed for effective mitigation of the risks that may occur for a quick and effective recovery. Attacks can trigger incidents that may jeopardise the overall system and, consequently, threaten the safety of the passengers and the involved parties. These incidents could be related to remote manipulation of the AVs, data exposure and disruption to the system's operations. The best practices include the essential protocols for reliable and expeditious recovery and can guarantee a continuous operation by minimising the risk. Furthermore, best practices suggest that the Incident Response section can be aligned to the four main phases of the incident response lifecycle: **prepare, find, fix, and close.**

Prepare includes the documentation of the plan to be followed when an incident occurs. The document classifies the incidents that may happen and assesses the possible damage that may cause. Essentially, this phase establishes a risk management plan by defining roles and responsibilities for persons to act accordingly once an incident occurs, as well as guides the decision makers. The plan should be tested and should be improved to reduce the potential risks.

The target of this step is to **Find** quickly and effectively escalate potential problems which have been identified. Best practices suggest the following steps for successful identification: log the incident, validate the incident, and finally, classify and escalate the incident. An incident can be also classified according to its likelihood, severity, and impact on the system.

Fix phase aims to activate a team for rapid risk mitigation, remediation, and recovery of the system. This phase focuses on executing technical response activities, notifying stakeholders and consistent incident coordination.

Close phase is important to take advantage of the lessons learned from the different incidents. It is essential to identify the strengths and weaknesses of the system. Strong remediation controls should be put in place, and the plan has to be updated accordingly to reflect the new risks and take advantage of the new technology in the market.

The creation of a **Computer Security Incident Response Team** (**CSIRT**) would be an important consideration for the projects that intend to put in place Incident Response mechanisms.

Collaboration and Engagement with third parties

The development of secure automotive's most times requires the participation of different entities. Shielding effectively against cyber attacks needs collaboration between the various stakeholders. For this reason, partnerships between several parties, such as industrial companies and organizations, government, researchers, and academia, are formed to boost vehicle cybersecurity. The risks are related to misconfigurations of the existing resources that may weaken the security of the system and lead to unpleasant situations and disrupt the established processes. In addition, the risks concern the unnecessary and unintended exposure of data, sensitive information, or intellectual property. The best practices in this Collaboration and Engagement with third parties' phase is divided in three subfields. These are: **information sharing, events, and programs**. Information sharing could be considered as the shared data, the system details or even the system vulnerabilities. Events target to a better collaboration by connecting the different parties and diverse groups of experts. For example, hackathon events and conferences. Programs could be the development of the standards, which are used for the system, the certifications and maybe professional exchanges.

Best practices for **information sharing** consist of the following topics:

- Identify content that is useful to be shared among the different organizations
- Collaborate with the proper stakeholders and partners
- Develop mechanisms to transfer the shared information with internal partners or even third parties
- Use the most suitable tools and technologies

Best practices for **events** are related to the identification of the events that have to be created for the cybersecurity enhancement. These events could be:

- Incident response trials
- Cybersecurity exercises
- Conferences
- Workshops
- Webinars

Best practices for **programs** related to vehicle cybersecurity could be:

- Intelligence sharing programs
- Vulnerability sharing programs
- Standards set up
- Research

Collaboration and Engagement best practices are comprehensively described in **ISO/IEC 27010:2012 referring to information security management**[13], **NIST SP 800-150 for sharing cyber threat information[14],** and other published resources such as **Auto-ISAC**[15].

Governance

Governance describes the methods used to align the cybersecurity of the vehicle with the different organisations and stakeholders who may participate in the project and their missions. There is no governance plan or strategy universally accepted and applied. As a result, each project may use a different approach for the government section. Best practices may not provide the strategy per se but provide a methodology with distinct sections for devising a project's strategy. Particularly, best practices suggest dividing the governance section into three smaller subsections that are **design, build and operate**.

Design subsection refers to the following tasks and relevant actions:

- Clarify and explain the projects' scopes by considering:
    - ❖ Organisation's size
    - ❖ Cybersecurity risk boundaries

[13] International Organization for Standardization. (2012). Information technology — Security techniques — Information security management for inter-sector and inter organizational communications (ISO/ IEC 27010). Retrieved from https://www.iso.org/standard/42509.html

[14] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST special publication, 800(150).

[15] Auto-ISAC Best Practices Working Group (2019). Automotive Cybersecurity Best Practices. Executive Summary.

    - Cybersecurity sophistication
    - Available resources
    - Prebuild structures and mechanisms
    - Customers' requirements, etc.
- Define the mission and vision of the project. These statements could include the following topics:
    - Customer demands
    - Passenger safety and privacy
    - Threat detection and prevention
    - Risk analysis and management
    - Security mechanisms which are going to be preinstalled in the vehicle
    - Data protection, etc.
- Recognise the projects' key functions. For example, the key functions could be the following processes:
    - Cybersecurity Risk Management
    - Policies and Requirements
    - Incident Response
    - Penetration testing
    - Third-party collaboration and engagement
    - Vehicle cybersecurity and monitoring, etc.

Design subsection essentially, explains the core aspect of governing a vehicle cybersecurity strategy by clarifying projects' main targets and the essential processes to be followed in order to achieve those targets.

Build subsection describes how to organise a cybersecurity project. This specific subsection can be divided into two main topics which are:

- **Internal processes**: Identify the leadership, the decision makers, the organisational hierarchy, create a model to host the staff, etc.
- **External processes**: Identify critical partnerships and synergies, define integration plans between vehicle cybersecurity and different business processes, establish protocols to escalate information to other companies

Operate subsection aims to define a set of guidelines about how to put in place a cybersecurity program that is efficient and effective and fulfils the project's requirements. These guidelines concern:

- Identifying policies and functions
- Governing efficiency through metrics
- Developing and preserving mechanisms for consistent resource management

Risk Assessment and Management

The **Risk Assessment and Management** section aims to define the possible impact of cybersecurity vulnerabilities in the system. There is a variety of different methodologies to perform risk analysis closely related to each organisation's needs and project's requirements. The risk assessment is a tool that helps to mitigate the risks of cyber threats by developing the proper cybersecurity measures. Risk Assessment and Management best practices are described in: **NIST 800-30: Guide for Conducting Risk**[16]. Best practices in Risk Assessment and Management section could include the following:

[16] Joint Task Force Transformation Initiative. (2012). SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. NIST.

