PRISSMA Project
Plateforme de Recherche et d’Investissement pour la Sûreté
et la Sécurité de la Mobilité Autonome
04/2021 - 04/2024

[L6.5] WP6 INTEGRATION OF AI SPECIFICATIONS INTO DESIGN STANDARDS

INTÉGRATION DES SPÉCIFICITÉS LIÉES A L’IA DANS LES STANDARDS DE CONCEPTION

Main authors: H. HUSSAIN and D. CARITEY (Airbus Protect), L. LEROUX (UTAC) and R. REGNIER (LNE)

Keywords: Autonomous urban shuttle, Requirements, AI specifications, AI design standards

Abstract. This document aims to recommend requirements to develop AI components involved in the Autonomous Driving System of fully autonomous urban shuttles and delivery robots. It develops a concept of Operation in its first part and then develops requirements classified in three categories: AI Component specific, Vehicle specific and Smart Mobility Systems specific. It also initiates requirements on tests whether they are done by simulation, in controlled environment or real environment.

Résumé. Ce document a pour but de recommander un jeu d’exigences pour développer les briques IA impliqués dans le system autonome de conduite des navettes urbaines et robot de livraison autonomes. Dans sa première partie, un concept d’opération est suggéré et suivent les exigences classifiées en trois catégories : spécifiques aux briques IA, spécifique aux véhicules et enfin spécifique aux systèmes de mobilité intelligents. Ce document initie également les exigences concernant les tests qu’ils soient menés par simulations, dans un environnement contrôlé ou en conditions réelles.

Table of content

1 INTRODUCTION

Artificial Intelligence (AI) is more and more integrated in smart mobility systems and one key issue is to perform its Integration, Verification, Validation and Qualification (IVVQ) activities. Obviously, these new systems have to comply with acceptable safety and security performance thresholds of existing standards. For this purpose, audits should be organized and this document aims to offer a framework of requirements, which development, delivery, operation and maintenance stakeholders of such systems shall follow.

The system addressed by this document is an integrated Smart Mobility System (SMS) including infrastructure, communication via 5G, etc. (an example of such systems is the Automated Road Transport System – ARTS – defined in the French regulation), but also the automated/autonomous Mobility Vectors (MVs) integrated in such mobility systems as standalone systems.

In this document, MV refers to an automated/autonomous MV possibly integrated in an ARTS.

Several stakeholders are working on a System of System where automated/autonomous vehicles do interact with smart infrastructures, other smart vehicles and with their customers. They paint a picture in which a transportation service provider could use different manufacturer's automated/autonomous vehicles for the same purpose. These automated/autonomous vehicles could be used as personal vehicles, taxis, delivery bots or autonomous urban shuttles. However, this document does not address intramodality and interoperability but the requirements for homologation for an automated/autonomous shuttle or bot interacting with conventional vehicles.

This document is addressed to many actors: manufacturers, integrators, suppliers, main contracting authorities (Project Manager "PM"/Project Owner "PO"), main contractors, operators, and maintainers, regulating authorities, owners, national, regional and political stakeholders.

Such contributor of a smart mobility system should be responsible of the development, deployment, or operation of:

- A whole or part of an integrated mobility system (System of System level e.g., ARTS)
- One or several MVs (System Level)
- AI bricks aimed to be or having been integrated in ARTS or in MVs

The focus of this document is ensuring safety-oriented requirements. Thus reliability, availability or continuity of service are not addressed.

While the System of System, in which the MV intervenes should be safe to operate, the MV is a standalone system that has to ensure its safety.

Other requirements could be added, concerning different specific AI technics: non supervised technics, reinforced deep learning, expert system including rules data base, Bayesian technics, genetic approaches…), "grilling" or probabilistic AI, etc. For the purpose of autonomous urban shuttle, no real time learning will be possible. Real Time collected big data recordings, circulation and operational behavior will be analyzed on a regular basis to identify operational scenarios which should generate a correction process.

Requirements related to justification documentation are in the scope of T6.3 deliverable 6.6 of the PRISSMA project and will be detailed in its allocated document.

2 FRAMEWORK FOR DEFINITION AND TECHNICAL ISSUES

This paragraph presents a framework of assumptions the supplier or the operator should comply with as well as the context of AI integration in system engineering development process.

AI is participating at the very core of decision making, thanks to pieces of information acquired through the eyes, ears and muscles of the ARTS. Its integration, validation and verification then become part of the classical process of system engineering since it’s fully a part of the system.

But, as mentioned by F. F. Philip Koopman author of the book “*How Many Operational Design Domains, Objects, and Events?”*, the use of machine learning techniques challenges classical system engineering, due to the use of training data rather than a traditional design process. Validation therefore requires at least ensuring that training data and testing cover all relevant operational conditions [1].

Moreover, since standards for acceptable decision have not been explored in their entirety, it becomes crucial to initiate the effort of considering the AI design, development and operation as a specific issue in system engineering.

2.1 Definitions and requirements

This paragraph is introducing definitions which will be the framework for a better understanding of the requirements following.

2.1.1. Operational Design Domain (ODD)

As described in the deliverable 8.11 of the PRISSMA [2] project and the ISO 34503 [3]: an ODD defines the operating conditions under which an MV is designed to operate safely.

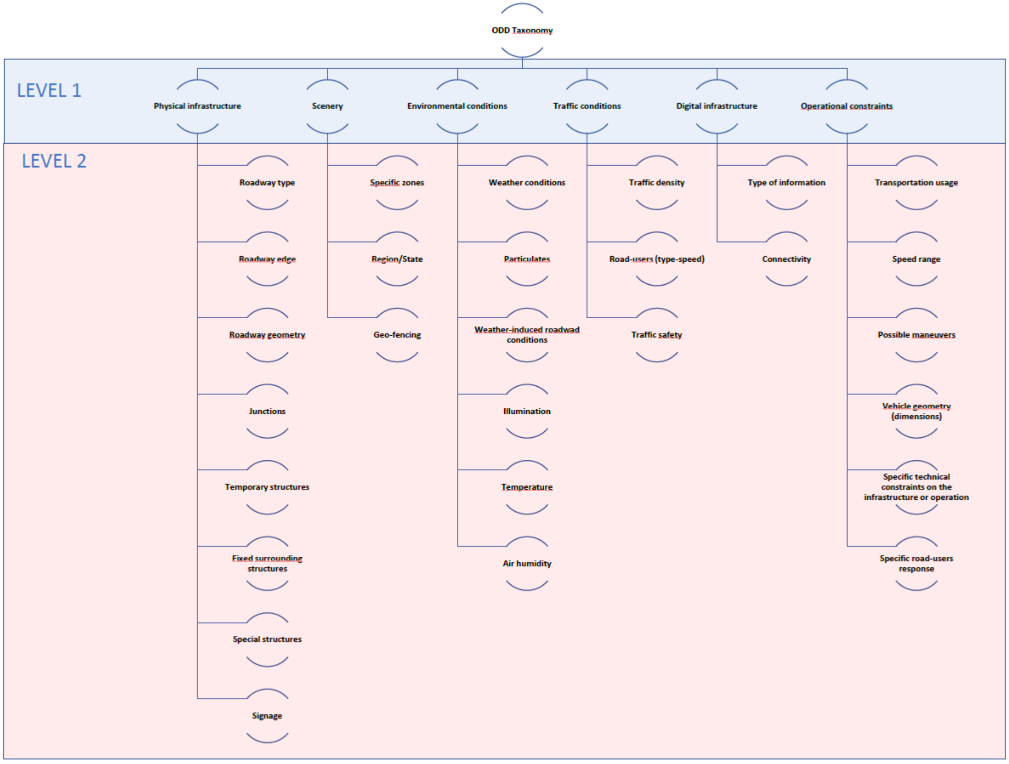


Figure 1: ODD taxonomy from the deliverable 8.11 from the PRISSMA project [2]

Meaning an ODD is a set of conditions in which the vehicle shall use its autonomous functions to a determined level driven by AI systems [4]. These conditions could be either weather conditions, localization, type of route, landscape, other vehicles behavior or so on. As a remark, to properly picture ODD for an ARTS, one needs to define scope and a strategy to cover the delta between the classical vehicles and the MV.

An ODD should be provided for system under analysis, as well as:

- Taxonomy applied
- Current Standard(s) or Guidelines referenced
- Methodological framework used to document it

For the purpose of this document, the MV has to operate in autonomous manner. Meaning, from the start of the vehicle until its return to the stocking facility, it should able to smoothly drive itself.
A special care for the choice of the operation routes should be taken in account as it will also define the ODD. Autonomous Line Keeping System (ALKS) or the EUropean Autonomous Driving System (EU ADS) are regulations that can be taken as examples.

In the Figure 2, an automated/autonomous shuttle has been represented in a 3-lanes setting in one way. For example, it is up to the manufacturer to define the level of safety it can guarantee on every lane. Same kind of remark applies to Minimum Risk Maneuver (MRM) procedures.

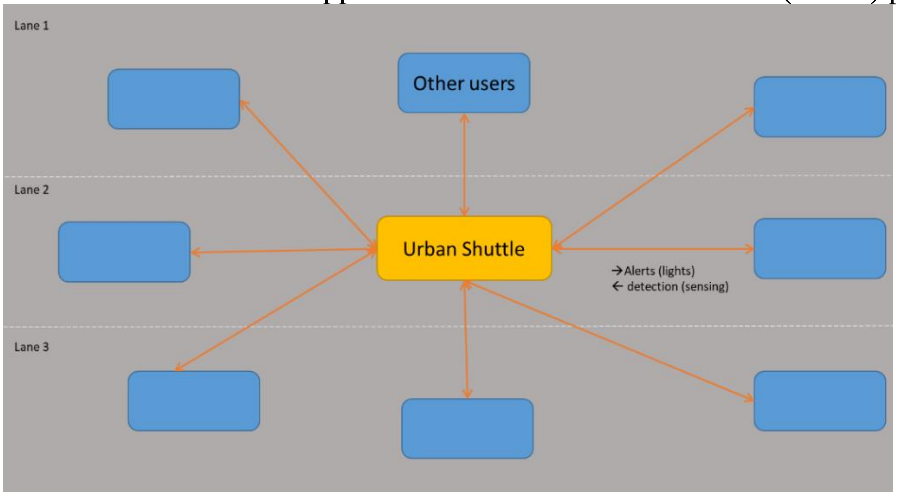


Figure 2: Urban shuttle in a 3-lane setting.

An exaggerated focus on edge cases shouldn’t divert from the most probable cases and their proper testing and validation.

- Develop input from How Many Operational Design Domains, objects, and events?
- Link with existing standards or official guidelines...

ODD should be devised in a way, it is possible to choose the applicable ODD, and not go through a lengthy compulsory list that might not be relevant neither for the manufacturer nor for the validating authorities.

2.1.2. Dynamic Driving Task (DDT)

To safely drive in the ODD the automated driving system (ADS) of the MV shall perform the Dynamic Driving Task (DDT).

As defined in the EU ADS 2022/1426 [5]. It is a task that includes all real time operational functions and tactical functions required to operate a vehicle, excluding strategic functions such as trip scheduling and selection of destinations and waypoints and including without limitation:

a. Lateral vehicle motion control via steering (operational);
b. Longitudinal vehicle motion control via acceleration and deceleration (operational);
c. Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical);
d. Object and event response execution (operational and tactical);
e. Maneuver planning (tactical);
f. Enhancing conspicuity via lighting, sounding the horn, signaling, gesturing, etc. (tactical).

To illustrate the DDT, the SAE J 3016 [6] propose the following workflow.

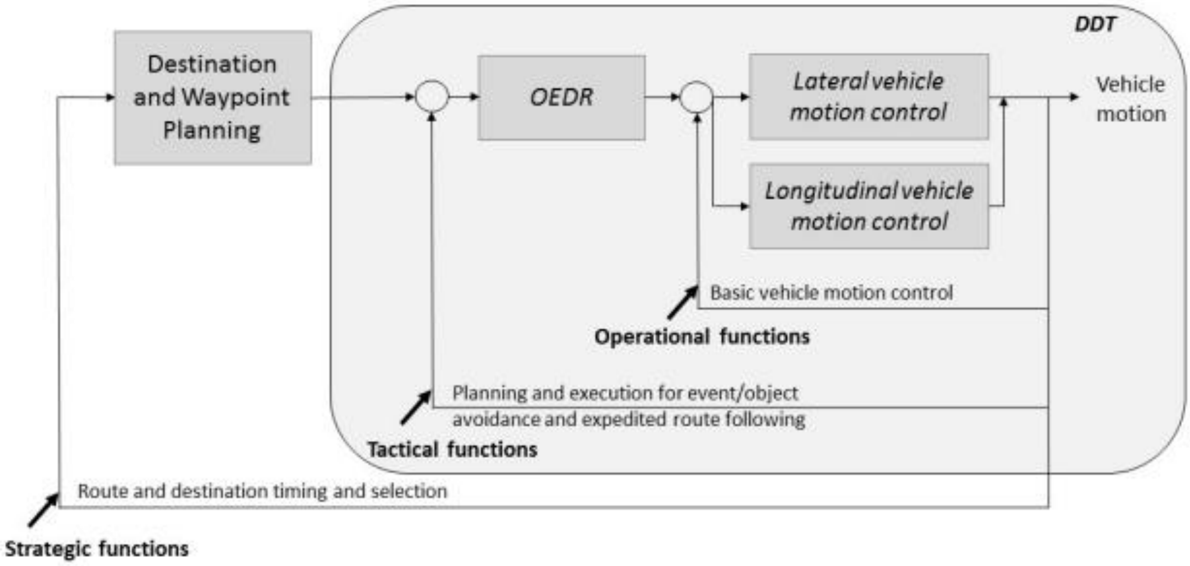

DDT
Destination and Waypoint Planning
OEDR
Lateral vehicle motion control
Longitudinal vehicle motion control
Vehicle motion
Basic vehicle motion control
Operational functions
Planning and execution for event/object avoidance and expedited route following
Tactical functions
Route and destination timing and selection
Strategic functions

Figure 3: Schematic view of a driving task showing DDT portion (SAE J 3016 [6])

For the scope of this document, no manual control has been considered except for well-defined emergency use-cases. Even more, since the document focuses on AI details it will be documented on the decision framework related with MRM/Emergency Maneuver (EM) and Objects and Events Detection and Response (OEDR). They are detailed in the following paragraphs.

2.1.2.1.Minimal Risk Maneuver (MRM)/Emergency Maneuver (EM)

This task is a part of maneuver planning of the DDT. In case of emergency, this maneuver consists to minimize risks in the traffic by stopping the vehicle in a safe state. It will depend on the situation but basically, the ADS of the MV integrated in the ARTS will stop the vehicle, switch on the hazard lights and wait for the situation to clear.

To comply with the DDT, the MRM of the automated/autonomous system shall follow the following requirements which detail the basic performances needed and behaviors to follow.

REQ#001) EM and MRM shall be available at all time throughout the ARTS operation.

REQ#002) The list of MRMs and EMs shall be defined based on its ODD

REQ#003) Consistency of these lists with ODD shall be demonstrated

REQ#004) AI Components that are not necessary for normal DDT shall not endanger the safe operation of the vehicle. In case a necessary AI Component is failed, the vehicle shall be able to perform EM or MRM independently of that failure.

REQ#005) If the vehicle encounters situations in which the dynamic driving task cannot be performed safely, it must be able to recognize this circumstance independently and initiate a minimal risk maneuver through an emergency driving function.

