SHared automation Operating models for Worldwide adoption

SHOW

Grant Agreement Number: 875530

D11.1: Technical validation protocol

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

The aim of this deliverable is to provide a methodology considering systems involved in SHOW pilots, considering vehicle safety and performance, cybersecurity and the communication of the vehicle with the infrastructure and the Mobility Service management service. The two levels of vehicles 1) "Market deployment" level – vehicles provided commercially by OEMs with the required AD functions; 2) "SHOW deployment" level – prototype vehicles developed mainly by research partners, will be considered in the methodology definition.

Apart from the layers, the technical assessment protocol of SHOW consists in two distinct phases, as follows:

1. **Technical verification & commissioning phase,** on individual technical aspects, including the typical vehicles commissioning and other standard processes required from the legislation perspective, among other. This phase addresses four key technical aspects, namely: **AD vehicle safety**, **Performance**, **Communications** and **Cybersecurity**. This phase will be conducted in either own premises of the test sites and their OEM's or at Ispra site that is described in this document. There has been defined 7 test communication test scenarios, 8 performance test scenarios and 4 safety test scenarios.
2. **Technical validation/commissioning on integrated service level phase**, which corresponds to a full and in-depth technical validation and commissioning on the planned integrated service level in each site. This Phase follows given the successful completion of the former one. Validation here is applied on Use/Demonstration case level of each site as planned and described in D9.2 experimental plans and it aims to address **Safety**, **Performance** and **Quality of Service**. This phase will be conducted in context. Meaning in the exact same real-life context that the pre-demo and final demo phases will be conducted.

In order to address the key aspects of the **technical verification & commissioning phase,** a set of technical requirements have been compiled. Based on these requirements, a set of common to all test scenarios have been created in order to be executed in all the SHOW Test Sites. The methodology focuses on procedures, not in technical results, which is the objective of the subsequent Deliverable of WP11, namely D11.2. For this reason, test case definitions and verification descriptions provided herein, are based on a generic approach and take the appropriate check points (to respond to the technical requirements) into consideration as well as potential different configurations that may emerge depending the variation of the context of each test site.

The technical validation phase will commence in the project right after the final release of the current protocol. The Appendices of this document provide the templates to be used for the reporting of results across all test sites and across both phases as listed above. The results of both phases will be reported in D11.2: Demos safety, reliability and robustness validation and commissioning.

Document Control Sheet

Start date of project:	01 January 2020
Duration:	48 months
SHOW Del. ID & Title:	Deliverable 11.1: Technical validation protocol
Dissemination level:	PU
Relevant Activities:	A11.1: Technical verification
Work package:	WP11: Technical verification & pre-demo evaluation
Lead authors:	Jordi Pont (IDIADA)
Other authors involved:	Maria Gkemou, Ioannis Gkragkopoulos (CERTH/HIT), Maria Alonso Raposo, Fabio Marques Dos Santos, Fabrizio Minarini, Biagio Ciuffo (JRC), Sophie De Lambert De Boisjean, Amine Boussouf (NAVYA), Anastasia Bolovinou (ICCS), Laura Coconea, Alberto Bellini, Alessandro Cerutti (SWARCO).
Internal Reviewers:	VALEO & IRIZAR
External Reviewers:	N/A
Actual submission date:	13/07/2021 (M19)
Status:	SUBMITTED
File Name:	SHOW_D11.1_Technical validation protocol_SUBMITTED

Document Revision History

Version	Date	Reason	Editor
0.1	02/03/2021	Table of contents, validation topics, requirements descriptions and cybersecurity methodology	Jordi Pont (IDIADA)
0.2	19/05/2021	Update on requirements and test cases sections	Jordi Pont (IDIADA)
0.3	26/05/2021	Update on sections after A11.1 meeting	Jordi Pont (IDIADA)
0.4	30/06/2021	Final contribution on all the sections	IDIADA, CERTH/HIT, NAVYA, SWARCO
0.5	01/07/2021	Internal review	JRC, CERTH/HIT, IDIADA
1.0	01/07/2021	Version sent for internal peer review.	IDIADA
2.0	13/07/2021	Peer reviewed version sent for submission.	IDIADA
2.1	14/07/2021	Final check for submission	Henriette Cornet (UITP)

Table of Contents

List of Tables

List of Figures

Abbreviation List

Abbreviation	Definition
ACC	Adaptive Cruise Control
AD	Automated Driving
API	Application Programming Interface
AV	Automated Vehicle
CAM	Cooperative Awareness Message
CCAV	Centre for connected and Autonomous Vehicles
CVE	Common Vulnerabilities and Exposures
DdoS	Distributed Denial of Service
DoS	Denial-of-Service
EU	European Union
FERMA	Federation of European Risk Management Associations
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Transport System
KPI	Key Performance Indicator
LFMP	Local Fleet Management Platform
MitM	Man-in-the-middle
MQTT	Message Queue Telemetry Transport
OBD	On-Board Diagnostics
ODD	Operational Domain Design
OEM	Original Equipment Manufacturer
PT	Public Transport
PTO	Public Telecommunications Operator
RSU	Road Site Unit
RTK	Real Time Kinematic
SAE	Society of Automotive Engineering
SMDP	Show Mobility Data Platform
SREM	Signal Request Extended Message
SSEM	Signal Request Status Extended Message
TLA	Traffic Light Assistance
TMC	Traffic Management Centre
UC	Use Case
USB	Universal Serial Bus
V2I	Vehicle to Infrastructure

1 Introduction

1.1 Purpose and structure of the document

The goal of the document is to define a common technical validation methodology to be executed in all test sites participating in SHOW Project. The main topics of the validation will be safety and performance of the vehicle, communications a cybersecurity in the first technical verification phase, while in the second technical validation phase it is safety, performance, and Quality of Service. This methodology will be followed and necessary to be executed by all the Pilot Sites before performing the public demos.

The deliverable includes 8 main chapters and two appendices containing the following information:

Chapter 1 – Introduction.

Chapter 2 – Methodological approach.

Chapter 3 – SHOW Technical Verification and Commissioning Site

Chapter 4 – Technical Requirements.

Chapter 5 – Test scenarios for Technical Verification & Commissioning Phase.

Chapter 6 – Cybersecurity approach.

Chapter 7 – Technical Commissioning on Integrated service Phase.

Chapter 8 – Conclusions.

Appendix I – Technical verification & commissioning reporting template.

Appendix II – Technical validation & commissioning on integrated service level.

1.2 Intended Audience

On the one hand, this document serves as a manual for the partners involved in WP11 and the SHOW Test Sites responsible by applying the protocol for their site, reporting, finally, the results that will emerge. On the other hand, it serves as an informative document describing the technical assessment protocol, that is relevant to CCAM in general, and can be useful for a series of other external parties that are interested to either build on it, endorse it or apply it to conduct their own assessment.

1.3 Interrelations

A11.1 is a central activity in SP3 interacting with WP9: Pilot plans, tools & ecosystem engagement and WP13: Impact assessment and being a prerequisite for WP12: Real-life demonstrations of the same SP. D11.1 has used inputs from SP1 (WP1 and WP3) and from SP2 (WP4, WP7 and WP8).

Input:

- Use cases definition and prioritisation in A1.3 (SHOW Use cases) has been the basis for the verification and validation methodology, since it defined aspects to be considered as operation speed, traffic and environmental context of operation, operational and technical dependencies and restrictions, etc.
- SHOW specific legal/regulatory and institutional restrictions in A3.1 (Legal requirements at European and sites level) which led to requirements to consider in the methodology.

- Requirements for communication and the cybersecurity module for SHOW in A4.2 and A4.3 (Communication layers, protocols and services and Cybersecurity module), since are two of the main aspects to be tested to ensure the safety, security and robustness of the vehicles.
- Detail regarding the automated vehicles functions to be implemented in the demo vehicles (WP7- Automated vehicles functions), since they have direct impact in the safety performance of the vehicles.
- Infrastructure system requirements from WP8, since the key layers of communications must be verified.
- Identification of instrumentation and data to be gathered from the vehicle in the demos in A9.2 (Capturing and monitoring tools) to include within the data readiness evaluation.
- Available and suitable technical and operational KPIs in A13.6 (Overall impact assessment and cross pilot comparisons) will be considered as criteria for test cases evaluation.

Output:

- Technical verification is needed for the deployment of real-life demonstrators in WP11 and WP12 pre-demo and final-demo phases respectively.

2 Methodological Approach

2.1 Overall approach

The methodology followed to create the technical assessment protocol in SHOW is as follows. Technical assessment in SHOW consists of two phases; one on technical verification level on individual technical aspects and one full technical validation and integrated service commissioning level that follows given the successful completion of the former one. The distinction among the two phases follows below:

- **Technical verification & commissioning phase**: Technical verification in SHOW will be accommodated by a series of test cases. A Test Case in the SHOW context is a concrete scenario with PASS/FAIL criteria. It is a set of requirements and variables against which the system will be tested and assessed. The results will determine whether the system complies with the respective requirements and satisfies the acceptance criteria. The process of developing test cases can also help to find problems in the requirements definition or design of an application/solution The test cases are tangibly described through a series of test scenarios on key aspects that have been designed in such a way so as to be common and parametric to all sites and be use cases and operational context agnostic (as much as possible). Those are provided in Chapter 5 of this document and have been designed to address the technical requirements of the project that have been consolidated and provided in Chapter 4 of this document.

  This phase results will be reported by each site on the basis of the template that is provided in Appendix I. The test scenarios are designed to ensure that the corresponding project objectives will be addressed. Still, as they related to commonly met aspects in road automation, it may be the case that some of the sites may have already tested them – partially or fully – in the context of audit processes required in the context of vehicles homologation (granting of approval by an official authority), commissioning (analysis of the design, installation and operation of the systems, with the intent of achieving the maximum design efficiency and expected operational performance) or test sites permits (official document giving the test site authorization to perform the tests); this latest phase depending the formality in each test site may belong also to the next technical validation phase. If this is the case and to the degree it is applicable, the test conductor – as shown in the template of Appendix I – is requested to provide the results of the respective test and all the relevant information as well as the evidence for the test conduct. It could be also the case that for this phase, the test conductor may vary depending the type of the test and include a series of entities, such as the vehicle provider, the site operator, a technical entity working on integrating solutions, etc.

- **Technical validation/commissioning on integrated service level** phase: Technical validation in SHOW follows technical verification and considers as a prerequisite that technical verification has been successful. A Use Case represents a specific scenario in which a solution, usually the system that is being developed, needs to be implemented. The use case describes various operational conditions in which the system shall respond. These conditions can be interactions from the system’s user, other traffic participants or road and other environmental conditions. For test objects having several functionalities it is expected to have several use cases.

  As such, this phase operates on Use/Demonstration Case and site operational level. It is totally specific to the project as well as each project test site and also on the way each use case will be configured and implemented for each site. The demonstration cases are provided in D9.2 [2]; are not repeated therein.

The assessment that will be conducted on this level will be conducted on test site level, it is **mandatory for all test sites** and regardless the type and number of entities that will be involved in that, it is the test site obligation to make sure that it will be conducted following the principles provided on Chapter 7 and that the results will be reported in accordance to the template provided in Appendix II. The successful outcome of this phase will directly mean a Pass to the pre-demo phase that will follow.