- Clarify the target and requirements which concern the benefits by implementing a risk assessment methodology.
- Different security assessments have to be devolved for the different phases in the product’s lifecycle circle. For example, if the V model is followed, best practices suggest a different Risk Assessment methodology for each phase. The phases in a V model are the following:
  - Design
  - Implementation and Integration
  - Testing
  - Production
  - Aftersales
- Determine a risk tolerance. Risk tolerance could vary in the lifecycle’s different phases
- Add risk assessment processes in the governance phase and control conformity

Vulnerability observation should be regularly performed. The time gap between vulnerabilities monitoring should be defined in the Risk Assessment, for example, every six months or more frequently but at least once a year.

The US transportation department (USDOT)[17] developed the documentation about best practices for automated vehicle cybersecurity with the use of penetration testing. The aforementioned report highlights the necessity of penetration testing to determine indications about the feasibility of attacks, which take advantage of vehicle vulnerabilities and the efficiency of current security measures. Moreover, it can be used to calculate the likelihood or the potential impact. The target of the penetration tests can include security policies, devices, applications, networks, access control, communications and configurations that could comprise the system. The report suggests focusing on the most critical processes, taking into account the **NISTIR 8179 Critically Analysis Process Model: Prioritising Systems and Components[18]**.

The calculation of the risk could be performed by using the following formula:

$$Risk = Likelihood \times Impact$$

This equation takes into consideration the likelihood of exploiting the threat and the impact if this threat is utilised.

Awareness and Training

The existence of a security policy is not sufficient to ensure the integrity of a system, as it should be applied by all the members that compose an organisation, even the small subsidiaries. The implementation of security policies should be audited, which means that the implementation of recommendations is regularly checked and monitored. Training of all users at all levels on the information security part is essential. Some of the tactics are: reminding of security rules, best practices and procedures, avoiding executing files that come from an unknown source, and maintaining the confidentiality of usernames and passwords.

Organisational member training and awareness programs can also be used to foster a culture of security and enforce cyber responsibilities. Best practices encourage

[17] https://www.transportation.gov/

[18] Paulsen, C., Boyens, J., Bartol, N., & Winkler, K. (2017). Criticality analysis process model: Prioritizing systems and components (No. NIST Internal or Interagency Report (NISTIR) 8179 (Draft)). National Institute of Standards and Technology.

educational training and awareness programs to enhance stakeholders understanding of cyber risks. This capability is typically described by four fundamental activities: **Design**, **Develop**, **Implement**, and **Improve**. These four activities provide a framework that companies can follow to use off-the-shelf programs or design their own.

Best Practices for Awareness and Training may include:

- Design awareness and training programs according to the responsibilities of each member, developing a specific strategy in the event of a threat.
- Encourage the acquisition or development of training curricula to promote a culture of learning.
- Integrate risk management processes and standards throughout the organisation's operations, as well as monitor and enforce compliance with security protocols.

Threat Detection, Monitoring and Analysis

Proactive cybersecurity includes the identification of system security gaps, threat detection and incident assessment, thereby enabling the relative risks of a cyber attack to be minimised and its consequences avoided. The process followed during the preventive audit increases the probability of detecting suspicious activity resulting in the immediate initiation of proceedings that include restoration and recovery.

Every organisation should implement a disaggregated logging regime to detect threats in network traffic, using either a comprehensive security information and incident management solution or through discrete logging tools. In addition, all organisations, either through pre-defined firewall rules or by configuring them themselves, should implement endpoint detection and network defense monitoring capabilities in conjunction with IP address blacklists and whitelists.

Best Practices for Threat Detection, Monitoring and Analysis may include:

- Develop a threat detection and analysis process by understanding your organisation's threat environment
- Develop a structure that categorise threats as well as an operating model that defines the roles and responsibilities of stakeholders.
- Determine the necessary threat information to help identify sources and the collection process.
- Establish a threat monitoring process by prioritising and identifying various techniques and methods.
- Define a threat analysis methodology that includes automatic identification of threat events in order to take necessary actions

Security by design

Most cyber attacks exploit security gaps found in vulnerable devices and services. They carry out brute force attacks with the aim of revealing usernames and passwords, and when is not possible, they use phishing techniques. Organisations and their customers should ensure they are aware of and can counter these attack methods. Helpful mitigation resources on initial compromise attack methods are listed below:

- Improve security of vulnerable devices
- Selecting and Hardening Remote Access VPN Solutions
- Vulnerability Scanning Tools and Services
- Protecting internet-facing services on public service
- Strategies for protecting web application systems against credential stuffing attacks

- Defend against brute force and password spraying
- Defend against phishing
- Spotting malicious email messages

Access control

Organisations should ensure the smooth operation and integrity of applications that allow remote access and enforce multifactor authentication (MFA) rules where possible to strengthen the security of the infrastructure. Various methods have recently demonstrated the ability to exploit default multifactor authentication protocols. For this reason, organisations should review their configuration policies to protect against "open failure" and rewrite scenarios.

Best Practices for access control:

- Organisations should recommend MFA adoption across all customer services and products.
- Organisations should also apply MFA to all accounts that the customer has access to, while these accounts will be designated as privileged.
- Customers should ensure that their contractual arrangements mandate the use of MFA in the services and products they receive.
- Contracts between organisation and customers should also require MFA to be enforced on all accounts.

Protection of Networks and Protocols

All organisations should follow best practices for protecting and managing passwords and permissions. Organisations should check logs for suspected failed authentication attempts. Specifically, failed authentication attempts although an account password has recently been changed could indicate that the account has been compromised in the past. Note that network administrators can proactively look for such intrusion attempts by examining log files after performing password changes. Once this is confirmed they can use off-net communications to notify users of the change if the account is considered sensitive.

Best practices for protection of networks and protocols:

- Organisations should verify that the customer restricts account access to systems managed by the organisation
- Customers should ensure that account credentials provided by their organisation are not leaked to individuals within or outside the organisation.
- Administrators should grant access and management permissions based on each member's role, using the principle of least privilege.
- Administrators, through audits, should confirm that the accounts granted are used for appropriate purposes and activities and not for personal reasons.
- Organisations should deactivate accounts when they are not actively used.