REQ#006) During the MRM, the MV shall be slowed down, with an aim of achieving a deceleration demand not greater than 4,0 m/s², to a full standstill in the safest possible place taking into account surrounding traffic and road infrastructure. Higher deceleration demand values are permitted in the event of a severe ADS or MV failure.

REQ#007) The ADS shall signal its intention to place the fully automated vehicle in an MRM to occupants of the fully automated vehicle as well as to other road users in accordance with traffic rules (e.g., by activating the hazard warning lights)

REQ#008) In case the ADS can no longer operate after the MRM, it shall report its status to the remote operators and trigger warnings for other users.

REQ#009) In case the ADS can still operate, after an MRM, while the MV is at standstill, a remote operator may request the ADS to perform safely a low-speed maneuver limited to 6 km/h with the remaining performance to evacuate the fully automated vehicle to a nearby preferable location (EU ADS 2022/1426, Definition §24 [5]).

REQ#010) A minimum risk maneuver shall only be terminated once the ADS is deactivated or the MV has been brought to a standstill.

REQ#011) The ADS shall only restart its mission after confirmation by self-checks of the MV or/and by the remote intervention of the remote operator that the cause of the MRM is no longer present.

REQ#012) The ADS shall be deactivated at the end of any minimum risk maneuver. The hazard warning lights shall remain activated unless deactivated manually and the vehicle shall not move away after standstill without a remote operator action.

REQ#013) At the end of the MRM:

- for a short period of time (typically 15 s), the MV is maintained standing still (e.g., despite a slope) without remote operator's action.
- after this period if there are still hazards or if remote operator decides to immobilize the MV:
  - Vehicle is definitively immobilized
  - MV is deactivated

REQ#014) The manufacturer shall declare the types of severe vehicle failures and severe AI components failures that will lead the ADS to initiate an MRM immediately

REQ#015) The ADS shall automatically detect an imminent collision, provide the users and remote operator with an appropriate warning and carry out EM.

REQ#016) Any longitudinal deceleration demand of more than 5.0 m/s² of the MV shall be considered to be an EM.

REQ#017) An EM shall not be terminated, unless the imminent collision risk disappeared.

REQ#018) After an EM is terminated, the system shall continue to operate.

REQ#019) If the EM results in the MV being at standstill, the signal to activate the hazard warning lights shall be generated. If the MV automatically drives off again, the signal to deactivate the hazard warning lights shall be generated automatically.

2.1.2.2.Objects and Events Detection and Response (OEDR)

This task is in close relationship with the MRM and is also part of the DDT.

OEDR is what separates the autonomy level 2 and 3 as per definition of Society of Automotive Engineers (SAE J 3016). For level 3 and above, the car does the detecting, recognizing, and classifying objects and events and preparing to respond as needed during the DDT [7].
In this document, the focus is on safety-oriented use cases for OEDR patterns.

Requirements of this paragraph address OEDR patterns focusing on safety critical scenarios exceeding for example perimeters of performance of AI Components and therefore producing a dysfunction/malfunction or producing an accident.

The following sub-sections explore and give an approach of regular operations and of the safety critical scenarios.

2.1.2.2.1. Regular operations

The EU Commission implementing regulation (EU) 2022/1426 (referred to as "EU ADS" in this document) [5] gives us a base on how to define the OEDR and what it should at least contain.

REQ#020) The OEDR shall follow at least the behavior competences for given events defined in the following table:

Events	Responses
Lead vehicle decelerating	Follow vehicle, decelerate, stop
Lead vehicle stopped	Decelerate, stop
Lead vehicle accelerating	Accelerate, follow vehicle
Lead vehicle turning	Decelerate, stop
Another vehicle changing lanes	Yield, decelerate, follow vehicle
Another vehicle cutting-in	Yield, decelerate, stop, follow vehicle
Vehicle entering roadway	Follow vehicle, decelerate, stop
Opposing vehicle encroaching	Decelerate, stop, shift within lane, shift outside lane
Adjacent vehicle encroaching	Yield, decelerate, stop
Lead vehicle cutting out	Accelerate, decelerate, stop
Pedestrian crossing road – inside crosswalk	Yield, decelerate, stop
Pedestrian crossing road – outside crosswalk	Yield, decelerate, stop
Cyclists riding in lane	Yield, follow
Cyclists riding in dedicated lane	Shift within lane
Cyclists crossing road – inside crosswalk	Yield, decelerate, stop
Cyclists crossing road – outside crosswalk	Yield, decelerate, stop

Table 1: Behavior competences for given events (EU ADS 2022/1426, table 2 [5])

This non-exhaustive list is just giving basic events and responses. More events/responses could be added.

2.1.2.2.2. Safety critical scenarios

For the following reasons, scenarios are much more important for AI being part of transportation systems than for classical systems not including AI.

Concerning an ARTS without AI, determining and tackling safety critical scenarios should be based on a conventional method:

- Hazard Analysis: Identifying potential hazards associated with the system’s usage.
- Safety Requirements: Establishing specific requirements to mitigate these hazards at system, software, and hardware levels.
- Risk Mitigation: Developing and implementing measures to reduce the identified risks.
- Verification: Demonstrating that the risk mitigation measures effectively reduce the risk to an acceptable level.
- Iteration: Repeating the process until the safety level is deemed acceptable.

On the contrary, states-of-the-art in AI shows that such approach won’t work for the AI that compose the ARTS:

- specifiability: behaviors easy to train for with datasets are very difficult to specify using requirements (example is pedestrian detection. What is a pedestrian? Does it mean that people in a wheelchair are not included in this category?)
- hazard assessment impossible without specification: How to define risk mitigation?
- requirements when functional requirements are not defined?

- risk mitigation verification is not possible: we cannot present irrefutable arguments demonstrating that these risk mitigation requirements are met (neither proof nor postulates that would demonstrate this coverage exist, due to issues of causality and non-linearity).
- achieved quality level is not quantifiable: it remains unclear when to stop this retraining process. Iterative improvement of this quality level is not possible
- isolation of defect: is almost impossible inside a neural network at the state of the art.
- quality assurance composition: demonstrating the system's quality assurance through the quality assurance of its AI components, similar to estimating system MTBF (Mean Time Between Failures) through the MTBF of internal components, is currently not possible at the state-of-the-art.

Based on the methodologic document from the DGITM: DGITM/DMR/TUD, three abstraction levels can be defined for safety critical scenarios:

- Functional scenario: that design a class, family of functional scenarios regrouped under a common name
- Logical scenario: that shows the logical sequence
- Concrete scenario: that is a sequence defined completely, with specified associated values and all its specifications are defined.

REQ#021) To guaranty the safety of the system the safety critical scenarios shall be concrete scenarios

RECC#01) Critical scenarios should be derived from edge-case assumptions.

RECC#02) These assumptions could be either based on data collected and analyzed, or knowledge-based approach, or directly issued from operational feedback.

2.2 General technical assumptions

The purpose of this document is to focus on the AI used in ARTS for people transport or autonomous droids for autonomous delivery of goods. In each case, their environment of integration should be identified precisely.

Moreover, a corner stone of system engineering process application is work breakdown structure of the asset under analysis. Decomposition architecture should be provided, highlighting system and subsystem splitting logics, as well as hardware and software line replaceable units and modules breakdown structures.

For the purpose of this document and to illustrate requirements, this following basic functional architecture and its links has been imagined. This is just provided as an example and other architectures could be designed justifying equivalent level of safety.

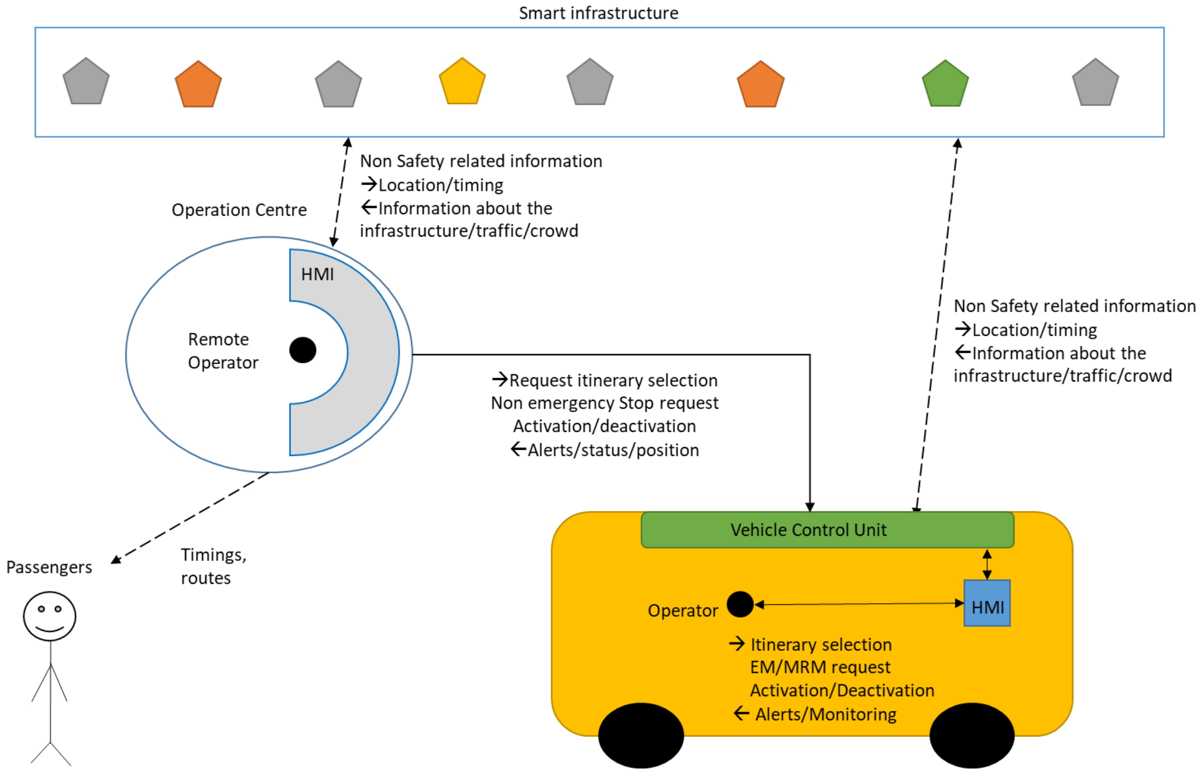


Figure 4: The System of System illustration for automated/autonomous shuttle and data exchange mapping

Note: Solid arrows represent safety related dataflow. Dashed arrows represent non-safety related dataflow exchange.

Though manufacturers could take different options on supervision and the distribution of control and information about their automated/autonomous shuttle, smart infrastructures could have beacons of any kind. In the case of an urban shuttle, it could stop where it picks up and drops passengers. Through these, it could give pieces of information ahead about the remaining time to reach the stop and also receive information about passengers on the bus stop to anticipate whether to stop or continue its journey.

For the purpose of this document some assumptions have been taken:

- There is a remote operator in the Operation Center who can push a request for a Non-Emergency Stop (NES) with regard to the traffic data he has access to. When this NES request is pushed to the vehicle, the MV analyzes the demand and initiates an MRM. When the automated/autonomous shuttle detects the need to perform an MRM or EM due to safety reasons, it initiates autonomously.
- The manufacturers may give different degrees of scope for action to the users of the vehicle. For this proposal, the user has room for action and can only modify routes or initiate the EM or MRM.
- As shown in the Figure 5, the MV may have more than one AI enhanced function that participate in the ADS. These AI Components may use common resources like sensing and detection devices.
- The vehicle will also carry recorders that allow collecting more data in case of an accident.

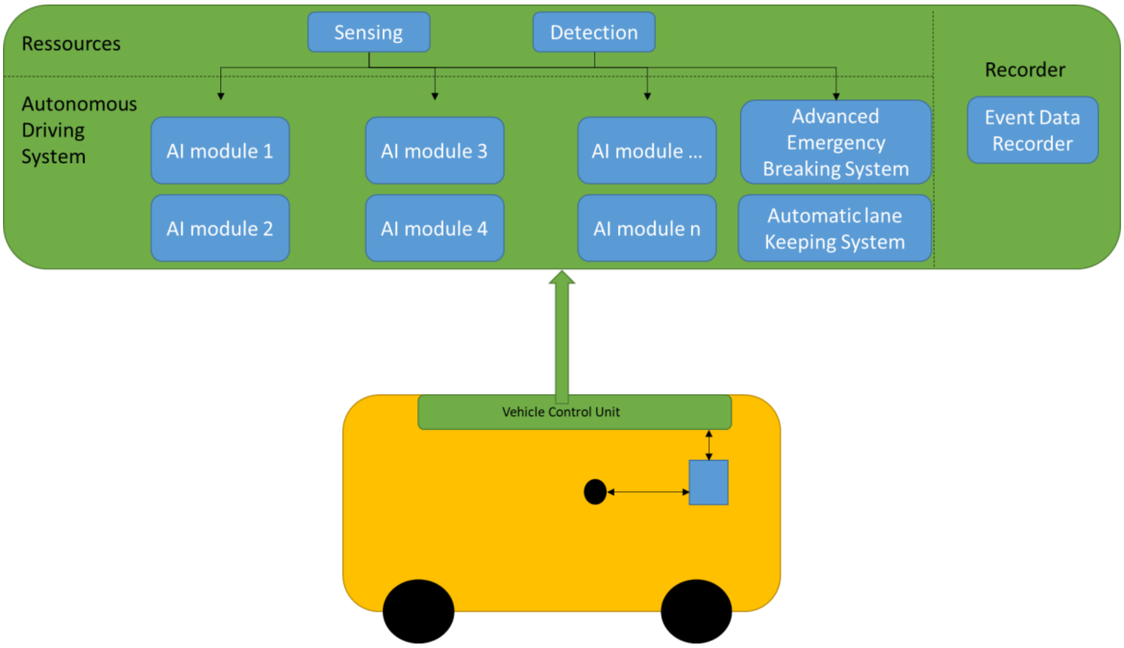


Figure 5: Breakdown of the AI components of the MV

The ODD of the ARTS may not be limited to a single lane and in need, it may be able to change lanes and perform overtaking/avoidance maneuvers.

2.3 General behavior assumptions

On the basis of the assumptions and definitions given above, we can define a basic behavior, as shown in Figure 6, which illustrates a basic behavior that an ARTS should have and which meets the objective of this document. Further actions can be implemented.

