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

[L8.4] REFERENCE REPORT ON VALIDATION PRINCIPLES AND PROCESSES AS WELL AS THE ACTORS' REPARTITION

RAPPORT DE RÉFÉRENCE SUR LES PRINCIPES ET PROCESSUS DE VALIDATION ET SUR LA RÉPARTITION DES ACTEURS

Main authors : Rafael de Sousa Fernandes (UTAC), Florent Sovignet (STRMTG), Elodie Chateauroux (Transpolis), Morayo Adedjouma (CEA), Christophe Gransart (UGE)

Keywords: Validation, Processes, Tools, Approval, Certification

Abstract.
This deliverable presents, a first state of the art is proposed on the different working groups, their positions and the works at national/international level in close connection with PRISSMA. This analysis focuses on the application modalities of security at the level of the different study perimeters and integrates, among others, the regulatory framework mentioned by the DGITM and the associated ARTS decrees. A survey of the different standards in the field of autonomous mobility, regarding the allocation of safety and security objectives, has also been made.

Résumé.
Ce livrable, propose un premier état des lieux sur les différents groupes de travail, leurs positions et les travaux à l'échelle nationale/internationale en lien étroit avec PRISSMA. Cette analyse se focalise sur les modalités d'application de la sécurité au niveau des différents périmètres d'étude et intègre, entre autres, le cadre réglementaire mentionné par la DGITM et les décrets STRA associés. Ce document inclus également un recensement des différents standards en matière de mobilité autonome, pour ce qui concerne l'allocation des objectifs de sûreté et de sécurité.

Authors	Rafael de Sousa Fernandes (UTAC), Florent Sovignet (STRMTG), Pierre Jouve (STRMTG), Elodie Chateauroux (Transpolis), Morayo Adedjouma (CEA), Diana Razafindrabe (CEA), Christophe Gransart (UGE), Michel Kaczmarek (APSYS)
Document ID	PRISSMA/L8.4/V10
Date	11/10/2021
Type of document	Report
Status	Deliverable
Confidentiality	Confidential
WP allocation	WP8-T8.3
Distribution	PRISSMA partners
History Version 0	 30/08/2021 Creation
Version 1	01/09/2021 Section 2.3.1 from Florent Sovignet (STRMTG) added
Version 2	05/10/2021 Section 6.1 from Elodie Chateauroux (Transpolis) added
Version 3	10/10/2021 Document restructuring
Version 4	11/10/2021 Section 6.2 from Morayo Adedjouma (CEA) added
Version 5	15/10/2021 Addition of the Appendices and the section 2.4 from Christophe Gransart (UGE)
Version 6	18/10/2021 Pagination correction and addition of the Section 6.4 from Michel Kaczmarek (APSYS)
Version 7	21/10/2021 Abstract added
Version 8	25/10/2021 Section 4.6 and 4.7 added, Annex VI added
Version 9	26/10/2021 Document update regarding Morayo Adedjouma remarks, Section 5.2 from Diana Razafindrabe (CEA) added
Version 10	28/10/2021 Document update regarding Florent Sovignet (STRMTG) remarks
Version 11	02/02/2022 layout updated to include the new logo ; Chapter 3 updated according to the last inputs from FRAV and VMAD

1 Introduction

This document is related to task T8.3 of WP8. This task aims to identify the working groups at national/international level with works closely related to the PRISSMA (Plateforme de Recherche et Investissement pour la Sûreté et la Sécurité de la Mobilité Autonome) project work, to complete their positions and to detail their works . This analysis will focus on the modalities of application of security at the level of the different study perimeters and will integrate, among others, for France, the regulatory framework set by the DGITM and the associated ARTS decree. The objective is to provide an initial baseline of the safety requirements that have to be refined to ensure the safety assurance of autonomous vehicle within the context of PRISSMA project.

The present document is structured in four main chapters, six appendices, a glossary and references.

The aim is to summarize the principles and processes of validation as well as the actors' repartition.

To do so, Chapter 1, establishes a first state of the art by focusing on the efforts made at the European level for the validation of AI systems. We will be interested more particularly, in how they are declined for the autonomous vehicles, but also the actions set up by the Member States in this context.

Chapter 2 and Chapter 3, details what the United Nations and other countries outside of EU are planning on the issue of AI system validation, respectively. For example, the first global technical regulation on autonomous vehicles - UNR157 – that is issued since January 2021 allows now any manufacturer to ask for the approval of the function Traffic Jam Chauffeur in Europe and in the countries that signed the 1968 Vienna agreements.

Chapter 4 highlights complementary or competing projects to PRISSMA as well as standards already in place

The inventory of the various standards should help understand the impact of the use of AI in the system engineering choices for autonomous vehicle that the PRISSMA project will analyze, including the consequences on the necessary evolutions.

2 European Union

In 2019 the High-Level Expert Group on Artificial Intelligence (AI HLEG), set up by the European Commission, published the Ethics Guidelines for Trustworthy Artificial Intelligence. The third chapter of those Guidelines contained an Assessment List to help assess whether the AI system that is being developed, deployed, procured or used, adheres to the seven requirements of Trustworthy Artificial Intelligence (AI), as specified in the Ethics Guidelines for Trustworthy AI:

1. Human Agency and Oversight;
2. Technical Robustness and Safety;
3. Privacy and Data Governance;
4. Transparency;
5. Diversity, Non-discrimination and Fairness;
6. Societal and Environmental Well-being;
7. Accountability.

A final version of this Assessment List was published in July 17th 2020.
For the European Commission (EC), a trustworthy approach is key to enabling responsible competitiveness where the design, development and use are lawful, ethical and robust of an AI system can trusted.
The recent proposal (published on April 21st) for a new framework called the AI Act quote the same approach. The AI act proposal defines the first-ever legal framework on AI and a new Coordinated Plan with Member States (updating a first plan dating from 2018), which describes the guidelines and investments needed to strengthen Europe's ambition to become the world leader on the AI topic. This follows the publication of the High-Level Expert Group on Artificial Intelligence (HLEG) developed Guidelines for Trustworthy AI in 2019, and an Assessment List for Trustworthy AI in 2020. In addition, the Commission's White Paper on AI, published on 19 February 2020, set out a clear vision for AI in Europe: an ecosystem of excellence and trust, setting the scene for today's proposal.
These documents give an overview of the regulatory context [Annex VI] that is emerging and that we will look at in more detail, particularly for the validation of embedded AI systems in the automobile, in the deliverables to come within the PRISSMA project.

2.1 Motor Vehicles Working Group (MVWG)

This working group exists since 1970 and is devoted to discussions between all stakeholders from governments, industry and consumer associations interested in the regulatory activities concerning motor vehicles.
Its task is to assist the Commission in the preparation of delegated acts, legislative proposals and policy initiatives.

2.1.1 Automated and Connected Vehicles (ACV)

This group is a sub-working group of the MVWG that is devoted to discussions between all stakeholders from governments, industry and consumer associations interested in the regulatory activities related to the automated and connected vehicles.
The group presented the following elements during the last session that occurred in October 2021. It is interesting to consider them in the understanding of the validation context of an ADS and later of an ADS embedding AI but they do not strictly represent the PRISSMA approach.

From the industry's perspective (OICA, ACEA), the certification of an ADS is a complex matter that goes beyond the application of prescriptive requirements and their assessment through a series of repeatable and reproducible tests, as common in the traditional certification regimes. Thus, the introduction of a scenario-based approach leveraging audit, simulations, and physical testing is deemed appropriate to assess the system performance against relevant requirements.
However, it is also true that given the multiplicity of variables, differences in the ODDs and functionalities offered by the manufacturers, ensuring a set of scenarios that is "fit-for-all applications" would be impracticable.
Therefore, this approach aims to suggest the use of harmonized tools and procedures to ensure that each ADS – identified with a unique ODD – is assessed within a range of scenarios that is representative of its specific performance, operational limits, and functionalities.
In addition, they pointed out the fact that providing some standardization in the assessment criteria, whilst ensuring the necessary flexibility to address the uniqueness of the ADS and its functionality, seems the most viable solution to ensure appropriate coverage when deriving scenarios for testing.

2.1.1.1 The importance of the ODD

During the exchanges in this working group, OICA proposed its vision of the Operational design domain (ODD), which for them, refers to the operating environment in which vehicles can operate safely (the elements necessary to understand this concept are detailed in PRISSMA deliverable L8-9). Considering that it covers environmental conditions such as rainfall, scenery elements such as drivable area, and dynamic element such as macroscopic traffic behavior and designated speed of the subject vehicle.
Given a specific ODD, and according to this approach, it should be crucial for the ADS to ensure that:

- it can operate safely within its ODD
- it will be primarily used within its ODD
- it can monitor whether it is inside/outside its ODD, and consequently react to it.

Commonly, ODD is associated with establishing relevant safety requirements (i.e., behavior competencies) for an ADS and has a key role to play in identifying scenarios that are useful in validating that the ADS has those competencies.
As ODD defines the operating conditions of the ADS, it also needs to support the scenario generation process for testing the ADS. Additionally, this definition of an ODD can also

potentially support the definition of scenario coverage and safety metrics in order to claim completeness. Furthermore, ODD could also provide requirements for simulation platforms when used as part of safety evidence generation using virtual testing (*More information on the exchanges within the VMAD on this topic §3.1.4*).

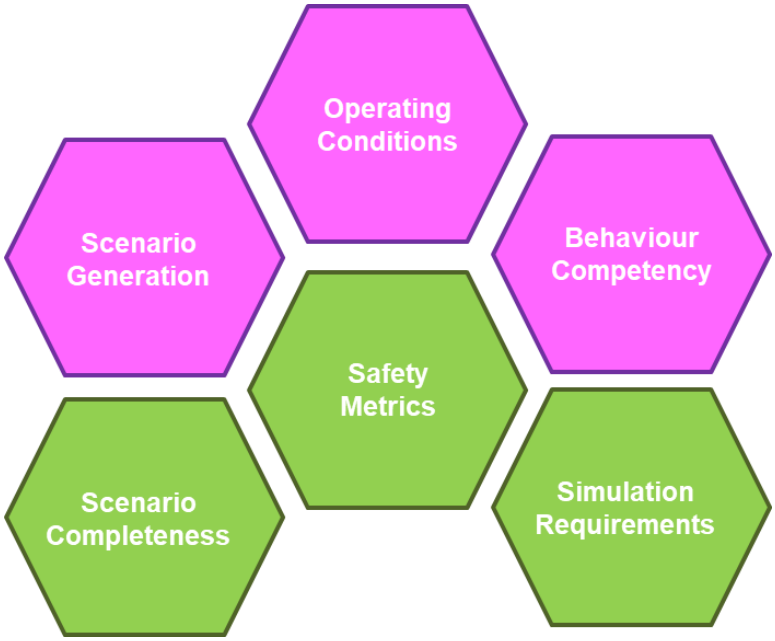


Figure 1: Scenario coverage and safety metrics [22]

From a process flow perspective, at a simplistic level, one could look at scenarios as a combination of ODD attributes and behavior competencies. Therefore, the combination of these elements will lead to the definition of functional, logical, and subsequently concrete scenarios.

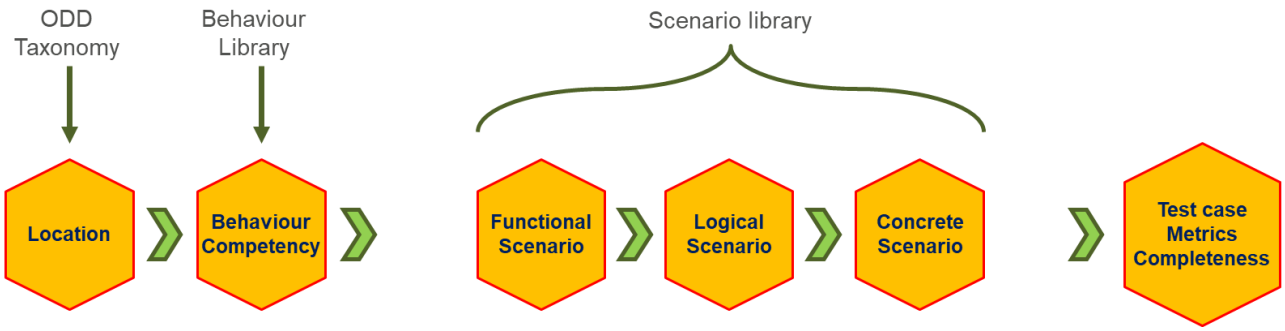


Figure 2: Scenario combination [22]

2.1.1.1.1 ODD-based safety framework approach

The approach presented in this document sets its foundations on the manufacturer or the ADS developer's description of the ODD for each of the ADS features available on the vehicle, according, as a minimum, to the provisions described in FRAV (*those provisions are described later in this deliverable §3.1.1).* The purpose of an ODD description is to inform determinations on the requirements and scenarios applicable to an ADS feature.

Figure 3 depicts the process flowchart used in the ODD-based approach. This can be summarized by considering the interaction of the following five key elements:

- Scenario Generation
- Scenario Classification
- Functional Requirements & Road Traffic Rules
- Overall ADS performance
- Scenario to test case generation

From a qualitative perspective, scenarios can be classified into:

- Nominal Scenarios
- Critical Scenarios
- Failure Scenarios

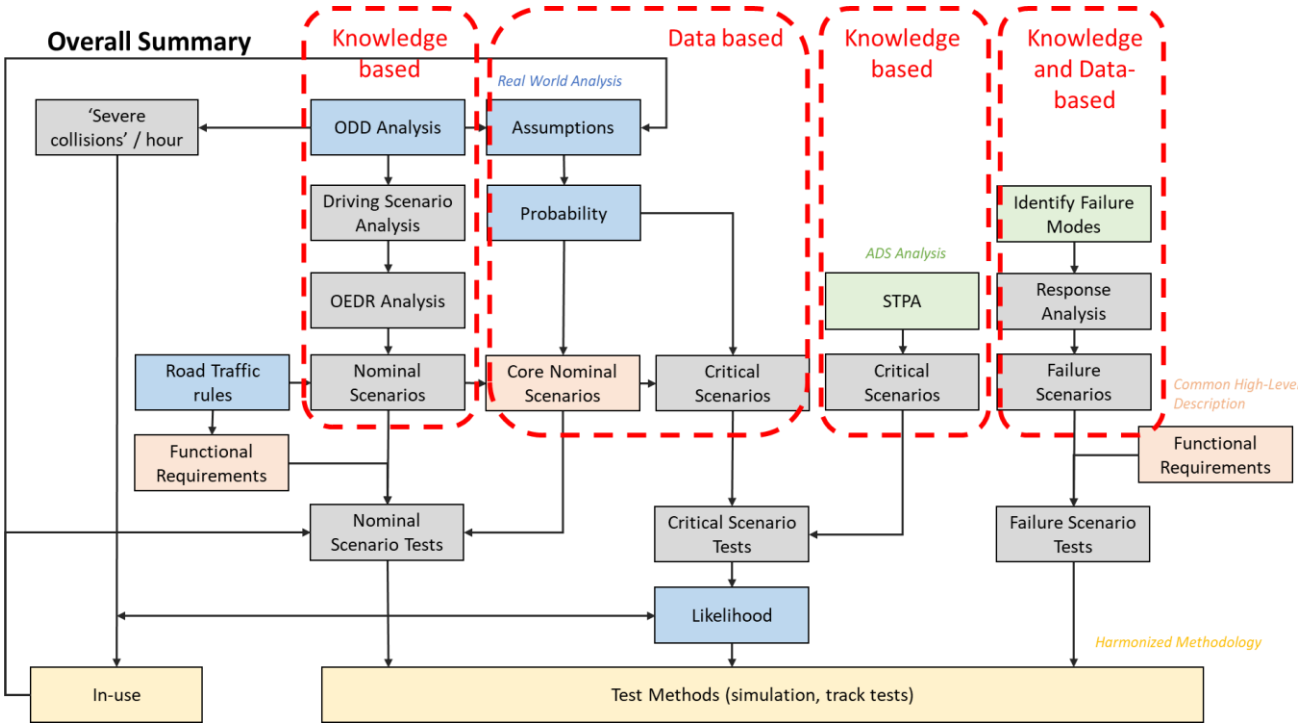


Figure 3: ODD-based approach flowchart [22]

For each of these categories, one can use either a data-based approach or a knowledge-based approach to generate scenarios. Erreur ! Source du renvoi introuvable. depicts how tools normally used during the development of the ADS could be applied to support scenario generation. Relevant techniques include driving scenarios, object and event detection and response for nominal conditions (e.g., SOTIF); safety analysis for critical and failure conditions (e.g., STPA, FTA, FMEA).

Assumptions and statistical analysis based on real-world taxonomy and data collection, performed by the manufacturer, are fundamental to ensure the correct scenarios parametrization (functional to logical to concrete); whilst functional requirements derived by FRAV, behavioral competences and the road traffic rules relevant to the country where the ADS is intended to operate are used to derive pass and fail criteria for each of the applicable scenario.

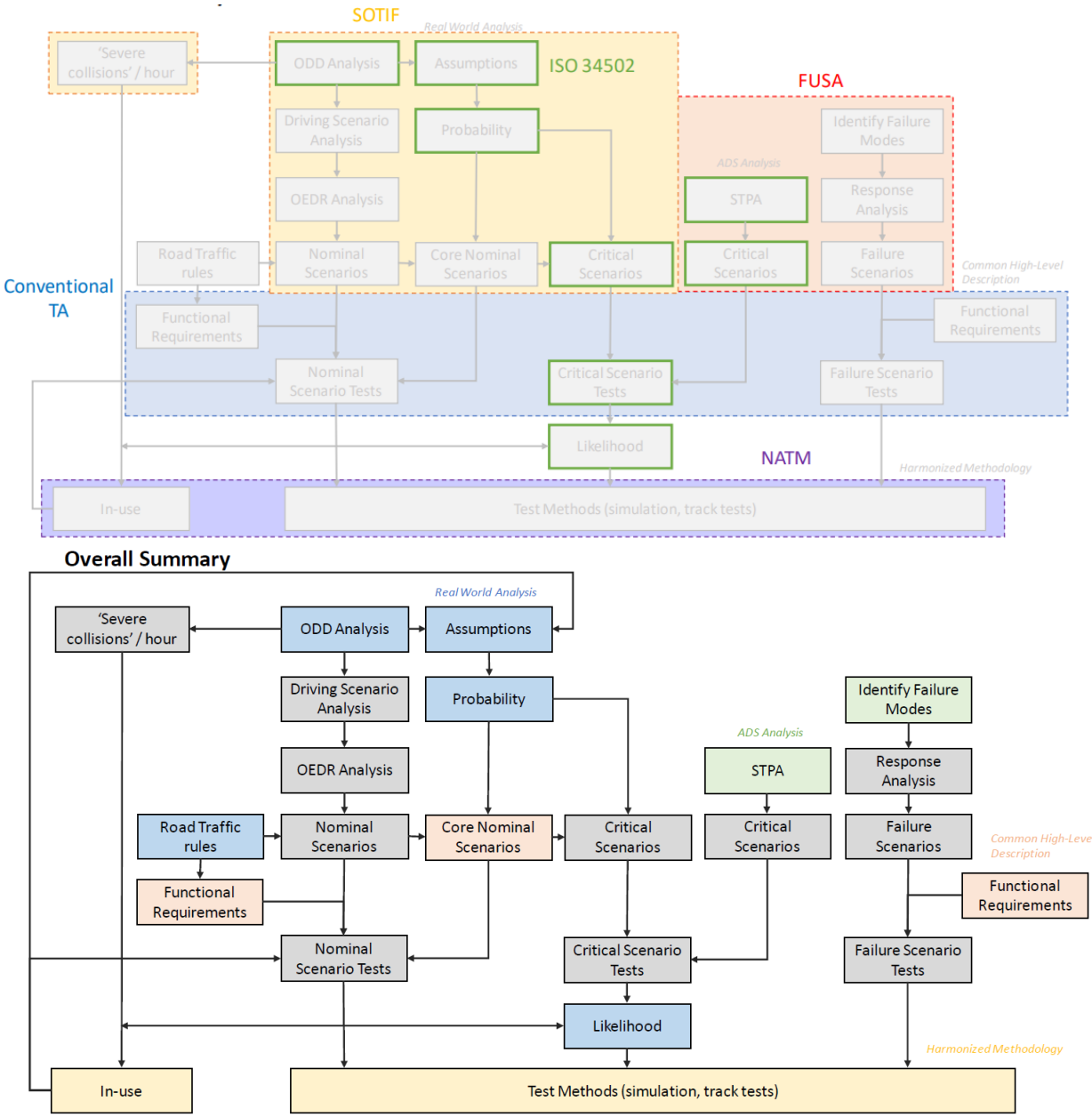


Figure 4 : Conventional TA, Functional and Operational Safety used in the ODD framework [22]

2.1.1.1.2 Scenario generation

From a scenario generation perspective, two types of methods may be used:

- Knowledge-based scenario generation
- Data-based scenario generation

A knowledge-driven scenario generation approach utilizes domain specific knowledge to identify hazardous events systematically and create scenarios. A data driven approach utilizes the available data to identify and classify occurring scenarios. Figure 4 illustrates various data-based and knowledge-based scenario generation methods.

Accident datasets and field data can be analyzed to identify accident hotspots and scenario parameters that contribute to causation of accidents carrying high levels of severity.

Knowledge based methods, an extension to the Systems Theoretic Process Analysis (STPA) method, can be used to analyze the characteristics of the ADS architecture and identify system failures and hazardous situations. The analysis was then converted into a set of logical scenarios together with their corresponding pass/fail criteria.

Other knowledge-based methods include the formal analysis approach with the highway code rules for scenario generation. Each of the highway code rules describes a hypothetical driving scenario with the corresponding behavior and ODD elements. The ODD is a specification set out by the manufacturer of an ADS and it defines the operating conditions within which the ADS can operate safely. Formal models are generated via a model template to create the mathematical representations of those scenarios, collecting the combinations of ODD and behavior parameters. The analysis reports the maneuver parameters that are close of violating the pass criteria and produce scenarios that represent these set of violations. Other knowledge-based methods use formal representation of the ODD and behavior competencies of the ADS for scenario generation.

Furthermore, the existing scenarios already defined in the standards, regulations or guidelines can also be utilized for the testing of ADSs, or example, the scenarios set out in ISO22737 and NCAP. ISO22737 has been developed for low-speed automated driving systems (LSAD) and the NCAP provides a set of testing scenarios for the safety assurance of vehicles.

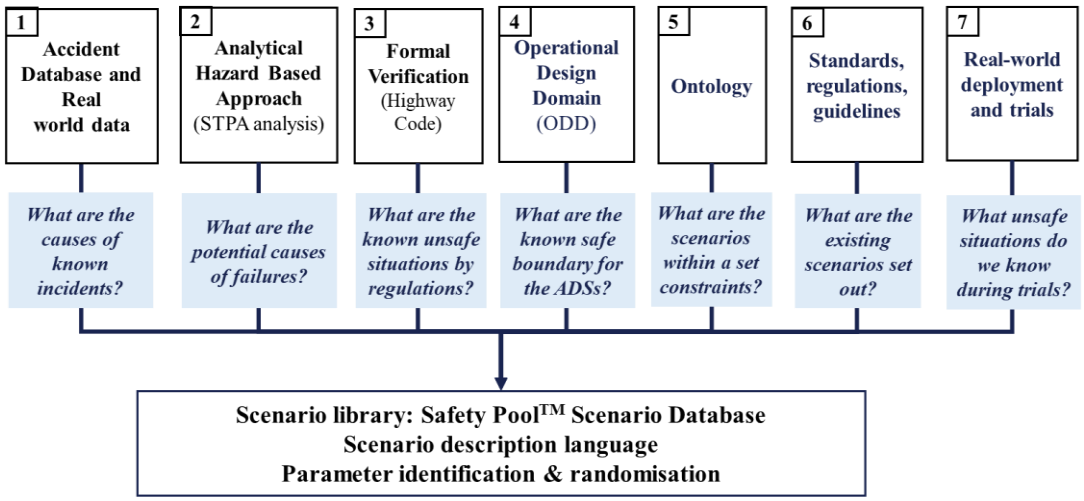


Figure 4: Scenario Generation sources [22]

2.1.1.2 Scenario classification

2.1.1.2.1 Nominal Scenarios

Nominal scenarios for the purpose of this document are reasonably foreseeable situations encountered by the ADS when operating within its ODD. These scenarios, often referred to as "traffic scenarios", represent the interaction of the ADS with other traffic participants.

A core set of nominal scenarios, based on the highway applications, is listed in **[Annex I]**. These scenarios are derived from a literature review of existing databases (see **[Annex II]** – Core Scenarios for a non-exhaustive list) and represent the very least common denominator to assess the ADS performance for the highway use-case.

However, it is understood that additional nominal scenarios are needed to ensure a robust coverage of the whole range of foreseeable situations that an ADS, might encounter during normal operations.

Therefore, the approach suggests a series of analytical frameworks that could help the manufacturer to derive nominal scenarios appropriate for the specific application. These frameworks are divided into:

- ODD Analysis
- Driving Scenario Analysis
- OEDR Analysis

2.1.1.2.1.1 ODD analysis

This analysis represents the first step performed by the manufacturer with the aim to identify the characteristics of the ODD. An ODD may consist of scenery elements (e.g., physical infrastructure), environmental conditions, dynamic elements (e.g., traffic, vulnerable road users) and operational constraints to the specific ADS application. Existing standards may be used as a reference, as shown in the Toolbox in **[Annex II]**.

2.1.1.2.2 Driving Analysis

In the driving analysis, the ODD relevant characteristics are then explored in more detail by associating properties and defining interactions between the objects. Here the effect of ODD on the behavior competencies is explored.

An example of the analysis is given in

Table 1, where the object "vehicles" is given a set of properties (behavior competencies) such as "acceleration", "deceleration", "cut-in"; whilst "pedestrians" are "crossing road", "walking on sidewalk", etc.

Objects	Events/Interactions
Vehicles (e.g., cars, light trucks, heavy trucks, buses, motorcycles)	**Lead vehicle decelerating (frontal), lead vehicle stopped (frontal), lead vehicle accelerating (frontal), changing lanes (frontal/side), cutting in (adjacent), turning (frontal), encroaching opposing vehicle (frontal/side), encroaching adjacent vehicle (frontal/side), entering roadway (frontal/side), cutting out (frontal)**
Pedestrians	**Crossing road – inside crosswalk (frontal), crossing road – outside crosswalk (frontal),** walking on sidewalk/shoulder
Pedalcyclists	**Riding in lane (frontal),** riding in adjacent lane (frontal/side), riding in dedicated lane (frontal/side), riding on sidewalk/shoulder, **crossing road – inside crosswalk (frontal/side), crossing road – outside crosswalk (frontal/side)**

Objects	Events/Interactions
Animals[5]	Static in lane (frontal), moving into/out of lane (frontal/side), static/moving in adjacent lane (frontal), static/moving on shoulder
Debris[6]	**Static in lane (frontal)**
Other dynamic objects (e.g., shopping carts)	**Static in lane (frontal/side), moving into/out of lane (frontal/side)**

Objects	Events/Interactions
Traffic signs[7]	Stop, yield, speed limit, crosswalk, railroad crossing, school zone
Traffic signals[7]	Intersection, railroad crossing, school zone
Vehicle signals	Turn signals

Table 1: Dynamic elements and their properties [22]

2.1.1.2.3 OEDR Analysis: Behavior competency identification

Once the objects and relevant behavior competencies have been identified, it is possible to map the appropriate ADS response. The response is modelled on applicable functional requirements, as developed by FRAV and by applying traffic laws of the country where the ADS is intended to operate, as referred to in the paragraph Functional Requirements.