Software security

Organisations should regularly check to update the software they use, including operating systems, applications and firmware. They should update security protocols on software that contains known exploited vulnerabilities.

Best practices for software security:

- Organisations should implement updates on internal networks as frequently as possible.

- Customers should ensure that they understand their organisation's policy regarding software updates.
- To request that comprehensive and timely updates to be provided as an ongoing service.

Data management

Organisations should update their systems regularly to minimize the risk of vulnerabilities and keep backups at both the data and operating system instances in case they need to roll back. Backups should be stored in separate locations and isolated from network connections that could allow a ransomware attack to be spread out. It should be noted that many ransomware variants attempt to detect and encrypt/delete accessible backups. Isolating backups makes it possible to restore systems/data to their previous state if they are encrypted with ransomware.

Best practices for data management include:

- Storing backups separately, such as on external media.
- Organisations should regularly back up customer data and internal data and maintain offline backups that will be encrypted with separate encryption keys and located outside of the network.
- Providers should encourage customers to create secure off-site backups with recovery capabilities.
- Customers should ensure that they maintain backup and backup services should meet resilience and disaster recovery requirements.
- Customers should demand from their organisation to implement an alternative solution of automatic and regular backs up of critical data and of system configurations while also storing backups in an easily retrievable location.

APPENDIX III Cybersecurity & Privacy Questionnaire

Table 13: Cybersecurity & Privacy questionnaire

Partner Partner name

Final Applications	
Q1	What are the applications that Partner is using and/or developing for SHOW?
Cybersecurity	
Q2	What are the security measures you have in place to prevent source code vulnerabilities?
Q3	Do you conduct internal pentests regularly or just if a risk is raised? Do you conduct hardware or software based pentests?
Q4	What is the minimum CVSS (Common Vulnerability Scoring System) accepted?
Q5	How are Spoofing and Jamming attacks prevented by the GNSS receiver at the level of the vehicle GPS?
Q6	Do you have any vulnerability report? How often are security audits conducted over the implemented application? Would you like to share with us your latest audit report?
Q7	Do you coordinate with other partners' cybersecurity teams to assess risks on connecting your platform to the other servers/systems?
Q8	Do you provide training to vehicle operators/supervisors to face cybersecurity attacks?
Q9	Are you working on the CSMS certification required by the UN 155 regulation?
Q10	How security is handled while doing a software update? Is there any vulnerability scanning before deploying a software update? Would your software update impact somehow the vehicle? Do yo refer to the UN R156 recommendations on vehicular software updates?
Q11	Do you refer to any security standard/ guidelines such as ISO9001, ISO27000, ISO/IEC20243....?
Data Privacy	
Q12	Does your application use any personal data? Does it aggregate data from other service providers?
Q13	Is the location data, collected through your applications encrypted/anonymized before it is saved on the database? Do you process any IMEI/MEID ID ? If yes, is it anonimyzed/pseudonymized?

Q14	How do you secure the connection and the data exchange between your applications and data providers services?
Q15	How data processing and storage are handled with regard to the GDPR recommendations as well as the FDPIC (Federal Data Protection and Information Commissioner) acts? How long is personal data stored? and how often it is destroyed? Do you ask for the user's consent before storing the data?
Q16	Do you share any data with any LBS (Location Based Services) platforms?
Q17	Which procedure do you deploy in case of a data breach? Do you have a clearly elaborated procedure?

APPENDIX IV: 3rd Risk Assessment Results

Table 14: 3rd SHOW Risk Assessment Round results.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
1	**Lack of will of PTAs/PTOs to create common business models for automated PT and non-automated PT mobility services disrupting the current state of**	Operational/ Business	Endangered real life deployment and later penetration - 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. Results show that automated PT is not cost-efficient	Progressively, during the entire project lifespan, throughout pilot operations, demo events and recollection from passengers and stakeholders through surveys and interviews.	WP2, WP12, WP17	Madrid	240	**High**	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	**Cannot be assessed yet**	Overall materialisation of this risk cannot be assessed before the end of the project. Still, Madrid/ EMT has some first indications.	Depending on the evolution of AV services in the market the PTO may change priorities and postpone certain decisions	Close monitoring of the AV sector evolution focusing on the local context (Madrid, Spain).

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
	art/ business.			and, thus, sustainable.					🟧	adequate awareness and engagement strategy, to be further strengthened through public pilot operations, demo and engagement events and training. Validate systemically the business models applied in each city ecosystem. If not yet available, create a			being beneficial for the CCAVs deployment in urban public transport.	

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										comprehensive integrated mobility strategy for each of the participating cities, regions and stakeholder eco-systems in the course of the project that will be able to host automated mobility in a sound manner.				
2	**Data platforms: risk related to the lack of**	Technical	No interoperability reached and able	"Closed systems" by OEMs, infrastructure operators	During iterative data collection in the course of	WP5, WP11, WP12	Up to a certain extent, applicable to	288,0	**High**	Development of a common data collection	**Partially materialised**	Up to a certain extent, has been materialised	It has been quite common that	Alternative interfaces and

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	openness between the systems, reducing the capability to provide data of a sufficient coverage.		to be proved. Robust cross-border evaluation of urban automated mobility in Europe is hindered.	and other industrial partners. Technical bottlenecks to share data.	pilot operations.		all sites.			platform and dashboard, use of open standards, common formats and alternative interfaces to collect data from all SHOW test sites.		in the past in most test sites.	access to specific data are restricted by the OEM or Tier1 supplier.	other indirect methods have been deployed for data collection or post-calculation of some of them.
3	**Liability and ownership of data produced as well as liability of services**	Legal/Regulatory	Barriers to deployment and exploitation.	Personal data protection and related IPR are not yet clear in the overall domain and	During Data Management Plan and Data Protection Impact Assessment subsequent	WP3, WP11, WP12, WP13, WP14	Cross-cutting to all test sites.	90	**Moderate**	Legal, regulatory and liability issues are dealt in the project in WP3 and WP14. All	**Not materialised**	By so far experience, there has been no concerns shared respectively.		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	that are built based on these data.			have not been clearly reflected in corresponding regulation.	versions issue. Also through deployment of data for several purposes in the project different phases (demonstration, evaluation, impact assessment).				🟨	actions anticipated (DMP, DPIA, etc.) have been applied already in the project. In addition, further Data Protection Agreements may occur until the end of the project for treating specific excerpts of data; though the key principles are defined already in the project				