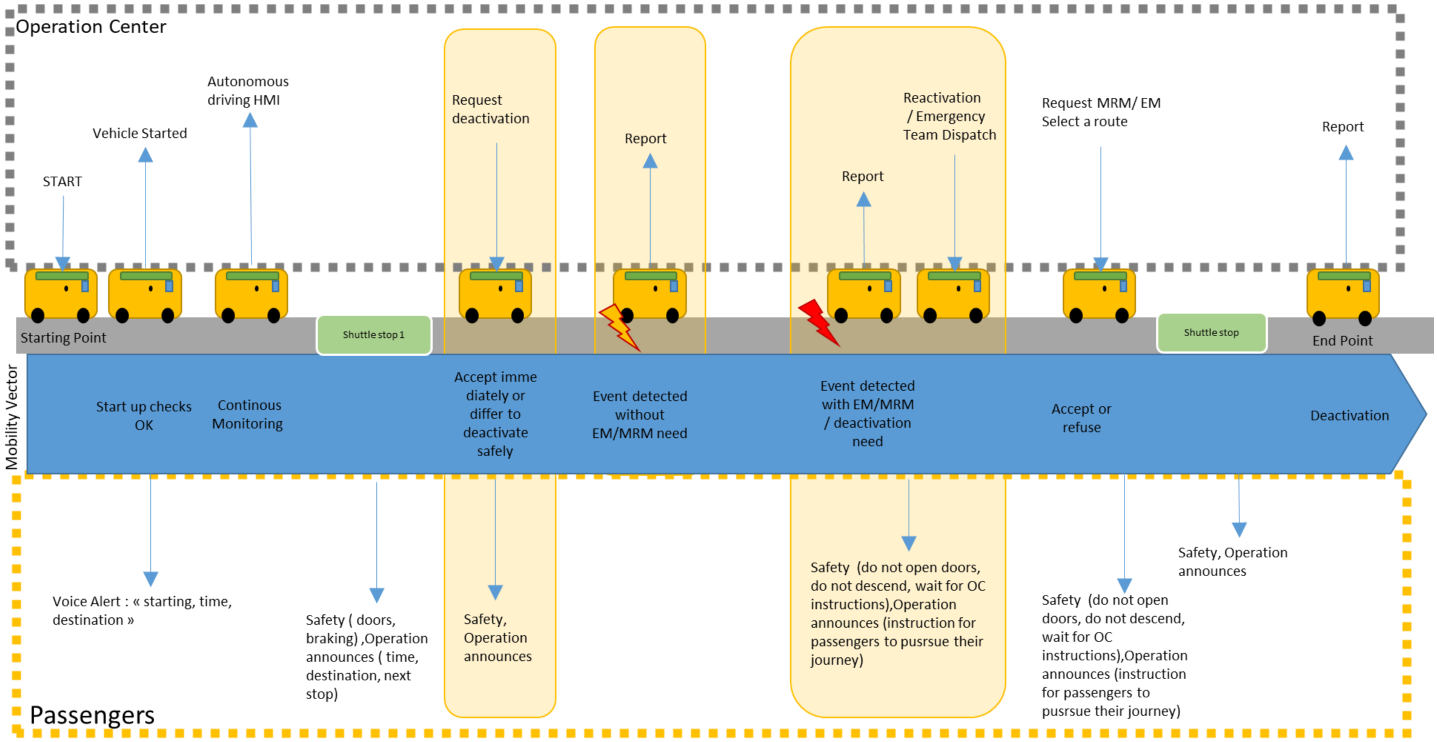

Operation Center
START
Vehicle Started
Autonomous driving HMI
Request deactivation
Report
Report
Reactivation / Emergency Team Dispatch
Request MRM/ EM Select a route
Report
Starting Point
Shuttle stop 1
Shuttle stop
End Point
Mobility Vector
Start up checks OK
Continous Monitoring
Accept imme diately or differ to deactivate safely
Event detected without EM/MRM need
Event detected with EM/MRM / deactivation need
Accept or refuse
Deactivation
Voice Alert : « starting, time, destination »
Safety (doors, braking) ,Operation announces (time, destination, next stop)
Safety, Operation announces
Safety (do not open doors, do not descend, wait for OC instructions),Operation announces (instruction for passengers to pusrsue their journey)
Safety (do not open doors, do not descend, wait for OC instructions),Operation announces (instruction for passengers to pusrsue their journey)
Safety, Operation announces
Passengers

Figure 6: Timeline of an automated/autonomous shuttle operation and its communications with Operation Center and Passengers

2.4 An interesting reference topic: Concept of Operations

The CONcept of OperationS (CONOPS) is a high-level requirement document that provide mechanism for the users to describe the global operation of a system. CONOPS has proven to be useful in aeronautics where drones bring a new set of operations. For some operation, national (Directorate General of Armaments “DGA”) and European authorities (Directorate General of Civil Aviation “DGCA”) provide guidelines to build a CONOPS. In this case, they are required for:

- ARTS or mobile vectors under analysis
- Global integrated Mobility Systems, especially concerning transversal services involving fixe infrastructures.

For this document, in order to provide clear requirements, a CONOPS has been imagined as an example. Other CONOPS could be accepted if they are justifying the same level of safety.

Perimeters have been identified:

- Nominal situation
- Degraded situation requiring an MRM
- Degraded situation requiring an EM

For the sake of simplicity, a single lane in both directions has been represented. But ARTS could operate on multi-lane roads, performing takeovers and changing lanes to avoid accidents or obstacles.

For the nominal perimeters a series steps have been identified (Figure 7):

1. Activation from OC/exit form depot/start the route
2. Stop at the shuttle stop
3. Follow its route/report its position and health status to OC
4. Stop at the shuttle stop
5. Go back to depot after finishing its route

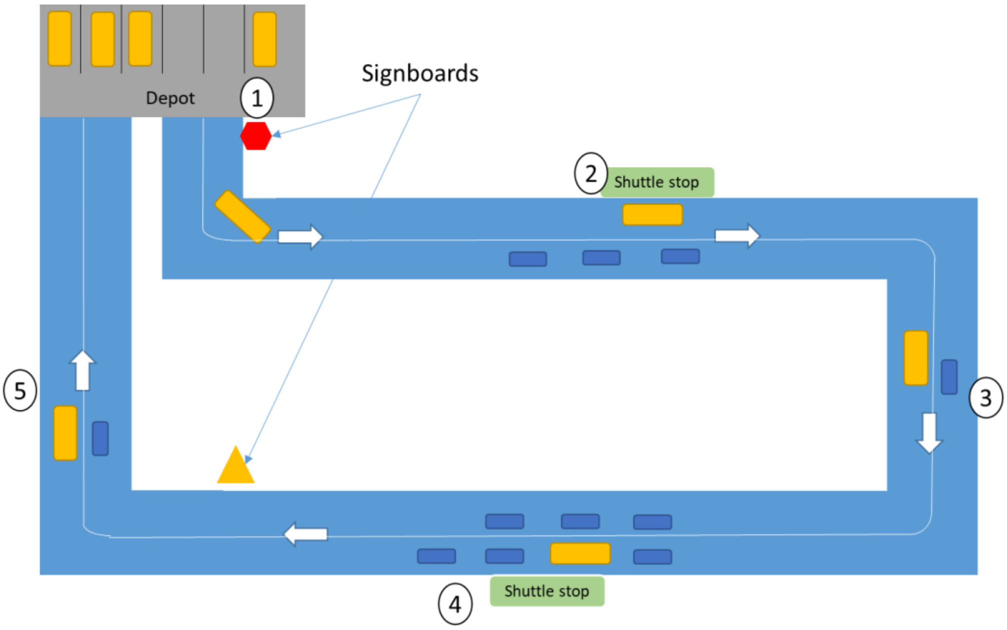


Figure 7: A nominal operation steps for autonomous urban shuttle

Same for the degraded situation leading to an MRM (Figure 8):

1. Detect adverse weather condition or any other failure not allowing to pursue the route
2. Perform an MRM
3. Report to OC
4. Deactivatesystem and wait for OC activation command

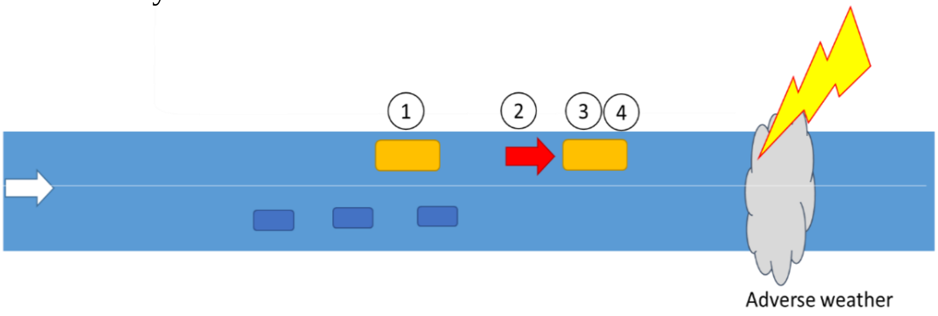


Figure 8: CONOPS in a degraded situation: MRM due to external conditions & obstacles.

The automated/autonomous shuttle could perform an EM/MRM in its lane or join a defined location by the manufacturer specified and maintained free for this purpose.

Concerning the degraded situation leading to an EM (Figure 9Figure 8):

1. Detect internal failure not allowing to pursue the route
2. Perform an EM
3. Report to OC
4. Deactivate system

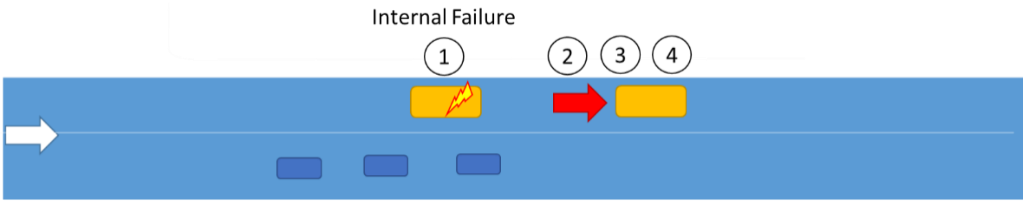


Figure 9: CONOPS in a degraded situation and trigger of an EM

This CONOPS topics has been introduced for ARTS engineering framework, through different tools such as OD, ODD, scenarios, use-cases…, to cope with combinatory and information inflation due to complexity.

3 PRODUCT AND PROCESS REQUIREMENTS

In this chapter, we outline some of the requirements needed to comply with the safety performance and the basic architecture presented in the chapter 2 Framework for definition and technical issues

3.1 General ARTS requirements

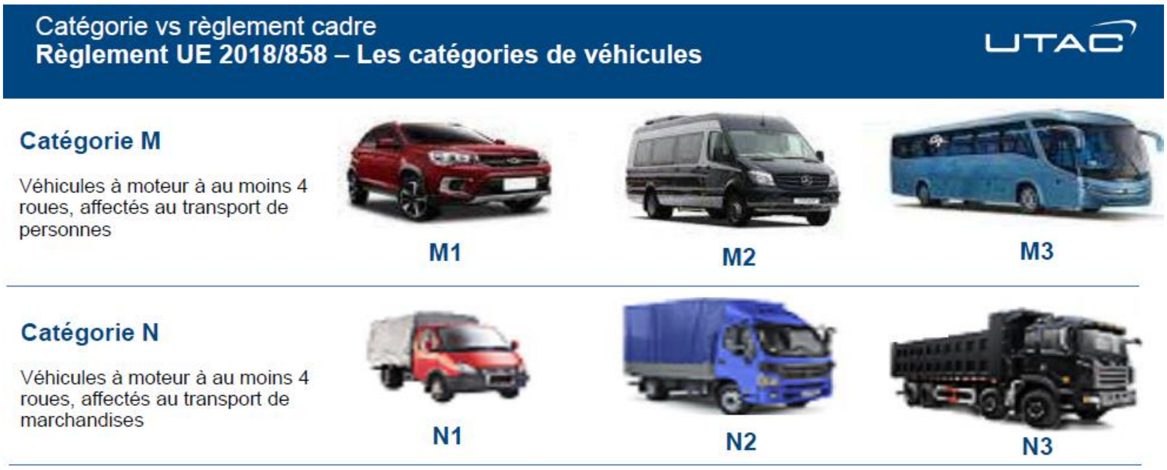
For AI concerned processes, normally followed processes should be adapted to take into account the purpose of AI and its influence on the normal behavior. Tests should take in account the operational specificities of AI Components.

It’s impossible to say at this point in time whether vehicles will be known by their control software or by traditional manufacturers as approached by the report “Le déploiement européen du véhicule autonome” [8].

Our focus is on the mobility vector that contains different types of AI powered modules.

3.1.1. General MV requirements

There are many definitions and names given to staff on board of MV. For the purpose of this documents the roles and responsibilities of the remote operator are described in paragraph 2.1. However, it is assumed that no manual control of the vehicle is possible by the user of the vehicle.



Catégorie vs règlement cadre
Règlement UE 2018/858 – Les catégories de véhicules

Catégorie M

Véhicules à moteur à au moins 4 roues, affectés au transport de personnes

Catégorie N

Véhicules à moteur à au moins 4 roues, affectés au transport de marchandises

Figure 10 Categories of Vehicles. Source UTAC

According to the EU 2018/858 regulation, vehicles are split in different categories Figure 10. MV transporting people fall under the M category and autonomous goods transportation vehicles fall under the category N or L7e for the drones (cf. chapter 1, §4.7 in the French traffic regulation).

It also approaches Advanced Emergency Braking System (AEBS). It is a system which can automatically detect an imminent forward collision and activate the vehicle braking system to decelerate the vehicle with the purpose of avoiding or mitigating a collision.

This braking system is regulated by UNR131 [9] or UNR152 [10] depending on the category of the vehicle. The system’s documentations, performances’ requirements and tests are specified in these regulations. In case the MV uses AEBS driven by AI, it shall comply to this regulation with additional AI Component requirements.

RECC#03) As recommended in these regulations: themselves cannot cover all the traffic conditions but: “Actual conditions and features in the real world should not result in false warnings or false braking to the extent that they encourage the driver to switch the system off.”

Moreover, to comply with the OEDR:

REQ#022) The MV shall be able to detect the risk of collision with other road users, or a suddenly appearing obstacle (debris, lost load) and shall be able to automatically perform appropriate emergency operation (braking, evasive steering) to avoid reasonably foreseeable collisions and minimize risks to safety of the vehicle occupants and other road users.

REQ#022-A) For each AI Component the MV shall recognize all situations when it cannot operate safely. The types of situations shall be declared in the document package (§5.3 UNR157).

REQ#022-B) The ADS shall detect the distance to the next vehicle in front as defined in REQ#096) and shall adapt the vehicle speed in order to avoid collision.

REQ#022-C) While the MV is not at standstill, the ADS shall adapt the speed to adjust the distance to a vehicle in front in the same lane to be equal or greater than the minimum following distance.

REQ#023) The MV shall implement a logic signal indicating emergency braking as specified in UN Regulation No. 13-H.

Regarding the Technical Readiness Level (TRL) described in the ISO16290 [11] (cf.: Annex 2: TRL Levels for a scheme summarizing the standard), as approached in the deliverable 1.5 from the PRISMA project:

REQ#024) The ARTS needs justifications for completeness, coverage, that allow for a consensus between industrialists and certification authorities

REQ#025) Level 4 shuttle types on a given route (typically the Paris2Connect case) must at least be TRL 8.

3.1.2. Event Data Recorder

In Aeronautics a Flight Data Recorder records dozens of flight parameters multiple times in a second continuously. The Cockpit Voice Recorder (CVR) collects the recent history of the sounds in the cockpit including pilots’ conversations. Both devices assist the investigation in case of an incident or accident.

“Event data recorder” (EDR) is a device or function in a vehicle (not necessarily automated/autonomous) that records the vehicle’s dynamic, time-series data during the time period just prior to an event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event.
For the purposes of this definition, the event data does not include audio and video data.[12].
“Event” means a crash or other physical occurrence that causes the trigger threshold to be met or exceeded, or any non-reversible deployable restraint to be deployed, whichever occurs first.

The Automated Lane Keeping Systems (ALKS) or UNR157 [13], is without prejudice to requirements of national and regional laws related to privacy and personal data processing. Hence following parameters are excluded; VIN, associated vehicle details, location/positioning data, information of the driver, and date and time of an event.

The ALKS regulation additionally introduces “Data Storage System for Automated Driving (DSSAD)” which enables the determination of interactions between the actual system and the human driver (UNR157 [13]).

However, the MVs considered in the scope of PRISSMA, autonomous urban shuttles and delivery robot do not fall under conventional categories where airbags or any restraining safety device will be triggered along with the EDR recording.

The UE ADS 2022/1426 [5] does not discriminate vehicles categories and builds a recording system where the ADS records some parameters in addition to EDR and that could be retrieved and protected in a similar way.