The outcome of the analysis is also a set of behavior competences that can be applied to the events characterizing the ODD to ensure compliance with the applicable regulatory and legal requirements. Table 2 provides a qualitative example of a matching event – response.

Event	Response
Lead vehicle decelerating	Follow vehicle, decelerate, stop
Lead vehicle stopped	Decelerate, stop
Lead vehicle accelerating	Accelerate, follow vehicle
Lead vehicle turning	Decelerate, stop
Vehicle changing lanes	Yield, decelerate, follow vehicle
Vehicle cutting in	Yield, decelerate, stop, follow vehicle
Vehicle entering roadway	Follow vehicle, decelerate, stop
Opposing vehicle encroaching	Decelerate, stop, shift within lane, shift outside of lane
Adjacent vehicle encroaching	Yield, decelerate, stop
Lead vehicle cutting out	Accelerate, decelerate, stop
Pedestrian crossing road – inside crosswalk	Yield, decelerate, stop
Pedestrian crossing road – outside of crosswalk	Yield, decelerate, stop
Pedalcyclist riding in lane	Yield, follow
Pedalcyclist riding in dedicated lane	Shift within lane[9]
Pedalcyclist crossing road – inside crosswalk	Yield, decelerate, stop
Pedalcyclist crossing road – outside crosswalk	Yield, decelerate, stop
Lead vehicle decelerating	Follow vehicle, decelerate, stop
Lead vehicle stopped	Decelerate, stop
Lead vehicle accelerating	Accelerate, follow vehicle

Table 2: Behavior competences for given events [22]

The combination of objects, events, and their potential interaction, as a function of the ODD, constitute the set of nominal scenarios pertinent to the ADS under analysis. An example of nominal scenarios is illustrated in

ODD (Dynamic) Element	Driving Behaviour	Traffic Rule	Functional Requirement	Behaviour Competency	Test Scenario
Bicycle	Riding in lane (Frontal)	Drivers will also need to use a minimum passing distance for bicycles of 1.5m in urban areas, and 2m out of town	The ADS should adapt its behaviour in line with safety risks	ADS should ensure relative velocity during passing manoeuver doesn't exceed [30]km/h	The ADS shall travel between [30-50]km/h on the centre line of the road. A cyclist shall travel in the same direction as the ADS between [10-20]km/h, [0.2-1]m away from the lane edge. Test scenarios that require lane crossing shall be conducted with/without oncoming traffic.
			The ADS should comply with road traffic rules	Shift in lane to pass by cyclist with 1.5m lateral distance	
			The ADS behaviour should not disrupt the flow of traffic	The ADS may cross the center lane marking to ensure the safe passing distance is not violated	
			The ADS should interact safely with other road users	The ADS shall activate the turn signal if the center lane marking is crossed	

Table 3.

Table 3: Example of Nominal Scenario [22]

As parameters (assumptions) for the events are yet to be defined, the nominal scenarios derived from the application of the analysis are to be considered in their functional and logical abstraction layer. **[Annex III] presents** examples of nominal scenarios in their concrete layer.

2.1.1.2.4 Critical Scenarios

Critical scenarios for the purpose of this document can be derived in two ways: by considering edge-case assumptions on nominal scenarios or by applying standardized methods for the evaluation of operational insufficiencies (e.g., STPA) – see **[Annex II]**. Focusing on the second methodology and by way of example, the STPA is based on System Engineering and considers system safety as a control problem. Therefore, breaches of control laws (or constraints) cause accidents. The analysis can be summarized by the following four steps:

- Identify System-level Hazards
- Creation of system control structure
- Identify Unsafe Control Actions (UCAs)
- Identify Causal Factors

Furthermore, the UCAs and causal factors can be parametrized to derive test scenarios and pass/fail criteria.

In the example depicted in Table 4, the identified hazard *"vehicle does not maintain safe distance from lead motor vehicle"* is linked to the relevant unsafe control action *"braking demand is not provided"* and to the potential causal factors *"undetected / misclassified object"* or *"incorrect sensor fusion results"*. The UCA and the causal factors can then be parametrized to generate a critical scenario.

Losses	Hazards	Unsafe Control Action	Loss Scenario	Casual Factors	Test Behaviour	Test Scenario
Collision with objects outside the vehicle	Vehicle does not maintain safe distance from lead motor vehicle	Braking demand is not requested	Object in vehicle trajectory is not detected	undetected / misclassified objects obscured object Incorrect sensor fusion results	ADS is following behind a lead vehicle. Headway between the two vehicles is set by the ADS. Lead vehicle decelerates at the max assumed rates depending on the weather conditions	Lead vehicle decelerates to turn [Right / Left] or travel straight on at a [mini / large] roundabout
			Object is not considered to be in the vehicle trajectory	Localisation issues leading to incorrect positioning of ego vehicle or object		Lead vehicle decelerates whilst shifting in lane to avoid [static object / other road user]

Table 4: Example of Critical Scenario derived from STPA [22]

As assumptions for the events are yet to be defined, the critical scenarios at this stage are to be considered in their functional/logical abstraction layer. **[Annex III] presents** examples of critical scenarios in their concrete layer.

2.1.1.2.5 Failure Scenarios

These scenarios aim to assess the response of the ADS to a failure. Different methods are available in literature - see **[Annex II]** for reference - and include the Failure Modes and Effects Analysis (FMEA) for which an example is given in Table 5.

An FMEA can generally include the following steps:

- Identify potential failure modes
- Identify potential causes and effects of those failure modes
- Prioritize the failure modes based upon risk
- Identify appropriate corrective actions or mitigation strategies

Behavior Failure	Effects
Fail to maintain lane	Impact adjacent vehicle or infrastructure
Fail to maintain safe following distance	Impact lead vehicle
Fail to detect and respond to maneuvers by other vehicles	Impact lead or adjacent vehicles
Fail to detect relevant obstacles in or near lane	Impact obstacles
Fail to identify ODD/OEDR boundary	Operate outside of ODD/OEDR capabilities

Table 5: Example of FMEA [22]

For each of the behavior failures and consequential effects listed, the manufacturer must put in place relevant strategies when developing the ADS (i.e., fail-safe).

When applying the failure scenarios, the objective is to assess the ability of the ADS to comply with requirements derived by FRAV for safety-critical situations, including for example "The ADS should manage safety-critical driving situations" and "The ADS should safely manage failure modes" and their respective sub-requirements, as described in Functional Requirements.

An example of Failure Scenario is reported in Table 6. For a more comprehensive list of failure scenarios, refer to **[Annex III]**.

Failure Type	Failure Mode	Potential Cause	Response	Functional Requirement	Test Scenario	Pass/Fail Criteria
Perception	Fail to identify ODD boundary	Failure to detect ODD attribute e.g. Heavy Rain / Fog	Safely stop in lane of travel	The ADS shall be able to detect the ODD and predict when the ADS is about to leave the ODD	The ADS shall operate upto and beyond the predfined ODD. ODD characteristic to consider include geographical area and weather conditions	The ADS detects the ODD conditions are not met and issues a minimal risk manoeuver.
				When the system detects that it is difficult to continue in the automated driving mode, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre.		The minimum risk manoeuver should not cause the vehicle to decelerate greater than 4m/s2
				Other road users and occupants shall be informed that the vehicle is performing a minimum risk manoeuvre in accordance with applicable traffic rules (e.g. hazard lights, brake lights, turning indicators)		The ADS should activate the hazard lights through out the minimal risk manoeuver.
				The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules.		The ADS shall use the turn indicator when changing lanes.

Table 6: Example of Failure Scenario [22]

2.1.1.2.5.1 Assumptions: Logical to concrete scenarios

To ensure that the nominal and critical scenarios identified in the previous paragraphs are ready to be assessed through the application of simulations or physical testing, as highlighted in the **[VMAD MD]**, the manufacturer or the ADS developer needs to coherently parametrize them by applying assumptions.

As assumptions carry a degree of subjectivity and therefore cannot be harmonized across different applications, the manufacturer or the ADS developer shall provide evidence to support the assumptions made. Several tools are available and include data collection campaigns performed during the development phase, real-world accidents and realistic driving behavior evaluations: amongst others.

Figure 5 provides an example of parametrization based on naturalistic driving data for three events. In the pedestrian crossing scenario, the ego vehicle speed, distance from the pedestrian and crossing speed from 2,689 events are ingested by a stochastic model that provides probability distributions of potential outcomes from which relevant parameters can be extrapolated. Different tools can be used for the scope, refer to **[Annex II]** for a non-exhaustive list.

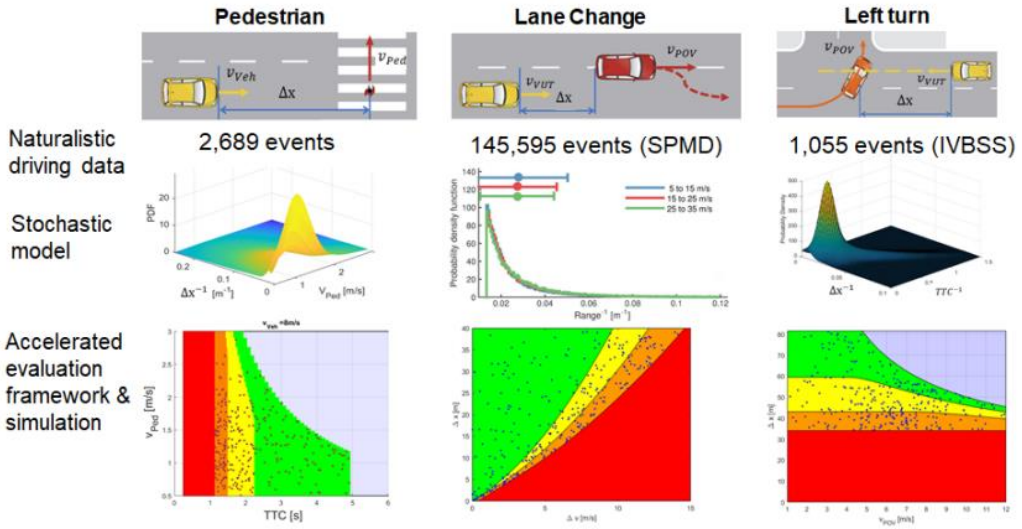


Figure 5: Statistical approaches to derive assumptions [22]

The parameters chosen for the specific scenario can then be representative of the median of the events (e.g., 50th percentile of lead vehicle deceleration at 0.5g) to parametrize nominal scenarios or tighter values could be used to explore the space of critical scenarios (e.g., deceleration at 0.9g), which include reasonably foreseeable and unpreventable situations.

An exemplificative list of nominal, critical and failure scenarios – with relevant assumptions - is given in **[Annex III]**.

It is also possible to use assumptions based on real-world data to generate logical scenarios (data-based scenario generation). Furthermore, assumptions may be applied across all nominal, critical and failure scenarios to create corresponding test cases.

2.1.2 Application of ODD based Rules of Road: As Pass criteria and requirements

One of the open questions in the scenario-based testing of ADS remains the definition of the pass or acceptance criteria. An approach to define an acceptance criterion is to evaluate the scenarios against the "rules of the road". [FRAV ADS Safety Topics] mention that *"The ADS should comply with traffic rules"*. It is challenging to test against this requirement in the absence of "codified rules of the road". Focusing on the interplay between FRAV and VMAD, the proposed approach thus provides necessary guidance to both:

- FRAV activities (from requirements perspective), and,
- VMAD activities (from pass/fail perspective).

Furthermore, they propose an approach to create a **natural language description** and **machine-readable description** of the codified rules of the road that can be used by:
Natural language description: Regulators or type approval authorities
Machine-readable: ADS developers, OEMs, Tier-1s etc. for simulation-based testing purposes and allowing them to identify gaps and contradictions in the rules

If one compares the scope of ODD and the content of current *"rules of the road for human drivers"* (e.g., UK's Highway Code), a large overlap of scenery aspects and environmental condition aspects can be observed. It is therefore plausible to follow an ODD based approach and an ODD taxonomy, to model the environmental and scenery aspects of the *"rules of the road"*. In addition, what is not part of the ODD but is also important for the safety assurance of ADS is the behavior aspect (i.e., behavior competencies). Behavior can be further divided into ego (vehicle under test) behaviors and actor behaviors.
Any rule of the road can be classified into two categories:

- Doing some "behavior" "somewhere"
- NOT doing some "behavior" "somewhere"

While doing or not doing some behavior can be defined as part of ADS's behavior competencies, *"somewhere"* could be considered as "operating condition" or part of the ODD definition. The approach is summarized in Figure 6.

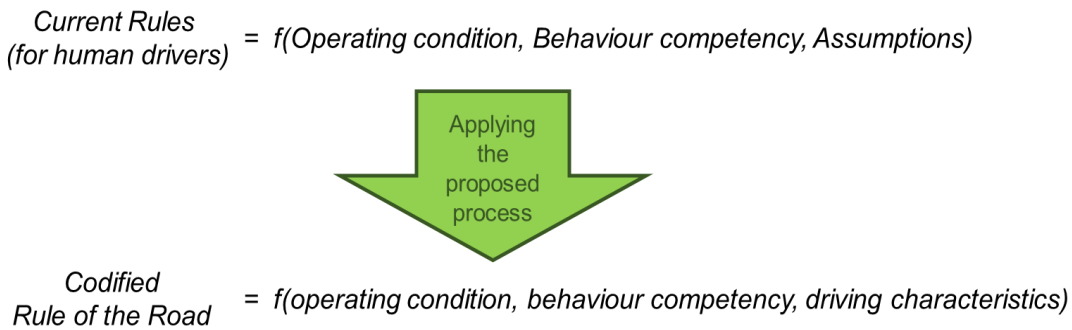


Figure 6: Example of codified Rules of the Road [22]

2.1.2.1 Using rules of the road as pass criteria

For safety assurance, we see FRAV and VMAD activities at three layers of abstraction (see Figure 9):

- Layer 1: Provides the high-level safety requirements **(FRAV Safety Topics)** (harmonized)
- Layer 2: Proves a process for converting high-level safety requirements to verifiable requirements (this paper) (proposal to harmonies)
- Layer 3: Provides concrete values/rules for the requirements (further FRAV/VMAD discussion) (may not be harmonized)

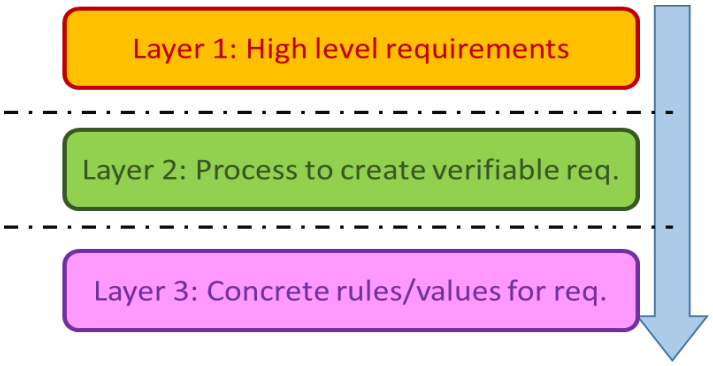


Figure 8 : Three abstraction layers [22]

Furthermore, Figure 7 illustrates the codified rules of the road as a pass criterion for scenario-based testing activities. By supporting scenario generation with ODD and behavior competencies and having rules of the road also supported by the same, it is possible to map every scenario to a corresponding rule(s) of the road using ODD and behavior tags or labels in a scenario catalogue **(VMAD)**.

This approach would allow the test engineer to map each scenario to a corresponding rule (or set of rules). These rules can then serve as the pass criteria during the scenario-based testing approach. This approach can thus enable engineers to show compliance to traffic rules by making the rules of the road verifiable.

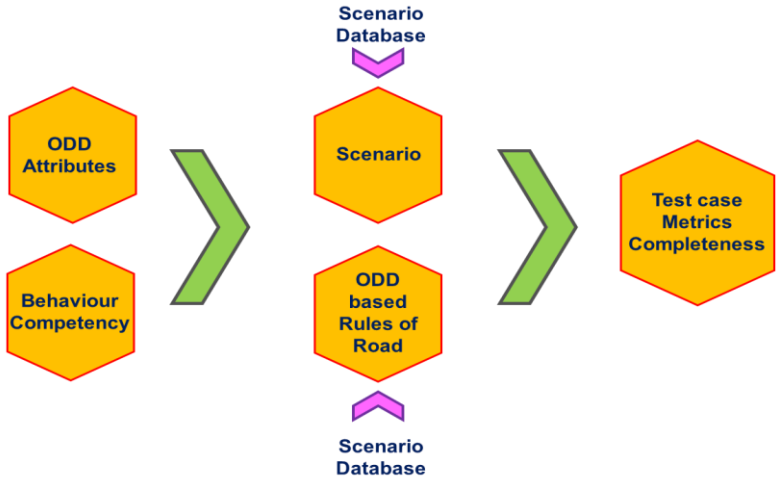


Figure 7: Rules of the Road as pass / fail criteria [22]

2.1.2.2 Performance Evaluation and targets

As previously highlighted, nominal scenarios are reasonably foreseeable and preventable situations within the ODD and therefore it is expected that the ADS would be capable of handling them without any resulting collision.

On the other hand, failure scenarios are performed to assess the ADS ability to recognize faults / failures in the system, and respond in compliance with the principles highlighted by FRAV.

Satisfactory performance for the ADS certification will require that in both nominal and failure scenarios the ADS will meet pass criteria.

A slightly different approach ought to be followed for critical scenarios, especially when derived from the application of assumptions with low likelihood to nominal scenarios. By applying these assumptions and keeping the same evaluation criteria as per the corresponding nominal scenario, the manufacturer would be able to explore the ADS boundaries and limitations, drawing a line between preventable and unpreventable situations.

The residual risk deemed acceptable for a specific ADS application, mapped to the likelihood of those critical scenarios in the operational domain, provides the ADS overall performance and demonstrates that the ADS is free of unreasonable risk.

It will be interesting to return to these elements of understanding with the productions of WP2 and WP3. The question of the definition of the edge cases, remains unresolved, and represents a key element of the validation by scenario.

2.2 Member States

Now that we have presented the work in progress within the European Commission itself, we propose to take a closer look at what is being proposed by some of the member states of the European union.

2.2.1 France

Since the end of 2017, France has committed to a global and coherent strategy for the development of automated vehicles for passengers and freight. ,With the appointment of a High representative in charge of the French strategy for the development of autonomous vehicles (Ms. Anne-Marie Idrac, former state Secretary for Transports) and the implementation of a collaborative working method between public authorities and private actors, led by "France Véhicules Autonomes". The strategic document released by the Government in May 2018 set four main objectives:

Establish the legislative and regulatory framework allowing the circulation of automated vehicles in France by 2022, taking into account the maturation of the various use cases at that time.
Support innovation, mainly through experimentation.
Prepare the security validation framework at the national, European and international scales.
Assess the acceptability issues and the economic outlook for deployment more precisely.

Consistently with objectives #1 and #3, the legislative framework resulting from the Mobility Orientation Law (LOM - 24 December 2019) will allow the circulation of automated vehicles beyond the experiments, thanks to an adapted liability regime, by setting the safety requirements. This framework:

Will cover high levels of automation, for which the systems are able to handle all driving situations in their operational domain without any driver intervention or when the operator is located outside the vehicle.
Will cover the transportation of passengers and the transportation of goods.
Will allow the circulation of public or shared transport of passengers on predefined routes in terms of regulations, from 2022, relying on reference documents for safety demonstration.

The LOM covers the use cases of Personal Vehicle, Road Automated Transport System and Goods Automated Transport. It provides for:
The possibility to adapt the Traffic Code for the circulation of automated vehicles in predefined conditions (routes, traffic, time…) (article 31).
The possibility under conditions for different actors to access the data of an automated vehicle in different situations (article 32).

At the international level, France has supported a systemic vision of safety (vehicles, infrastructure, connectivity, supervision), and the international driving regulation (Vienna Convention) has been adapted to allow the circulation of highly automated vehicles from 2022.

Objectives #2 and #4 led to a national experimentation coordinated program called EVRA launched in 2019: 2 projects (SAM and ENA), 16 experimentations, 3 years, 120 M€ including 42 M€ of subsidies.

SAM (« Sécurité et Acceptabilité de la conduite et de la Mobilité autonome ») : experiments of roll-out on dual carriageways, parking valet, on-demand transport in urban areas, regular transport complementary to existing networks, establishment service from a remote car park, use of a railway right-of-way , autonomous delivery vehicles)
ENA (« Expérimentations de Navettes Autonomes »): experiments of autonomous shuttle services complementary to the urban transport network and rural service.

These projects include use cases with the operator outside the vehicle. The experiments develop within a framework to pool the lessons learned, specifically with regard to liability, safety evaluation and acceptability. More than 120 authorizations to experiment have been granted since 2015.

In December 2020, the strategy has been refined through publication of document "The French strategy of automated road mobility 2020-2022". The willing of a systemic vision integrating the components of the system and the service is reaffirmed and three main goals are defined in order to develop automated road transport services:

Establish and develop the partnerships and synergies between sectors, industrial and service actors, new technology companies as well as traditional ones.
Entrench these new mobility services in the territories, because the success of their deployment depends on their integration into local mobility policies.
Act on a European scale to move forward on vehicle regulation, on the interoperability of connectivity systems, and on support for research and innovation.

The steps of strategy consist in:

Finalizing the development of rules allowing vehicles without an operator on board in some secured and supervised use cases.
Financing full-scale demonstrators.
Better taking into account the topics of physical and digital connectivity.
Supporting evolutions in logistics services.
Ensuring the integration of the French strategy in the European context.

The document formalizes concrete measures to be conducted until 2022. Some of them concern legislative or technical doctrine issues, including:

- Finalization of the different legislative and regulatory framework linked to Mobility Orientation Law (LOM).
- Development of the relevant regulatory framework for the use of automated freight and logistics.
- Development of French doctrine for the use of critical scenarios for validation.
- Definition of the priority needs of connectivity for automation use cases.
- Establishment of synergies between the various research projects relating to the cybersecurity of connected and automated mobility.

In the legislative and regulatory field, several actions have been conducted.

1 – Two orders linked to the LOM have been published in April 2021:

- Order 2021-442 (linked to art. 32 of the LOM) contains provisions concerning the access to the data.
- Order 2021-443 (linked to art. 31 of the LOM) modifies the Traffic Code and Penal Code concerning penal liability and modifies the Transport Code concerning safety and liability in the case of automated road transport systems.

2 - Decree n° 2021-873 has been published on the 29th of June 2021 (« décret portant application de l'ordonnance no 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation »). This decree attached to article 31 of the LOM deals with liability rules and conditions of use attached to the automated road vehicles (ARTS):

- The decree modifies the Traffic Code relatively to conditions of use and driver's obligations attached to use of automated driving systems.
- It modifies the Transport Code in order to cover the case of ARTS circulating on predefined route (i.e. highly or totally automated vehicles circulating on predefined routes equipped with technical installations dedicated to safety and to remote operation, completed with operation and maintenance rules). It defines:
    - A framework for the safety demonstration to be produced before an ARTS can be put into service onto a predefined route. This safety demonstration has to demonstrate that the whole system is globally-as-safe as a reference system (GAME). The framework has to be assessed by an independent body.
    - Missions assigned to the different stakeholders of a project: system designer, system operator, service organiser, third party. Especially:
        - The safety demonstration has to be assessed by a designated third-party organization.
        - STRMTG (technical administration, part of French Transportation Ministry, in charge of guided transportation systems safety) is responsible for technical regulation production and updating, third party organizations designation and gathering of feedback from the field.

The measures stated by the decree shall be enter into force in September 2022. The decree has still to be completed by technical regulation guides that will detail the safety demonstration contents and architecture.

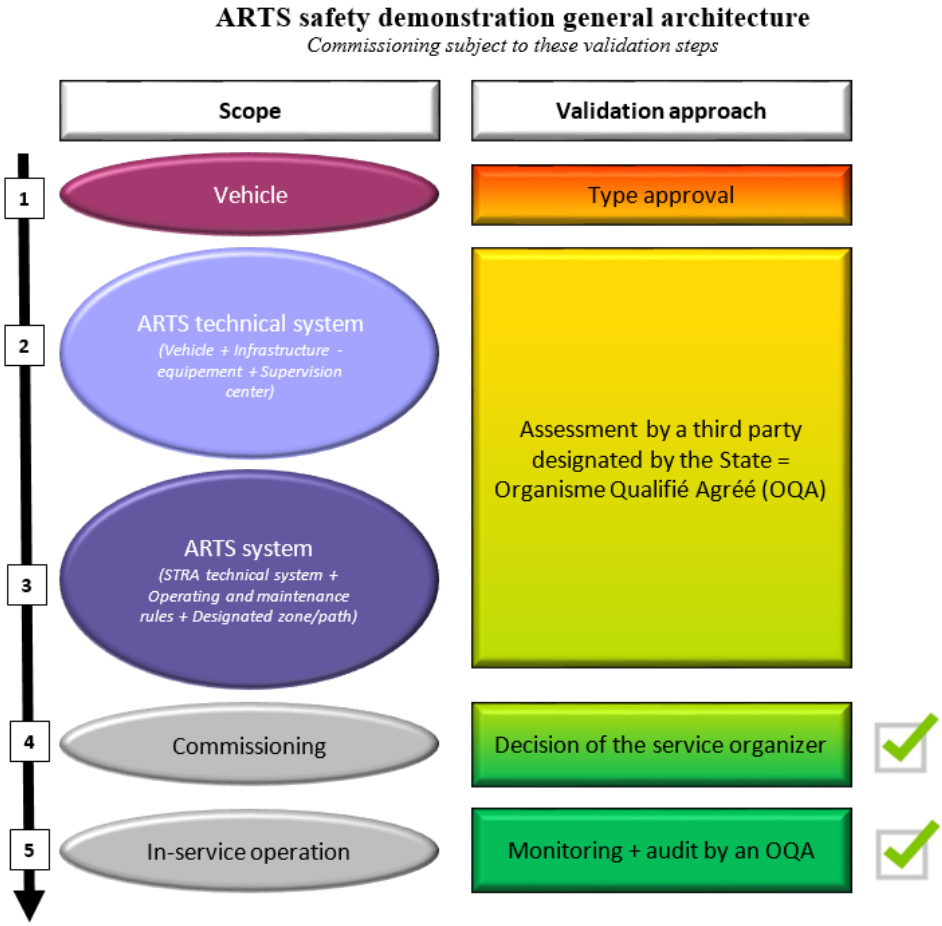


Figure 8: Safety demonstration general architecture

3 – The French Ministry of Transports is currently elaborating an order ("arrêté") dedicated to the automated shuttle vehicles (vehicles that carry 9 to 16 passengers, 5 of whom can be seated), which are not covered by the existing international categories M1, M2 or M3. The draft adapts current requirement for human driven shuttle to the automatic driving system case. This text is still in progress, but the main foreseen directions are:

- Safety demonstration based on the 4 pillars defined by VMAD, i.e. audit, simulation, testing and in-use monitoring.
- Requirements for cybersecurity based on UN R155 regulation, requirements for OTA software update based on UN R156 regulation and Data Storage System for Automated Driving obligation.
- List of tests to be passed by the vehicle (under construction).

Main actors in France in the field of automated mobility systems:

- Under the structure of French Automotive Platform (PFA), the "France Vehicule Autonome" (FVA) program gathers the main industrial and service French stakeholders in the road transport field: vehicle and equipment manufacturers, transport service operators, research organizations and bodies, laboratories involved in the field, closed-site testing facilities…).

