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

[L8.3] SUPPORT TO VALIDATION AND APPROVAL

Main authors: M. Douchain and E. Arbaretier (Airbus Protect)

Update: 2023-04-13

Keywords: Autonomous shuttle, Artificial Intelligence, Requirements, Diagnosis, Testing in simulated/controlled/real environments, Validation, Monitoring.

Abstract. This version of the document aims to provide an initial reflection on the essential elements to be taken into account in the validation and approval process of a system implemented on an autonomous vehicle.

Summary. This version of the document aims to conduct an initial reflection on the essential elements to be taken into account in the process of validation and certification of a system implemented on an autonomous vehicle.

TABLE DES MATIÈRES

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ADS
Autonomous Driving System,

AI
Artificial Intelligence,

CAV
Connected and Autonomous Vehicles,

DNN
Deep Neural Network,

FHA
Functional Hazard Analysis,

FMEA
Failure Modes, their Effects and their Analysis,

HIL
Hardware In the Loop,

MIL
Model In the Loop,

M&S toolchain
Modeling and Simulation toolchain,

OD
Operational Domain,

ODD
Operational Design Domain,

OEDR
Object and Event Detection Response,

SOTIF
Safety Of The Intended Fucntion,

VIL
Vehicle In the Loop,

1 Introduction

On every autonomous shuttle, all on-board navigation systems process and generate in real time a mass of data with heterogeneous formats and multiple dimensions. Conventional data processing systems are in constant use and therefore the Artificial Intelligence (AI) algorithms will trigger choices and decisions. These algorithms will determine the behaviours of the autonomous shuttle or vehicle, which must be safe in all dynamic situations encountered on the road and in the operating environment.

Hence in the current context of autonomous vehicles, the approval process is a key subject that should be highly focused on. Indeed, the aim of the present document is to define a support framework that should help the industrial actors to better know the different specifications that must be followed for being sure that the AI function they are building will be validated and approved.

Otherwise, this framework will be used as a standard not only for some common AI functions but will be the focal point of all the AI functions surrounding an AI autonomous vehicle project such as the Rennes Metropole or the Paris2Connect projects (cf. Liv. 4.1) in France.

Therefore, knowing that, we can easily understand how important the choices of the use cases are. An approach by use case or scenario proves to be more realistic and adapted to initiate analyzes at the heart of the data available in the recording system of an autonomous shuttle. Some data are fundamental to diagnose undesirable situations. Other data without direct link to the operations remain in the organizational register of the operator. In any case, all operational data must remain intact and inviolable to allow investigations after an incident, no matter how severe, like the black box of an aircraft or the event recorder of a train. As this post-processing of the operation data is done in deferred mode, a panel of driving situations that have not caused an incident should be analyzed over a period of time in order to refine the feedback and enrich the learning sequences of the images captured by the vehicle. This work will also allow to verify the confidence indices set during the design of the AI algorithms and the vehicle equipment.

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.

Nevertheless, it also aims to follow the evolution constraints of the AI-based developed functions in order to be constantly up to date and relevant.

As a reminder, document 8.3 is part of the Task 8.3 with the following deliverables:

i. Deliverable 8.4 aims to summarize validation principles processes as well as the distribution of the different project actors.
ii. Deliverable 8.5 aspires to be a repository of practices allowing an evolution of a perimeter. Deliverable 7.3 aims to write a process for the controlled update of the elements of the file (including scenarios and tools).
iii. Deliverable 7.4 aims to write a process for the secure deployment of updates.

A list of the documents I mention in the present framework is done in the part “REFERENCES” at the end of the document.

Nota: More documents have been used to create this deliverable. Indeed, they come from the Work Packages 2, 3, 4, 6, 7, and 8.

2 Support elements of the system engineering framework

First of all, it is important to mention that the approval process consists of several successive stages, the main ones being:

i. Examination of the application file (stage 1 audit).
ii. Completion of the initial approval audit (stage 2 audit).
iii. The return on the non-conformity sheets, if necessary.
iv. The study of the audit report by a reading committee which formulates an opinion on the approval.
v. If necessary, the issue of the certificate once the approval decision has been confirmed.

2.1 Audits

Then, we can precise that the audit process is intended to be a system engineering benchmark for suppliers.

Indeed, the company applying for approval must, so that the approval body can draw up the initial approval offer, send it the documentation precisely describing the scope covered by the approval (organisation, teams, workforce) as well as any approvals covering this scope (notably ISO 9001 or ISO 27001). The duration of the approval audit may be reduced in the event of ISO 9001 approval on a management system covering the processes covered by the approval.

Stage 1 Audit:

Upon acceptance of the initial approval offer, the company must send the approval body the documentation relating to the process(es) to be certified. This documentation must describe the design, development, evaluation and maintenance processes in operational conditions covered by the approval. It should include the following:

i. General documents related to the processes to be certified:
   - The declaration of applicability;
   - The definition of the inputs and outputs of the processes to be certified as well as a description of their interfaces;
   - A list of the procedures implemented as part of the processes to be certified;
   - A list of controls and objectives to demonstrate the ability of the certified processes to achieve the expected results;
   - A list of external service providers involved in the certified processes;
   - A criticality analysis of external service providers involved in the processes to be certified;
   - An analysis of the checks carried out.

ii. Documents related to each AI functionality developed as part of the processes to be certified:
   - AI Feature Specifications;
   - Preliminary risk analyses;
   - Characteristics of the areas of use with justification of the relevance of the influencing factors;
   - Lists of contraindications and non-indications;
   - Methods for estimating real distributions of data in learning bases, for example in the context of supervised learning;
   - Lists of rare events integrated into the learning databases as well as their frequency of occurrence and the method used to determine them;
   - Distributions of the cases covered by the test bases;

- Lists of rare events integrated into the test bases as well as their frequency of occurrence and the method used to determine them;
- Methods to ensure the quality of the initial learning process;
- Assessment protocols implemented;
- Detailed risk analyses;
- Descriptions of the mechanisms for controlling the evolution of performance within the framework of the MCO (*Maintien en Condition Opérationnelle* : Integrated Logistics Support);
- Update methods after deployment.

iii. All the documentation made available or communicated to customers (Product sheet in the case of AI functionalities developed for a generic customer).

The audit of stage 1 consists in determining if the audit of conformity of the processes (audit of stage 2) is possible taking into account the degree of completion of the documentation transmitted by the applicant. To do this, it is observed:

i. If the scope of approval is sufficiently precise and unambiguous.
ii. If the exclusions of requirements are duly justified.
iii. If the main documents and procedures required by this standard are present.

This involves determining whether the elements necessary for the operation of the processes in accordance with the reference system are present, and not verifying their application, which is the subject of the stage 2 audit.

At the end of the stage 1 audit, the approval body informs the applicant of the result.

If this step 1 concludes that the file is inadmissible, it is up to the approval applicant to respond to the approval body by providing the missing documents.

An additional offer may in this case be sent by the approval body if a second stage 1 audit is necessary.

Stage 2 Audit (Planning):

If the stage 1 audit is satisfactory, the file is admissible and the organisation contacts the company applying for approval, in order to define the places and dates of the stage 2 audit.

The duration of the stage 2 audit may be increased if it is necessary to travel to several sites, if subcontractors are involved in the design, development, evaluation and maintenance processes of the AI functionalities, covered by the approval, whose mastery is not ensured by the approval candidate and are not certified, or if it is necessary to call on an interpreter.

Stage 2 Audit (Realization):

The company must apply all the requirements of this standard, if they are applicable to its processes. All the points of the reference system and of the reference texts relating to the processes covered by the approval are examined. If the company applying for approval only performs part of the targeted operations (design, development, evaluation, MCO (*Maintien en Condition Opérationnelle*: Integrated Logistics Support)), only the processes related to the activities concerned will be audited and certified and this must be documented in the declaration of applicability. Only certified processes will be mentioned on the certificate. Detailed information concerning the scope of approval, taken from the declaration of applicability, will be included in the appendix to the certificate.

All of the audited paragraphs of the reference system are mentioned in the audit plan.

The stage 2 audit preferably takes place at the approval applicant's, on the site(s) where the design, development, evaluation and maintenance activities of the AI functionalities are carried out.

The approval applicant must ensure the availability of:

i. Interlocutor(s) mastering the processes implemented.
ii. Any other person deemed relevant.
iii. Documented information required by this standard and providing proof that the processes comply with the requirements of this standard.
iv. Documented information to demonstrate the compliance of the developed AI functionalities with the specified requirements.

It is reminded that the audit is based on a sampling of available information. The absence of non-compliance constitutes a presumption of compliance and not proof of compliance with the requirements of the standard.

Otherwise, there are more contents in the document *Referentiel de certification de processus pour l'IA* made by the LNE (cf.). For example, there are responses from non-conformity notes, a review of the audit report, and the reading committee’s decision.

Now, from another point of view, the objective of carrying out audit and evaluation is to assess and demonstrate that:

i. The system designers have implemented the correct processes to ensure the operational and functional safety of the system during its life cycle.
ii. The system design is safe by design and sufficiently validated before its introduction to the market.

This phase is composed of two main components: the audit of the systems designers' processes by a safety management system, the safety assessment of the system design.

You may be required to demonstrate:

i. The robustness of the processes in place to ensure safety during the life cycle of the system (development phase, production, but also operation and dismantling).
ii. Identification of risks and hazards relevant to the system under study and implementation of a “safe by design” concept to mitigate the risks.
iii. Validation of the risk assessment and the “safe by design” concept through testing by the designer to show that the system meets the safety requirements before being placed on the market.

As such, these elements (risk assessment, concept of security by design and validation testing) can be used to demonstrate overall system safety in a much stronger way than a limited number of physical/virtual tests.

The audit phase also includes the implementation of evaluation processes for the operational phase (reporting of accidents, events, new scenarios) in order to allow the entire ecosystem to learn from experience feedback operational.

The objective of the “safety and security by design” audit is to demonstrate that the risks and hazards relevant to the system have been identified and that a coherent concept of safety by design has been put in place to mitigate these risks. It also involves demonstrating that the assessment of risk and safety by design have been validated by the designer through testing; demonstrating, before the entry into service of the vehicle, that the system meets the safety requirements and in particular that the system does not present an unreasonably foreseeable risk for other road users.

Following paragraphs list different possible subjects addressed by these audits.

2.2 V/W Life cycle

V/W Life Cycle framework is essential for organisation of industrial activity as to system engineering process and system validation as well: to describe applied V/W Life Cycle framework as applied in house is an asset for an industrial partner to convince about his ability to validate his systems.

The contribution to the scenario-based safety demonstration enables to verify that an automated road transport system, characterized by a set of specifications resulting from its internal design and validation process, is capable of behaving safely in the driving situations it may encounter in traffic.

Schematically, the scenarios can be used, on the one hand, during the design of the systems and their validation by the designers; on the other hand, in the evaluation of the performance of the systems, once designed. The scenario approach constitutes the basis for defining the "at least equivalent" but also for proving that reasonably foreseeable risks have been taken into account (ISO 26262 and 214481), and that the safety objective has been achieved before marketing or commissioning. This can be represented by a V-cycle scheme such as in the figure below from the DGITM, *Conduite automatisée / Articulation des rôles du conducteur et du système : Approche descriptive à partir d'un panel de scénarios.* [14]

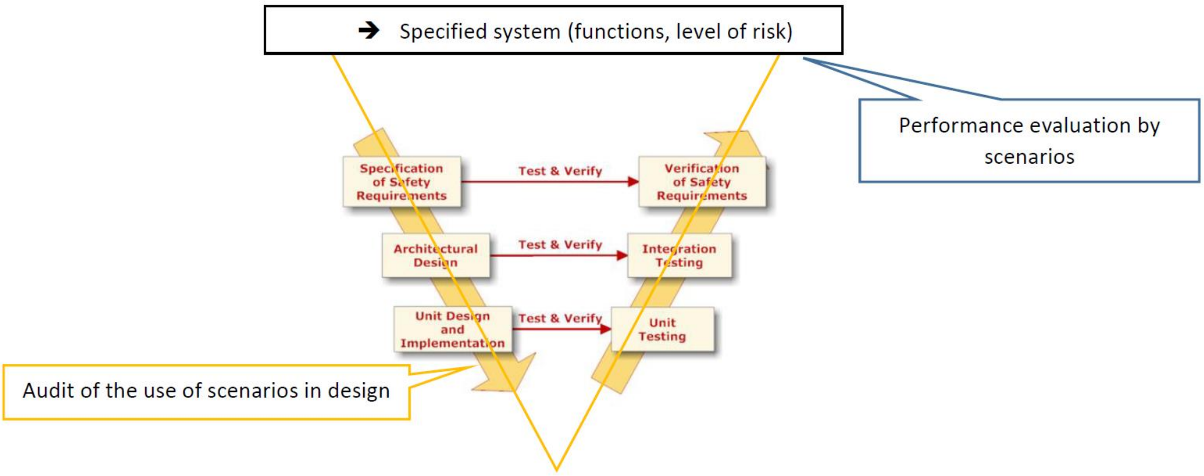

➔ Specified system (functions, level of risk)
Performance evaluation by scenarios
Specification of Safety Requirements
Test & Verify
Verification of Safety Requirements
Architectural Design
Test & Verify
Integration Testing
Unit Design and Implementation
Test & Verify
Unit Testing
Audit of the use of scenarios in design

Figure 1: Performance vision of the driving scenario approach.

Nevertheless, and this diagram reminds us of this, that the two principles introduced must be clearly dissociated:

i. The demonstration of functional safety which deals with the SOTIF,
ii. And the demonstration of safety which deals with safe behaviour in response to malfunctions.

The SOTIF-based functional safety demonstration introduces the notion of scenarios, which is essentially applicable in this framework.

Now, if we focus more on virtual testing, evaluation, validation, and approval, it enters a specific design plan adapted from the V-cycle, which is the reference to present the design life cycle of a product such as an ADAS or an ADS.

Below is a figure from the BPI France for the PRISSMA project, *Liv 2.8: Proofs-Of-Concept intermediate report development of platforms meeting the desired objectives of evaluating means of automated mobility*, 2022. [34]

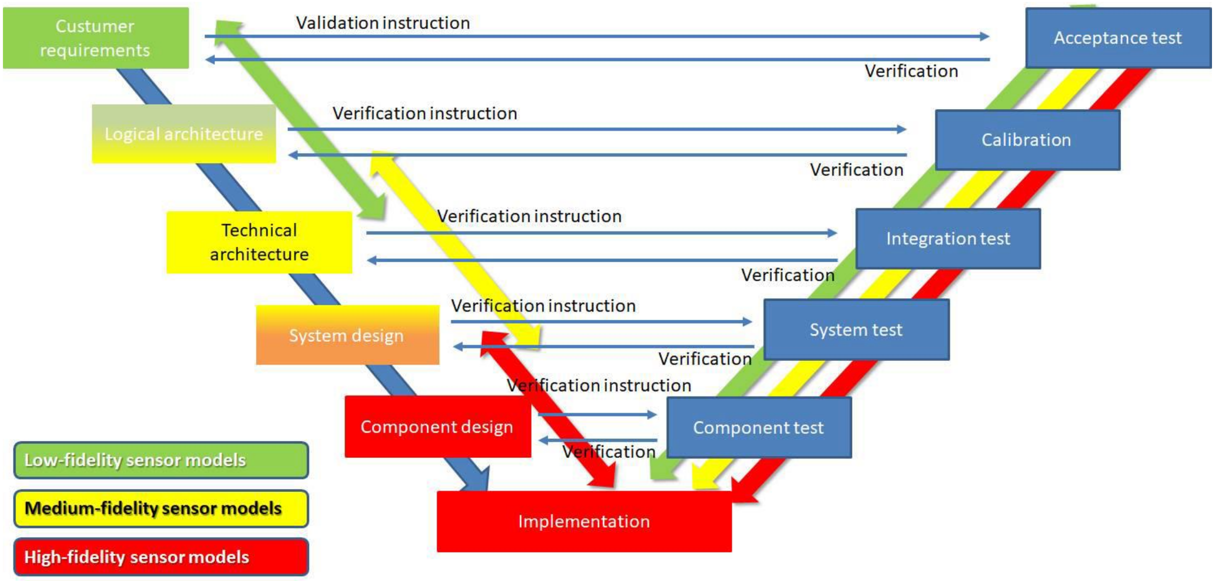


Figure 2: V-cycle for virtual prototyping, test, evaluation, and validation.

Indeed, virtual testing is introduced to reduce the burden of physical tests and effectively provides evidence on the AI performance across the operational domain of a CAV (Connected Autonomous Vehicle).The validation stream is always related to the specification stream, meaning that validation plans are designed concerning the specifications.

However, specifying and validating complex systems of systems such as a CAV is a challenging process. To operate validation plans showing a suitable level of safety and reliability with an acceptable time and budget, virtual method tests from MIL (Model-In-The-Loop) to VIL (Vehicle-In-The-Loop) now supplement physical testing: closed site tests and open road tests.

The validation phases go from the component tests to the functional test of the full system in its ODD. At the end of a CAV or an ADAS validation process, and homologation usually rely on physical tests. However, simulation results are included in the list of elements that can contribute to the safety demonstration for the authorization of a Highly Automated Vehicle to be operated on its ODD.

To demonstrate feasibility on the use of simulation tools for testing AI-based systems related to CAV within the PRISSMA project, four different POC have been proposed so far. It indicate different groups of partners that have been composed to work on specific systems and simulation environments. It also summarize the type of AI algorithm present in the system being tested with the simulation tools, as well as the equivalent physical site where physical tests may be conducted in other work packages of the PRISSMA project.

However, some AI bricks can see their performance managed in W cycle process:

i. So far, no standard RAMS performance (Reliability, Availability, Maintainability, and Safety) can naturally be defined for an AI software.
ii. From an academic point of view, the following performances are applicable and are subject to current R&T projects working about computation theories, methods and technics:
    - Relevancy performance: False Positive percentage (FP), False Negative percentage (FN) and combinations of these rates;
    - Steadiness: Ability of the brick to behave continuously depending on the input variations without incoherent behaviour;

- Resilience: Ability to keep a correct behaviour when input are unsteady or slightly beyond applicability domain regarding the input;
- Robustness: Ability to stabilize treatment process if data slightly overpass domain of validity.
- Explainability: Ability to explain and justify logically behaviour of the brick depending on the input;
- Interpretability: Ability to understand and interpret behaviour of the brick depending on the input with a human point of view;
- Coverage Rate: percentage of use cases “well covered” given a framework of reference scenarios…
- For many of these KPIs, very sophisticated mathematical methods may be used such as Topological Data Analysis, Abstract Interpretation, Adversarial Attacks…

Let's notice that System Engineering process of AI softwares rather refers to a W shaped process than a V shaped process as is illustrated by the following figure from the BPI France for the PRISSMA project, *Liv. 8.14: Report on the impact of AI in system engineering choices*, 2022. [12]

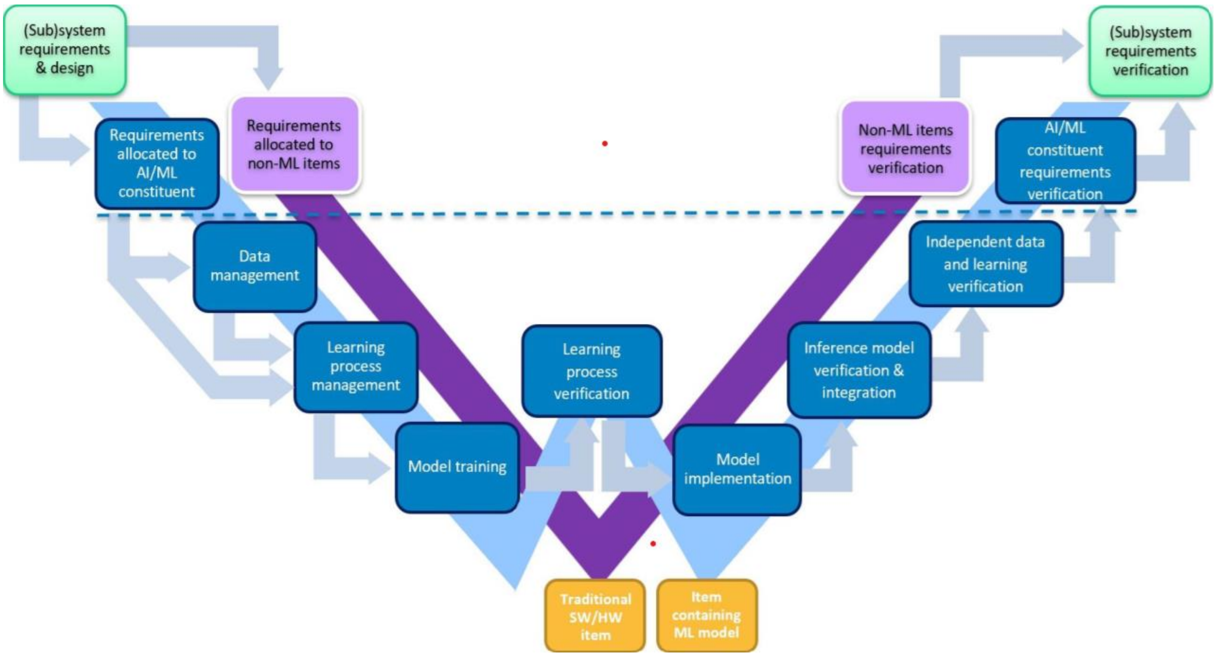

(Sub)system requirements & design
Requirements allocated to AI/ML constituent
Requirements allocated to non-ML items
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
AI/ML constituent requirements verification
Non-ML items requirements verification
(Sub)system requirements verification
Traditional SW/HW item
Item containing ML model

Figure 3: Development Process cycle of AI applications.

In Top-Down front end analysis phases, Validation & Verification Tools have to assess completeness and representativeness of Data Set.

In the meanwhile, methods and tools for quantification and generalization guarantees have to be provided concerning Machine Learning and Deep Learning applications, if AI softwares under analysis refer to these technics.

In the Bottom-Up phase, Methods and Tools for the verification of ML algorithm and model robustness and stability have to be deployed.

2.3 Requirements definition process

Based on the *WP6- Progress meeting 05/01/2023* presentation made by BPI France for the PRISSMA project (cf. [2]), here are some general requirements that the system should follow:

i. Context of AI integration in system engineering development process.
ii. System Architecture: SMS / Mobility Vector (Bus Shuttle or Logistic Droid) addressed.
iii. Operational Concept: CONOPS files associated, reports, separated homogeneous zone demonstration…).
iv. ODD: stakeholder has to describe ODD applicable to system under analysis.
v. OEDR: safety oriented use cases for OEDR patterns.
vi. Testing global strategy: virtual, controlled, real; how are they related?

Testing in simulated environment:

- Simulation strategy : MIL/HIL/VIL;
- Platform requirements / co-simulation workbench: possibility of subcontracting access to simulation assets;
- Scenario requirements: 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?
- Scenario processing trace: choice of metrics and justification of this choice as to Safety…

Testing in controlled environment:

- Test Plan and justification: subcontracting, on what trajectory?
- Test Cases and justification: consistency with simulation cases in complement or in confirmation process…
- Test Control methodology: how the environment is taken into account;
- Test processing methods: metrics, KPIs, calibration, validation;
- Relationship with simulation cases.

Testing in real environment:

- Test Plan and justification: subcontracting, on what trajectory?
- Test Cases and justification: consistency with simulation cases in complement or in confirmation process…
- Test Control methodology: how the environment is taken into account;
- Test processing methods: metrics, KPIs, calibration, validation;
- Relationship with controlled testing cases and simulation cases.

Other requirements:

- PHA requirements;
- Other theoretical demonstration means offered by RAMS / Risk Management can also be addressed;
- Fault trees;
- Reliability Diagrams;
- Markov Chains;
- …

NOTE: Relevancy of applicability and technical benefit has to be justified

Apart from this, about the management system some other requirements are:

i. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

ii. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating.

iii. Identification of the risks and determine appropriate mitigation measures, and to validate that the system runs consistently for the intended purpose.

Below are figures from the UTAC, *Vision du contexte réglementaire et des activités prenant en compte l'impact de l'IA sur la validation des véhicules automatisés*, chez *L'IA pour les nouvelles mobilités*, 21 & 22 Septembre 2022. [3]

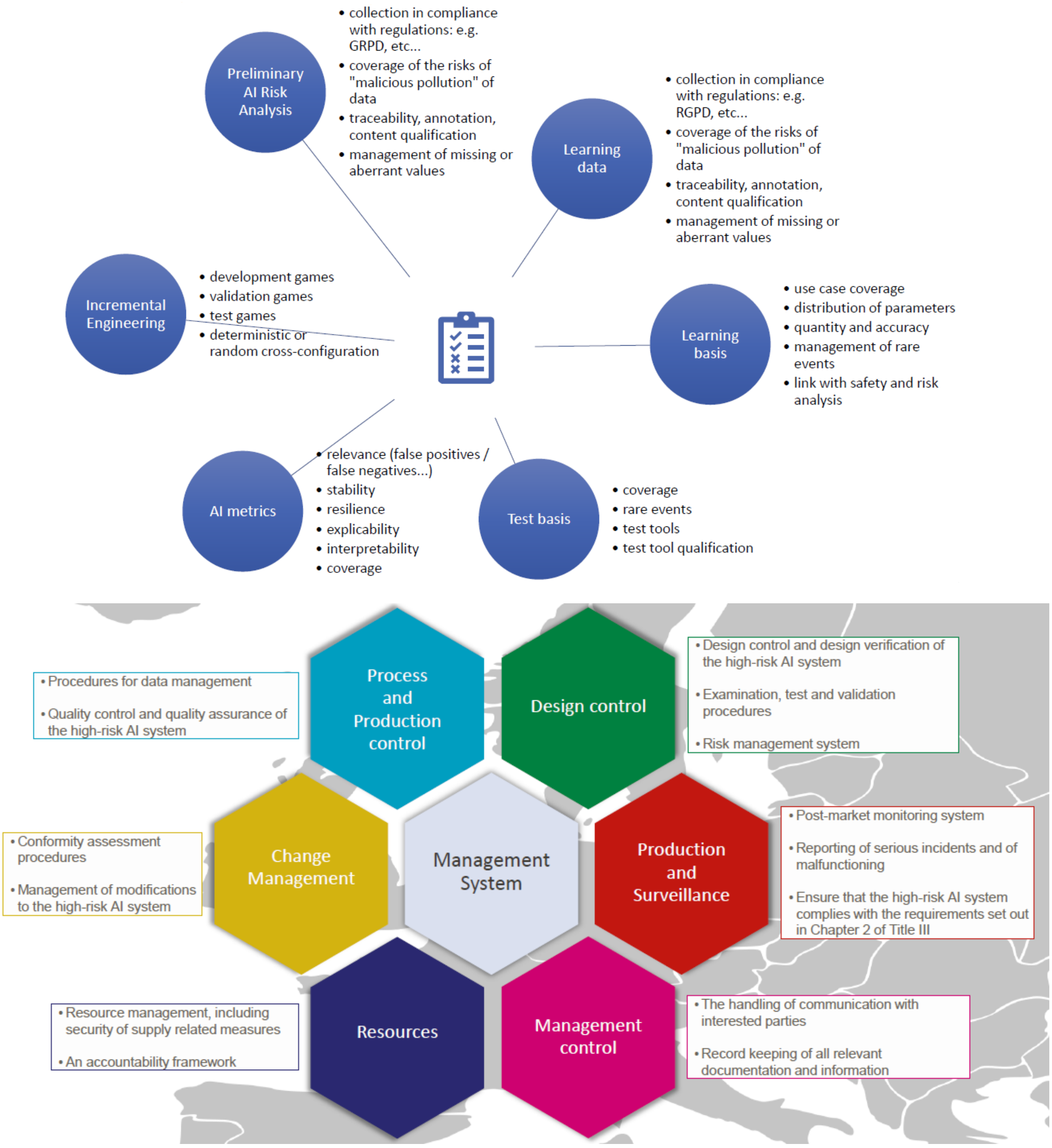

Preliminary AI Risk Analysis
• collection in compliance with regulations: e.g. GRPD, etc...
• coverage of the risks of "malicious pollution" of data
• traceability, annotation, content qualification
• management of missing or aberrant values
Learning data
• collection in compliance with regulations: e.g. RGPD, etc...
• coverage of the risks of "malicious pollution" of data
• traceability, annotation, content qualification
• management of missing or aberrant values
Incremental Engineering
• development games
• validation games
• test games
• deterministic or random cross-configuration
Learning basis
• use case coverage
• distribution of parameters
• quantity and accuracy
• management of rare events
• link with safety and risk analysis
AI metrics
• relevance (false positives / false negatives...)
• stability
• resilience
• explicability
• interpretability
• coverage
Test basis
• coverage
• rare events
• test tools
• test tool qualification
Process and Production control
• Procedures for data management
• Quality control and quality assurance of the high-risk AI system
Design control
• Design control and design verification of the high-risk AI system
• Examination, test and validation procedures
• Risk management system
Change Management
• Conformity assessment procedures
• Management of modifications to the high-risk AI system
Management System
Production and Surveillance
• Post-market monitoring system
• Reporting of serious incidents and of malfunctioning
• Ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of Title III
Resources
• Resource management, including security of supply related measures
• An accountability framework
Management control
• The handling of communication with interested parties
• Record keeping of all relevant documentation and information

Figure 4: Schemes of the entities which surround the Management System brick.

2.4 Architecture definition process

Regarding previous PRISSMA deliverables, the architecture of the AD system is out of scope of the PRISSMA project. The architecture under concern is the architecture of the test system: which components can be used to meet the test system requirements.

Nevertheless "architecture description format" is the corner stone of system engineering validation support for a system under development: it will be submitted to configuration management during the whole life cycle.

Moreover, based on the SOTIF process, it is required to elicit the triggering conditions of potential hazardous behaviours of the autonomous system which will be based on this architecture representation. This elicitation has to be made during the process of defining an autonomous driving system (so before the process of defining the vehicles and therefore before the processes that define the technology of the sensors and AI components that will realize the autonomous driving system). The architecture process is the appropriate process to tackle this discovery:

i. It is part of the definition of the autonomous driving system.
ii. But has to consider the technologies involved by its components which together are the solution to the need expressed for the autonomous driving system.
iii. The interfaces components (sensors) shall be extensively specified in this process, as any interface of any components of the system must be fully described during the architecture process to ensure successful integration.
iv. The inner components (AI) cannot be specified during this process, since they belong to the solution of the ADS components, and will be fully specified during the definition of these components. Instead, the constraints in the selection of such components shall be expressed during this step.

NOTE: The technologies of AI and sensors shall be specified during the architecture process of the ADS to enable the elicitation of triggering conditions of the autonomous driving system.

2.5 Design definition process

Description of a virtuous design process is an important asset of efficiency provided by an industrial stake holder.

For the design definition process, the input and output elements to be documented are at least:

i. For the elements input:
   - Customer requirements and expectations for AI functionality;
   - Applicable regulatory requirements;
   - Requirements arising from similar activities and/or uses (standards, rules of the art, feedback).

ii. For output items:
   - AI feature specifications;
   - The requirements concerning the associated documentation;
   - Communication needs with the client and users;
   - A preliminary risk analysis.

In addition to global description of design process, following requirements referring to it can be documented to complete and develop how this design process is developed through scientifical and technical studies, engineering tasks and so on, especially when integration of AI bricks may make it more complex and sophisticated:

I. The company must define the specifications relating to the AI functionality, document them and justify the acceptability criteria for each of the requirements thus defined. These elements must be communicated to the customer in the manner provided. The definition of the specifications must in particular consider the requirements possibly not formulated by the customers and cover the specifications:

- Use of the system as a whole;
- Use of the AI functionality (the automated task and its purpose must be specified);
- Documentation;
- Communication with the client (on the origin and composition of the training databases, the results of the evaluations, the explainability and interpretability of the functionality, the suggested post-processing, the expected performance and possible constraints on certain hardware resources, possible constraints related to the quality and maintenance of the sensors, whether or not it is open-source, modifications made to the AI functionality after deployment, the methods of subcontracting, on the management of negative impacts potential, etc.);
- Input data:
    - Types, formats and the compatibility of these formats with other solutions or environments (if interoperability is an issue for the customer),
    - Source/Acquisition Mode used by the AI functionality (if the source depends on the use cases, it must be specified for each use case),
    - Frequency and power flow for each data type,
    - Presence and nature of critical attributes.

- Output data:
    - Types, formats and the compatibility of these formats with other solutions or environments (if interoperability is an issue for the customer),
    - Frequency and output flux.

- From domain of use;
- Learning (especially in the case where relearning is possible after deployment);
- Levels of autonomy (human actions and controls on automated tasks);
- Performance, where applicable in terms of:
    - Precision,
    - Reliability,
    - Learning execution time / automated task execution time on target hardware,
    - Resilience to attacks and outliers,
    - Reproducibility.

- Privacy:
    - Respect for privacy,
    - Data Access.

- Transparency, where applicable in terms of:
    - Explainability and interpretability (including required elements and their retention period),
    - Traceability, auditability of learning and/or results.

- Diversity, non-discrimination and equity;
- Impact societal and environmental;
- Maintenance after delivery;
- Regulatory;

- Normative;
- Related to feedback;
- Deemed necessary by the feature developer;
- Related to interested parties deemed relevant;
- Related to the potential consequences of failure of AI functionality.

II. AI functionality specifications should be made available to anyone involved in the design, development, evaluation, or operational maintenance of the AI functionality.