Hence, for the scope of the vehicles considered in this document, an extended EDR is suggested that is not triggered by airbag or retraining device solicitation but is dependable on events specific to the MV like EM, MRM and request coming from the user of the shuttle or remote operator. Therefore, requirements from the UN 160 [12] and UNR157 [13] have been adapted for autonomous urban shuttle and delivery robot.

REQ#026) Each vehicle fitted with an EDR shall record the data elements specified as mandatory and those required under specified minimum conditions during the interval/time and at the sample rate specified in 14 Annex 1: EDR Data elements and format, which is adapted from Annex 4, Table 1 of UNR 160 [12]:

REQ#027) Concerning the data recorded:

REQ#027-A) Each data element recorded shall be reported in accordance with the range, accuracy, and resolution specified in Annex 1: EDR Data elements and format.

REQ#027-B) Data stored in the EDR shall be easily readable in a standardized way via the use of an electronic communication interface, at least through the standard interface (On-Board Diagnosis port; approached in the UNR157 [13]).

REQ#028) The longitudinal, lateral, and normal acceleration time-history data, as applicable, shall be filtered either during the recording phase or during the data downloading phase to include (UNR 160 §5.2.2 [12]):

REQ#028-A) The Time Step (TS) that is the inverse of the sampling frequency of the acceleration data and which has units of milliseconds.

REQ#028-B) The number of the first point (NFP), which is an integer that when multiplied by the TS equals the time relative to time zero of the first acceleration data point.

REQ#028-C) The number of the last point (NLP), which is an integer that when multiplied by the TS equals the time relative to time zero of the last acceleration data point; and

REQ#028-D) NLP – NFP + 1 acceleration values sequentially beginning with the acceleration at time NFP * TS and continue sampling the acceleration at TS increments in time until the time NLP * TS is reached.

REQ#029) Regarding the data capture:

REQ#029-A) The EDR shall record the captured data in the vehicle and this data shall remain in the vehicle subject to the provisions of REQ#033), at least until they are retrieved in compliance with national or regional legislation or they are overwritten in compliance with REQ#033). The EDR non-volatile memory buffer shall accommodate the data related to at least two different events.

REQ#029-B) The EDR non-volatile memory buffer shall accommodate the data related to at least two different events.

The data elements for every event shall be captured and recorded by the EDR, as specified in REQ#026) in accordance with the following conditions and circumstances:

REQ#030) An event shall be recorded by the EDR if one of the following threshold values is met or exceeded:

REQ#030-A) Change in longitudinal MV velocity more than 8 km/h within a 150ms or less interval.

REQ#030-B) Change in lateral MV velocity more than 8 km/h within a 150ms or less interval

REQ#030-C) Activation of Vulnerable Road User (VRU) secondary safety system.

If a vehicle is not fitted with any VRU secondary safety system, this document requires neither recording of data nor fitting of such systems. However, if the vehicle is fitted with such a system, then it is mandatory to record the event data following activation of this system.

REQ#031) Conditions for triggering locking of data (UN 160 §5.3.2 [12]): In the circumstances provided below, the memory for the event shall be locked to prevent any future overwriting of the data by subsequent event.

REQ#031-A) In the case of a frontal impact, if the vehicle is not fitted with a non-reversible restraint system for front impact, when the vehicle's velocity change in x-axis direction exceeds 25 km/h within 150ms or less interval.

REQ#031-B) Activation of Vulnerable Road User secondary safety system

REQ#031-C) Events listed in REQ#044) d) (if applicable).

REQ#032) Conditions for establishment of time zero: Time zero is established at the time when any of the following first occurs (UN 160 §5.3.3 [12]):

REQ#032-A) For continuously running algorithms, i - The first point in the interval where a longitudinal, cumulative delta-V of over 0.8 km/h is reached within a 20 ms time period; or

ii - For vehicles that record "delta-V, lateral," the first point in the interval where a lateral, cumulative delta-V of over 0.8 km/h is reached within a 5 ms time peri-od; or

REQ#032-B) Activation of VRU secondary safety protection system.

REQ#032-C) Events listed in REQ#044) (if applicable).

REQ#033) About overwriting (UN 160 §5.3.4 [12]):

REQ#033-A) If an EDR non-volatile memory buffer void of previous-event data is not available, the recorded data shall, subject to the provisions of REQ#031), be over-written by the current event data, on a first-in first-out basis, or according to different strategies decided by the manufacturer and made available to the relevant authorities of Contracting Parties.

REQ#033-B) Furthermore, if an EDR non-volatile memory buffer void of previous-event data is not available, data originating from non-reversible restraint system or Vulnerable Road User secondary safety system deployment events referred to in REQ#031)shall always overwrite any other data that is not locked per REQ#031).

REQ#034) Power failure (UN 160 §5.3.5 [12]): Data recorded in non-volatile memory is retained after loss of power.

REQ#035) Crash test performance and survivability (UN 160 §5.4 [12]):

REQ#035-A) Each Mobile Vector of an ARTS subject to the requirements of national or regional frontal crash test regulations, shall conform to the specifications in REQ#035-C).

REQ#035-B) 5.4.2. Each Mobile Vector of an ARTS subject to the requirements of national or regional side impact crash test regulations shall conform to the specifications of REQ#035-C).

REQ#035-C) The data elements required by REQ#068), shall be recorded in the format specified by REQ#028), exist at the completion of the crash test and the complete data recorded element shall read "yes" after the test. Elements that are not operating normally in crash tests (e.g., those related to engine operation, braking, etc.) are not required to meet the accuracy or resolution requirements in these crash tests.

The data shall be retrievable even after an impact of a severity level set by UN Regulations No 94 [14] , 95 [15] or 137 [16] depending on the class of vehicles.

REQ#036) Instructions from the manufacturer shall be provided on how to access the data (cf. UN160 [12]).

REQ#037) It shall not be possible to deactivate the Event Data Recorder (UN 160 §5.5 [12]).

REQ#038) Availability of EDR operation: EDR shall be able to communicate with the ARTS to inform that the EDR is operational.

REQ#039) Protection against manipulation. It shall be ensured that there is adequate protection against manipulation (e.g., data erasure) of stored data such as anti-tampering design (cf. UN160 [13]).

REQ#040) In case of an urban shuttle or delivery robot, there is no driver, the MV is responsible for its EM and MRM. The user can trigger an EM/MRM. DSSAS will then record the origin of the EM/MRM request but the MV conducts the maneuvers automatically. The remote operator could also emit EM/MRM request but it shall be assessed by the MV before engaging in such a maneuver.

REQ#041) The EDR and additional recorded data shall be available subject to requirements of national and regional law.

REQ#042) Documented evidence regarding the storage capacity shall be provided by the vehicle manufacturer.

REQ#043) For each event listed in REQ#044) the R15X SWIN for ADS, or the software versions relevant to ALKS, indicating the software that was present at the time when the event occurred, shall be clearly identifiable.

In addition to conventional data required by the EDR regulation which has been adapted to the scope of urban shuttle some parameters are specific to MVs incorporated in ARTS and delivery robot.

Hence some new parameters are to record. It is still to be decided whether they should be added to the conventional EDR list or recorded in a separate device. EDR recording is conventionally limited to contextual accident of an event. Whereas DSSAD recording may record data up to 6 months. So, if they are recorded in the same device EDR shall have more capacity. For the scope of document only one EDR has been considered recording both types of parameters.

REQ#044) Each autonomous urban shuttle or delivery robot shall record at least and entry for each of the following occurrences upon activation:

a) Activation/re-initialization of the ADS (if applicable)
b) Deactivation of the ADS
c) Request sent by the ADS to the remote intervention operator (if applicable)
d) Request/Input sent by the remote intervention operator (if applicable)
e) Command from user of the vehicle (for the autonomous urban shuttle)
f) Command from the remote operator in the Operation Center
    i. MRM command
    ii. EM command
    iii. Itinerary modification
g) Command from user of the vehicle
    i. MRM command
    ii. EM command
    iii. Itinerary modification

h) Start of Emergency Maneuver
i) End of Emergency Maneuver
j) Involved in a detected collision
k) Start of lane change procedure
l) End of lane change procedure
m) Abortion of lane change procedure
n) Change of lane
o) Minimum Risk Maneuver engagement by ADS
p) End of Minimum risk Maneuver (Minimum Risk Condition)
q) Severe Autonomous Driving System failure (Description)
r) Severe vehicle failure.

If this list is recorded in the EDR then REQ#031-C) and REQ#031-B) become applicable. This additional data could then follow the same format of recording as recommended by UNR160 [12]. For the moment UE ADS [5] and ALKS [13] require a time stamp with the actual date and GPS location.

3.1.3. Activation/Deactivation of Autonomous Driving System

In the case of fully autonomous urban shuttle and delivery robot there is no manual driving mode. The ADS is activated with the start of the MV. There are no transition phases from ADS to a driver. The users have limited agency over the ADS. They can modify the itinerary and command EM and MRM.

REQ#045) The manufacturer shall assess the AI Components failures and their management.

REQ#046) The automatic driving mode shall ensure all AI Components are operating to the necessary functioning level required to operate.

The UNR157 specifies how ALKS module shall operate. The aim of this AI Component being to keep the vehicle within the lane when activated. For other AI Components this regulation can be used as an example.

REQ#047) The ADS shall perform the DDT and shall manage all situations including failures, and shall be free of unreasonable risks for the vehicle occupants or any other road users.

REQ#048) The activated ADS shall not cause any collisions that are reasonably foreseeable and preventable. If a collision can be safely avoided without causing another one, it shall be avoided. When the vehicle is involved in a detectable collision, the vehicle shall be brought to a standstill. (UNR157 §5.1.[13])

REQ#049) The ADS shall comply with traffic rules relating to the DDT in the country of operation.

REQ#050) As approached in the EU ADS: the ADS shall activate the relevant vehicle systems when necessary and applicable (e.g., opening doors, activate wipers in case of rain, heating system, etc.)

REQ#051) A demand for remote operator intervention shall not endanger the safety of the vehicle occupants or other road users.

REQ#052) The ADS shall perform self-checks to detect the occurrence of failures and to confirm ADS performance at all times (e.g., after vehicle start the ARTS has at least once detected an object at the same or a higher distance than that declared as detection range according to REQ#094) and onward).

REQ#053) The effectiveness of the ADS shall not be adversely affected by magnetic or electrical fields. This shall be demonstrated by compliance with the 05 or later series of amendments to UN Regulation No. 10 [17].

REQ#054) The manufacturer shall take measures to guard against reasonably foreseeable misuse and tampering of the ADS.

REQ#055) When the ADS can no longer meet the requirements of the associated regulation when existing (like ALKS, AEBS, ADS), it shall not be possible to activate the ADS. In case there is no specific regulation for this situation, the manufacturer shall reach an equivalent level of requirements for its AI Component and deactivate when the essential set of requirements are not met.

REQ#056) The manufacturer shall identify roles and responsibility of each AI Component and its impact on dynamic driving task. The section 5.2 of UNR157 [13] can be used as a starting point including other AI Components impacts.

REQ#057) The user of the vehicle (urban shuttle) or remote operator actions to request EM/MRM shall be identical in both following cases:

- The remote operator interacts with the ADS from his/her own (without prior ADS request).
- After the ADS raised an alert within the vehicle and/or remote operation station.

REQ#058) When the remote operator/user pushes MRM or EM request on her/his own (without prior ADS alert), the vehicle shall not respond by an inappropriate action (e.g., by switching headlamps off, at night).

REQ#059) Each given AI Component shall be demonstrated to be safe, based on the ODD it's associated with.

REQ#060) In case the minimum time gap cannot be respected temporarily because of other road users (e.g., vehicle is cutting in, decelerating lead vehicle, etc.), the vehicle shall readjust the minimum following distance at the next available opportunity without any harsh braking unless an emergency maneuver would become necessary.

REQ#061) The minimum following distance shall be calculated using the formula given in UNR157 §5.2.3.3 [13]

REQ#062) The ADS shall be able to bring the vehicle to a complete stop behind a stationary vehicle, a stationary road user or a blocked lane of travel to avoid a collision. This shall be ensured up to the maximum operational speed of the system.

REQ#063) The ADS shall detect the risk of collision in particular with another road user ahead or beside the vehicle, due to a decelerating lead vehicle, a cutting in vehicle or a suddenly appearing obstacle and shall automatically perform appropriate maneuvers to minimize risks to safety of the vehicle occupants and other road users.

For conditions not specified in paragraphs REQ#062) and REQ#063) or its subparagraphs, this shall be ensured at least to the level at which a competent and careful human driver could minimize the risks. This shall be demonstrated in the assessment carried out under Annex 4 [13] and by taking guidance from Appendix 3 to Annex 4 in UNR157.

REQ#064) The ADS shall avoid a collision with a leading vehicle which decelerates up to its full braking performance provided that there was no undercut of the minimum following distance the ADS would adjust to a leading vehicle at the present speed due to a cut in maneuver of this lead vehicle.

REQ#065) The Ads shall avoid a collision with a cutting in vehicle,

REQ#065-A) As approached in the §5.2.5.2 UNR157 [13]:

i - Provided the cutting in vehicle maintains its longitudinal speed which is lower than the longitudinal speed of the ADS

ii - Provided that the lateral movement of the cutting in vehicle has been visible for a time of at least 0.72 seconds before the reference point for Time To Collision due to a lane intrusion ($TTC_{\text{lane intrusion}}$) is reached

iii - When the distance between the vehicle’s front and the cutting in vehicle’s rear corresponds to a $TTC_{\text{lane intrusion}}$ calculated the equation given in the same paragraph.

REQ#065-B) As approached in §1.4.2 of the EU ADS 2022/1426 [5]:

i - Collisions with cutting in vehicles, pedestrians and cyclists travelling in the same direction, as well as with pedestrians who can start to cross the street, shall be avoided.

ii - The conditions to avoid a collision is expressed by the equation shown in the same paragraph.

REQ#066) The ADS shall avoid a collision with an unobstructed crossing pedestrian in front of the vehicle. In a scenario with an unobstructed pedestrian crossing with a lateral speed component of not more than 5 km/h where the anticipated impact point is displaced by not more than 0.2 m compared to the vehicle longitudinal center plane, the ADS shall avoid a collision up to the maximum operational speed of the system.

REQ#067) It is recognized that the fulfilment of the requirement in REQ#063) may not be fully achieved in other conditions than those described above. However, the ADS shall not deactivate or unreasonably switch the control strategy in these other conditions. This shall be demonstrated in accordance with Annex 4 of UNR157 [13].

REQ#068) The manufacturer shall demonstrate that automatization modules are sufficient to control (position, interactions) autonomously the MV (urban shuttle and delivery robot) without a driver and precise clearly the roles and responsibilities of the remote operators and users of the vehicle.

REQ#069) The manufacturer shall declare and implement a process to manage the safety and continued compliance of the AI Components over lifetime.

3.1.4. Human Machine Interface/remote operator information

This paragraph provides requirements on Human Machine Interface and remote operator information.

REQ#070) The ADS shall become active only upon a deliberate action by the remote operator and if all the following conditions are met:

- No failure affecting the safe operation of ADS is present;
- EDR is operational
- The environmental and infrastructural conditions allow the operation;
- Positive confirmation of ADS self-check;

REQ#071) If any of the above conditions is no longer fulfilled, the ADS shall immediately initiate an MRM, report it to operation center and wait for its instructions.

REQ#072) The remote operator/user shall be able to select the itinerary the ADS is going to operate.

REQ#073) The means of selecting routes shall provide protection against erroneous for example by asking a confirmation or selection by name and by map display.