- Public administrations:
  - The ministry of "Transition écologique", especially departments DGITM (infrastructures and transports) and DGEC (energy and climate).
  - The technical public bodies depending from the ministry of "Transition écologique": CEREMA, CETU, CNRV, STRMTG.
  - The ministry of Industry.
  - The ministry of Interior especially department DSR (Road Safety).

- Universities:
  - "Université Gustave Eiffel".
- Technical bodies:
  - UTAC
  - TRANSPOLIS

- OrganisationsOrganizations in charge of the road infrastructure management

- Local authorities in charge of transport organization.

2.2.2 Germany

In 2017, Germany made amendments to its Road Traffic Act (Strassenverkehrsgesetz or "StVG") to allow the use of motor vehicles with highly or fully automated driving features. Most of these amendments focus on the liability of the driver of such a vehicle and their responsibilities. In terms of the approval of automated driving technologies, sections 1a (2) and (3) are the most relevant. These must be read with the Road Traffic Licensing Regulations (Straßenverkehrs-Zulassungs-Ordnung, or "StVZO") under which all vehicles in Germany are licensed for use on public roads.

Section 1a (2) defines "motor vehicles with highly or fully automated driving functions".
The first part of section 1a (2) states that such vehicles are those that have technology that:

1) when activated, can control the motor vehicle – including longitudinal and lateral control – to perform the driving task (vehicle control);
2) is able, during "highly" or "fully automated" driving, to comply with the relevant traffic rules and regulations for operating a vehicle;
3) can be overridden or deactivated manually by the driver at any time;
4) is able to identify when there is a need to hand back control to the driver;
5) is able to indicate to the driver – by means of a visible, audible, tactile or otherwise perceptible signal – the need to retake manual control of the vehicle with a sufficient time buffer before it returns control of the vehicle to the driver; and
6) indicates that the usage goes against the system description.

The second sentence of section 1a (2) then requires the manufacturer of such a vehicle to state in "a binding manner" that the vehicle meets the technical requirements set out in section 1a (2). It is not clear how, when or to whom this statement must be made. It appears to obligate the manufacturer to describe their system and to ensure that its limits are clear to the driver.

Section 1a (3) clarifies that the amendments only apply to vehicles which are licensed in accordance with the requirements of the StVG, fulfil the technical functions set out in 1a (2) and also whose highly or fully automated driving functions:

a) are described in international regulation applicable in the territorial extent of the Act and comply with them or have received a type-approval pursuant to Article 20 of Directive
b) 2007/46 EC of the European Parliament and Council (type-approval framework Directive).

Section 1a (3) indicates that the approval of such automated systems in Germany is still very much contingent on international type approval. Traditionally type approval requires some third-party testing .

However, section 1a (2) suggests that international type approval may not be wholly sufficient in all circumstances. Take an example where an ADS is approved by (say) the Korean type-approval authority but there are fears that it may not comply with all relevant traffic rules in Germany. In addition to showing UNECE type approval, the manufacturer must give a binding statement of compliance with the technological requirements set out in the StVG. Without this binding statement, the vehicles will not be regarded as highly or fully automated.

Other parts of the German amendments make clear that the user of a vehicle fitted with automated technology remains the driver of the vehicle.

In the annexes of the document published by the German authorities, there are several lists of elements of interest in the construction of the regulatory framework for autonomous vehicle. Below is an extract of these elements.

Functional requirements for vehicles with autonomous driving function;

- Dynamic driving task
- Avoidance of collision with other road users
- Interaction with other road users
- Planning of trajectories and speeds
- Response to environmental conditions
- Risk-minimal state
- Emergency driving function
- Manual driving mode
- Permanent system monitoring
- Data transmission
- Functional safety and functional safety
- Operator's manual
- Safety concept
    - Hazard analysis
    - Safety measures
- Periodic technical vehicle monitoring
- Sensors
- Aging and wear of the system

Test and validation methods for vehicles with autonomous driving function

1) Pass criteria

- Test and test cases
- Artificial faults and limits of operating range
- Test scenarios, deviations and pass criteria
    - Pass criteria from UN Regulation No. 152
    - Leaving the lane
    - Safety distance
    - Changing lanes of other vehicles
    - Collision avoidance with vehicles traveling in the same direction
    - Lane change maneuvers
    - Turning and intersecting
- Performance of tests
- Requirements for the test site and environmental conditions

2) Digital data storage

- Scope of application/scope
- Functional requirements - storage
- Events to be stored
- Data storage system

3) Requirements for man-machine interfaces

- Issuance of a driving maneuver release to the vehicle with autonomous driving function by the technical supervisor
- Assumption of the driving task by manual control outside the specified operating range

4) Information Technology Security Requirements

- Cyber Security Management System
- Cyber risk assessment of the vehicle with autonomous driving function
    - Testing and required measures
    - Sample testing
    - Risk assessment
    - Protection of critical elements
    - Verification
- Radio links

5) Technical and organizational requirements for the keeper

- Requirements for technical supervision
- Supplementary requirements for the performance of technical and organizational tasks

6) Documentation requirements of the manufacturer

- Functional description
- Operating manual
- Security concept
- Security in the field of information technology

3 United Nations

3.1 Groupe de Rapporteurs Véhicules Autonomes (GRVA)

3.1.1 Functional Requirements for Automated Vehicles (FRAV)

3.1.1.1 Safety

FRAV has held extensive discussions regarding expectations for ADS performance, criteria to guide the development of requirements, and methods for determining performance specifications.

FRAV agrees to say that the requirements for the safety of an individual ADS depends upon its intended uses and limitations on its use (i.e., its features). For example, all ADS would be expected to detect and respond to road conditions that may be encountered during operation. However, correct responses of individual ADS to these conditions may differ. The safety requirements, therefore, will cover ADS functions (such as detection of ODD conditions) and minimum performance specifications relevant to safety.

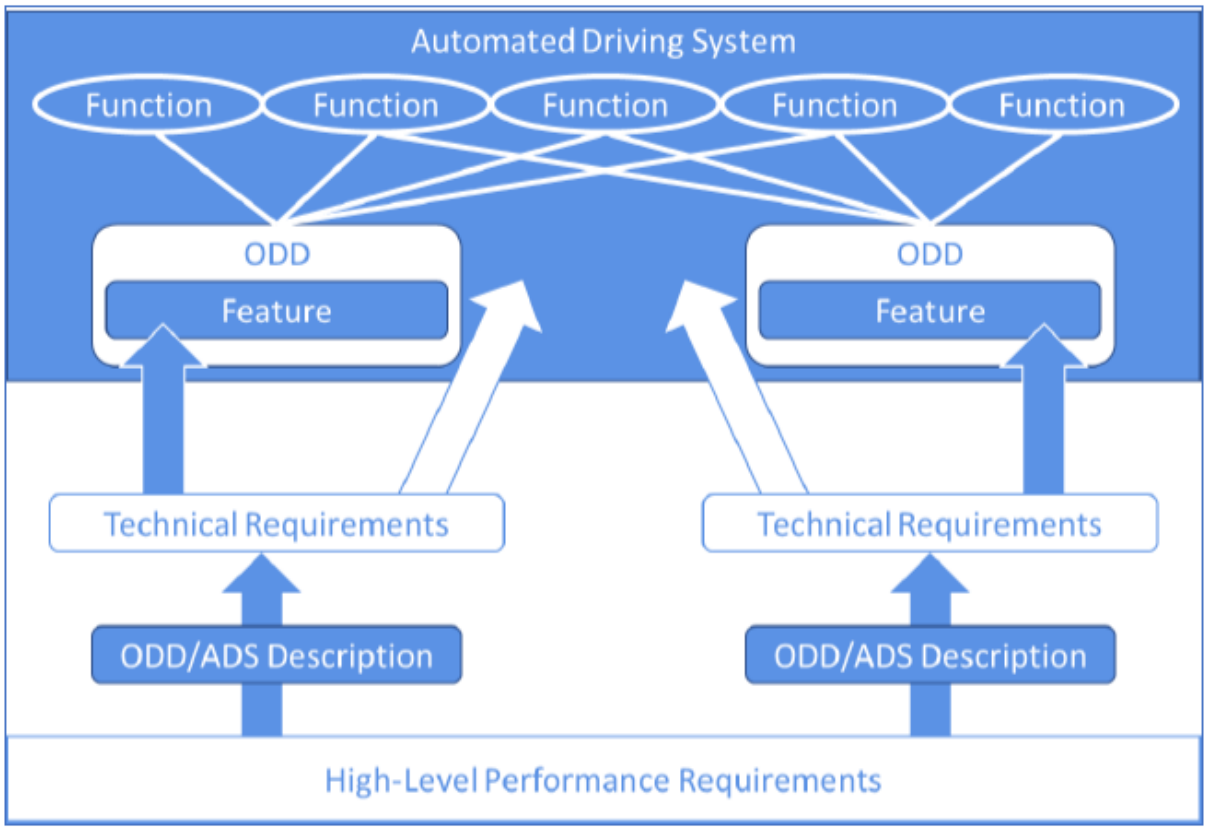


Figure 9: Overview of the process proposed by the FRAV [17]

3.1.1.1.1. Guiding principles

FRAV has also considered analysis of ADS technological capabilities under a « State-of-the-art » approach. Considering mathematical models to establish performance parameters and a « statistical positive risk balance » such that vehicles operating in automated mode demonstrate superior performance when compared statistically against human driving performance data. In some cases, combinations of these approaches offer paths towards defining optimal specifications. The outcome should be ADS performance that significantly improves road transport (including safety and efficiency) but also meets public expectations (social acceptance).

> ADS performance should be consistent with safe human driving behaviors while avoiding recognition, decision, and performance errors and the introduction of unreasonable ADS-specific risks.

Understanding the critical factors in crash causation supports deliberations on behaviors DS may encounter and informs discussions on ways that ADS may improve road safety. ADS cannot be expected to eliminate all factors in crash causation; however, ADS may address leading causes of crashes to produce a substantial positive risk balance.

Under this approach, FRAV gathered extensive input, including the review of national and regional guidelines regarding automated vehicles.

3.1.1.1.2. Five main aspects of ads performance

FRAV identified five main aspects of ADS performance:

1. ADS should drive safely. (Ensure safe behavior of the ADS as "the driver")
2. ADS should interact safely with the ADS user(s). (Ensure safe use of ADS and safe interactions with the user such as transfers of control, user override, etc.)
3. ADS should manage safety-critical situations. (Differentiate between normal driving and emergency situations to ensure safe responses to the latter)
4. ADS should safely manage failure modes. (Ensure safe responses to system malfunction, physical damage, etc.)
5. ADS should maintain a safe operational state. (Ensure safety throughout the useful life of the ADS, such as safety-critical updates, responses to obsolescence, end of production, etc.)

With those in mind, FRAV produced the following guidelines for ADS description and criteria definition

3.1.1.2 Status of FRAV activities

3.1.1.2.1 Data collection

Data on human driving, current traffic patterns, and crash causation are required to ensure that ADS performance requirements result in behaviors compatible with human-dominated traffic and real-world driving. FRAV has already received significant input concerning human driving behaviors, driver models, and traffic patterns and flows and has discussed methods for quantifying and otherwise analyzing human and ADS performance parameters.

3.1.1.2.2 Working in collaboration with VMAD

The leaderships of FRAV and VMAD hold regular meetings to review the status of their activities, expectations for progress, and anticipated needs, especially in the following areas;

3.1.1.2.3 Scenarios

FRAV distinguishes between the nominal driving behavior of ADS (e.g., ADS behavior should not cause crashes) and ADS behavior in response to safety-critical events (e.g., ADS response to error or negligence on the part of another road user). Nominal driving involves an understanding of typical and safe driving maneuvers and interactions with other road users. Safety-critical responses involve an understanding of crash causation and sudden conditions that may arise in the roadway.

3.1.1.2.4 Audit

To address failure management and operational safety. FRAV deliberations on safety requirements related to functions and system safety may contribute to the objective assessment of ADS functional safety.

3.1.1.2.5 Virtual testing

The complexity of traffic and a need to ensure ADS behaviors consistent with human-dominated traffic and human road-user expectations pushes the FRAV to deliberate on performance specifications conducive to the smooth integration of ADS into human-dominated traffic may provide context useful in assessing the fidelity of virtual testing tool chains.

3.1.1.2.6 Physical testing

Physical tests, such as responses to safety-critical conditions, ODD exits, or damage to a function should contribute to development of track, real-world, or other physical test methods

3.1.1.2.7 In-service performance

FRAV work should contribute to VMAD considerations regarding in-service monitoring and reporting on ADS performance

3.1.1.2.8 Integration under the New Assessment/Test Method (NATM) from VMAD

A manufacturer description of the ADS should be assessed. Therefore, the NATM will need a procedure for the review and verification of these ADS descriptions and so requirements for the preparation and contents of an ADS description (e.g., coverage of the ODD elements, stipulation of ODD conditions in accordance with the verifiable criteria specified by the description requirements). In addition, the application of the safety requirements depends upon the ODD of the ADS feature under assessment. For example, FRAV expects to define performance requirements related to ODD exits. The manufacturer specifies the ODD boundaries in the description of the ADS. Thus, assessment of fulfillment of the requirements for ODD exits will depend upon the boundaries stipulated by the manufacturer.

3.1.1.3 Guidelines for ADS descriptions

3.1.1.3.1 General considerations

- ADS may be designed for specific purposes and to operate under prescribed conditions.
    - The conditions under which an ADS is designed to operate are known collectively as the Operational Design Domain (ODD).
        - The ODD conditions include, but are not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.
- ADS may or may not be designed to transfer control to a qualified driver in the vehicle. The roles and responsibilities of an ADS user differ depending upon the ADS configuration, intended uses, and limitations on its use.
- ADS safety requirements need to address the diversity of configurations, intended uses, and limitations on use while addressing usage specifications of individual ADS.
- Therefore, FRAV intends to provide guidelines for the manufacturer's description of an ADS, including measurable/verifiable ODD specifications, to enable the application of safety requirements to the ADS under assessment.
    - The manufacturer shall describe the ADS configuration and the intended uses and limitations on the use of its feature(s).
        - The manufacturer shall list the potential faults covered by the diagnostic system(s) of the ADS.
    - The manufacturer shall establish the ODD conditions and boundaries of each ADS feature in measurable and/or verifiable terms.
        - The ODD conditions addressed by the manufacturer shall, at a minimum, include:
            - Precipitation (rain, snow).
            - Time of day (light intensity, including the case of the use of lighting devices).
            - Visibility.
            - Road and lane markings.
            - Road surface adhesion
            - Country of operation.
            - V2x dependencies, if any.
    - The manufacturer shall establish terms for the correct use of the ADS.
        - The manufacturer shall provide written information on the intended uses and limitations on the use of the ADS feature(s).

        - The manufacturer shall describe means made available to the public to promote a correct understanding of the intended uses and limitations on the use of the ADS.
        - The manufacturer shall provide the following information for ADS designed to interact with a fallback user.
            - The manufacturer shall provide written information on the roles and responsibilities of the fallback user, including activities other than driving.
            - The manufacturer shall provide written instructions for the activation and deactivation of the ADS.
            - The manufacturer shall provide written information on ADS responses to fallback user interventions in the dynamic control of the vehicle.
            - The manufacturer shall provide written descriptions of the transfer of control procedures, including ADS notifications and fallback user responses.
            - The manufacturer shall provide information detailing the human-machine interactions, including HMI tell-tales, indicators, and displays.

- ADS safety recommendations
    - ADS performance of the DDT
        - The ADS shall be capable of performing the entire Dynamic Driving Task (DDT) within the ODD of its feature(s).
        - The ADS shall recognize the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 3.3.
        - The ADS shall detect and respond to objects and events relevant to its performance of the DDT.
        - The ADS shall comply with safety-relevant traffic laws according to the ODD of the feature in use.
        - The ADS shall interact safely with other road users.
    - ADS interactions with ADS vehicle users
        - User interaction with and the interface of ADS (features) shall have a high-level commonality of design.
        - The ADS HMI shall provide clear and unambiguous information to the user.
        - The ADS shall be designed to prevent misuse and errors in operation.
        - The ADS shall be designed to ensure safe ADS feature activation.

        - An ADS which permits a transition of control shall be designed to ensure safe transitions of control.
        - An ADS which permits user takeovers of control shall be designed to ensure safe user-initiated takeovers.
        - The use of the ADS shall be supported by documentation and tools to facilitate the user in understanding the functionality and operation of the system.
    - ADS management of safety-critical situations
        - The ADS shall execute a fallback response in the event of a failure in the ADS and/or other vehicle system that prevents the ADS from performing the DDT.
        - The ADS shall signal its intention to place the vehicle in an MRC.
        - Pursuant to a traffic accident, the ADS shall stop the vehicle.
    - ADS management of system failures
        - The ADS shall detect and respond to system malfunctions and abnormalities relevant to its performance of the DDT.
        - The ADS shall be designed to protect against unauthorized access.
        - The ADS shall signal [faults/failures] compromising its capability to perform the entire DDT relevant to the ODD of its feature(s).
        - The ADS shall be designed to protect against unauthorized modifications to safety-critical hardware and software.
        - The ADS may continue to operate in the presence of [faults/failures] that do not prevent that ADS from fulfilling the safety recommendations applicable to the ADS.
        - The ADS shall signal [faults/failures] compromising its ability to execute the DDT.
    - ADS maintenance of a safe operational state.
        - The ADS should signal required system maintenance to the user.
        - The ADS should be accessible for the purposes of maintenance and repair to authorized persons.
        - ADS safety should be ensured in the event of discontinued production/support/maintenance.
    - The following table provides additional information on the elaboration of ADS safety requirements for use under the New Assessment/Test Method (NATM).
    - The left column ("safety requirements") reproduces ADS safety recommendations presented above (paras. 4.1-4.5. inclusive).
    - The right column ("detailed provisions") provides additional information concerning the elaboration of the safety recommendations in the left column.

- ADS safety requirements shall be verifiable and/or measurable under the NATM tools and methods.
- The right column highlights aspects that may be suitable for the development of such measurable/verifiable criteria for assessing ADS fulfilment of the safety requirements. These items are all under discussion and not yet agreed by FRAV.
- The elaboration of these safety requirements involves collaboration with the Validation Methods for Automated Driving informal working group.
    - Consideration of traffic scenarios that define conditions the ADS may encounter, including nominal performance of the DDT, ADS responses to safety-critical traffic situations, and ADS responses to system failures.
    - Consideration of the assessment methods to be used in evaluating ADS performance against the safety requirements such as virtual testing, track tests, and under real-world driving on public roads.
    - Consideration of the procedures for determining ADS configurations, intended uses, and limitations on use to ensure assessments appropriate across the diversity of ADS.
    - Consideration of procedures for monitoring the performance of ADS in the field, including attention to data collection and analysis to provide appropriate reporting on performance metrics.
    - Based on the above, FRAV anticipates the development of measurable/verifiable criteria for application of the safety requirements to the NATM methods and tools.

The following table provides additional information on the elaboration of ADS safety requirements for use under the New Assessment/Test Method (NATM);

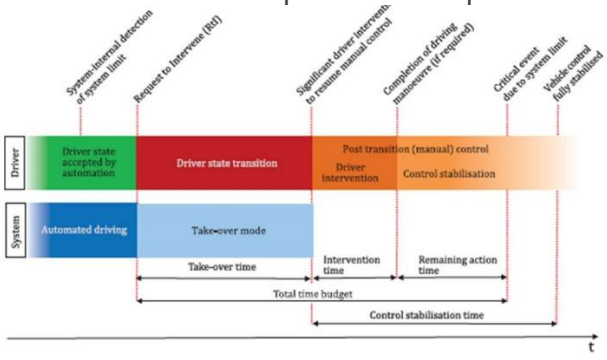
Table: ADS Safety Recommendations and Development of Detailed Provisions

	Safety Recommendations	Detailed Provisions (under discussion)
The ADS should drive safely.		
1.	The ADS shall be capable of performing the entire Dynamic Driving Task (DDT) within the ODD of its feature(s).	• The capability of the ADS to perform the entire DDT should be determined in the context of the ODD of the ADS • As part of the DDT, the ADS should be able to: o Operate at safe speeds. o Maintain appropriate distances from [other road users] by controlling the longitudinal and lateral motion of the vehicle. o Adapt its behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic). o Adapt its behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).
2.	The ADS shall recognize the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 3.3.	• The ADS should be able to determine when the conditions are met for activation. • The ADS should detect and respond when one or more ODD conditions are not or no longer fulfilled. • The ADS should be able to anticipate planned exits of the ODD • The ODD conditions and boundaries (measurable limits) should be established by the manufacturer. • The ODD conditions to be recognized by the ADS should include: o Precipitation (rain, snow) o Time of day (light intensity, including the case of the use of lighting devices) o Visibility o Road and lane markings
3.	The ADS shall detect and respond to objects and events relevant to its performance of the DDT.	• Objects and events might include, but are not limited, to: o Vehicles, motorcycles, bicycles, pedestrians, obstacles o Road accidents o Road safety agents / enforcement agents o Emergency vehicles • The ADS shall detect objects in and around its path of travel that exceed a minimum size. • The ADS shall recognize objects as static or mobile.

		• The ADS shall recognize markings and signals used to indicate priority vehicles within the ODD of its feature(s). • The ADS shall classify priority vehicles within the ODD of its feature(s) in accordance with the relevant traffic law(s). • The ADS shall yield the right of way to priority vehicles in service in accordance with the relevant traffic law(s).
4.	The ADS shall comply with safety-relevant traffic laws according to the ODD of the feature in use.	• ADS should comply with the traffic laws in nominal conditions, except when in specific circumstances or when necessary to enhance the safety of the vehicle's occupants and/or other road users.
5.	The ADS shall interact safely with other road users.	• The ADS shall avoid collisions with safety-relevant objects where possible. • The ADS shall signal intended changes of direction. • The ADS shall signal its operational status (active/inactive) as needed.
The ADS should interact safely with the ADS vehicle user(s).		

6.	User interaction with and the interface of ADS (features) shall have a high-level commonality of design.	• The ADS should be designed to foster a level of trust that is aligned with its capabilities and limitations to ensure proper use of the system.
		• The operation of the interaction shall have in common:
		  ○ use of common sequence of states in the transition/activation/overriding/…
		• The interaction should be simplified:
		  ○ Limit the number of roles
		  ○ Limit the number of potential transitions
		  ○ Limit the number of settings
		  ○ Limit the number of different interaction modes

7.	The ADS HMI shall provide clear and unambiguous information to the user.	• The vehicle shall indicate its ADS capabilities in terms of their automated features and their ODD.
		• The ADS shall inform the user on the current conditions:
		  ○ ADS status information
		  ○ The availability of ADS features
		  ○ User Role
		  ○ Responsibility
		  ○ Permitted NDRA
		  ○ Potential roles to activate
		  ○ "Standard" information:
		  ▪ Vehicle speed, range and Time to Fuel
		  ○ ADS failure information
		• The ADS shall inform the user on the upcoming conditions:
		  ○ ODD boundaries

		○ Upcoming actions or change in roles ○ Oncoming decisions/maneuvers ○ Estimated time until take over in normal conditions ○ Transition related communication. • The ADS shall ensure that safety related information is prioritized and presented in a clear and unambiguous manner.
8.	The ADS shall be designed to prevent misuse and errors in operation.	• The ADS shall be designed to prevent inadvertent activation or deactivation. • The controls dedicated to the ADS shall be clearly distinguishable from other controls. • The ADS shall provide feedback when the user attempts to enable unavailable functions.
9.	The ADS shall be designed to ensure safe ADS feature activation.	• The ADS shall inform the user that preconditions for activation are met. • The activation should follow a common sequence of actions and states: ○ Common sequence to be a pass/fail criterion. • The ADS shall provide confirmation that the system is activated.
10.	An ADS which permits a transition of control shall be designed to ensure safe transitions of control.	• The interaction shall follow a common sequence of actions and states in the Transition of control (change of user roles): ○ Common sequence to be a pass/fail criterion.  Figure 2 — System-initiated transition from automated to manual driving • Transition of control shall return to a common default user role (to prevent mode confusion and other risks): ○ This shall normally be fully engaged driving (conventional driver). ○ Common default user to be a pass/fail criterion. • The ADS shall continuously verify whether the user is available for the transition of control and warn the user if not available when required. • The ADS shall verify that the driver is in stable control of the vehicle to complete the transfer of control to the user.

		• During transition, the ADS shall remain active until the transition of control has been completed or the ADS reaches a minimal risk condition.

11.	An ADS which permits user takeovers of control shall be designed to ensure safe user-initiated takeovers.	• Under safe conditions the user is allowed to initiate a takeover of the ADS.
		• The deactivation should follow a common sequence.
		  o Common sequence to be a pass/fail criterion.
		• The ADS should prevent and warn a user for a user-initiated takeover that would likely lead to an unsafe situation.
		• The ADS should provide a clear feedback of the successful user initiated takeover.
		  o The clear feedback should be a pass/fail criterion.
		• The user-initiated takeover should return to a common default user role (to prevent mode confusion and other risks)
		  o This should normally be fully engaged driving (conventional driver).
		  o Common default user role to be a pass/fail criterion.

12.	The use of the ADS shall be supported by documentation and tools to facilitate the user in understanding the functionality and operation of the system.	Documentation: • The following information should be documented: • description of the possible educational approach: • Theoretical and practical training • How it aligns with common HMI and interaction • Operational Description of ADS (features) capabilities and limitations (the information should also refer to specific scenarios) • Description on roles and responsibility of driver/user and ADS when ADS (feature) is on/off • description of allowed transition of roles and procedure for the transition (activation/deactivation, ToC, Override) • general overview list of NDRA allowed when an ADS feature is active. Tools: • The ADS supports the user in correct operation (coaching). • The ADS gives prompt feedback on erroneous operation.
The ADS should manage safety-critical situations.		
13.	The ADS shall execute a fallback response in the event of a failure in the ADS and/or other vehicle	• In the absence of a fallback-ready user, the ADS should fall back directly to a Minimal Risk Condition (MRC)

	system that prevents the ADS from performing the DDT.	• If the ADS is designed to request and enable intervention by a human driver, the ADS should execute an MRM in the event of a failure in the transition of control to the user o Upon completion of an MRM, a user may be permitted to assume control of the vehicle o The user should be permitted to override the ADS to assume full control over the vehicle
14.	The ADS shall signal its intention to place the vehicle in an MRC.	• The ADS should signal its intention to place the vehicle in an MRC to: o ADS user or vehicle occupants o Other road users (e.g., by hazard lights)
15.	Pursuant to a traffic accident, the ADS shall stop the vehicle.	• ADS reactivation should not be possible until the safe operational state of the ADS has been verified.
The ADS should safely manage failure modes.		
16.	The ADS shall detect and respond to system malfunctions and abnormalities relevant to its performance of the DDT.	• The ADS should perform self-diagnosis of faults in accordance with the OEMs prescribed list • The ADS should detect system malfunctions/abnormalities and evaluate system's ability to fulfill the entire DDT
17.	The ADS shall be designed to protect against unauthorized access.	• The measures ensuring protection from an authorized access should be provided in alignment with engineering best practices.
18.	The ADS shall signal [faults/failures] compromising its capability to perform the entire DDT relevant to the ODD of its feature(s).	
19.	The ADS shall be designed to protect against unauthorized modifications to safety-critical hardware and software.	
20.	The ADS may continue to operate in the presence of [faults/failures] that do not prevent that ADS from fulfilling the safety recommendations applicable to the ADS.	• The limited operation of the ADS should comply to the normally applicable safety requirements. • For situations where the ADS is not able to perform the DDT safely, the ADS should have the function to prevent activation. If the ADS has OTA functionality, this function may be activated remotely if the authorities or the vehicle manufacturer determine that the ADS is unsafe.
21.	The ADS shall signal [faults/failures] compromising its ability to execute the DDT.	• The ADS should signal [faults/failures] affecting the ability to execute the DDT.