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										Consortium Agreement and the Data Policy of the project.				
4	**Lack of transferability of solutions.**	Technical Operational/ Business	Interoperability on operational level (on several layers) cannot be proved. Replication activities may be limited in the course of the project.	Highly specific requirements / legacy systems per site. Local business models and ecosystems may vary highly from site to site. Different proprietary solutions not able to talk to each other.	As per the outcomes of the replication activities of the project.	WP4, WP5, WP12, WP15	Applicable for the follower sites of the project.	96,0	**Moderate**	A sound system architecture has been established to enable interoperability / transferability of solutions as far as reasonably possible in two layers mainly: a) selection of common standardized protocols	**Not materialised**	There are already 10 follower sites engaged and expressing interest in the project. While regional replication, just launched, is expected to bring about further transferability. The follow-up		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
				Replication strategy of the project proving not effective.					🟨	for web-of-things IoT (connection with cloud data/fleet management platforms via REST or MQTT) and C-ITS (connection among the fleet vehicles and the infrastructure) networking that allows simultaneous operation of different OEMs/ providers in the same context; b)		activities planned will prove if the knowledge acquired through project pilot operations and the architecture put in place in SHOW will prove effective. The so far pilot operation does not indicate any important concerns in this respect.		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟨	common data format for SHOW data operations defined by taking into account the project needs and the SoA (itXPT specs e.t.c). In addition, the co-existence of so many different operational contexts in SHOW will allow creating a rich basis that will serve as				

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										knowledge platform for interoperability issues as well, among other, and, thus guide the guidelines shared with the follower sites that will be engaged in the project.				
5	**Low traveller acceptance and trust issues, services underuse and non-sustainabl**	Behavioural	Insufficient data availability for robust SHOW evaluation and impact assessment. SHOW and	Ineffective user and stakeholder engagement strategies for SHOW demonstration; ineffective engagement	During pre-demonstration phase for the first time in the project and iteratively throughout continuous pilot	WP7, WP9, WP11, WP12	All	84,0	**Moderate**	Emphasis is put within WP7 to enhance vehicle features including user experience inside the	**Not materialised**	The pre-demonstration phase (but also the final public phase in running test sites) has revealed great		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
	e operation.		shared CCAV services for urban contexts proving unsustainable. Barriers to deployment, exploitation and replication.	of local demonstration boards in SHOW; insufficient level of solutions and quality of service offered; generic challenges regarding CCAV trust beyond SHOW. COVID inferred restrictions and change of priorities on Cities level.	operation across all project test sites.				🟨	vehicle as well as the interface towards other travellers and the vehicles; to alleviate safety and security fears. Remote operation and safety drivers on board are expected to assist with the safety perception of passengers. Also, citizen engagemen		interest which imply that the risk of low engagement at least will not be materialised. Upon the first consolidated results from the pre-demo phase, and despite the fact that several weaknesses have been indeed identified from passengers and stakeholders		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟨	t strategies of A9.3 and tight coordination of demo communities and frequent organisation of local demo events that aim to attract and make aware passengers and stakeholders in the context of WP12 aim to help in this direction. The		, the average user acceptance is at 6, 84 [scale: 0-9] and the overall satisfaction level is at 84.8 [Scale: 0-100], while thousands of passengers have been transferred and the local demo events convened have gathered a considerable number of attendants.		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										iterative and large scale nature of pilot operations in SHOW is also expected to eliminate recognised weaknesses and laggings.		Still, COVID-19 inferred restrictions did not positively affect engagement.		
6	**Closed vendor systems whether these refer to OEM or PTOs.**	Technical Operational/ Business	Restrictions in data provision to allow in-depth assessment. Lack of interoperability hindering further deploymen	Inevitable "silos"; trust issue; lack of common Europe-wide vision on interoperable CCAM; gaps and in harmonisation in business	During iterative integration and piloting.	WP4, WP5, WP11, WP12	Cross-cutting to the project test sites, but addressing mostly the "comm	175	**Moderate**	This is being tackled via the mechanisms applied in the project by the Data Management Platform (A5.1) that orchestrate	**Not materialised**	So far, all test sites conform to the data requirements that have been imposed by the project. Have also revealed to be open to		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
			t and replication.	and operational models.			ercial" sites of the project (i.e. Frankfurt, Monheim, Gothenburg, ...)			s all flow of information between different ends of all test sites, defining and collecting the minimum set of data that is mandatory by all sites towards the fulfilment of the project KPIs.		share knowledge allowing external parties (of the project and beyond) to get insights in the operations strengths, weaknesses and potential.		
7	**The Marketplace fails to integrate CCAM services and**	Operational/ Business	Individual decentralised deployment of services instead;	Different, not aligned service definition and reluctance to share	During development/ integration.	WP6	Not applicable	18	**Low**	SHOW has built (in D6.1) a parametric infrastructure that allows	**Not materialised. To be ass**	Marketplace has been made public, supporting a series of functionalities, including		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
	systems in a single context.		SHOW failing to serve as a unified channel for SHOW and CCAM products acknowledgement and promotion.	services/products.						hosting and promotion of different types of CCAM products (also of different readiness), internal and external to the project.	**essed at the end of the project.**	already 20 products which are consistently described, endorsing also comments from the AB members and is ready for its formal opening to the public. The outcomes of promotion and acceptance by the CCAM community/ actors will be known towards the		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
												end of the project.		
8	**Cost explosion in the high-tech sector for system development (vehicle sensor implementation, infrastructure).**	Operational/ Business	Not able to fully meet the original project commitment, as it may infer discounts on several layers of development and, thus, on resulted solutions and their acceptance.	Under budgeted relevant costs in SHOW vs the dynamically changing market that is anyway disruptive and is more heavily (vs other sectors) affected by external factors (COVID, energy crisis, financial crisis).	Throughout development and integration.	WP7, WP8	In principle related to all test sites.	144,0	**Moderate**	SHOW, being an Innovation Action, has by default anticipated additional to its funding, national initiatives and complementary funding sources to be exploited as much as possible. Still, there is always a limit up to a European project can digest considerabl	**Partially materialised**	VALEO, NAVYA and the most of the OEMs have been certainly affected by the long delays the supply chain industry incurred the past years (and still does), which, in turn affected the in-time integration/ replacement of units in several occasions/ test sites.		