This methodology is based mainly on the H2020 research project HEADSTART (Harmonised European Solutions for Testing Automated Road Transport) which main objective is to define testing and validation procedures of Connected and Automated Driving functions including key technologies such as communications, cyber-security and positioning. Still, it is further enriched according to the contributing Partners expertise.

2.2 Scenarios definition

To define a test run, is necessary to identify and describe the test scenarios:

- **Functional scenario**. This level contains the high-level description of the test procedure, using words and images to describe the sequence. In this level, the scope, testing procedure, needed operational domain and acceptance criteria will be defined.
- **Logical scenario**. This level defines a range for each of parameters defined during functional scenario. Test executions is described more in detail using the layer model and linking the defined parameters to each concept in the test description and execution steps. A model for a systematic description of scenarios has been defined with the following six independent layers, restricting this large parameter space to the operational design domain (ODD) of the test object provides a full test space of the system.
- **Concrete scenario**. This level defines each specific parameter value and the step-by-step test sequence. The test results must be compared with the acceptance criteria, signals behavior and requirements.

We have integrated and adapted to the needs of SHOW project the three levels of scenarios, defining a unique level called test scenario which includes all the necessary information to execute it.

2.3 Technical aspects covered by the methodology

The aspects covered by the methodology are:

1. AD vehicle safety. To ensure that vehicle is safe to drive in public roads.
2. Performance. To ensure a minimum level of vehicle and devices performance.
3. Communications. To ensure a good communication between vehicles and devices.
4. Cybersecurity. To cover and mitigate all the possible cybersecurity risks.

The methodology only focusses on procedures, not in technical results. For this reason, test case definitions and verification descriptions are based on a generic approach and take the appropriate check points into consideration.

The result of the tests from the methodology will be PASS / NO PASS / PARTLY PASS.

3 SHOW Technical Verification and Commissioning Site

3.1 Introduction

In order to allow all project partners to apply the verification methodology laid down in the present deliverable, a technical verification and commissioning site has been established within the project. The Ispra site of the European Commission Joint Research Centre has been made available to carry out verification activities required by the different vehicles and systems included in the project. Access to the Ispra site was open to all project members, although it was considered from the beginning it to be particularly suitable for vehicles and systems developed by research and academic institutions without access to in-house testing capacity.

On this basis, the vehicles that will be transferred to the Ispra site, to current knowledge, are the passenger vehicles that will support the on-demand and first and last miles services of the Trikala and Turin satellite sites, provided by CERTH/HIT and Links respectively and retrofitted from Luxoft, among other. Still, further needs may emerge in the coming weeks (as of the current Del.issue). The updates will be reported in D11.3: Demos safety, reliability and robustness validation and commissioning.

A description of the JRC Ispra site and of the infrastructure and equipment available for the technical verification of the SHOW vehicles and systems, upon the test cases as defined in Chapter 5, is provided in the following sections.

3.2 The Ispra Site of European Commission Joint Research Centre

The JRC is the European Commission's science and knowledge service. Its scientific staff and research infrastructures are deployed over six campuses (or 'sites') in five EU countries. The site part of this project is the Ispra site, in the province of Varese (Italy), which is the 3rd largest premise of the European Commission after Brussels and Luxembourg and located 60 km northwest of Milan.

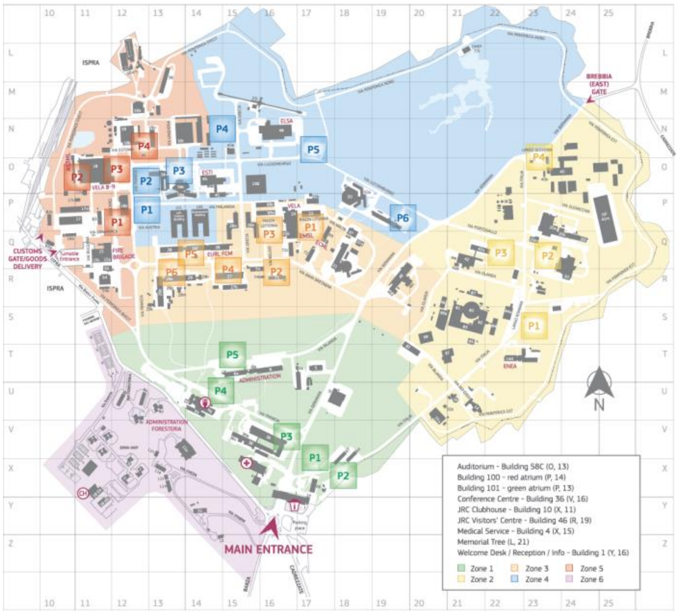

BREBBIA (EAST) GATE
CUSTOMS GATE/GOODS DELIVERY
MAIN ENTRANCE
ISPRA
ELSA
ESTI
FIRE BRIGADE
ADMINISTRATION
ADMINISTRATION FORESTERIA
ENEA
N
Auditorium - Building 58C (O, 13)
Building 100 - red atrium (P, 14)
Building 101 - green atrium (P, 13)
Conference Centre - Building 36 (V, 16)
JRC Clubhouse - Building 10 (X, 11)
JRC Visitors' Centre - Building 46 (R, 19)
Medical Service - Building 4 (X, 15)
Memorial Tree (L, 21)
Welcome Desk / Reception / Info - Building 1 (Y, 16)
Zone 1
Zone 2
Zone 3
Zone 4
Zone 5
Zone 6

Figure 1: Schematic representation of the JRC-Ispra site and its functional zoning.

The site features a daily population of roughly 2.200 Commission staff in over 100 buildings, 36 km of internal roads, and all the logistical services that are necessary to run a small town, including energy generation and water provision. All this in a fenced-in area of 167 ha providing a safe and secure, yet real environment, in which the JRC applies Italian law (related to safety, transportation, highway code and such like) under its own responsibility. A schematic representation of the site is reported in Figure 1.

3.3 Infrastructure available for testing

3.3.1 Road infrastructure

The whole road network included in the functional zones 1, 3, 4, 5 can be used for validating safety and drivability of the vehicles included in the project. This area includes a wide variety of infrastructural elements, from straight road segments to curves, to roundabouts, various types of zebra crossing areas, different layouts of parking areas, different types of asphalt conditions, etc.

In order to ensure the safe execution of the tests, during the project, a specific procedure has been set up to reserve one or more parts of the infrastructure to the exclusive use of the tests. In this case, with the support of the site management department, the interested portion of the road network will be closed to external traffic and the access to it safeguarded by dedicated operators. However, in the case that the technology readiness level of the vehicle/system would require a more controlled environment, the area of the Ispra site highlighted in Figure 2 can be used for testing in urban driving conditions. This area is composed by a 600m long closed circuit with three intersections and a roundabout. The area is normally closed to road traffic and therefore is has higher flexibility for hosting vehicle tests.

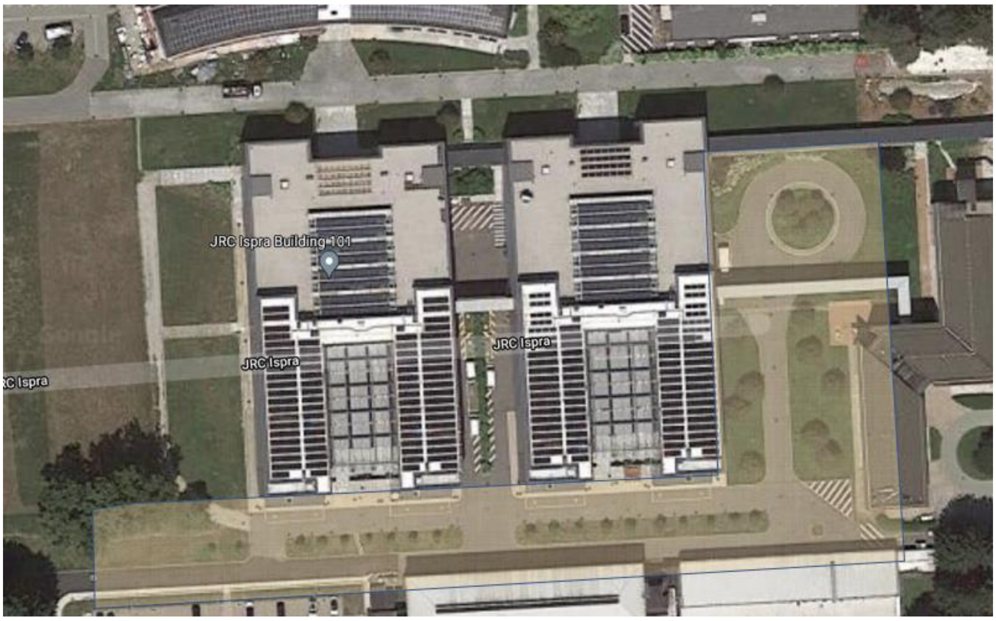


Figure 2: Urban track of the JRC Ispra site.

The only infrastructural element currently unavailable on site are traffic lights. This may represent a problem since many automated driving systems will rely on traffic lights and the capability to communicate with them in order to safely and efficiently merge with the traffic flow especially in urban contexts.

In order to allow testing static and cooperative interaction with signalized intersections as described in test cases defined in Chapter 5 in collaboration with the SHOW partner n.35 (Swarco Mizar), as will be specified in the amendment request n.1 to the grant agreement, cooperative traffic lights to regulate two intersections of the JRC urban track are being installed as specified in Figure 3.

The cooperative system will allow testing several types of C-ITS services for both the automated systems to be validated and the other road users, in order to test interoperability and efficiency of the strategy adopted and to assess the potential benefit of traffic management 2.0. Among the services that the system will allow, the green light optimised speed advisory, the time to green and the automated driving systems prioritization are among the most interesting ones for SHOW related solutions.

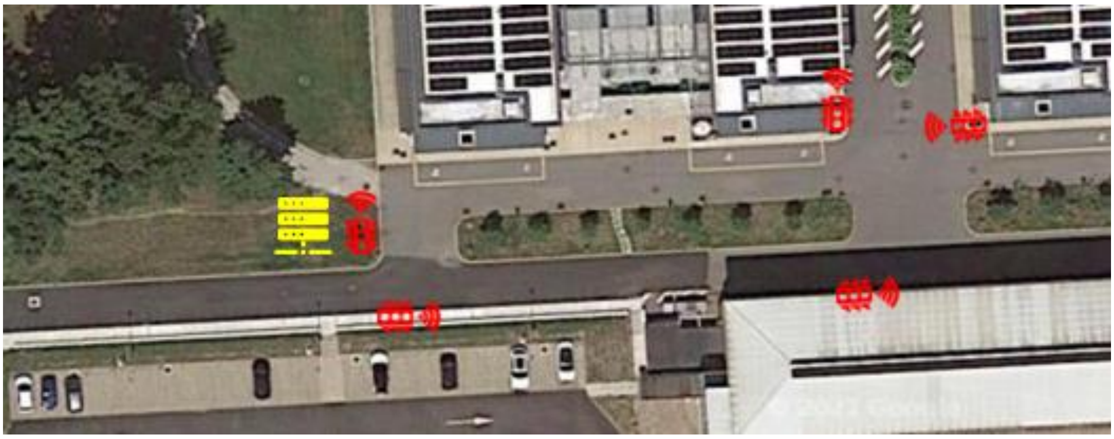


Figure 3: Layout of the cooperative traffic lights and the road side unit installed at JRC Ispra by Swarco Mizar.