The ADS should maintain a safe operational state.		
22.	The ADS should signal required system maintenance to the user.	
23.	The ADS should be accessible for the purposes of maintenance and repair to authorized persons.	
24.	ADS safety should be ensured in the event of discontinued production/support/maintenance.	

3.1.1.4 Outlook

FRAV expects to be able to deliver ADS safety requirements for GRVA consideration in February 2022,

Following so, safety aspects verification criteria by May 2022

- Specification for those criteria should come out by September 2021

3.1.2 Validation Method for Automated Driving (VMAD)

3.1.2.1 New Assessment/Test Method (NATM)

In order for the international community to maximize the potential safety benefits of ADS, a safety validation framework that can be adopted by Contracting Parties of both the 1958 and the 1998 UN vehicle regulations agreements must be established. The NATM developed by VMAD aims to provide clear direction for validating the safety of an ADS in a manner that is repeatable, objective and evidence-based, while remaining technology neutral and flexible enough to foster ongoing innovation by the automotive industry.

This document consolidates the work accomplished by VMAD to date to develop the NATM. It provides a clear overview of the NATM and its constituent pillars. This document also serves to promote coordination between VMAD and the work of the GRVA Informal Working Group on Functional Requirements for Automated Vehicles (FRAV). This coordination will ensure that the NATM also addresses the validation of compliance of an ADS to common functional performance requirements to be developed by FRAV.

Given the substantial technical work that is still needed to operationalize the NATM in practice, this version of the Master Document provides a high-level framework for the NATM, outlining:

- Scope and general overviews of the scenario catalogue and each of the pillars (simulation/virtual testing, test track, and real-world testing, audit/assessment and in-use monitoring); and,
- Overall process of the NATM (e.g., how the components of the NATM (i.e., the scenarios catalogue and pillars) operate together, producing an efficient, comprehensive, and cohesive process).

Going forward, this document will be further developed and regularly updated and informed by the outcomes of future VMAD sessions.

As VMAD continues to develop the elements of the NATM and FRAV continues to develop functional requirements for ADS, this document will be updated to incorporate this work.

Detailed technical documents will be outlined in an index of supporting reference materials, located at the end of this document, as these are developed by VMAD.
Subject to direction from GRVA and WP.29, once the NATM has reached a state of maturity to inform evaluation criteria (based on performance requirements specified by the IWG FRAV), it is anticipated that this document (and any supporting resources developed by VMAD) will be used to help inform validation process guidelines and/or regulations/requirements that align with the needs of both 1958 and 1998 Agreement parties (subject to approval by WP.29).

3.1.2.2 Multi-pillar approach

- **A scenarios catalogue**, consisting of a series of relevant and critical scenarios that represent real world traffic situations, will be a tool used by the following three pillars (testing methodologies) to validate the safety of an ADS. The goal of these scenarios is to exercise and challenge an ADS' capabilities to safely operate. This catalogue will provide a minimum baseline (non-exhaustive inventory) of scenarios that should be considered (and built upon as required) to validate each safety requirement for an ADS;

- **Simulation/virtual Testing** which uses software-in-the-loop (SIL), hardware-in-the-loop (HIL), and/or vehicle-in-the-loop simulation methods to model virtual scenario elements to test the capabilities of an ADS or its component(s);

- **Track testing** which uses a closed-access testing ground with various scenario elements to test the capabilities and functioning of an ADS;

- **Real world testing** which uses public roads to support testing, evaluation and functioning of ADS in real world traffic situations;

- **Audit/assessment** procedures that establish how manufacturers will be required to demonstrate to safety authorities using documentation, their simulation, test-track, and/or real-world testing of the capabilities of an ADS. The audit will validate that hazards and risk relevant for the system have been identified and that a consistent safety-by-design concept has been put in place. The audit will also verify that robust processes/mechanisms/strategies (i.e., safety management system) that are in place to ensure the ADS meets the relevant functional requirements throughout the vehicle lifecycle. It shall also assess the complementarity between the different pillars of the assessment and the overall scenario coverage;

- **In-service monitoring** and reporting addresses the in-service safety of the ADS after its placing on the market. It relies on the collection of fleet data in the field to assess whether the ADS continues to be safe when operated on the road. This data collection can also be used to fuel the common scenario database with new scenarios from the field and to allow the whole ADS community to learn from major ADS accidents/incidents.

Below, an extract from the overall process described above. A focus on this description is also provided in Appendix IV.

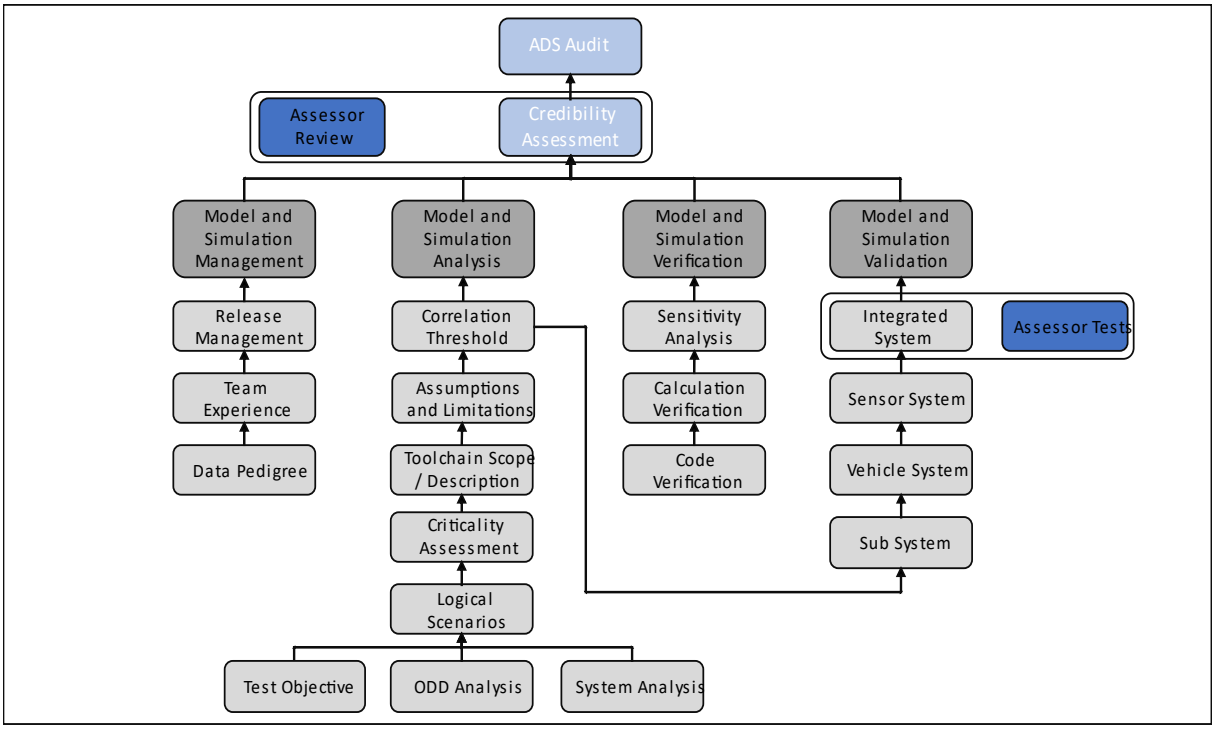


Figure 10: Credibility assessment framework applied to ADS validation for the Simulation pillar

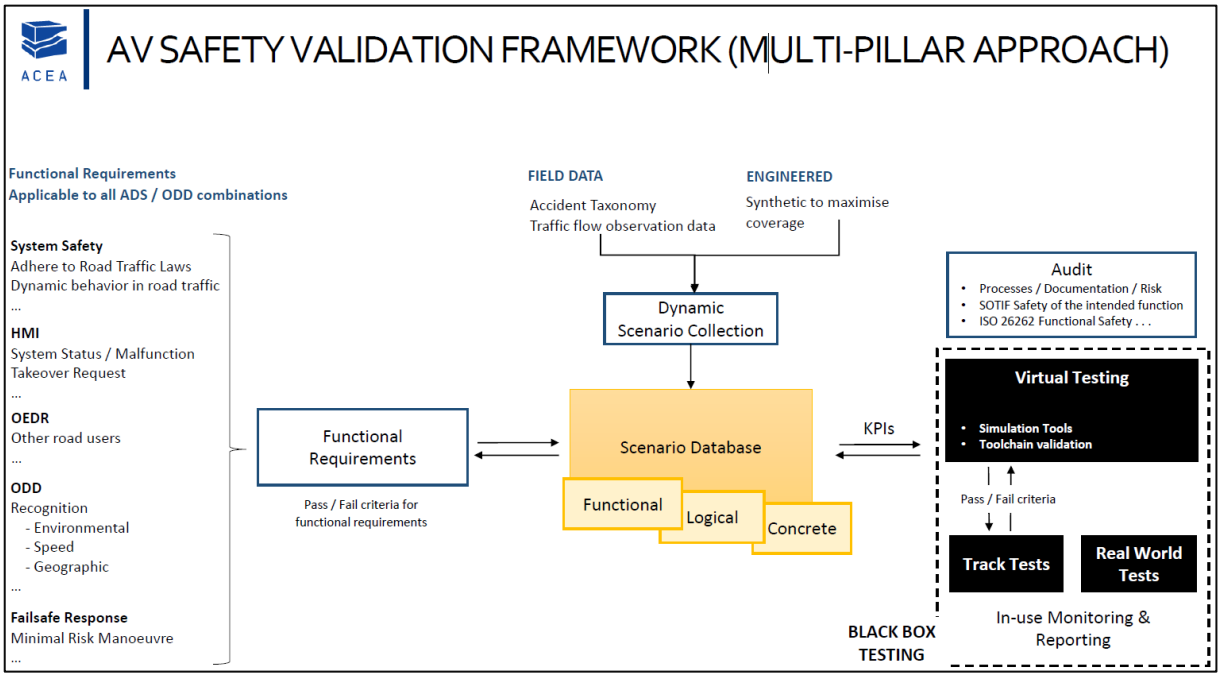


Figure 12 : Vision of the Multi-Pillar Approach from the ACEA

3.1.2.3 NATM Pillars/Element Interaction

The goal of the NATM guidelines document is to assess the safety of an ADS in a manner that is as repeatable, objective and evidence-based as possible, whilst remaining technology neutral and flexible enough to foster ongoing innovation in the automotive industry.
The overall purpose of the NATM is to assess, based on the safety requirements, whether the ADS is able to cope with occurrences that may be encountered in the real world. In particular, by looking at scenarios linked to road users behaviour/environmental conditions in Traffic scenarios as well as scenarios linked to driver behaviour (e.g. HMI) and ADS failures.
As previously noted, the multi-pillar approach recognizes that the safety of an ADS cannot be reliably assessed/validated using only one of the pillars. Each of the aforementioned testing methodologies possesses its own strengths and limitations, such as differing levels of environmental control, environmental fidelity, and scalability, which should be considered accordingly.
It is important to note that a single assessment or test method may not be enough to assess whether the ADS is able to cope with all occurrences that may be encountered in the real world. For instance, while real-world testing provides a high degree of environmental fidelity, a scenario-based testing methodology using only real-world testing could be costly, time-consuming, difficult to replicate, and pose safety risks. Consequently, track testing may be more appropriate methods to run higher risk scenarios without exposing other road users to potential harm. Further, test scenarios can also be more easily replicated in a closed track environment compared to the real-world. That said, test track scenarios can be potentially difficult to develop and implement, especially if there are numerous or complex scenarios, involving a variety of scenario elements.
Consideration should be given to the fact that simulation/virtual testing, by contrast, can be more scalable, cost-effective, safe, and efficient compared to track or real-world testing, allowing a test administrator to safely and easily create a wide range of scenarios, including complex scenarios, where a diverse range of elements are examined. However, simulations may have lower fidelity than the other methodologies. Simulation software may also vary in quality and tests could be difficult to replicate across different simulation platforms.
In-service monitoring and reporting should be used to confirm the pre-deployment safety assessment and fill the gaps between safety validation through virtual/physical testing and real-life conditions. Evaluation of in-service performance should also be used to update the scenario database with new scenarios deriving from increasing deployment of driving automation. Finally, the feedback from operational experience can support ex-post evaluation of regulatory requirements.
In addition to the respective strengths and weakness of each test pillar, the nature of the safety requirements being assessed will also inform what pillars are used:

(a) For instance: the most appropriate method to assess an ADS's overall system safety prior to market introduction may be the audit pillar, using a systematic approach to perform a risk analysis. The audit could include information such as safety by design confirmed validation outputs as well as analysis of data collected in the field by the manufacturer.

(b) Virtual testing may be more suitable when there is a need to vary test parameters and a large number of tests need to be carried out to support efficient scenario coverage (e.g., for path planning and control, or assessing perception quality with pre-recorded sensor data).

(c) Track tests may be best suited for when the performance of an ADS can be assessed in a discrete number of physical tests, and the assessment would benefit from higher levels of fidelity (e.g., for HMI or fall back, critical traffic situations).

(d) Real-world testing may be more suitable where the scenario may not be precisely represented virtually or on a test track (e.g., interactions with other road-users and perception quality may be assessed through real world evaluation).

(e) In-service monitoring and reporting of field data represent the best way to confirm the safety performance of an ADS in the field after market introduction over a wide variety of real driving traffic and environmental conditions.

Given these considerations, it should be noted that the sequence and composition of test pillars used to assess each safety requirement may vary. While some testing might follow a logical sequence from simulation to track and then to real world testing, there may be deviations depending on the specific safety requirement being tested.
It is therefore necessary for the NATM pillars to be used together to produce an efficient, comprehensive, and cohesive process, considering their strengths and limitations. The methods should complement one another, avoiding excessive overlaps or redundancy to ensure an efficient and effective validation strategy.
As previously noted, the NATM pillars not only include the three aforementioned test methods but also an aggregated analysis (e.g., an audit/assessment /in service monitoring/reporting pillar). Whereas the test methods will assess the safety of the ADS, the audit/assessment pillar will serve to assess the safety of the ADS as well as the robustness of organizational processes/strategies. Elements of the audit are:

(a) Assessment of the robustness of safety management system,

(b) Assessment of the (identified) hazards and risks for the system,

(c) Assessment of the Verification strategy (e.g. verification plan and matrix) that describe the validation strategy and the integrated use of the pillars to achieve the adequate coverage

(d) Assessment of the level of compliance with requirements achieved through an integrated use of all pillars, including consistency between the outcomes of one pillar as input for another pillar (forward and backward) and adequate use of scenarios. This level of compliance concerns both new vehicles as vehicles in use.

(e) The audit/assessment phase also incorporate results from the Simulation, Track test and Real-World tests carried out by the manufacturer.

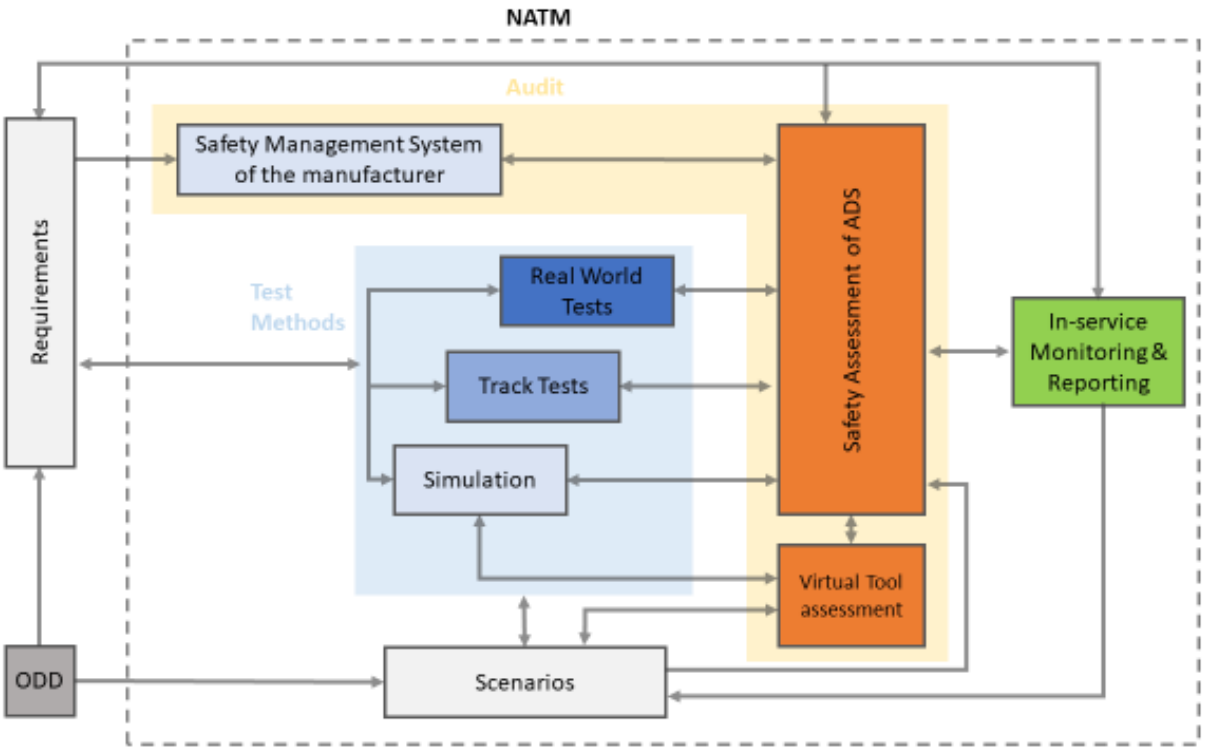


Figure 13: Relationship between VMAD Pillars, Scenarios and FRAV Safety Requirements [26]

4 Actions outside the European Union

Other countries have also considered the balance between self-certification and third-party testing. Below it is outlined the approach taken in a few prominent jurisdictions.
It is important to note that some of the following countries (e.g., USA, Japan, Canada) are also members of the GRVA working groups.

4.1 The United Kingdom's

The following lines focuses on how The United Kingdom's intends to assess whether an automated vehicle (AV) is as safe as it needs to be before it is allowed on the road, and the practicalities of assessing AV safety. Most of the following elements are extracted from the "*The Law Commissions' final AV consultation: a regulatory framework for AVs*" published in December 2020, giving the UK's view.

For The United Kingdom's, a key question is how far a safety assurance agency should rely on self-certification by manufacturers and how far it should require testing by third parties. There are also a variety of testing approaches - using test tracks, public roads and simulation - each with its own strengths and weaknesses.
Based on this observation, The United Kingdom's wrote its proposal for a legal framework to provide initial approval of automated driving systems.
One clear message though, is that the safety of a particular AV cannot be assessed at one single point of time. Automated driving systems (ADS) and the vehicles in which they are fitted will need to be assessed before they are deployed on the road - and then will need to be monitored in practice on an ongoing basis.

4.1.1 Testing Methods

The UK adopts an approach very similar to the one proposed in the New Assessment/Test Method (NATM) from the Validation Method for Automated Driving (VMAD) (method detailed later in this document)
As part of the authorization process, an ADS will have to be validated against safety requirements. The manufacturer or developer will need to provide documentation to demonstrate that the system is safe. The documentation may show that a prescribed set of engineering standards were followed or that something has been proven to meet the requisite level of safety through use.
However, most AV documentation will rely on testing. The documentation will need to rely on tests of specific scenarios and, possibly, on "brute force" testing (to show thousands of hours of simulation or millions of miles driven on the road without mishap). The approval authority may then want to carry out its own tests, either itself or through approved technical services.
Whether tests are carried out by developers or by regulators, there is no one perfect method of testing. A mix of methods will be needed. Therefore, The United Kingdom's is considering the three main following testing methods: track testing, road tests and simulations.

4.1.2 Track testing

In an AV context, the UK Government has focused investment in this area, developing Connected and Automated Mobility (CAM) Testbed UK. The recent UNECE Regulation on Automated Lane Keeping Systems (ALKS) for example, requires six specific track tests, including avoiding a collision with a road user, following a lead vehicle and dealing with a cut-in vehicle.
Specialist track testing can offer valuable insights into the way an ADS reacts in given scenarios. It is especially suitable for scenarios that are high-risk or highly dynamic which would not be safe to test on public roads. It also offers a high level of control and repeatability when compared to road testing. However, it can only offer insight into the scenarios tested. Real roads are environments that are more complicated and AVs will encounter many scenarios not tested on the track.

Road testing
Public road trials offer the opportunity to test an ADS under "real-world conditions". It has, to date, been the most prominent method of testing AV safety.
Many jurisdictions around the world require manufacturers to apply for a permit before testing on public roads. Currently, this is not required in the UK. Testing and trialing AVs on public roads in the UK is possible "if carried out in line with UK law". As part of complying with the law, Centre for Connected and Autonomous Vehicles (CCAV) Code of Practice emphasizes that trialing organizations must have:

1) a driver or operator, in or out of the vehicle, who is ready, able, and willing to resume control of the vehicle;
2) a roadworthy vehicle; and
3) appropriate insurance in place.

Data from public road trials is likely to play an important role in assuring the approval authorities that an ADS system is ready for widespread deployment. Public road trials may also be used to validate track tests and simulation results. It is at the center of the National Highway Traffic Safety Administration's (NHTSA) Automated Vehicle Transparency and Engagement for Safe Testing Initiative (AV TEST Initiative) launched in June 2020.
However, public road trials alone can be an impractical way to validate AV safety. They require an enormous number of miles driven to provide a statistically credible safety argument. Vehicles also need to be able to handle unusual situations that are rarely encountered during public road trials. Additionally, every time the ADS software is updated, more public road testing would need to be performed to ensure that the safety argument remains valid. This is also true for track testing and simulation, but the process for public road trials is more time-consuming and expensive.

4.1.3 Simulation

Simulations involve testing the ADS without deploying the vehicle on a road. As the name suggests, tests of the ADS's driving capabilities are simulated at a software, hardware and vehicle level. Simulation is seen as an effective way to assess the capability of ADSs and it offers several potential advantages over road testing. First and foremost, it is safer. It also has lower operational costs. Simulations, when used to supplement on-road testing, can drastically reduce the time taken to validate the safety of an ADS. Simulation also offers the chance to test "corner cases" and known rare events that would not be as readily testable in the real world.

However, to ensure that the simulation testing produces accurate results, scenarios must adequately reflect actual road conditions and the Operational Design Domain (ODD) within which AVs will operate. Simulations must also be sufficiently varied to check that the ADS is capable of dealing with all the situations it might encounter.

4.1.4 Self-certification and third-party testing

The United Kingdom's reports a variety of opinions on how third-party testing might be conducted. Some argued for a standardized set of scenarios that could be used by a third party to test the ADS. To prevent developers from designing for the test, the third-party should randomize these scenarios from an extensive test set.

Others saw the role of the third-party as being an auditor of the developer's safety case. These audits would verify that the testing data was accurate and that the evidence obtained was robust. There was also a need for the regulator to ensure that appropriate processes were in place to manage the ongoing safety of the ADS once deployed.

Some respondents stressed the importance of third-party testing using the final, complete automated vehicle on test tracks and on public roads.

4.1.5 Safety cases

Whatever the final mix of assessment techniques, it is likely that a large part of the process will involve regulators assessing documentation from the manufacturer or developer offering evidence that the system is safe. This is a common process in many high-risk industries.

Regulations require that operators present a safety case at the approval stage and maintain the safety case throughout the operational life of the system.

The safety case is a document, or a set of documents, which present a clear, comprehensive and defensible argument for the safety of a given system in a given context. The British Ministry of Defense describes a safety case as: a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.

In accordance with the evidence requested above, the manufacturers and operators must demonstrate that they have tried to understand systematically and proactively the risks of their systems and the measures needed to reduce these risks. Appropriate processes must also be put in place to measure the effectiveness of any risk control measures.

4.1.6 What is in a safety case?

A safety case consists of three main elements: claims, argument and evidence. The claims should define the safety objective or requirements of the system. The argument must then communicate the relationship between the evidence and the claims - implied arguments are not enough.

The safety objective or requirements will vary depending on the industry. For many safety-critical industries, the objective is to reduce the risks to a level As Low As Reasonably Practicable (ALARP).

A safety case should generally provide the following:

1) a system description and its operational context;
2) the safety claims and safety criteria;
3) what hazards have been identified;
4) what risk control measures have been put in place;
5) why the residual level of risk is acceptable; and
6) an overview of the how safety management system is organized, including roles responsibilities and safety polices.

The safety case should highlight the major hazards and concentrate on these: it should not be packed with detail on trivial risks. Preliminary hazard identification and analysis should be done early in the project lifecycle to scope the activities and resources needed to build the safety case. Evidence should be provided throughout to back up claims made by the safety case.

4.1.7 Safety cases in the automotive industry

The UK recalls that ISO 26262 was developed in response to the increasing complexity of electric, electronic and programmable systems (E/E/P) in vehicles. It requires that manufacturers develop a safety case that progressively compiles the work products of each development stage. These work products then form the evidence for the safety case.

Some existing UNECE regulations are also recalled by The UK as requiring safety cases as part of the type approval of certain complex systems. For example, Annex 8 of Regulation 13 H for braking and Annex 6 of Regulation 79 on steering set out requirements for evidence-based documentation that must be presented to the approval authority. Annex 4 of the recent ALKS regulation also has similar requirements.
Automotive safety cases generally have safety goals, functional safety requirements, and technical safety requirements. High-level arguments are used to show that the manufacturer has eliminated unreasonable risks and met the safety goals. Technical and regulatory requirements are incorporated into the arguments.
Importantly the arguments should not be limited to the design of the vehicle but should also address the entire lifecycle of the vehicle. These include production, maintenance, and how to evaluate and respond to incidents once the vehicle is deployed.

4.1.8 Safety cases and AV standards

The BSI PAS 1881 standard is designed specifically to help developers build safety cases for automated vehicle trials and development testing in the UK. Similarly, the SaFad white paper specifies the use of ISO 26262 compliant processes to validate the safety of an AV. It also specifies particulars that "support" and "build" an AV safety case.

The UL 4600 standard was developed by Edge Case Research and Underwriters Laboratories. It is another standard explicitly designed to help developers and manufacturers of automated products like self-driving cars to build a safety case for their product. It sets out a methodology by which the developer or manufacturer can explain why an AV is acceptably safe through a comprehensive and structured set of claims or goals. These claims or goals must then be supported by arguments and evidence.
As an example, if the manufacturer of an AV were to claim that their AV "will not hit pedestrians", this must be supported by arguments such as "the AV will detect all pedestrians" or the "AV will stop or avoid detected pedestrians". This would then need to backed by evidence, such as detection tests performed on the AV. The aim is to get the manufacturer to explain the specifics of their claims so that an independent assessor can analyze whether the product is safe.
UL 4600 also sets out a structure for the safety case, dividing claims into areas such as "risk assessment", "interacting with Non-Driver Humans" and "verification, validation, and testing". Throughout it has extensive lists to "prompt" users to consider things that the standard defines as "mandatory", "required", "highly recommended" and "recommended". It also specifies how conformity with these prompts will be achieved and potential "pitfalls". For example, in the risk assessment component it details problems encountered when using certain methods of risk estimation.
As with many safety cases, the UL 4600 standard adopts a "lifecycle approach". It requires developers to consider the use of the vehicle throughout its operational life.
This approach also requires that the supply chain for the maintenance of the vehicle has been considered. For example, if a claim is made that a camera will be clean due to the use of a spray wash, developers should account for a faulty low-fluid sensor, or the possibility that fluid has insufficient anti-freeze for winter. UL 4600 is structured to provide feedback. The standard requires developers to have mechanisms in place for collecting and processing field feedback data. They must also have processes for managing any uncertainties, assumptions and potential gaps in the safety case on an ongoing basis.

