Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

PFA | FILIÈRE
AUTOMOBILE
& MOBILITÉS

Direction générale des infrastructures, des transports et de la mer
Direction générale de l'énergie et du climat

Automated driving safety validation: proposals from the French Eco-system

Working concept paper

January 2020

Foreword :

Automated driving systems (ADS) with high levels of automation (i.e. where the driver is not the fallback) require to set commonly and widely accepted and applied high level safety rules and efficient validation framework to ensure safety. This is not only a matter of safety, but, furthermore, of acceptability. In this period when technologies maturity enable large-scale real-life deployments and promising market developments, it seems important that the industry has a clearer perspective on the future of validation, and, in particular, how public authorities intend to shape it.

Reflections on the future of autonomous driving safety validation have been very active recently, based on the general consensus that existing validation approaches have to be significantly modified. Academia, the industry, standardization and regulators have produced a significant stock of ideas and proposals. Several countries or groups of stakeholders have recently issued position papers. At the UN level, a dedicated group has been set up, co-chaired by Japan and The Netherlands, under Working Party on Automated/Autonomous and Connected Vehicles (WP29/GRVA/VMAD). At the EU level, the Commission has launched a working group on the future of approvals approaches, led by the Joint Research Center. Each contribution so far has brought important value added on this complex issue. This document has been drafted considering that it is worth pursuing in the general ***commonalities of concepts*** reached so far, in order to ***foster convergence*** among different approaches.

This document is a French contribution to on-going reflections on autonomous driving safety validation. This concept paper has been drafted by experts from the French directorates in charge of vehicle regulation and transports, in concertation with the French autonomous driving eco-system ("France véhicules autonomes"). Though this concertation is still on going, so that this document is still a draft, it provides some background to feed ongoing reflections on new validation approaches. As these reflections feed a work on progress, this document is not a formal nor definitive position from French authorities nor French industry, on regulatory options.

This document is the third French contribution on these issues. The first one (august 2017), focused on the need for a systemic regulatory approach (so called "horizontal regulation"[1]), proposed first concepts for validation approaches, and was presented at UN level (ITS/AD 12th session, 22 June 2017). The second proposed draft concepts for safety validation, and was presented at UN level (GRVA/VMAD session, 12 october 2019).

As regard to existing publications, this document intends to bring three specificities:

- It intends to be as much as possible ***ADS agnostic***, considering that the focus on motorway-individual-cars L3 and L4 cases might not be sufficiently forward looking; that public validation methods should be consistent for similar objects.
- It focuses on ***public expectations towards validation, and homologation/certification approaches***;
- It reflects common ***public-private*** discussions and thoughts from experts contributing to future regulations in the French automated driving eco-system.

After considering the context and the general framework for future homologation/certification approaches, this document proposes some high-level principles and some discussion on each validation pillar. It then focuses on expected items from OEM for homologation / certification. The conclusion opens the discussion on necessity of standardization activities.

[1] Cf. www.ecologique-solidaire.gouv.fr/sites/default/files/2017%2008%2010%20-%20Automated%20vehicle%20horizontal%20regulation%20-%20french%20proposed%20approach.pdf

Abstract

Sound, shared and transparent approaches for automated driving systems' safety validation are key to their development and acceptance. Validation will involve both public authorities and manufacturers. Validation should combine two main axes :

- a **process-centered** axis, to be mainly scrutinized by public authorities through **audit** of conception and validation methods ;
- a **performance-centered** axis, to be mainly scrutinized by public authorities through **tests**.

The efficient combination of these two axis strongly relies on the management of driving **scenarios** for the conception and validation of automated driving systems.

Audit should mainly focus on :

- description of systems' functions and design domain
- description and implementation of safety rules
- description and implementation of safety validation methods and tools (including simulation and tests) by the manufacturer, during the conception phase
- description and implementation of driving scenarios' management for conception, validation, including through in-use data collection

Tests should mainly focus on systems' performance in controlled environments (closed sites) and/or open environment (public roads). Tests should combine predefined standardized tests as well as more specific tests, based on a given use case's specific driving scenarios. Random approached deserve attention.

Closed site tests' relevant focus is manly on system performance verification, based on repeatable maneuvers potentially dangerous on open roads ("edge secnarios"). Closed site tests should also contribute to assess the relevance of simulation.

Open road tests' relevant focus is mainly on operational design domain (ODD) relevance and compliance, system performance assessment in "classical – non edge" scenarios, as well as interactions with other users (including human-system interfaces).