III. In the context of a customer/supplier relationship (BtoB), these requirements and the acceptability criteria must be established in conjunction with the customer and the company must, before launching the development of the functionality, verify and validate the requirements previously mentioned in order to ensure that it is able to respond to them.

IV. Design assumptions made on AI functionality (including statistical assumptions that may vary over time) and the approach taken for model type selection and AI functionality assessment should be documented. If the assumptions or requirements for the AI functionality change, the business must ensure:
   - That an impact analysis is carried out to ensure that the modifications do not have a negative impact on the conformity of the requirements relating to the AI functionality;
   - Correct information of the people involved in the certified processes.

V. A preliminary risk analysis at the relevant development phase adapted to the use of the AI functionality must make it possible to identify, assess and document the risks associated with its use and their potential impacts. This analysis must foresee the case of use of erroneous data which may be due to faulty sensors, formatting errors, bugs in the data management system or cyberattacks and relate to the components and sub-components as well as to the interfaces between components of the AI functionality. The different failure modes of the AI functionality and their consequences must be established in order to allow the user to be aware of the residual risks to which he is exposed and that he accepts.

   The input and output elements to be documented are at least:
   i. For input items:
      - The defined specifications,
      - Preliminary risk analysis,
      - Documentation needs related to AI functionality.

   ii. For output items:
      - The AI functionality whose field of use, uses and performance will be evaluated,
      - The associated documentation (user manual, model description, etc.).

VI. The type(s) of algorithms as well as the type of learning used by the AI functionality must be documented with regard to the constraints of performance, maintenance and explainability.

VII. The possible constraints of the hardware resources on which the learning of the AI functionality can be carried out must be documented.

VIII. If the feature is deployed on the customer's infrastructure, the infrastructure (hardware, operating system and software), deployment types (public or private cloud, on premise, etc.)

supported by the AI feature and reliance on underlying AI technologies must be documented and communicated to the customer as provided.

IX. The interfaces necessary for the use of the AI functionality must be documented and communicated to the client in the manner provided.

X. Characteristics of the intended area of use, including those that influence the performance of the AI functionality, should be documented. For each influencing factor analysed, the justification of its relevance or its exclusion with respect to the area of use must be documented and communicated to the customer in the manner provided.

XI. Contraindications must be documented and communicated to the client in the manner provided.

XII. Known non-indications must be documented and communicated to the client in the manner provided.

XIII. The overall architecture of the source code of the project as well as the network architecture underlying the AI functionality and in particular the input and output flows must be documented. The network architecture and the input/output flows must be communicated to the customer according to the terms provided.

2.6 System analysis process

System analysis process is the heart of IVVQ and global dynamic and iterative is always difficult to figure out to be able to express its density and added value. We chose to select some graphical schemas which provide better understanding about dynamic achievement and contribution of these analysis processes.

Therefore, for that part, based on the summary of the *L'IA pour les nouvelles mobilités* conference done by UTAC (cf. [3]), we will simply represent the system process through two complete schemes illustrating two phases:

About the design:

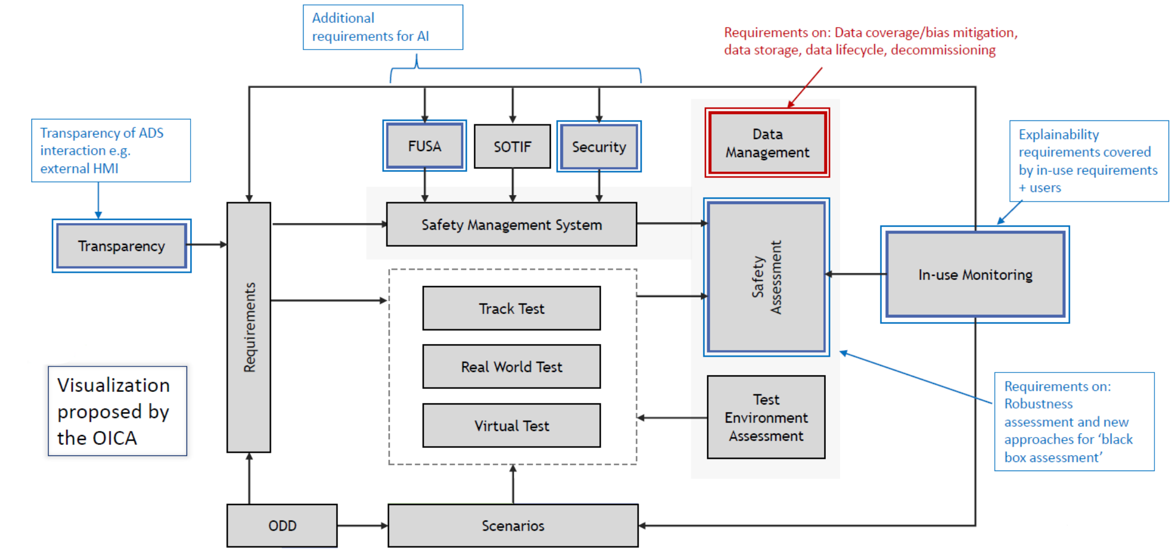

Additional requirements for AI
Requirements on: Data coverage/bias mitigation, data storage, data lifecycle, decommissioning
Transparency of ADS interaction e.g. external HMI
FUSA
SOTIF
Security
Data Management
Explainability requirements covered by in-use requirements + users
Transparency
Requirements
Safety Management System
Safety Assessment
In-use Monitoring
Track Test
Real World Test
Virtual Test
Test Environment Assessment
Visualization proposed by the OICA
Requirements on: Robustness assessment and new approaches for 'black box assessment'
ODD
Scenarios

Figure 5: Impact of AI.

About the life cycle:

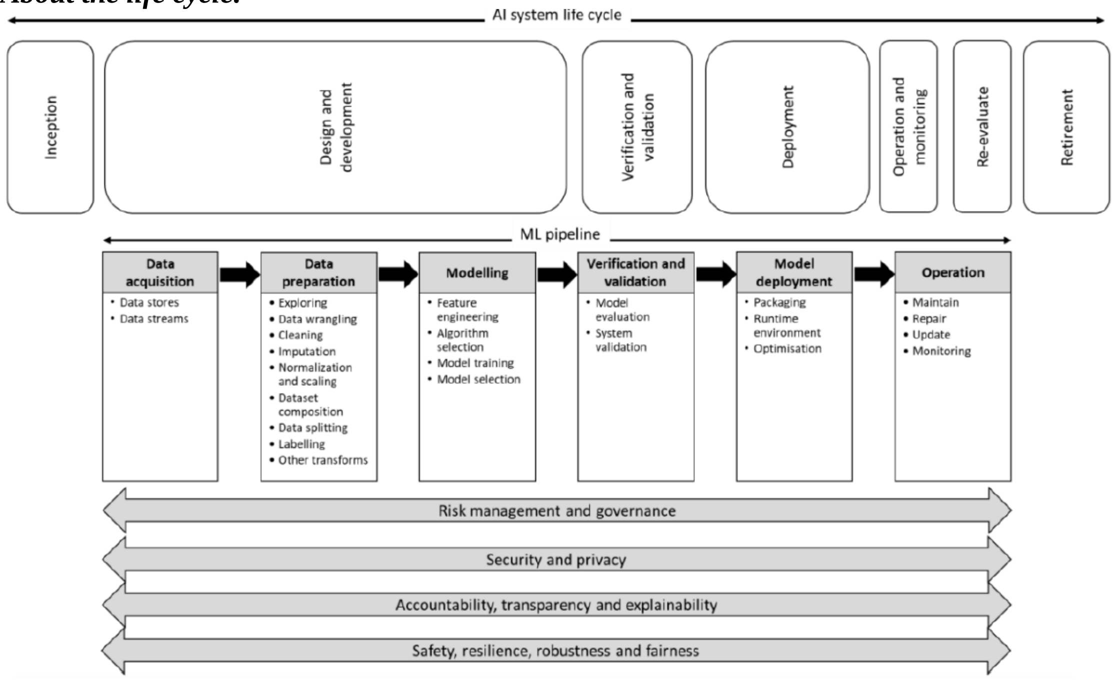


Figure 6: AI system lifecycle.

2.7 Preliminary Hazard Analysis and Hazard Analysis

First, it is not possible to deal with system IVVQ process, without focusing about evidences from industrial stakeholder about having achieved a PHA approach: this is a common initialization of Risk Analysis and Management, Safety Analysis, and especially concerning dreaded event identification and characterization.

It is useful to visualize how the Preliminary Hazard Analysis has been taken into account through the system lifecycle using a figure from the BPI France for the PRISSMA project, *Liv. 6.2: State Of The Art risk assessment and certification for AI: Intermediate report*, 2022. [11]

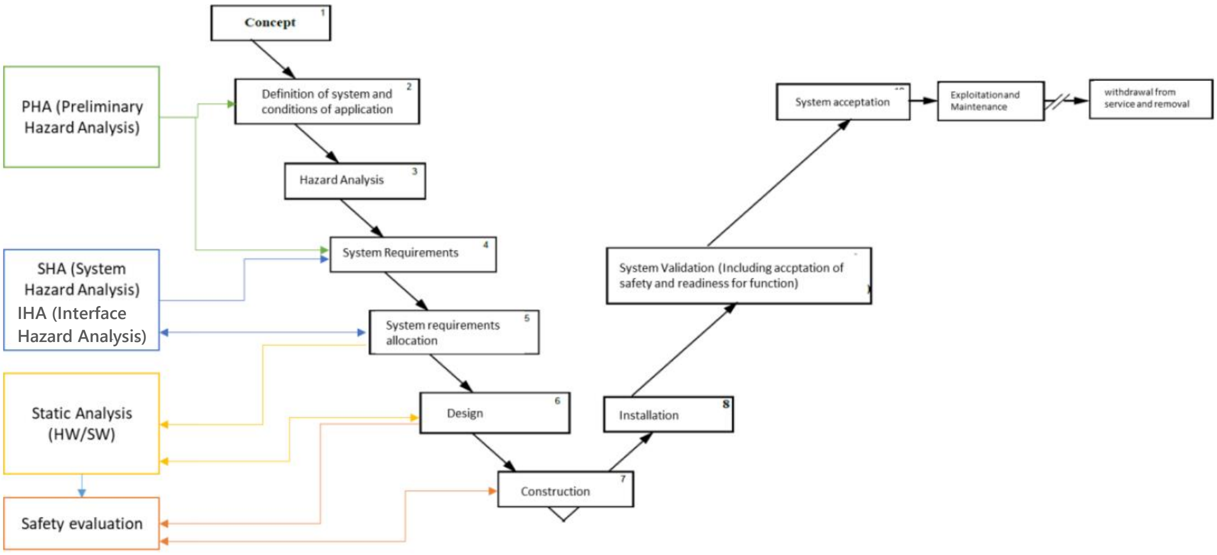

Concept 1
Definition of system and conditions of application 2
Hazard Analysis 3
System Requirements 4
System requirements allocation 5
Design 6
Construction 7
Installation 8
System Validation (Including accptation of safety and readiness for function)
System acceptation
Exploitationand Maintenance
withdrawal from service and removal
PHA (Preliminary Hazard Analysis)
SHA (System Hazard Analysis)
IHA (Interface Hazard Analysis)
Static Analysis (HW/SW)
Safety evaluation

Figure 7: Articulation of a lifecycle system.

Then, about the safety analysis, it is necessary to show how it has been carried out by specialist teams which are independent from design teams. The global safety process is unfolded through 5 principle phases:

i. A definition of system that identifies whether the change is impacting safety.
ii. A Preliminary Risk or Hazard Analysis.
iii. Acceptance of risk following a non-regressive approach.
iv. Definition of safety requirements.
v. Demonstration of compliance with these requirements by the follow ups and tests.

Preliminary Risk Analysis (PRA) / Preliminary Hazard Analysis (PHA) can be either per-formed according to deductive approach going from failures events to digging in the causes or inductive with identifying causes and their consequences.

The deductive approach allows:

i. Identification of the risks.
ii. Allocation of safety requirements (occurrence rate linked to criticality).
iii. Mitigation of risks.
iv. Building of the Register of Dangerous Situations (RSD).
v. Confrontation of analysis results with safety objectives.

The inductive approach allows, stemming from the general serious dangers in rail classified by time (phase) and space (station, in transit, within the train our out of train, etc.) to reach to reasons that could cause them and define coverage characteristics by sub-systems.

FHA is the first step of Safety analysis. Following these steps one can define safety targets to meet for each function.

i. Identify all functions.
ii. List failure Modes.
iii. Consequences of each failure mode.
iv. Associate a criticality level to each effect.
v. Allocate mitigations to reduce the criticality to an acceptable level.

Now, by a more concrete way, about the scenarios from risk analysis studies:

i. Dangerous scenarios are taken from risk analysis linked to the system studied, in order to define safety concepts necessary to cover all reasonably foreseeable risks with regard to the intended use (preliminary danger analysis, preliminary risk analysis and route safety analysis, threats and attacks ...).

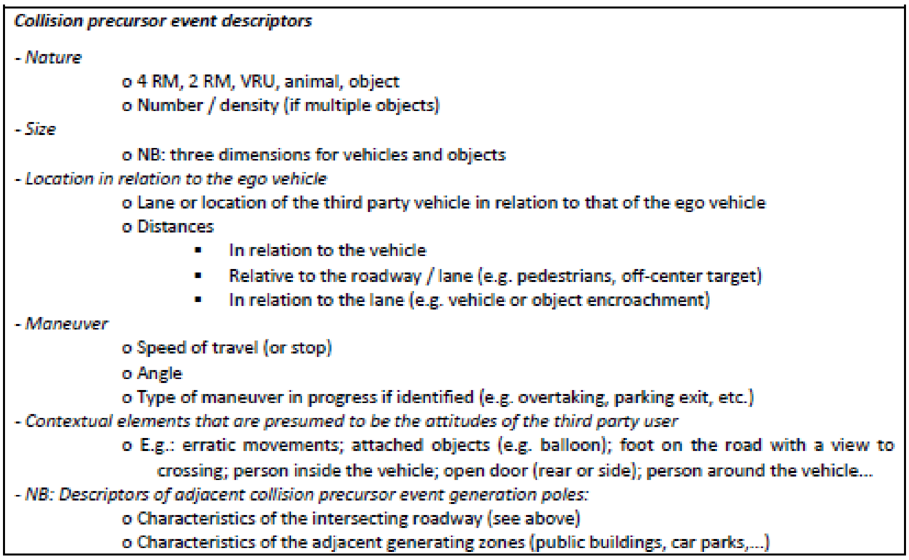
ii. Covering scenarios are necessary elements that permits to define safety concepts, notably by combining deductive and inductive approaches aimed at favoring the exhaustiveness of risk identification. A safety concept defined for a "covering scenario" can make it possible to cover the risk associated with several nominal scenarios, or several accident or "black swans / edge cases" scenarios. Safety concepts defined on the basis of "covering scenarios" shall cover all the risks of dysfunctional causes (failure and SOTIF functional insufficiencies).

In addition to the inductive (Preliminary Risk Analysis) and deductive (Preliminary Hazard Analysis) methods, the French autonomous road transport system (ARTS) ecosystem recommends carrying out a safety analysis of the route at the autonomous road transport system (ARTS) level or ODD /OEDR at the automated driving system level, to exhaustively identify new potentially dangerous scenarios particularly linked to a driving context. The safety analysis of the route or the ODD which allows possible new scenarios of dangerous situations linked to the particularities of the route (i.e. the specific characteristics of the route which generate or amplify the possibility of accidents, or which require a particular response of the system).

This theoretical study is supplemented by driving in the selected operational context, making it possible to validate it and make it robust if necessary when new rare scenarios, until then unknown are detected and analyzed.

It should be noted that dangerous situations and safety requirements specified in safety analyzes can be linked to the scenarios concerned.

Below is a figure from the DGITM/SAGS/EP, *Safety demonstration of automated road transport systems (ARTS): Excepted contributions of the driving scenarios*, 2022. [15]



Collision precursor event descriptors

- *Nature*
    - o 4 RM, 2 RM, VRU, animal, object
    - o Number / density (if multiple objects)
- *Size*
    - o NB: three dimensions for vehicles and objects
- *Location in relation to the ego vehicle*
    - o Lane or location of the third party vehicle in relation to that of the ego vehicle
    - o Distances
        - ▪ In relation to the vehicle
        - ▪ Relative to the roadway / lane (e.g. pedestrians, off-center target)
        - ▪ In relation to the lane (e.g. vehicle or object encroachment)
- *Maneuver*
    - o Speed of travel (or stop)
    - o Angle
    - o Type of maneuver in progress if identified (e.g. overtaking, parking exit, etc.)
- *Contextual elements that are presumed to be the attitudes of the third party user*
    - o E.g.: erratic movements; attached objects (e.g. balloon); foot on the road with a view to crossing; person inside the vehicle; open door (rear or side); person around the vehicle...
- *NB: Descriptors of adjacent collision precursor event generation poles:*
    - o Characteristics of the intersecting roadway (see above)
    - o Characteristics of the adjacent generating zones (public buildings, car parks,...)

Figure 8: Collision precursor event descriptors.

The hazards consist of:

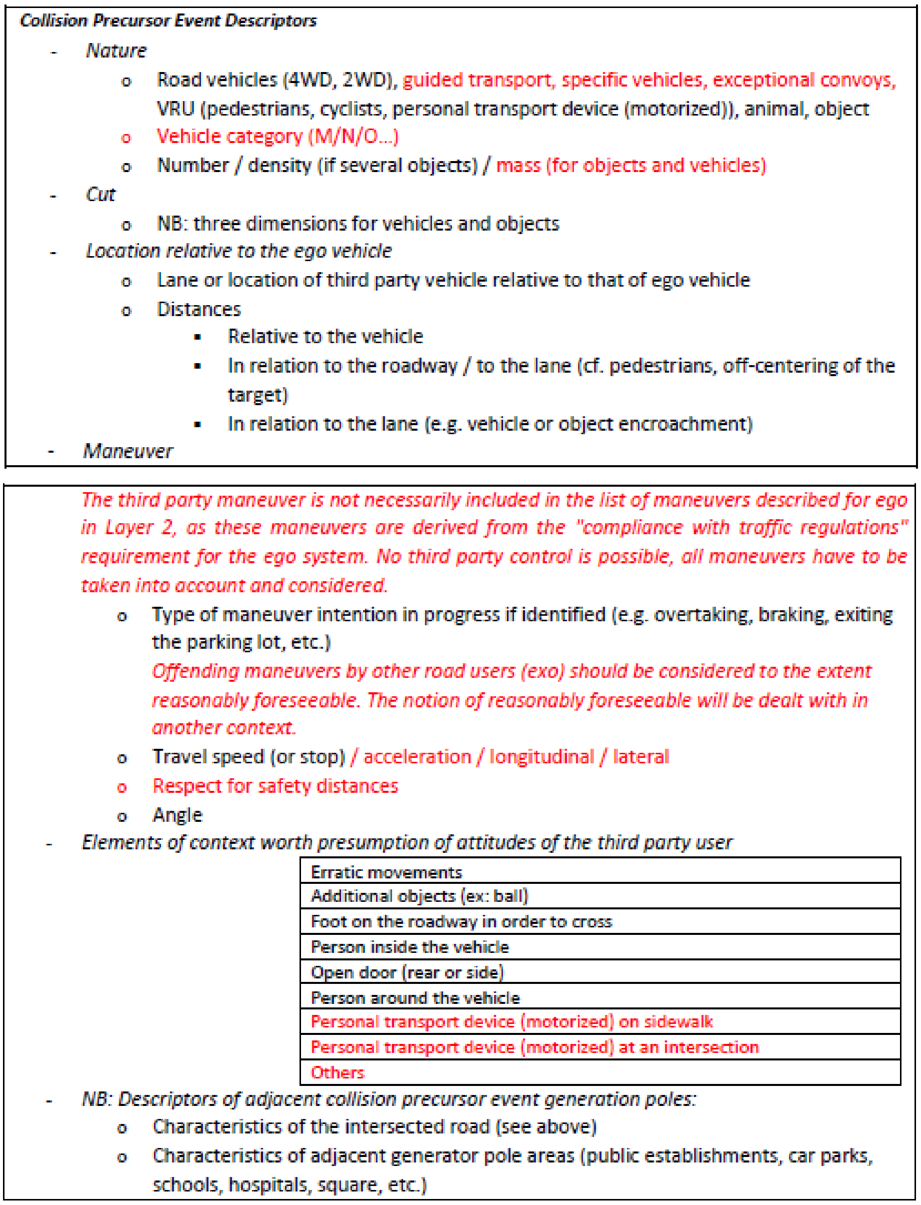
i. Collision precursor events directly attributable to objects and other road users.
ii. System malfunctions: failures, functional insufficiencies and misuse (are not the subject of this deliverable).

In this part are taken into account behaviours of third parties potentially encountered by the ego as well as their behaviours.

To go back to the precise causes of an accident, a detailed accident study (EDA) must be carried out, comparable to the field investigation which is required for Judicial Treatment. In the absence of a field investigation, police reports can help to reconstruct a probable scenario which may be derived from the risky behaviour of third parties, as carried out within the framework of VOIESUR, for MOSAR. Similarly, since elements of description below have been devised for the safety demonstration of systems, a large number of descriptors do not appear in the BAAC database to date because of the responsibility attributed to each driver to be attentive to his environment: we enter the subjective part of the analysis of the scene.

On the other hand, the comparisons carried out have made it possible to update an initial complement based on the observed behaviour of third parties and, in particular, on accident situations.

Below is a figure from the DGITM/SAGS/EP, *Safety demonstration of automated road transport systems (ARTS): Excepted contributions of the driving scenarios*, 2022. [15]



Collision Precursor Event Descriptors

- *Nature*
    - Road vehicles (4WD, 2WD), guided transport, specific vehicles, exceptional convoys, VRU (pedestrians, cyclists, personal transport device (motorized)), animal, object
    - Vehicle category (M/N/O…)
    - Number / density (if several objects) / mass (for objects and vehicles)
- *Cut*
    - NB: three dimensions for vehicles and objects
- *Location relative to the ego vehicle*
    - Lane or location of third party vehicle relative to that of ego vehicle
    - Distances
        - Relative to the vehicle
        - In relation to the roadway / to the lane (cf. pedestrians, off-centering of the target)
        - In relation to the lane (e.g. vehicle or object encroachment)
- *Maneuver*

The third party maneuver is not necessarily included in the list of maneuvers described for ego in Layer 2, as these maneuvers are derived from the "compliance with traffic regulations" requirement for the ego system. No third party control is possible, all maneuvers have to be taken into account and considered.

- Type of maneuver intention in progress if identified (e.g. overtaking, braking, exiting the parking lot, etc.)

  Offending maneuvers by other road users (exo) should be considered to the extent reasonably foreseeable. The notion of reasonably foreseeable will be dealt with in another context.
- Travel speed (or stop) / acceleration / longitudinal / lateral
- Respect for safety distances
- Angle

- *Elements of context worth presumption of attitudes of the third party user*

Erratic movements
Additional objects (ex: ball)
Foot on the roadway in order to cross
Person inside the vehicle
Open door (rear or side)
Person around the vehicle
Personal transport device (motorized) on sidewalk
Personal transport device (motorized) at an intersection
Others

- *NB: Descriptors of adjacent collision precursor event generation poles:*
    - Characteristics of the intersected road (see above)
    - Characteristics of adjacent generator pole areas (public establishments, car parks, schools, hospitals, square, etc.)

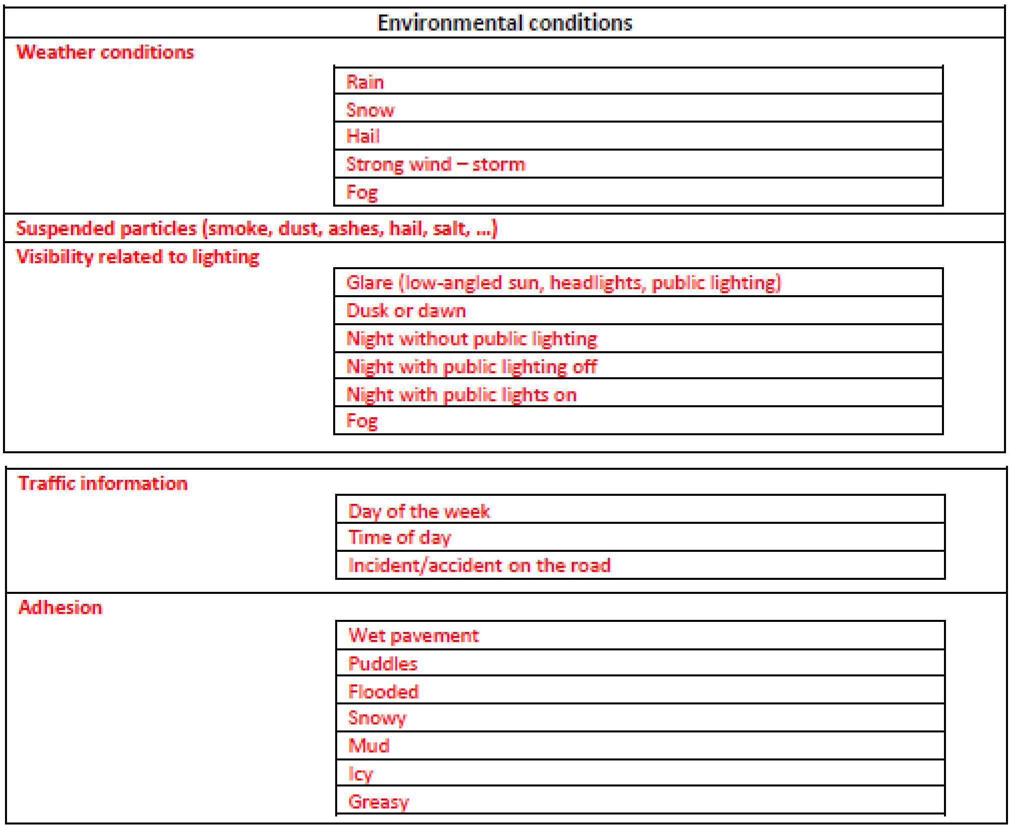
Figure 9: Updated collision precursor event descriptors.

Hazards affecting system response:

A specific point of view applicable to CAV systems can be adopted concerning critical factors able to facilitate appearance of catastrophic situations or dreaded events.

Several types of hazards are described in this section, such as the Environmental conditions, which temporarily impact and complicate the nominal environment and infrastructure.

Below is a table from the DGITM/SAGS/EP, *Safety demonstration of automated road transport systems (ARTS): Excepted contributions of the driving scenarios*, 2022. [15]



Environmental conditions	
Weather conditions	Rain
	Snow
	Hail
	Strong wind – storm
	Fog
Suspended particles (smoke, dust, ashes, hail, salt, …)	
Visibility related to lighting	Glare (low-angled sun, headlights, public lighting)
	Dusk or dawn
	Night without public lighting
	Night with public lighting off
	Night with public lights on
	Fog
Traffic information	Day of the week
	Time of day
	Incident/accident on the road
Adhesion	Wet pavement
	Puddles
	Flooded
	Snowy
	Mud
	Icy
	Greasy

Table 1: Hazardous environmental conditions.

2.8 Integration process

Integration process may be also a critical phase, and has to be well addressed and documented to prove it might not produce non conformities or failures.

Based on the *L8.14 - Report on the impact of AI in system engineering choices* document done by BPI France for the PRISSMA project (cf. [12]), the integration of a given set of elements of a system needs some particular tests to be taken to assess the capabilities of this set regarding system's requirements. Depending on the system of interest, the scope of the tests to be taken should be analyzed properly:

i. AD vehicle: the SOI is one vehicle. The integration of some components, including AI components, is a state-of-the art activity in system engineering: the context of these components is simulated. The configuration management of the set of these system's element AND its test system should be done carefully.

ii. AD system of system: one AD system is a part of the AD system of systems. Even if this AD system comprising the AD vehicle fleet and possible remote supervision has been validated, the operation of the first vehicles in the Road is an integration for the AD system of system. The transition from validation to operation of a given AD system should be ruled and audited by authoritative organisations.

2.9 Verification process

The same way, verification process is a key phase, and has to be well addressed and documented to prove system developed fulfils functional and non-functional performances required initially.

In this regard, PRISSMA project focuses on some particular verification activities such as the tests that can applied to an AD system (simulation test, closed road or open road tests).

Since the verification scope is to verify a system against its requirements, and not the stakeholder's needs it fulfills, the quality of the requirements will have a particularly strong impact on the seamless transition of the verification success to the validation success: if the system has good requirements, then a successful verification will enable a successful validation. But if the system requirements definition process has flaw, then the delivered system fulfilling its requirements but may not fill the stakeholders' needs.

In addition, the system and the components (sensors, algorithms and actuators) shall be verified to show that they behave as expected for known hazardous scenarios and reasonably foreseeable misuse (derived from previous analyzes and knowledge). It shall be verified that system and components are covered sufficiently by the tests.

To support the achievement of the objectives of this clause, the following information can be considered:

i. Verification strategy.
ii. Functional concept, including sensors, actuators and algorithm specification.
iii. System design specification.
iv. Verification targets.
v. Vehicle design (e.g. mounting position).
vi. Analysis of triggering events results.

Finally, based on the *Regulation 2022R1426 - Interpretation* document (cf. [4]), there are additional elements needed in order to carry out the virtual tests that go beyond the crafting of virtual models. It is also represented through the illustration below coming from the document mentioned previously.

Among them: time-steps definition, solvers, and coupling algorithms. Despite the adoption of validated sub-components, the overall virtual test's outcome might not well represent the RWS due to integration and software implementation issues which shall be addressed using software verification techniques.

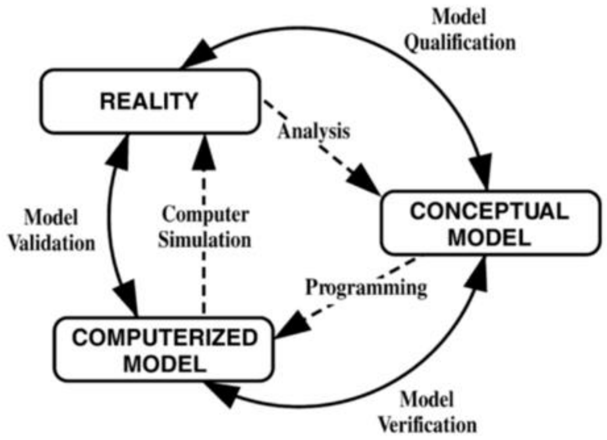


Figure 10: V&V approach.

It is thus advised that the M&S toolchain undergoes a verification phase. In particular, the verification exercise aims at assessing the correct implementation of the conceptual model. During this phase, the sources of numerical errors should be assigned an upper bound. Three steps are discussed hereafter.

Otherwise, according to the NASA credibility framework (NASA, 2016) , a five-level score can be assigned to the verification step depending on the degree of fulfillment of the factor.

This five-level score is represented in the table below that come from the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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*, 2022. [4]

Level	**Model Verification Degree**	**Error Bounding**
0	No/insufficient evidence is given	No/insufficient evidence is given
1	Informal practices applied to some of the models/features of the M&S toolchain	Informal practices applied to assess errors
2	Documented practices applied to verify all the M&S features	Most important errors satisfy requirements
3	Formal practices applied to verify end-to-end the M&S toolchain	All-important errors satisfy requirements
4	Reliable practices applied to verify end-to-end the M&S toolchain	All model errors satisfy requirements

Table 2: Template for verification credibility level.

For the code verification phase, it is concerned with the execution of virtual tests demonstrating that no numerical/logical flaws affect the virtual models with respect to the intended purpose of the M&S toolchain and that the numerical algorithms are implemented correctly. Code verification is typically carried out by the simulation software producer as it is not model-specific. Nevertheless, it is up to the applicant to retrieve evidence for code verification procedures being enforced in the software used to develop the M&S toolchain.

Below is a figure from the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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*, 2022. [4]

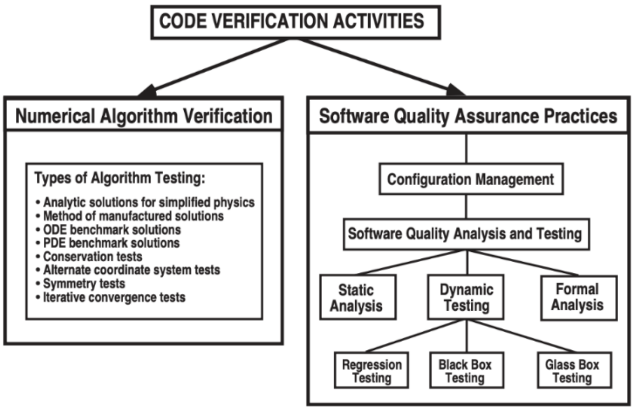

CODE VERIFICATION ACTIVITIES
Numerical Algorithm Verification
Types of Algorithm Testing:
• Analytic solutions for simplified physics
• Method of manufactured solutions
• ODE benchmark solutions
• PDE benchmark solutions
• Conservation tests
• Alternate coordinate system tests
• Symmetry tests
• Iterative convergence tests
Software Quality Assurance Practices
Configuration Management
Software Quality Analysis and Testing
Static Analysis
Dynamic Testing
Formal Analysis
Regression Testing
Black Box Testing
Glass Box Testing

Figure 11: Code verification procedures, (W. L. Oberkampf et al. 2004).

Concerning, classiqual computing language (not AI based), here are examples of techniques that might be used to support the code verification argument:

i. **Unit testing:** execution of a series of low-level tests and comparison of the implemented (coded) model with the conceptual/mathematical models (NASA, 2019) .
ii. **Model (code) coverage:** execution of virtual tests to determine that all logical branches within the model are executed (NASA, 2019) .
iii. **Static testing**: checking of compilation warnings and errors, consistency analysis in the use of the computer language (EASA, 2020) .
iv. **Dynamic testing:** code execution to investigate memory leaking.