3.3.2 Communication infrastructure

In terms of communication and network coverage, the site hosts an internal base-station of a 4G commercial operator. For this reason, latency and power of the existing system allows the testing of vehicle teleoperation and other remotely controlled services (although for the full deployment of the service on site a 5G network would be required). In addition, on site there is availability of both ITS-5G[1] and LTE-V2X[2] road site units to allow cooperative vehicle to infrastructure testing in case foreseen by the automated vehicle/service to be tested on site.

3.3.3 Testing equipment

Finally, in order to validate the capability of automated driving systems to safely interact with other road users, a series of soft targets for vehicle safety testing have been procured. This includes:

- a 2D soft vehicle target
- a 3D foam vehicle target
- a pedestrian dummy (adult)
- a pedestrian dummy (child)
- a dummy cyclist

Pictures of the available targets are included in Figure 4. All safety targets are compliant with EU standards for vehicle safety tests and allow the test of various types of driving scenarios without risks for vehicles, drivers, and other road users.

[1] https://cohdawireless.com/solutions/hardware/mk5-rsu/

[2] https://cohdawireless.com/solutions/hardware/mk6c-rsu-evk/

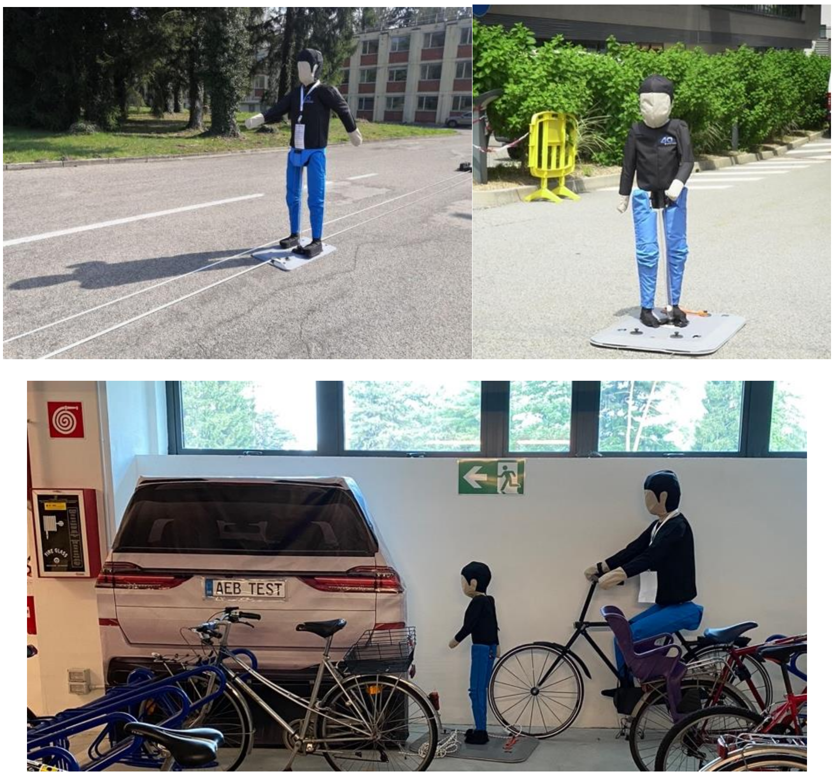


Figure 4: Example of targets used for vehicle safety testing.

4 Technical requirements

4.1 Introduction

This section describes the requirements that the test scenarios for the technical verification phase are designed to meet.

Each High-Level Requirement contained in this document meets the following conditions:

- Atomic - A requirement cannot be divided into smaller units
- Understandable - A requirement shall be clear and simple to read
- Testable - Any test engineer must be able to test and validate a requirement
- Justified - Every requirement must have a justification.

4.1.1 Use of words

Use of words "shall", "should", "must", "will" and "may" within this document shall be according to the following criteria:

- **"Shall".** The word SHALL expresses a mandatory requirement on the system to which this document refers to.
- **"Should".** The word SHOULD expresses a recommendation or advice on implementing such a requirement of this document. Such recommendations or advices are expected to be followed unless good reasons are stated for not doing so.
- **"May".** The word MAY expresses a permissible practice or action. It does not express a requirement of this document.
- **"Must".** The word MUST expresses a levied requirement on another system.

4.1.2 Definitions

Calibration parameter: Parameter that can be tuned to modify the performance of the function but it is not accessible for the driver to modify since its value has been settled before production. These parameters can only be modified by calibration specialists.

Configuration parameter: Levels of customisation provided to the driver to adjust the performance of the function depending on user preference.

Forward vehicle: Vehicle in front of the subject vehicle and moving in the same direction and lane as the subject vehicle, or which is oriented in the same direction if it is not moving

Stationary vehicles: Any vehicle that is currently not moving. A distinction can be made between the following cases:

> **Stopped vehicle:** Any vehicle which is currently not moving, but it has been, at some time, detected by the system as a moving vehicle.
>
> **Parked vehicle:** Any vehicle which has always been detected by the system as not moving.

Subject vehicle: Vehicle equipped with the functionality described in this document.

Vehicle: Any licensed/able to be licensed motor vehicle intended for use on public roads, i.e. motorcycles, cars, light trucks, buses, motor coaches, and other heavy vehicles.

4.1.3 Requirement identification

The requirements defined in this document shall have a unique requirement ID. The ID shall be composed by a fixed field and a variable number.

The proposal for SHOW project is:

Fixed field: **SHOW_**

Variable field: **01** (Safety), **02** (Performance), **03** (Communications)

Variable number: **001, 002, 003**...

Example for a communication requirement ID:

SHOW_03_001

Example for a safety requirement ID:

SHOW_01_001

4.1.4 Requirements format

ID	*Requirement unique identifier*
Use Case	*Use case where the requirement affects*
Description	*Description of the requirement following the guidelines described in the previous section*
Relevant Pilot Site	*Pilot Site where the requirement should apply*
Relevant Activity	*Task where the requirement has been defined*
Requirement issuer	*Partner responsible for the requirement definition*

Table 1 Requirement format template

4.1.5 List of technical requirements

4.1.5.1 Safety Requirements

Table 2: Safety requirements.

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_01_001	All	Redundant lane markings at bus stops/bays must be removed to minimise any adverse effects on lane keep assist systems.	All applicable	A8.1, A7.1, A7.2	AIT

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_01_002	All	Road agencies must stop the practice of mixing yellow and white pavement markings on construction sites.	All applicable	A8.1, A7.1, A7.2	AIT
SHOW_01_003	All	Pilot site managers must improve longitudinal pavement markings at intersections to support AVs.	All applicable	A8.1, A7.1, A7.2	AIT
SHOW_01_004	All	Pilot sites must improve current pavement marking asset conditions to improve the brightness and quality of lane markings.	All applicable	A8.1, A7.1, A7.2	AIT
SHOW_01_005	All	Road agencies should maintain traffic signs in flawless conditions, namely replace worn out signs, maintain their proper position, and make sure there is no obscured visibility.	All	A8.1, A7.1, A7.2	AIT

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_ 01_006	All	Regulators may establish unified system of machine-readable signs that could be used for easier recognition by perception systems of AVs.	All	A8.1, A7.1, A7.2	AIT
SHOW_ 01_007	All	Pilot sites must make sure there are no obstacles around the route, including intersections, that could create problems for perception systems of AV to detect incoming traffic in time. Obstacles include static and dynamic obstacles that are not anticipated to be on the route. In the same context, pilot sites and municipalities must attend to the vegetation maintenance on the side road and cleaning of the road.	All	A8.1, A7.1, A7.2	AIT, NAVYA, TRANSDEV
SHOW_ 01_008	All	Pilot sites must make sure all the parked cars are correctly parked and have pre-defined parking lot	All	WP7	NAVYA, TRANSDEV

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
		zones on the AV’s route.			
SHOW_ 01_009	All	The AV shall avoid collisions with obstacles that could lead to a dangerous situation (for the passengers or other road users).	All	WP7	NAVYA, EASYMILE
SHOW_ 01_010	All	The AV shall never leave its lane unless explicitly asked/intending to do so.	All	WP7	NAVYA, EASYMILE
SHOW_ 01_011	All, especially UC1.7	The safety driver (and/or the remote operator is the responsible one according to the legislation) shall be able to override the automated driving functionality with emergency functions/mechanisms/processes at any moment.	All (if applicable)	A7.4	IDIADA

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_01_012	All, especially UC1.7	The safety driver (on-board) shall be notified about the need to takeover control at the end of ODD and the notification should be given with the appropriate modality and at the appropriate time to ensure a safe handover of control.	All (if applicable)	A7.4	ICCS
SHOW_01_013	All, especially UC1.7	The safety driver (on-board) shall be warned about the need to takeover control due to an emergency and the warning should be given with the appropriate modality and at the appropriate time to ensure a safe handover of control	All (if applicable)	A7.4	ICCS
SHOW_01_014	All	The loss of communication from an obstacle detection sensor shall lead to stop the AV.	All	WP7	NAVYA, EASYMILE
SHOW_01_015	All	The loss of localization function shall lead to stop the AV.	All	WP7	NAVYA, EASYMILE

4.1.5.2 Performance Requirements

Table 3: Performance requirements.

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_02_001	ALL	The local fleet management cloud platform (LFMP), when available, and the SMDP (SHOW Mobility Data Platform) shall support storage of big data from continuous operation.	All applicable	A4.1, A5.1	ICCS, CERTH/ITI
SHOW_02_002	ALL (when applicable)	V2X packet loss ratio: Packet loss ratio should not exceed 10%.	All applicable	A8.2, A7.5	CERTH/HIT
SHOW_02_003	ALL (when applicable)	V2X communication range: V2X communication range should not be less than 400 meters.	All applicable	A8.2, A7.5	CERTH/HIT
SHOW_02_004	ALL (when applicable)	Typical GNSS positioning accuracy: The positioning accuracy provided by GNSS devices should be less than 5 meters.	All applicable	A8.2, A7.5	CERTH/HIT
SHOW_02_005	ALL (when applicable)	Enhanced GNSS positioning accuracy: The positioning accuracy provided by devices that implement enhanced GNSS systems and services (e.g. RTK) should be less than 1 meter.	All applicable	A8.2, A7.5	CERTH/HIT

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_02_006	ALL (when applicable)	The vehicle shall adapt its speed to the route's specificities: if there is a priority zone ahead (e.g. intersection, pedestrian crossing, stop traffic sign, curve in the road, narrow route), the vehicle will decelerate and move with a lower speed than average. If there is a high visibility straight road ahead with no priority zone and with only predictive situations under ODD, the vehicle may accelerate.	All	WP7	Navya, Transdev
SHOW_02_007	UC3.4, UC3.5	The AV shall manage the arrival at the station / pick-up place for person or goods in autonomous mode.	All those deploying the respective Use Cases.	WP7	Navya
SHOW_02_008	ALL (when applicable); especially UC1.10.	Seamless service provision shall be ensured on the same route when different OEMs and/PTOs are involved.	Any site confronting with the specific interoperability case.	A4.5	ICCS, CERTH/HIT
SHOW_02_009	All	SHOW data registry protocol principles and mechanisms shall be applied for data/KPIs sharing between the LFMP (Local Fleet Management Platform) or other third parties and the SMDP (SHOW	All	A4.3, A4.5, A5.1	ICCS, CERTH/HIT

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
		Mobility Data Platform).			
SHOW_02_010	UC1.5, UC3.4	TLA service shall be computed and delivered with delays acceptable (≤ 3 sec) by the target application (a target application depends on the service; it is generally defined as the ITS application that provides the specific service to the user/driver/vehicle).	All deploying UC1.5 as a minimum.	A8.3	SWARCO
SHOW_02_011	UC1.5, UC3.4	Prioritization shall be computed and granted with delays acceptable (≤ 3 sec) by the target application (a target application depends on the service; it is generally defined as the ITS application that provides the specific service to the user/driver/vehicle).	All deploying UC1.5 as a minimum.	A8.3	SWARCO

4.1.5.3 Communications Requirements

Table 4: Communications requirements.