REQ#074) The means to push an EM or an MRM request shall be protected against an unintentional request for example by requiring a single input exceeding a certain threshold of time or a double press, or two separate but simultaneous inputs.

REQ#075) The ADS shall not be deactivated other than

- by a demand of the remote operator
- after an ADS failure not allowing to continue the mission.

REQ#076) In case of an ongoing emergency maneuver, the deactivation of the ADS may be delayed until the imminent collision risk disappeared.

REQ#077) In case of a severe vehicle failure or a severe failure on an autonomous function the AI Component may employ different strategies with regard to deactivation.

REQ#078) These different strategies shall be declared by the manufacturer and their effectiveness shall be assessed by the Technical Service with regard to ensuring a safe MRM or EM to reach MRC.

REQ#079) The ADS shall execute an MRM to achieve an MRC in the event of a failure of the ADS and/or other vehicle system that prevents the ADS from performing the DDT. (UE ADS 2022/1426, §4.1.2.2 [5])

REQ#080) The ADS shall immediately upon detection, signal major failures and resulting operational status to vehicle occupants or to the remote intervention operator (if relevant), as well as to other road users in accordance with traffic rules (e.g., activation of the hazard warning lights). (UE ADS 4.1.2.3.)

REQ#081) Notwithstanding one autonomous function failure, any other safety system delivering longitudinal or lateral support in imminent collision situations (e.g., Advanced Emergency Braking System (AEBS), Electronic Stability Control (ESC), Brake Assist System (BAS) or Emergency Steering Function (ESF)) shall not be deactivated in case of deactivation of one function.

As MV is either an autonomous shuttle or delivery robot no control of operator is needed to operate MRM or EM. Thus, there is no need to monitor their presence and focus. The alerts are sent to Operation Center for information to retrieve the MV in case of severe failure and operation abortion.

REQ#082) The following information shall be indicated to the operators:

a) The ADS status as defined in paragraph below
b) Any failure affecting the operation of the ADS with at least an optical signal
c) Minimum risk maneuver by at least an optical signal and in addition an acoustic and/or a haptic warning signal and
d) Emergency maneuver by an optical signal
e) The optical signals above shall be adequate in size and contrast. The acoustic signals above shall be loud and clear

3.1.5. ARTS status

This section provides requirements on the ARTS status for the users of the vehicle and the remote operator based on the approach of the §6 of the EU ADS [5].

REQ#083) Adequate information shall be given to the occupants of the ARTS wherever needed for safe operation and with regard to safety hazards.

REQ#084) The ARTS shall provide means for MV occupants to call the remote operator through an audiovisual interface in the fully automated vehicle.

REQ#085) The ADS shall provide vehicle occupants with means to request an MRM to stop the fully automated vehicle. In case of emergency:

REQ#085-A) for vehicles equipped with automatically operated doors, the unlocking of the doors shall be conducted automatically when it is safe to do so,

REQ#085-B) a mean shall be given to passengers to exit a vehicle at standstill (opening the doors or via an emergency exit).

REQ#086) The ARTS shall provide vision systems of the occupant space inside the vehicle and of the surrounding of the vehicle to allow the remote intervention operator to assess the situation inside and outside of the vehicle.

RECC#04) The vision systems provided should follow chapter 6 of ISO 16505 [22]

REQ#087) It shall be possible for the remote operator to open the power operated service door remotely.

3.2 AI related requirements

The following requirements gives an approach for AI related product and process.

REQ#088) Data set produced for learning process shall be protected against damage (alteration, substitution or mishandling).

REQ#089) Data set used for learning process shall comply with GDPR

REQ#090) The ADS shall be embedded with one or more itinerary the MV will follow in a secure way. It shall not be possible to alter them by exterior menace and by interior fault. If a corruption is detected the ADS shall initiate an MRM.

REQ#091) The AI Components shall keep the vehicle inside its lane of travel while driving in nominal situation and ensure that the vehicle does not cross any lane marking (outer edge of the front tyre to outer edge of the lane marking). The ADS shall aim to keep the vehicle in a stable lateral position inside the lane of travel to avoid confusing other road users. (UNR157, §5.2.1 [13])

REQ#092) The AI Components shall detect a vehicle driving beside as defined in next requirements and, if necessary, adjust the speed and/or the lateral position of the vehicle within its lane as appropriate. (UNR157, §5.2.2.[13])

REQ#093) As the §1.2 from the EU ADS [5] details: the ADS shall detect and respond appropriately to objects and events relevant for the DDT within the ODD. Objects and events might include, but are not limited, to:

a) motor vehicles and other road user such as motorcycles, bicycles, scooters, wheelchair users, pedestrians, and obstacles (e.g., debris, lost cargo);
b) road accidents;
c) traffic congestions;
d) road works;
e) road safety officers and law enforcement agents;
f) emergency vehicles;
g) traffic signs, road markings;
h) environmental conditions (e.g., lower speed due to rain, snow).

REQ#094) Concerning the Sensing requirements: the fulfilment of the provisions of this requirement shall be demonstrated by the manufacturer to the technical service during the inspection of the safety approach as part of the assessment to Annex 4 (UNR157,[13]) and according to the relevant tests in Annex 5 (UNR157, §7.1 [13])

REQ#095) The MV shall be equipped with a sensing system such that, it can at least determine the driving environment (e.g., road geometry ahead, lane markings, traffic lights, signboards) and the traffic dynamics:

REQ#095-A) Across the full width of its own traffic lane, the full width of the traffic lanes immediately to its left and to its right, up to the limit of the forward detection range;

REQ#095-B) Along the full length of the vehicle and up to the limit of the lateral detection range.

REQ#095-C) Even when infrastructure is temporary for example underwork may have additional signboards, modified traffic lights, modified route geometry and additional infrastructure.

REQ#096) Concerning the forward detection range:

REQ#096-A) The manufacturer shall declare the forward detection range measured from the forward most point of the vehicle. This declared value shall be at least 46 meters.

REQ#096-B) The Technical Service shall verify that the distance at which the vehicle sensing system detects a road user during the relevant test in Annex 5 (UNR157, [13]) is equal or greater than the declared value.

REQ#097) Lateral detection range: The manufacturer shall declare the lateral detection range. The declared range shall be sufficient to cover the full width of the lane immediately to the left and of the lane immediately to the right of the vehicle.

REQ#098) The ARTS shall implement strategies to detect and compensate for environmental conditions that reduce the detection range, e.g., alerting the remote operator and passengers via voice alerting and reducing the speed when visibility is too low. These strategies shall be described by the manufacturer and assessed according to Annex 4 (UNR157, §7.1.3.[13])

REQ#099) A single perception malfunction without failure should not induce hazardous event. The design strategies put in place shall be described by the vehicle manufacturer and their safety shall be demonstrated to the satisfaction of the technical service in accordance with Annex 4. (UNR157, 7.1.6 [13])

REQ#100) Use mechanisms to ensure responsibility and accountability for AI systems and their outcomes, both before and after their development, deployment and use.

REQ#101) Identify the various specifications that influence the later life cycle stages of the vehicle and those of the implemented AI Components.

3.3 System of system level: Smart Mobility System

REQ#102) The Mobile Vector of an ARTS should be able to provide the user and remote operator with information about itself and its activity. This information should be displayed to the users and remote operator via an interface with a real view of the MV environment.

REQ#102-A) A special care for the choice of the operation routes should be taken in account in compliancy with the ODD.

4 OTHER PROCESS AND AUDIT REQUIREMENTS

The following requirements details how the process should proceed and how the audit should be conducted.

4.1 Question list to carry an audit

The purpose of this section is to provide the auditor with a list of questions that can be used while carrying an audit, and which are proposed as examples:

- How is your Engineering process organized?
- Who are the actors and their roles?
- How do you prove relevancy of your engineering processes to the use of AI?
- How do you specifically target functional Added value of AI in product?
- What are the CONOPS of your system?
- What is your Engineering process framework?
- What Tools do support your Engineering Process?
- How do you manage Work Breakdown Structure of your Engineering process?
- What is your Configuration Management Process, how is it managed?
- How AI is specifically targeted in your Engineering process?

This list isn’t exhaustive other questions could be added.

4.2 System engineering process requirements

All complex systems need a highly coordinated process that needs to go through all the phases of life cycle. To achieve the goal, which is the purpose of this document, we can focus on certification process. To achieve certification, one product needs to satisfy the certification criterion for every step of its designing process.

REQ#103) An impact analysis on the production without AI system engineering shall be carried out with regard to that product integrating AI.

REQ#104) The process of system engineering shall adapt to the new product and well define the roles and responsibilities of all the stakeholders of the project.

REQ#105) Description and structuration of development process shall be provided.

REQ#106) Organization supporting development process should be described and roles shall be detailed concerning all actors or services being involved in this process.

REQ#107) Specification process shall be documented. Meaning a list of specifications/requirements needs to be built and checked through every phase of the product development life cycle.

REQ#108) Performance allocation process shall be documented

REQ#109) Hazard Analysis (HA) shall be documented to exhibit how AI bricks may produce feared events or situation

REQ#110) Preliminary Hazard Analysis (PHA) and HA results post processing must highlight how performance is allocated on AI.

REQ#111) Demonstration or justification process about allocated performance shall be documented.

REQ#112) Validation process shall be documented.

REQ#113) Iteration process shall be documented and the way how incremental loops are processed- regarding events producing these loops.

REQ#114) The Original Equipment Manufacturers (OEMs) shall set up a common process to create and maintain a common catalog (*) of scenario, including misuses, to be used for safety argumentation during design and verification/validation phases (**).
(*) the catalog will be enriched continuously trough feedback through the life of the product
(**) in compliance with laws (e.g., competitive laws)

REQ#115) The OEM shall set up internally, a process to collect, archive (General Data Protection Regulation "GDPR", time of archiving, structuration…), analyze and treat incidents/accidents faced by the customers, and if necessary, update the vehicles.
UNR157 concerning Automated Lane Keeping System requires demonstration with regards to sensing during the safety approach inspection. An automated urban shuttle shall be equipped with more than one AI enhanced system (other than ALKS).

REQ#116) The OEM shall demonstrate acceptable safety levels for all AI enhanced functionalities taking example on the last available regulations.

4.3 General requirements about global safety assurance methods and processes

Concerning the general requirements about global safety assurance methods and processes, the annex 2 of deliverable 1.5 from the PRISSMA project [19] give us an approach.

To evaluate AI systems for automated and autonomous mobility vectors and ensure their operation, several challenges related to autonomous systems and AI must be addressed:

1. Accounting for the "non-deterministic" nature of AI techniques.
2. Managing the life cycle and evolution capabilities of systems and functions, particularly after the use of AI-based techniques.
3. Maintaining auditability, robustness, and safety requirements specific to critical functions and systems.
4. Standardizing the methods considered to enable compatibility with international work and to enable their deployment on a large scale.
5. Managing the inherent complexity of a system of systems.

To develop a global safety approach, one should initially target the three following objectives:

1. Identify and list safety and reliability objectives for AI-based autonomous mobility systems and develop complete validation processes for reliability aimed at the commercial operation of SAE Level 4 autonomous mobility services by 2024.
2. Ensure the availability of shared concepts to address the complexity of AI-based autonomous mobility systems, which can be used internationally.

3. Participate in implementing prerequisites that will enable France to position itself at the European level to host one of the autonomous mobility test centers that will be developed in the coming years.

To ensure the safety and reliability of systems deployed for commercial operation, the first step will be to identify the characteristics of an AI-based system and its components, as well as the key performance indicators (KPI) corresponding to the objective to be achieved to demonstrate mastery of the system and the methods and processes to be implemented.

Once the demonstration scope is identified, a general safety process will need:

- to develop questions to be asked to the actor wishing to obtain the commissioning of an AI-based autonomous mobility system
- to determine acceptable evidence
- to specify the means of demonstrations and associated tools allowing this actor to demonstrate the safety of their system.

The demonstration objectives will be consolidated into a common reference and may result from ongoing work at the French, European, and international levels.

For this purpose, one will thus determine the means of qualifying simulation tools and associated databases, as well as requirements for processes using them.

The challenge of this safety process is the integration of simulation as a means of demonstration through the provision of acceptable proof. The use of this process as a necessary step in demonstrating mastery of functions is recognized as essential to bring autonomous mobility services to market due to the complexity of combinations of events and situations that may arise. A global safety process will need to propose elements enabling the demonstration of this mastery, going up to homologation and incorporating improvements throughout the ARTS life cycle.

4.4 Further audit on the design

4.4.1. AI oriented ARTS requirements

This paragraph provides requirements for AI oriented ARTS requirements

REQ#117) The Technical Service shall verify that the MV sensing system detects vehicles during the relevant test in Annex 5 (UNR157 [13])**.** This range shall be equal or greater than the declared range (UNR157, 7.1.2 [13]).

REQ#118) The manufacturer of Mobile Vector of ARTS shall provide evidence that the effects of wear and ageing do not reduce the performance of the sensing system below the minimum required value specified in REQ#107-111 over the lifetime of the system/vehicle. (UNR157, 7.1.4 [13])

REQ#119) The fulfilment of the provisions of the above REQ#094) to REQ#098) and its subparagraphs shall be demonstrated to the technical service and tested according to the relevant tests in Annex 5 (UNR157 [13])**.**

REQ#120) Develop, deploy and use AI systems in a way that adheres to the ethical principles of: respect for human autonomy, prevention of harm, fairness and explicability. Acknowledge and address the potential tensions between these principles.

REQ#121) A set of information must be clearly identified and reported about the expected purpose of the ARTS; for instance, pieces of information are:

- The expected purpose of the ARTS, the expected users of the ARTS, and the laws that must and must not be followed.
- The characteristics of the dataset, its collection method, associated preprocessing, and the tasks for which it should be used and those for which it should not.
- The characteristics of the model, the algorithm used, and its evaluation procedures.
- The known or expected limitations of the datasets used to train the decision-making models

REQ#122) Each AI system must be trustworthy:

- it should be lawful (complying with all applicable laws and regulations)
- it should be ethical, ensuring adherence to ethical principles and values and
- It should be robust both from technical and social perspective.

REQ#123) The manufacturer shall ensure that the development, deployment and use of AI Component meets the seven key requirements for Trustworthy AI: (1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability.

REQ#124) The manufacturer shall communicate, in a clear and proactive manner, information to stakeholders about the vehicle's capabilities and limitations, enabling realistic expectation setting, and about the manner in which the requirements are implemented. Be transparent about the fact that they are dealing with an AI system.

REQ#125) The manufacturer shall facilitate the traceability and auditability of the vehicle, particularly in critical contexts or situations.

REQ#126) The manufacturer shall involve stakeholders throughout the vehicle's life cycle. Foster training and education so that all stakeholders are aware of and trained in Trustworthy AI.

REQ#127) The manufacturer shall be mindful that there might be fundamental tensions between different principles and requirements. Continuously identify, evaluate, document and communicate these trade-offs and their solutions.

REQ#128) The manufacturer shall create a model card to disclose information about each AI Component.

4.5 IVVQ process audit on specific modular AI bricks

In the case of vector of mobility (shuttles or droids) there are three levels of framework. Each one of them requires different kind of focus:

1. AI Component level: certification requirements
2. Mobility Vector level: homologation requirements
3. System of system level: validation requirements

The corner stone of certification of system, including AI bricks, refers to specific IVVQ process audit on specific modular AI bricks at AI Component level.

This means minimum requirements shall be applied to elementary AI bricks at each step of their integration.

4.5.1. AI Component level

Among the following requirements, those concerning “data set” mainly apply to supervised Machine Learning based AI technics.