Some questions are only touched upon in this document and deserve more in-depth reflections, namely :

- lessons learnt from field experience
- validation of new releases, and its link with software update regulations
- validation of validation by simulation, and the need to adapt or upgrade existing regulations
- in-use performance monitoring and assessment
- automated driving systems where infrastructure and/or connectivity provides a significant part of safety : infrastructure safety validation and/or compliance assessment
- needs and challenges of focusing validation on specific subsystems (e.g. perception, recognition, positioning, mapping, connectivity, human-system interfaces)
- specific challenges for remote maneuvers' control.

Table des matières

Scope

This document intends to cover part of issues already put forward by other recent contributions[2], on autonomous driving safety and validation. The main focus of this document is on safety validation. However, in line with other contributions, it also addresses safety rules, though even more preliminary than validation principles. Schematically, this document covers :

Items	✓ *Covered - not : /*
AD System	
AD System description	✓
Operational Design Domain	✓
System architecture and redundancies	✓
Object and Event Detection and Response	✓
Qualitative Safety rules	✓
Risk Analysis	✓
AD features/functionalities	
Human machine interfaces	✓
System activation / deactivation / transition	✓
Remote monitoring and/or actuation	✓
Maneuvers specification and validation	✓
Minimum risk maneuvers	✓
Concept of safety envelop	✓
Validation Methods	
Management of validation scenarios	✓
Aftermarket monitoring and system update	✓
Quantitative criteria to stop validation	✓
Public Validation methods	
Role of Audit	✓
Relevance of simulations and tests	✓
Concept of "driving license"	✓
Not covered by this document (possibly covered by other regulation)	
Cybersecurity	/
Software update	
Privacy	/
Data recording / Accident data recording	/
Crashworthiness	/
Education, awareness, training	/
Responsibility	/

[2] Main references :

- EC : guidance for application of article 20 of vehicle safety Directive, 2019
- US-DOT : autonomous driving vision for safety & framework for ADS testable cases and scenarios, 2018
- Transport Canada : safety assessment for ADS in Canada, 2018
- Japan MLIT : autonomous driving safety guidelines, 2018
- NL-RDW : software driving license for autonomous cars, 2017
- OICA : future certification of ADS, 2018
- Rand Corporation, AV safety measurement, 2018
- Intel, Aptive et al : safety first for autonomous driving, 2019
- Mercedes and Bosch, reinventing safety : a joint approach to automated driving systems, 2018
- Mobileye : Responsibility-Sensitive Safety (RSS) : a mathematical model for autonomous vehicle safety & implementing in NHTSA pre-crash scenarios, 2018

Context

Automated driving systems development is focusing attention by regulators in most countries, considering that technologies' maturity enables a diversity of use-cases and services uptake in individual cars, shared and public transport, freight and logistics. The present turn of a decade might see the switch from limited scale experimentation to large-scale commercial services. Though the future development path is rather uncertain, due to technology challenges and uncertainties on willingness-to-pay and incorporation in mobility behaviors and policies, this path will certainly continue. However, uncertainty on development scenarios remains, and reachable use-cases in the next years are far from certain.

This uncertain-multi-path development should be kept in mind: this requires regulation to be flexible enough to cope with use-cases diversity. Tailor-made regulation for limited short-term use cases could lead to inefficiencies and discrepancies among different markets.

Industry has clearly acknowledged the importance of safety for automated driving development systems, which is the counterpart of highlighting expected safety benefits of autonomous driving compared to human driving. This priority is reinforced by convergent surveys and studies[3] showing that safety concerns are the main users' acceptability factor. National regulators have begun to put forward their concerns, concepts or proposals for autonomous driving safety in various strategic or guidance documents.

Significant work is undertaken, since the middle of the 2000s, to review validation approaches. At the industry level, the main stream has been the extension of conception-validation approaches applied to on-board electronics (ISO 26262 standard) to automated functionalities (safety of the intended functionalities - SOTIF). Other views have been put forward, such as the "safety envelop" concept. Academia has produced numbers of articles on this topic.

At this stage, the general consensus seems to be that existing validation approaches are not able to cope with automation challenges. At the core of automation is the revolutionary concept that a system takes the lead on driving over the human, which requires a change in concepts and approaches and a change in scale of risks to be considered. However, this necessary revolution in validation approaches still needs to take into account existing methods and accumulated validation knowledge and competencies, e.g. in testing.