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_03_001	All	Fleet to cloud data transfer: Assuming a local fleet management cloud platform (LFMP), both periodic exchange of vehicle/trip static data and close to real time vehicle/trip data shall be enabled according to SHOW data model via data APIs (MQTT or HTTPs).	ALL	A4.1, A8.2, A5.1, A5.3, A8.2	ICCS
SHOW_03_002	All if applicable	Standardized LFMP to fleet orders/notifications data transfer: Assuming a local fleet management cloud platform (LFMP), ad-hoc notifications from the local test site remote control/monitoring centre to the fleet members shall be supported in order to transfer Fleet missions/ Operational notifications to fleet members.	ALL sites that support an LFMP	A4.1, A8.2	ICCS

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_03_003	UC1.7	**Standardized LFMP to fleet tele-operation commands and VoIP transfer**: Assuming a local fleet management cloud platform (LFMP), a data/voice/image (upon event or continuously as required by legislation, bi-directional) connection from remote control/monitoring centre to the fleet members shall be supported in order to transfer tele-operation commands.	ALL sites that support a LFMP and tele-operation	A4.1, A4.5, A8.2	ICCS
SHOW_03_004	All UCs that include use of external traffic/charging /transit data for a specific service provision	LFMP (Local Fleet Management Platform) system integration with external data providers like PT backend, TMC, smart city backend for traffic, transit and charging data retrieval should be supported via standardized APIs when a service requires those data.	All sites deploying the respective levels of integration (with PT backend and TMC).	A4.1, A4.5, A8.2	ICCS

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
SHOW_03_005	All UCs that include services that may proliferate from historic traffic/transit data (mainly UC3.1 & UC3.2)	SHOW data portal or LFMP (Local Fleet Management Platform) communicating with external PT data open sources like NAPs (see EU directive 2017/1926) or OpenMobilityData feeds via standardized interfaces may be established for collecting of additional data to be used in AI algorithms/ML models training.	All sites deploying UC3.1 and UC3.2 as a minimum.	A4.1, A4.5, A8.2	ICCS
SHOW_03_006	ALL	If applicable, 3rd party systems residing on the test site shall establish a successful connection to SHOW Dashboard via data API interfaces (MQTT and REST), enabling the direct retrieval by the Dashboard of related KPIs and other data.	ALL applicable	A4.3	RISE
SHOW_03_007	Any UC that will involve V2X	Standardized V2X technologies: At least one of the standardized V2X technologies in Europe (ITS-G5, C-V2X direct or networked based) shall be used wherever is required by the AVs	All applicable (using V2X)	A8.2, A7.5	CEA, CERTH/HIT

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
		or infrastructure to implement the relevant UCs.			
SHOW_03_008	Any UC that will involve V2X	V2X devices released standards compliance: All devices that implement V2X connectivity shall comply to published standards.	All applicable (using V2X)	A8.2, A7.5	CERTH/HIT
SHOW_03_009	Any UC that will involve V2X	V2X devices released standards version match: All V2X devices concurrently participating at the same site shall comply to the same version of V2X related released standards.	All applicable (using V2X)	A8.2, A8.3, A7.5	CERTH/HIT
SHOW_03_010	Any UC that will involve V2X	V2X implemented services: AVs or infrastructure shall implement all the required V2X services required by the relevant UCs (e.g. traffic light prioritisation, forward collision warning, …).	All applicable (using V2X)	A8.2, A8.3, A7.5	CERTH/HIT
SHOW_03_011	ALL	GNSS site coverage: GNSS coverage form at least one of the GNSS systems	All applicable	A8.2, A7.5	CEA, CERTH/HIT

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
		(GPS, GLONASS, Galileo, Beidou) must be available throughout AV's itinerary.			
SHOW_03_012	ALL	GNSS enhancement at site: Positioning enhancement systems and services (e.g. RTK over ITS-G5 or other wireless network) should be available at pilot sites when it is required by the AV.	All applicable	A8.2, A7.5	CEA, CERTH/HIT
SHOW_03_013	ALL	Cellular network coverage: Cellular Network coverage (LTE and above) must be present throughout the itinerary of the AV.	All applicable	A8.2, A7.5	CEA, CERTH/HIT
SHOW_03_014	UC1.7	Cellular network coverage for safety critical cases: Cellular Network should guaranty the required bandwidth and latency needed to support safety critical functions like remote driving and remote monitoring.	All applicable	A8.2, A7.5	CERTH/HIT
SHOW_03_015	UC1.5 (UC3.4)	Data sent by the TMC shall follow relevant industry standards, according to the content of the message (e.g., Prioritization and	All deploying UC1.5 as a minimum.	A8.3	SWARCO

ID	Use Case(s) related	Description	Relevant Pilot Site(s)	Relevant Activity	Requirement issuer
		Traffic Light Forecast).			
SHOW_03_016	UC1.5 (UC3.4)	The network shall guarantee persistent connection between TMC and Roadside units/road sensors and vice versa.	All deploying UC1.5 as a minimum.	A8.3	SWARCO

5 Test scenarios for Technical Verification & Commissioning Phase

5.1 Template for test scenarios definition

The following template will be used to define the test scenarios that will cover all the requirements described in the previous section. In the context of this phase, each test site will be performing all the test scenarios planned, in at least **5 repetitions** each one under different environmental conditions set, or as many times as required beyond that, in order to ensure an accepted result in terms of safety and performance, before they move to the validation phase.

Table 5: Template for test scenarios.

Test scenario identifier	(S or P or C) TSXX
Test scenario description	Description of the test scenario
Reference requirement	Add all the requirements that are going to be tested. WP5 service requirements Ex: Req1, Req2, Req3, etc.
Pass/Fail criteria	Describe the pass-fail criteria. Ex: • The longitudinal acceleration should be within [-4, 4] m/s^2. (7.2.25, 7.2.26)

Expected Test Sequence

Step	Type	Description	Req.
0	Action	• Each vehicle perfectly centered on its lane. • EGO vehicle in L3 automation level.	
1	Verify	Driver Monitoring System is working.	Req2
2	Action	The driver request to change to L4.	Req1
4	Verify	HMI alert the driver of the automation level change (image, sound and vibration).	7.2.31
		EGO vehicle in L4 automation level.	7.2.32
5	Action	Driver is inattentive.	
6	Action	After 5 seconds, all target vehicles except TV1 accelerate to 90 km/h.	
7	Verify	The EGO vehicle performs an overtaking maneuver respect the TV1.	

5.2 Safety test scenarios

Table 6: Safety test scenario 01.

Test scenario identifier	STS01
Test scenario description	Lane marking and traffic signs detection
Reference requirement	SHOW_01_001, SHOW_01_002, SHOW_01_003, SHOW_01_004, SHOW_01_005, SHOW_01_006
Pass/Fail criteria	• The perception system of the AVs is able to detect correctly the lane markings and traffic signs on the road.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	Remove redundant lane markings at bus stops/bays to minimize any adverse effects on lane keep assist systems (if applicable).	SHOW_01_001
1	Action	Ensure that there are no yellow and white mixed in pavement markings on construction site (if applicable).	SHOW_01_002
2	Action	Improve longitudinal pavement markings at intersections (if applicable).	SHOW_01_003
3	Action	Improve current pavement marking asset conditions to enhance brightness and quality of the lane marking (if applicable).	SHOW_01_004
4	Verify	Ensure that the AV is able to detect properly all the lane and pavement marks.	SHOW_01_001, SHOW_01_002, SHOW_01_003, SHOW_01_004
5	Action	Maintain traffic signs in flawless conditions, namely replace worn out signs, maintain their proper position and make sure there is no obscured visibility.	SHOW_01_005
6	Action	Establish unified system of machine-readable signs that for easier recognition.	SHOW_01_006
7	Verify	Ensure that the AV is able to identify properly all the traffic signs.	SHOW_01_005, SHOW_01_006

Table 7: Safety test scenario 02.

Test scenario identifier	STS02
Test scenario description	Dynamic and static objects detection
Reference requirement	SHOW_01_007, SHOW_01_008, SHOW_01_009,
Pass/Fail criteria	• The AV is able to detect all the dynamic and static objects that are planned to be in its route. No other obstacles should be present during the test.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	Ensure that there are no obstacles around the route, including intersections with incoming traffic, that are not part of the test.	SHOW_01_007
1	Action	Ensure that there are no static and dynamic obstacles that are not anticipated to be on the route.	SHOW_01_007
2	Action	Attend to the vegetation maintenance on the side road and cleaning of the road.	SHOW_01_007
3	Action	Ensure that all the parked cars are correctly parked and have pre-defined parking lot zones	SHOW_01_008
4	Verify	The AV is able to detect the dynamic and static objects anticipated to be on the route.	SHOW_01_007, SHOW_01_008
5	Verify	The AV is able to avoid collisions with obstacles that could lead to a dangerous situation.	SHOW_01_009

Table 8: Safety test scenario 03.

Test scenario identifier	STS03
Test scenario description	Lane keeping and override
Reference requirement	SHOW_01_010, SHOW_01_011, SHOW_01_012, SHOW_01_013
Pass/Fail criteria	• The AV drives within the limits of the lane. • The driver can override the automated driving at any moment.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	The AV is driving at constant speed in autonomous mode.	SHOW_01_010

Test scenario identifier	STS03

1	Verify	The AV is not leaving its lane.	SHOW_01_010
2	Action	The driver wishes to perform an override.	SHOW_01_011
3	Verify	The driver can take back the control of the vehicle.	SHOW_01_011
4	Action	The driver activates the autonomous mode again.	
5	Action	A notification is shown to the driver to take over the control of the vehicle at the end of ODD.	SHOW_01_012
6	Action	A notification is shown to the driver to take over the control of the vehicle due to an emergency.	SHOW_01_013
7	Verify	The notification is shown with sufficient time for the driver to take the control back.	SHOW_01_012, SHOW_01_013

Table 9: Safety test scenario 04.