REQ#129) Each equipment comprising AI functionality shall have his own certification and therefore shall have been submitted to a specific IVVQ process.

REQ#130) Data Set used for learning process shall be qualified, traced and annotated as from the meaning and relevancy of the content.

REQ#131) Data Set used for learning process shall be managed as to failure or uncoherent pieces of information.

REQ#132) Design Data Set, Validation Data Set and Evaluation Data Set shall be supplied as well as methodology applied to mix or cross check those Data Set on a deterministic or stochastic way.

REQ#133) Data Set and Data Base shall be qualified as to its coverage, parameter distribution, volume and precision issues.

REQ#134) Data Set and Data Base content shall be assessed from Safety and Rare Events issues.

REQ#135) Tools used for Data Set assessment campaigns shall be qualified and certified.

REQ#136) Key performance Indicators (KPI) used to quantify AI Component performance shall be communicated and justify. Here is a list of examples of KPI needed: relevancy, resilience, stability, robustness, explainability, interpretability…

4.5.2. System of System Level: Smart Mobility System

ARTS/droid system of system may differ from one site of operation to the other. Even within one site systems may vary. It will highly depend on available infrastructure, landscape, culture, available technologies and their coverage of the city.

ARTS might be logistically supervised in different ways. There can be multiple solution to come up with a safe operation.

The whole existing infrastructure and technologies will not be submitted to a constraining audit as for AI Components or ARTS. Rather, tests will be conducted in all representative segments of a system of system to guarantee an end-to-end safe operation.

REQ#137) Main Contractor (MC) shall provide a list of services provided by ARTS and independent from Hardware / Software variability of MV.

REQ#138) MC shall supply test report of those services and type of MVs which have been involved in these tests.

REQ#139) MC shall specify minimum safety rules to be complied with by MVs so that to be resilient to any failure of integrity default generated by these services (wrong position or obstacle information transmitted by 5G. In the documentation package required by UNR157 [13] it should include the safety concept of the manufacturer, safety management system process audit).

RECC#05) The MV should be able to generate the bird’s eye view to give the human supervisor a better perspective of its surroundings.

4.5.2.1.Cyber Security

The effectiveness of the ARTS shall not be adversely affected by cyber-attacks, cyber threats and vulnerabilities. For MVs, the effectiveness of the security measures shall be demonstrated by compliance with UN Regulation No. 157.

REQ#140) If the MV permits software updates, the effectiveness of the software update procedures and processes shall be demonstrated by compliance with UN Regulation No. 157. (UNR157, 9.2 [13])

Concerning requirements for software identification (UNR157, 9.3 [13]):

REQ#141) For the purpose of ensuring the software of the ADS can be identified, an R15XSWIN may be implemented by the vehicle manufacturer. If R15XSWIN is not implemented, an alternative software identification system (i.e., software version) shall be implemented.

REQ#142) If the manufacturer implements an R15XWIN the following shall apply:

REQ#142-A) The vehicle manufacturer shall provide the following information in the communication form of this Regulation:

a) The R15XSWIN

b) How to read the R15XSWIN or software version(s) in case the R15XSWIN is not held on the vehicle

REQ#142-B) The vehicle manufacturer may provide in the communication form of this Regulation a list of the relevant parameters that will allow the identification of those vehicles that can be updated with the software represented by the R15XSWIN. The information provided shall be declared by the vehicle manufacturer and may not be verified by an Approval Authority.

REQ#142-C) The vehicle manufacturer may obtain a new vehicle approval for the purpose of differentiating software versions intended to be used on vehicles already registered in the market from the software versions that are used on new vehicles. This may cover the situations where type approval regulations are updated or hardware changes are made to vehicles in series production. In agreement with the testing agency, duplication of tests shall be avoided where possible.

REQ#143) The vehicle manufacturer shall have a valid approval according to UN Regulation No. 157 [13] (Software Update Regulation).

REQ#144) All safety related dataflow on board of the vehicle and between the Operation Center and the vehicle shall be protected against any malevolent attack and use.

4.6 Data set and Key Performance metrics

The following requirements impact the data set required for learning of one AI Component:

REQ#145) The manufacturer shall guarantee the correct selection of dataset for training, training methods, testing methods (metrics) and correction methods.

REQ#146) The manufacturer should/shall justify the choice of metrics to test the relevancy.

4.7 Justification evidences to provide

It can be limiting for manufacturers of AI containing systems to provide a strict set of justification. It might also hinder innovations.

Therefore, justification evidences shall contain all the data relevant to the specific AI and all the tests and evaluation systems put in place by the manufacturer to guarantee the safe function.

Everything focused on the justification dossier is addressed in the deliverable 6.6 of the Prisma project [20].

4.8 Subsystem, AI Components and System of System development standard

This paragraph is a formulation requirement to ensure consistency between engineering process of AI Components, ARTS Mobile Vectors and System of System Smart Mobility System (SMS).

REQ#147) Integration process shall be documented.

REQ#148) All parts and modules composing ARTS system must be tested individually as well as when implementing them.

REQ#149) Test reports shall be saved.

5 SIMULATION REQUIREMENTS

5.1 Introduction

This paragraph is built with other PRISSMA Work Package result, more precisely with the WP2 which cover the simulation tests as well as PoC about it.

As approached in the deliverable 2.7 from the PRISSMA project, safety of the AI-based systems has taken a center stage in the validation of the whole system. Even more, it has a direct impact on humans' lives and so it asks for a heightened level of scrutiny in their evaluation procedure. Thus, it is mandatory to establish a comprehensive and rigorous processes to ensure effectiveness.

REQ#150) The high-level process for the evaluation should at least follow the workflow shown in Annex 3: global process for evaluating a critical AI-based system issued from the Deliverable 2.7

Focusing on simulations, they have to be performed to demonstrate Safety performance in a "Digital twin" context, following questions should be answered:

- What is the Simulation strategy? Model In the Loop (MIL)/ Hardware In the Loop (HIL)/ Vehicle In the Loop (VIL)?
- What is the description of the Simulation Platform?
- How "co-simulation" process has been achieved in this workbench?
- Have simulation tasks been subcontracted to other suppliers?
- Is it possible to have access to simulation assets?
- What is the Scenario Library considered: industrial will provide description of scenarios simulated, justification of choice of scenarios as to safety and coverage of CONOPS, severity qualification of scenarios?
- How are these scenarios chosen? Language used?
- Is it possible to have access to scenario processing trace: choice of metrics and justification of this choice as to Safety?

5.2 The generic PRISSMA's evaluation /validation framework issued by the deliverable 2.7

Considering all constraints and requirements a generic evaluation/validation framework has been proposed by the deliverable 2.7 issued by the PRISSMA project based on 3 layers:

1) **Layer 1:** this layer is dedicated to the definition and the generation of the system under test, the simulation environment, the testing objectives and constraint.
2) **Layer 2:** the second layer consists to apply the scenarios on the system/component in the testing objective framework with constraints and limits provided by ODD in order to collect data about the behavior of the system/components respecting the OEDR.
3) **Layer 3:** the last layer will use the 2 datasets generated by the previous layer in order to evaluate and validate the performances of the system in specific environments and conditions.

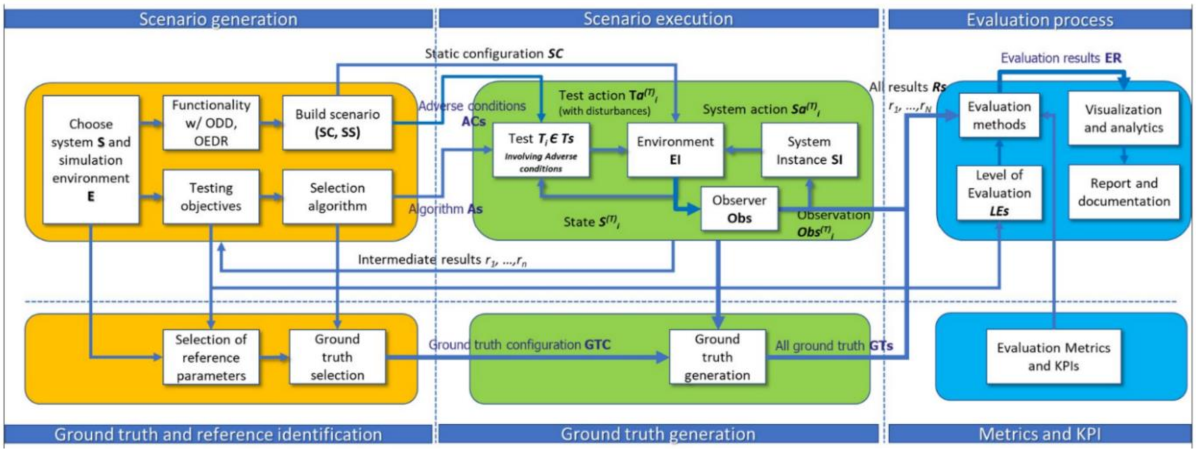

Scenario generation
Scenario execution
Evaluation process
Static configuration SC
Choose system S and simulation environment E
Functionality w/ ODD, OEDR
Build scenario (SC, SS)
Testing objectives
Selection algorithm
Adverse conditions ACs
Algorithm As
Test action $Ta^{(T)}_i$ (with disturbances)
System action $Sa^{(T)}_i$
Test $T_i \in Ts$ Involving Adverse conditions
Environment EI
System Instance SI
Observer Obs
State $S^{(T)}_i$
Observation $Obs^{(T)}_i$
Intermediate results $r_1, \ldots, r_n$
All results Rs $r_1, \ldots, r_N$
Evaluation results ER
Evaluation methods
Visualization and analytics
Level of Evaluation LEs
Report and documentation
Selection of reference parameters
Ground truth selection
Ground truth configuration GTC
Ground truth generation
All ground truth GTs
Evaluation Metrics and KPIs
Ground truth and reference identification
Ground truth generation
Metrics and KPI

Figure 11: Simulation framework for evaluation of AI-powered systems in ARTS issued by the deliverable 2.7 (PRISSMA)

NB: cf. deliverable 2.7 for more detail on the method

5.3 Simulation Platform Requirements

The life cycle of a successful simulation study should follow different steps. Here they are listed per categories.

Following points have to be addressed.

REQ#151) Concerning the objectives, simulations' objectives will define accurately the parameters and variables to take into account as well as the level of evaluation (service, system, component).

REQ#152) Concerning the platform and model description, the different models and the overall objectives of the simulation campaigns shall be clearly identified and communicated (the specific questions to be answered by the simulations, the metrics and performance measures of the model processing, the system configurations to be modeled, the time frame of the simulation campaigns and the required resources).

REQ#153) Concerning technical solutions, all alternative techniques, tools and languages that have been used to perform the simulation shall be identified.

REQ#154) As for the specification model,

REQ#154-A) the conceptual model of the simulation platform shall be formulated with tools, connectors and languages mentioned in it.

REQ#154-B) The conceptual model of the platform shall not exclude the essential elements of the platform and should not include unnecessary details (appropriate level of details).

REQ#154-C) The conceptual model shall be as simple as possible to meet the objectives of the simulation study. Unlike complex models, simple models have many advantages:

- It can be developed faster
- It is more flexible

- It requires less data
- It runs faster
- It is cheaper
- Its simulation results are better understood since the structure of the model is less complex
- The conceptual model should include detailed description of each module, and their interactions above all concerning data exchange and time sampling process
- The simplifying assumptions should be communicated and justified

5.4 Communicative and workflow exchange model:

Concerning the communicative and workflow exchange model:

REQ#155) If there are any errors or omissions, the conceptual model must be updated before processing result of simulation.

REQ#156) The communicative model shall prove that the conceptual model can be developed into a computer model that is sufficiently accurate for the purpose at hand.

5.5 Use Case Requirements:

Program the different use cases under analysis using a language programming or a simulation software

REQ#157) Define use cases that will help for the simulation:

a) Define parameters of the ODD and the OEDR of the system
b) Define constraints that will influence the model
c) Define events that will influence the model

5.6 Simulation Requirements:

The following section focus on the simulation requirements.

REQ#158) Sensitivity analyses shall be performed on the simulated use cases to determine which factors in the model have the greatest impact on the performance measures and therefore should be modeled carefully.

REQ#159) The results of the simulation with the modeled vehicle should be analyzed and it should be decided whether additional experiments (controlled testing or real testing) or another system to be modeled to study an alternative solution to the problem are needed.

REQ#160) The building/validation process of the simulation campaigns, the computer program, and the results/conclusions for the safety analysis should be discussed and documented with rationale and graphic animation if needed.

5.7 Simulation audit requirements

To allow audits on the simulation, the following requirements address the document and proofs needed.

REQ#161) A communicative model shall be addressed in order to represent the conceptual model to tools and data repository of the project team for validation.

REQ#162) the conceptual model shall be approved by the client through a validation process focusing on the following points:

REQ#162-A) Designers and client shall confirm the utility of the conceptual model, ensuring that it is developed into a useful computer model. e.g., as a decision aid in the specific context.

REQ#162-B) Designers and clients shall confirm the feasibility of the conceptual model, ensuring that it can be developed into a computer model with the time, resource and data available.

REQ#162-C) The client shall validate the conceptual model.

6 TESTING IN CONTROLLED ENVIRONMENT REQUIREMENTS

6.1 Introduction

This section provides requirements to define tests in controlled environment. It is based on the WP3 of the PRISSMA project which focus on same theme.

REQ#163) The Technical Service shall ensure that the MV is subject to at least the tests outlined in this section.

REQ#164) The specific test parameters for each test shall be selected by the Technical Service and shall be recorded in the test report in such a manner that allows traceability and repeatability of the test setup.

REQ#165) Pass-and-Fail-Criteria for tests are derived solely from the technical requirements in paragraphs 4 of the Regulation.

REQ#166) Since testing in controlled environment is expensive, test scenarios shall be preset to include all the tests' parameters that needed to be checked.

The test specifications in this document are meant to be a basic set of tests. The technical service authorities may perform any other test within the system boundaries and may then confront the measured results against the requirements.

6.2 Carrying the controlled-environment test requirement

6.2.1. The test conditions

As addressed in the ALKS, §3.1 [13]:

REQ#167) The tests shall be performed under conditions (e.g., environmental, road geometry) that allow the operation of MV (urban shuttle, delivery robot).

REQ#168) If ADS modifications are required in order to allow testing, e.g., road type assessment criteria or road type information (map data), it shall be ensured that these modifications don't have an effect on the test results. These modifications shall in principle be documented and annexed to the test report. The description and the evidence of influence (if any) of these modifications shall be documented and annexed to the test report.

REQ#169) The test surface shall afford at least the adhesion required by the scenario in order to achieve the expected test result.

6.2.2. Test targets

To address the test Targets:

REQ#170) The target used for the vehicle detection tests shall be a regular high-volume series production vehicle of Category M or N or alternatively a "soft target" representative of a vehicle in terms of its identification characteristics applicable to the sensor system of the MV under test according to ISO 19206-3:2018 [21]. The reference point for the location of the vehicle shall be the most rearward point on the centerline of the vehicle.

REQ#171) The target used for the Powered-Two-wheeler tests shall be a test device according to ISO CD 19206-5 [21]or a type approved high volume series production motorcycle of Category L3 with an engine capacity not exceeding 600 cm3. The reference point for the location of the motorcycle shall be the most backward point on the centerline of the motorcycle

REQ#172) The target used for the pedestrian detection tests shall be an “articulated soft target” and be representative of the human attributes applicable to the sensor system of the AEBS under test according to ISO 19206-2:2018 [21].