Or also:

i. **Convergence testing:** execution of tests to demonstrate the convergence to a stationary value while iterating spatial/temporal discretization.
ii. **Order of accuracy:** execution of tests aiming at assessing whether the solution/discretization error converges with the expected rate.
iii. **Comparison with a known analytical solution:** whenever a known (analytical) solution is known it should be compared to the corresponding simulation model code realization.
iv. **Method of Manufactures Solutions:** (MMS) create an analytical solution for the set of equations (ODEs or PDEs) defining the model under analysis without necessarily resorting to a solution backed by physical meaning (WL Oberkampf et al., 2004) .

To sum up, the main aim of the code verification phase, from the perspective of the credibility assessment, is to provide evidence of:

i. The correctness and fidelity of the numerical algorithms used in the code relative to the mathematical model.
ii. The correctness of the source code.
iii. The configuration management, control, and testing of software through SQE practices.

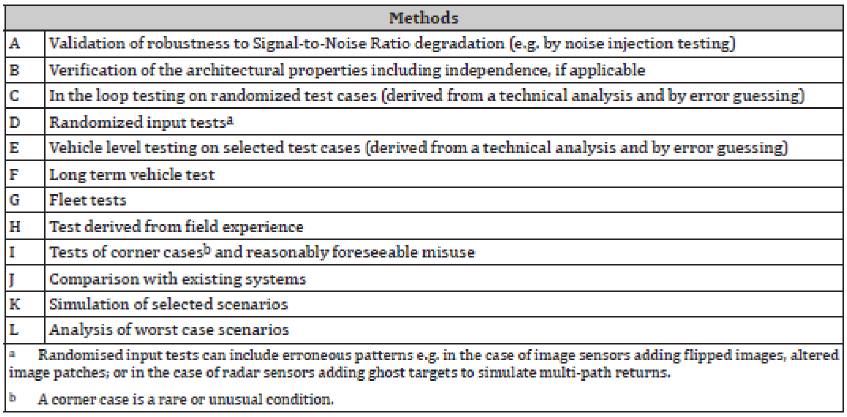
2.10 Validation process

Validation process is as well a very important process which occurs all along the development cycles and may concern very different performance metrics.

In a first part, it is important to mention that the functions of the system and the components (sensors, decision-algorithms and actuators) shall be validated to show that they do not cause an unreasonable level of risk in real-life use cases. This requires evidence that the validation targets are met. To support the achievement of this objective the following information can be considered:

i. Validation strategy.
ii. Verification results in defined use cases.
iii. Functional concept, including sensors, actuators and decision-algorithm specification.
iv. System design specification.
v. Validation targets.
vi. Vehicle design (e.g. sensor mounting position).
vii. Analysis of triggering events results.

Methods to evaluate the residual risk arising from real-life situations, that could trigger a hazardous behaviour of the system when integrated in the vehicle, can be applied as illustrated by the following table that come from the AFNOR, *ISO/PAS 21448,* 2019.) [33]



	Methods
A	Validation of robustness to Signal-to-Noise Ratio degradation (e.g. by noise injection testing)
B	Verification of the architectural properties including independence, if applicable
C	In the loop testing on randomized test cases (derived from a technical analysis and by error guessing)
D	Randomized input tests[a]
E	Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing)
F	Long term vehicle test
G	Fleet tests
H	Test derived from field experience
I	Tests of corner cases[b] and reasonably foreseeable misuse
J	Comparison with existing systems
K	Simulation of selected scenarios
L	Analysis of worst case scenarios

[a] Randomised input tests can include erroneous patterns e.g. in the case of image sensors adding flipped images, altered image patches; or in the case of radar sensors adding ghost targets to simulate multi-path returns.

[b] A corner case is a rare or unusual condition.

Table 3: Evaluation of residual risk table.

For each of the applied methods described in the previous table, an appropriate cumulative test length is selected. A rationale for the test length selected is provided and correlated with the number and distribution of scenarios. Generally, for all selected test methods a rationale is provided establishing that the resulting distribution of system inputs is representative of either the general operational environment or the specific use case, scene or scenario. Vehicle test length determination (long term tests, fleet tests) can take into account knowledge from prior vehicle programs, driver controllability, or the criticality of selected test routes. In the case of the use of randomized input tests, the number of scenarios being simulated in which erroneous patterns are injected can be correlated with the test length and test content that is representative of the target market.

Example

When evaluating an image recognition algorithm using simulation, a cumulative test length of X hours is selected, with Y different scenarios. The distribution of scenarios is adjusted according to the challenging scenarios and the distribution of driving use cases from traffic data. The susceptibility of the algorithm to real life triggers is identified by analysis of the algorithm and its decision paths. Scenarios with the most sensitive algorithm characteristics are included with a distribution emphasizing the challenging scenarios and representing their statistical relevance. The probabilities of occurrence of the influencing parameters in real-life use cases can also be considered to determine the appropriate test length.

Below is a figure from the BPI France for the PRISSMA project, *Liv. 6.2 : State Of The Art risk assessment and certification for AI : Intermediate report*, 2022. [11]

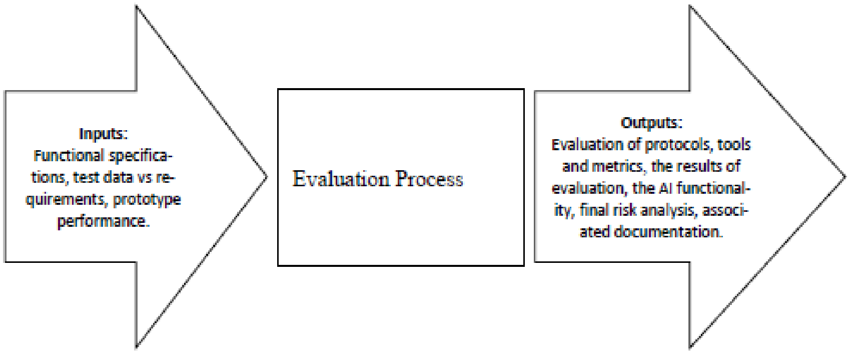

Inputs:
Functional specifications, test data vs requirements, prototype performance.
Evaluation Process
Outputs:
Evaluation of protocols, tools and metrics, the results of evaluation, the AI functionality, final risk analysis, associated documentation.

Figure 12: Evaluation Process inputs and outputs (LNE certification standard for AI processes).

In addition, based on the *International horizontal regulation of automated vehicles* document (cf. [5]), the validation methodology below can be used to perform the validation process:

This part of the working document proposes preliminary considerations on the possible adequation of validation approaches and tools to the different “regulation building blocks” presented above. This chapter is not, by any means, a formal position of the French authorities on the future of systems validation, nor, in the EU context, on the future of type-approval.

Different validation approaches are possible in order to address different parts of the above regulation architecture. A schematic mapping of these approaches can be useful.

i. First, a typology of validation approaches could be drawn considering their main scope:
    - Risk analysis or assessment;
    - Analysis or validation of Responses (to risk).

ii. Risk assessment methods can, broadly speaking, either:
    - Follow no specific methodology;
    - Follow a declared methodology;
    - Follow a mandatory methodology.

iii. Requirements towards the system could also, schematically, be defined gradually, from mere existence of a function, to a real performance level, as listed in chapter 5 above:
    - Situation and event knowledge;
    - Situation and event response availability;
    - Situation and event response functional description;
    - Situation and event response required functionalities;
    - Situation and event response required performance.

iv. It could also be useful to draw different levels of performance validation, depending on the involvement of “third parties”, especially public authorities, such as:
    - Declared performance (or existence or functionality);
    - Evidence-based performance (or existence or functionalities);
    - Certified performance (or existence or functionalities);
    - Tested performance (or existence or functionalities).

v. The validation tools could also usefully distinguish:
    - Documentation screening or analysis;
    - Simulations;
    - Testing in real conditions (“one driver” or “drivers sample”).

vi. In the same respect, validation tools could also be split into two main categories, depending on the fact that automated vehicles' operation domains are defined by:
    - Generic driving conditions;
    - Specific local geo-fenced driving conditions.

vii. Finally, the typology or mapping of validation approaches could distinguish between the vehicle's life phase:
    - Vehicle admittance;
    - In-use control.

The following paragraphs propose to focus on three of the main typology parameters listed above, in order to elaborate first considerations of possible adequation between validation approaches and types of requirements.

The typology dimensions or parameters considered at this stage are:

i. Requirements towards the system
   - Situation and event knowledge;
   - Response availability;
   - Response functional description;
   - Response required functionalities;
   - Response required performance.

ii. Level of verification:
   - (Self) declared;
   - Evidence- based;
   - Certified (by third party);
   - Tested (by public authority).

iii. Validation tools
   - Documentation screening or analysis;
   - Simulations;
   - Testing.

The following tables and graphs illustrate the proposed approach, pointing out the proportionality between criticality of identified situations and events on one hand, requirements and validation tools on the other hand. These illustrations come from the DGITM/SAGS/EP, DGEC/SD6, Ministère de la transition écologique et solidaire, et Ministère des transports., *International horizontal regulation of automated vehicles*, 10/08/2017. [5]

Step 1: use case description + risk analysis

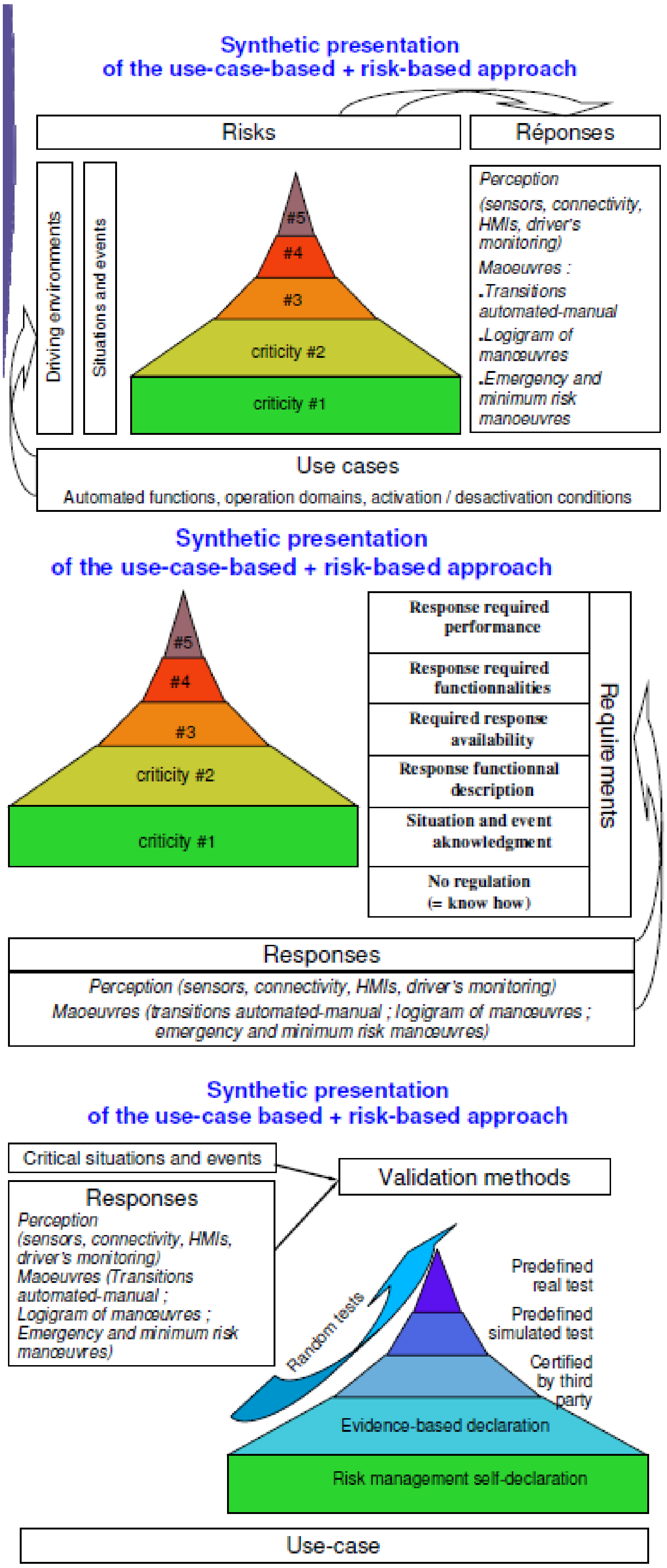
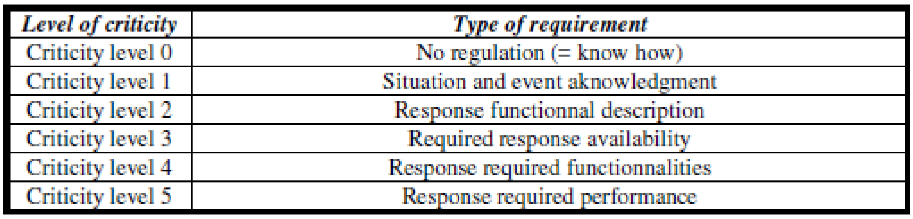

Synthetic presentation
of the use-case-based + risk-based approach
Risks
Réponses
Driving environments
Situations and events
#5
#4
#3
criticity #2
criticity #1
Perception
(sensors, connectivity, HMIs, driver's monitoring)
Maoeuvres :
.Transitions automated-manual
.Logigram of manoeuvres
.Emergency and minimum risk manoeuvres
Use cases
Automated functions, operation domains, activation / desactivation conditions
Synthetic presentation
of the use-case-based + risk-based approach
#5
#4
#3
criticity #2
criticity #1
Response required performance
Response required functionnalities
Required response availability
Response functionnal description
Situation and event aknowledgment
No regulation
(= know how)
Requirements
Responses
Perception (sensors, connectivity, HMIs, driver's monitoring)
Maoeuvres (transitions automated-manual ; logigram of manœuvres ; emergency and minimum risk manœuvres)
Synthetic presentation
of the use-case based + risk-based approach
Critical situations and events
Validation methods
Responses
Perception
(sensors, connectivity, HMIs, driver's monitoring)
Maoeuvres (Transitions automated-manual ;
Logigram of manœuvres ;
Emergency and minimum risk manœuvres)
Random tests
Predefined real test
Predefined simulated test
Certified by third party
Evidence-based declaration
Risk management self-declaration
Use-case

Figure 13: Schemes of the use-case-based and the risk =-based approaches.

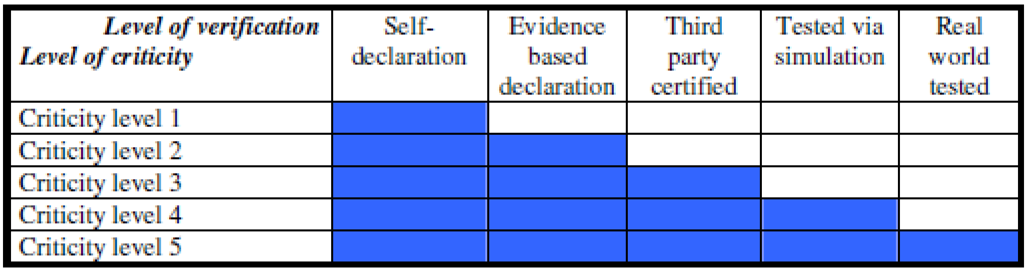
Step 2: proportionate use-case requirements



Level of criticity	*Type of requirement*
Criticity level 0	No regulation (= know how)
Criticity level 1	Situation and event aknowledgment
Criticity level 2	Response functionnal description
Criticity level 3	Required response availability
Criticity level 4	Response required functionnalities
Criticity level 5	Response required performance

Table 4: Criticity levels and theirs associated requirements.

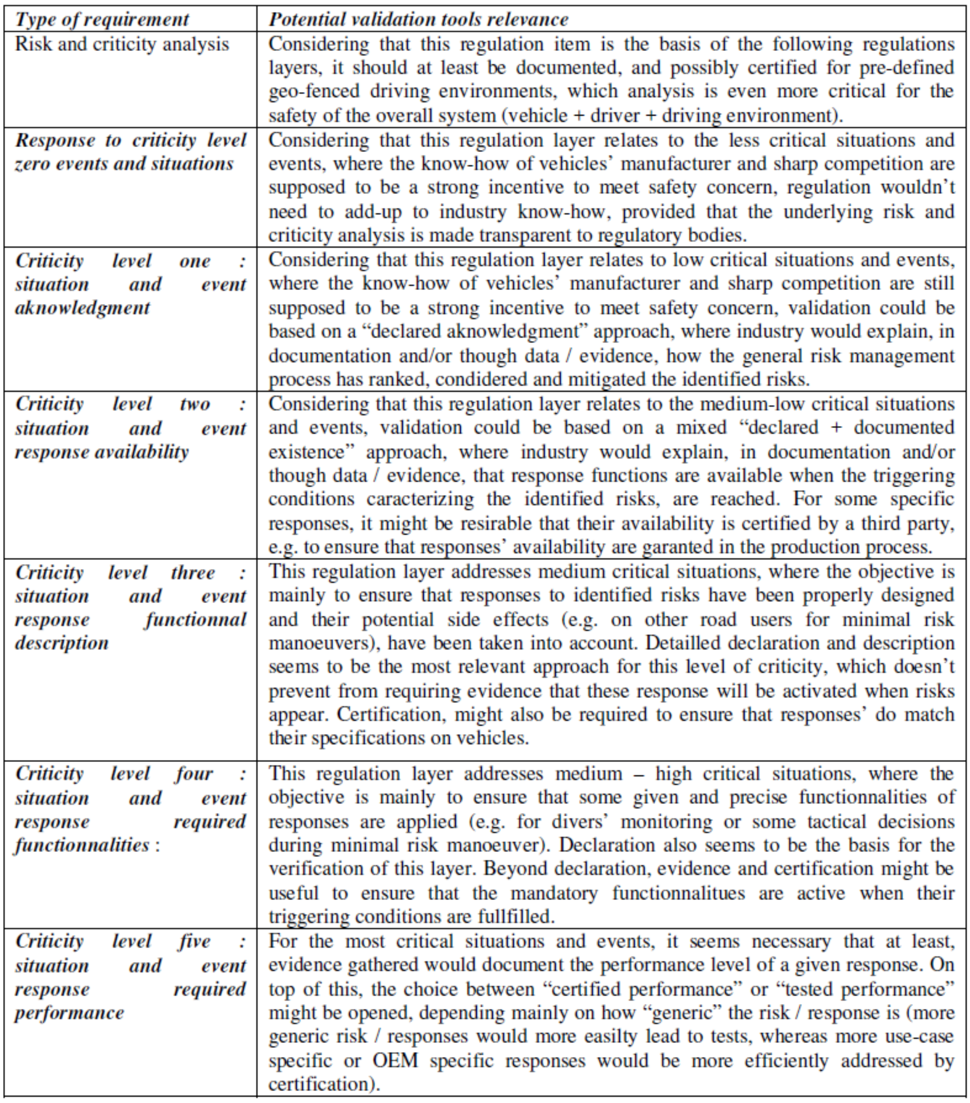
Step 3: proportional validation methods



Level of verification *Level of criticity*	Self-declaration	Evidence based declaration	Third party certified	Tested via simulation	Real world tested
Criticity level 1	🟦				
Criticity level 2	🟦	🟦			
Criticity level 3	🟦	🟦	🟦		
Criticity level 4	🟦	🟦	🟦	🟦	
Criticity level 5	🟦	🟦	🟦	🟦	🟦

Table 5: Criticity levels and theirs associated verification levels.

Along with this proportionate deterministic approach, where a given requirement on a response is dealt with a given validation tool, it might be useful to add a random approach, where some requirements / responses would be submitted to tighter validation tools.



Type of requirement	*Potential validation tools relevance*
Risk and criticity analysis	Considering that this regulation item is the basis of the following regulations layers, it should at least be documented, and possibly certified for pre-defined geo-fenced driving environments, which analysis is even more critical for the safety of the overall system (vehicle + driver + driving environment).
Response to criticity level zero events and situations	Considering that this regulation layer relates to the less critical situations and events, where the know-how of vehicles' manufacturer and sharp competition are supposed to be a strong incentive to meet safety concern, regulation wouldn't need to add-up to industry know-how, provided that the underlying risk and criticity analysis is made transparent to regulatory bodies.
Criticity level one : situation and event aknowledgment	Considering that this regulation layer relates to low critical situations and events, where the know-how of vehicles' manufacturer and sharp competition are still supposed to be a strong incentive to meet safety concern, validation could be based on a "declared aknowledgment" approach, where industry would explain, in documentation and/or though data / evidence, how the general risk management process has ranked, condidered and mitigated the identified risks.
Criticity level two : situation and event response availability	Considering that this regulation layer relates to the medium-low critical situations and events, validation could be based on a mixed "declared + documented existence" approach, where industry would explain, in documentation and/or though data / evidence, that response functions are available when the triggering conditions caracterizing the identified risks, are reached. For some specific responses, it might be resirable that their availability is certified by a third party, e.g. to ensure that responses' availability are garanted in the production process.
Criticity level three : situation and event response functionnal description	This regulation layer addresses medium critical situations, where the objective is mainly to ensure that responses to identified risks have been properly designed and their potential side effects (e.g. on other road users for minimal risk manoeuvers), have been taken into account. Detailled declaration and description seems to be the most relevant approach for this level of criticity, which doesn't prevent from requiring evidence that these response will be activated when risks appear. Certification, might also be required to ensure that responses' do match their specifications on vehicles.
Criticity level four : situation and event response required functionnalities :	This regulation layer addresses medium – high critical situations, where the objective is mainly to ensure that some given and precise functionnalities of responses are applied (e.g. for divers' monitoring or some tactical decisions during minimal risk manoeuver). Declaration also seems to be the basis for the verification of this layer. Beyond declaration, evidence and certification might be useful to ensure that the mandatory functionnalitues are active when their triggering conditions are fullfilled.
Criticity level five : situation and event response required performance	For the most critical situations and events, it seems necessary that at least, evidence gathered would document the performance level of a given response. On top of this, the choice between "certified performance" or "tested performance" might be opened, depending mainly on how "generic" the risk / response is (more generic risk / responses would more easilty lead to tests, whereas more use-case specific or OEM specific responses would be more efficiently addressed by certification).

Table 6: European Commission Study on the assessment and certification of automated vehicles, 2016: The "V approach" to validation under ISO 26262.

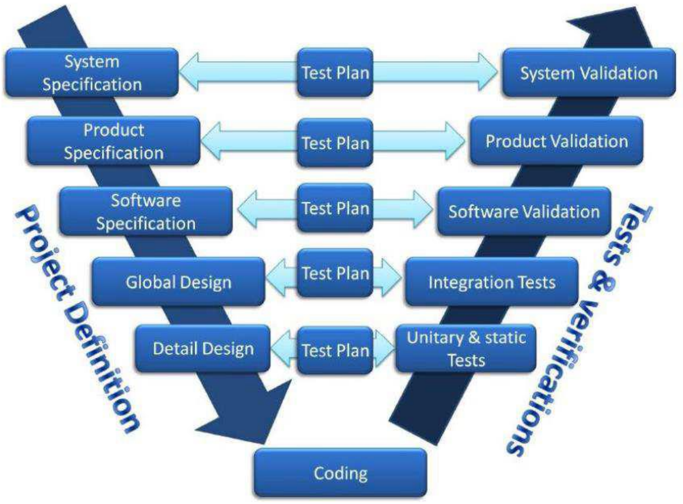


Figure 14: Considerations on the possible correspondence between requirements and theirs verification/validation tools.

2.11 Specific support elements

Certain validation support elements have appeared specifically in the engineering process of CAV systems.

2.11.1 OD

First, the definition of the OD or Operational Domain is:

The OD equals to the real operating conditions that are encountered by the ego-vehicle. The attributes of OD address the question “Which conditions does the system encounter on its current route?”

For instance, “1.1.6. Ego allowed to drive on traffic lane n°3 = yes” and “1.1.7. Use of traffic lane n°3 = all traffic lane”: on its current route section, the ego vehicle drives on lane n°3 which is allowed for all kind of traffic. The 1.1.6. is not enough generic for describing a system capability.

Now, below is illustrated a representation of what an OD perimeter can looks like and the comparison between what the ODD can looks like, which come from the cf. LNE, *Referentiel de certification de processus pour l'IA - Ref: LNE/DEC/CITI/CH*, 12/07/2021. [1]

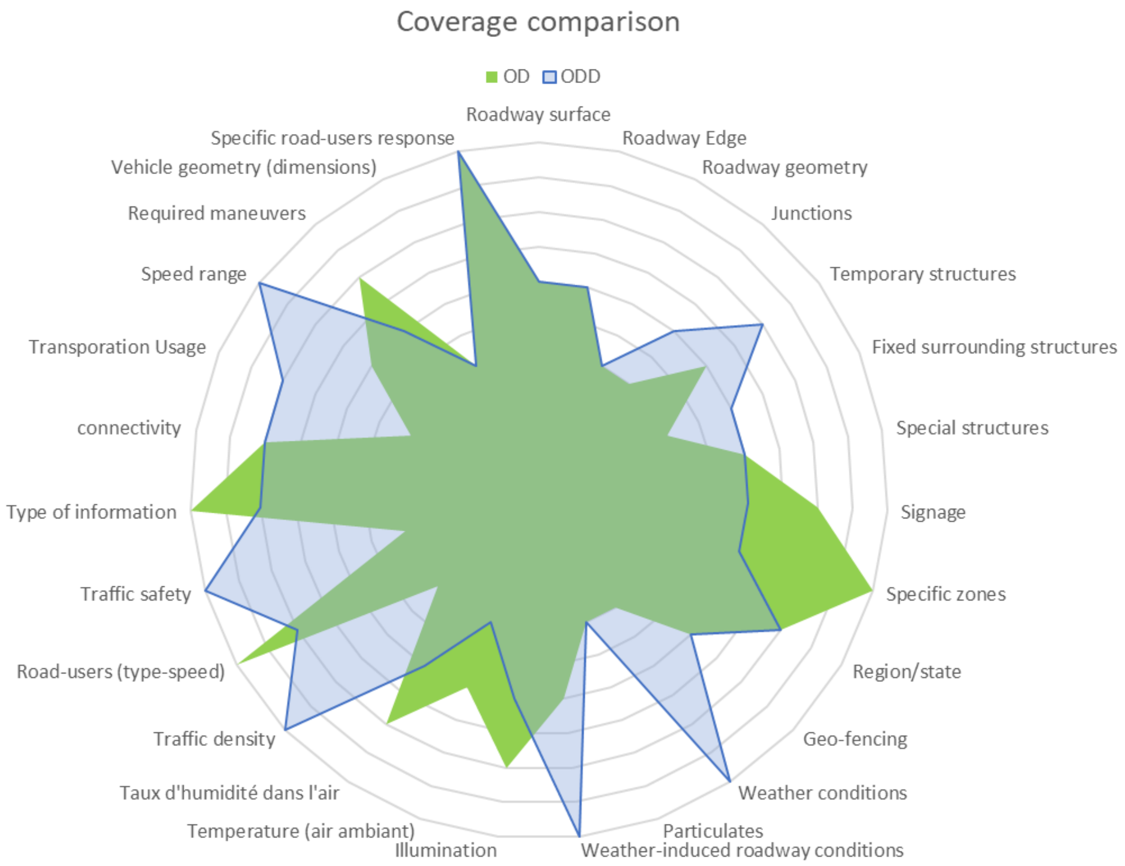


Figure 15: Example of the comparison between an OD and an ODD – Route analysis.

2.11.2 ODD

In addition, the definition of the ODD given by the summary of the *L'IA pour les nouvelles mobilités* conference done by UTAC (cf. [3]) is:

The ODD equals to the conditions that allow ego vehicle to perform safely the dynamic driving tasks (system capabilities). The attributes of ODD address the question “Which conditions may the system accept while operating safely?”

For instance, “1.1.5. Usage of the ego lane = All traffic lane”: the ego vehicle has the capability to drive safely on a lane with all kind of traffic. The 1.1.6. attribute is not enough precise for describing an actual situation.

Indeed, the operational design domain (ODD) defines the conditions under which a driving automation sys-tem is designed to perform the dynamic driving tasks (DDT).

Besides the automation level, the ODD description is the key point of the Automated Driving Systems (ADS) performance. The capability of ADS to safely perform the dynamic driving task is demonstrated under the particular operational conditions limited by the ODD. Where a Level 5 (from the SAE rating) ADS is not supposed to have any ODD limitation, the level 3 or 4 will have ODD limitations such as speed range, environmental conditions, traffic conditions, road conditions, etc. Therefore, the ODD will have to be monitored and any ODD exit must lead to a DDT fallback.

The definition of ODD must therefore allow describing in an unambiguous manner the external world within which the ADS can perform the DDT. The way (e.g. terms, scales, quality) the ODD is described will be used widely throughout the whole ADS specification, design, validation and operation phases, making it a founding milestone of the process.

Otherwise, below is illustrated a representation of what an ODD perimeter can looks like from the LNE, *Referentiel de certification de processus pour l'IA - Ref: LNE/DEC/CITI/CH*, 12/07/2021. [1]

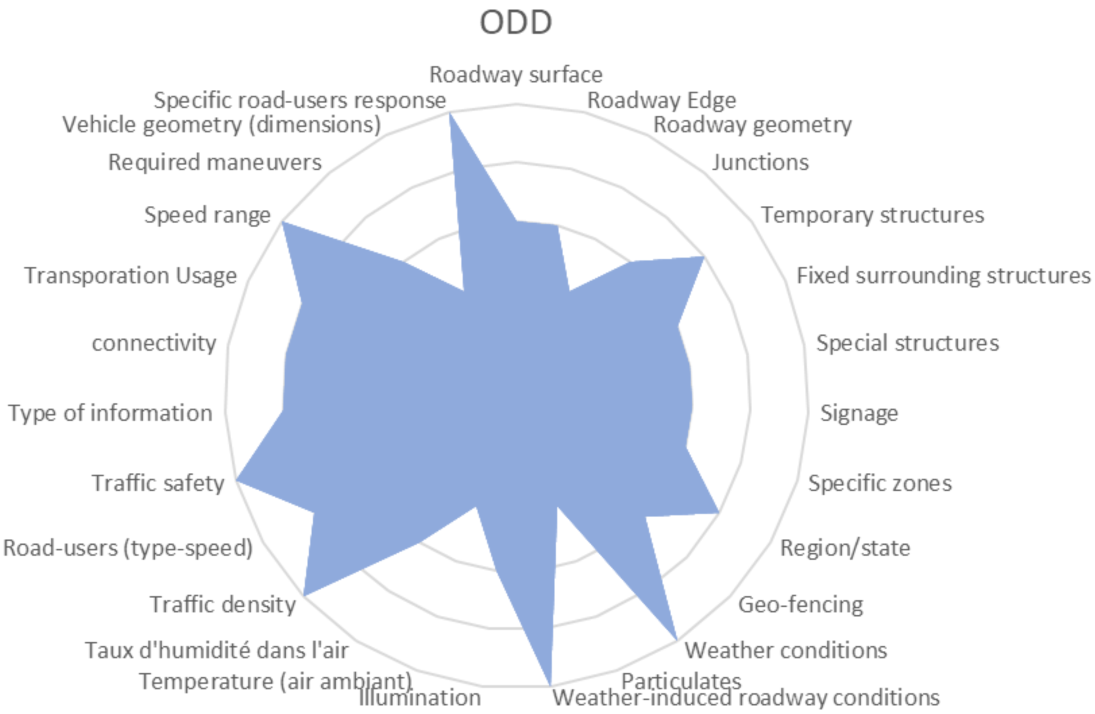


Figure 16: Example of an ODD – Route analysis.