Test scenario identifier	STS04
Test scenario description	Loss of communication from sensors
Reference requirement	SHOW_01_014, SHOW_01_015
Pass/Fail criteria	• The loss of communication of perception sensors or localization devices shall lead to a safe stop of the vehicle.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	The AV loses communication with its perception sensors.	SHOW_01_014
1	Verify	The AV performs a safe stop.	SHOW_01_014
2	Action	The AV recovers from the loss of communication and continues its route.	
3	Action	The AV loses communication with the GNSS.	SHOW_01_015
4	Verify	The AV performs a safe stop.	SHOW_01_015

5.3 Performance test scenarios

Table 10: Performance test scenario 01.

Test scenario identifier	PTS01
Test scenario description	Cloud platform storage
Reference requirement	SHOW_02_001
Pass/Fail criteria	• The local fleet management cloud platform (LFMP), when available, and the SMDP (SHOW Mobility Data Platform) shall support storage of big data from continuous operation

Expected Test Sequence

Step	Type	Description	Req.
0	Action	Perform a stress test in the cloud platform.	SHOW_02_001
1	Verify	Ensure that the data platform supports high volume of traffic with no affect to its performance.	SHOW_02_001

Table 11: Performance test scenario 02.

Test scenario identifier	PTS02
Test scenario description	V2X communication performance
Reference requirement	SHOW_02_002, SHOW_02_003
Pass/Fail criteria	• V2X packet loss ratio should not exceed 10%. • V2X communication range should not be less than 400 meters.

Expected Test Sequence

Step	Type	Description	Req.
0	Action	Every V2X device that participates in the realization of site's UCs, should be able to transmit and receive all required V2X messages.	SHOW_02_002 SHOW_02_003
1	Action	The devices under test are placed in a range close to each other (for example within 50 m radius) and start to operate normally. They log every transmitted and received during a predefined time period (at least 100 seconds).	SHOW_02_002
2	Verify	The recorded log files are compared after the test and the maximum packet loss ratio should not exceed 10%.	SHOW_02_002
3	Action	A pair of V2X devices repeat Action 1 with an increasing range from 100m to 400m, using a 50m increase step.	SHOW_02_003

Test scenario identifier	PTS02

4	Verify	The recorded log files are compared after the test and the maximum packet loss ratio should not exceed 10% for every range distance tested. The longest distance that this condition is satisfied should be considered as the V2X communication range.	SHOW_02_003

Rules applied:

- The V2X devices should operate in a way that will lead to the generation of highest amount of V2X packets with 10 Hz rate.

Table 12: Performance test scenario 03.

Test scenario identifier	PTS03
Test scenario description	GNSS performance
Reference requirement	SHOW_02_004, SHOW_02_005
Pass/Fail criteria	• Positioning accuracy based on GNSS should be less than 5 m. • When enhanced positioning services are utilized the provided accuracy should be less than 1 m.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	Every device that incorporates a plain GNSS receiver or enhanced positioning services should be able to store/transmit the obtained positioning solution (including the timestamp with millisecond resolution).	SHOW_02_004 SHOW_02_005
1	Action	In case a positioning enhancement service is being implemented and utilized by some or all positioning devices it should operate normally during testing.	SHOW_02_005
3	Verify	The obtained positioning solutions are evaluated against the real position of the device at the time of generation. The mean solution’s accuracy should be less than 5 m.	SHOW_02_004
4	Verify	The obtained positioning solutions are evaluated against the real position of the device at the time of generation. The mean solution’s accuracy should be less than 1 m.	SHOW_02_005

Rules applied:

Test scenario identifier	PTS03
- Each positioning device should operate in an environment without obstacles occluding clear sky view. - In case of vehicle positioning devices, the vehicle should be stationary during testing.	

Table 13: Performance test scenario 04.

Test scenario identifier	PTS04
Test scenario description	Speed adaptation
Reference requirement	SHOW_02_006
Pass/Fail criteria	The condition described in the Verify cell is met
Expected Test Sequence	

Step	Type	Description	Req.
0	Verify	Verify with the FAV’s OEM, integrator, or constructor which technology is chosen for speed adaptation: - Predefined speed zone in path And / or - Adaptive Cruise Control and traffic sign reading - Other…	SHOW_02_006
1	Verify	If in the pre-defined speed zone in path, verify that the information is shared with the site authorities during the mapping of the site according to the risk analysis that is done by OEMs (items considered: ODD, traffic density, visibility, localization, etc.).	SHOW_02_006
2	Verify	Verify that the vehicle can adapt its speed depending on the environment conditions on specific sections on the path, (the ACC shall be tested apart from this requirement).	SHOW_02_006
3	Action	This will be checked during the deployment on site.	SHOW_02_006

Table 14: Performance test scenario 05.

Test scenario identifier	PTS05
Test scenario description	AV arrival / pick-up management
Reference requirement	SHOW_02_007
Pass/Fail criteria	If the condition described in the Verify cell are not met
Expected Test Sequence	

Step	Type	Description	Req.

Test scenario identifier	PTS05

0	Action	The AV is driving to priority node A. There is no obstacle on priority zones 1 and 3. An obstacle moving in the AV's opposite direction (cyclist at V = TBD m/s) enters the priority zone 2 when the AV arrives at node A.	SHOW_02_007
1	Verify	The AV shall stop.	SHOW_02_007
2	Verify	The AV shall start driving to the station when the bicycle is not on the AV's trajectory anymore.	SHOW_02_007

Table 15: Performance test scenario 06.

Test scenario identifier	PTS06
Test scenario description	Service provision
Reference requirement	SHOW_02_008
Pass/Fail criteria	Seamless service provision shall be ensured on the same route when different OEMs and/PTOs are involved.

Expected Test Sequence

Step	Type	Description	Req.
0	Action	Two or more OEMs / PTOs involved in the same route.	SHOW_02_008
1	Verify	Ensure that the service provision used by the different OEMs / PTOs is the same when the operation transits from the Area of Operator A to the Area of Operator B.	SHOW_02_008

Table 16: Performance test scenario 07.

Test scenario identifier	PTS07
Test scenario description	Data Registry protocol
Reference requirement	SHOW_02_009
Pass/Fail criteria	SHOW data registry protocol principles and mechanisms shall be applied for data/KPIs sharing between the LFMP (Local Fleet Management Platform) or other third parties and the SMDP (SHOW Mobility Data Platform).

Expected Test Sequence

Step	Type	Description	Req.

Test scenario identifier	PTS07

0	Action	Analyze log files produced during a test scenario.	SHOW_02_009
1	Verify	Ensure that the data registry protocol principles and mechanisms are applied.	SHOW_02_009
2	Verify	Ensure that the actual data transfer to the platform through the given API is successful.	SHOW_02_009

Table 17: Performance test scenario 08.

Test scenario identifier	PTS08
Test scenario description	TLA service and prioritization delays
Reference requirement	SHOW_02_010, SHOW_02_011
Pass/Fail criteria	TLA service and prioritization shall be computed and delivered with delays acceptable (≤ 3 sec) by the target application (a target application depends on the service; it is generally defined as the ITS application that provides the specific service to the user/driver/vehicle).

Expected Test Sequence

Step	Type	Description	Req.
0	Verify	Ensure that TLA service is computed and delivered with a delay lower than 3 seconds.	SHOW_02_010
1	Verify	Ensure that prioritization is computed and granted with a delay lower than 3 seconds.	SHOW_02_011

5.4 Communication test scenarios

Table 18: Communication test scenario 01.

Test scenario identifier	CTS01
Test scenario description	Fleet to cloud data transfer, notifications, tele-operation commands and VoIP transfer.
Reference requirement	SHOW_03_001, SHOW_03_002, SHOW_03_003
Pass/Fail criteria	• Assuming a local fleet management cloud platform (LFMP): o Both periodic exchange of vehicle/trip static data and close to real time vehicle/trip data shall be enabled according to SHOW data model via data APIs (MQTT or HTTPs). o Ad-hoc notifications from the local test site remote control/monitoring

Test scenario identifier	CTS01
	center to the fleet members shall be supported in order to transfer Fleet missions/ Operational notifications to fleet members. ○ A data/voice/image (upon event or continuously as required by legislation, bi-directional) connection from remote control/monitoring center to the fleet members shall be supported in order to transfer tele-operation commands.

Expected Test Sequence

The expected test sequence will be common for all the combinations in the parameter space. Some verifications might be parameterized.

Step	Type	Description	Req.
0	Action	Perform an exchange of vehicle/trip static data and close real time data / trip data.	
1	Verify	The exchange of data shall be enabled via data APIs (MQTT or HTTPs) and it achieves a specific latency of completeness.	SHOW_03_001
2	Verify	Ensure that fleet members are able to receive fleet missions / operational notifications.	SHOW_03_002
3	Verify	Ensure that fleet members are able to receive data / voice / image (tele-operation commands).	SHOW_03_003

Table 19: Communication test scenario 02.

Test scenario identifier	CTS02
Test scenario description	LFMP integration with external data providers
Reference requirement	SHOW_03_004, SHOW_03_005
Pass/Fail criteria	• LFMP (Local Fleet Management Platform) system integration with external data providers like PT backend, TMC, smart city backend for traffic, transit and charging data retrieval should be supported via standardized APIs when a service requires those data. • SHOW data portal or LFMP (Local Fleet Management Platform) communicating with external PT data open sources like NAPs (see EU directive 2017/1926) or OpenMobilityData feeds via standardized interfaces may be established for collecting

Test scenario identifier	CTS02
	of additional data to be used in AI algorithms/ML models training.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	Perform a data exchange between LFMP and an external data provider (e.g. PT backend, TMC, smart city backend…)	
1	Verify	Ensure that the data exchange is supported via standardized APIs and it achieves a specific latency of completeness.	SHOW_03_004
2	Verify	Ensure that the communication is done via standardized interfaces.	SHOW_03_005

Table 20: Communication test scenario 03.

Test scenario identifier	CTS03
Test scenario description	3r party systems communication
Reference requirement	SHOW_03_006
Pass/Fail criteria	• 3rd party systems residing on the test site shall establish a successful connection to SHOW Dashboard via data API interfaces (MQTT and REST), enabling the direct retrieval by the Dashboard of related KPIs and other data.

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	Establish a connection between the SHOW Dashboard and a 3rd party system residing on test site.	
1	Verify	Ensure that the connection is done via API interfaces (MQTT and REST) and it achieves a specific latency of completeness.	SHOW_03_006

Table 21: Communication test scenario 04.

Test scenario identifier	CTS04
Test scenario description	V2X standard compliance
Reference requirement	SHOW_03_007, SHOW_03_008, SHOW_03_009
Pass/Fail criteria	• Availability of V2X technology on site. • Conformance of on-site used V2X devices to published standards and version interoperability in all applied relative protocols and services.