4.1.9 Using safety cases during the approval process

The UK reminds that even though much work is being done on technical regulations at a UNECE level to ensure that automated features can be incorporated into the type approval process, technical regulations take time to develop. Also, in the early years of development, AVs may well use different standards and technologies. Therefore, it is stated that it is almost inevitable that safety cases will form part - probably a crucial part - of any approval process. As is has been developed, safety cases are already a significant part of the ALKS Regulation for example.
A safety case requires the manufacturer or developer to come up with an argument demonstrating why the system is safe. In other words, those wishing to deploy systems must proactively assess risks. It allows a developer or manufacturer to argue for their own approach to safety. In the absence of widely accepted technical standards, this could allow the regulator to assess each ADS on its merits.
Another benefit is that a safety case integrates evidence from the development process in a structured way. For example, evidence from road trials, simulation and track tests can be presented in a comprehensive and cohesive format, allowing the regulator to assess a given system.

Finally, under this proposed scheme, the Automated Driving System Entity (ADSE) will have significant responsibilities for the safety of the ADS on an ongoing basis, perhaps for the entire

operational life of the vehicle. A properly constructed safety case could take an entire lifecycle approach, allowing the ADSE to demonstrate how it will fulfil their ongoing duties.

This is not to say that the safety case approach is perfect. For example, the Health Company noted the following dangers of safety cases:

1) if not implemented properly, safety cases could become a paper exercise;
2) they might be removed from everyday practice and become exercises in shifting potential liability; and
3) they might be produced by the wrong people or those outside the organization.

Furthermore, it may also be a significant challenge for the developer or manufacturer to generate appropriate evidence for the claims they make or the ODDs in which they seek to deploy. ODDs that are more complex may require more robust evidence.

Given that safety cases are likely to play a significant role in assessing AVs, The UK considers important that they are compiled honestly and accurately and do not suppress evidence.

4.2 Australia

In June 2017, the National Transport Commission (NTC) of Australia consulted on whether to require third-party testing in the context of automated vehicles. Following consultation, they concluded that pre-market approval by a third party would be "resource-intensive and time consuming" and could limit or obstruct safety-related innovations. However, the NTC thought that pre-market checks might be more feasible in the long term, once regulators have a better understanding of the technology and its risks.
The NTC subsequently published a 2018 Regulation Impact Statement. This put forward their preferred option under which the ADSE would provide self-certification against fixed criteria. This would be combined with oversight by a government agency, specific offences and enforcement measures. The ADSE would also be subject to a "primary safety duty" which was described as: overarching and positive general safety duty… to ensure that the ADS is as safe as reasonably practicable.
Furthermore, it is foreseen this duty would: support the mandatory self-certification approach as an ongoing duty throughout the life cycle of the ADS. It would aim to ensure that in-service safety risks and hazards that are not identified through the safety assurance system process are managed and that unsafe behaviors that are not captured otherwise by prescribed offences are prevented.

4.3 United States of America

The National Highway Traffic Safety Administration (NHTSA) of the Department of Transportation is seeking public comment on the development of a framework to govern the safety of automated driving systems (ADS). NHTSA submitted the advanced notice of proposed rulemaking (ANPRM) to the Federal Register on November 19, 2020.

The ANPRM marks a departure from previous regulatory notices on ADS. It looks beyond the existing non-binding guidance documents and limited regulatory modifications, and instead contemplates the establishment of a new framework tailored to ADS. The new framework could combine a spectrum of regulatory tools from new, non-binding guidance at one end, to new, performance based FMVSS at the other.
In contrast to prior efforts, this guidance suggests a desire within parts of the Agency to create a more comprehensive set of regulatory measures to monitor, measure, encourage, and/or mandate the safety of autonomous vehicles in the future. Going forward, NHTSA will emphasize a framework approach to ADS safety that may use a variety of approaches and metrics (including a focus on "ADS competence").
Consistent with NHTSA past and current practice, the ANPRM makes it clear that the Agency will not prescribe specific design characteristics or features that could constrain innovation and development. NHTSA proposes to develop a new, phased-in safety framework that would guide the evaluation and demonstration of the safety of new ADS systems.

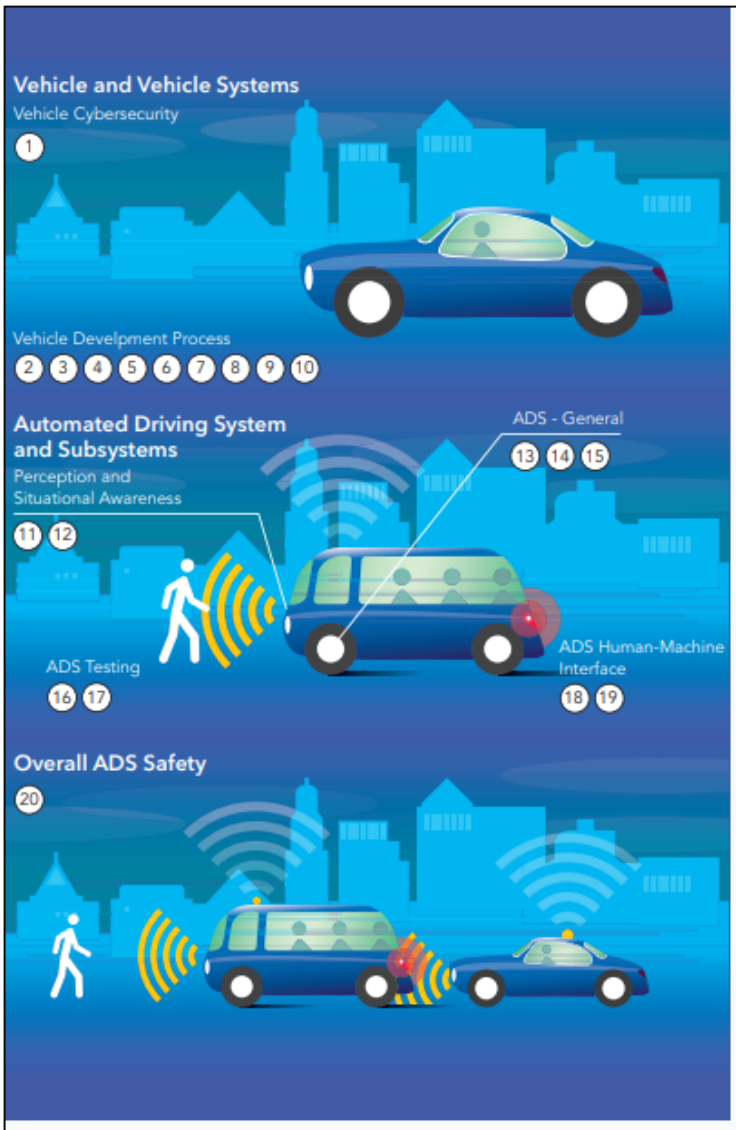
The framework would include guidance, standards, regulations, and other mechanisms to facilitate development of rapidly developing ADS technology.
The ANPRM emphasizes that the phased-in framework approach has two major benefits:

- First, it avoids setting rules about specific design features or content of ADS that may freeze development in its current state and hamper innovation.
- Second, the ANPRM indicates that widespread deployment of autonomous vehicles (AV) appears to be years away, and the phased approach allows NHTSA to leverage this long timeline by strategically determining which aspects of ADS safety require attention and when.

Like NHTSA's previous AV guidance documents, the framework is intended to evolve as ADS technology evolves. NHTSA identified four primary ADS functions that will be the focus of the safety framework:

- Sensing: How the ADS receives information about its environment through sensors.
- Perception: How the ADS detects and categorizes other road users, infrastructure, and conditions and predicts their future behavior.
- Planning: How the ADS analyzes a situation, plans the route it will take on its way to an intended destination, and decides how to respond appropriately to the road users, infrastructure, and conditions it detects and categorizes.
- Control: How the ADS executes the driving functions necessary to carry out its continuously updated driving plan.

The proposed ADS safety framework would include an array of mechanisms for implementation and oversight, including both voluntary programs and formal regulations. Voluntary mechanisms will promote information sharing and encourage best safety practices in the AV industry. These programs could include voluntary disclosures from manufacturers, car assessment programs, and guidance documents describing best industry practices. Regulatory mechanisms would be deployed later in the process, after ADS technology has further developed and NHTSA has studied ADS safety needs. These non-voluntary mechanisms could include mandatory reporting and the promulgation of ADS-specific FMVSS. Below, are the standards anticipated in the validation framework for ADS:



VEHICLE CYBERSECURITY

1. ISO 21434 (forthcoming): Road Vehicles - Cybersecurity Engineering

VEHICLE DEVELOPMENT PROCESS

2. ISO 26262: Road Vehicles - Functional safety
3. ISO 15288: Systems and software engineering System lifecycle processes
4. ASPICE 3.0: Automotive Software Process Improvement and Capability Determination (ASPICE)
5. AUTOSAR: Automotive Open System Architecture (AUTOSAR)
6. IATF 16949/ISO 9001: International Standard for Automotive Quality Management Systems
7. MIL-STD-882E: Standard Practice for System Safety
8. SAE J2998: Model Description Documentation Recommended Practice for Ground Vehicle System and Subsystem Simulation
9. SAE J3049: Model Architecture and Interfaces Recommended Practice for Ground Vehicle System and Subsystem Dynamical Simulation
10. SAE AS5553A: Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*

PERCEPTION AND SITUATIONAL AWARENESS

11. ISO/PAS 21448 SOTIF: Road Vehicles -- Safety of the Intended Functionality
12. SAE J3088: Active Safety System Sensors

ADS - GENERAL

13. SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
14. AVSC00002202004: AVSC Best Practice for Describing an Operational Design Domain: Conceptual Framework and Lexicon
15. SAE J3197: Automated Driving System Data Logger

ADS TESTING

16. SAE J3018: Guidelines for Safe On-Road Testing of SAE Level 3, 4, and 5 Prototype Automated Driving Systems
17. AVSC00001201911: AVSC Best Practice for safety operator selection, training, and oversight procedures for automated vehicles under test

ADS HUMAN-MACHINE INTERFACE

18. AVSC00003202006: AVSC Best Practice for Passenger-Initiated Emergency Trip Interruption
19. SAE J3114: Human Factors Definitions for Automated Driving and Related Research Topics

OVERALL ADS SAFETY

20. UL4600: Standard for Safety for the Evaluation of Autonomous Products

*Recently published NHTSA research explored the potential applicability of SAE AS5553A - originally developed for the aerospace industry - to the automotive sector (see Bielawski, R., Gaynier, R., Ma, D., Lauzon, S., & Weimerskirch, A. (2020, October). Cybersecurity of Firmware Updates (Report No. DOT HS 812 807). National Highway Traffic Safety Administration (https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf).). Note that this standard has been updated to SAE AS5553C subsequent to the completion of the research and analysis conducted to inform this report.

Figure 14: Extract from the comprehensive plan [25]

4.4 California

In April 2018, California established regulatory regimes for the testing and deployment of automated vehicles. These regimes provide for vehicles which do not have a safety driver. The Californian system is based on self-certification by a "manufacturer". This covers not only those who produce an autonomous vehicle from raw materials or basic components, but also a person who modifies any vehicle by installing autonomous technology.
To obtain a deployment permit the manufacturer must certify that it has "conducted test and validation methods and is satisfied that the vehicle is safe for deployment on public roads". The manufacturer or their authorized representative must sign and certify under penalty of perjury that, among other things, their automated vehicles:

(1) are designed to be incapable of operating in autonomous mode outside their operational design domains;
(2) are equipped with data recorders capable of recording and storing all relevant data;
(3) are designed to detect and respond to roadway situations in compliance with the California Vehicle Code and local regulations, *except* when necessary to enhance the safety of the vehicle's occupants and/or other road users; and
(4) meets current industry standards on cyber-security.

The manufacturer must also undertake to provide updates that ensure compliance with any changes to the California Vehicle Code and local regulation.
If a manufacturer intends for a vehicle to be sold or leased to other people, a consumer or end user education plan must be submitted with the application. The plan must include an explanation of how the end-user will receive education after purchasing a previously owned vehicle.

4.5 Singapore

In 2017, Singapore amended its Road Traffic Act to provide for approved trials and approved "special use" of "autonomous motor vehicles". The definition of autonomous motor vehicles is similar to the UK definition of self-driving under the AEV Act 2018. It refers to a motor vehicle that is fitted "wholly or substantially" with an "autonomous system". An autonomous systems is defined as a system that enables the operation of the motor vehicle without the active physical control of, or monitoring by, a human operator.
A "special use" covers "the use on a road of an autonomous motor vehicle by a specified person authorized by the Authority".
The amendments give the Minister broad powers to make rules. When approving a trial or special use the Minister can prescribe the use of the autonomous motor vehicles in the approved trial or approved special use, and their construction, design and equipment, for the safety of other road users or for public safety or both.
So, for example, the rules may exempt AVs from construction or use rules that apply to ordinary vehicles.
This regime is intended as a "regulatory sandbox" with which to trial AV technologies in Singapore. At the end of five years, the Ministry of Transport in Singapore will consider enacting more permanent legislation.
In addition to the amendments to the Road Traffic Act, Singapore authorities have also worked on developing standards for AVs. In 2019 Enterprise Singapore and Singapore's Land Transport Authority (LTA) published a set of provision national AV standards, referred to as Technical Reference 68 (TR 68). These standards outline basic behaviors to which AVs should be capable of adhering. TR 68 also gives guidance on general safety considerations, cybersecurity and the capture and formatting of data. Currently the standard is provisional and only voluntary in nature. It will be developed over the coming years based on feedback received from those applying it.

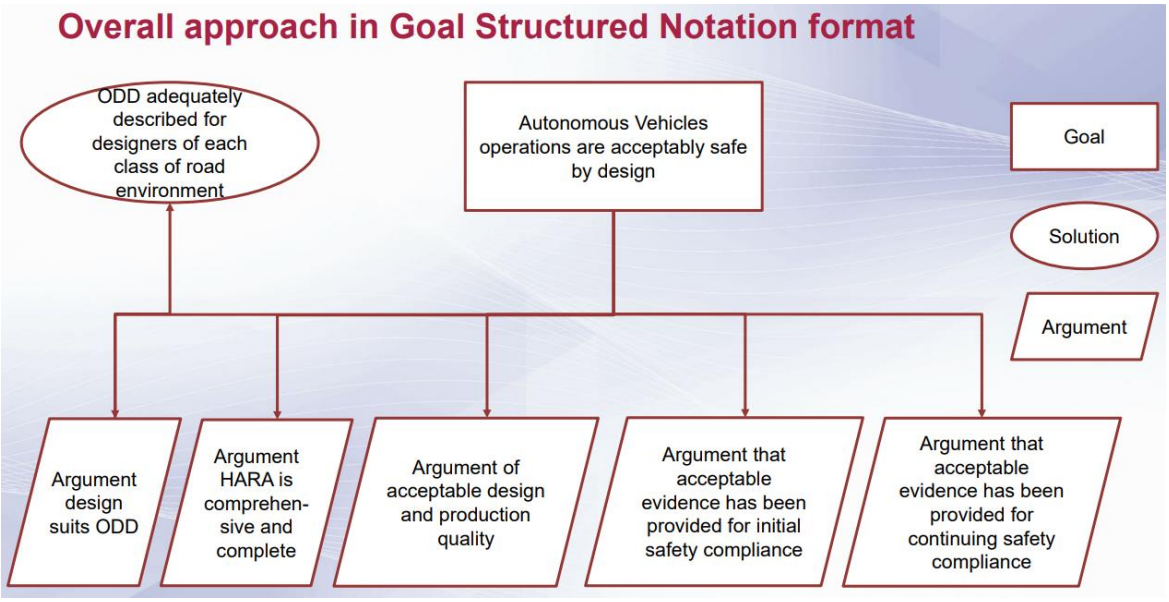


Figure 11: Overall test scope tailored to the operational environment and capabilities of the vehicle presented by the TR 68

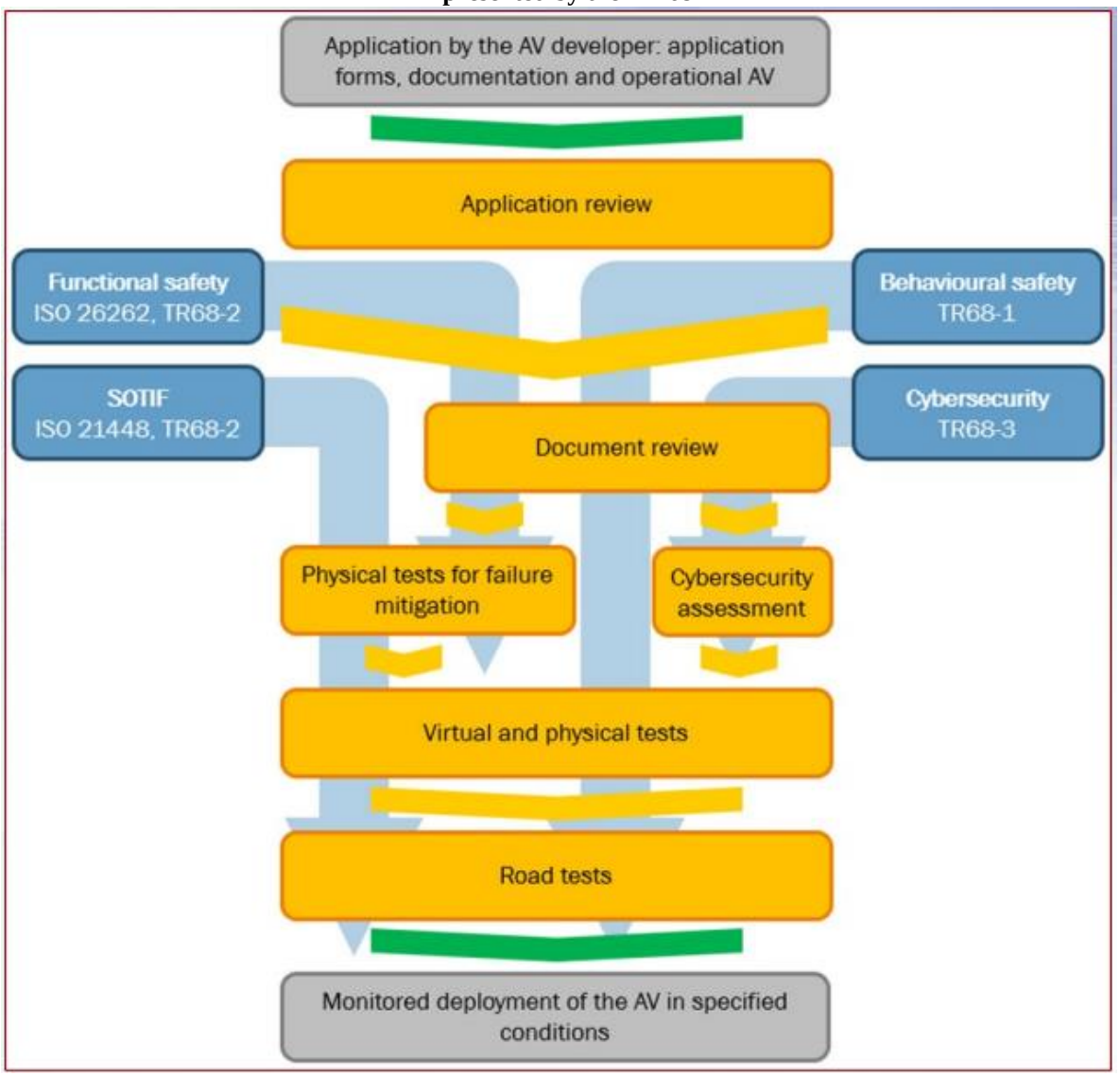


Figure 16: Description of the approval process

4.6 China

On April 12, 2018, the Ministry of Industry and Information Technology, the Ministry of Public Security and the Ministry of Transportation jointly issued the Administrative Rules of Road Testing of Intelligent Connected Vehicles (for Trial Implementation) (the "Administrative Rules"), which subsequently came into force on May 1, 2018. The Administrative Rules are the first national level regulatory document on road testing of ICVs. By standardizing and unifying the Local Rules, the Administrative Rules serve to accelerate the development of road testing processes for ICVs in China.

4.6.1 Safety Guarantee: Admission and Management of the Testing Party

The Administrative Rules set out the requirements and conditions for test vehicles, test applicants and test drivers, and include a number of requirements for the management of tests to ensure safety during the road testing of ICVs.

4.6.1.1 Test Vehicles: Six Requirements

The Administrative Rules set out six specific requirements for test vehicles, relating to their registration, mandatory items for testing, switching between self-driving and manual modes, data recording and real-time information monitoring, testing locations, and third-party verification of testing. Detailed requirements for ICV test vehicles ("test vehicles") are as follows:

- A test vehicle cannot be registered as a motor vehicle;
- Mandatory items for test vehicles should satisfy relevant requirements for corresponding non-self-drive vehicles, with the exception of durability. If, during testing, a particular mandatory testing item is not met due to the self-driving function, it will need to be proved that this has not in any way jeopardized the safety performance of the test vehicle;
- A test vehicle should be able to be steered both manually and automatically, and it should be able to be switched safely, rapidly and easily between the self-driving and manual driving modes;
- A test vehicle should have the capability to record, store and monitor the status of the vehicle, providing real-time information about the current vehicle control mode and other specified information, and should automatically record and store data for at least 90 seconds prior to any vehicle accident or malfunction, with the data stored for at least three years;
- Field tests for test vehicles should be conducted only in locations approved for testing, such as closed roads or sites;
- The self-driving function of test vehicles should be tested and verified by a third-party testing institute with the necessary inspection license as specified in the Administrative Rules.

In addition, in order to ensure safety during testing, the Administrative Rules stipulate that during a test, a test vehicle shall not carry any person or freight that is not of relevance to that test. The Administrative Rules further stipulate that the self-driving mode shall not be employed during an ongoing test, except when the test vehicle is running on roads designated for testing, and that the test vehicle shall be driven manually from the parking lot to the road designated for testing purposes.
In terms of the requirements on test vehicles, the Administrative Rules appear to draw lessons from the road test rules issued by various local government authorities, and in particular those of the Shanghai local government authority.

4.6.1.2 Test Applicants: Seven Conditions

The Administrative Rules set out seven conditions for test applicants relating to the nature of the business entity, the scope of business, the capacity to compensate in the event of an accident, test evaluation, remote monitoring, event record analysis and conformity with laws and regulations. Detailed requirements are as follows. An applicant for a test should:

- Be an independent legal entity registered within the territory of the People's Republic of China;
- Have business capacity of relevance to intelligent ICVs, such as automobile and spare parts manufacturing, research and development of technology, and experimentation and testing;
- Have the financial capacity to cover civil compensation for any damages caused to people or property by ICVs during testing;
- Have its own evaluation rules for the testing of the self-driving functions of ICVs;
- Have the capability to conduct real-time, remote monitoring of test vehicles;
- Have the capability to record, analyze and reproduce events performed by test vehicles;
- Comply with other conditions required by laws, regulations and rules.

The Administrative Rules do not set out any special requirements for foreign invested enterprises, with the above provisions applied equally to foreign invested enterprises and to Sino-foreign joint ventures registered in China.
Comparing the Administrative Rules with the rules of road testing previously issued by Beijing, Shanghai and other cities suggests that the Administrative Rules have for the most part taken as their basis the Shanghai rules relating to the conditions for the testing applicant.

4.6.1.3 Test Drivers: Eight Requirements

Based on the rules of road testing issued in Beijing and Shanghai, the Administrative Rules include eight requirements for test drivers addressing items including employment and labor

service contracts, self-driving training, and major traffic violation records. Specifically, test drivers should:

- Have an employment contract or a labor service contract with the test applicant;
- Have held a driving license for driving the corresponding type of vehicle and have driving experience of at least three years;
- Have not received twelve points under the demerit point system in the three most recent demerit periods;
- In the past year, have no record of serious traffic violations, for example driving at a speed exceeding 50% of the upper limit, or violating traffic light rules;
- Have no record of drink-driving or taking State-controlled psychotropic or narcotic drugs;
- Have no record of traffic accidents causing death or serious personal injuries;
- Have familiarity with the testing rules and operation of self-driving vehicles following self-driving training sessions provided by the test applicant, and be capable of responding to emergencies; and
- Comply with other requirements specified in laws, regulations and rules.

In addition, in order to ensure safety, and on the basis of insights gained from the accident caused by Uber's self-driving vehicles, the Administrative Rules specify that a test driver: 1) must always be seated in the driver's seat of the test vehicle, 2) must observe the driving status of the test vehicle and the surrounding environment during the entire test process, and 3) must be ready at all times to take control of the vehicle.

4.6.2 Safety Guarantee II: Revocation of Testing Notice

The Administrative Rules set out various requirements on test vehicles, test applicants and test drivers in order to ensure safety during the testing. At the same time, the Administrative Rules refer to the road testing rules issued in Beijing and Shanghai, and especially the rules in Shanghai, and empower the competent authorities to revoke a testing notice under certain conditions. The Administrative Rules stipulate that the competent authorities can revoke the testing notice and suspend the test, should any of the following safety issues arise during the testing period:
The relevant competent authorities of the provincial or municipal government believe that the testing activities carry major safety risks;

- The test vehicle is involved in a serious violation of traffic rules, such as violating traffic light rules, driving in the wrong direction, or other serious traffic violations for which the penalty under traffic law may be to temporarily detain or to revoke the driving license or to hold the violator in custody;

- The party owning the test vehicle has the main responsibility in a serious traffic accident, which, for example results in serious personal injury, death or significant damage to a vehicle.

There is currently no specific provision in Administrative Rules as to what subsequent impact the revocation of a testing notice might have on the testing applicant, such as whether the testing applicant can re-apply for a test, and if so how long it would need to wait to re-apply for such test. These details await further definition in future Local Rules.

4.6.3 Safety Guarantee III: Assumption of Liability for Accident

In order to assign responsibility to the violating parties involved in traffic violations or accidents during an ongoing test, the Administrative Rules provide a specific section, entitled "Handling of Traffic Violations and Accidents". The section clarifies how to handle traffic violations, identify the liability of the parties involved, and specify the relevant departments responsible for handling accidents and imposing punishment. The Administrative Rules also stipulate the obligations of the concerned parties and the reporting requirements on the test applicants and provincial and municipal competent authorities following any accident. Details are as follows:

- In the event of a traffic violation being committed during an ongoing test, the traffic administrative department of the public security authority shall deal with the test driver according to the existing laws and regulations regarding road traffic safety;

- In the event of a traffic accident occurring during an ongoing test, the liability of the concerned party shall be determined according to existing road traffic safety laws and regulations, and the liability for damages shall be determined in accordance with relevant laws, regulations and judicial interpretations. Where a crime has been committed, criminal liability shall be pursued according to law.

In summary, in the event of any traffic violation, the liability should be assumed by the test driver, and in the case of traffic accidents, the party assuming the liability for the accident and damages should be determined according to the law. The Administrative Rules do not specify in any detail the liability of the test applicant. Whether the test applicant, as an employer, should assume overall liability for compensation, whether they should assume joint liability with the employee, or whether the producer and/or seller of the test vehicle should assume product liability require determination from subsequent legislation or judicial practice.