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										e disruptive changes as the ones occurring the last years.		Still, back up plans were iteratively built case base case in the project to eliminate as much as possible the negative effects in the pilot operations planning.		
9	**(sufficient) Technical readiness of vehicles for safe operation on public roads not available in due**	Technical Operational/ Business	Delays in operation, smaller fleets, deployment with less advanced/ of lower TRL solutions, low acceptanc	Insufficient project planning or inevitable/uncontrollable technical issues in combination with external factors - see risk "Cost explosion in	During development/ integration, technical validation and pre-demo phase.	WP7; WP11	Gothenburg, Linköping, Madrid, Turin, Carinthia	168	**Moderate**	Full technical verification and validation performed in the project, prior to the pre-demo phase launch	**Partially materialised**	Gothenburg, Linköping, Madrid (EMT), Turin, Carinthia	In Turin case, Luxoft was not able to develop their vehicle on time and in a way to meet	Luxoft withdrew from the project and the vehicle was replaced by

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	time for the project pilots.		e rates, limited value added and impact.	the high-tech sector for system development (vehicle sensor implementation, infrastructure)". Delay in type approvals. Technical validation proving insufficient readiness. Technical deadlocks that cannot be overridden.					🟨	(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 later the operation,			the legal requirements; thus it had to be replaced (by NAVYA). In Gothenburg, Linköping and Carinthia, failures in systems were occurring in OEM fleet	another OEM, internal to the Consortium (NAVYA). Madrid (EMT) is under agreement with Villaverde municipality to supervise testing area with local

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟨	transfer of know-how and products from other sites, also external to the project.			taking time to resolve, leading to pauses of operation. Villaverde scenario in Madrid is subject to permission for open traffic which has been challen	police. Once permissions are obtained activity A11.2 validation will start.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
													ging to get.	
10	**Lack of adoption of the guidelines / lack of implementation resources & competence in the public sector or other stakeholders.**	Operational/ Business	Barriers to wide deployment, exploitation and replication.	Current practice proving stronger; delay in digestion of changed and harmonised processes; resources issues; COVID-19 effects.	Through public pilot phase and during replication phase towards the end of the project.	WP12, WP14, WP15, WP16, WP17	Referring mainly to replication sites/regions but also to further exploitation of SHOW services across the project pilot sites and ecosystems	195	**Moderate**	Establishment of a competence group within the framework of SHOW (possibly led by UITP in the context of WP14/WP15/WP17), which will be also available after the end of the project. Tight coordination of local demo communitie	**Not materialised. To be assessed at the end of the project and beyond.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
							beyond /after the project.			s and successful engagement and follow-up of the project replication sites in the course of the project. Effective reflection of SHOW and CCAM related plans in the context of local/regional SUMPs.				
11	**Lack of endorsement for the regulatory and operational**	Operational/ Business	Lack of interoperability; limited impact of SHOW and CCAM	Insufficient engagement strategies and mechanisms; not useful enough	During replication and exploitation phase of the project.	WP3, WP12, WP16, WP15	Referring mainly to replication sites/re	252	**High**	This will be averted by a series of project mechanisms, both technical	**Not materialised. To be ass**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
	guidance and recommendations.		in shared PT world; late or unsuccessful deployment of CCAM in shared PT.	DSS tools (WP17); market and society unreadiness to CCAM encompassing also shifting of Cities and PTOs priorities; low interest on behalf of stakeholders.		, WP17	gions but also to further exploitation of SHOW services across the project pilot sites and ecosystems beyond /after the project.		🟧	and operational. Through the interoperability principles and mechanisms of the project (WP4), through specific customised engagement plans of the test sites and the creation of strong local communities that will outlive the project (WP9) as	**essed at the end of the project and beyond.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟧	well as through the replication mechanisms that have already started in the project (WP12, WP15), which includes lobbying of public authorities to encourage them to define policies allowing the endorsement of outcomes on regulations				

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
									🟧	and operational procedures.				
12	**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, (WP12)	Cross-cutting to all test sites.	60,0	**Low**	Through the standard compliant cybersecurity mechanisms of WP4 that will be assessed through the technical validation of WP11 in first place, but also iteratively during the public pilot phase of the test sites.	**Not materialised**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
13	**Lack of sharing data and info exchange between different Partners in the value chain but also from each local ecosystem to SHOW, in the context of pilot field trials.**	Operational/ Business	Endangering valuable and reliable results consolidation and impact assessment, affecting also further deployment beyond the end of the project.	Unwillingness to share data; "silo" systems by OEMs and PTOs (also from OEM to PTO); unclear data policy in the project.	During the demo phases of the project and, in specific, when data collection either for DMP (performance data) or subjective aspects capture is tackled.	WP5, WP9, WP11, WP12	In principle applicable to all; basically in the sites where specific commercial OEMs/ vehicle providers are deploying.	24	**Low**	Pre-agreed data exchange in the context of WP5 and mapping to project KPIs. Specific mechanisms and rules established for the data sharing. Tight daily (literally) monitoring of the process on technical management level; streamlining conflicts occurring. Revision	**Partially materialised and already resolved.**	A few instances have been detected regarding unwillingness to share data, from the side of the OEM towards the PTO.	Such conflicts were related to commercial/ financial issues. The sharing of data of all stakeholders' sites with the project has been clarified from the early beginning of	Alternative mechanisms on technical side along with a tremendous effort in all aspects from WP5 team have been dedicated to allow a sound and

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										and strengthening of business and operational models on test site level that will allow the smooth collaboration between different stakeholders.			the project; still there have been several technical wise challenges of different types.	consistent data sharing to satisfy the project KPIs. For strategic issues, the technical management team has resolved the issue on upper

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
														level reaching an agreement accepted by all.
14	**Non compatible operation plans of mixed passenger cargo UC's.**	Operational/ Business	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, Trikala, follower site of Geneva	72,0	**Moderate**	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	**Not materialised**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										viable solutions from the operational and business point of view are being 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				