Expected Test Sequence

Step	Type	Description	Req.
0	Verify	Each involved partner that operates V2X devices shall report and share in detail all the relative implemented V2X protocols and the corresponding standards versions. For example, “ETSI EN 302 637-2 V1.4.1” for Cooperative Awareness Basic service.	SHOW_03_008 SHOW_03_009
1	Action	Devices under testing (OBUs, RSUs) shall be able to trigger the generation of all used V2X messages (CAM, DENM, MAPEM, SPATEM, CPM, …) upon external request.	
2	Action	Each device generates, encodes and transmits every message that is responsible for, in a real use case scenario. The tests should be performed with a series of consequent messages of the same kind. For example, generation and transmission of CAM messages only. This step shall be a repetitive process for each used V2X message ID.	SHOW_03_008 SHOW_03_009
3	Verify	Every device that is a common receiver of the messages sent in step 2, verifies the reception and correct decoding of the sent messages.	SHOW_03_008 SHOW_03_009

Test run:

- Steps 0 and 1 are accomplished via information exchange between relevant partners.
- Steps 2 and 3 should be repeated for all exchanged V2X messages IDs.

Table 22: Communication test scenario 05.

Test scenario identifier	CTC05
Test scenario description	V2X implemented services
Reference requirement	SHOW_03_010
Pass/Fail criteria	• Implementation of V2X services required for the relevant UC realization and verification of specified operation.

Expected Test Sequence

Step	Type	Description	Req.
0	Action	Each involved partner that implements a V2X based service, shall report the availability of such a service and	SHOW_03_010

Test scenario identifier	CTC05

		describe the necessary steps for evaluation.	
1	Action	Each implemented service shall be tested for correct operation. The actual required steps for each service depend heavily upon the nature of the tested service and the required actors. For example, a traffic light prioritization service requires a smart traffic light that implements the service and vehicles that will receive or not traffic prioritization benefits.	SHOW_03_010
2	Verify	Correct operation of each implemented service should be verified in analytical steps accordingly.	SHOW_03_010

Test run:

- Steps 1 and 2 cannot be described in detail as a common test step sequence, since they are heavily dependent on the nature of the service that is being tested.

Table 23: Communication test scenario 06.

Test scenario identifier	CTC06
Test scenario description	GNSS and cellular network coverage
Reference requirement	SHOW_03_011, SHOW_03_012, SHOW_03_013, SHOW_03_014
Pass/Fail criteria	• Site adequate GNSS coverage • Site positioning enhancement service coverage • Site adequate cellular network coverage (LTE and above) • Site enhanced cellular network coverage for high bandwidth and/or low latency safety critical applications

Expected Test Sequence

Step	**Type**	**Description**	**Req.**
0	Action	Initially the itinerary of the AVs on the pilot sites shall be identified and planned	SHOW_03_011 SHOW_03_012 SHOW_03_013 SHOW_03_014
1	Action	For the evaluation of the GNSS, the enhanced positioning service and the cellular network coverage on site, any device or a combination of devices utilizing these services may be used. Preferably the on-board device that	SHOW_03_011 SHOW_03_012 SHOW_03_013 SHOW_03_014

Test scenario identifier	CTC06

		offers the positioning service of the AV and the one with the higher demands of the cellular network coverage (bandwidth and latency wise) should be used (for example the tele-operation device on the vehicle side). The AV should follow the itinerary route on a test run, while the selected test devices are operating.	
1	Action	In case a positioning enhancement service is being implemented and utilized by some or all positioning devices it should operate normally during testing.	SHOW_03_012
2	Action	The positioning device (plain GNSS and/or utilizing positioning enhancement services) constantly logs and/or transmits the positioning solution obtained throughout the whole selected route.	SHOW_03_011 SHOW_03_012
3	Verify	The positioning solutions are evaluated against the real position of the vehicle at the time of generation. Possible “blind” or poor positioning performance spots during the course of the AV should be identified.	SHOW_03_011 SHOW_03_012
4	Action	The identified device with the higher cellular network demands (throughput, latency) operates continuously throughout the selected route.	SHOW_03_013 SHOW_03_014
5	Verify	Successful operation is evaluated with respect to cellular network coverage, offered bandwidth and latency requirements.	SHOW_03_013 SHOW_03_014

Rules applied:

- These tests can only be performed on the real pilot sites and not in any other test facility.

Table 24: Communication test scenario 07.

Test scenario identifier	CTC07
Test scenario description	TMC connection and standard compliance
Reference requirement	SHOW_02_011, SHOW_03_015, SHOW_03_016

Test scenario identifier	CTC07
Pass/Fail criteria	• Communication chain is complete (messages are received/sent by all actors)

Expected Test Sequence

Step	Type	Description	Req.
0	Action	A vehicle is approaching a signalised intersection.	
1	Action	The vehicle sends a CAM message to the RSU to ask the priority to cross the intersection.	
2	Verify	RSU receives the CAM message.	SHOW_03_016
3	Action	RSU generates a SREM with the priority request, and it forwards the request to the TMC.	
4	Verify	TMC receives the SREM message.	SHOW_03_016,
5	Action	TMC checks the right of the vehicle and decides whether it has the adequate permission to ask priority.	
6	Action	TMC generates SSEM message and sends it to the RSU.	SHOW_03_015
7	Verify	RSU receives the SSEM with information about granted priority, within 3 seconds from the generation of the SREM message.	SHOW_02_011, SHOW_03_016
8	Verify	If priority is granted, vehicle passes with green right at the intersection.	

6 Cybersecurity approach

The legal stakes around data security are extremely high for connected and automated driving. Cybersecurity breaches would have major legal and business consequences for car manufacturers, other equipment makers, service providers, mobile network operators and all other stakeholders.

6.1 Key principles

The following list provides some key principles related to cybersecurity in vehicular systems.

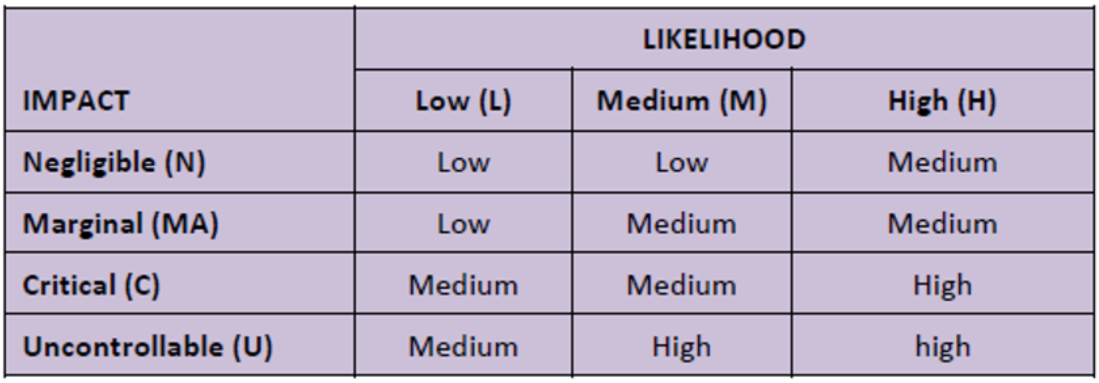
- Defence in depth for the highest risk threats. Threat mitigation should not rely on only a single cybersecurity control while leaving other vulnerabilities could let opened a door to hack and exploit the system if the primary cybersecurity control is penetrated.
- Protect sensitive data and personally identifiable information. PII stored on the vehicle should be protected, and access to the data stored should be controlled and limited. To reach the previous mentioned the next points should be followed.
    - Ask to the responsible of the data before collecting or transferring it.
    - Prevent unauthorized access from third parties by protecting data stored in access control lists.
    - Limit the default access settings.
- No permission to make changes to calibrations or software that have not been analysed and tested.
- Least privilege principle, all the components should run with the fewest possible permissions.
- Vehicle owners should not be capable, intentionally or unintentionally, to make unauthorized changes to the system that could introduce potential vulnerabilities. Some ways that can introduce vulnerabilities in the system are for example.
    - Change calibration settings or software to get different powertrain performance features.
    - Software provided by devices such as USBs, Bluetooth-paired phones, etc. These devices may attempt to install not controlled features via the vehicle's entertainment systems. All the software installations must be informed to the users and agreed.

6.2 Methodology

The first step in a cybersecurity validation [5] is the identification of potential cybersecurity issues. This phase starts with the feature definition in which the technology is studied. The study consists on the elaboration of a report about the used technologies in the system. This report considers the communication channels, the communication protocols, the hardware.

In the second step, initiation of cybersecurity plan, the report exposes the state of the art of the cybersecurity threats related to the features of the system. Threats regarding to back-end services, communication channels, updates, unintended human actions, external connectivity, and connections.

In the third step, the threat analysis risk assessment is the method to compute the risk according to the possible threats. The recommended method for computing the risk is the FERMA standard approach. This method permits to compute in a standard way the risk score according to different grades of severity. Each threat detected in previous steps must be evaluated using this method.



IMPACT	LIKELIHOOD		
	Low (L)	Medium (M)	High (H)
Negligible (N)	Low	Low	Medium
Marginal (MA)	Low	Medium	Medium
Critical (C)	Medium	Medium	High
Uncontrollable (U)	Medium	High	high

Figure 5: FERMA Standard [3].

In the fourth step, the cybersecurity concept consists in the development of the security plan for threat study, threat prevention and threat mitigation. This phase could include a definition of a pentesting plan as a security check, draw the route map to be followed according to the known threats and the score risk they have. The threats should be analysed, and the risk should be considered in order to determine the actions and countermeasures to be applied. The idea is to isolate the elements that are the source of the problem. When the source of the problem is known, the process continues classifying the problem into: hardware, protocols, interfaces, channels of communication, encryption key failure, etc. Taking into account the source of the problem, the cybersecurity concept will provide some options to solve or mitigate the problem to reduce the risk to the minimum possible.

Finally, the cybersecurity assessment consists of a process to execute the security tests and apply the security concept. Extracting conclusions from the analysis of the threats and apply preventions and mitigation against them. See possible legal responsibilities in threats in relation to data privacy, in case of leakage.

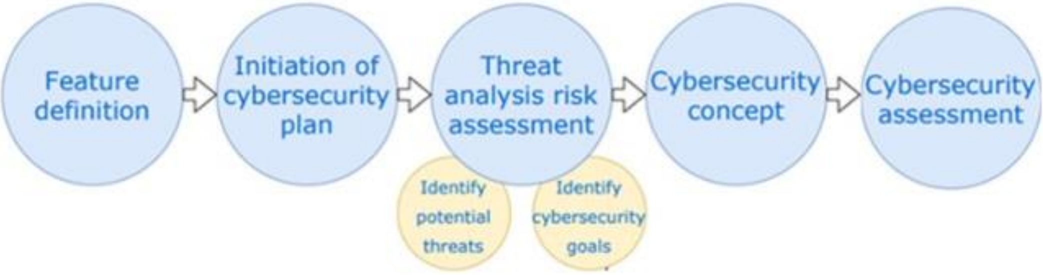

Feature definition
Initiation of cybersecurity plan
Threat analysis risk assessment
Cybersecurity concept
Cybersecurity assessment
Identify potential threats
Identify cybersecurity goals

Figure 6: Methodology adapted and based from SAEJ3061.