4.7 Japan

The Japan Automobile Manufacturers Association Inc. (JAMA) has summarized the best practice on safety argumentation structuring, safety evaluation, and safety assessment methods needed to enable logical completeness, practicability, and transparency of AD safety on limited access highways. This document aims;

- To enhance safety and efficiency of AD systems development by providing guidelines that serve as a common ground for each JAMA member at each product development stage, from planning and design to evaluation.

- To gain a common technical understanding when international regulations and standards are formulated.

- To clarify JAMA position when cooperating with international projects.

Although JAMA member manufacturers have established them for application in safety evaluation and verification procedures in every phase of the development, design and assessment of their technologies, it is hoped that the guidelines will also serve as a useful reference in technology development for other stakeholders.
JAMA believes that these guidelines can help propel domestic and international projects related to automated driving technology safety evaluation and contribute to the development of international standards and regulations.

4.8 Current standards

The last few years have seen many initiatives to develop standards for AVs. However, there is no single agreed standard governing the industry. Some standards are high-level and aspirational. Others are very specific, relating to AV terminology, the behavior of the vehicle or one part of the development process.

CCAV have sponsored the British Standards Institute to develop four standards related to AV development. One of these is the PAS 1881:2020 Assuring the Safety of Automated Vehicle Trials and Testing – Specification has now been published. It is intended to support the safe testing and trials of CAVs. PAS 1881 specifies minimum requirements for safety cases for automated vehicle trials and development testing in the UK to demonstrate activities can be undertaken safely. This PAS is relevant to stakeholders including (but not limited to) trialing organizations, local authorities, highway authorities, road operators, landowners, leaseholders, insurers, test beds and licensing agencies.
However, the standard focusses on operational control measures such as the training of safety drivers to demonstrate that risk has been managed but does not consider the safety of the automated systems themselves.

IEEE 1616-2004 - Institute of Electrical and Electronics Engineers (IEEE) Standard for Motor Vehicle Event Data Recorder (MVEDR): This standard defines a protocol for MVEDR output data compatibility and export protocols of MVEDR data elements. It does not prescribe which specific data elements shall be recorded, or how the data are to be collected, recorded and stored. (See in addition IEEE 1616a-2010 - IEEE Standard for Motor Vehicle Event Data Recorders (MVEDRs) Amendment 1: MVEDR Connector Lockout Apparatus (MVEDRCLA))

IEEE P7001 - IEEE Draft Standard for Transparency of Autonomous Systems: aims to describe measurable, testable levels of transparency, so that autonomous systems can be objectively assessed and levels of compliance determined.

The IEEE have also created a working group to develop a standard (IEEE 2846) based on the Responsibility-Sensitive Safety (RSS) model.

SAE J1698_201703: These series describe common definitions and operational elements of Event Data Recorders. It consists of:

- SAE J1698-1 - Event Data Recorder - Output Data Definition
- SAE J1698-2 - Event Data Recorder - Retrieval Tool Protocol
- SAE J1698-3 - Event Data Recorder - Compliance Assessment

SAE J3237 Operational Safety Metrics for Verification and Validation (V&V) of Automated Driving Systems (ADS): this report contains definitions and lexicon for describing operational safety metrics for quantifying the operational safety performance of ADS and ADS-operated vehicles.

SAE J3197 Automated Driving System Data Logger: this is a recommended practice that provides common data output formats and definitions for a variety of data elements that may be useful for analyzing the performance of (ADS) during an event that meets the trigger threshold criteria specified in this document. This document is intended to govern data element definitions, to provide a minimum data element set, and to specify a common ADS data logger record format as applicable for motor vehicle applications.

ISO/PAS 21448: Road Vehicles — Safety of the Intended Functionality (SOTIF): Safety Of The Intended Functionality (SOTIF) refers to the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons. This standard is intended to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms; especially emergency intervention systems and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA/SAE standard J3016 automation scales. This document can be considered for higher levels of automation, however it is pointed out that additional measures might be necessary.

ISO 26262: Road vehicles — Functional safety: This document concerns safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. It covers possible hazards caused by malfunctioning behavior of these systems.

Neither of these two previous standards was specifically developed for automated driving. There is debate about how far these standards can be applied to AVs. It can be noted that ISO 26262 focusses on each individual E/E/P system rather than on the automated driving system as a whole. As an ADS may be comprised of many individual E/E/P systems, the concern is that ISO 26262 may not adequately assess how these systems interact and work together.

At the same time, it is expected that AVs will be trained with artificial intelligence and machine learning. One of the proclaimed benefits is that AVs will "learn" to become safer over time. However, this also means that the system could learn to react in a way that was not foreseen during the design and approval process. The methods in ISO 21448 may be insufficient for

considering machine learning systems which are "non-deterministic". In other words, not all the actions of the system can be accounted for or explained by its designers.

Manufacturers have also begun to develop standards for AVs. In September 2019, a consortium of Original Equipment Manufacturers (OEMs) and mobility companies published a white paper, "Safety First for Automated Driving" ("SaFAD"). The paper provides guidance on developing and validating a safe automated driving system and has been developed into an industry-wide standard. It foresees that simulations, track testing and real-world testing will all be used in constructing a safety case. It also suggests continued field-monitoring throughout the lifetime of a system.

Standards directed at ongoing management might also be applicable. The ISO 9001 series, for example, sets out criteria to ensure a quality management system. This standard might be used by an ADSE to ensure that they have an adequate management system in place to ensure they fulfil their duties in relation to the ongoing safety of an ADS.

5 Other Projects and key aspects

5.1 Focus on the COVADEC project

COVADEC stands for Conception et Validation des Systèmes Embarqués d'Aide à la Conduite, meaning in French: Design and validation of Embedded ADAS.
This collaborative project was launched in 2013 for 3 years. Its budget was 4.2 million euros, and it was partially funded by the French State.
The COVADEC consortium included 6 companies: ALL4TEC (program leader), Civitec, INTEMPORA, MAGILLEM DESIGN SERVICES, PSA GROUPE, Valeo - Site de Créteil and 2 public research institutes: ARMINES and INP Grenoble.

The project targeted the definition and development of methods and tools to:
Optimise tests scenarios to reduce the necessary number of kilometers run for ADAS validation
Optimise time and cost of ADAS validation
Meet the reliability requirements
Standardise ADAS validation methods and tools

Since it is an industrial program, most of COVADEC results were confidential. However, 4 publications about the project were found: Raffaelli & Rouah (2014)[3] , Raffaelli (2015) [4], Raffaelli, Vallée et al. 2016 [5], Raffaelli, Fayolle et al. 2016 [6].

The work was organized in 5 work packages (WP) (plus the management) as shown on **[Figure 23]**.

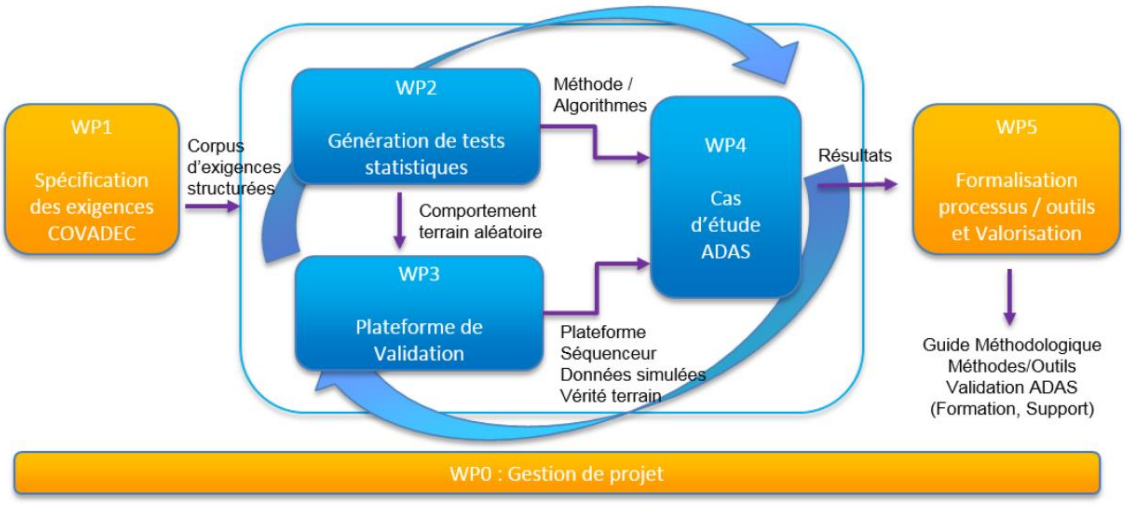


Figure 17: COVADEC work packages definition - Raffaelli, Fayolle et al. 2016[6]

The project focused on camera vision based ADAS systems. Moreover, the tools and methods were dedicated to Model in the loop (MIL) and Software in the loop (SIL), the early stages of an ADAS validation.
The two use cases selected to apply the methods and tools in WP4 were an Autonomous Emergency Braking (AEB) and a Lane Departure Warning (LDW).

Most of WP1 was dedicated to the development of Model-Based Testing (MBT) methods to generate scenarios and a full validation process for reliability test and for safety tests.

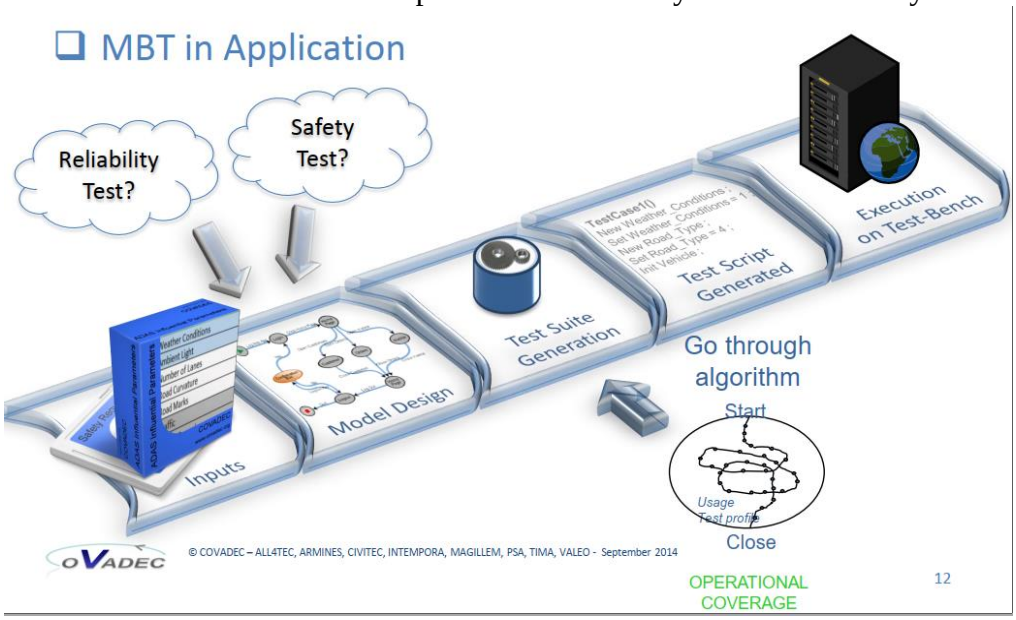


Figure 18 : COVADEC MBT approach and its tool chain - Raffaelli & Rouah (2014) [3]

A statistical approach was chosen. However, modelling was found out to be a complex process as most of scenario variables were not independent and combinations of the variables would also lead to an exponential number of test cases and most of these test cases would be unrealistic or have no interest to validate an ADAS.
Therefore, the COVADEC project used methods based on Markov Test Logic in the tool MaTeLo combined with Monte Carlo methods and a Gibbs sampler (Raffaelli, Fayolle et al. 2016, [6]).
Another innovation in the COVADEC project is to combine real world data with the MBT to ensure realistic and relevant test case selection. But a great limitation came with the use of real data recorded on the road, it is a lake of dangerous situations needed for a deep validation of the ADAS.

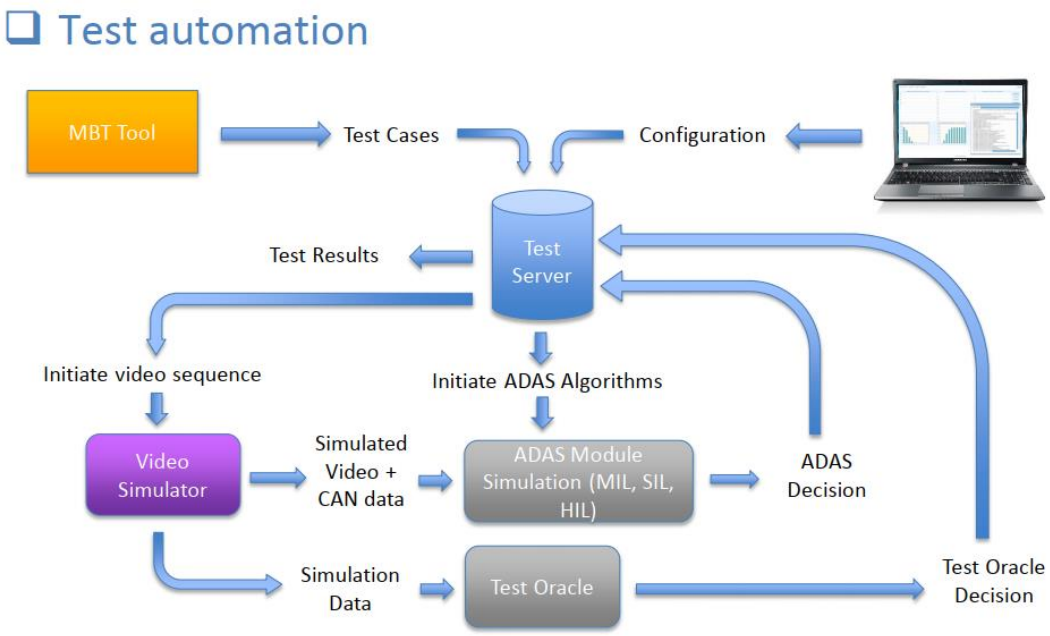


Figure 19: COVADEC testing process

As shown in **[**Erreur ! Source du renvoi introuvable.**]**, the testing process used a test oracle. This test oracle is an algorithm base on parameters from the video simulator and not relying on video analyses. The oracle predicts the correct behavior the ADAS should have. Then, it makes possible to assess automatically the results of the ADAS. However, the articles do not give further details about the implementation and functioning of this oracle.

The chain of tools used or developed during the project is the following (see also **[Figure 26]**):

- MaTelo (All4Tech): modelling and sampling;
- DEEP (Intempora): automated test server;
- Pro-SiVIC (CIVITEC/ESI): scenario simulator;
- RTMaps (Intempora): framework for real time ADAS algorithms execution;
- Dataloggers from Intempora;
- Rabbits (TIMA): ADAS hardware architecture simulator.

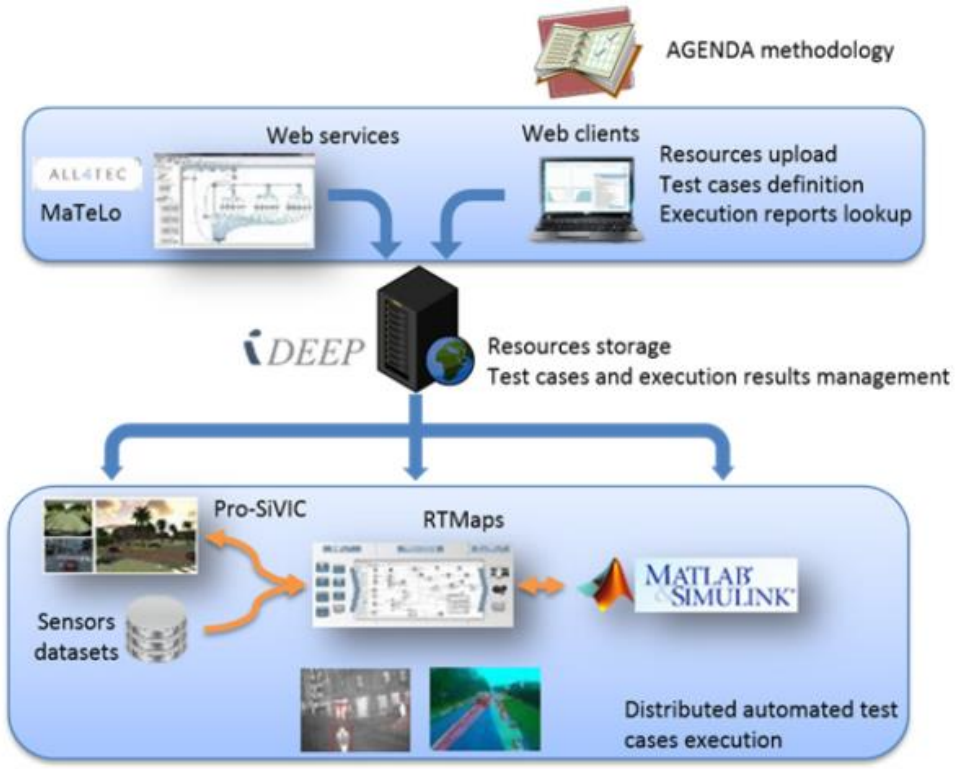


Figure 20: COVADEC tool chain

5.1.1 COVADEC vs PRISSMA

COVADEC project was launched in 2013 making its findings and processes a bit dated. However, most of the tools developed or used during the project are still used for ADAS validation and they are still evolving.
The COVADEC process focused on camera vision based ADAS and does not treat the data fusion with other sensors such as radars.
It also focused on MIL and SIL, the early stages of ADAS validation.
No reference is made to the validation of an artificial intelligent (use of neural network) algorithm. However, the validation process and the tool chain from the MBT to the use of an oracle is still very relevant to validate a vison-based AI. Likewise, the process could generate datasets of scenarios used during the learning process of a vision-based AI.
No mention to the notion of ODD was found, but the models are based on parameters for:
Weather conditions
Structure of the road and of the environment
Behavior of the surrounding vehicles
Pedestrians
Obstacles and disturbances

As an industrial project, all the results from COVADEC were not published but the information given in the few articles and the quality of the tools developed or used, make COVADEC an interesting project for PRISMMA.

5.2 SESNA project

SESNA (Supervision Et Sûreté de l'Exploitation d'un service de Navettes Autonomes sur site sensible) is a collaborative 3-year project launched in January 2017 under the FUI 22 call for a budget of 4.7 million euros. SESNA focuses on the on-site testing of the deployment of a fleet of autonomous shuttles with the aim of:

- Developing a validation methodology for a shuttle system with regard to safety and performance
- Studying the challenges with regard to cybersecurity
- Identifying the building blocks of an SAE (Operating Assistance System)
- Defining a benchmark of requirements (normative framework) for shuttle fleet deployment

The consortium was composed of one academic (CEA LIST) and four companies: Sherpa Engineering, Bureau Veritas, Easymile, BMCP. The CEA-Saclay center hosts the real-life experimentation as sensitive site.

The project was organized in 5 sub project (SP) as shown in Figure . The SP1 ensured the management, coordination and dissemination of results of the overall project. The others SP focused on different technical areas.

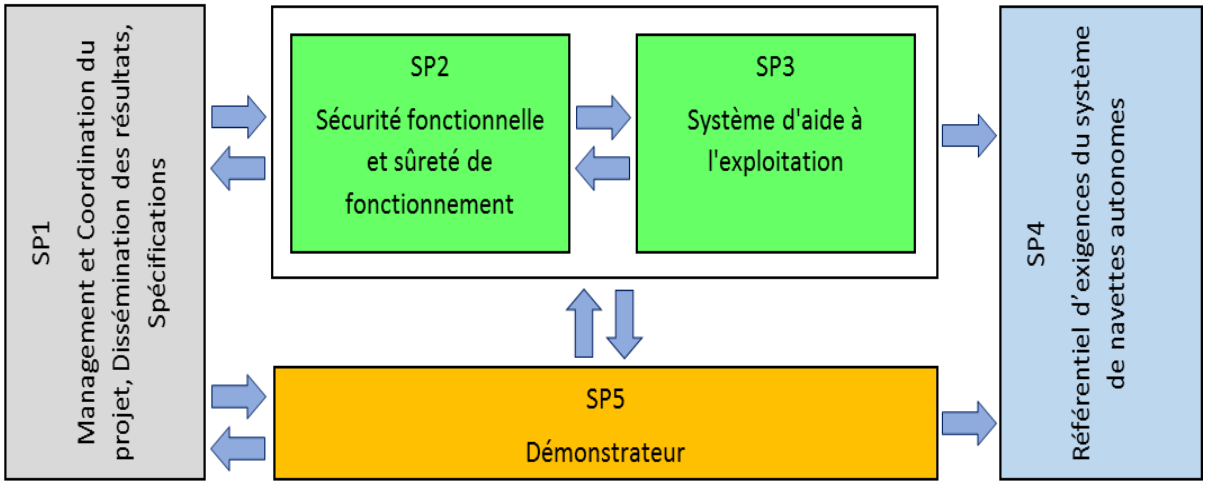


Figure 21: SESNA project organization in Work Package

The SP2 deals with functional safety and dependability of the overall system and the software controllers. SP2 main objective is to develop a tooled methodology for validating an internal service system on a sensitive site including a fleet of autonomous shuttles and to deploy it through the real demonstrator set up in the project. The validation reveals functional safety issues that the manufacturer was able to correct before the final deployment of the shuttles on CEA-Saclay site, or that they can take into account in future versions of the shuttles that they will put on the market for the more complex failures requiring modification during the design of the shuttles. SP2 methodology was based on modeling, decomposition and analysis at different levels of the service system with:

- Functional modeling at different levels of the service system and autonomous shuttles at shown on **[**Figure **]**: at the service level, at the level of the shuttle system in their environment and at the shuttle level;
- The risk analysis carried out at these different modeling levels (see Figure)
- A simulation model coupled with the model of the internal service system that will be used for the evaluation of the design and the verification of functional safety (see Figure)

- A formal validation of critical components
- A validation by simulation of the formal analysis by faults and feared events injection;

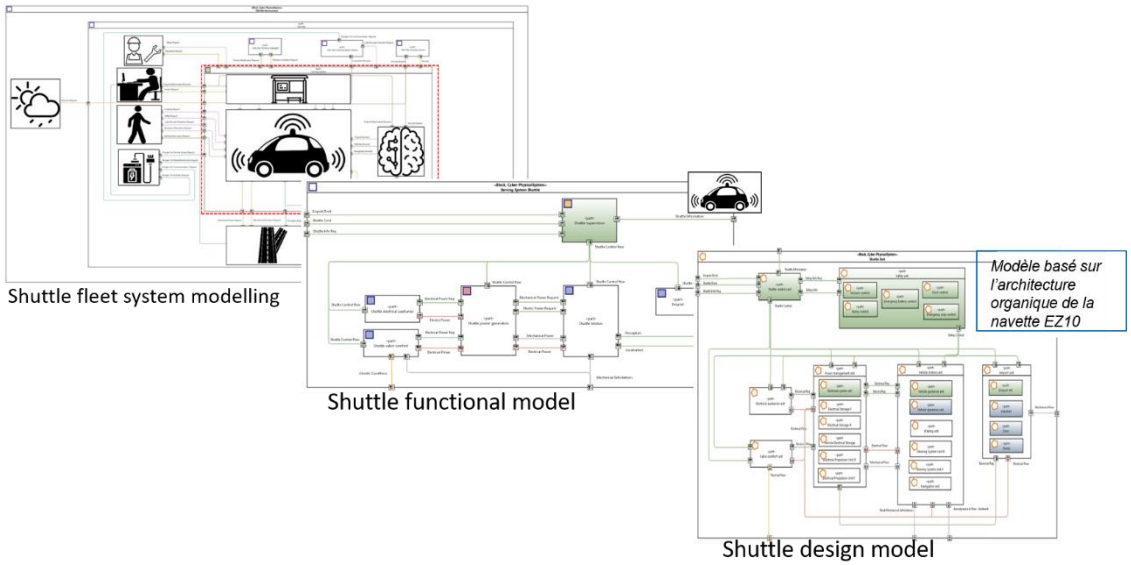


Figure 22: Different modelling levels of a shuttle fleet system

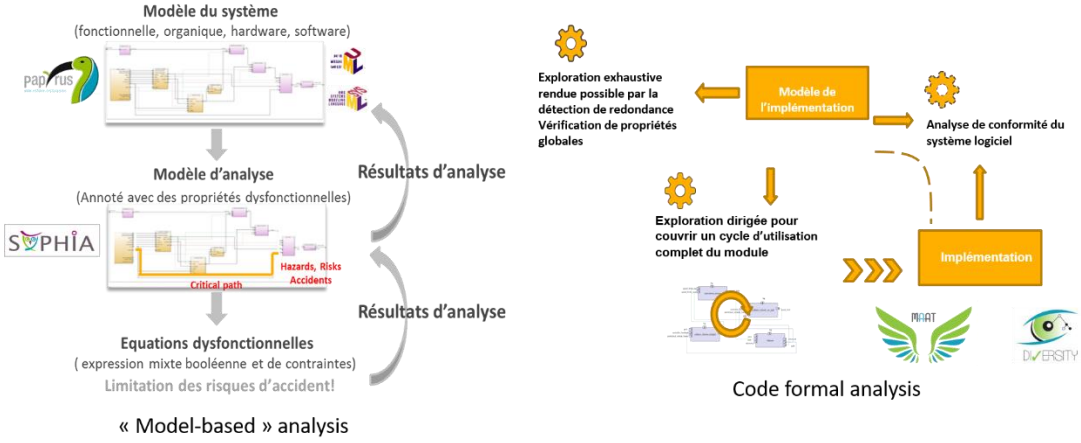


Figure 23: Tool chain for dependability analysis of autonomous system from model to code level

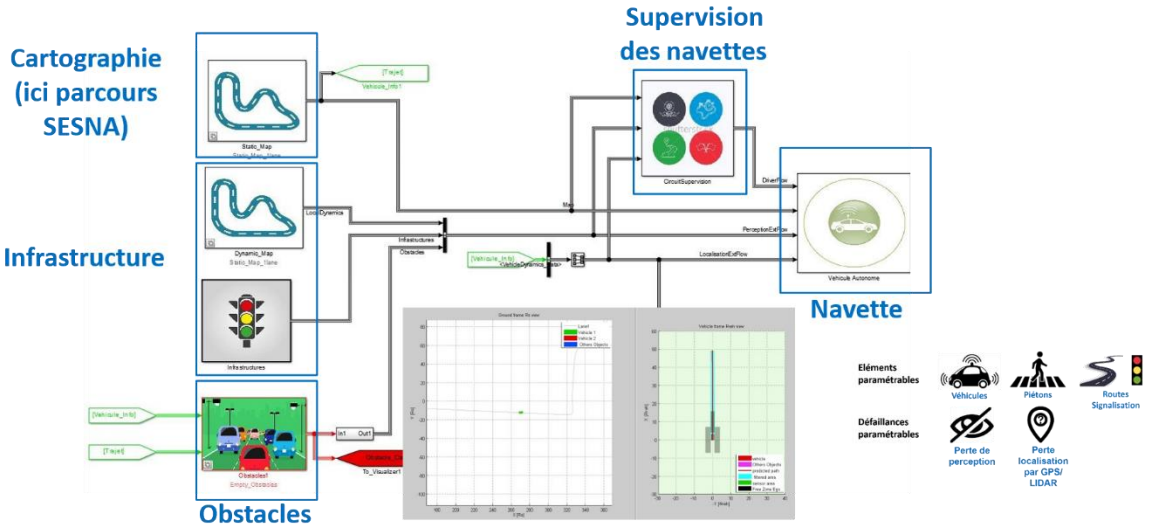


Figure 24: SESNA simulation framework

The SP3 studied the problem of the operation of the shuttles with regard to the challenges of:
- Cybersecurity associated with their deployment and remote monitoring;
- Global operating assistance system, integrating the issues of supervision, regulation, interoperability and management of degraded modes.