Furthermore, from the same source, the following flowchart represents how the Taxonomy and the Guide to characterizing the ODD are generated from the ODD definition:

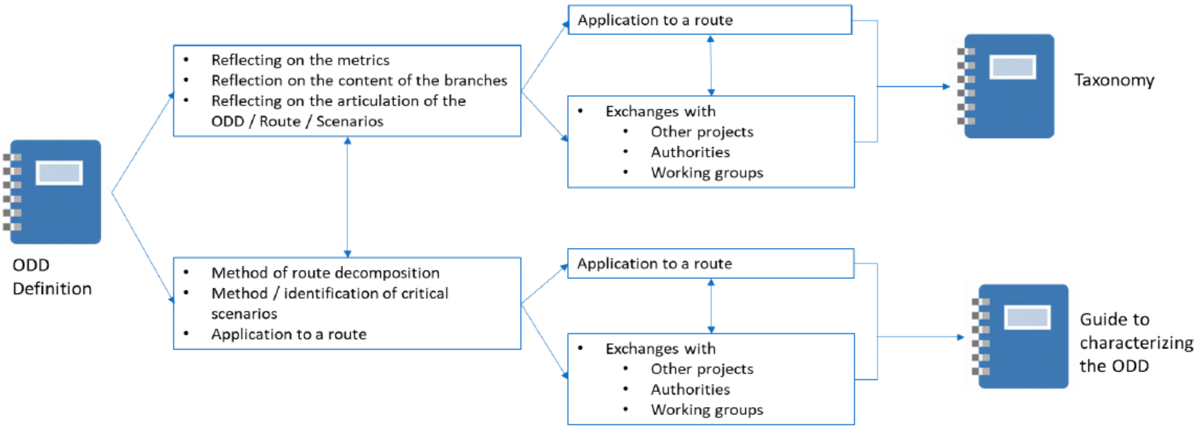
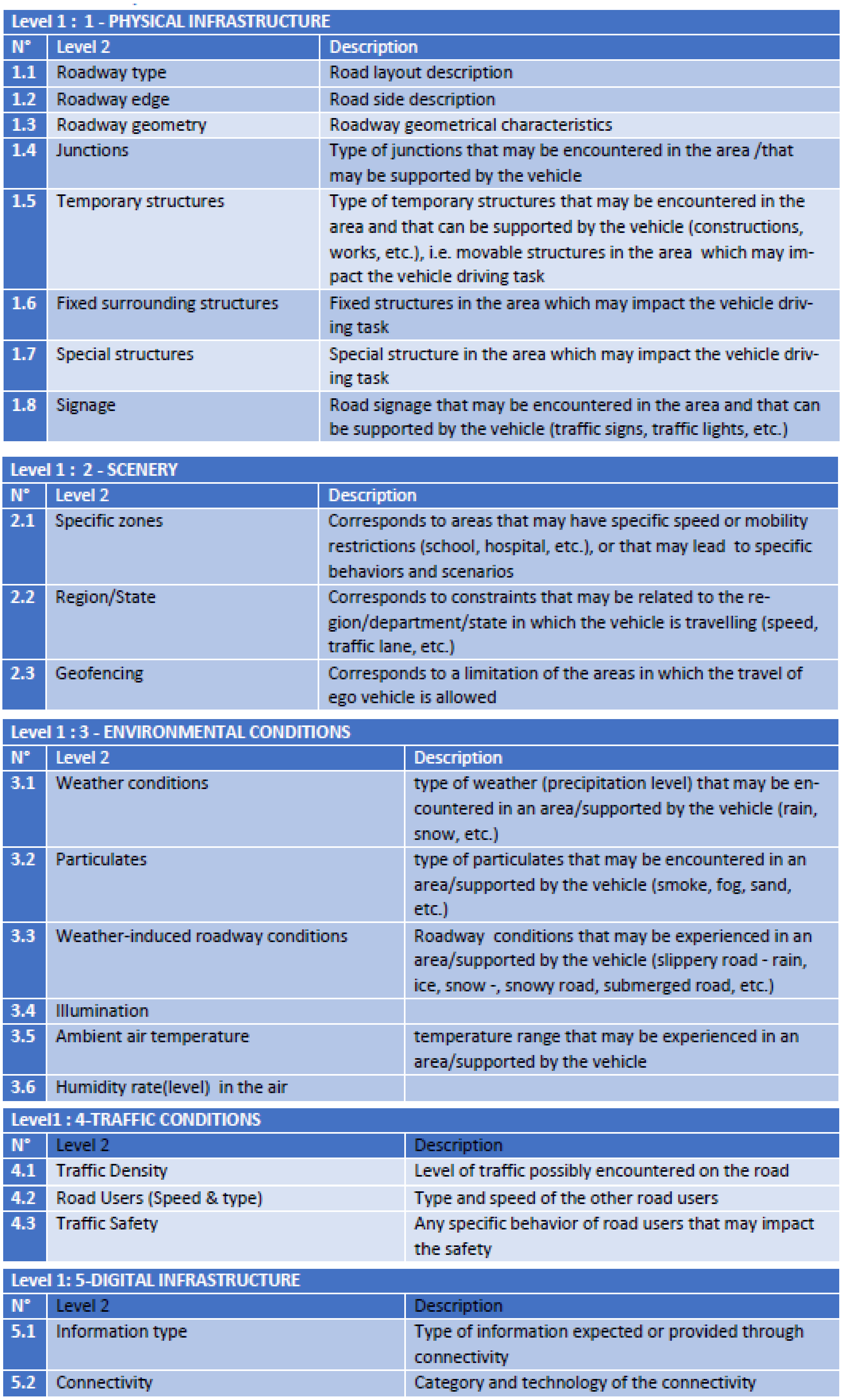


Figure 17: ODD and route descriptors.

Then, from the BPI France for the PRISSMA project, *Liv. 8.11 : Operational Design Domain*, 2022 [13] are presented some tables that list ODD descriptions that have been established by other deliverables, In those, the term “automated vehicle” refers to automated passenger transportation shuttles and to automated goods delivery vehicles, which are the target use cases of PRISSMA.



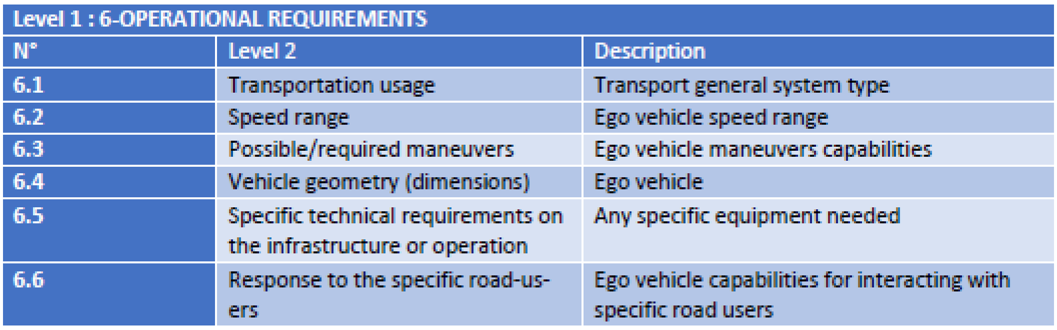
Level 1 : 1 - PHYSICAL INFRASTRUCTURE		
N°	Level 2	Description
1.1	Roadway type	Road layout description
1.2	Roadway edge	Road side description
1.3	Roadway geometry	Roadway geometrical characteristics
1.4	Junctions	Type of junctions that may be encountered in the area /that may be supported by the vehicle
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
2.2	Region/State	Corresponds to constraints that may be related to the region/department/state in which the vehicle is travelling (speed, traffic lane, etc.)
2.3	Geofencing	Corresponds to a limitation of the areas in which the travel of ego vehicle is allowed

Level 1 : 3 - ENVIRONMENTAL CONDITIONS		
N°	Level 2	Description
3.1	Weather conditions	type of weather (precipitation level) that may be encountered in an area/supported by the vehicle (rain, snow, etc.)
3.2	Particulates	type of particulates that may be encountered in an area/supported by the vehicle (smoke, fog, sand, etc.)
3.3	Weather-induced roadway conditions	Roadway conditions that may be experienced in an area/supported by the vehicle (slippery road - rain, ice, snow -, snowy road, submerged road, etc.)
3.4	Illumination	
3.5	Ambient air temperature	temperature range that may be experienced in an area/supported by the vehicle
3.6	Humidity rate(level) in the air	

Level1 : 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

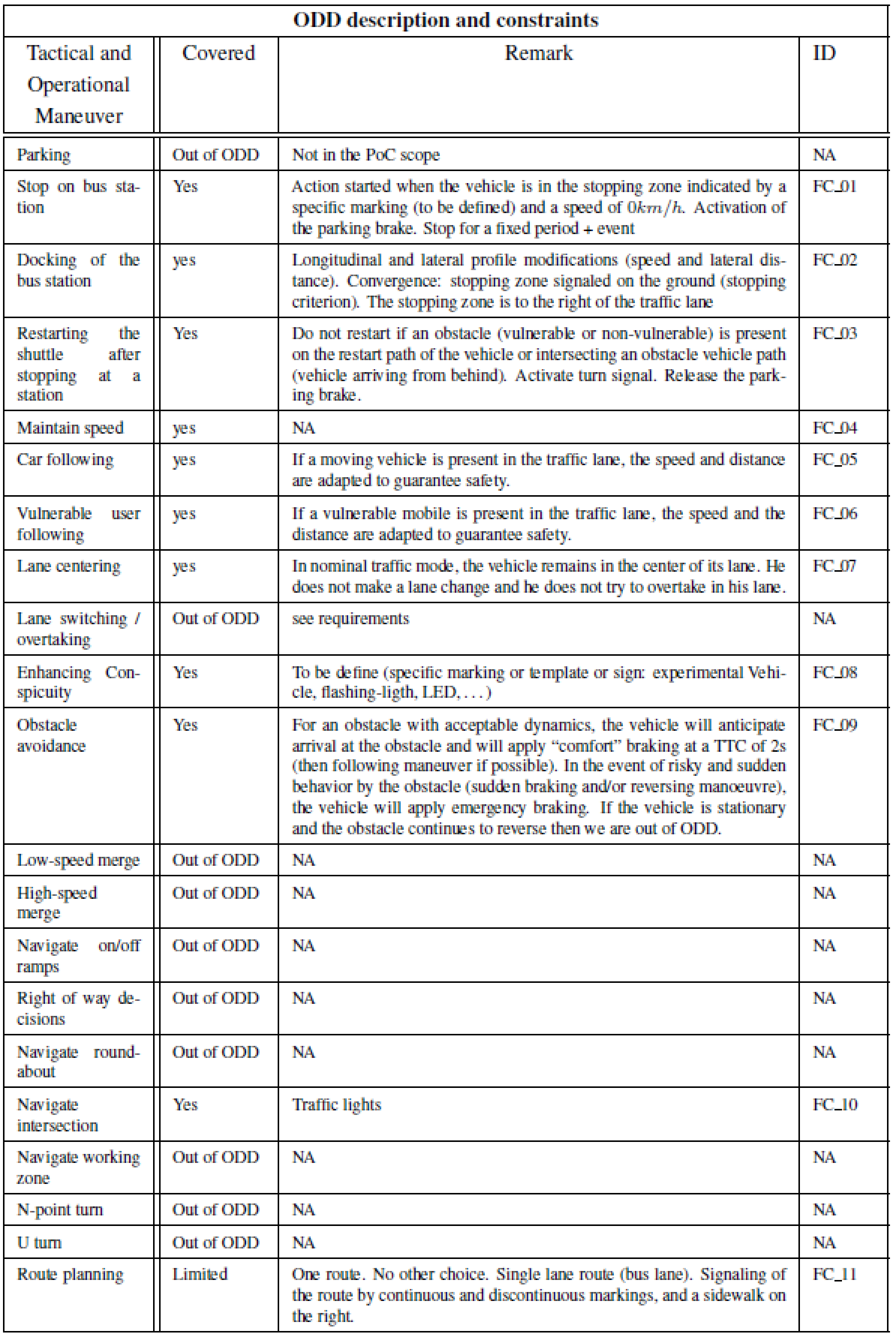
Level 1: 5-DIGITAL INFRASTRUCTURE		
N°	Level 2	Description
5.1	Information type	Type of information expected or provided through connectivity
5.2	Connectivity	Category and technology of the connectivity



Level 1 : 6-OPERATIONAL REQUIREMENTS		
N°	Level 2	Description
6.1	Transportation usage	Transport general system type
6.2	Speed range	Ego vehicle speed range
6.3	Possible/required maneuvers	Ego vehicle maneuvers capabilities
6.4	Vehicle geometry (dimensions)	Ego vehicle
6.5	Specific technical requirements on the infrastructure or operation	Any specific equipment needed
6.6	Response to the specific road-users	Ego vehicle capabilities for interacting with specific road users

Table 7: ODD descriptions.

Moreover, there is a list of ODD constraints that has been drafted which also includes their associated descriptions which comes from the BPI France for the PRISSMA project, *Liv 2.8 : Proofs-Of-Concept intermediate report developement of platforms meeting the desired objectives of evaluating means of automated mobility*, 2022. [34]



ODD description and constraints			
Tactical and Operational Maneuver	Covered	Remark	ID
Parking	Out of ODD	Not in the PoC scope	NA
Stop on bus station	Yes	Action started when the vehicle is in the stopping zone indicated by a specific marking (to be defined) and a speed of $0km/h$. Activation of the parking brake. Stop for a fixed period + event	FC_01
Docking of the bus station	yes	Longitudinal and lateral profile modifications (speed and lateral distance). Convergence: stopping zone signaled on the ground (stopping criterion). The stopping zone is to the right of the traffic lane	FC_02
Restarting the shuttle after stopping at a station	Yes	Do not restart if an obstacle (vulnerable or non-vulnerable) is present on the restart path of the vehicle or intersecting an obstacle vehicle path (vehicle arriving from behind). Activate turn signal. Release the parking brake.	FC_03
Maintain speed	yes	NA	FC_04
Car following	yes	If a moving vehicle is present in the traffic lane, the speed and distance are adapted to guarantee safety.	FC_05
Vulnerable user following	yes	If a vulnerable mobile is present in the traffic lane, the speed and the distance are adapted to guarantee safety.	FC_06
Lane centering	yes	In nominal traffic mode, the vehicle remains in the center of its lane. He does not make a lane change and he does not try to overtake in his lane.	FC_07
Lane switching / overtaking	Out of ODD	see requirements	NA
Enhancing Conspicuity	Yes	To be define (specific marking or template or sign: experimental Vehicle, flashing-ligth, LED, . . .)	FC_08
Obstacle avoidance	Yes	For an obstacle with acceptable dynamics, the vehicle will anticipate arrival at the obstacle and will apply “comfort” braking at a TTC of 2s (then following maneuver if possible). In the event of risky and sudden behavior by the obstacle (sudden braking and/or reversing manoeuvre), the vehicle will apply emergency braking. If the vehicle is stationary and the obstacle continues to reverse then we are out of ODD.	FC_09
Low-speed merge	Out of ODD	NA	NA
High-speed merge	Out of ODD	NA	NA
Navigate on/off ramps	Out of ODD	NA	NA
Right of way decisions	Out of ODD	NA	NA
Navigate roundabout	Out of ODD	NA	NA
Navigate intersection	Yes	Traffic lights	FC_10
Navigate working zone	Out of ODD	NA	NA
N-point turn	Out of ODD	NA	NA
U turn	Out of ODD	NA	NA
Route planning	Limited	One route. No other choice. Single lane route (bus lane). Signaling of the route by continuous and discontinuous markings, and a sidewalk on the right.	FC_11

Table 8: ODD Description and constraints.

Finally, in a more precise way, the ODD application to the developed service under test identified a set of requirements which are:

i. **Requirement 1:** For the moment, we do not take into account the opening of the doors, the closing of the doors, the signalling (alert) of starting the vehicle.

ii. **Requirement 2:** Do not restart if an obstacle (vulnerable or non-vulnerable) is present in the vehicle's restart path.

iii. **Requirement 3:** The vehicle moves on the bus lane (always the same lane).

iv. **Requirement 4:** No overtaking manoeuvre. The vehicle always stays on the same lane (bus/bike lane). The vehicle is using the far right lane.

v. **Requirement 5:** The road surface and road material conditions are: asphalt, cobblestone, concrete. No snowy surface. For the paved road, it is possible to take into account the vibration of the tires and the shock absorbers. Taking into account the pavement roughness and high frequencies produced by the pavement. These vibrations have an impact on both the vehicle and the sensor behaviour.

vi. **Requirement 6:** The types of users that the vehicle may encounter: car, bus, scooter, motorcycle, bicycle, pedestrian, van (i.e. moving company, delivery).

vii. **Requirement 7:** The vehicle does not change lanes. It stays in its lane.

viii. **Requirement 8:** The vehicle does not overtake an object in its lane.

ix. **Requirement 9:** The vehicle cannot cross the speed limit fixed to 20km/h

x. **Requirement 10:** The vehicle can move backward (reversing speed).

xi. **Requirement 11:** The vehicle in nominal mode cannot apply accelerations of more than 3 m/s2 and decelerations of more than 3m/s

xii. **Requirement 12:** In critical situation (TTC <= 1s), the vehicle must apply an emergency braking (1G: 9.81m/s)

2.11.3 OEDR

First, here is a simple description of an OEDR:

The OEDR perimeter described the factors determined to be out of scope for a particular identified ODD. These can generally be broken down into two sub-categories: objects and events. Specific events might not be applicable if no associated relevant objects are encompassed by the ODD.

Also, as a reminder, the definition of event is:

An event is a specific fact building a specific situation or condition for a set of scene elements. The event is more the observation of the realization of a configuration/ conjuncture with possible conditions. In fact, an event represents anything that happens in an instant of time (frame). Therefore, any instantaneous change of state caused by an Object or an element of the context can be defined as an Event. These changes usually cause a new occurrence and, depending on the duration, this can be defined as a new Event or an Action.

In fact the scenario approach, by aiming to inventory the driving situations that the automated road system may encounter in order to minimize the number of unknown dangerous scenarios, is presented as a process whose genesis can be found in the "OEDR" approach, whose underlying idea is to ensure the completeness of the system's responses through a three-step inventory reasoning:

i. Traffic hazards ("objects and events");

ii. Detection and recognition performance (“detection”);

iii. System response performance.

Besides, an interesting illustration has been done by the DGITM/SAGS/EP, DGEC/SD6, Ministère de la transition écologique et solidaire, et Ministère des transports., *International horizontal regulation of automated vehicles*, 10/08/2017 [5] which describe the interaction that the OEDR have with the other elements:

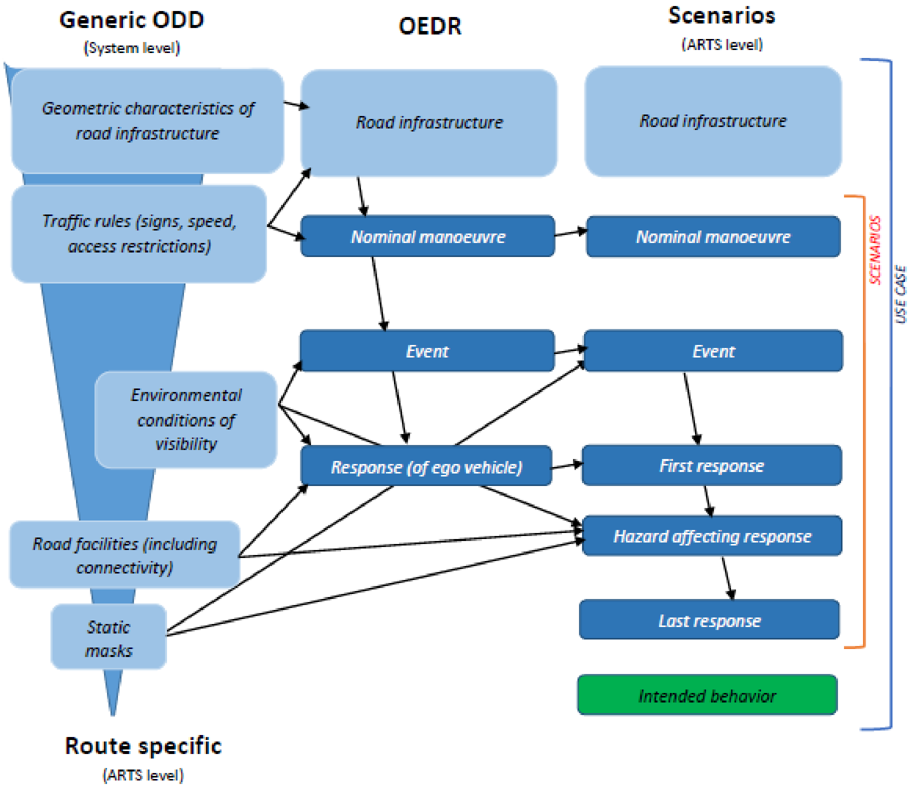
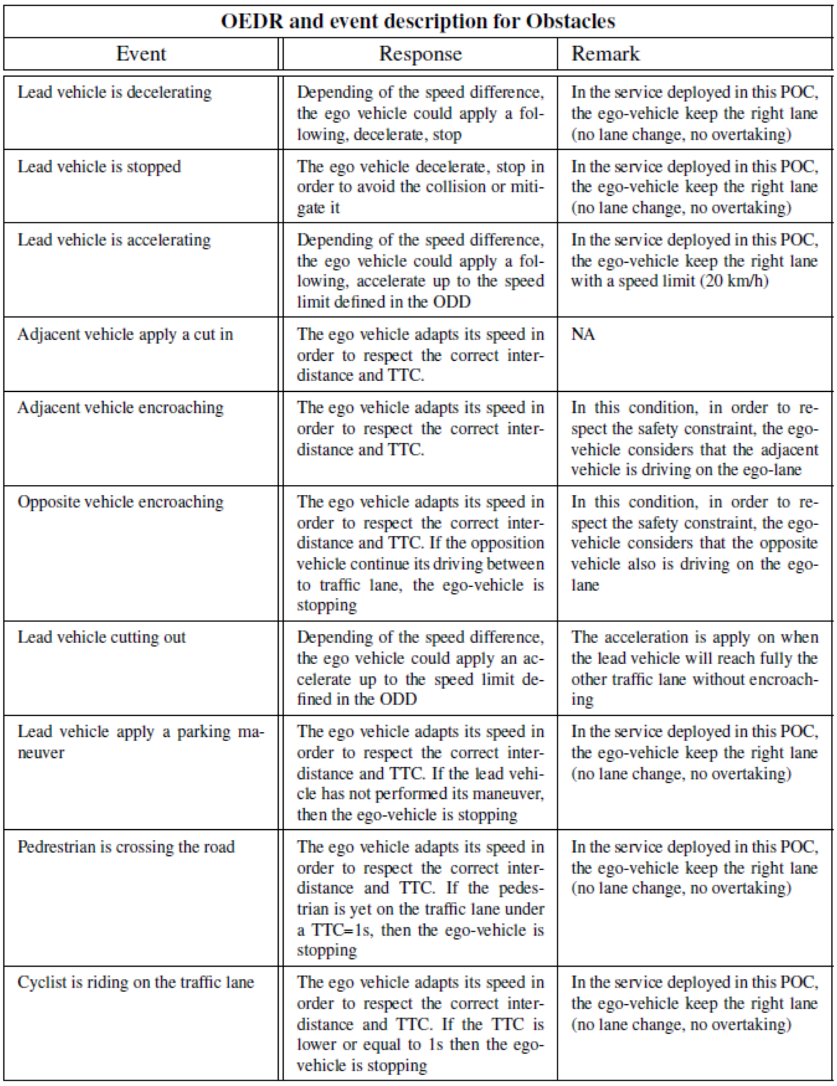


Figure 18: Articulation between the ODDs, the OEDR and the scenarios.

Now, here is a presentation of what an OEDR can looks like:

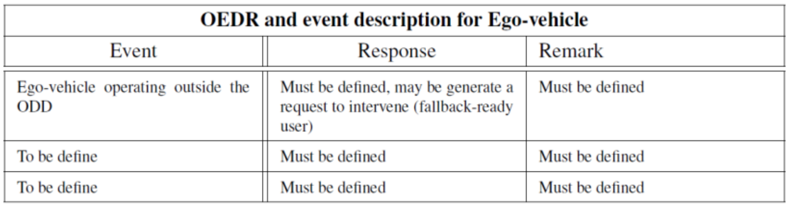
In order to define the different types of events, we have decided to share the events in function of the concerned environment key components: obstacles, road, ego-vehicle, and environment.

The following tables coming from the BPI France for the PRISSMA project, *Liv 2.8 : Proofs-Of-Concept intermediate report developement of platforms meeting the desired objectives of evaluating means of automated mobility*, 2022 [34] present the events encountering with an input from static and dynamic physical obstacle:



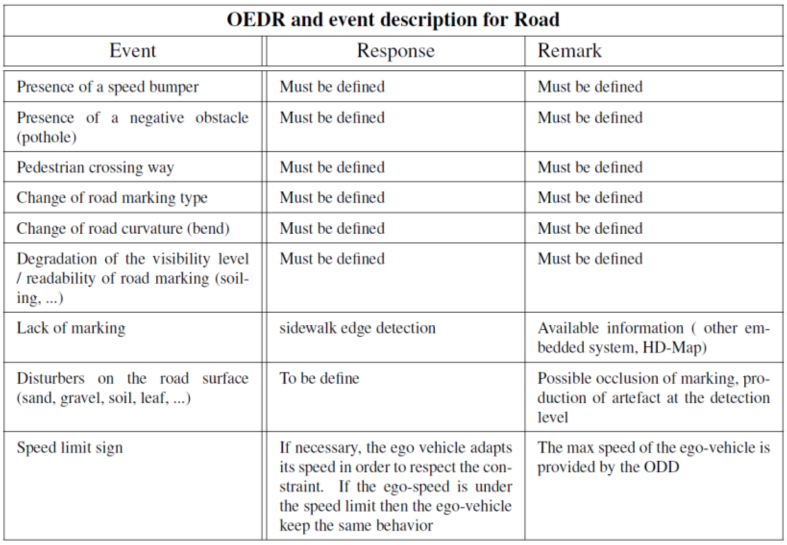
OEDR and event description for Obstacles		
Event	Response	Remark
Lead vehicle is decelerating	Depending of the speed difference, the ego vehicle could apply a following, decelerate, stop	In the service deployed in this POC, the ego-vehicle keep the right lane (no lane change, no overtaking)
Lead vehicle is stopped	The ego vehicle decelerate, stop in order to avoid the collision or mitigate it	In the service deployed in this POC, the ego-vehicle keep the right lane (no lane change, no overtaking)
Lead vehicle is accelerating	Depending of the speed difference, the ego vehicle could apply a following, accelerate up to the speed limit defined in the ODD	In the service deployed in this POC, the ego-vehicle keep the right lane with a speed limit (20 km/h)
Adjacent vehicle apply a cut in	The ego vehicle adapts its speed in order to respect the correct inter-distance and TTC.	NA
Adjacent vehicle encroaching	The ego vehicle adapts its speed in order to respect the correct inter-distance and TTC.	In this condition, in order to respect the safety constraint, the ego-vehicle considers that the adjacent vehicle is driving on the ego-lane
Opposite vehicle encroaching	The ego vehicle adapts its speed in order to respect the correct inter-distance and TTC. If the opposition vehicle continue its driving between to traffic lane, the ego-vehicle is stopping	In this condition, in order to respect the safety constraint, the ego-vehicle considers that the opposite vehicle also is driving on the ego-lane
Lead vehicle cutting out	Depending of the speed difference, the ego vehicle could apply an accelerate up to the speed limit defined in the ODD	The acceleration is apply on when the lead vehicle will reach fully the other traffic lane without encroaching
Lead vehicle apply a parking maneuver	The ego vehicle adapts its speed in order to respect the correct inter-distance and TTC. If the lead vehicle has not performed its maneuver, then the ego-vehicle is stopping	In the service deployed in this POC, the ego-vehicle keep the right lane (no lane change, no overtaking)
Pedrestrian is crossing the road	The ego vehicle adapts its speed in order to respect the correct inter-distance and TTC. If the pedestrian is yet on the traffic lane under a TTC=1s, then the ego-vehicle is stopping	In the service deployed in this POC, the ego-vehicle keep the right lane (no lane change, no overtaking)
Cyclist is riding on the traffic lane	The ego vehicle adapts its speed in order to respect the correct inter-distance and TTC. If the TTC is lower or equal to 1s then the ego-vehicle is stopping	In the service deployed in this POC, the ego-vehicle keep the right lane (no lane change, no overtaking)

Table 9: List of the events encountering with an input from the Obstacles.



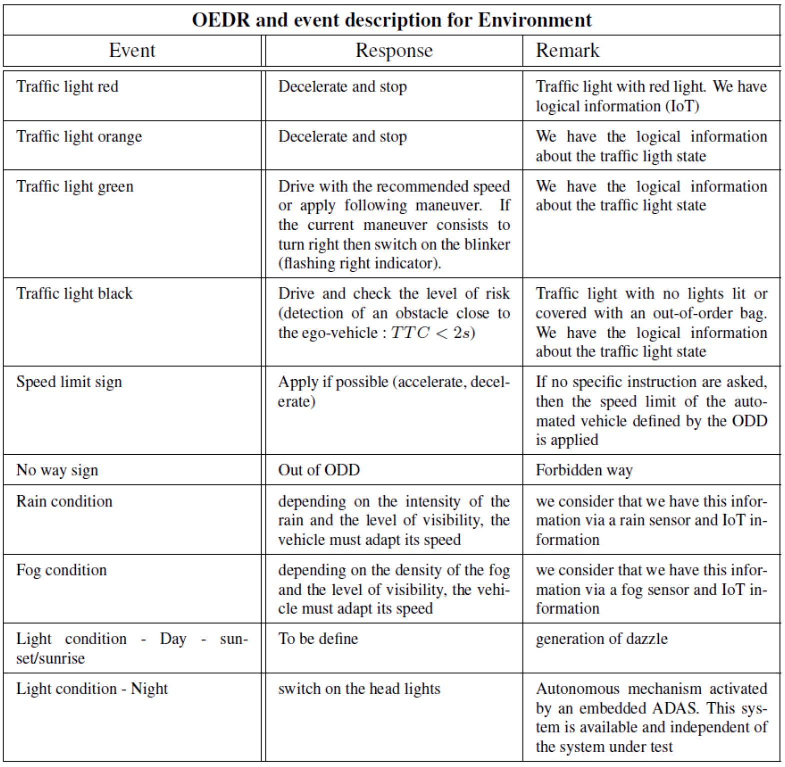
OEDR and event description for Ego-vehicle		
Event	Response	Remark
Ego-vehicle operating outside the ODD	Must be defined, may be generate a request to intervene (fallback-ready user)	Must be defined
To be define	Must be defined	Must be defined
To be define	Must be defined	Must be defined

Table 10: List of the events encountering with an input from the Ego-vehicle.



OEDR and event description for Road		
Event	Response	Remark
Presence of a speed bumper	Must be defined	Must be defined
Presence of a negative obstacle (pothole)	Must be defined	Must be defined
Pedestrian crossing way	Must be defined	Must be defined
Change of road marking type	Must be defined	Must be defined
Change of road curvature (bend)	Must be defined	Must be defined
Degradation of the visibility level / readability of road marking (soiling, ...)	Must be defined	Must be defined
Lack of marking	sidewalk edge detection	Available information (other embedded system, HD-Map)
Disturbers on the road surface (sand, gravel, soil, leaf, ...)	To be define	Possible occlusion of marking, production of artefact at the detection level
Speed limit sign	If necessary, the ego vehicle adapts its speed in order to respect the constraint. If the ego-speed is under the speed limit then the ego-vehicle keep the same behavior	The max speed of the ego-vehicle is provided by the ODD

Table 11: List of the events encountering with an input from the Road.



OEDR and event description for Environment		
Event	Response	Remark
Traffic light red	Decelerate and stop	Traffic light with red light. We have logical information (IoT)
Traffic light orange	Decelerate and stop	We have the logical information about the traffic ligth state
Traffic light green	Drive with the recommended speed or apply following maneuver. If the current maneuver consists to turn right then switch on the blinker (flashing right indicator).	We have the logical information about the traffic light state
Traffic light black	Drive and check the level of risk (detection of an obstacle close to the ego-vehicle : $TTC < 2s$)	Traffic light with no lights lit or covered with an out-of-order bag. We have the logical information about the traffic light state
Speed limit sign	Apply if possible (accelerate, decelerate)	If no specific instruction are asked, then the speed limit of the automated vehicle defined by the ODD is applied
No way sign	Out of ODD	Forbidden way
Rain condition	depending on the intensity of the rain and the level of visibility, the vehicle must adapt its speed	we consider that we have this information via a rain sensor and IoT information
Fog condition	depending on the density of the fog and the level of visibility, the vehicle must adapt its speed	we consider that we have this information via a fog sensor and IoT information
Light condition - Day - sunset/sunrise	To be define	generation of dazzle
Light condition - Night	switch on the head lights	Autonomous mechanism activated by an embedded ADAS. This system is available and independent of the system under test

Table 12: List of the events encountering with an input from the Environment.

So, about the different events identified in the 4 previous tables, a set of requirements has been identified:

i. **Requirement 13:** In degraded weather conditions, the vehicle has data sources to know the intensity of the event (rain, fog) and the visibility distance (for impacted sensors). This information is therefore produced by another actor.

ii. **Requirement 14:** The vehicle lighting system is managed automatically according to the conditions present in the environment.

iii. **Requirement 15:** The semantic state of traffic lights is considered known and available (Internet of Things or embedded system allowing this state to be detected). This information is therefore produced by another actor.

2.11.4 Relevant metrics

The assertion of the safety of AI based AS system will probably involve some KPI evaluating the quality of the tests taken on AD systems.

The relevant metrics which are necessary for the successful completion of the PRISSMA project are partially presented in the following parts, 3.1.1 Qualitative measures and the 3.1.2 Quantitative measures. The remainder metrics such as the choice of KPIs must be consistent with the ODD or ROD chosen for the test. In the case where the test procedure is proposed by the AI system manufacturer, an evaluation of the protocol and the chosen metrics will be essential.

3 Specific support elements for AI functions tests and demonstrations

In this paragraph we list very specific validation support elements and items which are for example key assumptions and factors documenting validation process for CAV systems including AI bricks.

3.1 Testing in simulated environment

3.1.1 Qualitative measures

First, it has to be mentioned that there are various forms of qualitative methods.

In the field of AI, reasoning based on causal modeling has been proposed. By definition, diagnosis is a causal process because its objective is to determine assumptions about the faulty elements that cause the observed malfunction. It has been defined that causal structure as "the effect or influence that system entities (e.g. variables, faults) have on each other". This structure can be represented in the form of a digraph such as a signed graph (ODD). This type of graph is composed of directed arcs leading from "cause" nodes to "effect" nodes. These arcs are associated with either a positive or negative sign.

Each node in the graph corresponds to events or variables in the system, and the edges represent relationships between the nodes. It is also possible to represent this type of structure with a causal graph. This type of graph is often called an influence graph. Each node of the graph corresponds to the variables of the system and the arcs represent the normal and deterministic relations between them. The objective of such a graph is to "find the source variable whose deviation is sufficient to explain all the deviations detected on other variables.