New validation approaches will have to reconcile various possibly contradictory objectives:

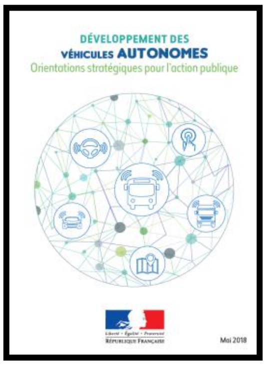
- Cover as many automated driving systems as possible, though different use cases bring their own specific safety challenges, among which some are very local, while other must be handled at the appropriate international level in order to avoid market fragmentation ;
- Be as forward-looking as possible, though use cases come to maturity incrementally, with different paths, and with uncertainty ;
- Cope with the complexity of these new systems, while remaining intelligible to the common user and citizen.

Transparency of validation approaches is key for acceptance and market uptake. Acceptance surveys[3] confirm the importance of this issue to citizens. Concepts for the evolution of validation approaches should not remain within technical fora, but be opened to public debate.

[3] Cf https://www.ecologique-solidaire.gouv.fr/vehicules-autonomes#e3

The French national strategy on autonomous driving[4], published in May 2018 and updated in April 2019, sets the following key priorities:

- Foster testing
- Adapt driving rules
- Adapt responsibility rules
- Upgrade safety validation / approval framework
- Assess needs and challenges of connectivity for AD
- Assess acceptance challenges
- Integrate AD in local mobility policies
- Assess and prepare skills adaptation


DÉVELOPPEMENT DES
VÉHICULES AUTONOMES
Orientations stratégiques pour l'action publique
Liberté • Égalité • Fraternité
République Française
Mai 2018

Under this strategy, the main actions undertaken cover the following axis:

- A revised testing authorization framework has been enacted to cover use cases where the driver is not due to have permanent control from inside the vehicle.
- The new Mobility Law (in Parliament) sets up the regulatory framework for responsibility and public validation of autonomous driving systems as well as vehicles' data exchange.
- Testing objectives have been set up and derived in a national program (cf. bellow).
- First guidance for tests' outcomes sharing have been published.
- France has taken the lead on a reflection on the Vienna Convention revision.
- A review of national driving code gaps has been undertaken.
- A national roundtable on acceptance has been set up with stakeholders; it will be extended to mobility policy challenges with local authorities.

1. *Eco-system organization*

France has set up a national program on automated driving in 2015, led by the industry, under the New Industrial Action Plan (Nouvelle France Industrielle), with three main priorities :

- foster dialogue among different sectors of the industry contributing to automated driving development,
- identify common interest technology blocks,
- identify regulatory gaps

This program has been organized in a matrix approach, i.e. by use cases (individual cars, public transport, freight and logistics) crossed with technological and regulatory issues (i.e. safety, validation, testing facilities, common technological blocks).

In 2018-2019, in parallel with the preparation of French national strategy, the program has been restructured, putting forward safety validation as the core task. The program has been renamed "France Véhicules Autonomes". Back-to-back groups have been set up with ministries on:

- safety validation
- responsibility
- driving code
- vehicles identification
- experimentation

France Vehicules Autonomes is an active member of the National Roundtable on acceptance.

[4] www.ecologique-solidaire.gouv.fr/sites/default/files/18029_D%C3%A9veloppement-VA_8p_EN_Pour%20BAT-3.pdf

General approach to safety validation

The approach to safety validation and homologation/certification should take into account the following main considerations:

- ***ADS description:*** Innovation and differentiation will come together with the ***diversification of automated driving system***, namely their operational design domain and functionalities. In this respect, international reflections should seek convergence on validation approaches, not on a particular ADS regulation**.** Said differently, a given ADS, as it is proposed by industry, should always be the starting point for applying validation methods and tools. The counterpart of this is to require precise ADS descriptions. In line with this, approaches should cover the highest levels of automation, including when the driver is to take control from outside the vehicle in certain circumstances and ADSs where safety is locally provided, to a large extent, by infrastructure, its equipment and connectivity.
- ***Capability-based approach :*** ADSs will be designed, manufactured and implemented under diverse design approaches, some being traditionally applied in the automobile industry, such as the V cycle-approach, some being more innovative, because classical V cycle is not sufficient and shall be completed by continuous integration, and software update even after sale. In this respect, the focus for homologation/certification should be on systems' capability.
- ***Responses, maneuvers_:*** In a capabilities-based approach, responses, and their sequences, should play a central role in ADSs description and validation approaches. The concept of response is key: driving, even automated, will remain a sequence of unitary responses that allow to go from point A to point B in sometimes hazardous driving conditions. Non-automated driving regulation (and namely, traffic rules and driving license examinations) are based on the concept of responses. Human drivers interact by observing and anticipating others' responses.
- ***Scenarios management:*** the main challenge of automated driving validation and homologation/certification (compared to traditional automobile validation), is to manage not only system failures but to be able to manage driving hazards (previously handled by the driver) in risk analysis. Industry has undertaken this new item in standardization, under the safety of intended functionalities (SOTIF) framework. Risk analysis, dependent of the ADS, is at the core of validation. Relevent scenarios to design & validate ADS should be managed (because of their huge number) to comply SOTIF and identify the residual risk. Scenario management should be the frame for validation architecture and the main window through which public authorities can scrutinize industry validation processes. SOTIF also requested an "acceptance criteria" which is a validation stop quantitative criteria, to ensure that the introduction of a highly automated vehicle on highways will not increase the risk level. It also ensures that the safety demonstration and its validation have a sufficient coverage.
- ***In use system monitoring and systems + validation improvement :*** another key challenge for safety, validation and homologation/certification is to collect and take into account new rare scenarios, in order to improve systems' safety and validation capabilities.

Validation will be a shared task between industry and authorities.

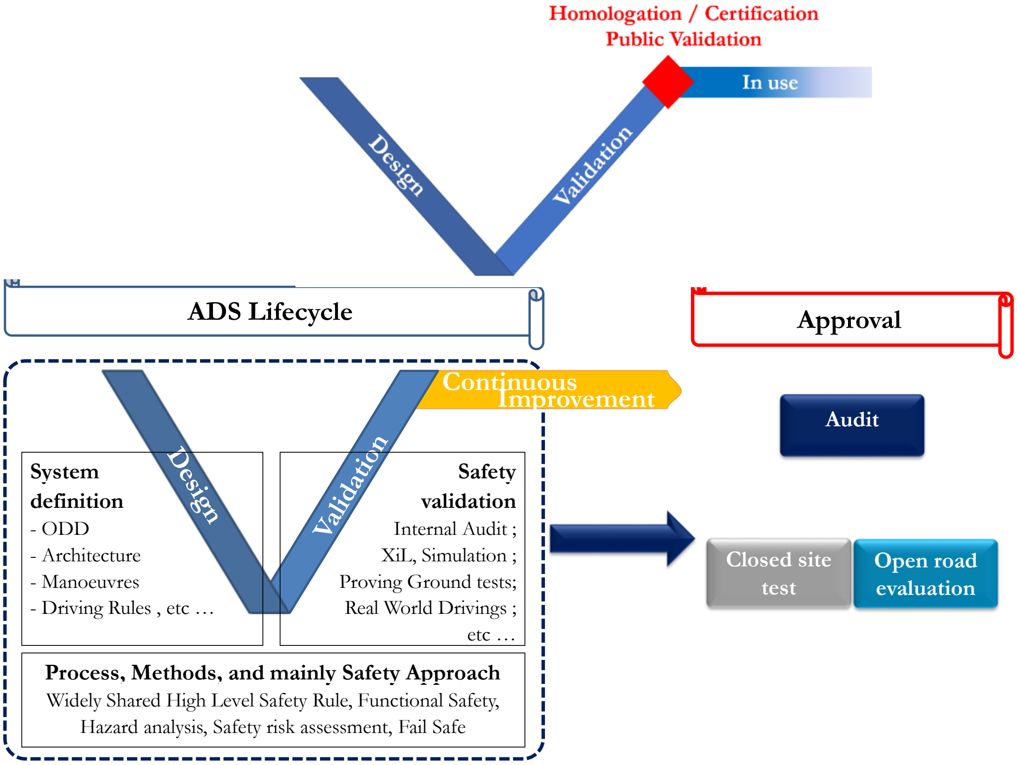
In this respect, ***the focus for public validation should be on systems' performance*** (output approach). This can be ***supplemented by validation by process design quality*** (input approach), but the performance-based approach should be predominant.

This approach does not underestimate the importance of safety-by-design, but stresses the importance of another angle for public validation, based on performances.