As results, SP3 provides:

- an assessment of the system from a cybersecurity point of view coupled with the safety assessment viewpoint (see Figure);
- a specification of countermeasures to the identified potential attacks;
- a vulnerability analysis and formal validation of the implementation of software countermeasures;
- a specification of the operating assistance system dealing with technical information and communication issues (information system / VA control command system interaction) and functional issues of operating a public transport system. Note that since the project was not able to deploy on the experimentation site a concrete operating assistance system due to sensitive site restrictions, the latter analysis was performed only at a theoretical level.

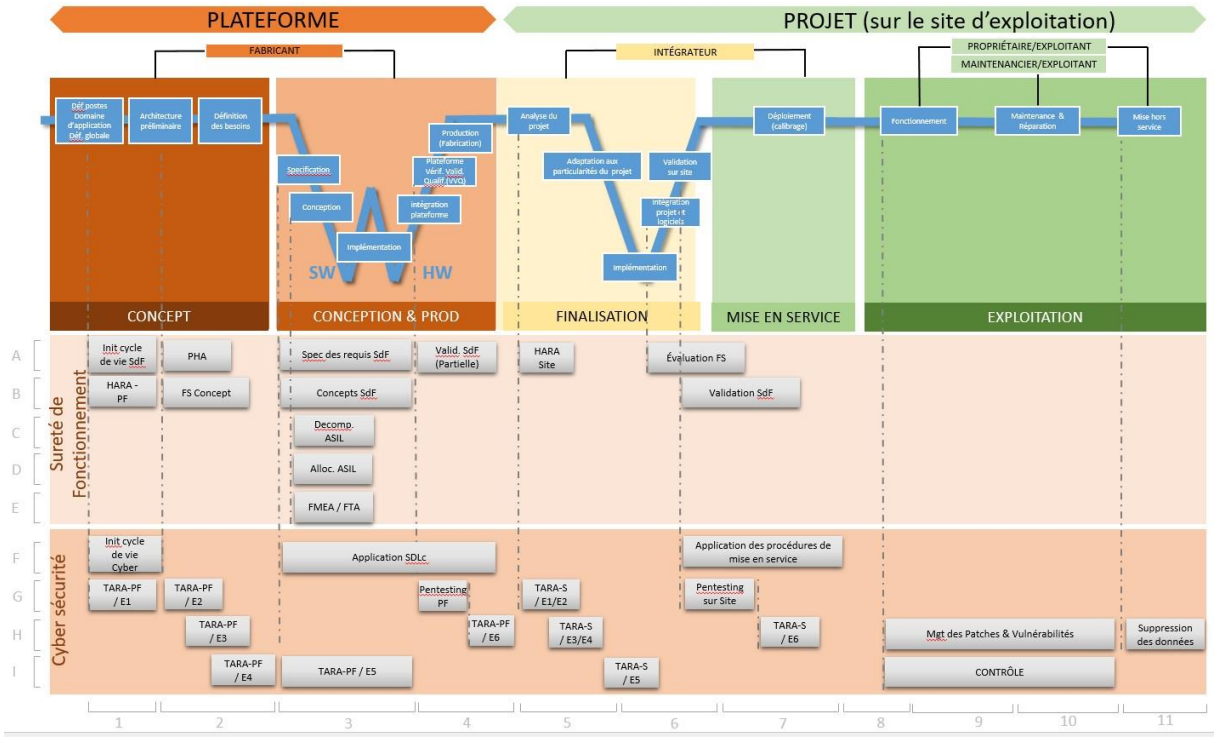


Figure 25: Integrated Safety and cybersecurity analyses on system shuttle system's lifecycle

The SP4 objective was to define a harmonized framework with technical prescriptions necessary for the construction of the safety case (combining verifications, tests applicable to autonomous shuttles, demonstrations, specification documents, etc.) for the deployment of autonomous shuttle. The framework gather requirements covering all stages of the shuttle system's life cycle as shown on **Figure 31** : components, separate technical units and equipment, design, manufacture, operation, maintenance, disposal, etc. A multi-domain normative and regulatory inventory was carried out in order to identify the relevant existing sources (Regulations, Directives, standards, decrees, etc.) to be considered (partially or totally) for the drafting of this standard dedicated to autonomous shuttles for a passenger transport application on private sites.

The SP5 was to validate the different technological elements developed in SP2 and SP3 on Easymile shuttles in order to benefit from feedback of the exploitation on real conditions. The project collect exploitation data during the real experimentation on site and come up with several recommendations and findings on: the shuttle and its environment, shuttle operation, maintenance and storage, and security aspects regarding the deployment on sensitive site.

The project makes use of several tools:

- Papyrus and Physistem (Sherpa tool) for the modelling aspect
- Phisim (Sherpa tool) for the simulation platform
- Papyrus extension for Safety (Sophia) and Cybersecurity (Ares) for the dependability analysis
- Maat and Diversity (CEA) for the formal analysis

As a summary, SESNA project develop a framework based on modeling, simulation, formal validation methods and tools for the validation of autonomous systems.

5.2.1 SESNA vs PRISSMA

Some specificities of the project can be interesting for the PRISSMA work:

- the project defines an operating perimeter for the experimentation on site. This perimeter was characterized to be able to reproduce a similar environment on virtual platform including infrastructure, weather and traffic conditions. This context characterization resembles in its definition to an Operational design domain.
- The project evaluates the risks and criticality (safety and cybersecurity issues) that present the shuttle operations by zones in order to be able to constraints its functionalities, when necessary, e.g. particular requirements and rules was defined for the crossing of intersections, roundabout, etc.
- Taking into account the presence or absence of an operator (controllability factor), the project also defines a set of recommendations, particularly on emergency and fallback maneuvers as similar to an OEDR analysis.

5.3 SVA

5.3.1 Stakeholders

As part of the Nouvelle France Industrielle (NFI) plan, the SVA "Simulation for Autonomous Vehicle Safety" project aims to respond to the challenge consisting in demonstrating the safety and harmlessness of embedded functions in autonomous vehicles.
The System X Research and Technology Institute is piloting the realization of this project in which partners are associated, RENAULT, PSA (Stellantis), Valeo, Continental, APSYS, SECTOR, LNE, CEA, Oktal, All4tech and Assystem.
This work took place over the period 2015-2018

5.3.2 The objectives of the project

The objective of the SVA project is to respond through digital simulation to the challenge of demonstrating the safety of an autonomous vehicle, in a context of validation. The complexity, generated by a large number of situations that the vehicle faces on the road, uncertainties of all kinds, linked to embedded technologies, make validations by tests in real conditions extremely time-consuming and above all costly, or even most of the time impossible in certain use cases.
An autonomous vehicle is a system of systems constantly interacting with its environment. :

- It captures this environment with the help of equipment reproducing 'images' interpreted by decision algorithms,
- It generates actions based on updating its "theater in which it moves" over time.

In this context, one of the major challenges of the SVA project is to be able to qualify the level of security of the perception and decision algorithms of the autonomous vehicle in an environment generating situations that are most of the time referenced in a deterministic way and may even often evoluate on a stochastic way. These algorithms can also be disrupted in their decision-making process by:

- Random internal failures or systematic errors, which can lead, in certain configurations, to the system to have unwanted and potentially dangerous behaviors.
- Environmental disturbances or interference that could lead the system to a bad decision and therefore to a dangerous action for the passengers of the autonomous vehicle and the other people and vehicles moving in its surrounding.

5.3.3 The SVA project objectives

a) Provide methods, techniques or tools likely to produce "safety arguments"

- Identification of the risks of predictable "unwanted" behavior
- Coverage of specific risks
- "Demonstration" (limit inaccessible as it is)
- Lack of existing normative / methodological repository

b) Provide methods, techniques or tools for design assistance and verification assistance

c) Provide methods, techniques or tools allowing manufacturers to constitute a "validation aid"

- On track tests
- On road tests
- Validation tests linked to modeling and "simulations"

5.3.4 The autonomous vehicle in its environment

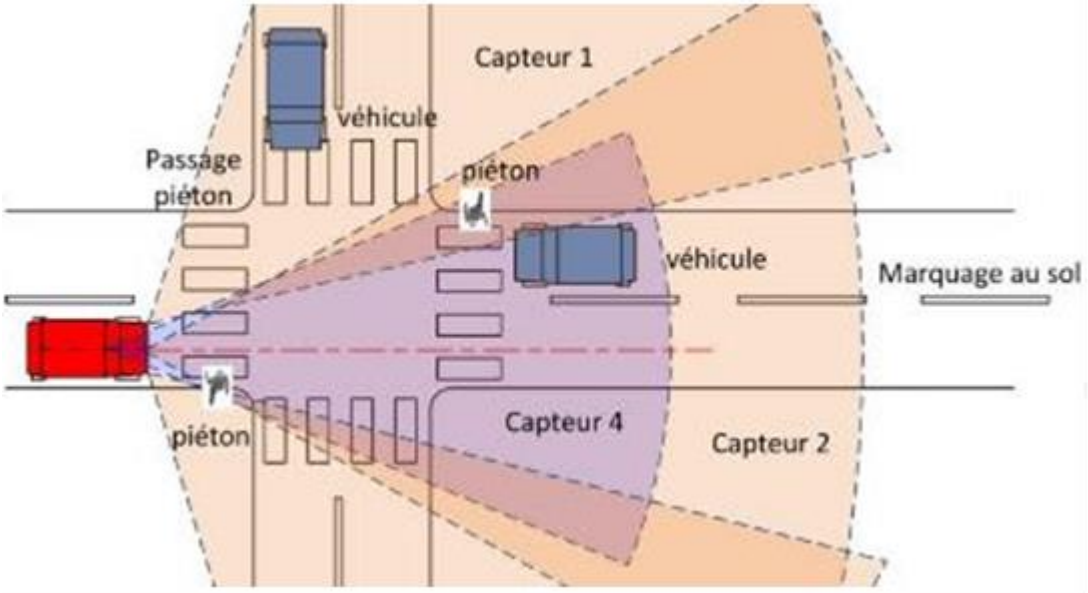


Figure 26: Autonomous environment representation

5.3.5 Lessons learned from the project

The process of developing the functions of autonomous vehicles (autonomous driving or autonomous mobility) requires new methodological responses to the scientific upheavals presented by the validation cycles of autonomous systems which are part of an "open" and "changing" environment. This concerns the applicable system engineering framework, and the definition of metrics or security performances that may be applied to them.

Technological innovations produce strong changes in the existing repositories of methods, techniques and associated standards, commonly accepted in the field of risk management. The first phase of the project highlights challenges of change regarding the concepts and approaches implemented so far in various fields such as aeronautics, rail, automotive and energy. It attempts to draw the outline of a new system engineering framework while integrating more specifically the characteristics of these technological innovations that break with the know-how and

practices deployed in most industrial fields. This new framework would aim to validate the safety of autonomous driving.

5.3.6 Validation by simulation

The validation by simulation that is developed in the SVA project makes it possible to:

- Avoid the prohibitive costs of operational test campaigns (infinite number of use cases)
- Bypass the obstacle of the "infinite universe of use cases" through technical possibilities of parallelization, "reduction", and sensitivity analyzes;
- Use the power and diversity of frameworks for the mathematical conceptualization of reality (Markov chains, algebraic topologies, etc.);
- "Take back control" of the problem of the infinite universe of use cases by associating it with the notion of selective and representative exploration, with scientific criteria of sampling relevance.

5.3.7 Conclusions and perspectives

The work carried out in SVA puts forward a whole reflection on a panoply of tools and methods related to the field of "validation by simulation and virtualization" in order to provide a multidisciplinary solution to the problem of engineering of safe design of autonomous systems. This reflexion goes forward the challenges of simulation and it obviously touches on the issue of validation benchmarks and security criteria in order to develop the acceptability of security risks, and the adaptation of regulatory frameworks and normative.

5.4 Database construction

Many OEMs and developers are developing their own databases of scenarios to test in simulation. Several initiatives have sought to create standardized systems, which bring databases together. Examples are PEGASUS ("Pegasus Method: An Overview," 2019), ASAM (ASAM Open SCENARIO," 26 July 2017), MUSICC (Multi User Scenario Catalogue for Connected Autonomous Vehicles," 2019) and the Midlands Future Mobility National Scenario database. The European Commission's joint research center has also proposed that a centralized scenario database should be established at an EU or international level. Data could then be collected from different sources and used by developers to validate their systems. This would prevent a siloed approach where the developer or approval authority used their own, perhaps relatively limited, scenario database.
We can also note that the PEGASUS project finds its equivalent in Japan with the SAKURA project.

For the simulation to play a key part in assessing safety;

1) One issue is how scenarios should be assessed. The MUSICC database, for example, proposes pass/fail scoring to assess the results of individual scenarios. As the project documentation acknowledges, some road behaviors are categorized easily as pass/fail in simulation (such as speeding or running a red light). Others are risk based and harder to score (such as the amount of distance to leave between cars in inclement weather).

2) If simulation alone is used, there is a risk that actual vehicle dynamics and subsystem interactions will not be modelled adequately.
3) Simulation can only validate against scenarios that are tested. There is always a risk that situations will arise after the vehicle has been deployed which were not covered by the simulation.

One challenge will be to include a sufficiently wide variety of scenarios that also accurately represents the intended ODD of an ADS. AVs should be tested in their dealings with all possible road users, including the full diversity of pedestrians, cycles, prams, pushchairs, wheelchairs, pets and horses. As Sustrans put it, the technology needs to respond to the diversity of bike types, with "tandems, recumbents, electrically-assisted bikes and children's bikes" all part of the fleet. Furthermore, the range of road users changes constantly.

The fear is that the smaller and more homogeneous the group responsible for collecting the scenarios, and the more remote that group is from the communities affected, the greater the chance that some scenarios could be overlooked. Where a scenario database is used in the assessment process, there should be some formal mechanisms for consulting on the range of scenarios included.

5.5 Cybersecurity related documents to AI eco system

This section summarizes several documents related to cybersecurity and artificial intelligence.

5.5.1 AI cybersecurity challenges

The following text is extracted mainly from AI CYBERSECURITY CHALLENGES Threat Landscape for Artificial Intelligence, ENISA, 2020, ISBN 978-92-9204-462-6 - DOI 10.2824/238222.This report made by ENISA presenting the Agency's active mapping of the AI cybersecurity ecosystem and its Threat Landscape, realized with the support of the Ad-Hoc Working Group on Artificial Intelligence Cybersecurity. The main highlights of the report include the following:

- Definition of the scope of AI in the context of cybersecurity following a lifecycle approach. Taking into account the different stages of the AI lifecycle from requirements analysis to deployment, the ecosystem of AI systems and applications is delineated.
- Identification of assets of the AI ecosystem as a fundamental step in pinpointing what needs to be protected and what could possibly go wrong in terms of security of the AI ecosystem.
- Mapping of the AI threat landscape by means of a detailed taxonomy. This serves as a baseline for the identification of potential vulnerabilities, eventually attack scenarios for specific use cases, and thus serve in forthcoming sectorial risk assessments and listing of proportionate security controls.
- Classification of threats for the different assets and in the context of the diverse AI lifecycle stages, also listing relevant threat actors. The impact of threats to different security properties is also highlighted.

The report is structure as follow:

- Chapter 2 presents a generic reference model for the lifecycle of AI systems, in order to set the foundation for asset and processes identification.
- Chapter 3 details the assets in the AI ecosystem based on the lifecycle stages defined in Chapter 2 and categorizes them in 6 groups.
- Chapter 4 introduces the threat taxonomy of AI systems, where relevant threats are presented and mapped to corresponding assets that were introduced in Chapter 3.
- Chapter 5 concludes the report by highlighting cybersecurity-related challenges to AI and proposes high-level recommendations.

5.5.1.1 AI Lifecycle

The lifecycle of an AI system includes several interdependent phases ranging from its design and development (including sub-phases such as requirement analysis, data collection, training, testing, integration), installation, deployment, operation, maintenance, and disposal. Given the complexity of AI (and in general information) systems, several models and methodologies have been defined to manage this complexity, especially during the design and development phases, such as waterfall, spiral, agile software development, rapid prototyping, and incremental. The AI lifecycle defines the phases that an organization should follow to take advantage of AI techniques and in particular of Machine Learning (ML) models to derive practical business value. For the purposes of this document, ML models are used to represent a mathematical transformation of the input data into a new result, e.g. use image input data to recognize faces. Conversely, algorithms are used to update the model parameters (training) or to discover patterns and relations in newly provided data and infer the result

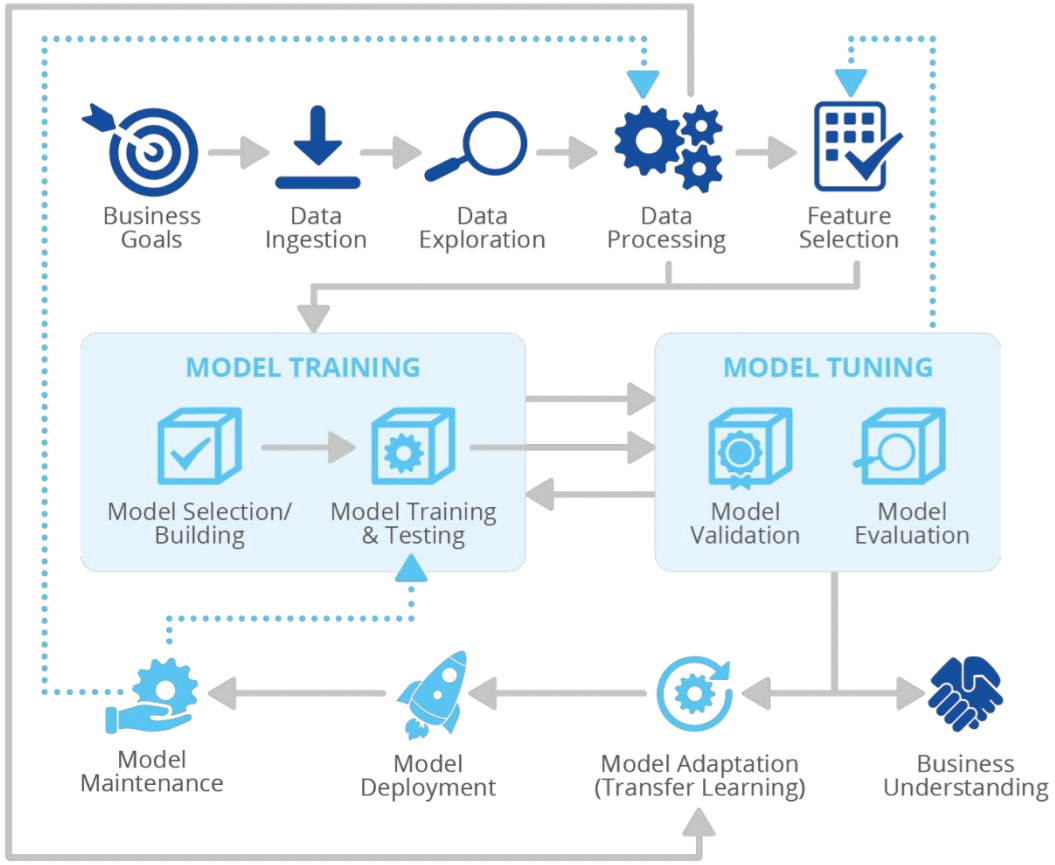


Figure 27: AI lifecycle generic reference model

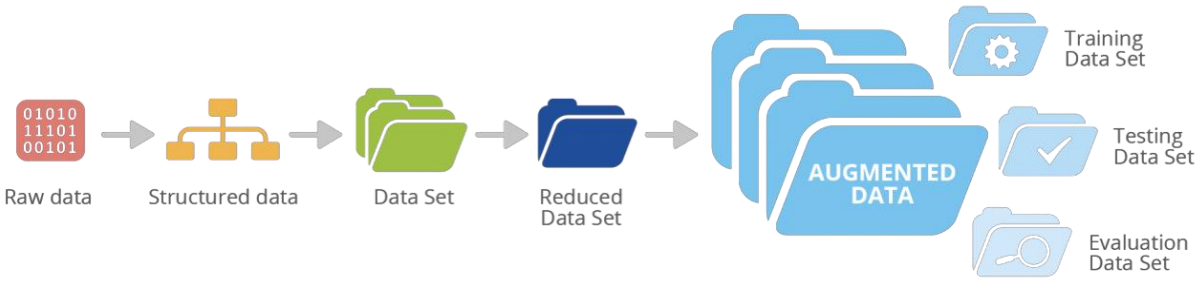


Figure 28: Transformation of data

5.5.1.2 AI Assets

A critical element in threat landscaping is identifying the categories of assets to which threats can be posed. Assets are defined as anything that has value to an individual or organization, and therefore requires protection. In the case of AI, assets are also those that are crucial to meet the needs for which they are being used.

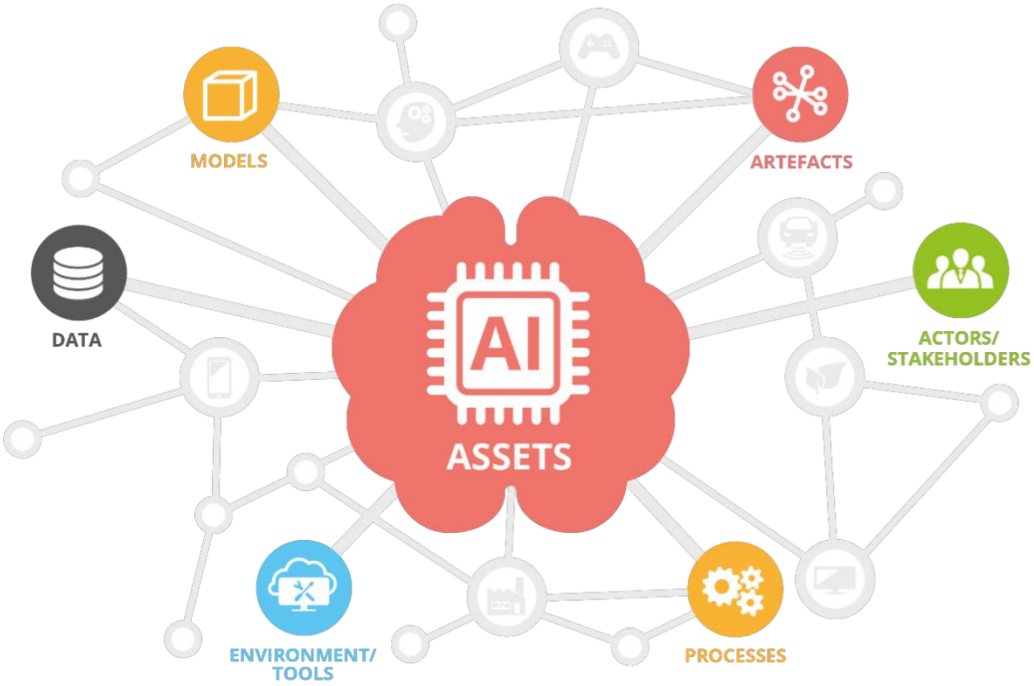


Figure 29: AI assets'categories

Figure 30: full taxonomy

5.5.1.3 AI threats

Some actors could be involved in this threat landscape. The chapter 4 of the document describes the different kinds of the threat actors. A description is done into the text and the following picture resumes the actor landscape

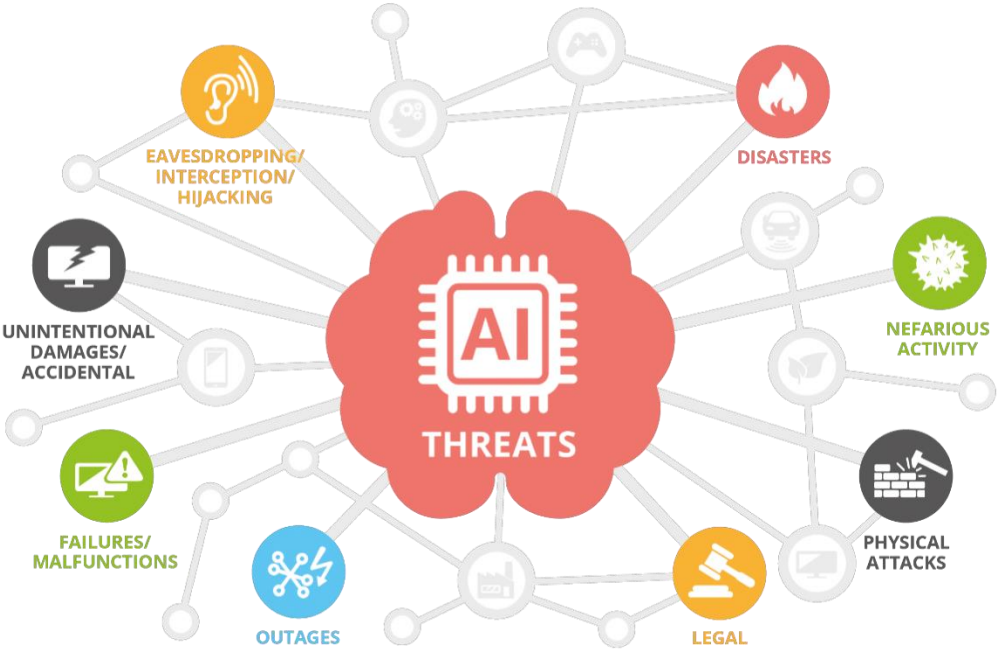


Figure 31: Threat taxonomy

Since a long time, ENISA has developed a taxonomy for the threats:

- **Nefarious activity/abuse (NAA):** "intended actions that target ICT systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target".
- **Eavesdropping/Interception/ Hijacking (EIH):** "actions aiming to listen, interrupt, or seize control of a third-party communication without consent".
- **Physical attacks (PA):** "actions which aim to destroy, expose, alter, disable, steal or gain unauthorized access to physical assets such as infrastructure, hardware, or interconnection".
- **Unintentional Damage (UD):** unintentional actions causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness".
- **Failures or malfunctions (FM):** "Partial or full insufficient functioning of an asset (hardware or software)".
- **Outages (OUT):** "unexpected disruptions of service or decrease in quality falling below a required level".
- **Disaster (DIS):** "a sudden accident or a natural catastrophe that causes great damage or loss of life".
- **Legal (LEG):** "legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law".

The next slide resumes all the threats currently evaluated.

Figure 32: General description of each threat

Annex B of the document give a general description of each threat. These information should be taken into account by WP2, 3 and 4.

5.5.2 Cybersecurity Challenges in the uptake of artificial intelligence in autonomous driving

This report from ENISA presents the technical aspects of AI in the automotive sector. The following text is mainly extracted from "*Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A. and Sanchez, I., Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving, EUR 30568 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-28646-2, doi:10.2760/551271, JRC122440*."