Another type of model is the bond-graph. This type of approach is considered in particular for modeling the dynamics of mechanical and electronic systems. It is possible to represent a complex system with an abstraction hierarchy. The objective is to deduct the behaviour of the system only from the laws defining the behaviour of the subsystems.

3.1.2 Quantitative measures

Foremost, different research works as well as the experimentation of shuttles and autonomous vehicles have allowed to define metrics on different spatial-temporal registers, as well as composite indicators. Their use or the production of other specific metrics depend on the model chosen by the designer, to drive the autonomous vehicle in an environment, with potentially existing AI bricks or specially designed to meet the functional requirements of the system engineering.

The following table gives an overview of the safety metrics adapted to the autonomous shuttle that can be used to identify and analyse a single situation, without being exhaustive. The source of it is the BPI France for the PRISSMA project, *Liv. 7.2 : Data analysis process and identification of single situations,* 12/01/2023 [8]

Metric [reference]	Acronym	Description	Inconvenience
Collision Event Probability (density)	CEP	The probability density of a collision event at a given time.	/
Collision State Probability	CSP	Probability of spatial overlap of two objects at a given time.	/
Crash Index	THIS	Influence of speed on the kinetic energy involved in collisions.	Describes only safety information about two vehicles at a given time and place. Not suitable for lane change or head-on collision. In addition, must rely on other approaches for data collection.
Crash potential Index	ICC	The probability that a given vehicle DRAC will exceed its maximum available deceleration rate during a given time interval.	Not suitable for lateral movements; mainly applicable at the intersection.
Criticality Index Function	CIF	Multiplication of vehicle speed with the required deceleration.	This indicator considers the constant speed of the consecutive vehicle.
Deceleration Rate to Avoid Collision	DRAC	Differential speed between a following/intervening vehicle and its corresponding subject/leading vehicle divided by their closing time	Fails to accurately identify the potential conflict situation. Also not suitable for lateral movements.
Difference of Space distance and Stopping distance	DSS	The difference between the space and the stopping distances. For instance, the space distance is the sum of differences between the leading and following vehicles. The braking distance of the leading vehicle and the stopping distance is the sum of the brake reaction distance and the braking distance of the following vehicle.	Provides information on the number of dangerous vehicles but does not take into account the degree of danger and the duration.
Gap Time	GT	Describes the potential for a collision. For example, a large positive GT would indicate that a long time duration exists between the end of encroachment and arrival of the through vehicle at the potential point of collision, and vice versa. Therefore one could assume that the severity of the conflict or the potential for a collision was indicated by the magnitude of the GT value.	/

Metric [reference]	Acronym	Description	Inconvenience
Inevitable Collision State	ICS	A state for which, no matter what the future trajectory followed by the system is, a collision with an obstacle eventually occurs.	/
Initially Attempt Post Encroachment Time	IAPT	The time from the start of the encroachment of the turning vehicle, plus the expected time for the passing vehicle to reach the collision point, to the end of the encroachment of the turning vehicle.	/
Injury severity score	ISS	This indicator is a medical score established to assess the severity of trauma.	/
Integrated Conflict Risk Indexes	ICRI	The conflict risk index can be divided into time indicators and an energy index. The time index reflects the risk probability of the traffic events (e.g., TTC), while the energy index reflects the severity of the traffic events (e.g., DRAC).	/
Inter-Vehicular Time	TIV	The time required for the EGO vehicle to travel the distance to the target at constant speed.	Difficult to use for several manoeuvres.
jerks	/	A composite of g-force and speed or a derivative of acceleration. Jerks evaluated the relationship between the left/right, accelerate/decelerate and composite g-force and mean speed and frequency of accidents.	/
J-Value	/	An accumulative safety indicator related to the accumulation of risk of vehicles inside a platoon. Its parameters values are obtained from individual vehicle data (e.g. time gap between two consecutive vehicles, and vehicular speed.	/
Lateral avoidance acceleration	VAC	Instantaneous lateral acceleration required to avoid a vehicle in its lane.	/
Longitudinal avoidance deceleration	DCC	The instantaneous longitudinal deceleration required to avoid a vehicle in its lane.	/
Margin to Collision	TCM	Represents the possibility of a collision if the preceding vehicle and the following one suddenly decelerates at the same time.	This indicator is identical to the stopping distance. It does not consider the reaction time of the following vehicle. It is a non-dimensional parameter.

Metric [reference]	Acronym	Description	Inconvenience
Modified Time to Collision	MTTC	Extension of the TCC. MTTC takes into account all potential longitudinal conflict scenarios due to acceleration or deceleration deviations.	Not suitable for lane changes or head-on collisions. In addition, this indicator does not reflect the severity of a collision.
Overall Collision Probability	OCP	Defines the collision probability of a trajectory during and beyond the planning horizon.	High calculated cost.
Post Encroachment Time	PET	The time between when a vehicle leaves the potential collision area and when the other vehicle arrives in the collision area.	Only useful for transverse trajectories (e.g. right angle collision). The severity level is not taken into account. Also, does not reflect dynamic changes in critical events.
Potential Index for Collision with Urgent Deceleration	PICUD	The distance between the two vehicles considered at a complete stop. PICUD assesses the possibility that two consecutive vehicles collide, assuming that the leading vehicle applies its emergency brake, especially during a lane change.	Mainly applicable in case of lane change when the leading vehicle applies emergency braking. In addition, this indicator does not take into account side conflicts.
Predicted Minimum Distance	PMD	The minimum distance between a vehicle and a potential obstacle predicted in real time	/
Probabilistic collision states	PCS	PCS is a probabilistic generalization of the ICS concept. Instead of checking for the existence of at least one collision-free path to a safe state, the collision probabilities of the paths are evaluated.	/
Proportion of Stopping Distance	PSD	The ratio of the remaining distance to the potential collision point to the minimum acceptable stopping distance.	Less focus on a specific safety issue as PSDs provide a greater percentage of vehicle interaction and conflict exposure time.
Proportion of stopping distance	PSD	Ratio between the remaining distance to the potential point of collision and the minimum acceptable stopping distance.	This indicator provides a greater percentage of interpolation between vehicles and time of exposure to conflict. This indicator is less focused on a specific safety issue.
region proportion	R-PROP	Occupancy rate of a danger zone.	/
Responsibility Sensitive Safety	RSS	Rigorous mathematical model that formalizes an interpretation of the "Duty of Care" of tort law applicable to self-driving cars.	/

Metric [reference]	Acronym	Description	Inconvenience
Road Safety Index [WP2-PRISSMA]	ROI	An indicator that is a function of the Injury Severity Score (ISS), traffic volume and number of accidents. It corresponds to a road safety indicator.	/
Standard Deviation of Lateral Position	SDLP	This measure is similar in nature to the degree of vehicle control that a driver exercises in a particular driving situation. SDLP is mainly suitable for driving simulator or instrumented vehicle studies, i.e. a naturalistic driving situation.	Not preferable in a static field measurement as an indicator of safety.
Time Exposed to Time to Collision	TFW	The summation of all times (over the considered period) that a driver approaches a front vehicle with a TTC below a threshold.	Does not provide the severity of the variation of the different TTC values below the threshold value. Threshold value. It requires a lot of data and is only feasible in a simulation environment.
Time Headway	H	The elapsed time between the front of the leading vehicle passing a point on the roadway and the front of the following vehicle passing the same point.	Mainly applicable in conflicts related to following manoeuvre and does not take into account conflicts due to lateral movements, such as changing lanes or overtaking.
Time Integrated DSS	TIDSS	Evaluates the safety of traffic flow by the total value of the time integrated value gap between DSS and the dangerous threshold value.	Mainly suitable for conflict from the rear.
Time Integrated Time to collision	TIT	Integral of the TTC-profile during the time when it is below the threshold.	/
Time to Crash	YOUR	The time left to an accident from when one of the road users starts an evasive action if they had continued at unchanged speed and directions.	Often criticized for relying heavily on subjective judgment of speed and distance. Rely mainly on avoidance. Other metric identical to TTC.
Time-to-Brake	VF	The time after which a braking manoeuvre has to be started to prevent the collision. If TTB is smaller than 0, collision cannot be avoided by braking.	/
Time To Closest Encounter	TTCE	The time remaining for the vehicle to react before the closet encounter point (and thus the maximum risk of collision) is reached.	/

Metric [reference]	Acronym	Description	Inconvenience
Time-to-Collision	tax included	The time that remains until a collision between two vehicles would have occurred if the collision course and speed difference are maintained.	Considering the speeds of the leading and following vehicles as constant does not capture the variations in speed due to acceleration and deceleration of vehicles. Furthermore, this indicator can provide an indication of magnitude but not severity.
Time to React	TTR	The time which is left to avoid the collision within the physical constraints of the vehicle.	/
Time to Steer	TTS	The time after which an evasive manoeuvre has to be started to prevent the collision. If the TTS is smaller than 0, a collision cannot be avoided by steering.	/
Unsafe Density	UD	Level of "unsafety" in the relationship between two consecutive vehicles on the road for a given simulation step.	The value of this parameter has no real application meaning in itself and should be used for comparison purposes only.

Table 13: Summary of safety metrics.

From another point of view, for example in the simulation environment, the expected results could be the following:

i. To define a generic and inter-operable simulation architecture allowing to replace, to add, to update tools and models (vehicles, sensors, environment, ...) with a generic method.
ii. To generate a set of accurate and relevant ground truth (segmentation of the environment, observers, depth map, etc...) in order to feed the evaluation and validation process.
iii. To develop an efficient and easy to use scenario manager involving a clear and scalable description of scenario generation based on a generic ODD framework.
iv. To propose a library of metrics (levels system, component, tool and model) and the generic process to use it in an evaluation and validation process.
v. To provide the capability to compare the real and virtual test process with the challenge to prove the representativeness of the simulation in comparison to the real-life.
vi. To develop a ViL platform with the capability to merge real and virtual data and environment
vii. To propose some models and ways in order to take into account degraded and adverse conditions, failures, and cyber-attack
viii. To propose a template of scenarios allowing to test the performances of AI-based systems

At this end, we will have to provide a fully operating ViL platform with the Top-Down design method allowing to evaluate and validate a service/system/application/component involving IA-based system.

3.1.3 Criteria and thresholds for metrics

In this part, the thresholds are presented trough a special way, the safety:

Safety as a threshold uses target values based on some kind of driving measurable performance or other metrics. It is a straightforward approach; however, consensus on the reference metrics and values could be difficult to achieve at least at the initial stage of ADS technology.

Safety as a threshold can be divided into categories based on the threshold definition: based on human drivers (careful driver, better-than-average driver, car technology level should be identified); based on ADS performance; based on absolute goals.

Despite being a straightforward approach, setting a threshold carries the risk of not pursuing technology development or setting overly ambitious goal.

The ALARA (As Low As Reasonably Achievable) /ALARP (As Low As Reasonably Practicable) principles are examples of risk acceptance method for safety as a threshold based on current data; whereas MEM (Minimum Endogenous Mortality), GAMAB (Globally At Least As Good) and Vision Zero are examples of acceptability criteria based on transportation-system-wide goals.

The safety as a threshold approach can be informed by measures or processes or considered on its own; it can be internal for developers, or external for other stakeholders; it can evolve as the technology develops, ADS usage expands, and expectations rise (see Figure 19 below). For the sake of clarity, this Appendix refers solely to the current text of Regulation 2022/1426, and the reader should not consider nor expect technological improvement to be reflected in the safety as a threshold demonstration at type approval. However, the manufacturers should be aware of the strategic framework in which the Regulation 2022/1426 was generated. So it is expected that the safety threshold will become stricter over the time. None of these approaches stands alone, the three approaches complement, support, and interact with each other. The aim of combining the approaches in Regulation 2022/1426 is to provide a common framework for both assessing and communicating ADS safety.

The combined approaches are also meant to sustain the future progress in road safety towards the Commission Vision Zero (close to zero fatalities on road by 2050).

Below is a figure from the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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*, 2022. [4]

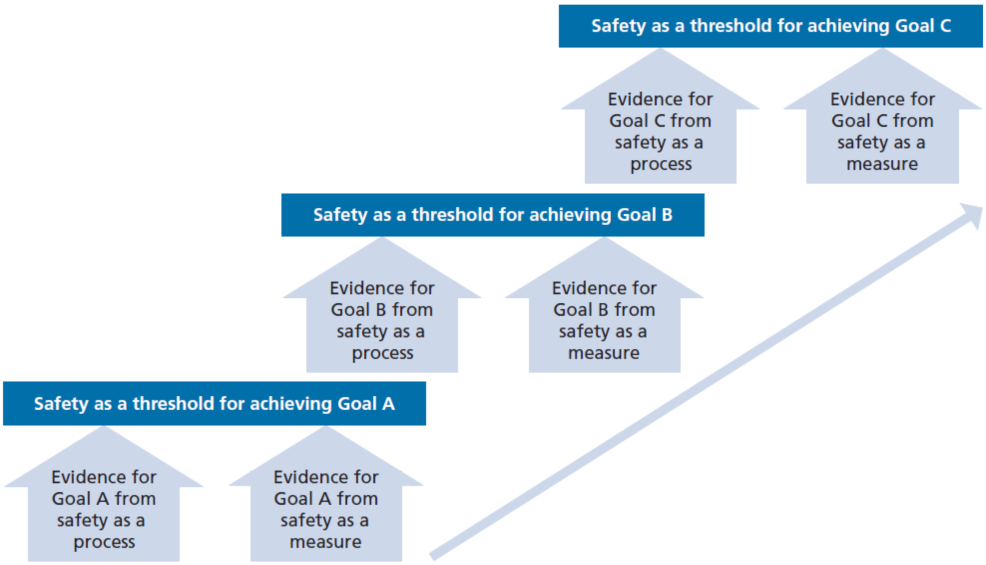

Safety as a threshold for achieving Goal C
Evidence for Goal C from safety as a process
Evidence for Goal C from safety as a measure
Safety as a threshold for achieving Goal B
Evidence for Goal B from safety as a process
Evidence for Goal B from safety as a measure
Safety as a threshold for achieving Goal A
Evidence for Goal A from safety as a process
Evidence for Goal A from safety as a measure

Figure 19: Improving goals scheme.

Methodologies for Demonstration of Safety as a Threshold (Acceptable Means of Compliance):

The present section provides guidance on the methodologies suitable to demonstrate compliance with the Regulation in relation to the safety as a threshold approach. It presents a collection of acceptable means of compliance, namely the methodologies that would be acceptable for the Type Approval Authorities. The content of this section is applicable on a voluntary basis and it is not intended to be exhaustive. Depending on the vehicle type defined by the vehicle manufacturer, and the practices and procedures they use, alternative and/or equivalent methodologies may be used and information may be supplied to comply with the requirements established in the Regulation.

Probabilistic Approach

This section reports an approach based on probabilistic assessment developed by JRC.

The proposed approach leverages the scenarios identified according to the ODD-based Framework approach and is used to derive a specific probability of occurrence for each scenario.

The first step is the identification of a set of safety-relevant parameters. Each parameter is then analyzed and subdivided into a number of different possible conditions (set values or ranges), obviously consistent with the ODD. The probability of occurrence of each condition for that particular parameter in that specific ODD is then evaluated. The probability can be based on actual data, engineering judgment or other type of evaluation.

A hypothetical example is provided in the following table coming from the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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,* 2022. [4]

Main parameters	**Conditions and probabilities**			
Road conditions	Dry 60%	Frozen 5%	Snow 15%	Wet 20%
Velocity of the vehicle	10-20 km/h 20%	20-40km/h 50%	40-60km/h 30%	
Meteorological conditions	Clear 40%	fog 20%	Rain 20%	Snow 20%
Type of possible obstacles	Animals 5%	Other vehicles 70%	Pedestrians 20%	Tracks 5%
Distance from possible obstacles *(e.g., vehicles suddenly cutting in in front of the ADS)*	1-10m 5%	10-20m 35%	20-40m 60%	
Relative velocity vehicle-obstacles	20-10km/h 15%	10-5km/h 50%	5-0km/h 35%	
Traffic conditions	50-20 coaches/km 20%	20-10 coaches/km 70%	<10 car/km 10%	
Failures (those are related to the system)	Main System 1%	Secondary System 2%	*Ancillary Systems 3%*	*No Failure 94%*

Table 14: Example of main parameters and their subdivision in conditions and related probability.

The second step implies the creation of a set of scenarios obtained by combining the possible conditions for each parameter. Each scenario has an associated probability of occurrence obtained by combining the probabilities of the conditions defining the scenario itself.

Not every possible combination of conditions results in acceptable scenarios; a consistency check of the scenarios generated has to be performed and unacceptable scenarios must be disregarded, namely: scenario characterized by contradictory conditions (e.g. road condition “Dry” and meteorological condition “Rain”), by combination of conditions not expected to occur (e.g., meteorological conditions “Fog” and the highest velocity of the vehicle). In addition, scenarios characterized by extremely low probability of occurrence can be neglected because they generate negligible risks.

As an example, using the data from the Table 14, the scenario defined by road: “Frozen”, velocity of the vehicle:10-20 km/h, meteorological: “Snow”, type of obstacle: “Animals”, distance from obstacles: “1-10 m”, relative velocity: “20-10 km/h”, traffic: “<10 cars/km”, failure: “Main system” has a probability of occurrence equal to 7.5·10-11, and therefore it can be neglected.

The following figure depicts a logical scheme of the scenario generation process described above. The source of it is the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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*, 2022. [4]

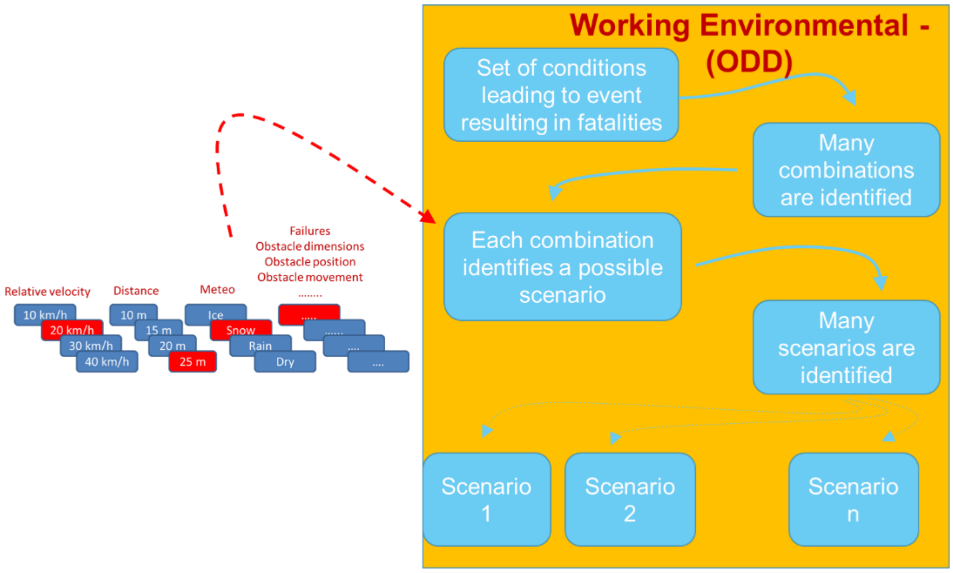


Figure 20: Flowchart of scenarios generation.

The following step is the categorization of the scenarios obtained so far. The purpose is twofold:

i. Grouping similar scenarios for an easier management.
ii. Identifying the most relevant scenarios (so-called “limiting scenarios”) within each category.

A limiting scenario is a scenario that envelops other scenarios and that is acknowledged to be challenging for the system.

Each limiting scenario is accompanied by a probability of occurrence. Higher probability identifies the scenarios that imply larger demand for the system in terms of safety, and, as a consequence, also identify what are the margins and the “directions” to spend efforts on improving system safety.

As an example, using the data in the Table 14, the most probable scenario (road: “Dry”, velocity of the vehicle:”20-40 km/h”, meteorological: “Clear”, type of obstacle: “Other vehicle ”, distance from obstacles: “20-40 m”, relative velocity: “10-5 km/h”, traffic: “20-10 cars/km”, failure: “no failure”) has a probability of occurrence of about 0.016. The maximum effort for safety improvement and future development of the system should be focused on this scenario.

The requirements imposed by the regulatory authority or selected by the system manufacturers must be verified for each of the limiting scenario.

In particular, if only conditions potentially causing a specific damage (e.g. death, injuries) are selected, the probability of occurrence of the resulting scenarios can be used as criteria for safety evaluation.

As an example, let assume that the following combination of conditions potentially causes a specific damage (e.g., death):

i. Road: “Frozen” (probability 0.05).
ii. Velocity: “50-60 km/h” (probability 0.1).
iii. Weather: “Snow” (probability 0.01).
iv. Minimal distance from a pedestrian before breaking: “10-20 m” (probability 0.01).

Assuming also as irrelevant the probability of the type of obstacle (pedestrian) and irrelevant all the other conditions probability, the probability of the scenario composed by those conditions is 5·10-7. This value can be compared with a reference value for safety acceptability.

Metrics for the definition of the safety threshold:

The Regulation does not define a specific metric to be adopted by the manufacturer. The manufacturer is allowed to use any metric (as well as any acceptance criteria and approach) provided that is able to demonstrate that its use does not decrease the safety level in comparison with similar services in the same operational environment, “ taking into account, *where available, existing accident data”* .

Fatality Rate

The Regulation uses the concept of validation targets and global safety threshold for the acceptability of the residual risk. The example of acceptance criteria indicated in the footnote of Paragraph 7.1.1 in based on the analysis of current EU road accidents aggregated data and relied on a metric based on the number of fatalities per hour of operation. The threshold is then set to 10^{-7} (fatalities per hour of operation).

Such metric and threshold are suitable for the market introduction of ADS, since they have been extrapolated from available state-of-the-art.

The manufacturer is in charge of the identification and selection of similar services and situations for the evaluation of the current level of risk of those services in similar ODD. Such risk can be extrapolated by analysing available data. A collection of available data and databases is reported in section 5 below.

3.1.4 Determination of the need of making an AI bricks diagnosis after a simulated environment test

As a reminder, the objective of this tool of recommendation or decision represented in a preliminary way by a matrix (cf. Table 15), is based on the more or less unfavourable combination of metrics or failures of a system (or sub-system, component), or of an AI brick whatever its function, which have been linked, accumulated or not, to reach a driving situation characterized by an incident (irrelevant behaviour), a near miss or an accident.

The metrics listed below are those used in the process to assess the behaviour of the shuttle and the state of its components in order to determine whether the failure is related to a bug in an AI brick.

i. The reaction time of the vehicle, compared to the human ability to react in less than 1 second (metric associated with OEDR).
ii. A safety metric relating to the shuttle's protection zone, an object passes the perimeter of this zone, which can for example be an ellipse and moves away from it (the metric

value increases⬆ or the object approaches the vehicle inside the safety perimeter (the metric value decreases⬇).

iii. The state of a sensor that may be defective or have an embedded AI brick that is malfunctioning (Bug).

iv. The location of the shuttle in relation to its ODD (IN or OUT).

v. The state of one or all AI bricks that make up the fusion, decision and response functionalities of the shuttle.

The recommendation or decision to be taken is characterized by:

i. The realization of an AI diagnosis (generic recommendation to be improved according to the architectures and the nature of the embedded AI).

ii. Carrying out a classic failure diagnosis and an FMEA.

iii. Corrective analysis of the system engineering phases.

iv. No particular action because the shuttle behaviour was nominal.

Below is a table from the BPI France for the PRISSMA project, *Liv. 7.2: Data analysis process and identification of single situations*, 12/01/2023. [8]

Response Time metric	Detection failure 1/n		Shuttle's Behaviour/ ODD		Safety Metric 1/n		Merger, decision Response process		Single-situation			Instructions of maintenance
	Tech	AI	IN	OUT	⬆	⬇	No bug AI	AI Bug	Incident	near miss	Accident	
> 1 sec.			X		X							System Eng.
> 1 sec.		X		X								System Eng.
> 1 sec.			X			X	X		X			System Eng.
> 1 sec.				X	X		X		X			System Eng.
> 1 sec.				X		X	X		X			System Eng.
> 1 sec.			X		X		X		X			System Eng.
> 1 sec.				X	X			X	X			Diagnosis AI
> 1 sec.				X		X		X	X			Diagnosis AI
> 1 sec.	X		X		X		X		X			RAS
> 1 sec.		X	X		X		X		X			Diagnosis AI
> 1 sec.	X			X	X		X		X			Diagnosis AI
> 1 sec.		X		X	X		X		X			Diagnosis AI
> 1 sec.	X		X		X			X	X			Diagnosis AI
> 1 sec.		X	X		X			X	X			Diagnosis AI
> 1 sec.	X			X	X			X	X			Diagnosis AI
> 1 sec.		X		X	X			X	X			Diagnosis AI
> 1 sec.	X		X			X	X		X			RAS

Response Time metric	Detection failure 1/n		Shuttle's Behaviour/ ODD		Safety Metric 1/n		Merger, decision Response process		Single-situation			Instructions of maintenance
	Tech	AI	IN	OUT	⬆	⬇	No bug AI	AI Bug	Incident	near miss	Accident	
> 1 sec.		X	X			X	X		X			Diagnosis AI
> 1 sec.	X			X		X	X		X			??
> 1 sec.		X		X		X	X		X			Diagnosis AI
> 1 sec.	X		X			X		X	X			Diagnosis AI
> 1 sec.		X	X			X		X	X			Diagnosis AI
> 1 sec.	X			X		X		X	X			Diagnosis AI
> 1 sec.		X		X		X		X	X			Diagnosis AI
> 1 sec.			X		X		X			X		Diagnosis / FMEA
> 1 sec.			X			X	X			X		Diagnosis / FMEA
> 1 sec.				X	X		X			X		Diagnosis /
> 1 sec.				X		X	X			X		FMEA
> 1 sec.			X		X		X			X		Diagnosis /
> 1 sec.			X			X	X			X		FMEA
> 1 sec.				X	X			X		X		Diagnosis AI
> 1 sec.				X		X		X		X		Diagnosis AI
> 1 sec.	X		X		X		X			X		Diagnosis AI
> 1 sec.		X	X		X		X			X		Diagnosis AI
> 1 sec.	X			X	X		X			X		???
> 1 sec.		X		X	X		X			X		Diagnosis AI
> 1 sec.		X	X		X			X		X		AI Diagnosis
> 1 sec.	X			X	X			X		X		Diagnosis AI
> 1 sec.		X		X	X			X		X		Diagnosis AI
> 1 sec.	X		X			X	X			X		???
> 1 sec.		X	X			X	X			X		Diagnosis AI
> 1 sec.	X			X		X	X			X		Diagnosis / FMEA
> 1 sec.		X		X		X	X			X		Diagnosis AI
> 1 sec.	X		X			X		X		X		Diagnosis AI
> 1 sec.		X	X			X		X		X		Diagnosis AI
> 1 sec.	X			X		X		X		X		Diagnosis AI
> 1 sec.		X		X		X		X		X		Diagnosis AI

Response Time metric	Detection failure 1/n		Shuttle's Behaviour/ ODD		Safety Metric 1/n		Merger, decision Response process		Single-situation			Instructions of maintenance
	Tech	AI	IN	OUT	⬆	⬇	No bug AI	AI Bug	Incident	near miss	Accident	
> 1 sec.			X		X		X				X	Diagnosis / FMEA
> 1 sec.			X			X	X				X	Diagnosis / FMEA
> 1 sec.				X	X		X				X	Diagnosis / FMEA
> 1 sec.				X		X	X				X	Diagnosis / FMEA
> 1 sec.			X		X		X				X	???
> 1 sec.			X			X	X				X	Diagnosis / FMEA
> 1 sec.				X	X			X			X	Diagnosis AI
> 1 sec.				X		X		X			X	Diagnosis AI
> 1 sec.	X		X		X		X				X	Diagnosis / FMEA
> 1 sec.		X	X		X		X				X	Diagnosis AI
> 1 sec.	X			X	X		X				X	Diagnosis / FMEA
> 1 sec.		X		X	X		X				X	Diagnosis AI
> 1 sec.	X		X		X			X			X	Diagnosis AI
> 1 sec.		X	X		X			X			X	Diagnosis AI
> 1 sec.	X			X	X			X			X	Diagnosis AI
> 1 sec.		X		X	X			X			X	Diagnosis AI
> 1 sec.	X		X			X	X				X	Diagnosis / FMEA
> 1 sec.		X	X			X	X				X	Diagnosis AI
> 1 sec.	X			X		X	X				X	Diagnosis / FMEA
> 1 sec.		X		X		X	X				X	Diagnosis AI
> 1 sec.	X		X			X		X			X	Diagnosis AI
> 1 sec.		X	X			X		X			X	Diagnosis AI
> 1 sec.	X			X		X		X			X	Diagnosis AI
> 1 sec.		X		X		X		X			X	Diagnosis AI
< 1 sec.			X		X		X		X			Diagnosis / FMEA
< 1 sec.			X			X	X		X			Diagnosis / FMEA
< 1 sec.				X	X		X		X			Diagnosis / FMEA

Response Time metric	Detection failure 1/n		Shuttle's Behaviour/ ODD		Safety Metric 1/n		Merger, decision Response process		Single-situation			Instructions of maintenance
	Tech	AI	IN	OUT	⬆	⬇	No bug AI	AI Bug	Incident	near miss	Accident	
< 1 sec.				X		X	X		X			????
< 1 sec.			X		X		X		X			Diagnosis / FMEA
< 1 sec.			X			X	X		X			???
< 1 sec.				X	X			X	X			Diagnosis AI
< 1 sec.				X		X		X	X			Diagnosis AI
< 1 sec.	X		X		X		X		X			Diagnosis / FMEA
< 1 sec.		X	X		X		X		X			Diagnosis AI
< 1 sec.	X			X	X		X		X			???
< 1 sec.		X		X	X		X		X			Diagnosis AI
< 1 sec.	X		X		X			X	X			Diagnosis AI
< 1 sec.		X	X		X			X	X			Diagnosis AI
< 1 sec.	X			X	X			X	X			Diagnosis AI
< 1 sec.		X		X	X			X	X			Diagnosis AI
< 1 sec.	X		X			X	X		X			???
< 1 sec.		X	X			X	X		X			Diagnosis AI
< 1 sec.	X			X		X	X		X			???
< 1 sec.		X		X		X	X		X			Diagnosis AI
< 1 sec.	X		X			X		X	X			Diagnosis AI
< 1 sec.		X	X			X		X	X			Diagnosis AI
< 1 sec.	X			X		X		X	X			Diagnosis AI
< 1 sec.		X		X		X		X	X			Diagnosis AI
< 1 sec.			X		X		X			X		Diagnosis / FMEA
< 1 sec.			X			X	X			X		Diagnosis / FMEA
< 1 sec.				X	X		X			X		Diagnosis / FMEA
< 1 sec.				X		X	X			X		Diagnosis / FMEA
< 1 sec.			X		X		X			X		Diagnosis / FMEA
< 1 sec.			X			X	X			X		Diagnosis / FMEA
< 1 sec.				X	X			X		X		Diagnosis AI
< 1 sec.				X		X		X		X		Diagnosis AI

Response Time metric	Detection failure 1/n		Shuttle's Behaviour/ ODD		Safety Metric 1/n		Merger, decision Response process		Single-situation			Instructions of maintenance
	Tech	AI	IN	OUT	⬆	⬇	No bug AI	AI Bug	Incident	near miss	Accident	
< 1 sec.	X		X		X		X			X		Diagnosis / FMEA
< 1 sec.		X	X		X		X			X		Diagnosis AI
< 1 sec.	X			X	X		X			X		Diagnosis AI
< 1 sec.		X		X	X		X			X		Diagnosis AI
< 1 sec.	X		X		X			X		X		Diagnosis AI
< 1 sec.		X	X		X			X		X		Diagnosis AI
< 1 sec.	X			X	X			X		X		Diagnosis AI
< 1 sec.		X		X	X			X		X		Diagnosis AI
< 1 sec.	X		X			X	X			X		Diagnosis / FMEA
< 1 sec.		X	X			X	X			X		Diagnosis AI
< 1 sec.	X			X		X	X			X		Diagnosis / FMEA
< 1 sec.		X		X		X	X			X		Diagnosis AI
< 1 sec.	X		X			X		X		X		Diagnosis AI
< 1 sec.		X	X			X		X		X		Diagnosis AI
< 1 sec.	X			X		X		X		X		Diagnosis AI
< 1 sec.		X		X		X		X		X		Diagnosis AI
< 1 sec.			X		X		X				X	Diagnosis / FMEA
< 1 sec.			X			X	X				X	Diagnosis / FMEA
< 1 sec.				X	X		X				X	Diagnosis / FMEA
< 1 sec.				X		X	X				X	Diagnosis / FMEA
< 1 sec.			X		X		X				X	Diagnosis / FMEA
< 1 sec.			X			X	X				X	Diagnosis / FMEA
< 1 sec.				X	X			X			X	Diagnosis AI
< 1 sec.				X		X		X			X	Diagnosis AI
< 1 sec.	X		X		X		X				X	Diagnosis / FMEA
< 1 sec.		X	X		X		X				X	Diagnosis AI

Response Time metric	Detection failure 1/n		Shuttle's Behaviour/ ODD		Safety Metric 1/n		Merger, decision Response process		Single-situation			Instructions of maintenance
	Tech	AI	IN	OUT	⬆	⬇	No bug AI	AI Bug	Incident	near miss	Accident	
< 1 sec.	X			X	X		X				X	Diagnosis / FMEA
< 1 sec.		X		X	X		X				X	Diagnosis AI
< 1 sec.	X		X		X			X			X	Diagnosis AI
< 1 sec.		X	X		X			X			X	Diagnosis AI
< 1 sec.	X			X	X			X			X	Diagnosis AI
< 1 sec.		X		X	X			X			X	Diagnosis AI
< 1 sec.	X		X			X	X				X	Diagnosis / FMEA
< 1 sec.		X	X			X	X				X	Diagnosis AI
< 1 sec.	X			X		X	X				X	Diagnosis / FMEA
< 1 sec.		X		X		X	X				X	Diagnosis AI
< 1 sec.	X		X			X		X			X	Diagnosis AI
< 1 sec.		X	X			X		X			X	Diagnosis AI
< 1 sec.	X			X		X		X			X	Diagnosis AI
< 1 sec.		X		X		X		X			X	Diagnosis AI

Table 15: Tool for determining whether a diagnosis of AI bricks is necessary after a real driving.