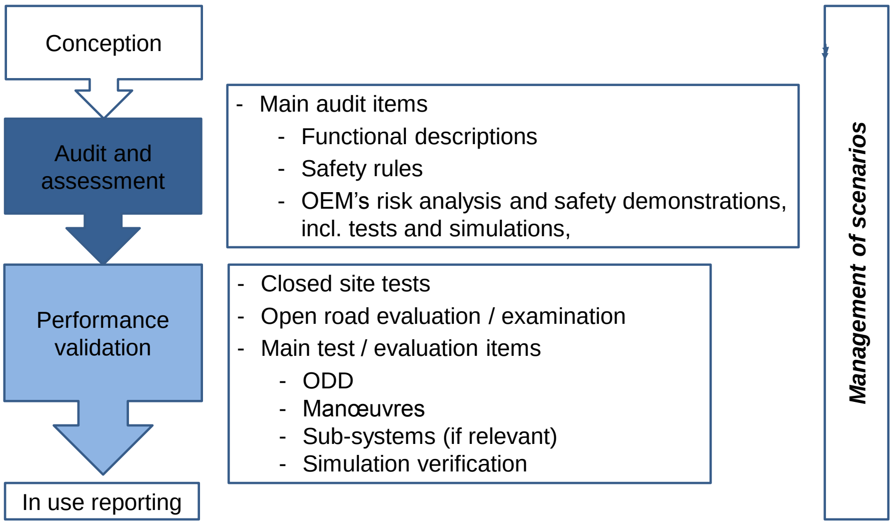
In a performance-based approach, ***manoeuvers or responses, and their sequences, should play a central role in uses cases description and validation approaches.***

Risk scenarios management should be the frame for validation architecture and an important angle through which public authorities can scrutinize industry validation processes.

Overall validation architecture



Overall approach including design, validation, and approval


Conception
Audit and assessment
Performance validation
In use reporting
- Main audit items
- Functional descriptions
- Safety rules
- OEM’s risk analysis and safety demonstrations, incl. tests and simulations,
- Closed site tests
- Open road evaluation / examination
- Main test / evaluation items
- ODD
- Manœuvres
- Sub-systems (if relevant)
- Simulation verification
Management of scenarios

Validation principles

Based on the previous preliminary considerations, the following principles should shape the design of new safety validation approaches:

- Principle # 1: Validation should handle a wide variety of use-cases (functions, ODDs, maneuvers)
- Principle # 2: Validation should verify that reasonably foreseeable risks, combining system failures and driving hazards, are identified and addressed, and their impacts are minimized
- Principle # 3 : Public validation should combine physical or simulated tests and audits in order to assess results (or performance) and processes, based on a sufficient knowledge of the system's design
    - Principle # 3.1: Validation by public authorities should focus on driving responses (manoeuvers) to systems failures and driving hazards and assess both :
        - critical maneuvers' safety, responding to edge scenarios
        - current maneuvers carefulness or roadmanship
    - Principle # 3.2: Physical tests should combine :
        - a standardized approach, for a limited set of common functions or maneuvers
        - a use-case-specific approach, based on risk analysis, including randomly
    - Principle # 3.3: Audits should be based on manageable and interpretable descriptions of :
        - ODDs
        - system architectures and description of safety-relevant functions
        - manoeuvers and their logical sequence
        - systems' and manoeuvers' overarching safety rules
        - scenario management, risk screening and scoring methods and relevant results, covering system failures and driving hazards scenarios
        - rationale for internal combination of different safety demonstration tools (e.g. tests, simulations with various Xs-in-the-loop)
        - safety demonstration methods, tools and facilities, with a focus on simulation tools' calibration.
        - behavior and perception studies
- Principle # 4: Validation may look at specific functional sub-systems, whenever they are safety-critical and suitable for replicable validation tools. This is presumably the case for HD mapping, human-machine interfaces, V2X connectivity and objects/event detection and recognition.
- Principle # 5: Transparency of managing risk scenarios for safety analysis is key to build a proper balance between internal validation processes and public validation scrutiny
- Principle # 6 : In-use data reporting should enrich common state of the art and public validation processes. Inter alia, public authorities should develop knowledge on critical driving situations, based on feedbacks by the industry.