6.2.1 Assessment process

Each threat should be considered with the possible tests to evaluate the possibility of exploitation. The use of threats and vulnerabilities databases helps the test users to elaborate the penetration tests for the evaluation of the risks. The results of the tests will determine, joined to the risk score of the threat, the possible actions to be executed to mitigate the risk if it is necessary. If the risk score is high and the result of the pentesting shows the possibility of exploitation, the threat must be solved. In case of a low risk score and the result of the pentesting shows it is not possible of exploiting (under the conditions of the tests), the mitigation actions of the problem should be considered.

Once the cybersecurity goals are defined, it is necessary to determine whether the vulnerabilities associated with the risks encountered exist in the vehicle at the beginning of the test. This step follows a similar methodology to "pentesting" in the IT world:

- **Recognition** - The vector to be tested is investigated to learn the technology used and the possible ways to attack it.
- **Enumeration –** Data found from the vector in the vehicle are listed and will be used for further analysis and exploitations.
- **Analysis** - Potential vulnerabilities existing in the system and threats that can pose risks to the vehicle are analysed. The previously calculated risk eases the analysis.
- **Exploitation** - The potential vulnerabilities are demonstrated by attacking the vehicle and checking whether the tested vectors are protected against these attacks. If the attack is unsuccessful, it means that the vehicle meets the prerequisites and thus can be considered protected.
- **Documentation** - Test results are analysed, and the level of the vehicle's cybersecurity is documented, providing a rating.

6.3 Threats

According to UNECE, there are some known threats to vehicles [4] and the vulnerabilities can be classified in relation to the threats.

- **Threats regarding back-end servers:**
  - Back-end servers used to attack a vehicle or extract data.
  - Services from back-end server being disrupted, affecting the operation of a vehicle.
  - Data held on back-end servers being lost or compromised ("data breach").
- **Threats to vehicles regarding their communication channels:**
  - Spoofing of messages or data received by the vehicle.
  - Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data.
  - Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks.
  - Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders.
  - Denial of service attacks via communication channels to disrupt vehicle functions.
  - An unprivileged user is able to gain privileged access to vehicle systems.
  - Viruses embedded in communication media are able to infect vehicle systems.
  - Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content.
- **Threats to vehicles regarding their update procedures:**
  - Misuse or compromise of update procedures.
  - It is possible to deny legitimate updates.
  - Misconfiguration of equipment or systems by legitimate actor, e.g. owner or maintenance community.
  - Legitimate actors are able to take actions that would unwittingly facilitate a cyberattack
- **Threats to vehicles regarding their external connectivity and connections:**

  - Manipulation of the connectivity of vehicle functions enables a cyberattack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications.
  - Hosted 3rd party software, e.g. entertainment applications, used as a means to attack vehicle systems.
  - Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems.
- **Potential targets of, or motivations for, an attack:**
  - Extraction of vehicle data/code.
  - Manipulation of vehicle data/code.
  - Erasure of data/code.
  - Introduction of malware.
  - Introduction of new software or overwrite existing software.
  - Disruption of systems or operations.
  - Manipulation of vehicle parameters.
- **Potential vulnerabilities that could be exploited if not sufficiently protected or hardened:**
  - Cryptographic technologies can be compromised or are insufficiently applied.
  - Parts or supplies could be compromised to permit vehicles to be attacked.
  - Software or hardware development permits vulnerabilities.
  - Network design introduces vulnerabilities.
  - Physical loss of data can occur.
  - Unintended transfer of data can occur.
  - Physical manipulation of systems can enable an attack.

6.3.1 Threats applicable to SHOW project

Risk / Threat #1: Unused Services and Open Ports (Servers)

Likelihood: Medium Impact: Critical Exposure level: Medium

Impact: An attacker can exploit misconfigured services.

Risk / Threat #2: Unpatched Services (Servers)

Likelihood: Medium Impact: Marginal Exposure level: Medium

Impact: An attacker can exploit known or undiscovered software vulnerabilities.

Risk / Threat #3: Inattentive Administration (Servers)

Likelihood: Medium Impact: Marginal Exposure level: Medium

Impact: Often untrained and inexperienced administrators have the duty to maintain security in the system.

Risk / Threat #4: DoS/DdoS CVE exploitation MitM Drive-by Password attack (Servers)

Likelihood: High Impact: Uncontrollable Exposure level: High

Impact: An attacker makes a network unavailable by overloading the system with numerous and large requests.

Risk / Threat #5: Spyware (Servers)

Likelihood: High Impact: Uncontrollable Exposure level: High

Impact: Spyware can steal critical information and sensitive data from servers.

Risk / Threat #6: Ransomware (Servers)

Likelihood: High Impact: Uncontrollable Exposure level: High

Impact: Ransomware is malicious software that infects servers and personal computers and displays messages demanding a fee to be paid in order for the computer to work again. It has the ability to lock a computer screen or encrypt important, predetermined files with a password.

Risk / Threat #7: Unauthorized access (Servers)

Likelihood: High Impact: Critical Exposure level: High

Impact: An attacker can gain unauthorized access to host machine.

Risk / Threat #8: Unauthorized network scanning

Likelihood: Low Impact: Marginal Exposure level: Low

Impact: An attacker performs a network scan to detect which services of the host machine are online.

Risk / Threat #9: Non-invasive Attacks (Vehicle Related Threats)

Likelihood: High Impact: Uncontrollable Exposure level: High

Impact: An attacker can physically access the device.

Risk / Threat #10: Side Channel Attacks (Vehicle Related Threats)

Likelihood: Medium Impact: Critical Exposure level: Medium

Impact: An attacker can gather information from data and packets in transit.

Risk / Threat #11: Code Modification (Vehicle Related Threats)

Likelihood: Low Impact: Critical Exposure level: Medium

Impact: An attacker can modify a “Secure” tool that is connected to the system with malicious code.

Risk / Threat #12: Code Injection (Vehicle Related Threats)

Likelihood: Medium Impact: Critical Exposure level: Medium

Impact: Trojans, Viruses and Spyware.

Risk / Threat #13: Packet Sniffing (Vehicle Related Threats)

Likelihood: High Impact: Marginal Exposure level: Medium

Impact: An attacker can sniff the packets in transit between two parties.

Risk / Threat #14: Packet Fuzzing (Vehicle Related Threats)

Likelihood: Medium Impact: Marginal Exposure level: Medium

Impact: An attacker can send a fake message nearly identical to a trusted one. The system believes that the fake message is secure.

Risk / Threat #15: In vehicle spoofing (Vehicle Related Threats)

Likelihood: Low Impact: Critical Exposure level: Medium

Impact: An attacker pretends to be a legitimate user in order to displace a default component and replace it with a modified spoofing component.

Risk / Threat #16: GPS spoofing (Vehicle Related Threats)

Likelihood: Low Impact: Critical Exposure level: Medium

Impact: An attacker transmits fake GPS signals from a device he owns.

Risk / Threat #17: Jamming (Vehicle Related Threats)

Likelihood: Low Impact: Critical Exposure level: Medium

Impact: An attacker can use a device called jammer to interrupt the sensors from receiving data.

6.4 Mitigations and security mechanisms

Within the data processing systems technical standards for cybersecurity have to be considered State-of-the-art technical security measures should be implemented such as:

- Access control and authentication
- Password rules for use of secure passwords
- Logging and monitoring
- Security for databases, servers and workstations
- Use of encryption solutions for specific files and pseudonymisation techniques
- Fixed security settings for workstations
- Use of constantly updated antivirus applications
- Firewalls which are properly configured and using the latest software
- Network and communication security
- Use of cryptographic protocols
- Controlled access to wireless network only for specific users
- Monitoring of traffic inbound and outbound, controlled through Firewalls
- Mobile device security
- Implementation of rules for proper use of mobile devices and roles and responsibilities for device management
- Use of encryption software and theft protection
- Application lifecycle security process
- Early definition of specific security requirements
- Use of secure coding standards
- Implementation of testing procedures
- Rules and strategy for data deletion and disposal
- Data deletion process of outdated and irrelevant personal data should be established, additional physical destruction of media (CDs) if needed

6.4.1 Mitigation actions in SHOW project

Risk / Threat #1: Unused Services and Open Ports (Servers)

Mitigation action: The network administrator must disable all unused services and close all the unused ports.

Risk / Threat #2: Unpatched Services (Servers)

Mitigation action:

- Penetration testing must be performed in order to detect known security vulnerabilities.
- Trusted, secure and experienced in production environment software must be chosen for the system architecture.
- Regular and effective system maintenance should be required from the administrator.
  Proper debugging techniques may be developed.

Risk / Threat #3: Inattentive Administration (Servers)

Mitigation action: Security maintenance is a critical factor for the success or failure of the system and must be taken seriously and the overall procedure should follow international Security Standards.

Risk / Threat #4: DoS/DdoS CVE exploitation MitM Drive-by Password attack (Servers)

Mitigation action:

- Intrusion detection must be developed to protect the server on which the user logs in. It can detect any possible attack or policy violation.
- Network IPS should be used to traffic abnormal requests.
- Attack mode should be created.
- Application front end hardware should be used to analyse the data entering the system and identify those that are dangerous.
- Firewall must be used in case of simple attacks to deny all the incoming traffic from the attackers.

Risk / Threat #5: Spyware (Servers)

Mitigation action: An anti-spyware software must be deployed in order to detect and then prevent malicious actions.

Risk / Threat #6: Ransomware (Servers)

Mitigation action:

- System Administrator must always keep snapshots of the file system in order to use it as backup system.
- An IDS and IPS must be deployed to stop the attack before it begins.
- An antimalware may be deployed in order to recognize the ransomware software.

Risk / Threat #7: Unauthorized access (Servers)

Mitigation action:

- A firewall must be deployed which can monitor and controls incoming and outgoing network traffic based on the user's IP address.

- A VPN should be deployed to give restricted access to a user.

Risk / Threat #8: Unauthorized network scanning

Mitigation action:

- A honeypot may deploy in order to detect, deflect, or counteract attempts at unauthorized use of information systems.
- A firewall must be deployed which can monitor and controls incoming and outgoing network traffic based on the user's IP address.
- A VPN should deploy to give restrict access to a user.

Risk / Threat #9: Non-invasive Attacks (Vehicle Related Threats)

Mitigation action: Security measures must be taken to prevent physically access to the infrastructure of the system. Isolation for all critical components.

Risk / Threat #10: Side Channel Attacks (Vehicle Related Threats)

Mitigation action:

- Asynchronous processing architecture shall be applied.
- End to end encryption must be placed for the communications.

Risk / Threat #11: Code Modification (Vehicle Related Threats)

Mitigation action:

- IDS must be placed to analyse the data and network packets for each device which is connected to the system.
- Privileged Access Management strategy and restrict access to system's resources must be followed.
- Antivirus should be placed.
- Stateful Firewall to whitelist/ blacklist any suspicious connections should be used.
- End to end encryption must be placed for the communications.

Risk / Threat #12: Code Injection (Vehicle Related Threats)

Mitigation action:

- IDS must be placed to analyse the data and network packets for each device which is connected to the system.
- Privileged Access Management strategy and restrict access to system's resources must be followed.
- Antivirus must be placed in every critical device for the system.

Risk / Threat #13: Packet Sniffing (Vehicle Related Threats)

Mitigation action:

- IDS must be placed to analyse the data and network packets for each device which is connected to the system.
- Privileged Access Management strategy and restrict access to system's resources must be followed.
- Antivirus must be placed in every critical device for the system.