This example of a tool is based on criteria that have been subject to arbitration concerning the choice of metrics, failures and the operational context. However, each autonomous shuttle manufacturer retains the initiative to establish his own evaluation and decision tool according to the system architecture, the system engineering developed for both the physical system and the inclusion of an AI brick architecture. The main thing is to identify each incident, near miss or accident situation without fail and to be able to exploit the parameters of the last few tens of seconds preceding this situation (this time will depend on the technology used and the choice of manufacturers). The time taken to archive all the driving parameters will be developed in a dedicated section.

3.1.5 Method of diagnosis and correction of AI bricks

The learning models of the AI bricks of the autonomous driving system require diagnosis when failure cases are encountered during the use of the autonomous vehicle. These learning models have to follow an elaborate testing and approval process to avoid accidents. This process is time consuming and can take up to 6 months to 1 year for each update. However, we expect that customers will always encounter failures that are underrepresented in the training data and not taken into account in the test data or due to missing features in the learning model.

Thus, an important issue facing autonomous vehicle companies is the maintenance of the autonomous software of AI bricks between major software updates, in order to fix the driving behaviour of the autonomous module on the encountered failure cases or to add the requested missing functionalities of the model without the need to validate the whole system from the beginning. We believe that the diagnosis and maintainability of learning models are important challenges for the success of autonomous shuttles. The maintainability of autonomous driving systems must correct the failures of the learning models without changing the driving behaviour over all the kilometres that have been successfully driven before.

3.1.6 Support for testing in a simulated environment

Virtual testing can be used in different phases of the ADS development and validation.

Indeed, virtual testing can be used to explore in a comprehensive and cost-effective way an ADS (or of part of it) in a wide range of traffic scenarios across different ODD and for a variety of additional purposes. Relying on simulation, virtual testing is particularly indicated to test the ADS under safety critical scenarios that would be difficult and/or unsafe to reproduce on test tracks or public roads.

Virtual testing includes replacing one or more physical elements characterized in a scenario-based test by a simulation model. The goal of such virtualization is to resemble, to a sufficient extent, the original physical elements. For automotive applications, virtual testing can be used to reproduce the driving environment and the objects operating therein that interact with either the entire system (e.g. a full vehicle with tires and ADS functions), a subsystem (e.g. an actuator or a hardware controller), or a component (e.g. a sensor).

Through this approach, an assessor can get confidence about the ADS based on the virtual tests and validation that was performed by the developer in an agile, controllable, predictable, repeatable, and efficient manner.

The simulation toolchain used for virtual testing may result in the combination of different approaches. In particular, tests can be performed:

i. Entirely inside a computer (referred to as Model or Software in the Loop testing, MIL/SIL), with the model of the elements involved (e.g. a simple representation of the control logic of an ADS) interacting in a simulated environment.

ii. With a sensor, a subsystem, or the whole vehicle interacting with a virtual environment (Hardware or Vehicle in the Loop testing, HIL/VIL). For VIL testing, the vehicle can either be in:
   - A laboratory where the vehicle would be standing still or moving on a chassis dynamometer or powertrain test bed and be connected to the environment model by wire or by direct stimulation of its sensors;
   - A proving ground where the vehicle would be connected to an environment model and would interact with virtual objects by physically moving on the test-track.

iii. With a subsystem interacting with a real driver (DIL testing).

The interaction between the system under the test and the environment can either be an open- or closed-loop.

i. Open-loop virtual tests (also referred to as software or hardware reprocessing, shadow mode, etc.) could be done through a variety of methods, such as the ADS interacting with virtual situations collected from the real world. In this case, virtual objects' actions are data-driven only and the information is not self-corrected based on feedback from the output. Because the open-loop controller may vary due to external disturbances without the ADS and/or the assessor being aware, the applicability of open-loop tests in the ADS validation may be limited.

ii. Closed-loop virtual tests includes a feedback loop that continuously sends information from the closed-loop controller to the ADS. Within these test systems, the behaviour of the digital objects could react in different ways depending on the action of the system under test.

Selecting an open- or closed-loop test could depend on factors such as the objectives of the virtual testing activity and the status of development of the system under test. For ADS validation it is expected that mainly closed-loop virtual testing will be considered.

Below is a table from the VMAD, *New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS),* 2022. [27]

Benefits	Disadvantages
• controllability of all test aspects/parameters; • agility: system changes can be re-evaluated immediately; • efficiency: virtual tests can be generated in accelerated mode, allowing more tests to be performed in a shorter period of time; • profitability: the operating costs linked to the use of the tool chain are low compared to physical tests, despite the development, validation and maintenance investments; • large coverage of scenarios by a variety of testable combinations, making it possible to reduce the " unknown " space; • data collection and analysis facilitated by a recovery platform; • repeatability and replicability.	• lower reliability/fidelity of the environment and of the responses associated with elements outside the system; • sure-trust risk; • costly software life cycle.

Table 16: Strengths and weaknesses.

Virtual testing will have strong relationships with other elements. In particular:

i. Virtual testing expands the scope of physical testing to account for the diversity of traffic. The strength of virtual testing lies in its ability to cost-effectively assess performance across ranges of variables and arrays of scenarios. Virtual testing enables results of limited physical tests to be supplemented by verifiable data covering variations on the physical test scenario. Virtual testing enables coverage of safety-critical scenarios at their logical abstraction levels, confirming that an ADS will perform as intended across the parameter ranges. These advantages reduce the burden on physical tests (offsetting their weaknesses) to improve the efficiency of the overall assessment. Virtual testing can also be effectively used to identify and cover edge cases and other low-probability scenarios to increase confidence on their performances.

ii. Virtual testing can play an important role in the development of performance requirements and traffic scenarios. Virtual testing also enables assessment of ADS performance boundaries, enabling precision of limits between collision avoidance and crash mitigation. Through methods of randomization and compositions, virtual testing enables the developer or the assessor to challenge the ADS with unexpected, unplanned scenarios, and thus increases the confidence in the performance of the ADS when challenged with low probability events.

iii. Virtual testing will be a key element in the audit assessment. Results of virtual testing carried out both during vehicle development and in the verification and validation phase will represent an important element to be subject to audit. Manufacturers will need to provide evidence and documentation about how the virtual testing is carried out and how the underlying simulation toolchain has been validated.

iv. Real-world tests can aid in the generation of realistic simulation models and in establishing their accuracy:
  - Real-world data for vehicle and component model validation: vehicle data and data measured via vehicle sensors are important sources for quantifying and arguing model accuracy (e.g. vehicle dynamics or sensor models).
  - Real-world data for traffic modelling: the generation of novel scenarios requires realistic road user behaviour for the simulation environment to remain meaningful and representative.

v. Virtual testing can play an important role in responding to concerns identified through in-use monitoring of ADS performance. Virtual testing provides speed and flexibility in analysing real-world events to verify ADS performance against such events and, if necessary, support modifications to improve performance. Scenario descriptions can be shared and integrated rapidly into virtual testing regimes worldwide. The various types of virtual testing, including HIL methods that come close to matching physical testing, ensure robust and rapid responses.

Also, the life cycle of a successful simulation study should follow different steps. Here they are listed by categories.

Platform and model description:
REQ#144: 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 modelled, the time frame of the simulation campaigns and the required resources).

Technical solutions:
REQ#145: All alternative techniques, tools and languages that have been used to perform the simulation shall be identified
REQ#146: The technique with the highest estimated benefits/cost ratio shall be justified.
REQ#147: Characteristics of the competitive platforms that comply with the formulated objectives shall be investigated for consideration in platform definition and specification.

Specification model:
REQ#148: The conceptual model of the simulation platform shall be formulated with tools, connectors and languages mentioned in it.
REQ#149: 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#150: 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:

i. It can be developed faster
ii. It is more flexible
iii. It requires less data
iv. It runs faster

v. It simulation results are better understood since the structure of the model is less complex

vi. The conceptual model should include detailed description of each module, and their interactions above all concerning data exchange and time sampling process

vii. The simplifying assumptions should be communicated and justified

Communicative and workflow exchange model:

REQ#151: A communicative model shall be addressed in order to represent the conceptual model to tools and information repository of the project team for validation.

REQ#152: If there are any errors or omissions, the conceptual model must be updated before processing result of simulation.

REQ#153: 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.

REQ#154: The conceptual model shall be validated by the client(s).

REQ#155: Designers and clients shall confirm the utility of the conceptual model, ensuring that it can be developed into a useful computer model, e.g., as a decision aid in the specific context.

REQ#156: 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

Use Case Requirements:

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

Simulation Requirements:

REQ#157: Sensitivity analyzes should 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 modelled carefully.

REQ#158: The results of the simulation with the modelled vehicle should be analyzed and it should be decided whether additional experiments (controlled testing or real testing) or another system to be modelled to study an alternative solution to the problem are needed.

REQ#159: The building/validation process of the simulation campaigns, the computer pro-gram, and the results/conclusions for the safety analysis should be discussed and documented with rationale and graphic animation if needed.

3.2 Testing in controlled environment

3.2.1 Qualitative measures

The qualitative measurements that have to be done during a controlled environment are the same as presented in the 3.1.1 Qualitative measures from the Testing in simulated environment subpart.

3.2.2 Quantitative measures

The quantitative measurements that have to be done during a controlled environment are the same as presented in the 3.1.2 Quantitative measures from the Testing in simulated environment subpart.

3.2.3 Criteria and thresholds for metrics

The criteria and thresholds for metrics that have to be defined during a controlled environment are the same as presented in the 3.1.3 Criteria and thresholds for metrics from the Testing in simulated environment subpart.

3.2.4 Determination of the need of making an AI bricks diagnosis after a controlled environment test

The determination of the need of making an AI bricks diagnosis that have to be done during a controlled environment test are the same as presented in the 3.1.4 Determination of the need of making an AI bricks diagnosis after a simulated environment test from the Testing in simulated environment subpart.

3.2.5 Method of diagnosis and correction of AI bricks

The method of diagnosis and correction of AI bricks that have to be applied during a controlled environment test are the same as presented in the 3.1.5 Method of diagnosis and correction of AI bricks from the Testing in simulated environment subpart.

3.2.6 Support for testing in a controlled environment

These tests use a restricted-access test track to evaluate various test scenarios to verify the capabilities and operation of an automated driving system under controlled conditions of the test site's controlled environment.

Track tests in a closed and controlled environment make it possible to test the capacities and operation of the system under study under a set of parameterized scenarios.

Closed, controlled and safe environment test track testing uses real obstacles and obstacle surrogates (e.g. impactables targets representing vehicles, pedestrians) to assess the safety requirements of a system. These inputs and external conditions can be controlled or measured during a test, allowing high repeatability and accuracy.

Track testing can usefully be used to assess system performance in a number of selected significant nominal and critical scenarios, including with respect to the human factor and its interactions or minimal risk manoeuvres and emergency manoeuvres. Track testing can accelerate exposure to known rare events or safety-critical scenarios in a more controlled and safer environment. Track testing may be more appropriate for evaluating system capabilities in a discrete number of nominal scenarios and critical scenarios.

An initial review of practices, procedures, technical resources and tool chains relating to test track testing was carried out by the dedicated VMAD sub-group. This highlights that a multitude of test procedures and standards have been developed for the verification of vehicles equipped with automated driving systems and in particular driving assistance systems, which can serve as a basis for the design of track test methodologies.

On the other hand, it also appears that no procedure for evaluating the safety of vehicles with automated driving systems on roads open to public traffic has been developed.

The starting point for the development of test methods, whether on the test track or on the open road, is the test matrix approach. This approach recommends the use of a general matrix for physical tests, as well as two test matrices specifically designed for track tests and real-world tests respectively.

The purpose of the general matrix is to provide a clear overview of the safety requirements, whether for track or open road testing, or both. The test matrices, respectively for track testing and real-world testing, would be of different design, in order to take into account the different contexts in which the tests are carried out, as well as to ensure that the strengths of each method test can be used.

The general matrix gives an overview of the type or types of tests to be carried out to assess compliance with the safety requirements. The general matrix gives a list of high-level requirements on general safety such as "the system must fully perform the dynamic driving task" or "the system must control the longitudinal and lateral movements of the vehicle", which will then have to (or not) follow through on physical road testing. These high-level requirements will be supplemented by pass / fail criteria.

The on-track test matrix will be a variation of the general matrix by incorporating both scenarios making it possible to meet high-level requirements, safety requirements on the state and responses of the system, additional specifications (minimum duration of test, particular parameters) and the evaluation of the specifications.

Information generated during track testing can usefully be used as data to validate virtual testing by comparing the system's performance in a virtual test with its performance on a test track when running the same scenario.

The following table coming from the DGITM/DMR/TUD, *Utilisation des scénarios pour la démonstration de la sécurité des systèmes de transports routiers automatisés,* 2023 [31] outlines the pros and cons of this pillar of test track testing.

Benefits	Disadvantages
• controllability: many aspects of the tests are controlled , including certain aspects of the ODD; • fidelity: the systems integrated in the tests are realistic; • reproducibility: test cases can be reproduced in different places by different test entities; • repeatability: multiple iterations can be performed with the same parameters, under the same conditions; • efficiency: closed-loop testing can accelerate exposure to known rare events or safety-critical scenarios by setting them up as explicitly designed test scenarios; • track testing can be used to validate the quality of the simulation tool chain by comparing a system's performance under simulation testing with its performance on a test track when running of the same scenario.	• significant time: a test may require a lot of time for setting and execution; • costly: personnel required and cost of the devices used; • limited variability: the infrastructure and the construction conditions can be difficult to implement and can be restricted (geometries, dimensions, etc.); • Safety risks: Track testing with physical vehicles and real obstacles is a potentially uncertain and dangerous environment for participants. • limited representativeness even with increased fidelity (example of pedestrians represented by mannequins).

Table 17: Pros and Cons of the track testing process.

Now, according to the *L6.4 - WP6 - Integration of AI specifications into design standards* document done by BPI France for the PRISSMA project (cf. [6]), this section initiates testing requirements, but is subject to evolution in the next version taking input from other Work Packages of PRISSMA.

The Technical Service shall ensure that the ADS is subject to at least the tests outlined in this section. 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.

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

Test conditions

REQ#160: The tests shall be performed under conditions (e.g. environmental, road geometry) that allow the operation of MV (urban shuttle, delivery robot).

REQ#161: 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#162: The test surface shall afford at least the adhesion required by the scenario in order to achieve the expected test result.

Test Targets

REQ#163: 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. The reference point for the location of the vehicle shall be the most rearward point on the centerline of the vehicle.

REQ#164: The target used for the Powered-Two-wheeler tests shall be a test device according to ISO CD 19206-5 or a type approved high volume series production motorcycle of Cate-gory 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#165: 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.

REQ#166: Details that enable the target(s) to be specifically identified and reproduced shall be recorded in the vehicle type approval documentation.

Test parameter variation

REQ#167: The manufacturer shall declare the system boundaries to the Technical Service. 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.

If this is deemed justified, the Technical Service may test additionally any other combination of parameters.

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.

Now, test scenarios to assess the performance of the system with regard to the dynamic driving task:

Lane Keeping

REQ#168: 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#169: The test shall be executed at least:

i. With a minimum test duration of 5 minutes.
ii. With a passenger car target as well as a PTW target as the lead vehicle / other vehicle.
iii. With a lead vehicle swerving in the lane.
iv. With another vehicle driving close beside in the adjacent lane.

Avoid a collision with a road user or object blocking the lane

REQ#170: 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 sys-tem.

REQ#171: This test shall be executed at least:

i. With a stationary passenger car target.
ii. With a stationary powered two-wheeler target.
iii. With a stationary pedestrian target.
iv. With a pedestrian target crossing the lane with a speed of 5 km/h.
v. With a target representing a blocked lane.
vi. With a target partially within the lane.
vii. With multiple consecutive obstacles blocking the lane (e.g. in the following order: ego-vehicle -motorcycle - car).
viii. We have a curved section of road.

Following a lead vehicle

REQ#172: 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#173: This test shall be executed at least:

i. Across the entire speed range of the MV.
ii. 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.
iii. For constant and varying lead vehicle velocities (e.g. following a realistic speed profile from existing driving database).
iv. For straight and curved sections of road.
v. For different lateral positions of lead vehicle in the lane.
vi. With a deceleration of the lead vehicle of at least 6 m/s2 mean fully developed deceleration until standstill.

Lane change of another vehicle into lane

REQ#174: The test shall demonstrate that the MV is capable of avoiding a collision with a vehicle cutting into the lane of the MV vehicle up to a certain criticality of the cut-in manoeuvre.

REQ#175: The criticality of the cut-in manoeuvre shall be determined according to TTC, longitudinal distance between rear-most point of the cutting in vehicle and front-most point of the MV vehicle, the lateral velocity of the cutting-in vehicle and the longitudinal movement of the cutting-in vehicle, as defined in paragraph REQ#78 of this Regulation.

REQ#176: This test shall be executed taking into consideration at least the following conditions:

i. For different TTC, distance and relative velocity values of the cut-in manoeuvre, covering types of cut-in scenarios in which a collision can be avoided and those in which a collision cannot be avoided.
ii. For cutting-in vehicles traveling at constant longitudinal speed, accelerating and decelerating.
iii. For different lateral velocities, lateral accelerations of the cut-in vehicle.
iv. 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.

Stationary obstacle after lane change of the lead vehicle

REQ#177: 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 manoeuvre.

REQ#178: The test shall be executed at least:

i. With a stationary passenger car target centered in lane.
ii. With a powered two-wheeler target centered in lane.

iii. With a stationary pedestrian target centered in lane.
iv. With a target representing a blocked lane centered in lane.
v. With multiple consecutive obstacles blocking the lane (e.g. in the following order: ego-vehicle – lane change vehicle – motorcycle – car).

Field of View test

REQ#179: 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 be-side within the lateral detection area up to at least the full width of the adjacent lane.

REQ#180: The test for the forward detection range shall be executed at least:

i. When approaching a motorcycle target positioned at the outer edge of each adjacent lane.
ii. When approaching a stationary pedestrian target positioned at the outer edge of each adjacent lane.
iii. When approaching a stationary motorcycle target positioned within the ego lane.
iv. When approaching a stationary pedestrian target positioned within the ego lane.

REQ#181: The test for the lateral detection range shall be executed at least:

i. With a motorcycle target approaching the MV vehicle from the left adjacent lane.
ii. With a motorcycle target approaching the MV vehicle from the right adjacent lane.

REQ#182: Additional other test cases may be assessed if it is deemed justified by the Technical Service. Some of the cases may include:

i. Y-split of highway lanes.
ii. Vehicles entering or exiting the highway.
iii. Partially blocked ego lane, tunnel.
iv. Traffic lights.
v. Emergency vehicles.
vi. Building areas.
vii. Faded/erased/hidden lane markings.
viii. Emergency/personal service directing traffic.
ix. Change in road characteristics (no longer divided, pedestrians permitted, roundabout, intersection).
x. Normal traffic flow resumed (i.e. all vehicles moving > 60km/h).

3.3 Real-world testing

3.3.1 Qualitative measures

The qualitative measurements that have to be done during a real-world environment are the same as presented in the 3.1.1 Qualitative measures from the Testing in simulated environment subpart.

3.3.2 Quantitative measures

The quantitative measurements that have to be done during a real-world environment are the same as presented in the 3.1.2 Quantitative measures from the Testing in simulated environment subpart.

3.3.3 Criteria and thresholds for metrics

The criteria and thresholds for metrics that have to be defined during a real-world environment are the same as presented in the 3.1.3 Criteria and thresholds for metrics from the Testing in simulated environment subpart.

3.3.4 Determination of the need of making an AI bricks diagnosis after a real-world environment test

The determination of the need of making an AI bricks diagnosis that have to be done during a real-world environment test are the same as presented in the 3.1.4 Determination of the need of making an AI bricks diagnosis after a simulated environment test from the Testing in simulated environment subpart.

3.3.5 Method of diagnosis and correction of AI bricks

The method of diagnosis and correction of AI bricks that have to be applied during a real-world environment test are the same as presented in the 3.1.5 Method of diagnosis and correction of AI bricks from the Testing in simulated environment subpart.

3.3.6 Support for testing in real environments

These tests use public and open roads to test and evaluate the performance of the system, related to its ability to provide dynamic control under real traffic conditions.

Tests on the open road, using lanes open to public traffic, should make it possible to test and evaluate the performance of the system under study in real traffic conditions. The use of open road tests may be possible and correlated with simulation tests and tests in a controlled environment:

i. For which the use of other types of activity is not technically possible, or representative (allowing the system to be exposed to a particular environment, detecting functional deficiencies).
ii. For which the associated risks for test personnel and third parties is not unacceptable.

Real-world tests are also used to assess aspects of Autonomous Road Transport System (RAS) performance at certain ODD boundaries (nominal and complex scenarios), including requests for remote intervention when needed.

In addition, open-road testing helps detect issues that might not be well captured by track testing and simulation, such as limitation of perception quality (e.g. due to light conditions, the rain).

Open road testing can also allow the identification of extreme cases and other unforeseen dangerous situations generated by an unexpected alteration of the characteristics of the route, which could contribute to the improvement of risk analyzes and ultimately the design of safe systems. . Although it is not possible to encounter all traffic scenarios in a real-world test, the likelihood of covering specific complex scenarios could be increased by examining, on the course, when and where specific items (e.g. example, high or low density traffic) usually occur. Open road tests in the area where the traffic route of an Autonomous Road Transport System (RAS) can help identify critical situations.

The number of scenarios feasible in real conditions is limited, which implies seeking to increase the probability of coverage of complex and specific scenarios by selecting a specific type of field of employment and examining the places and times when specific elements are likely to occur (which is carried out via risk analyses).

These tests in real conditions are complementary to the two previous types of tests. Data generated during real-world testing can be used as supplemental data to validate the suitability of simulations and track testing against actual operating conditions. It can also make it possible to enrich the base of scenarios and therefore enrich simulations and tests in a controlled environment with new scenarios, making it possible to identify so-called “edge cases” scenarios and enrich quantified risk analyses.

The following table presents the advantages and disadvantages of this test pillar in real conditions and it comes from the DGITM/DMR/TUD, *Utilisation des scénarios pour la démonstration de la sécurité des systèmes de transports routiers automatisés,* 2023. [31]

Benefits	Disadvantages
• high validity of the field of use: the system is validated in its field of use; • can be used to test scenario elements such as environmental conditions and certain infrastructures (tunnels, bridge); • allows simulations and track tests to be validated by comparing system performance for the same scenario; • can be used to assess aspects of system performance related to its interactions with other road users, its courtesy to other vehicles; • validate models, software and tool chains	• restricted controllability: the field of use on open roads is difficult to control; • limited reproducibility: the replication of scenarios on the open road is difficult; • limited repeatability: multiple iterations are difficult to do on the open road; • limited scalability: little evolution of scenarios; • expensive but not as much as track testing; • potential impacts on traffic and safety authorities; • new skills to be acquired by the authorities; • safety risks: test personnel and the public may be subject to significant risks and unsafe behaviour.

Table 18: Pros and Cons of the real-world tests.

Otherwise, the purpose of this test is to support the Technical Service in understanding the functionality of the system in its operating environment.

The real-world test shall enable the Technical Service to identify areas of system performance that may require further assessment, through testing.

During the real-world assessment, the Technical Service shall assess at least:

i. Prevention of activation when the ADS is outside of its technical boundaries/requirements for ALKS.
ii. No violation of traffic rules.
iii. Response to a planned event.
iv. Response to an unplanned event.
v. Detection of the presence of other road users within the frontal and lateral detection ranges.
vi. Vehicle behaviour in response to other road users (following distance, cut-in scenario, cut-out scenario etc.).
vii. System override.

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

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.

It is recommended that the real-world test is 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.

Now, based on the *New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS)* document wrtitten by VMAD (cf. [27]), good practices for the real-world testing are:

i. Real-world testing uses public roads to test the capabilities and compliance with safety requirements (e.g., human factors, safety system) of a vehicle with an automated driving system (ADS) in real-world traffic. It therefore provides an opportunity to validate the safety of the ADS within its true operating environment.

ii. It is recommended that real world testing be considered for assessing aspects of the ADS performance related to its capability to drive in real traffic conditions, e.g. smooth driving, capability to deal with dense traffic, interaction with other road users, maintaining flow of traffic, being considerate and courteous to other vehicles.

iii. Real world testing should also be considered for assessing aspects of the ADS performance at some ODD boundaries (nominal and complex scenarios), i.e. is the system triggering transition demands to the driver when it is supposed to (e.g. end of the ODD, weather conditions) . The same testing could be used to confirm the performances related to human factors under these conditions.

iv. Furthermore, it is recommended that on road testing be considered for detecting issues that may not be well captured by track tests and simulation, such as perception quality limitation (e.g. due to light conditions, rain, etc.).

v. Although it may not be possible to encounter all traffic scenarios during a real-world test, the likelihood of covering specific complex scenarios could be increased by selecting a specific type of ODD (e.g., highway) and examining when and where specific elements (e.g., high- or low-density traffic) typically occur.

vi. Specific offenses identified during real-world testing may be reviewed and/or assessed by evaluating the data gathered during the original test and any data gathered during additional virtual, track and real-world testing.

How the real-world tests interact with other elements

i. Data generated during real-world testing may be used as additional data to validate whether portions of a virtual and/or track-testing environment were modelled properly by comparing an ADS' performance within a simulation and track test with its performance in a real-world environment when executing the same test scenario.

ii. It can also be used to support the development of new traffic scenarios for track and virtual testing, allowing for the identification of edge cases and other unanticipated hazardous situations that could challenge the ADS.

iii. The information gathered from real world testing may also support improvements in the hazard and risk analysis and design of the ADS systems.

4 List of criteria and rationale for the identification and justification of near miss and accident scenarios, having led to critical situations

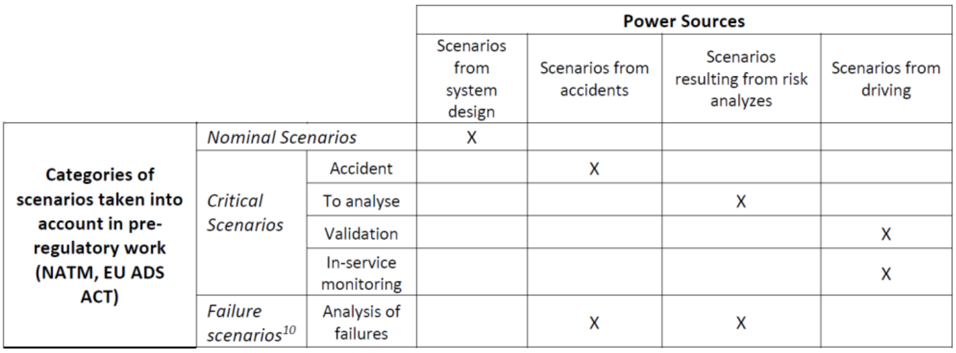
Decision framework for identifying unacceptable scenarios is a key validation support element for the whole process, especially for second part of the life cycle, that’s why it is worthy developing it in this paragraph.

Accident scenarios can be used to identify dangerous behaviours of the system studied, which can lead to dangerous situations (including those having led to accidents in particular contexts, recorded in accidentally).

Accident scenarios contribute:

- Firstly, to the construction of safety by promoting exhaustiveness in risk analysis (i.e. avoiding omissions);
- Then, to the definition of the expected results of the system (to avoid the accident or to mitigate its consequences), following the expression of the safety requirements covering safe behaviours.

Below is a table from the DGITM/SAGS/EP, *Safety demonstration of automated road transport systems (ARTS): Excepted contributions of the driving scenarios*, 2022. [15]



			Power Sources			
			Scenarios from system design	Scenarios from accidents	Scenarios resulting from risk analyzes	Scenarios from driving
Categories of scenarios taken into account in pre-regulatory work (NATM, EU ADS ACT)	*Nominal Scenarios*		X			
	Critical Scenarios	Accident		X		
		To analyse			X	
		Validation				X
		In-service monitoring				X
	Failure scenarios[10]	Analysis of failures		X	X	

Table 19: Link between the four categories of scenarios in the document and the categories of scenarios internationally requested.

Also, based on the *Data analysis process and identification of single situations* document done by BPI France for the PRISSMA project (cf. [8]), the main elements that characterize the three degrees of severity of an event is resulting in: an accident, a near miss or irrelevant behaviour.

i. **Characterization of an accident:** an accident is characterized by material contact between the autonomous vehicle and any other element of the driving environment. This material contact may cause a frank or even violent impact, which may result in significant material damage and above all an attack on at least one human being. An accident can be the result of:
   - Leaving the track;
   - Frontal collision with a moving or fixed obstacle;
   - Side or rear-end collision with a moving or fixed obstacle;
   - Or overtaking.

ii. **Characterization of a near miss:** in real-life conditions, even on a predefined route, an autonomous shuttle can be faced with unexpected situations, requiring a reaction. Decision-making based on current parameters, speed and position measurements, and interpretation of images or the scenery can avoid a collision or a more serious accident. The following list is intended to give examples of possible events or environmental changes that initiate "near miss" situations:
   - From the metrics used by the autonomous shuttle while driving (excluding manoeuvres):
     - Overlap of buffer zones between the autonomous shuttle and another vehicle on approach,
     - Penetration of an “intruder object” into the protective buffer zone of the autonomous shuttle,
     - Rapid degradation of a distance or time metric predicting a likely collision,
     - Abrupt reaction of the autonomous shuttle to restore deviating metrics quickly,

  - Reaction of the autonomous shuttle in a context where some sensors have gone out of their reliable range.

- From the metrics used by the autonomous shuttle during its authorized manoeuvres:
  - "Time to collision" below a certain distance value,
  - "Time to break" less than a certain value of time.

It is important, in the context of a near miss, to take into account the differences between the real situations encountered and those transposed in a simulator. In the case of a near miss, the reaction of the autonomous shuttle is sufficiently relevant, fast and accurate to avoid a collision (the relevant parameters have not exceeded certain thresholds defined during the design based on the combination of the overall performance of the sensors, mechanics and artificial intelligence).

iii. **Characterization of irrelevant behaviour:** the autonomous shuttle may become a widespread means of road transport in the world. However, the general public must accept this technology to a large extent. Comfort is one of the factors positively influencing acceptance and is strongly correlated with trust. Irrelevant behaviour of the autonomous shuttle (too jerky, too close, too fast or too slow) is detrimental to the comfort and sense of safety of the passengers. This unexpected behaviour may be defined as an "over-reaction of the vehicle to a benign event in a "human perception" logic or process. The events that can provide such behaviour are:

- Sensor fooled by a falling tree leaf or equivalent;
- sensor misled by sun glaze;
- Sensor fooled by a shadow (camera);
- Sensor accuracy reduced by weather (rain, snow, fog…).

Irrelevant behaviour differs from near misses in that the metrics characterizing it do not cause an alarm or preservation (protection) response to a potentially hostile event, but influence the behaviour of the shuttle in terms of the smoothness of driving sequences.

Identification and analysis of single situations:

This section deals with the elements which can be useful for the identification and analysis of single situations that may occur during an operational scenario. The result of this step will then be used to analyse and diagnose the cause of the unexpected events of the identified single situations.

Events that may lead to single situations

The following table provides a classification of main events that can lead the autonomous shuttle to a single situation (accident, near miss or irrelevant behaviour). These events are classified into 7 categories: events related to the trajectory of the autonomous shuttle, events related to the manoeuvres performed by the autonomous shuttle, events related to the protective actions of the autonomous shuttle, events impacting the comfort and safety of the passengers, events related to the reliability of the autonomous shuttle, and events dedicated to its digital infrastructure.