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										everyday operation the mixed case will be decoupled and the common vehicle will be used either for passenger or for cargo transportation, at different timeframes of the Pilot.				
15	**Lack of sufficient traffic demand for platooning UC.**	Operational/ Business	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	Madrid, Trikala, Brainport, Karlsruhe	135,0	**Moderate**	The ability of this functionality will be demonstrated; even if used not frequently/ regularly at	**Not materialised**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										everyday operations during the Pilot. Traffic demand is definitely an aspect that the project cannot control, but can be simulated, if needed, for assessment reasons.				
16	**Contradicting needs and wants of AV's HMI between different vendors and Pilot sites.**	Behavioural Operational/ Business	No serious risk - there is room for alternative strategies among different vendors.	Alternative strategies among vendors.	During development phase.	WP7	Tampere	30	**Low**	Different ones (multivendor approach) will be applied and then benchmarked between then and with SoA.	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										WP7 (A7.4: HMI & Control/Handover strategies) will provide just the framework, some recommended elements, principles and guidelines but will allow each vendor/site to follow its own “look and feel”.				
17	**AI algorithms not leading to improved**	Technical	No enhanced services emerging as an	Technical fact. May be due to several reasons;	During development/ exploration phase.	WP5	Gothenburg, Linköping, Graz,	45,0	**Low**	Several alternative and complementary	**Not materialised. To**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
	or acceptable operational schemes.		outcome of SHOW.	insufficient basis provided by the sites; insufficient data, low interest, etc.			Salzburg, Carinthia, Tampere, Brno, Monheim, Trikala			algorithms for services will be employed within WP5 to be offered to the test sites. The AI services to be offered through WP5 are not blocking any operation; they are value added services provided on top of the existing planned services in	**be assessed at the end of the project.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										each test site.				
18	**Operators of PT at Pilot sites not ready to apply safely and efficiently the new AV-based operational schemes.**	Operational/ Business	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 (bureaucratic, operational, etc.) for delay.	During pre-demonstration phase (in first place).	WP11, WP12, WP15	Cross-cutting to all test sites.	144,0	**Moderate**	To be resolved through tight monitoring of the test sites plans (WP9), the demo sites communities (WP11, WP12) and appropriate training sessions (WP15) whenever applicable.	**Not materialised.**			
19	**Not enough or compatible data from**	Technical	No enhanced services emerging as an	Actual data missing (due to insufficient logging	During development phase.	WP5, WP10	Cross-cutting to all test sites.	70,0	**Moderate**	The relevant activities (WP5 and W10) will	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	previous research to develop AI algorithms and/or train simulation tools.		outcome of SHOW.	mechanisms, etc.) and/or unwillingness to share them.						use pre-Pilot data (from WP11) and intermediate sets of data from real-life tests. The Gantt Chart allows for recovery actions. If needed, external sources will be exploited.				
20	**Business models influenced and challenged by unexpected**	Operational/ Business	Disturbance in field trials process and local ecosystems	Competitive market by nature.	During pre-demonstration phase (in first place).	WP2, WP4, WP5, WP6, WP11, WP12	Cross-cutting to the sites.	81,0	**Moderate**	Relevant activities range over the whole project duration and will be open to	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	emerging competing services by third parties.		functioning .			, WP16				external stakeholders; ready to establish local alliances to emerging services (through the open architecture and API's of WP4 and WP5). Local demo communities continuous engagement as well as close monitoring and follow-up of the business plan and				

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										exploitation activities (WP2, WP16) are expected to tackle also with such aspects, if arisen.				
21	**Sentiment analysis (of A1.2) not possible to be legally performed in third party social media.**	Legal/Regulatory	Not the broadest possible impact that could be achieved.	IPR.	During the actual use of the tools from the first period of the project.	WP1	Not applicable.	12	**Low**	To be performed in project's own social media.	**Partially materialised.**	Concerning the full project and ITML as a performer.	Indeed, sentiment analysis was possible to be performed only on Twitter & Reddit.	The use of the feasible to use social media along with an appropriate treatment of analysis is considered

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
														sufficient for the project purposes.
22	**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	Madrid	34,4	**Low**	Partially covered through A7.4 HMI adaptability and personalisation.	**Not materialised.**			
23	**Lack of a clear governance on mobility data**	Legal/ Regulatory	Unsuccessful utilisation of data for feeding all the	Not clear picture on all the data types and the feasibility to	During development phase (in first place).	WP5	Cross-cutting to all test sites and	60	**Low**	A unified data registry has been constructed in WP5 to	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	encompassing lack of level playing field in data sharing (the user of the data should share back the enriched data).	Technical	different tasks (services and modules operation, evaluation, simulation and impact assessment).	get them. IPR issues. Unwillingness to share and abide to centralised principles of the project.			mentioned activities.			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 problems are emerging.				
24	**Lack of consumer**	Legal/Regulatory	Low participation in trials	Unclear or insufficiently communicat	During pre-demonstratio	WP3, WP9, WP11	Cross-cutting to all	112	**Moderate**	Specific data privacy and ethics	**Not material**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
	protection.		and user acceptance - complaints and problems in field trials execution.	ed data privacy policy.	n phase (in first place).	, WP12	test sites.		🟨	policy and evaluation protocols defined in the project to be applied by all sites.	ised.			
25	**Verification and validation 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	Before the approval of the final version of the technical validation framework.	WP11	Cross-cutting to all test sites.	20	**Low**	Active 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	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
			pilot/pilot phase.	certain site-specific aspects.						able to cover all site specific aspects.				
26	**Exceeding the capacity of JRC to test the vehicles during technical validation phase.**	Operational/ Business	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 test vehicles in the same period this capacity might be exceeded. In addition, the specific infrastructur	The risk to be detected during the technical validation phase (A11.2)	WP11	Ad-hoc for specific sites.	36	**Low**	Tight monitoring and scheduling of technical validation. Keeping a buffer timeslot for emergency cases, e.g. when some extra testing is needed. Providing a clear list of available tests and infrastructure by JRC. Obliging the	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
				e deemed necessary for some specific validation purposes might not be present at JRC site.						partners to "book" in time JRC for testing.				
27	**Covid-19 related cross-cutting effects.**	Operational/ Business	Delays in vehicle procurements and type approvals, permit processes, development and validation phases’ execution. Changes in demo sites creating	Mobility restrictions due to COVID affect technical work on field as well as the actual operation. Passengers’ engagement is also prohibited. Working routines, developmen	Monitored continuously, depending on the evolution of pandemic situation and related restrictions.	WP11, WP12	Gothenburg, Madrid	64,0	**Low**	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	**Partially materialised.**	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 expecte	Intensification of communication efforts and engagement strategies. Rescheduling of planne