REQ#173) Details that enable the target(s) to be specifically identified and reproduced shall be recorded in the vehicle type approval documentation.

6.2.3. Test parameters variations

This section addresses the requirements concerning parameters’ variations

REQ#174) Regarding test parameter variation:

a) The manufacturer shall declare the system boundaries to the Technical Service.
b) The Technical Service shall define different combinations of test parameters (e.g., present speed of the MV, type and offset of target, curvature of lane) in order to cover scenarios in which a collision shall be avoided by the system as well as those in which a collision is not expected to be avoided, where applicable.
c) If this is deemed justified, the Technical Service may test additionally any other combination of parameters.
d) If a collision cannot be avoided for some test parameters, the manufacturer shall demonstrate either by documentation or, if possible, by verification/testing that the system doesn’t unreasonably switch its control strategy.

6.2.4. Lane keeping

To address lane keeping:

REQ#175) The test shall demonstrate that the MV does not leave its travel lane and maintains a stable position inside its ego lane across the speed range and different curvatures within its system boundaries.

REQ#176) The test shall be executed at least:

a) With a minimum test duration of 5 minutes;
b) With a passenger car target as well as a PTW target as the lead vehicle / other vehicle;
c) With a lead vehicle swerving in the lane; and
d) With another vehicle driving close beside in the adjacent lane.

6.2.5. Avoiding collision with a road user or an object blocking the lane

Concerning avoiding a collision with a road user or object blocking the lane:

REQ#177) The test shall demonstrate that the MV avoids a collision with a stationary vehicle, road user or fully or partially blocked lane up to the maximum specified speed of the system.

REQ#178) This test shall be executed at least:

a) With a stationary passenger car target;
b) With a stationary powered two-wheeler target;
c) With a stationary pedestrian target;
d) With a pedestrian target crossing the lane with a speed of 5 km/h;
e) With a target representing a blocked lane;
f) With a target partially within the lane;
g) With multiple consecutive obstacles blocking the lane (e.g., in the following order: ego-vehicle -motorcycle – car);
h) On a curved section of road.

6.2.6. Following a lead vehicle

As approach in the §4.3 of the UNR157 [13]:

REQ#179) The test shall demonstrate that the MV is able to maintain and restore the required safety distance to a vehicle in front and is able to avoid a collision with a lead vehicle which decelerates up to its maximum deceleration.

REQ#180) This test shall be executed at least:

a) Across the entire speed range of the MV
b) For a passenger car target as well as a PTW target as lead vehicle, provided standardized PTW targets suitable to safely perform the test are available
c) For constant and varying lead vehicle velocities (e.g., following a realistic speed profile from existing driving database)
d) For straight and curved sections of road
e) For different lateral positions of lead vehicle in the lane
f) With a deceleration of the lead vehicle of at least 6 m/s^2 mean fully developed deceleration until standstill.

6.2.7. Lane change of another vehicle into the lane

Concerning the lane change of another vehicle into lane, as addressed in the §4.4 of the UN157 [13])

REQ#181) The test shall demonstrate that the MV can avoid a collision with a vehicle cutting into the lane of the MV up to a certain criticality of the cut-in maneuver.

REQ#182) The criticality of the cut-in maneuver shall be determined according to TTC_{cut-in}, longitudinal distance between rear-most point of the cutting in vehicle and front-most point of the MV, the lateral velocity of the cutting-in vehicle and the longitudinal movement of the cutting-in vehicle, as defined in paragraph REQ#063) of this regulation.

REQ#183) This test shall be executed taking into consideration at least the following conditions:

a) For different TTC_{cut-in}, distance and relative velocity values of the cut-in maneuver, covering types of cut-in scenarios in which a collision can be avoided and those in which a collision cannot be avoided;
b) For cutting-in vehicles travelling at constant longitudinal speed, accelerating and decelerating;

c) For different lateral velocities, lateral accelerations of the cut-in vehicle;

For passenger car as well as PTW targets as the cutting-in vehicle, provided standardized PTW targets suitable to safely perform the test are available

6.2.8. stationary obstacle after lane change of the lead vehicle

Concerning Testing the stationary obstacle after lane change of the lead vehicle, as assessed in the §4.5 of the UNR157 [13].

REQ#184) The test shall demonstrate that the MV is capable of avoiding a collision with a stationary vehicle, road user or blocked lane that becomes visible after a preceding vehicle avoided a collision by an evasive maneuver.

REQ#185) The test shall be executed at least:

a) With a stationary passenger car target centered in lane
b) With a powered two-wheeler target centered in lane
c) With a stationary pedestrian target centered in lane
d) With a target representing a blocked lane centered in lane
e) With multiple consecutive obstacles blocking the lane (e.g., in the following order: ego-vehicle – lane change vehicle – motorcycle – car)

6.2.9. Field of view test

As assessed in the §4.6 of the UNR157 [13], concerning the field of view test.

REQ#186) The test shall demonstrate that the MV is capable of detecting another road user within the forward detection area up to the declared forward detection range and a vehicle beside within the lateral detection area up to at least the full width of the adjacent lane.

REQ#187) The test for the forward detection range shall be executed at least:

a) When approaching a motorcycle target positioned at the outer edge of each adjacent lane;
b) When approaching a stationary pedestrian target positioned at the outer edge of each adjacent lane;
c) When approaching a stationary motorcycle target positioned within the ego lane;
d) When approaching a stationary pedestrian target positioned within the ego lane.

REQ#188) The test for the lateral detection range shall be executed at least:

a) With a motorcycle target approaching the MV from the left adjacent lane;
b) With a motorcycle target approaching the MV from the right adjacent lane.

REQ#189) Additional other test cases may be assessed if it is deemed justified by the Technical Service. Some of the cases may include (UNR157, §5.3 [13]):

a) Y-split of highway lanes
b) Vehicles entering or exiting the highway
c) Partially blocked ego lane, tunnel
d) Traffic lights
e) Emergency vehicles
f) Construction zones
g) Faded/erased/hidden lane markings

h) Emergency/Service personnel directing traffic
i) Change in road characteristics (no longer divided, pedestrians permitted, roundabout, intersection)
j) Normal traffic flow resumed (i.e., all vehicles moving > 60km/h)”

7 TESTING IN REAL ENVIRONMENT REQUIREMENTS

This paragraph has been built based on the input coming from the WP4 of PRISSMA, as well as other regulation which details real-environment testing.

First and foremost:

REQ#190) The real-world test shall be undertaken once the system has passed all of the other tests outlined in this document and upon completion of a risk assessment by the Technical Service.

7.1 Methodology

The aim of this paragraph is to define the requirements for the methodology to set up a real environment test.

7.1.1. Defining a test route

First step is selecting a route that will be able to encounter most of the scenarios expected when designing the ARTS.

REQ#191) The route and the digital infrastructure of the ARTS shall be analysed

REQ#192) Criterions that show the consistency between the ODD and OEDR shall define the route that validate assumptions

REQ#193) The location and selection of the test route, time-of-day and environmental conditions shall be determined by the Technical Service.

7.1.2. Setting use cases

Second step is to bring out the logical scenarios expected on the route that will help to illustrate the well-behavior of the MVs of the ARTS.

RECC#06) Organize the scenarios by type (crossing, lane change, occluded pedestrian, and so on).

REQ#194) The functional and logical scenarios shall be described and documented following its key frame which allow to characterize each logical scenario with relevant parameters for first scene, intermediate scenes, and final scene (deliverable 4.3, §2 [22])

REQ#195) In real world testing, concrete scenarios are collections of precise situations encountered and are classified into logical scenarios.

Setting up concrete scenarios help setting up the use case of the ARTS on its test route.

7.1.3. Defining pathway sections

To observe the use cases of the ARTS the route should be split in sections.

REQ#196) To define sections on the route, one shall use criterions in the tables of 17 Annex 4: Pathway section selection criteria’s tables from the deliverable 4.3.

The tables shown in 17 Annex 4: Pathway section selection criteria's tables from the deliverable 4.3 present the list of selection criteria for the sections of the pathway. These criteria are the descriptors selected and considered sufficient for the description proposed in deliverable 8.11 [2]. This list isn't exhaustive more criterion could be added.

An example of use of these criterions exists in the deliverable 4.3 Annex 1 [22].

7.1.4. Feedback and validations

The following requirements address how to acquire feedback and validate the test

REQ#197) The test drive shall be recorded and the test vehicle instrumented with non-perturbing equipment. The Technical Service may log, or request logs of any data channels used or generated by the system as deemed necessary for post-test evaluation.

REQ#198) The technical service shall conduct, or shall witness, an assessment of the system, in a fault-free condition, in the presence of traffic (a 'real-world' test).

The purpose of this test is to support the technical service in understanding the functionality of the system in its operating environment and to complement the assessment of the documentation provided under Annex 4 (UNR157 [13]). Together, the assessment of Annex 4 (UNR157 [13]) and the real-world test shall enable the technical service to identify areas of system performance that may require further assessment, either through testing or further review of Annex 4 (UNR157 [13]).

REQ#199) During the real-world assessment, the technical service shall assess at least:

a) Prevention of activation when the ADS is outside of its ODD.
b) No violation of traffic rules.
c) Response to a planned event.
d) Response to an unplanned event.
e) Detection of the presence of other road users within the frontal and lateral detection ranges.
f) Vehicle behavior in response to other road users (following distance, cut-in scenario, cut-out scenario etc.).
g) System override.

8 OTHER REQUIREMENTS

This section contains all the other requirements that might be relevant for the fully automatic urban shuttle and delivery robot.

REQ#200) Concerning ethical problems:

REQ#200-A) one shall acknowledge that, while bringing substantial benefits to individuals and society, AI systems also pose certain risks and may have a negative impact, including impacts which may be difficult to anticipate, identify or measure (e.g., on democracy, the rule of law and distributive justice, or on the human mind itself.) The authorities shall adopt adequate measures to mitigate these risks when appropriate, and proportionately to the magnitude of the risk.

REQ#200-B) AI systems must be transparent, accountable and fair.

REQ#201) To help research one manufacturer shall foster it as well as innovation to help assess AI systems and to further the achievement of the requirements; disseminate results and open questions to the wider public, and systematically train a new generation of experts in AI ethics.

REQ#202) The user and remote operator shall follow an adequate training and be authorized to interact with the vehicle.

REQ#203) Characteristics of the competitive platforms that comply with the formulated objectives shall be investigated for consideration in platform definition and specification.

9 CONCLUSION

Thanks to the regulations, the norms and deliverables from the PRISSMA project a list of requirements and recommendations has been set up.

This list allows any manufacturer to design, audit, simulate and test an ARTS.

However, this non-exhaustive list is only an approach fixed in time. More norms or regulations might be published in the years to come but also current norms and regulations could evolve to include the feedback on the use of ARTS.

10 ACRONYMS

Acronyms	DESCRIPTION
AD	Automated Driving
ASIL	Automotive Safety Integrity Level
CONOPS	Concept of Operations
DDT	Dynamic Driving Task is the control and execution of all longitudinal and lateral movements of the vehicle.
DGA	Directorate General of Armaments
DGCA	Directorate General of Civil Aviation
DSSAD	Data Storage System for Automated Driving enables the determination of interactions between the ALKS and the human driver.
GDPR	General Data Protection Regulation
HA	Hazard Analysis
HIL	Hardware In the Loop
HITL	Human In The Loop
IVVQ	Integration, Verification, Validation and Qualification
KPI	Key Performance Indicators
MC	Main Contractor
MOC	Maintenance in Operational Condition
MIL	Model In the Loop
MRM	Minimum Risk Maneuver
MV	Mobility vector
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
PHA	Preliminary Hazard Analysis
PM/PO	Project Manager/Project Owner
SAE	Society of Automotive Engineers
SMS	Smart Mobility System
TTC	Time to Collision means the value of time obtained by dividing the longitudinal distance (in the direction of travel of the subject vehicle) between the subject vehicle and the target by the longitudinal relative speed of the subject vehicle and the target, at any instant in time
VIL	Vehicle In the Loop
VRU	“Vulnerable Road User secondary safety system” means a deployable vehicle system outside the occupant compartment designed to mitigate injury consequences to vulnerable road users during a collision.
OFFSET	The distance between the vehicles and the respective target’s longitudinal median plane in driving direction, measured on the ground, normalized by the half the vehicle width excluding devices for indirect vision and corrected by adding 50 per cent.
Pedestrian Target	A soft target that represents a pedestrian.
Passenger car Target	A target that represents a passenger car vehicle.

Acronyms	DESCRIPTION
Powered Two-Wheeler Target (PTW)	A target that is a combination of a motorcycle and motorcyclist.

11 FIGURES

12 TABLE LIST

13 REFERENCES

[1] F. F. Philip Koopman, How Many Operational Design Domains, Objects, and Events?, Carnegie Mellon University, 2019.

[2] PRISSMA, Deliverable 8.11, OPERATIONAL DESIGN DOMAIN ,2023

[3] ISO, ISO 34503, Road Vehicles - Test scenarios for automated driving systems - Specification for operational design domain, 2023

[4] A. David, "The levels of automation – The Operational Design Domain", https://www.linkedin.com/pulse/levels-automation-operational-design-domain-part-2-n-david-apelt-1d/, 2019

[5] EU, 32022R1426, Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles, 2022.

[6] SAE, SAE J 3016, surface vehicle recommended practice, 2021.

[7] A. David" The levels of automation – Object and Event Detection and Response (OEDR) and the Game of Thrones",

http://www.linkedin.com/pulse/levels-automation-object-event-detection-response-oedr-david-apelt/, 2019.

[8] Damien Pichereau, Le déploiement européen du véhicule autonome, 2021.

[9] UN/ECE, UN regulation 131, Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking Systems (AEBS), 2014

[10] UN/ECE, UN regulation 152, Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles, 2020

[11] ISO, ISO16290, Space systems - Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment, 2013

[12] United Nations, UN Regulation No. 160, Event Data Recorder, 2021.

[13] United Nations, UN Regulation No. 157, Automated Lane Keeping Systems (ALKS), 2021.