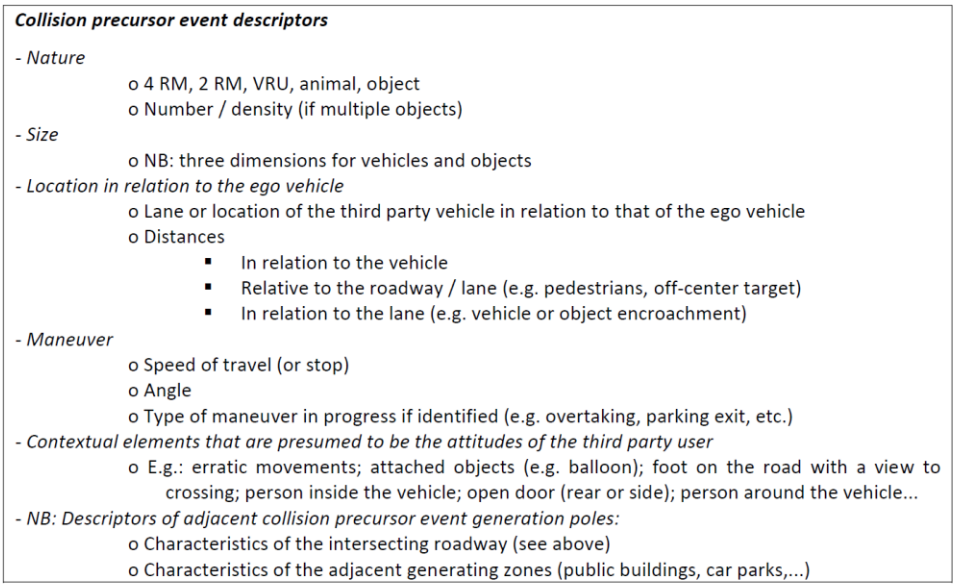
Below is a table from the BPI France for the PRISSMA project, *Liv. 7.2 : Data analysis process and identification of single situations,* 12/01/2023. [8]

Category	Event	Accident	near miss	Irrelevant behaviour
Trajectory	Off-track encroachment	x	x	x
	yaw	x	x	x
	Non-centered position		x	x
	Obstacle avoidance	x	x	x
	left hand traffic	x	x	x
	Ground handling, slip on start-up	x	x	x

Category	Event	Accident	near miss	Irrelevant behaviour
	Tight or wide negotiated turn	x	x	x
	Shifting trajectory	x	x	x
	Unexpected change of trajectory	x	x	x
Manoeuvre	Emergency braking	x	x	x
	Powerful braking	x	x	x
	Stop not adjusted	x	x	x
	Blocking behind a stopped vehicle			x
	Commitment intersection	x	x	
AS protection	Improper signal lights (flashing etc.)		x	x
	Front safety distance	x	x	x
	Lateral safety distance	x	x	x
	Stopping in the middle of the road	x	x	x
	Failure to follow the announced route	x	x	x
	Failure to comply with traffic regulations (misreading of signs)	x	x	x
passenger comfort	Unwanted speed variations		x	x
	Too high speed			x
	Too slow speed			x
	Failure to follow the announced route			x
	Failure to respect passenger stops			x
	Unexpected braking	x	x	x
passenger security	Stop not allowing safe access		x	x
	Passenger emergency stop		x	x
Reliability	Energy failure		x	x
	mechanical failure	x	x	x
Digital infrastructure	Expected information not provided			

Table 20: Table of events that may lead to single situations.

From the DGITM/SAGS/EP, *Safety demonstration of automated road transport systems (ARTS): Excepted contributions of the driving scenarios*, 2022 [15], here is detailed the description of a collision precursor event:



Collision precursor event descriptors

- *Nature*
  - o 4 RM, 2 RM, VRU, animal, object
  - o Number / density (if multiple objects)
- *Size*
  - o NB: three dimensions for vehicles and objects
- *Location in relation to the ego vehicle*
  - o Lane or location of the third party vehicle in relation to that of the ego vehicle
  - o Distances
    - ▪ In relation to the vehicle
    - ▪ Relative to the roadway / lane (e.g. pedestrians, off-center target)
    - ▪ In relation to the lane (e.g. vehicle or object encroachment)
- *Maneuver*
  - o Speed of travel (or stop)
  - o Angle
  - o Type of maneuver in progress if identified (e.g. overtaking, parking exit, etc.)
- *Contextual elements that are presumed to be the attitudes of the third party user*
  - o E.g.: erratic movements; attached objects (e.g. balloon); foot on the road with a view to crossing; person inside the vehicle; open door (rear or side); person around the vehicle...
- *NB: Descriptors of adjacent collision precursor event generation poles:*
  - o Characteristics of the intersecting roadway (see above)
  - o Characteristics of the adjacent generating zones (public buildings, car parks,...)

Figure 21: Collision precursor event descriptors.

5 List of diagnoses and corrective actions related to critical situations

This framework is critical to dimension support validation elements of system life cycle support.

First, a diagnosis is the process of determining what is wrong and what has caused the unique situation, i.e. irrelevant or accidental behaviour.

The objective of determining whether a diagnosis of AI bricks is necessary after real driving is based on the more or less unfavourable combination of metrics or failures of a system (or sub-system, component), or of an AI brick whatever its function, which have been linked, accumulated or not, to reach a driving situation characterized by an incident (irrelevant behaviour), a near miss or an accident.

As a reminder, the metrics listed below are those used in the tool to assess the behaviour of the shuttle and the state of its components in order to determine whether the failure is related to a bug in an AI brick.

i. The reaction time of the vehicle, compared to the human ability to react in less than 1 second (metric associated with OEDR).
ii. A safety metric relating to the shuttle's protection zone, an object passes the perimeter of this zone, which can for example be an ellipse and moves away from it (the metric value increases or the object approaches the vehicle inside the safety perimeter (the metric value decreases).
iii. The state of a sensor that may be defective or have an embedded AI brick that is malfunctioning (Bug).
iv. The location of the shuttle in relation to its ODD.
v. The state of one or all AI bricks that make up the fusion, decision and response functionalities of the shuttle.

The recommendation or decision to be taken is characterized by:

i. The realization of an AI diagnosis (generic recommendation to be improved according to the architectures and the nature of the embedded AI).
ii. Carrying out a classic failure diagnosis and an FMEA.
iii. Corrective analysis of the system engineering phases.
iv. No particular action because the shuttle behaviour was nominal.

Corrective maintenance issues of AI bricks using deep networks:

DNNs have been successfully applied to a wide variety of problems, including image recognition, medical diagnosis and self-driving cars. However, DNNs are far from infallible, and bugs in their algorithms have led to loss of life and unjustified arrests. This has motivated recent advances in understanding, verifying, testing and fixing DNNs.

After deployment, the DNN may have errors, for example due to misclassification of images. To repair the DNN, one could re-train the network using the original training dataset with the newly identified faulty inputs added. However, retraining is extremely inefficient (i.e. training can take a long time (days or weeks with the most sophisticated equipment). Even worse, the original training data set may not be available for retraining; for example, it may be missing or lost. Indeed, in some cases, privacy regulations require companies to regularly delete private data. Retraining can also lead to arbitrary changes in the network and often introduce new bugs in the behaviour of the network. In addition, standard software programs and DNN models are fundamentally different in terms of bug detection and correction.

For example, standard software programs are tested by comparing the actual output with the expected output. If the two outputs are different, then we consider the program to have a bug. On the other hand, DNN -based software has a complex structure, and it learns from a set of training data. If the DNN produces an incorrect classification during training, we call it a failure case, it is not necessarily that the

DNN contains a bug, because a DNN cannot guarantee 100% correct classifications. Furthermore, unlike an ordinary program, a DNN program uses weights between neurons and non-linear activation functions for similar purposes, which makes debugging and testing DNN -based software difficult. Several researchers have been interested in this problem and have proposed approaches and tools for diagnosing and correcting bugs in deep learning programs. In the following section we present some of them.

6 List of constraints On the evolution of AI functions

One of the AI evolution constraints is the uncertainty of the estimations.

Indeed, related to the input data, quality/adequacy is the characterization of the input uncertainty.

Sources of uncertainty may result from different aspects. A typical characterization is the following:

i. *Epistemic uncertainty:* lack of knowledge in some of the parameters/processes (can be reduced via increasing knowledge about the RWS).

ii. *Random uncertainty:* inherent variation in the physical system (irreducible).

The maximum credibility for an M&S is obtained when the epistemic uncertainty is reduced. For the sake of the credibility analysis, the way uncertainty has been determined/evaluated has to be reported.

Output data pedigree - Uncertainty estimation

Related to the output data, credibility is the characterization of the uncertainty. Maximum credibility is obtained when a quantitative description of the results' uncertainty is provided and methodologies are enforced to mitigate the impact of the resulting uncertainties (NASA, 2019) . Vice versa, no contribution to the credibility is provided when no qualitative or quantitative estimation is given. An intermediate credibility contribution is represented by a qualitative description.

The following table coming from the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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,* 2022 [4] might be used as a template for the uncertainty characterization score assessment:

Level	Uncertainty Sources	Uncertainty Assessment
0	No/insufficient evidence	No/insufficient evidence
1	Some sources of uncertainty identified	Qualitative assessment
2	Most sources quantitatively identified	Propagation of known uncertainties
3	All known sources quantified	Quantitative uncertainty of M&S output
4	All known sources quantified	Statistical analysis of M&S output

Table 21: Template for the credibility assessment of output data uncertainty, (NASA, 2019).

A common method to provide a quantitative estimation of the uncertainty is Monte Carlo simulation (EASA, 2020) . In a Monte Carlo simulation, multiple simulations are executed by randomly sampling within the uncertainty interval the M&S parameters to generate confidence intervals.

Nevertheless, the Modeling Approach Credibility is another factor of the AI evolution constraints.

In fact, state-of-the-art literature provides guidance for M&S validation best practices. In particular, a generic framework to assess the credibility of the modeling approach is given in (W. Oberkampf et al., 2007) which provides support to define:

i. The degree to which models are physics-based.
ii. The degree to which models are calibrated.
iii. The degree to which models are being extrapolated from the validation and calibration database to the conditions of the application of interest.
iv. The quality and degree of coupling multiphysics effects that exist in the application of interest.

Based on the considerations above, a framework to assess the maturity level of the M&S toolchain from the perspective of the modeling approach is provided.

The highest maturity level (Level 3) is associated with an M&S toolchain based on fully physical approaches relying on a bidirectional coupling of each simulation model. On the contrary, fully empirical models that only fit experimental data without a reconstruction of the physics behind the phenomena modelled are associated with the lowest grade (Level 0). The lowest maturity, and thus minimal contribution to the credibility, is due to the limited domain of application of those M&S approaches that can be applied only within the range used for calibration with minimal or non-existent extrapolation capabilities.

Below are tables/figures from the European Commission MVWG-ACV, *Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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,* 2022. [4]

Level	Technical Validation	Maturity
0	• Judgment only • Model forms are either unknown or fully empirical • Few, if any, physics-informed models • No coupling of models	low-consequence Minimal M&S impact
1	• Some models are physics-based and are calibrated using data from related systems • Minimal or ad-hoc coupling of models	Moderate consequences Some M&S impact
2	• Physics-based models for all important processes • Significant calibration needed using SETs and IETs • One-way coupling of models • Some peer review conducted	High consequence High M&S impact
3	• All models are physics-based • Minimal need for calibration using SETs and IETs • Sound physical basis for extrapolation and coupling of models • Full, two-way coupling of models • Independent peer review conducted	High consequence Decision-making based on M&S

Table 22: Template for modeling approach credibility assessment as of (W. Oberkampf et al., 2007).

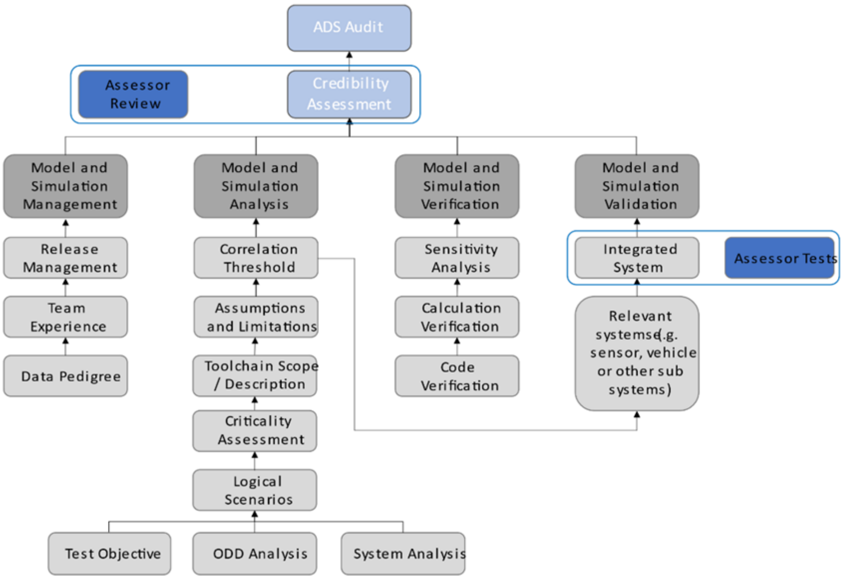


Figure 22: Simulation credibility framework, (EU Commission, 2022b).

7 Validation support issued from existing regulations and methodological frameworks

7.1 Standards

The following parts aims to make a synthesis of the different existing frameworks that can be directly linked to the WP8.3:

7.1.1 *Quelques éléments d'éclairage sur les compétences de supervision et d'intervention à distance,* DGITM/SAGS/EP1. (18/01/2022).

The following document deals with the authorization of persons responsible for remote intervention. It presents the legislative aspects of automated road transport systems at national, European and international level.

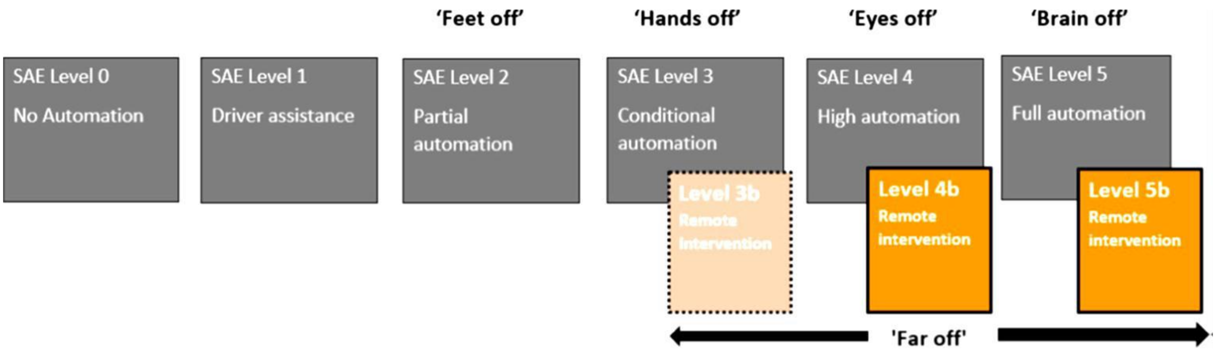


Figure 23: Schematic representation of what each SAE level induced to the driving conditions.

7.1.2 *Démonstration de sécurité des systèmes de transports routiers automatisés : Génération, alimentation et enrichissement des scénarios de conduite,* DGITM/DMR/TUD.

The following document handles the safety demonstration of automated road transport systems (ARTS) via the contribution of driving scenarios (generation, supply and enrichment). Indeed, it is composed of the following subjects: the scenarios/use cases, the kind of events, the scenarios infrastructures descriptions, the critical situations, and some examples of scenarios factors.

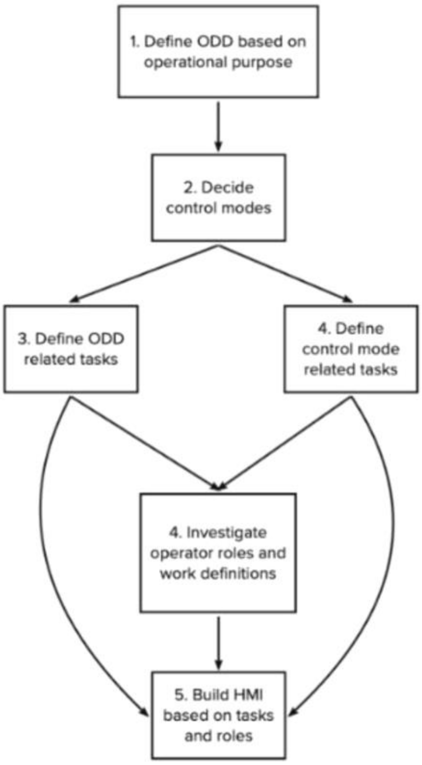

1. Define ODD based on operational purpose
2. Decide control modes
3. Define ODD related tasks
4. Define control mode related tasks
4. Investigate operator roles and work definitions
5. Build HMI based on tasks and roles

Figure 24: Flowchart of the integration of the operator roles in the automated driving conception process.

7.1.3 *Utilisation des scénarios pour la démonstration de la sécurité des systèmes de transports routiers automatisés : Document méthodologique,* DGITM/DMR/TUD.

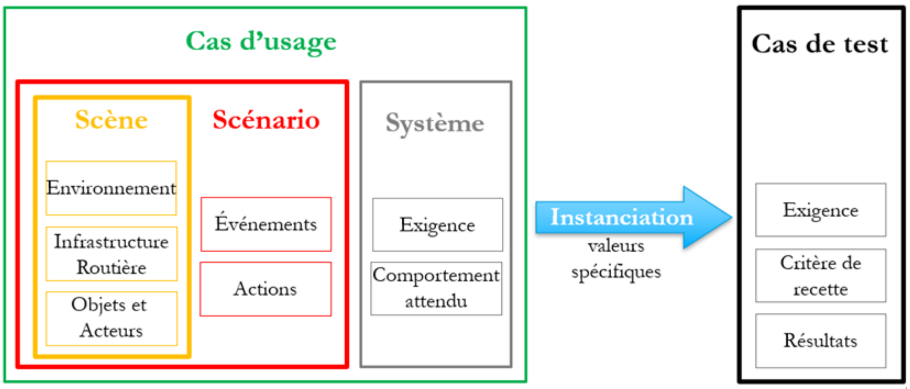


Figure 25: Description of use cases macro-elements and their impact on the tests.

The following document highlights the safety demonstration of automated road transport systems via the New Assessment Test Method performing the 3 tests.

To be precise, it shows how to slice the safety demonstration elements by realizing a simulated test, followed by a track test, and concluded by a road test permits a multi-point evaluation of the AI capabilities.

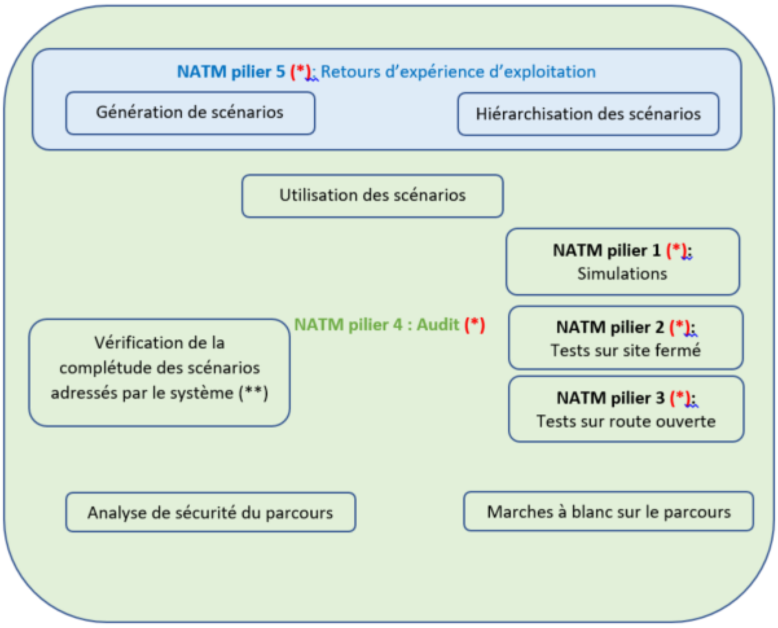

NATM pilier 5 (*): Retours d'expérience d'exploitation
Génération de scénarios
Hiérarchisation des scénarios
Utilisation des scénarios
NATM pilier 1 (*): Simulations
NATM pilier 4 : Audit (*)
Vérification de la complétude des scénarios adressés par le système (**)
NATM pilier 2 (*): Tests sur site fermé
NATM pilier 3 (*): Tests sur route ouverte
Analyse de sécurité du parcours
Marches à blanc sur le parcours

Figure 26: Summary of the organisation of the pillars of the New Assessment Test Method.

7.1.4 *Arrêté du 2 août 2022 pris en application de l'article R. 3152-30 du code des transports, et Arrêté du 5 août 2022 pris en application de l'article R. 3152-24 du code des transports,* Ministère de la transition écologique et de la cohésion des territoires. (12/08/2022).

The following document from the French ministry of ecological transition regulates the content of the opinions from approved qualified institutions and the accreditation procedure for qualified organisations.

Also, it specifies that there are 4 levels of documentation expected by the STRMTG:

i. DCST (*Technical System Design Report* : technical system design report)
ii. DPS (*Preliminary Safety Report* : preliminary safety report)
iii. DPE (*Dossier Préliminaire d'Exploitation:* preliminary operating report)
iv. DS (*Safety File:* safety report)

7.1.5 *Guide d'application du principe GAME*, STRMTG. (20 Décembre 2021).

The following document speaks about the GAME (Globally *At Least Equivalent:* globally at least equivalent) principle in the Automated Road Transport System and the conditions in which it can be used / is applicable. In more details, it permits the justification of a safety global approach and the risks coverage arrangements.

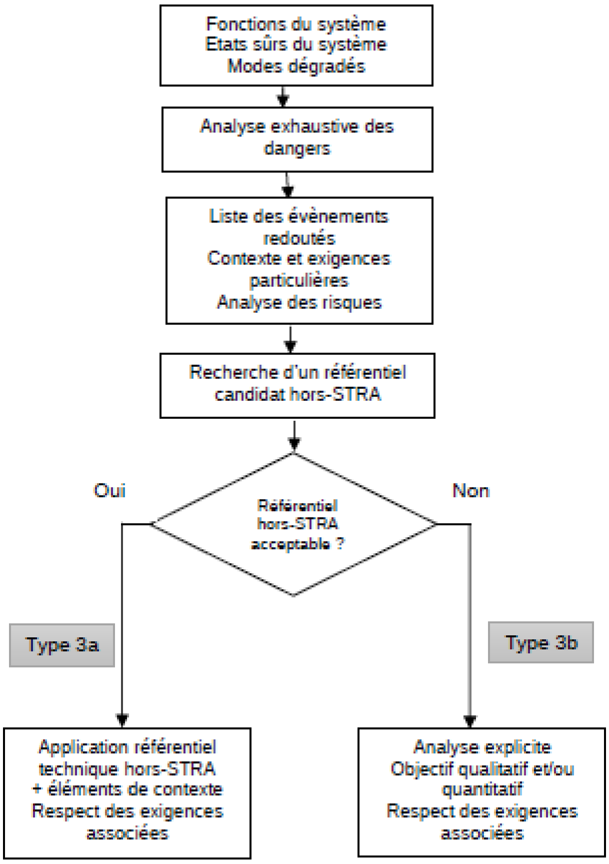
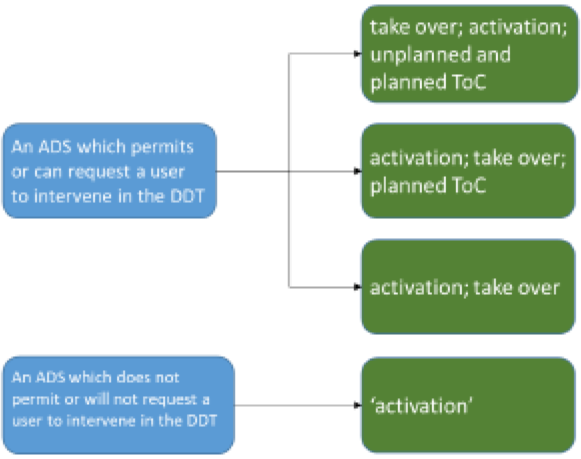

Fonctions du système
Etats sûrs du système
Modes dégradés
Analyse exhaustive des dangers
Liste des évènements redoutés
Contexte et exigences particulières
Analyse des risques
Recherche d'un référentiel candidat hors-STRA
Référentiel hors-STRA acceptable ?
Oui
Non
Type 3a
Type 3b
Application référentiel technique hors-STRA + éléments de contexte Respect des exigences associées
Analyse explicite Objectif qualitatif et/ou quantitatif Respect des exigences associées

Figure 27: Flowchart of requirements for detailed risk analysis.

7.1.6 *Recommendations concerning Safety Requirements for the Assessment of Automated Driving Systems and ADS Vehicles,* FRAV. (10/01/2023).

The following document describes all the recommendations concerning Safety Requirements for the Assessment of Automated Driving Systems and ADS Vehicles. Otherwise, ODD descriptions for ADS features are also detailed.


An ADS which permits or can request a user to intervene in the DDT
take over; activation; unplanned and planned ToC
activation; take over; planned ToC
activation; take over
An ADS which does not permit or will not request a user to intervene in the DDT
'activation'

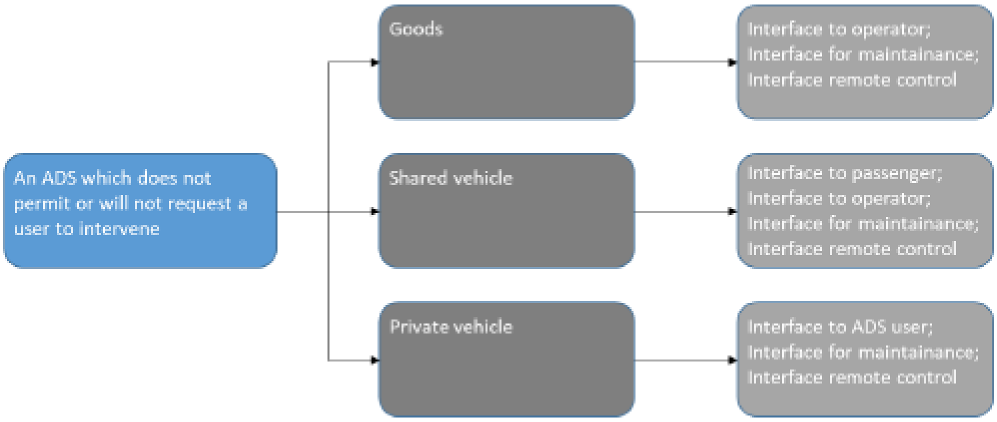


Figure 28: Diagram of the resulting actions from the intervention or not of the user on ADS.

7.1.7 *Systèmes de Transport Routier Automatisés: Guide d'application relatif à la cybersécurité pour les STRA,* STRMTG. (19/12/2022).

The following document refers to the cybersecurity in the Automated Road Transport Systems. It enumerates the responsible entities per considered systems, the scenario risks, but also the cybersecurity risks in all the project phases starting with the conception until the service withdrawal.

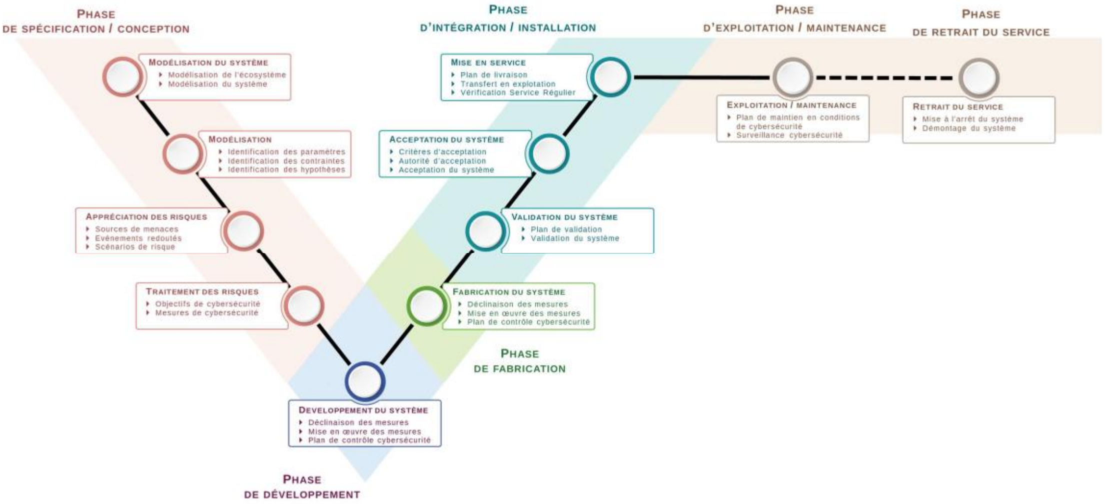


Figure 29: Representation of the cybersecurity activities integrated into the life cycle of the system under consideration in the form of a V-cycle diagram.

7.1.8 *Systèmes de Transport Routier Automatisés: Mission de l'organisme qualifié agréé pour l'évaluation de la sécurité et pour l'audit de sécurité en exploitation des STRA,* STRMTG. (26/10/2022).

The following document points out different aspects of the AI functions evaluation processes established by the qualification and approval organisation (OQA: *Organisme de Qualification et d'Approbation)*. Indeed, inside in, there are relevant information about the evaluation process by report progress stages. Above all, the safety global evaluation developed by the global security management system (SGS: *Système de gestion Globale de la Sécurité)* is the main topic of this document, and it is completed with evaluation reports.

The mission of the OQA is not limited to a "simple" evaluation of the system development process but leads to an evaluation of the system itself and its subsystems during the design, implementation, and testing and / or operational phases.

7.1.9 *Systèmes de Transport Routier Automatisés: Guide technique relatif à la démonstration « GAME » pour les STRA*, STRMTG. (31/08/2022).

The following document introduces the GAME principle through a technical guide. Furthermore, it is composed of detailed risk analysis, a severity and frequency estimation method, a list of high level requirements, a critical situation list, a list of points of attention/identification of causes of hazardous events, and also a Preliminary Risk Analysis. This document also includes a state of the art of high level safety requirements.

Moreover, it aims to bring back the old fault tree methods without running virtual simulation campaigns.

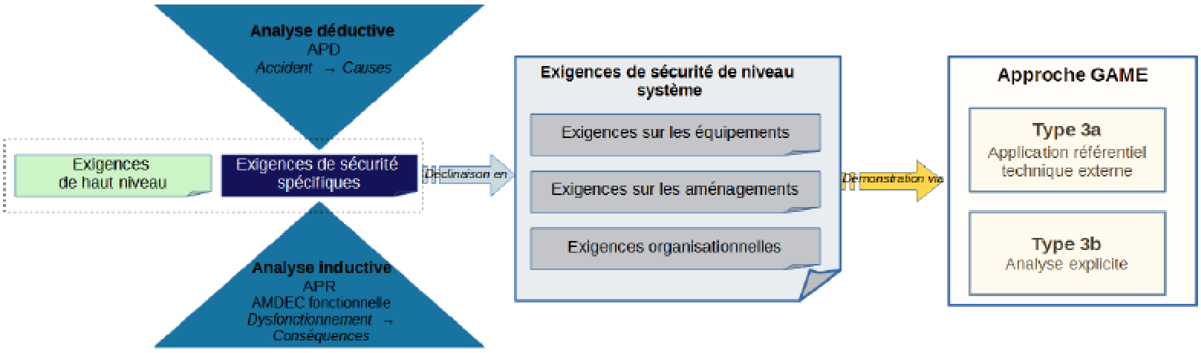
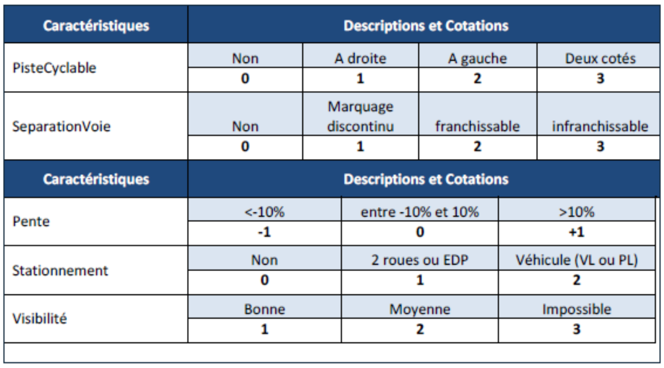


Figure 30: Diagram of the detailed analysis of high-level and specific requirements.

7.1.10 *Méthode UGE/STRMTG Caractérisation des parcours*, Université Gustave Eiffel / STRMTG. (19/05/2021).

The following document explains the different steps of a route characterization methodology that can be used. In fact, it starts by a route slicing breakdown, followed by a hazard rating, then there is a nominal and feared event hazard evaluation on the infrastructures plus the environment, and finally some examples of the application of this methodology.



Caractéristiques	Descriptions et Cotations			
PisteCyclable	Non	A droite	A gauche	Deux cotés
	0	1	2	3
SeparationVoie	Non	Marquage discontinu	franchissable	infranchissable
	0	1	2	3
Caractéristiques	**Descriptions et Cotations**			
Pente	<-10%	entre -10% et 10%	>10%	
	-1	0	+1	
Stationnement	Non	2 roues ou EDP	Véhicule (VL ou PL)	
	0	1	2	
Visibilité	Bonne	Moyenne	Impossible	
	1	2	3	

Table 23: Rating table for infrastructure characteristics.

7.1.11 *New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS)*, VMAD. (02/2022).

The following document is part of the New Assessment Test Method for Automated Driving presented that aims to be a guidelines document for validating Automated Driving System. Furthermore, it shows list and classification of the scenarios. Moreover, it detailed the simulation/track/real-world tests, plus an in-service monitoring and reporting system. As well, verification and validation processes are included. And finally, matrices of the 3 kind of tests, completed by what could be the next steps of the test accompanied by the validation of the global testing approach.