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
			further delays. Economic crisis affecting demo sites resulting in even more further delays. Constraints regarding transport of passengers (allowed number of passengers). Finally, delay in the start of pre-demo and/or final demo phase.	t and permit 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 of real life scenarios. Operation routines of						all those fail and depending the size and duration of the pandemic, short extension of the project duration will be considered.			d. Cities priorities changed, at least for specific periods of time. In a lot of cases, Covid-19 has delayed considerably the actions and measures to be taken. Also, due to	d itineraries to make them denser. Planning of more local demo events to attract audience/passengers. Intensification of local ecosystem efforts for elimina

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
				scheduled trials inevitably affected as well.									Covid measures the amount of passengers allowed on the shuttles have to be reduced in all European countries, which puts in danger the fulfilment of the initial commitment	ting as much as possible the delays. A project extension will be asked to counterbalance the effects.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
													and target regarding transport of passengers and cargo.	
28	**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.	Cross-cutting to the whole project.	25,0	**Low**	Regular technical (virtual) meetings at all levels, daily monitoring and technical management constantly creating and maintaining liaisons and	**Not materialised.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										synergies, several management mechanisms applied.				
29	**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 demo phases.	WP11, WP12	Gothenburg, Tampere, Madrid	60,0	**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	**Partially materialised.**	So far, three critical 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

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										pre-demo phase in each site. Safety 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 occurrence.				iteration.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										Iterative optimisation and support from OEM with s/w upgrades, when applicable, to eliminate incidents.				
30	**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 and continuous/ seamless follow-up of the trials.	WP11, WP12	In principle, applicable to all test sites.	32	**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	**Not materialised or if materialised was done on purpose for better outcomes or enriching the routes of the site maximising the service.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										Use Cases to other sites of the Mega Site.				
31	**Insufficient numbers of safety operators recruited.**	Demonstration/Evaluation	Delay in the start of pre-demo and/or demonstration phases, shortened pre-demo and/or demonstration phases, less trips - smaller service coverage.	Limited financial and time resources available. COVID related effects.	Continuous monitoring and recruitment process since the very beginning of the project.	WP11, WP12	In principle, applicable to all test sites.	35	**Low**	Early awareness and engagement campaigns in each site to recruit safety operators. When needed, conduct of dedicated training sessions to endorse drivers not familiar to automation.	**Partially Materialised.**	Madrid/Carabanchel	EMT drivers not trained in the use of the ɑautonomous Gulliver. No drivers available for the Irizar bus.	Theoretical and practical training sessions organized to train both EMT personnel and outsourced drivers for the

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
														Irizar bus.
32	**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 are not enough for longer testing, COVID-19	Continuous monitoring; first evidence since the first year of the project.	WP11, WP12	Could be applicable to all test sites.	216	**Moderate**	Flexibility in the conduct of the field trials; short extension of the project; identification of further metrics for success of demonstration activities (e.g. number of trips conducted).	**Partially materialised (as an anticipation).**	Madrid/Villaverde	Several sites have acknowledged such a risk. Still, the exact deviation will be evident at the last year of the project, since there are continuous efforts	All possible efforts are being made from all possible ends in order to eliminate the risk as much as possible. Among other,

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
				related effects.									on-going to mitigate this.	services have been tried to become denser to attract sufficient number of passengers and conduct bigger number of trips at a shorter period of time.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
														In the last year of the project, a project extension will be discussed with the PO, as one of the mitigation measures.
33	**Insufficient localization on the test route.**	Technical	High degree of localization uncertainty	Poor GNSS-RTK localization.	During the technical validation phase hopefully for	WP11, WP12	In principle, could be	120	**Moderate**	Adaptation of the used method; exploration of other	**Partially material**	Gothenburg, Madrid/Carabanchel	Planned routes could not be run in	Changed place of antennas and

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
			is expected to be potentially creating safety risks and services insufficient operation.		the first time, before starting the actual field trials and apply corrective actions in time.		applicable to all sites.			possible localisation methods exploiting the cooperative context; optimisation of the placement of GNSS antennas; use of GNSS correction method provided by BOSCH (WP8).	**ised.**		auto-mode in some cases.	used combined transmitters. Restart corrections service to reinstate RTK mode for high precision in GNSS module.
34	**Insufficient 4G coverage on the test route.**	Technical	Connectivity uncertainty is expected	Poor 4G coverage.	During the technical validation phase hopefully for	WP11, WP12	Gothenburg, Madrid	64	**Low**	Identification of factors that lead to poor 4G coverage	**Partially material**	Madrid/Carabanchel/WP11 (as an example; similar in a	Corrections for GNSS and MQTT	To mitigate the safety risk,

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
			to be creating safety risks and services insufficient operation.		the first time, before starting the actual field trials and apply corrective actions in time.					and in-time technical mitigation. Mitigation actions for at least preventing accidents (i.e. acknowledgment of safety driver).	**ised.**	couple of other cases as well)	connectivity is halted.	connectivity alert is presented at safety driver HMI, and automated driving services do not start again until cellular internet is available.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
35	**Test permits are not issued in time.**	Legal/Regulatory	Delay in the start of pre-demo and/or demonstration phases and/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 regulations that undergo continuous revisions.	Since the first year of the project when the permit processes have started and continuously.	WP3, WP11, WP12	In principle, can be emerging as a case in all test sites.	126	**Moderate**	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. Continuous effort in local demo communities to engage	**Partially materialised.**	Copenhagen site(MOVIA), Turin site (LINKS), Graz site (VIF), Madrid (Villaverde). All incidences have been resolved in alternative ways so far apart from Villaverde case in Madrid.	In Copenhagen the usual process has been very long and cumbersome; this was not possible to be resolved in time and led (together with other reasons) to the	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.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
										relevant stakeholders responsible for giving permits. 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. In the worst case,			shift to another site that would assume Copenhagen use cases (extended Tampere). In Turin, the current legislation does not cover SHOW plans; thus an exemption has been	Graz), 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 regulati