[14] UN/ECE, UN regulation 94, Uniform provisions concerning the approval of vehicles with regard to the protection of the occupants in the event of a frontal collision, 2012

[15] UN/ECE, Addendum 94 - UN regulation 95, Uniform provisions concerning the approval of vehicles with regard to the protection of the occupants in the event of a lateral collision, 2021

[16] UN/ECE, UN regulation 137, Uniform provisions concerning the approval of passenger cars in the event of a frontal collision with focus on the restraint system, 2020

[17] UN/ECE, Addendum 9, UN Regulation 10, Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility, 2014

[18] UN/ECE, UN Regulation 121, Uniform provisions concerning the approval of vehicles with regard to the location and identification of hand controls, tell-tales and indicators, 2016

[19] PRISSMA, deliverable 1.5, TESTS AND AUDIT REQUIREMENTS, 2023

[20] PRISSMA, deliverable 6.6, EVIDENCE TO BE PROVIDED ON THE DEVELOPMENT PROCESS, WITH IDENTIFICATION OF POSSIBLE COVERAGE OF APPROVAL REQUIREMENTS, 2024

[21] ISO, ISO19206-5, Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions - Part 5: Requirements for Powered Two-Wheeler targets, 2018

[22] PRISSMA, Deliverable 4.3, REAL CONDITION TESTS METHODS: INFRASTRUCTURE ANALYSES, PATHWAY SELECTION CRITERIA, 2023

[23] PRISSMA, Deliverable 2.7, METHODOLOGY, PROCEDURES AND

PROTOCOLS FOR EVALUATION OF APPLICATIONS AND VIRTUAL TEST FACILITIES

[22] ISO, ISO 16505, Road vehicles - Ergonomic and performance aspects of Camera Monitor Systems - Requirements and test procedures, 2019

14 ANNEX 1: EDR DATA ELEMENTS AND FORMAT

DATA ELEMENT	CONDITION FOR REQUIREMENT[1]	RECORDING INTERVAL/TIME[2] (RELATIVE TO TIME ZERO)	DATA SAMPLE RATE (SAMPLES PER SECOND)	MINIMUM RANGE	ACCURACY[3]	RESOLUTION	EVENT(S) RECORDED FOR[4]
Delta-V, longitudinal	Mandatory - not required if longitudinal acceleration recorded at ≥500 Hz with sufficient range and resolution to calculate delta-v with required accuracy	0 to 250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	100	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar
Maximum delta-V, longitudinal	Mandatory - not required if longitudinal acceleration recorded at ≥500 Hz	0–300 ms or 0 to End of Event Time plus 30 ms whichever is shorter.	N/A	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar
Time, maximum delta-V, longitudinal	Mandatory - not required if longitudinal acceleration recorded at ≥500 Hz	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A	0–300 ms, or 0-End of Event Time plus 30 ms, whichever is shorter.	±3 ms	2.5 ms.	Planar
Speed, vehicle indicated	Mandatory	-5.0 to 0 sec	2	0 km/h to 250 km/h	±1 km/h	1 km/h.	Planar VRU Rollover
Engine throttle, % full (or accelerator pedal, % full)	Mandatory	-5.0 to 0 sec	2	0 to 100%	±5%	1%	Planar Rollover VRU
Service brake, on/off	Mandatory	-5.0 to 0 sec	2	On or Off	N/A	On or Off.	Planar VRU Rollover
Ignition cycle, crash	Mandatory	-1.0 sec	N/A	0 to 60,000	±1 cycle	1 cycle.	Planar VRU Rollover
Ignition cycle, download	Mandatory	At time of download[5]	N/A	0 to 60,000	±1 cycle	1 cycle.	Planar VRU Rollover
Multi-event crash, number of events	If recorded[6]	Event	N/A	1 or more	N/A	1 or more.	Planar VRU Rollover
Time from event 1 to 2	Mandatory	As needed	N/A	0 to 5.0 sec	±0.1 sec	0.1 sec.	Planar Rollover
Complete file recorded (yes, no)	Mandatory	Following other data	N/A	Yes or No	N/A	Yes or No.	Planar VRU Rollover
Lateral acceleration (post-crash)	If recorded	0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	500	-50 to +50g	+/- 10%	1 g	Planar Rollover
Longitudinal acceleration (post-crash)	If recorded	0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	500	-50 to +50g	+/- 10%	1 g	Planar
Normal acceleration (post-crash)	If recorded	-1.0 to 5.0 sec[7]	10 Hz	-5 g to +5 g	±10%	0.5 g	Rollover
Delta-V, lateral	Mandatory - not required if lateral acceleration recorded at ≥500 Hz and with sufficient range and resolution to calculate delta-v with required accuracy	0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	100	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar
Maximum delta-V, lateral	Mandatory - not required if lateral acceleration recorded at ≥500 Hz	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar
Time maximum delta-V, lateral	Mandatory - not required if lateral acceleration recorded at ≥500 Hz	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A .	0–300 ms, or 0-End of Event Time plus 30 ms, whichever is shorter.	±3 ms	2.5 ms	Planar
Time for maximum delta-V, resultant.	Mandatory - not required if relevant acceleration recorded at ≥500 Hz	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A	0–300 ms, or 0- End of Event Time plus 30ms, whichever is shorter.	±3 ms	2.5 ms.	Planar
Engine rpm	Mandatory	-5.0 to 0 sec	2	0 to 10,000 rpm	±100 rpm[8]	100 rpm.	Planar Rollover
Vehicle roll angle	If recorded	-1.0 up to 5.0 sec[12]	10	-1080 deg to + 1080 deg.	±10%	10 deg.	Rollover
Anti-lock Brake System activity	Mandatory	-5.0 to 0 sec	2	Faulted, Active, Intervening[9]	N/A	Faulted, Active, Intervening	Planar VRU Rollover
Stability control	Mandatory	-5.0 to 0 sec	2	Faulted, On, Off, Intervening	N/A	Faulted, On, Off, Intervening	Planar VRU Rollover

[1] "Mandatory" is subject to the conditions detailed in Section 1.

[2] Pre-crash data and crash data are asynchronous. The sample time accuracy requirement for pre-crash time is -0.1 to 1.0 sec (e.g., T = -1 would need to occur between -1.1 and 0 seconds.)

[3] Accuracy requirement only applies within the range of the physical sensor. If measurements captured by a sensor exceed the design range of the sensor, the reported element shall indicate when the measurement first exceeded the design range of the sensor.

[4] "Planar" includes triggered events where there is a lateral or longitudinal velocity change more than8km/h within a 150ms or less interval. (5.3.1.1, 5.3.1.2 [5]) and “VRU” includes triggered events where a Vulnerable Road User secondary safety system is deployed if installed on the vehicle.

[5] The ignition cycle at the time of download is not required to be recorded at the time of the crash but shall be reported during the download process.

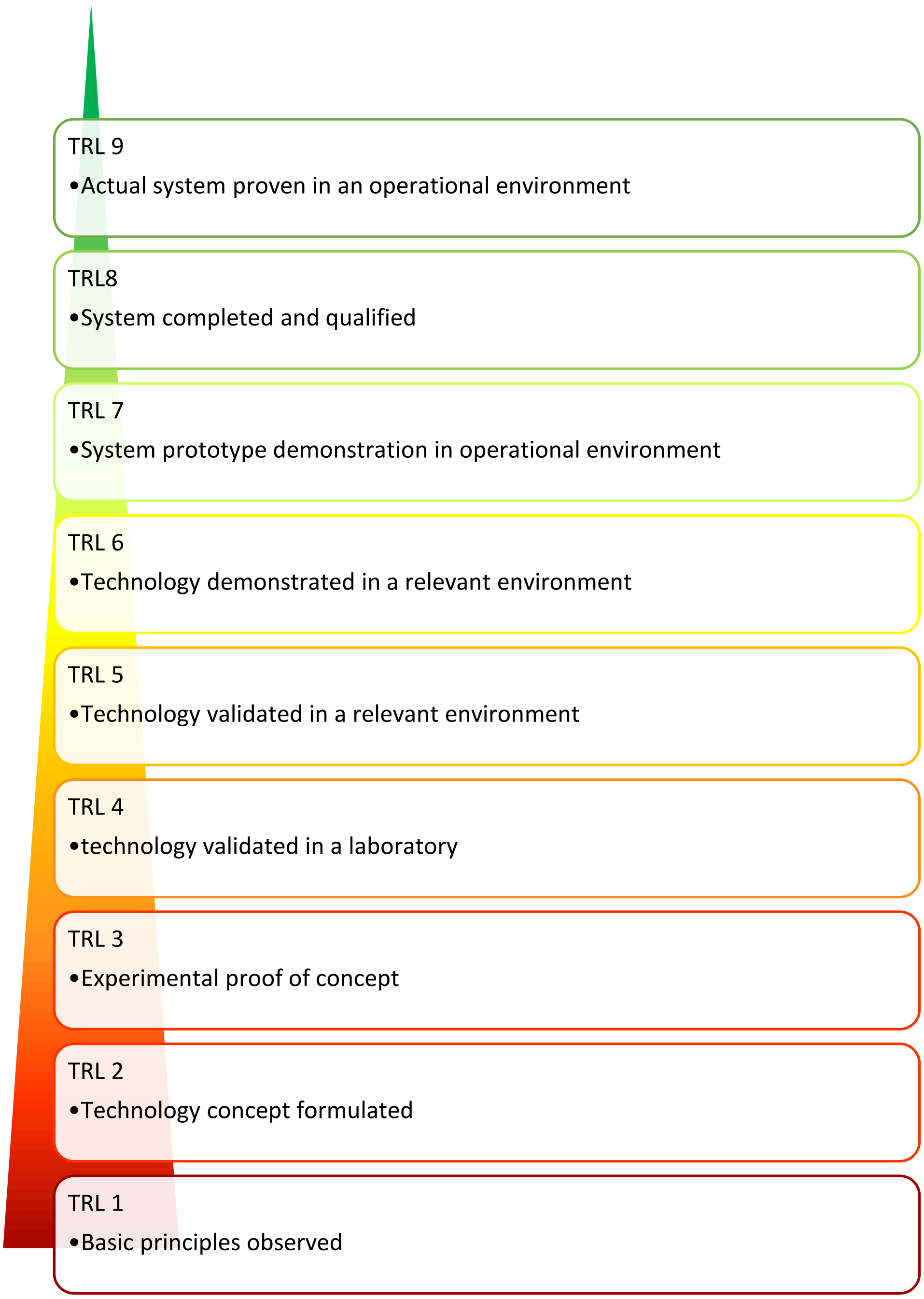
[6] "If recorded" means if the data is recorded in non-volatile memory for the purpose of subsequent downloading.

[7] May be recorded in any time duration; -1.0 to 5.0 sec is suggested

[8] These elements do not need to meet the accuracy and resolution requirements in specified crash tests.

[9] Manufacturers can include other system states

15 ANNEX 2: TRL LEVELS FOR ARTS



TRL 9
- Actual system proven in an operational environment

TRL8
- System completed and qualified

TRL 7
- System prototype demonstration in operational environment

TRL 6
- Technology demonstrated in a relevant environment

TRL 5
- Technology validated in a relevant environment

TRL 4
- technology validated in a laboratory

TRL 3
- Experimental proof of concept

TRL 2
- Technology concept formulated

TRL 1
- Basic principles observed

Figure 12: TRL levels scale based on the ISO16290

16 ANNEX 3: GLOBAL PROCESS FOR EVALUATING A CRITICAL AI-BASED SYSTEM ISSUED FROM THE DELIVERABLE 2.7

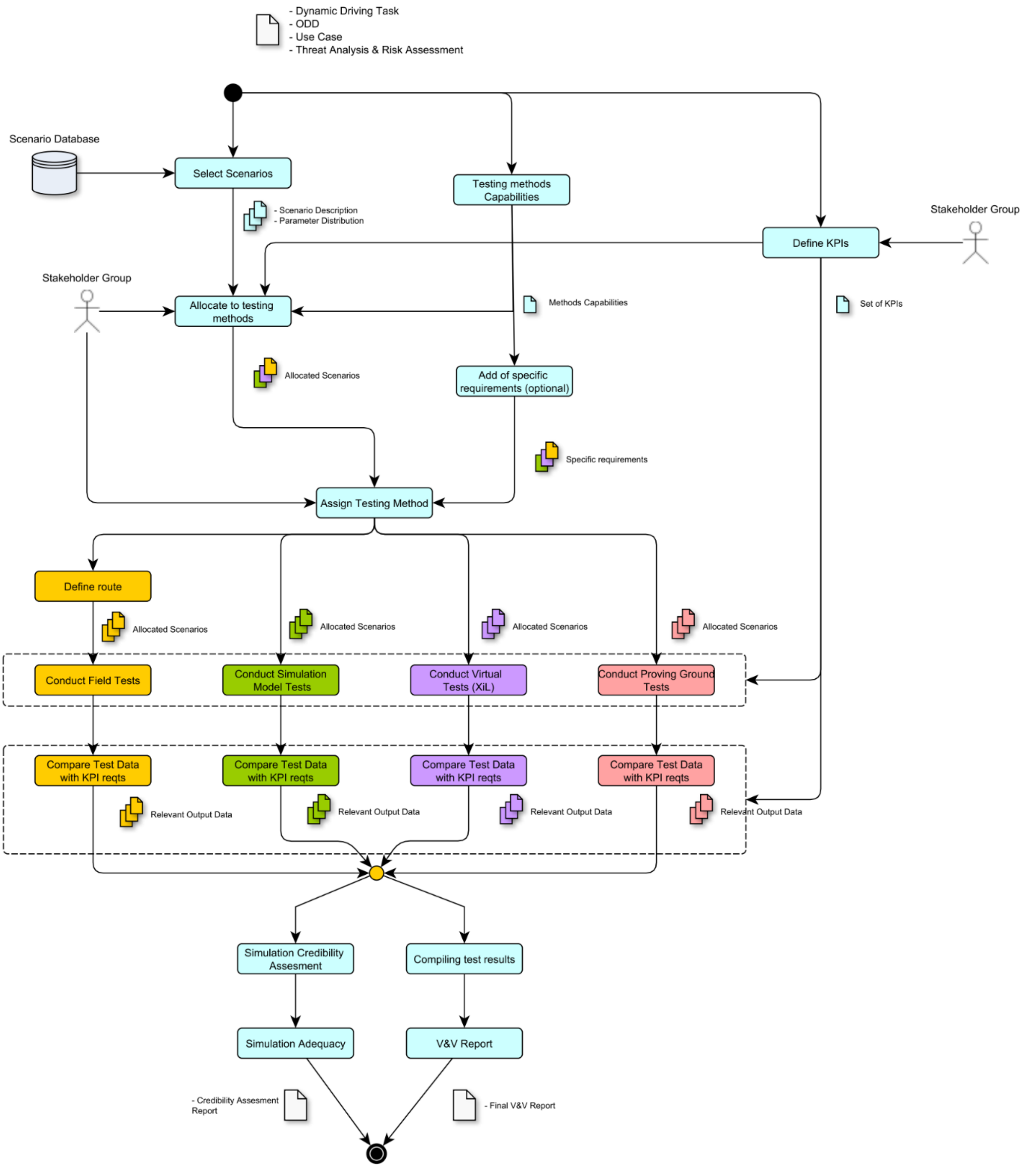


Figure 13: Workflow issued from the deliverable 2.7 [23] (authors: Remi Regnier and Dominique Gruyer)

17 ANNEX 4: PATHWAY SECTION SELECTION CRITERIA'S TABLES FROM THE DELIVERABLE 4.3

Level 1: 1 - PHYSICAL INFRASTRUCTURE

N°	Level 2	Description
1.1	Roadway type	Road layout description
1.2	Roadway edge	Roadside description
1.3	Roadway geometry	Roadway geometrical characteristics
1.4	Junctions	Type of junctions that may be encountered in the area /that may be supported by the vehicle
1.5	Temporary structures	Type of temporary structures that may be encountered in the area and that can be supported by the vehicle (constructions, works, etc.), i.e., movable structures in the area which may impact the vehicle driving task
1.6	Fixed surrounding structures	Fixed structures in the area which may impact the vehicle driving task
1.7	Special structures	Special structure in the area which may impact the vehicle driving task
1.8	Signage	Road signage that may be encountered in the area and that can be supported by the vehicle (traffic signs, traffic lights, etc.)

Level 1: 2 - SCENERY

N°	Level 2	Description
2.1	Specific zones	Corresponds to areas that may have specific speed or mobility restrictions (school, hospital, etc.), or that may lead to specific behaviors and scenarios

Level 1: 3 - ENVIRONMENTAL CONDITIONS

N°	Level 2	Description
3.1	Illumination	

Level 1: 4-TRAFFIC CONDITIONS

N°	Level 2	Description
4.1	Traffic Density	Level of traffic possibly encountered on the road
4.2	Road Users (Speed & type)	Type and speed of the other road users
4.3	Traffic Safety	Any specific behavior of road users that may impact the safety

Level 1: 5-OPERATIONNAL REQUIREMENTS

N°	Level 2	Description
5.1	Ego speed	Link to speed limitation
5.2	Maneuvers type	Any event