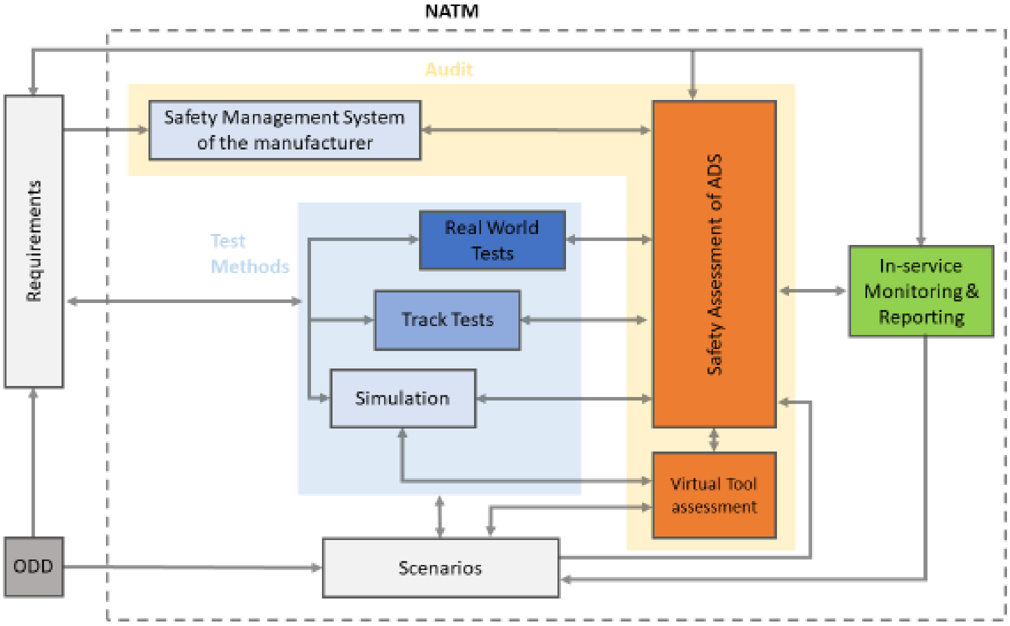


Figure 31: Scheme representing the relationship between VMAD Pillars, Scenarios and FRAV Safety Requirements.

7.2 Additional standards

7.2.1 *ISO/PAS 21448*, AFNOR, 2019.

This document states that the system verification and validation activities with regard to the risk of potentially hazardous behaviour excluding the faults addressed by the ISO 26262 series include integration testing activities to address the following scope:

- The ability of sensors and the sensor processing algorithms to model the environment
- The ability of the decision algorithms to handle both known and unknown situations and to make the appropriate decisions according to the environment model and the system architecture
- The robustness of the system or function
- The ability of the HMI to prevent reasonably foreseeable misuse and
- The manageability of the handover scenario by the driver.

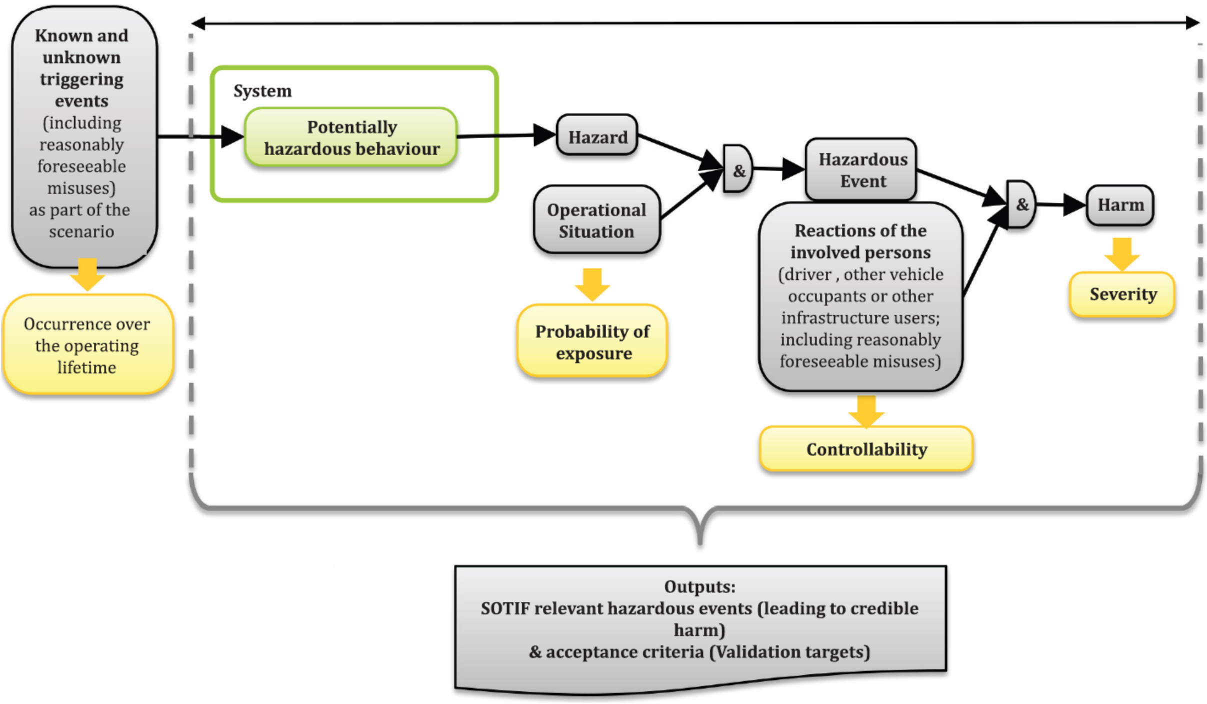

Known and unknown triggering events (including reasonably foreseeable misuses) as part of the scenario
Occurrence over the operating lifetime
System
Potentially hazardous behaviour
Hazard
Operational Situation
Probability of exposure
&
Hazardous Event
Reactions of the involved persons (driver , other vehicle occupants or other infrastructure users; including reasonably foreseeable misuses)
Controllability
&
Harm
Severity
Outputs:
SOTIF relevant hazardous events (leading to credible harm)
& acceptance criteria (Validation targets)

Figure 32: An illustration of common elements of hazard analysis in the ISO 26262 series.

7.2.2 *Vehicles and automated transport systems: First principles and questions for the definition of the ODD*, DGITM/DMR/TUD-VA, 2022.

This document deals with the question of the definition of objects or events recognizable by the system which raises a specificity linked to this dimension of the ODD such as its strong dependence on the capacities or performances of the system.

Indeed, the hazards that can be addressed by the system must be able, by definition, to be recognizable and measurable by the detection and recognition capabilities of the system, example: nature, speed and size of vulnerable users

The assumption that these ODD border objects are recognized unequivocally, is linked to nominal operating assumptions of perception, which is not the case in practice, either in the event of a failure or in the event of changes in visibility fog, rain, and brightness.

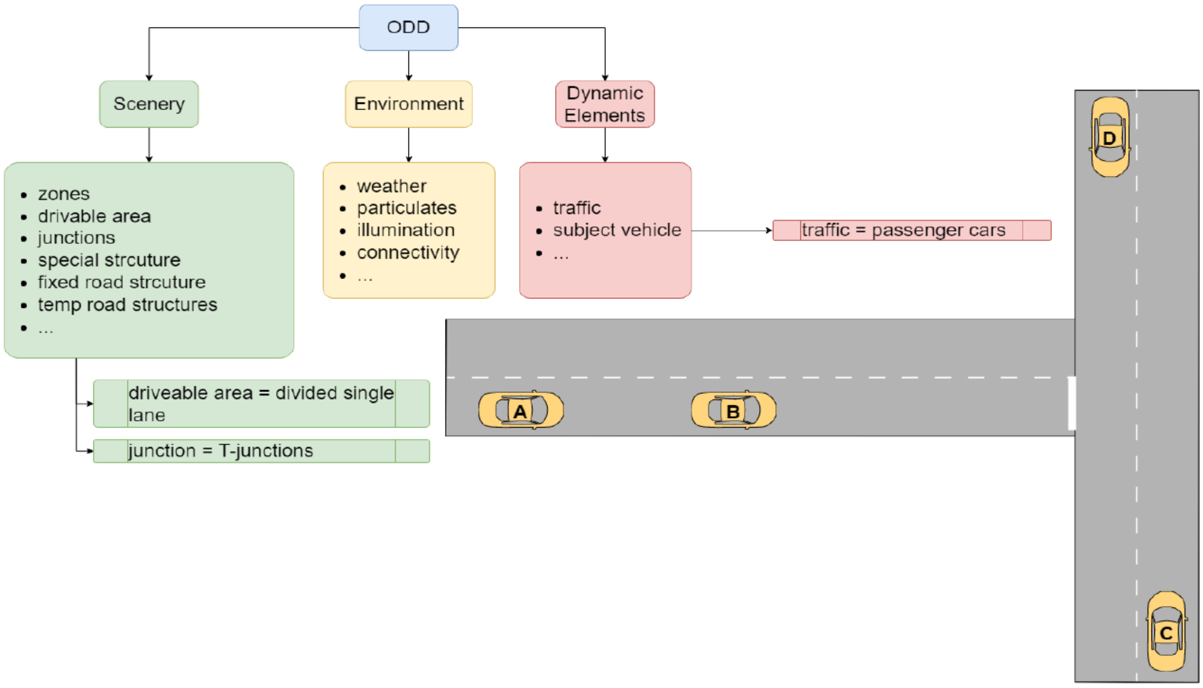


Figure 33: Scheme of what an ODD can be composed of.

7.2.3 Liv 2.8: Proofs-Of-Concept intermediate report development of platforms meeting the desired objectives of evaluating means of automated mobility, BPI France for the PRISSMA project, 2022.

This document describes the intermediate state of the implementation of proofs-of-concept (POC) that aim at demonstrating the use of simulation tests during the homologation and certification processes of autonomous vehicles. Several POC are currently being developed within the PRISSMA project and their particular ongoing work is presented separately.

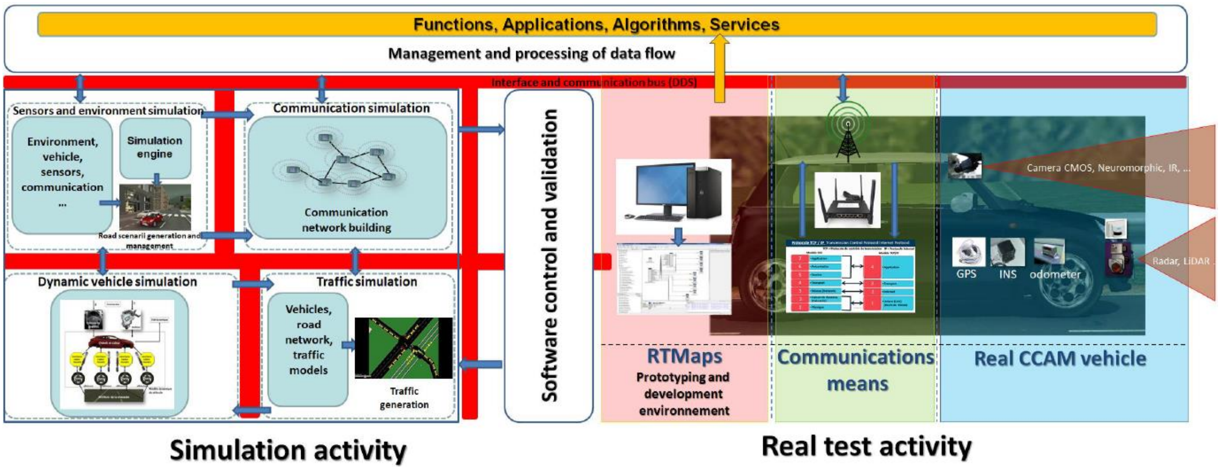

Functions, Applications, Algorithms, Services
Management and processing of data flow
Interface and communication bus (DDS)
Sensors and environment simulation
Environment, vehicle, sensors, communication ...
Simulation engine
Road scenarii generation and management
Communication simulation
Communication network building
Dynamic vehicle simulation
Traffic simulation
Vehicles, road network, traffic models
Traffic generation
Software control and validation
RTMaps
Prototyping and development environnement
Communications means
Real CCAM vehicle
Camera CMOS, Neuromorphic, IR, ...
GPS
INS
odometer
Radar, LiDAR
Simulation activity
Real test activity

Figure 34: Interconnection of real and virtual test facilities for augmented reality.

7.2.4 *Liv. 6.2 : State Of The Art risk assessment and certification for AI : Intermediate report*, BPI France for the PRISSMA project, 2022.

This document establish a state of the art of risk assessments in different sectors and initiates mapping certification efforts to evaluate artificial intelligence. The first part of the document focuses on the state of the art of risk assessment in transportation means such as aeronautics and Rail, in critical infrastructures such as off-shore and nuclear plants and finally in medical robots as they perform automated tasks in close interface with human beings. The second part presents a mapping of certification, labelling standards for AI evaluation as well as an example of certification of processes for AI.

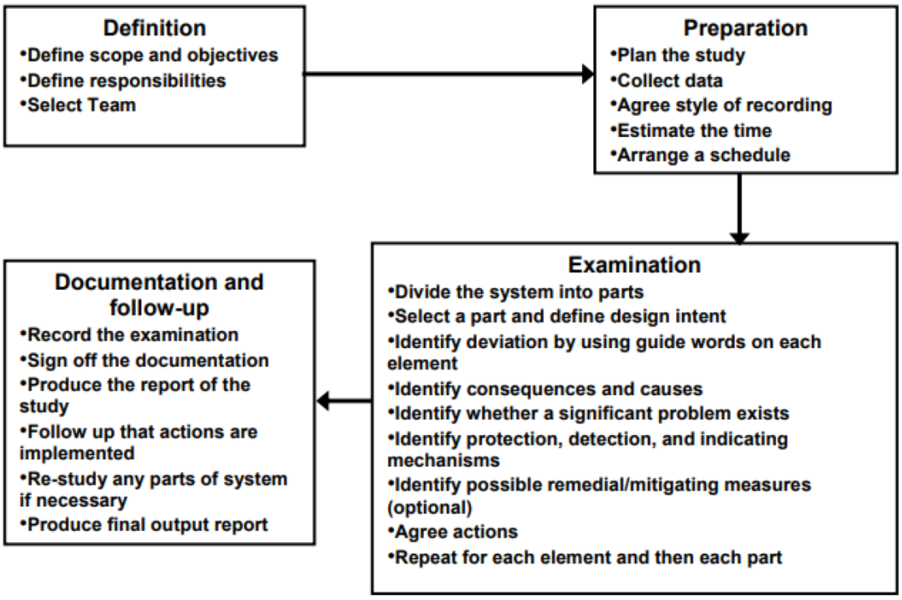

Definition
•Define scope and objectives
•Define responsibilities
•Select Team
Preparation
•Plan the study
•Collect data
•Agree style of recording
•Estimate the time
•Arrange a schedule
Examination
•Divide the system into parts
•Select a part and define design intent
•Identify deviation by using guide words on each element
•Identify consequences and causes
•Identify whether a significant problem exists
•Identify protection, detection, and indicating mechanisms
•Identify possible remedial/mitigating measures (optional)
•Agree actions
•Repeat for each element and then each part
Documentation and follow-up
•Record the examination
•Sign off the documentation
•Produce the report of the study
•Follow up that actions are implemented
•Re-study any parts of system if necessary
•Produce final output report

Figure 35: Example of how the HAZOP methodology works.

7.2.5 *Liv. 6.4 : Integration of AI specifications into design standards,* BPI France for the PRISSMA Project, 2022

This document recommend requirements to develop IA modules involved in the Autonomous Driving System of fully autonomous urban shuttle and delivery robot. It develops a concept of Operation in its first part and then develops requirements classified in three categories: AI Module specific, Vehicle specific and Smart Mobility Systems’ system of system specific. It also initiates requirements on tests whether they are done by simulation, in control-led environment or real environment.

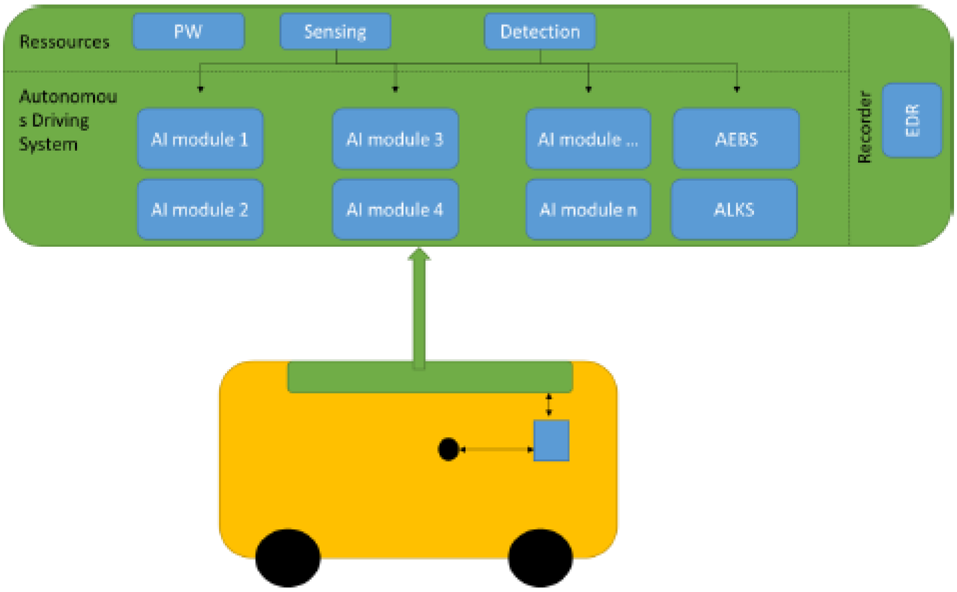
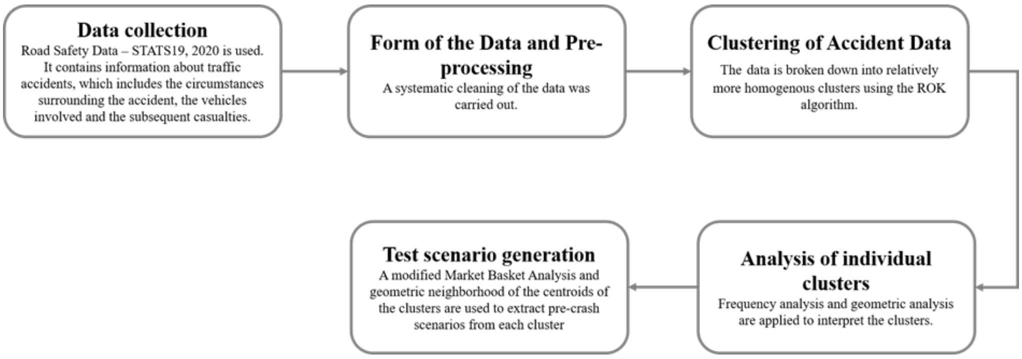


Figure 36: Breakdown of the autonomous urban shuttle.

7.2.6 *Liv. 7.2 : Data analysis process and identification of single situations*, BPI France for the PRISSMA project, 12/01/2023.

This document aims at defining the basic approach for data processing, the refinement of the feedback of the real driving conditions, the diagnosis of failures or irrelevant behaviours of the autonomous shuttles with artificial intelligence bricks, and the process of correction of these artificial intelligence bricks.


Data collection
Form of the Data and Pre-processing
Clustering of Accident Data
Analysis of individual clusters
Test scenario generation

Road Safety Data – STATS19, 2020 is used. It contains information about traffic accidents, which includes the circumstances surrounding the accident, the vehicles involved and the subsequent casualties.

A systematic cleaning of the data was carried out.

The data is broken down into relatively more homogenous clusters using the ROK algorithm.

Frequency analysis and geometric analysis are applied to interpret the clusters.

A modified Market Basket Analysis and geometric neighborhood of the centroids of the clusters are used to extract pre-crash scenarios from each cluster

Figure 37: A data mining approach for traffic accidents, patterns extraction and test scenario generation for autonomous vehicles.

7.2.7 *Liv. 8.14 : Report on the impact of AI in system engineering choices*, BPI France for the PRISSMA project, 2022.

This document introduces some of the main aspects of the AI impacting the system engineering process and the major hypothesis regarding these impacts.

The IA constraints and state-of-the-art knowledge can challenge the processes for engineering classical systems. The SOTIF principles is the state of the art for the commissioning of a vehicle and assessing the safety of the intended functionality beyond the classical functional safety applied to well-known functions of autonomous vehicle.

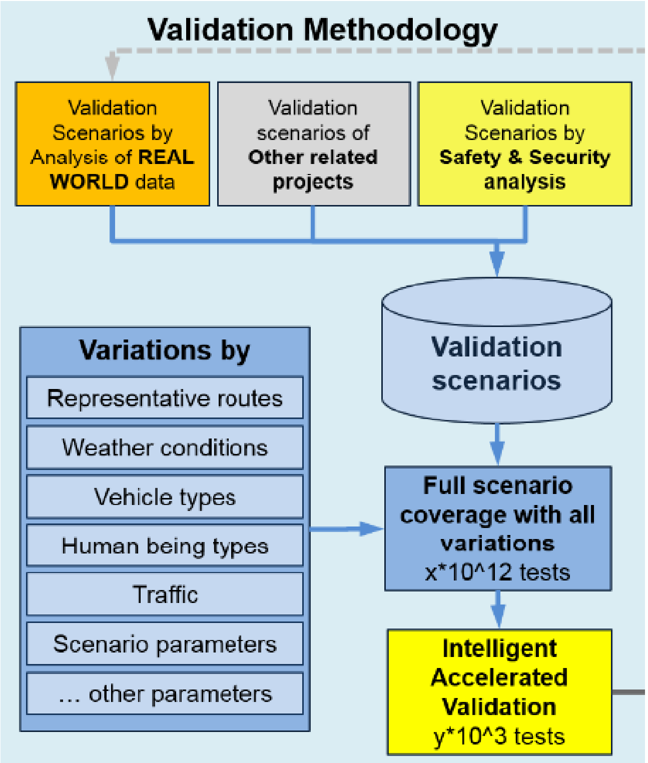

Validation Methodology
Validation Scenarios by Analysis of REAL WORLD data
Validation scenarios of Other related projects
Validation Scenarios by Safety & Security analysis
Validation scenarios
Variations by
Representative routes
Weather conditions
Vehicle types
Human being types
Traffic
Scenario parameters
… other parameters
Full scenario coverage with all variations x*10^12 tests
Intelligent Accelerated Validation y*10^3 tests

Figure 38: Flowchart of a validation process.

8 Generalization, monitoring and implementation of the different support elements throughout the whole life cycle

The main purpose of in-service reporting is to identify possible improvement for the ADS safety performance, and not to attribute blame or liability

In-Service Reporting addresses the reporting of the in-service ADS occurrences and safety performance by the manufacturer. The Reporting applies to occurrences which endanger or which, if not corrected, would endanger a vehicle, its occupants or any other person, and in more general terms, the reporting of all occurrences relevant to the safety performance of the ADS.

Also, it enables the identification of unreasonable risks related to the use of an ADS on public roads and the evaluation of its safety performance during real-world operation.

Moreover, it requires manufacturers to collect and analyse the safety-relevant information related to their in-service ADS' operation and report data on safety related concerns, occurrences and performance metrics to the relevant authority.

Furthermore, it is a mechanism to provide safety authorities with information about a manufacturer's ADS that complements information that may be gathered from other sources.

The aim of this process is to contribute to the improvement of road safety by ensuring that relevant information on safety is collected, processed and disseminated.

The In-Service Reporting aims to fulfil three main objectives:

i. Identify safety risks related to ADS performance that need to be addressed, including instances of non-compliance with ADS safety requirements.

ii. Support the development of scenarios through capturing information when the ADS does not perform safely in unanticipated situations.

iii. Share information and recommendations to promote continuous improvement of ADS safety performance.

Once there are enough ADS vehicles in-service that have encountered a sufficient range of traffic and environmental conditions then their safety needs to be evaluated. It is therefore essential that a feedback loop, facilitated by In-Service Reporting, is in place. This will provide data to assess and review the ADS manufacturer's safety case and to validate the information that was used to enable market introduction. The operational experience feedback from In-Service Reporting will also allow ex-post evaluation of the regulatory requirements and validation methods, providing an indication of any issues and consequently the need for any modification.

For example, using the information on ADS performance under real-world conditions could help to enhance or modify track tests. Furthermore, In-Service Reporting concerning user-interaction metrics could provide information useful for improving an ADS' HMI, its usability, and user education.

Unanticipated situations, risks and hazards might be identified during real-world ADS operation, and this information could be used to develop new scenarios.

In addition, in the early phase of market introduction of ADS vehicles, it is essential that the whole community learns from safety-critical situations involving an ADS. It is important therefore that there is a mechanism that allows information from the In-Service Reporting and recommendations from its analysis to be shared with the ADS community. This will allow others to react and should lead to developments that reduce or prevent that situation from occurring in another ADS.

Collection, processing and dissemination of information related to ADS safety performance from the In-Service Reporting will also help to evaluate the impact of ADS on the safety of the road network.

It is expected that a reporting system is established at national level by means of a common national database and at European level by means of a Common Central Repository.

Data quality and consistency should be ensured both at national and European level by establishing checking processes.

Short term and periodic reports should be stored within the common national database and made accessible to the relevant stakeholders as per this regulation or other applicable national laws.

Finally, another key part of this follow up is to standardize and generalize the monitoring and reporting all along the lifecycle of the system. For that, the different actors of the autonomous vehicle will have to implement a connected data reporting system in order to analyse the behaviour of the shuttle in lifecycle in order to develop improvements for the future systems.

8.1 Different levels of maintenance and associated skills

Based on the *Data analysis process and identification of single situations* document done by BPI France for the PRISSMA project (cf. [8]), the definition of the maintenance levels and the correspondence of the associated skills is represented in the following table:

levels	Definition	Actors (skills)
1	Simple actions necessary for operation and carried out on easily accessible elements in complete	User of the asset or qualified "maintenance" staff

levels	Definition	Actors (skills)
	safety using support equipment integrated into the asset.	
2	Actions that require simple procedures and/or support equipment (integrated into the asset or external) that are easy to use or implement.	Qualified maintenance staff
3	Operations that require complex procedures and/or portable support equipment that are complex to use or implement.	Qualified technician
4	Operations whose procedures involve the mastery of a particular technique or technology and/or the use of specialized support equipment.	Senior Technician
5	Operations whose procedures involve know-how, using particular techniques or technologies, processes and/or industrial support equipment.	Manufacturer or specialist department or company

Table 24: Standard FD X 60-000.

8.2 Need to standardize the responsibility and skills of the actors involved in an AI brick

According to the *Data analysis process and identification of single situations* document done by BPI France for the PRISSMA project (cf. [8]) document, in the context of the maintenance of AI algorithms, it seems appropriate to create a table of standards, which links the possible actions on the type of AI, the method of correction, the level of risk of regression, the level of the action and the skills required of the operators. These future standards should be applicable to any component used in autonomous shuttle:

i. Infrastructure.
ii. Main decision software.
iii. Any embedded component with AI data processing.
iv. Test and diagnosis equipment.
v. Data management and analysis services.

Some refinements should be proposed to quantify the level of regression risk (e.g. based on the risk analysis level matrix) and the level of action (in terms of technical difficulty). In addition, a list of different actor involved in AI bricks skills should be standardized.

8.3 Responsibility and distribution of information and data processing

The different responsibilities attribution encountered issues by the AI vehicle actors are reported in the following table draw in the *Data analysis process and identification of single situations* document done by BPI for the PRISSMA project (cf. [8]):

Some responsibility attribution issues	Definition
"Responsibility gap"	With regard to autonomously learning and acting machines: how can humans be held responsible when they have no or insufficient control?
"Problem of many hands" In response, some authors have proposed the concept of distributed responsibility. 'The effects of decisions or actions based on AI are often the result of countless interactions among many actors, including designers, developers, users, software, and hardware…. With distributed agency comes distributed responsibility'.	There are usually many people causally involved in the action, which renders it difficult if not impossible to (a) find the responsible individual, if there is only one individual responsible, or (b) hold any one individual responsible: there may be more people responsible since there are so many agents involved.
"Problem of temporal dimension"	Who does what at what time (and where)? This can refer to the use of the technology and specific operations, for example who does what at what time in the cockpit of an airplane (e.g. to deal with an autopilot software problem), but it can also extend to the development of the technology. In the case of technology use and development, there is often a long causal chain of human agency. In the case of AI this is especially so since complex software often has a long history with many developers involved at various stages for various parts of the software.
"Knowledge problems: transparency and explicability"	How "voluntary" and "free" the use of AI is when considering the end-user, given that this user might not understand AI or might not even know that she uses AI (or indeed is used by AI). This leads us to questions concerning knowledge.

Table 25: Definition of some responsibility attribution issues.

9 CONCLUSION

To conclude, in order to successfully develop an AI vehicle, it is not advisable to skimp on the validation and approval norms. Indeed, it can be a real blocking point, so the present document aims to enumerate and identify all the different elements that should be taken into account for having a complete regulated system in the shortest possible time.

This inventory has to be updated when new important frameworks or contents are published and may complete or modify current status about these different validation and approval support elements which constitute at the end of the day a meaningful and comprehensive corpus of justification and demonstration rationale for acceptance of those complex systems.

10 REFERENCES

[1] LNE, «Referentiel de certification de processus pour l'IA - Ref : LNE/DEC/CITI/CH,» 12/07/2021.

[2] BPI France - Projet PRISSMA, «WP6 - Progress meeting,» 05/01/2023.

[3] UTAC - Rafael DE SOUSA FERNANDES, «Vision du contexte réglementaire et des activités prenant en compte l'impact de l'IA sur la validation des véhicules automatisés.,» chez *L'IA pour les nouvelles mobilités*, 21 & 22 Septembre 2022.

[4] European Commission MVWG-ACV, “Proposals for Interpretation Document for the Commission Implementing Regulation (EU) 2022/1426 on 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,” 2022.

[5] DGITM/SAGS/EP, DGEC/SD6, Ministère de la transition écologique et solidaire, et Ministère des transports., “International horizontal regulation of automated vehicles,” 10/08/2017.

[6] BPI France for the PRISSMA Project, “Liv. 6.4 : Integration of AI specifications into design standards.,” 2022.

[7] VMAD, “New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS),” 2022.

[8] BPI France for the PRISSMA project, “Liv. 7.2 : Data analysis process and identification of single situations.,” 12/01/2023.

[9] BPI France for the PRISSMA project, “Liv. 3.1 : State Of The Art and inventory of the existing situation.,” 2022.

[10] BPI France for the PRISSMA project, “Liv. 0.1 : Tests in real conditions State Of The Art : Primarily report.,” 2022.

[11] BPI France for the PRISSMA project, “Liv. 6.2 : State Of The Art risk assessment and certification for AI : Intermediate report.,” 2022.

[12] BPI France for the PRISSMA project, “Liv. 8.14 : Report on the impact of AI in system engineering choices.,” 2022.

[13] BPI France for the PRISSMA project, “Liv. 8.11 : Operational Design Domain.,” 2022.

[14] DGITM, «Conduite automatisée / Articulation des rôles du conducteur et du système : Approche descriptive à partir d'un panel de scénarios.».

[15] DGITM/SAGS/EP, “Safety demonstration of automated road transport systems (ARTS): Excepted contributions of the driving scenarios.,” 2022.

[16] DGITM, «Nouvelle approche de validation des systèmes et d’homologation des véhicules.,» 2019.

[17] DGITM/STRMTG/IFSTTAR/Ministère de la transition écologique et solidaire, «STPA : Analyse de securite des parcours prédéfinis.,» 2021.

[18] DGITM/DMR/TUD, “Safety demonstration of automated road transport systems: contribution of driving scenarios.,” 2022.

[19] DGITM/DMR/TUD-VA, “Vehicles and automated transport systems: First principles and questions for the definition of the ODD.,” 2022.

[20] DGITM/DMR/TUD-VA, “Safety validation of automated road transport systems: Clarification through the analysis of accident data.,” 2022.

[21] STRMTG/Ministère chargé des transports, «Systèmes de transport routier automatisés : Mission de l'organisme qualifié agréé pour l'évaluation de la sécurité et pour l'audit de sécurité en exploitation des STRA.,» 2022.

[22] STRMTG/Ministère chargé des transports, «Systèmes de Transport Routier Automatisés : Guide technique relatif à la démonstration GAME pour les STRA.,» 2022.

[23] DGITM/SAGS/EP1, «Quelques éléments d’éclairage sur les compétences de supervision et d’intervention à distance.,» 18/01/2022.

[24] DGITM/DMR/TUD, «Démonstration de sécurité des systèmes de transports routiers automatisés : Apport des scénarios de conduite.,» 2022.

[25] Ministère de la transition écologique et de la cohésion des territoires, «Arrêté du 5 août 2022 pris en application de l’article R. 3152-24 du code des transports relatif au contenu des avis des organismes qualifiés agréés.,» 2022.

[26] Ministère de la transition écologique et de la cohésion des territoires, «Arrêté du 2 août 2022 pris en application de l’article R. 3152-30 du code des transports, relatif à la procédure d’agrément des organismes qualifiés.,» 2022.

[27] VMAD, “New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS).,” 02/2022.

[28] Université Gustave Eiffel/STRMTG, «Méthode de caractérisation des parcours.,» 2021.

[29] FRAV, “Recommendations concerning Safety Requirements for the Assessment of Automated Driving Systems and ADS Vehicles.,” 2023.

[30] STRMTG/Ministère chargé des transports, «Systèmes de Transport Routier Automatisés : Guide d'application relatif à la cybersecurite pour les STRA.,» 2022.

[31] DGITM/DMR/TUD, «Utilisation des scénarios pour la démonstration de la sécurité des systèmes de transports routiers automatisés.,» 2023.

[32] BPI France/PFA/Université Gustave Eiffel, «Analyse de l'ISO24737 Low Speed Automated Driving systems.».

[33] AFNOR, “ISO/PAS 21448.,” 2019.

[34] BPI France for the PRISSMA project, “Liv 2.8 : Proofs-Of-Concept intermediate report developement of platforms meeting the desired objectives of evaluating means of automated mobility.,” 2022.