Risk / Threat #14: Packet Fuzzing (Vehicle Related Threats)

Mitigation action:

- Test the system with fake data. The errors must be fixed and the system must identify the message which has been send from the attacker.
- IDS must be placed to analyse all the inbound messages.

Risk / Threat #15: In vehicle spoofing (Vehicle Related Threats)

Mitigation action:

- Anti-spoofing techniques must be placed.
- IDS must be developed to detect packages with false addresses.

Risk / Threat #16: GPS spoofing (Vehicle Related Threats)

Mitigation action:

- Identity authentication mechanisms should be used.
- The system shall cross check the data with the data of another vehicle.
- IDS should be placed for anomaly detection in the signals' Amplitude.

Risk / Threat #17: Jamming (Vehicle Related Threats)

Mitigation action: To prevent Jamming attacks near infrared filters in cameras should be used.

The Test Sites are encouraged to implement the mitigation actions as listed above to prevent the specific risks mapped to them, that could affect each of the Test Sites. The validation on this layer can be done only upon event. This means that all the above measures are listed here on proactive basis for the test sites consideration, to make sure that the coming real life operations will be free of cybersecurity threats able to jeopardise the operation.

7 Technical Commissioning on Integrated service Phase

The technical validation phase of SHOW will follow the technical verification phase as this will be accommodated through the test scenarios presented in the previous Chapters and as it will be reported through the template of Appendix I.

Given the successful outcome in all the critical aspects of the technical verification scenarios steps (corresponding to "PASS" as it can be seen in the template of Appendix I), each SHOW test site is required to proceed with the technical validation phase.

In the context of this phase, each test site will be performing all its demonstration cases planned for the pre-demo phase in the exact same context as it has been planned for the pre-demo phase (1st pilot round of SHOW), in at least **5 iterations** each, or as many times as required above that, in order to ensure an accepted result in terms of **safety** and **performance**, before they move to the pre-demo phase.

In this phase, **no passengers will be put on-board**. Only the technical validation teams' personnel that will be appointed on test site level will participate. This phase **does not aim to evaluate any acceptance part** – which is a clear objective of the pre-demo and the later real-life phase.

It stands as a full and in-depth technical walkthrough of all the test site solutions in context. The **upper goal of this phase** is to undergo a deep and analytical validation and commissioning of the integrated shared CCAV solutions that will be tested in real life in the coming two phases of the project and, finally, **to ensure that all the safety and performance standards, as a minimum, are met.** In specific,

- **Safety** is assumed to be ensured when no accident or incident is anticipated for any user involved in any way in the operation, under any condition of operation.
- **Performance** is assumed to be ensured when all performance targets of the planned operation in each specific context are met, at least to the level that they do not hinder the seamlessness of the operation.
- Other than the above, there might be other **Quality of Service** requirements, specific to each site and operation that might be needed to be met and are subject to definition by the test sites.

This apparently means that the process may turn to be iterative, meaning that will lead to a series of optimisation rounds until the key objectives of safety and performance, at least, are fully met.

Still, all the other elements as anticipated in the latest update of the D9.2 experimental plans will be present. This encompasses the following:

- the **vehicle demonstrators** in the exact same format that they will operate during the real-life evaluation.
- the **coupled physical and digital (and communication) infrastructure** in place.
- **all the communication established** between the previous two – to accommodate the planned demonstration cases – as well as the **interfaces built to the data collection platform and dashboard of the project**.
- the **enabling passenger, operator and any other third-party services** that will be deployed during operation.

- the **traffic and environmental context and the very specific routes** defined for the later real-life evaluation.

This phase is mandatory for all Mega and Satellite sites of SHOW as well as for those Follower Sites that also aim at real life operations in the lifetime of the project and is a **prerequisite for proceeding to the pre-demo phase** (1st pilot phase of SHOW).

Reporting on the outcomes and the optimisation that will be inferred upon them before moving to the next phase will be included in D11.2 and will be accommodated through the Appendix II. All test sites are required to keep/store locally all the analytical results to justify the consolidated reporting of Appendix II as well as clearly describe all the optimisations inferred as of the technical validation phase before moving to the pre-demo phase.

8 Conclusions

This deliverable defines the technical assessment methodology and protocol to be followed by all the SHOW Test Sites for evaluating across a series of aspects and layers their solutions before they move with evaluation with passengers. As described in the previous chapters, the technical assessment will consist of two phases: one on technical verification & commissioning level and one integrated service technical validation & commissioning level. Both phases will need to be passed in every Test Site before moving from the first to the second one and, in turn, before moving from the second one to the pre-demo phase of the project.

The technical verification will consist of list of test scenarios to be executed on the Test sites in relation to vehicle safety, performance, and communications. A cybersecurity analysis is also provided to analyse the possible risks and mitigate them. If the Test Sites already have executed similar tests in the past and they have an official certificate to prove it, it will be not necessary to execute them.

The technical validation phase will consist on Use Case specific tests and will be specific for the project and for the Test Site. It will be executed after passing the verification phase and mandatory for all Test Sites before going to the pre-demo phase. Templates to report the results for both phases have been provided in the Appendices of this deliverable. Results of both phases will be reported in D11.2: Demos safety, reliability and robustness validation and commissioning.

WP11 members participate to the Automated and Connected Vehicle subgroup of the Motor vehicle Working Group (MVWG-ACV), which is the official working group set-up by the European Commission to steer the development of legislation concerning the validation of automated and autonomous vehicles. The work of the MVWG-ACV is currently focused on developing procedures for shuttles and robo-taxi applications. In this light the validation procedure presented in D11.1 can represent an important input to the future legislation that will be proposed by the European Commission.

References

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

[2] SHOW (2020). D9.2 Pilot experimental plans & impact assessment framework for pre-demo evaluation. Deliverable of the Horizon-2020 SHOW project, Grant Agreement No. 875530.

[3] Federation of European Risk Management Associations. FERMA Standard https://www.ferma.eu/

[4] Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA (2018, September 20). https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

[5] AUTOPILOT (2017). D4.10 Legal Perspectives on use of IoT. Deliverable of the Horizon-2020 AUTOPILOT project, Grant Agreement No. 731993.

Appendix I - Technical verification & commissioning reporting template

<Note: If you have previously or in other occasions (e.g. in the context of commissioning, audit or other processes) performed some or all of the expected test scenarios), please provide all the details requested below as well as an overview of the results and an evidence that the tests indeed have been realized. >

1. **SHOW Test Site Concerned:**
2. **Test conducting entity(ies) per test scenario ID below:**
3. **Time of conduct:** <From when to when>
4. **(physical) Place of technical verification:**
5. **Set-up (vehicles, physical infra, digital infra, other) for technical verification (photos/evidence to be included):**
6. **Reporting on deviations/configurations done for the testing of the following scenarios:**
7. **Number of iterations per scenario and the different configurations/environmental conditions set tested per each:**
8. **Test Scenario (ID) outcome:** <Please repeat the following table for each testing scenario tested, adding subsections respectively; for each table, repeat the steps as included in the protocol and applied>

   a. **Test Scenario (ID) aggregated outcome**[3]**:**

Step	Type	Description	PASS/ NOT PASS/ PARTLY PASS

   b. **Comments/Justification on outcome:** <Please comment on the outcomes, provide details for the results (numerical results, etc.) and justifications>

9. **Final Aggregated Outcome**

<Please explain the aggregated outcome upon all scenarios and if the technical verification is considered accepted to you.>

10. **Comments on the overall outcome and actions taken, if applicable, prior to technical validation**

[3] Derived as of all iterations.

Appendix II - Technical validation & commissioning on integrated service level

1. **SHOW Test Site Concerned:**
2. **Test conducting entity(ies) participating:**
3. **Time of conduct:** <From when to when>
4. **Testing Environment:**

- <Please provide a brief description of the setting. Please embed pictures/ illustrations/maps and refer to the specific km of the route(s) and the geographical position of the routes.>

5. **Physical and Digital (and Communication) Infrastructure:**

Please describe as analytically as possible the physical and digital infrastructure deployed. If possible, mark their key elements on the images depicting the routes (requested above).

6. **Testing context:**

<Please provide the following tables and give as much additional information required as possible. Please give some screenshots from validation.>

7. **Demonstration cases:**

Please describe in short, the demonstration cases along with enabling services, if any, that have been tested. Make sure that there is clear mapping to D1.2 use cases.

8. **Vehicle demonstrators:**

<Please provide short description of the vehicle demonstrators deployed. Include among other photos as well as the vehicle brand model, the vehicle type, the SAE level, the technical characteristics, the HMI hand-over strategies applied, APIs and communication capabilities, and other physical characteristics, like size, capacity allowing, etc.>.

9. **Experimental tools:** Please refer in short in all the experimental tools (e.g. logging systems) that you have used for the scope of the technical validation.

10. Technical validation objectives:

<Please interpret what it means to each of your planned demonstration cases operation safety, performance and quality of service, adding more research layers, being also part of the validation, if applicable. All should be measurable; meaning including the success threshold. **Any type of communication and interfaces foreseen to local and central to the project entities have to be reflected below**>

Test/Use Case [as coded above]	**Technical Validation objectives**			
	Safety	**Performance**	**Quality of Service**	**Other (if applicable)**

11. Testing framework:

<Please complete the following table to give the overview of the testing framework>

Test/Use Case [as coded above]	Vehicle demonstrators deployed [as coded above]	Physical & Digital Infra deployed [in summary]	Average Km run (from all iterations)	Operation features				
				Maximum speed reached during the trials (km/h)	**Average speed during the trials (km/h)**	**Weather, sight & road conditions**	**Any special events triggered (e.g. road works, pedestrians crossing, etc.)**	**Traffic context and conditions**

12. Validation Outcomes

a. Aggregated technical validation outcome[4]:

Test/Use Case [as coded above]	Number of iterations required for fully successful outcome:	**Safety** results (in direct reference to the targets defined above)	**Performance** results (in direct reference to the targets defined above)	**Quality of Service** results (in direct reference to the targets defined above)	**Other (if applicable)** results (in direct reference to the targets defined above)	PASS/ NOT PASS/ PARTLY PASS

b. **Comments/Justification on outcome:** <Please comment on the outcomes, provide details for the results (numerical results, etc.) and justifications and add details on the iterative optimization that had to be done, if any, during this phase>

[4] Derived as of all iterations.

13. **Final Checkpoint -** How much ready we are to move to the pre-demo phase trials and what is needed to get completely ready and confident for them? Please rank your site from a scale from 1 to 5 (√ in the corresponding box) and explain in short.

Readiness level towards final evaluation round of SHOW				
1 - Not ready at all – A lot to do more	**2 – Not ready – Significant corrections/development/integration and optimisation is still required**	**3 – Half ready; good basis but a series of additional development/integration and optimisation is still required**	**4 – Quite ready to go – several optimisations are still required**	**5 – Almost ready to go – only minor optimisation is required**
Ranking justification – what needs to be done in short:				
Estimation of time required for getting 100% ready for the pre-demo phase trials (in weeks):	………………weeks			