This includes an extended description of the areas in which AI plays a role, to ensure the proper implementation of cognitive capabilities inside automotive systems. Autonomous driving requires addressing a host of smaller subtasks (recognizing traffic signs or roads, detecting vehicles, estimating their speed, planning the path of the vehicle, etc.), each of them trivially performed by humans, but requiring carefully engineered AI systems to automatically address them. AI software components in an AV do not form a monolithic system, but rather rely on a complex combination of large and varied collections of data, themselves obtained by several types of sensors, and a rich set of AI methodologies, based on scientific works from statistics, mathematics, computing, and robotics. Starting from the high-level functions, an extended description of the landscape combining AI techniques, sensors, data types, and cognitive tasks highlights the sheer abundance of approaches and ideas that have made AV a reality. We claim that the understanding of these technical elements in the automotive context is essential to put into perspective their cybersecurity implications of these AI-based components. A mapping of automotive functions to AI techniques is provided to highlight the connections between automotive and scientific concepts, making direct links between automotive functionalities, intermediate subtasks, and ML techniques.

After this technical presentation, a state-of-the-art literature survey on security of AI in the automotive context discusses the main concepts behind the cybersecurity of AI for autonomous cars. Security of AI in general lies outside the scope of this report, and the interested reader is referred to the recently published ENISA AI Threat Landscape [1] to get the full picture on this matter. Instead, a focus is made specifically on adversarial machine learning that regroups a set of techniques that are currently the main approaches susceptible to compromise AI components of AVs. They allow a malicious actor to design specific attacks that could deceive AI systems while staying undetectable by human supervisors. Concretely, carefully crafted patterns can be disseminated in the environment to alter the decision-making process and induce unexpected behavior of the vehicle. Typical examples include adding paint on the road to misguide the navigation, or stickers on a stop sign to prevent its recognition. Despite the complexity to undertake these kinds of attacks, and in particular to make them undetectable by human eyes, the dire consequences in terms of safety should encourage car manufacturers to implement defense mechanisms to mitigate these type of AI risks. The description of these attacks, which may not necessarily require access to the internal system of the vehicle, is accompanied by real-world cases involving autonomous or semi-autonomous cars fooled by attackers. This is illustrated subsequently, both theoretically and experimentally, by realistic attack scenarios against the AI components of vehicles, extending the discussion to other types of vulnerabilities of AI.

In conclusion of this report, a set of challenges and recommendations is provided to improve AI security in AVs and mitigate potential threats and risks. This is motivated by the importance of relying on the pillars that have been at the core of cybersecurity methodologies developed

along the years for traditional software, while at the same time taking into account the particularities of AI systems. In light of the connections between AI and AVs brought forward in this report and their consequences in terms of security, the following recommendations are put forward.

The chapter 2 presents the High-level automotive functions:

• **Adaptive cruise control** (ACC) consists in adjusting the speed of the vehicle in order to maintain an optimal distance from vehicles ahead. ACC estimates the distance between vehicles and accelerate or decelerate to preserve the right distance.
• **Automatic Parking** (or parking assistance) systems consist in moving the vehicle from a traffic lane into a car park. This includes taking into account the markings on the road, the surroundings vehicles, and the space available, and generate a sequence of commands to perform the maneuver.
• **Automotive navigation** consists in finding directions to reach the desired destination, using position data provided by GNSS devices and the position of the vehicle in the perceived environment.
• **Blind spot / cross traffic / lane change assistance** consists in the detection of vehicles and pedestrians located on the side, behind and in front of the vehicle, e.g. when the vehicle turns in an intersection or when it changes lanes. Detection is performed usually using sensors located in different points of the car.
• **Collision avoidance (or forward collision warning) systems**, consist in detecting potential forward collisions, and monitoring the speed to avoid them. These systems typically estimate the location and the speed of forward vehicles, pedestrians, or objects blocking a road, and react proactively to situations where a collision might happen.
• **Automated lane keeping systems (ALKS)** consist in keeping the vehicle centered in its traffic lane, through steering. This includes the detection of lane markings, the estimation of the trajectory of the lane in possible challenging conditions, and the generation of actions to steer the vehicle.
• **Traffic sign recognition** consists in recognizing the traffic signs put on the road and more generally all traffic markings giving driving instructions, such as traffic lights, road markings or signs. This implies to detect from camera sensors various indicators based on shape, colors, symbols, and texts.
• **Environmental sound detection** consists in the detection and interpretation of environmental sounds that are relevant in a driving context, such as horn honking or sirens. This requires performing sound event detection in noisy situations.

Next a description of hardware and sensors is presented with a focus on how AI could be benefic for these sensors.

Chapter 3 presents some threats against AI system in the context of autonomous driving in the domains of computer vision, physical adversarial. Some attacks scenarios are described.
The picture below presents an example of the scenario attack against street sign recognition and lane detection.

AUTONOMOUS VEHICLE COMPROMISE

DESCRIPTION

Adversaries introduce physical perturbations on the road markings to deceive the model into perceiving wrong information about the environment. This includes alterations, placement of stickers, or projection of light on the painting of the road lanes or on road signs (stop signs, speed limit signs, etc.). These carefully crafted patterns lead to a misclassification of objects or symbols by the perception component, and subsequently to misbehaviours of the AVs.

IMPACT

Medium - High: The impact depends on the target markings, and the role that it plays in other autonomous driving functions. Misclassification of markings can easily generate safety issues, triggering misbehaviours in autonomous navigation functions endangering road users' safety and leading to driver, passenger, or pedestrian deaths.

EASE OF DETECTION	CASCADE EFFECT RISK
Easy - Medium - Hard: Depending on the nature of the attack, the alterations could be detected easily, or on the contrary remain undetected by human eyes before an accident occurs.	**Low:** The perturbation is local, and may affect only the cars passing by the modified marking.
ASSETS AFFECTED	**STAKEHOLDERS INVOLVED**
Markings recognition algorithms Sensors Vehicle functions	OEMs Road infrastructure

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The attacker first analyses the capabilities of the targeted versions of cameras and AI-based image classifier and designs an adversarial attack able to alter the outputs. This phase may require trying multiple perturbation patterns or display parameters. The attacker needs to perform some physical experimentation as well to ensure that the attack will succeed.
2. At a next step, the attacker performs the alteration of the targeted marking or traffic sign to cause misclassification by the AV.
3. Due to the added perturbation, targeted autonomous cars passing by the altered marking or traffic sign will erroneously classify it into the attacker's chosen class (e.g. interpret a stop sign as a speed limit sign) and react accordingly (e.g. reduce speed instead of stopping the vehicle).

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium: Sensor fooling attacks can go unnoticed. Once detected, modified markings or traffic signs can be reverted in hours.	Markings and traffic sign authentication Design of robust AI models Collaboration of vehicles

COUNTERMEASURES

1. Hardening against adversarial examples.
2. Use of hardware redundancy mechanisms.
3. Use of data redundancy mechanisms, such as multiple sensors.
4. Perform data validation, for instance by comparing sign information collected by sensor with information from digital maps stored in the vehicle.
5. Use V2X communication to receive read sign information.

Figure 33: Adversarial perturbation against image processing models for street sign recognition and lane detection

The conclusion chapter propose recommendations for autonomous driving. The main recommendation is about the evaluation of the AI system. This evaluation must be done during all the life cycle of the application.

5.5.3 Machine Learning and Cybersecurity – hype and reality

This document produced by CSET (Center for Security and Emerging Technology) presents where ML could be used for cybersecurity.

The document describes the different AI architectures: deep learning, reinforcement learning, GAN (Generator) and massive natural language models.

Next, the documents presents where AI could be used in Prevention, Detection, Response and recovery and finally active defense.

6 Conclusion

Methods of assessment are beginning to emerge and will develop in time. However, there are significant challenges involved in assessing the safety of the first generations of AVs. All the available assessment methods have both strengths and weaknesses, with no consensus on how to proceed.

Regulators play a significant role, both in specifying what must be in the safety case and in providing independent assessment. The assessment is essential, and this is especially true in light of the high-stakes, high-pressure environment of AV development. Beyond providing essential checks and balances on system safety, independent assessment can provide a way to share lessons learned without revealing proprietary design details.

The final key is feedback: safety is not a one-off assessment but an ongoing process, in which manufacturers and assessors are continually learning from experience.

From this review of possible methods, we can agree with that conclusion. Assessment methods are still developing, and best practice would suggest simulations, track tests and road tests are all required. These need to be carried out by the developer during the development process, with additional checks by the regulator at the end of the process. The exact combination should be evaluated constantly and will need to be adjusted in line with best practice as it emerges.

The approach describing the ODD and its implication in the validation process above is of undeniable interest. However, it is worth remembering that the approach that will be maintained in the rest of the work of the PRISSMA project will be the one presented in Deliverable 8.9, which is based on the most exhaustive vision possible of the existing literature on the ODD.

Another key aspect that deserves to be detailed further is the validation of scenario databases. Several works at the national level (France) but also on the VMAD side are in progress and we should see an evolution on this subject.

7 Glossary

ACEA	Association des Constructeurs Européens Automobile
ADS	Automated Driving System
Art.	Article
ARTS	Automated Road Transport System
CCAV	Centre for Connected and Autonomous Vehicles
EU	European Union
ODD	Operational Design Domain
OICA	Organisation Internationale des Constructeurs Automobile
PLD	EU Product Liability Directive 85/374/EEC of 25 July 1985
SAE	Society of Automotive Engineers
UN	United Nations
UNECE	United Nations Economic Commission for Europe
GRVA	Groupe de Rapporteurs Véhicules Autonomes
VMAD	Validation Method for Automated Driving
FRAV	Functional Requirements for Automated Vehicles
STPA	Systems Theoretic Process Analysis
STRA	Système de Transport Routier Automatisé
OEDR	Object and Event Detection and Response
FTA	Federal Transit Administration
FMEA	Failure Modes and Effects Analysis
SOTIF	Safety Of The Intended Functionality
LSAD	Low-Speed Automated Driving systems
UCA	Unsafe Control Actions
FMVSS	Federal Motor Vehicle Safety Standards
NHTSA	The National Highway Traffic Safety Administration
ANPRM	Advanced Notice of Proposed RuleMaking
JAMA	The Japan Automobile Manufacturers Association Inc.
ICV	Intelligent Connected Vehicle

8 References

[1] PFA Position paper - AD Safety WG - 2019-V1.0

[2] VMAD-05-12 AD safety validation - french views - Vdef, 2020

[3] L. Raffaelli & X. Rouah (2014), Model-Based Testing and Test Automation applied to Advanced Driver Assistance Systems Validation

[4] L. Raffaelli. IMPROVING ADAS VALIDATION WITH MBT. 3e user conference on Advanced Automated testing. Oct. 2015

[5] L. Raffaelli, F. Vallée, G. Fayolle, P. de Souza, X. Rouah, et al.. Facing ADAS validation complexity with usage oriented testing. ERTS 2016, Jan 2016, Toulouse, France. pp.13. ⟨hal-01277494⟩

[6] L. Raffaelli, G. Fayolle, F. Vallée. ADAS Reliability and Safety. 20ème Congrès de maîtrise des risques et de sûreté de fonctionnement, Institut pour la Maîtrise des Risques (IMdR), Oct 2016, Saint-Malo, France. pp.10. ffhal-01398428

[7] Federal Register / Vol. 85, No. 233 / Thursday, December 3, 2020 / Proposed Rules

[8] Federal Register / Vol. 86, No. 18 / Friday, January 29, 2021 / Proposed Rules

[9] National Highway Traffic Safety Administration, 49 CFR Part 571, [Docket No. NHTSA-2020-0106], RIN 2127-AM15, "Framework for Automated Driving System Safety"

[10] ERTRAC Working Group. (2021). New Mobility Services Roadmap.

[11] ERTRAC Working Group. (2021). Urban Mobility Resilience Roadmap.

[12] European Comission. (2020). White paper on artificial intelligence.

[13] European Comission. (2021). Harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts.

[14] European Comission. (2021). Uniform procedures and technical specifications for the type-approval of motor vehicles with regard to their automated driving system (ADS).

[15] Federal Ministry of Transport and Digital Infrastructure. (2020). Act amending the Road Traffic Legislation – Act on Autonomous Driving.

[16] MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE. (2021). Décret no 2021-873.

[17] Functional Requirements for Automated Vehicles (FRAV). (2021). Progress Report to GRVA. "FRAV-23-05-Rev.2.pdf"

[18] SMMT. (2020). The Law Commissions' final AV consultation: A regulatory framework for AVs.

[19] L3 Pilot Driving Automation, Deliverable D3.4 – Evaluation Plan, 2021

[20] OICA, Validation and Management Framework for Safety of Automated Driving, 2021

[21] TSO, Automated and Electric Vehicle Act, 2018

[22] OICA, ODD framework, 2021

[23] https://www.conventuslaw.com/report/china-national-administrative-rules-of-road/, 3 August, 2018

[24] Automated Driving Safety Framework, Japan Automobile Manufacturers Association, Inc. (JAMA), AD Safety Assurance Expert Group, October 2020

[25] Automated vehicles comprehensive plan, U.S. Department of Transportation, January 2021

[26] New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving (ADS) Safety, "VMAD-23-06-rev.1 NATM Guidelines Clean Version.docx"

9 Annex

9.1 Annex I – Core Set of Nominal Scenario for the Highway use-case (ODD Framework – OICA)

Function	Ego Vehicle Behavior	ORUs Behavior	Scenario
Driving behavior	Lane Keeping		Ego vehicle driving in lane at constant speed, ORUs starts in a lane adjacent and drives along the curve ahead of ego
			Ego vehicle drives on straight road, multiple speed limit signs provided on different lanes.
			Ego vehicle drives on lane with a lead vehicle.
		Stationary	Ego vehicle drives in lane that has an impassable within its lane object.
			Ego vehicle drives in lane that has an impassable object blocking the entire road.
			Ego vehicle drives in lane that has a stationary object that occupy part of the lane (passable)
		Accelerating / Decelerating / Stopping	Ego vehicle drives in lane (cruising or accelerating), following a lead vehicle that accelerates / decelerates / brakes suddenly (including stop and go)
			Ego vehicle approaching stopped lead vehicle in its lane of travel.
		Swerving	Ego vehicle drives in lane, with vehicle in adjacent lane swerving towards ego vehicle. Swerving does not result in crossing of a lane marking.
		Cut-in	Ego vehicle drives straight, vehicle in adjacent lane cut-in between ego and lead vehicle
			Ego vehicle drives straight, other vehicle merge in at highway entry.

			TBC ORU behavior (e.g. use of indicators)
		Cut-out	Ego vehicle drives straight, leading vehicle cut-out exposing decelerating / stationary vehicle in front
	Lane-change		Ego vehicle starts to perform a lane change, other vehicle in the target lane approaching from the rear / decelerating from front
			Ego vehicle performs a lane change into an occupied lane with another vehicle approaching from the rear / decelerating from front
			Ego vehicle performs a lane change to leave the highway, lead vehicle decelerating and occupying target lane
Faults / Failures			Ego vehicle is travelling at the speed limit. - EE fault is detected (e.g. single ADS sensor fault occurs) - A severe failure occurs (e.g. core ADS ECU failure)
			Vehicles drives on a highway and a sudden mechanical failure occurs.
Critical			Ego vehicle is travelling on road and encounters environmental conditions: 1) At the limit of the ODD (e.g. heavy rainfall, streetlight power outage)2) Outside of ODD (e.g. severe snow, storm)
Others			Ego vehicle travels on road with pedestrian(s): - That are crossing the lane of travel that ADS is in - That are walking along the edge of lane
			Ego vehicle encounters presence workers / law enforcement agents directing traffic

			Ego vehicle encounters presence of emergency/enforcement vehicles - With sirens and light signals ON - Without sirens and light signals ON
			Ego vehicle encounters presence of animals on the highway
			Ego vehicle encounters presence of faded or missing roadway markings

9.2 Annex II – Tools (ODD Framework – OICA)

ODD Framework Toolbox

Scenario Categorization	Natural Language scenarios description	Scenarios description	Scenario Database	Core Scenarios
ISO 34502	StiEF, WMG-SDL	ASAM OpenDRIVE, ASAM OpenSCENARIO, M-SDL, H-SDL, ADSL, WMG-SDL	Safety Pool, TNO, CATARC, SAKURA, *France*	NHTSA Test Cases, Safety Pool, ISO 34502, Japan, Foretellix, Germany, Netherlands/Singapore, Waymo, M-CITY
Assumptions	**Likelihood**	**ODD Taxonomy**	**Virtual Testing**	**Logical to Concrete**
IEEE P2846, Accident Data, SPMD	TNO, HEADSTART	PAS 1883, ISO 34503	CARLA, DriveSIM, LGSVL, PreScan, RFPro	Constrained random, pseudo random, AI/ML, Bayesian Optimization
Safety Analysis				
STPA, FTA, FMEA				

- A Number of tools are needed to support the ODD based framework. FRAV/VMAD framework should define what tools are needed but shouldn't specify which tool is most appropriate.
- Core scenario list may be Harmonized after review of existing tools.
- With more real world experience, and when ADS is to be regulated then specific tools may be harmonized where needed.

9.3 Annex III – Nominal, Critical and Failure Scenarios (ODD Framework – OICA)

Nominal Scenarios examples

ODD (Dynamic) Element		Driving Behaviour	Traffic Rule	Functional Requirement	Behaviour Competency	Assumption	Test Scenario	Pass/Fail Criteria
Bicycle		Riding in lane (Frontal)	Drivers will also need to use a minimum passing distance for bicycles of 1.5m in urban areas, and 2m out of town	The ADS should adapt its behaviour in line with safety risks	ADS should ensure relative velocity during passing manoeuver doesn't exceed [30]km/h	bicycle Vlong 4.3 [SD 0.57] (Avg) m/s	The ADS shall travel between [30-50]km/h on the centre line of the road. A cyclist shall travel in the same direction as the ADS between [10-20]km/h, [0.2-1]m away from the lane edge. Test scenarios that require lane crossing shall be conducted with/without oncoming traffic.	The relative speed between the cyclist and the ADS shall not exceed 30km/h
				The ADS should comply with road traffic rules	Shift in lane to pass by cyclist with 1.5m lateral distance			The passing distance between the cyclist and ADS is not less than 1.5m
				The ADS behaviour should not disrupt the flow of traffic	The ADS may cross the center lane marking to ensure the safe passing distance is not violated			The ADS may cross the center lane marking to ensure the safe passing distance is not violated
				The ADS should interact safely with other road users	The ADS shall activate the turn signal if the center lane marking is crossed			The ADS activates the turn signal if the center lane marking is crossed
Speed Sign		Lower speed limit (Frontal)	You must not exceed 70 mph (112 km/h), or the maximum speed limit permitted for your vehicle. If a lower speed limit is in force, either permanently or temporarily, at road works for example, you must not exceed the lower limit.	The ADS should comply with road traffic rules	The ADS should ensure the absolute velocity of the ego vehicle does not exceed the designated speed limit when passing the sign			The ADS shall not exceed the speed limit indicated by the traffic sign.
Speed Sign		Higher speed limit (Frontal)	You must not exceed 70 mph (112 km/h), or the maximum speed limit permitted for your vehicle. If a lower speed limit is in force, either permanently or temporarily, at road works for example, you must not exceed the lower limit.	The ADS should comply with road traffic rules	The ADS should ensure the absolute velocity of the ego vehicle does not exceed the designated speed limit when passing the sign			The ADS shall not exceed the speed limit indicated by the traffic sign.
				The ADS behaviour should not disrupt the flow of traffic	The ADS should attempt to travel at the speed limit unless it is not aligned with safety risks			
				The ADS should adapt its behaviour in line with safety risks	The ADS should travel at a speed that ensure that the entire length of the stopping distance is visible			
Heavy rain			In wet weather you should keep well back from the vehicle in front. This will increase your ability to see and plan ahead	The ADS should adapt its behaviour in line with safety risks	The ADS should increase the minimum headway behind the lead vehicle			
				The ADS should adapt its behaviour in line with safety risks	The ADS should travel at a speed that ensure that the entire length of the stopping distance is visible			

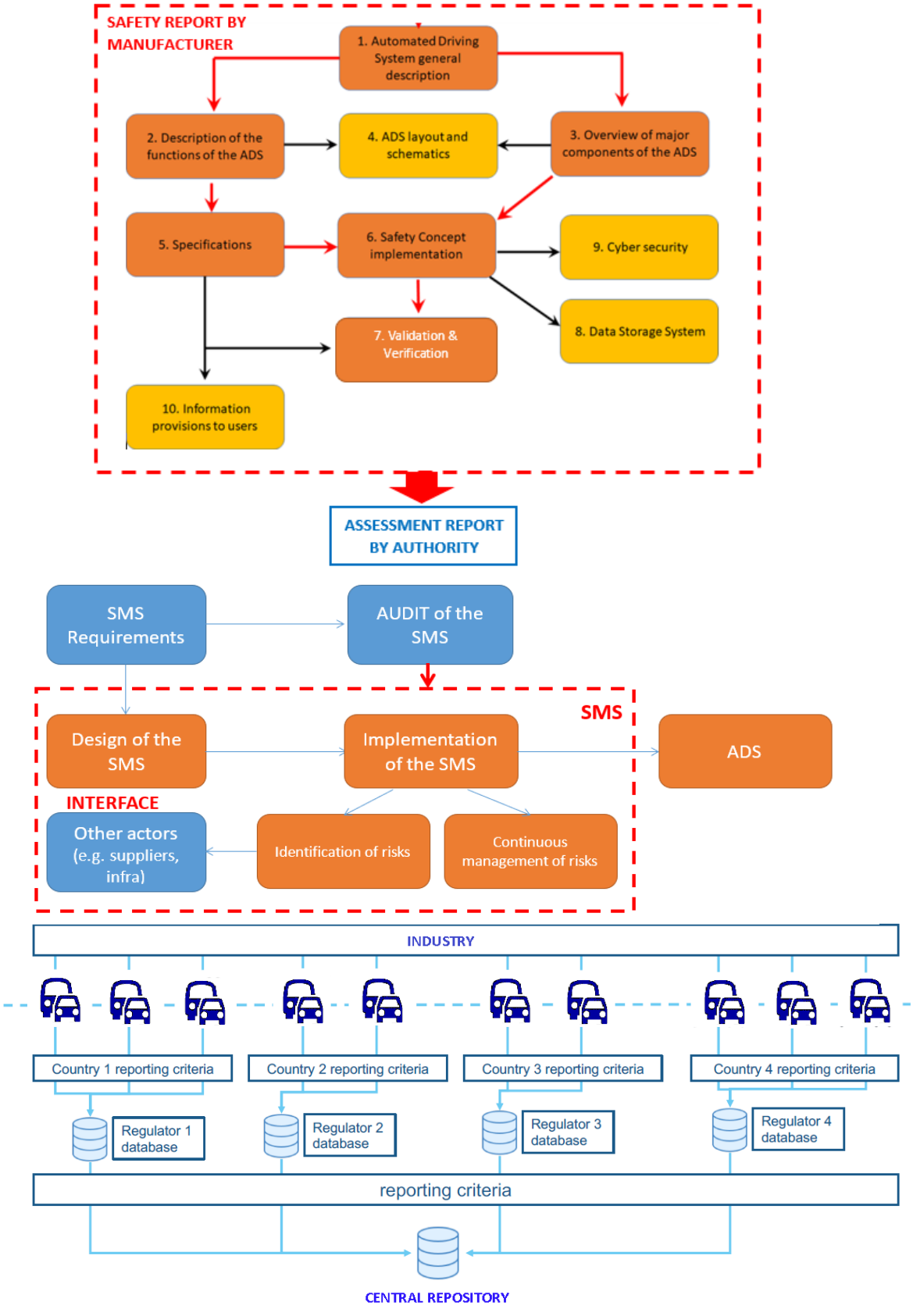
Critical Scenarios examples

Losses	Hazards	ODD	Control Structure	Control Actions	Unsafe Control Action	Loss Scenario	Casual Factors	Assumption	Test Behaviour	Test Scenario	Pass/Fail Criteria
Collision with objects outside the vehicle	Vehicle does not maintain safe distance from lead motor vehicle	Urban Environment Day and Night All weather conditions	Level 4 (no Driver) Sensors: LIDAR, RADAR, Camera Actuation: Brake, Accelerator, Steering no V2X	Request braking command	Braking demand is not requested	Object in vehicle trajectory is not detected	undetected / misclassified objects obscured object Incorrect sensor fusion results	lead Vehicle deceleration 7.0 [SD 2.3] (Dry) 4.4 [SD 1.0] (Wet) (Max Avg) m/s2	ADS is following behind a lead vehicle. Headway between the two vehicles is set by the ADS. Lead vehicle decelerates at the max assumed rates depending on the weather conditions	Lead vehicle decelerates to turn [Right / Left] or travel straight on at a [mini / large] roundabout	The ADS avoids a collision with the lead vehicle
						Object is not considered to be in the vehicle trajectory	Localisation issues leading to incorrect positioning of ego vehicle or object			Lead vehicle decelerates whilst shifting in lane to avoid [static object / other road user]	The ADS avoids a collision with the lead vehicle
					Braking demand is requested too late after conflict is unavoidable	Object in vehicle trajectory is not detected	undetected / misclassified objects obscured object Incorrect sensor fusion results			Lead vehicle decelerates whilst travelling on straight road with thick foliage and overhanging trees	The ADS avoids a collision with the lead vehicle
						Object is not considered to be in the vehicle trajectory	Localisation issues leading to incorrect positioning of ego vehicle or object				

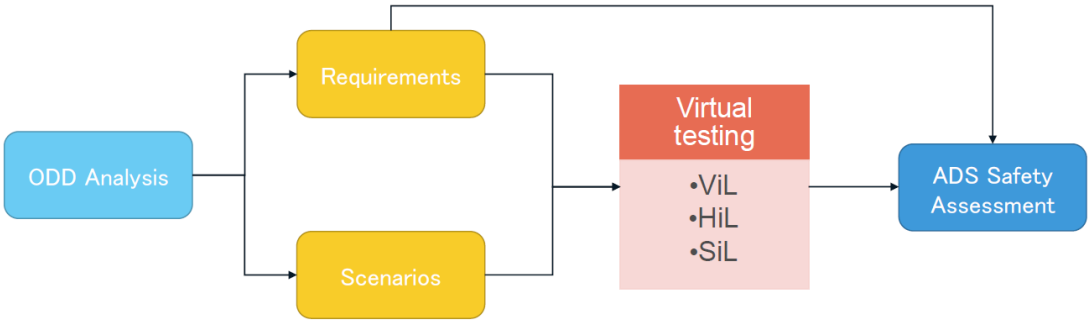
Failure Scenarios examples

Failure Type	Failure Mode	Potential Cause	Response	Functional Requirement	Assumption	Test Scenario	Pass/Fail Criteria
Perception	Fail to identify ODD boundary	Failure to detect ODD attribute e.g. Heavy Rain / Fog	Safely stop in lane of travel	The ADS shall be able to detect the ODD and predict when the ADS is about to leave the ODD	N/A	The ADS shall operate upto and beyond the predfined ODD. ODD characteristic to consider include geographical area and weather conditions	The ADS detects the ODD conditions are not met and issues a minimal risk manoeuver.
				When the system detects that it is difficult to continue in the automated driving mode, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre.			The minimum risk manoeuver should not cause the vehicle to decelerate greater than 4m/s2
				Other road users and occupants shall be informed that the vehicle is performing a minimum risk manoeuvre in accordance with applicable traffic rules (e.g. hazard lights, brake lights, turning indicators)			The ADS should activate the hazard lights through out the minimal risk manoeuver.
				The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules.			The ADS shall use the turn indicator when changing lanes.

9.4 Annex IV - Breakdown of the evaluation scheme proposed by the VMAD for the Audit/Assessment pillar



9.5 Annex V - Virtual testing vision from VMAD



9.6 Annex VI – Regulatory context for AI systems validation