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟨	change/shift of site.			asked. In Graz, there was a gap for passenger AVs and as such a new legislation text was on-going; released in early 2022. In Madrid, in specific there have been difficulties to	on that 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 test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
													get permits which also related to difficulties to adapt the road infrastructure to the demo needs. Also, risks due to the topology of the road, many intersections	granted to the Turin site of SHOW. In Madrid Site, extensive work has been done to accelerate the technical inspection for the vehicle Gulliver and work

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
													with high risk of clasehs with regular traffic make the permit grant more challenging.	has been done with the city council to create a sandbox area so that the regulatory process is faster than normal and that the tests can be

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
														conducted in a real environment without risk to the AVs or regular vehicles (for Villaverde).
36	**Low number of passengers**	Demonstration/Evaluation	Cannot reach the number of passengers stated in the GA; no effect on the technical performance,	COVID-19 related effects; ineffective awareness and engagement strategies in local sites; overambitious targets.	During the first months of the final demo phase across test sites.	WP9, WP12	Cross-cutting to all test sites.	180,0	**Moderate**	Effective awareness and engagement campaigns. More intense engagement of fewer users as a	**Cannot be assessed at this stage.**			

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
			however, proved impact will be less significant.							back-up plan; endorsement of "focus groups" and "supertesters". Recruitment of users from the extended SHOW Consortium.				
37	**Critical changes in vehicles or demo sites plans - unavailability of vehicles, cities segments, not**	Demonstration/Evaluation	Risk lies in need to change a part/element of the pilot (vehicles, routes, services) or totally replace it for a	COVID-19 related effects (related also to financial crisis) mainly; technical and operational challenges (including permits and	Continuous monitoring since the very beginning of the project and resolution case by case, through numerous technical	WP11, WP12	In principle, applicable to all test sites.	75,0	**Moderate**	Recognition of mitigation actions ad-hoc depending the case. On-going amendment processes to tackle with each issue separately,	Materialised (all issues recognised tackled in the cont	Eindhoven/Brainport; Copenhagen site; Aachen site; Rennes site; Turin site, Salzburg Site	All critical issues as have been outlined and addressed in Amendment 2.	All specific to site mitigation actions, as reported in Amendment 2.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
	applicable routes, etc.		variety of reasons.	safety risks related to routes selection, i.e. dense traffic routes) hindering the realisation of the plan.	management mechanisms.					if needed. At the time of writing, all cases recognised in the past have been resolved in the context of Amendment 2.	ext of Amendment 2).			
38	**Software problems on the vehicle.**	Technical	Pause/delay in operation.	Software problems/malfunctions of several types.	Experiencing the problems in real life demonstration phases.	WP11, WP12	In principle, applicable to any site.	140,0	**Moderate**	Continuous exchange with OEM and supervision. Ad hoc optimisation/replacements of failing components. Purchase components in stock.	**Partially materialised (resolution of problems ad**	Carinthia site, Madrid site, Turin site, Gothenburg site, Tampere site	Encountered several types of problems during operation. Delivery of some components for the automat	Continuous exchange with OEMs; replacement of components. In Madrid, for

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟨	Consideration of backup plan with different components or components utilised by affiliated entities and projects (whenever possible).Identifying in the pre-demo phase which are the safe conditions boundaries that AVs can operate without problems.	**hoc).**		ization of vehicles are delayed affecting inevitably the development/ integration process, especially in research based sites. Running of AVs under heavy rain,	example, the pending components are currently being borrowed by a research institute which cooperates with EMT. In other cases, h/w compo

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
									🟨	Optimising as much as possible vehicles technology on the basis of the technical validation and pre-demo phase outcomes.			snow or temperatures around - 10-25 degrees C has been creating some technical problems, some of which cannot be overridden through the current vehicle technology in	nents have been replaced by OEMs or s/w upgrades have been done remotely. Make a Spare part plans with OEM have been made (lesson learned).

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
													place. In other cases, failing components led to pause of operation for safety reasons.	
39	**Wrongly parked vehicles during field trials**	Operational/ Business	Jeopardisation of AVs operation.	Inappropriate parked vehicles along the route of AVs.	Experiencing the problems in real life demonstration phases.	WP11, WP12	Tampere, Gothenburg, Turin	90,0	**Moderate**	Plan for routes with margin from the parking lots. Manual overtaking for specific parts of the route. Collaboratio	**Partially materialised.**	Gothenburg site	Parked cars along the route of the AV necessitating manual	Replan routes with margin from the parking lots.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	**Description of problem/ difficulty**	**Specific mitigation measure(s) taken/ planned**
										n with local authorities for maintaining clear routes during AVs operation.			overtaking.	
40	**Bottlenecks in demonstration of planned logistics cases.**	Demonstration/Evaluation	Planned logistics cases may not be fully demonstrated and assessed or launch time may be delayed. It may also cause a slight delay on the impact assessment works, cargo units	Technical/ service level barriers; legal/regulatory barriers (lack of regulation and legal aspects regarding logistics case study implementations in an urban area); low interest/ engagement of relevant City and site	During demonstration phases and their planning.	WP9, WP10, WP11, WP12, WP13	Carinthia, Karlsruhe, Trikala (new French site - Crest Val de Drôme), Geneva follower site	72	**Moderate**	Establishment and continuous effort of logistics task force - regular technical meetings planned both bilateral and with all logistics sites partners. In the worst case scenarios,	**Partially materialised (although on track).**	Several sites have acknowledged multiple types of problems that are under resolution in an on-going manner or have been already resolved.	Several challenges have been detected related to regulatory issues (unclarity of regulations regarding "how to apply	Continuous and bilateral monitoring and support (in relation to scenarios and KPIs clarification

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
			transported, data collection, as well as other relevant topics as simulation input-data, business model data collection, etc.	stakeholders and/or "clients".					🟨	logistics will be demonstrated/ assessed in a more confined manner as a proof of concept.			automated logistics on city roads" and "what are the requirements"), technical development requirements, some of them related also to Covid-related effects (i.e. start of	and development of service(s) to the logistics pilot sites.

#	Risk Definition	Type of Risk	Risk Effect	Risk Cause	Risk Detection	Relevant WPs	Applicable test sites	Consolidated Overall RN	Risk Level	Risk Mitigation Measures	Risk Materialisation Status	(So far) materialisation		
												Overall & on Pilot site/Partner level (if applicable)	Description of problem/ difficulty	Specific mitigation measure(s) taken/ planned
													respective operation).	