Expectations towards audit

▪ *General considerations*

Generally speaking, audits should mainly address the following concerns :

- verify that processes for conception / development / risk analysis / safety demonstrations, are documented and, provided so, comply with internal design rules ;
- assess the relevance of internal design rules as regard to state of the art ;
- assess the ability of internal risk analysis and safety demonstration processes, to cover the largest scope of reasonably foreseeable risks.

Audits are not meant to assess performance of systems per se, which should be the role of tests (or simulations).

Performance validation on one hand and conception audit on the other should be articulated.

Generally speaking, self-assessment, external audit and external tests could be combined to proportionate validation efforts by industry and authorities according to the criticity level of risk at stake. Schematically, one could imagine that, from low level critical events, responses (via maneuvers) are assessed with a "completeness" criteria, i.e. ensuring that this type of event is identified properly and addressed by a response (maneuver). For the highest levels of criticity, the relevance and, furthermost, the safety of the response becomes the assessment criteria. For these responses (maneuvers), a reference description must be available to audit and test may be prescribed. In particular :

- audits should support a certain degree of "tailor-made" or "endogenous" testing strategies, based on use-case description and the corresponding risk analysis ;
- the combination of audits and tests should help to handle the difficult questions of national safety rules or "etiquette" : autonomous systems will have to comply to national traffic laws that may, to a certain extent, lead to (slightly or significantly) different design rules. In this context, national reception authorities will be tight to their national driving code in defining tests or to national "etiquette" to assess driving behavior on road or perception by other users. Audits should supplement this with the ability to verify that a given array of national rules or "etiquettes" has been included in maneuvers and ODD's design.

▪ *Candidate high level principles for audit*

- ➢ A safety management system shall be established, documented and implemented by the manufacturer.
- ➢ It shall include a clear process for : Safety by design, hazard and risk analysis, verification, validation safety demonstration and field monitoring.
- ➢ OEM shall document and demonstrate how they ensure the capability to manage safety during the lifecycle of the vehicle internally and externally.
- ➢ OEM process shall include independent internal audit to ensure that the process is implemented consistently throughout the different phases of product lifecycle.
- ➢ OEM shall ensure that relevant parts of the safety management scheme are implemented by suppliers and sub-contractors
- ➢ OEM shall have processes to monitor incident/accidents with their vehicles overtime and react appropriately .

- Possible fail criteriae :
    - process not documented,
    - no demonstration of an appropriate level of management
    - process not implemented in a consistent manner.

- ***ODD description***

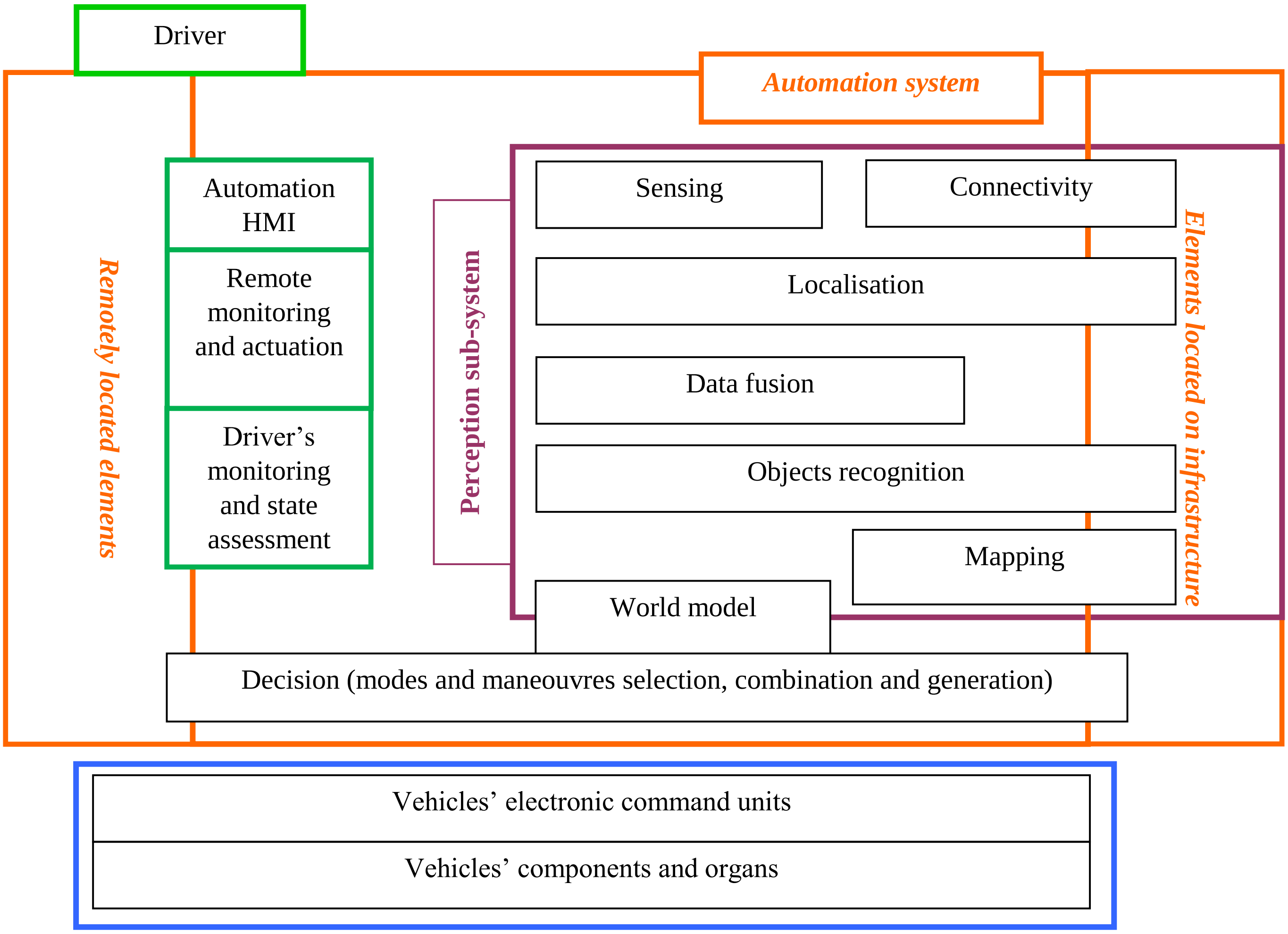
ODD description could take into account the following parameters:

- Type of infrastructure
- Hours / period
- Visibility conditions
- Surface conditions
- Contextual speed and traffic conditions
- Eligible lanes (position, min-max width, lane merges, incoming ramps, exits)
- Eligibility of specific sections or zones under autonomous mode (cf. above)

- ***System architecture's description***

System architecture could take into account the following sub-systems:

- Driver
- Human-machine interfaces
- Automation system per se (with its possible components located on infrastructure)
- Driving organs


Driver
Automation system
Remotely located elements
Automation HMI
Remote monitoring and actuation
Driver's monitoring and state assessment
Perception sub-system
Sensing
Connectivity
Localisation
Data fusion
Objects recognition
Mapping
World model
Elements located on infrastructure
Decision (modes and maneouvres selection, combination and generation)
Vehicles' electronic command units
Vehicles' components and organs

Maneuvers / responses description

Maneuvers description is a key input to validation.

Autonomous driving systems will develop specific maneuvers as responses to objects and events' detection. Maneuvers' features and performances, along with objects and events recognition, will be at the core of innovation and commercial differentiation within the industry. This foreseen diversity of maneuvers should be preserved in the validation process. Hence, the only criteria for validating a maneuver should, in theory, be its safety. This principle may, however, raise issues on the compatibility of a given maneuver with national traffic rules. Besides, this general principe should be balanced considering that should be understandable by the "common alter driver", especially emergency maneuvers, for which understandability challenges are even more important for safety.

Maneuvers should be considered with two different and complementary angles : a large-angle view should consider a maneuver characterized by the overall driving intention (e.g. keep in line, overtake, turn left, exit a motorway, park) ; a focused-angle should consider sub-maneuvers contribution to the overall driving intention (e.g decelerate, activate lights, pass lane, accelerate,…). The main focus for validation and interpretability assessment should be on the overall intended maneuver. However, some sub-maneuvers might have specific safety and interpretability challenges that should be identified as such and addressed by relevant validation or interpretability assessment tools.

Maneuvers description could take into account the following items (cf. box) :

- Activation conditions (including HMIs)
    - Proposal by the system (when in ODD) or not
    - Positioning conditions (e.g. in lane and distance to lead vehicle to activate)
    - If not in ODD, information of the driver when refusing to activate
    - If in ODD, time for the driver to accept the proposal and activate
- Transitions
    - Buffer-time for assessing ODD conditions
    - Alerts and transition requests for end of ODD (triggering conditions + modes)
    - Alerts and transition requests for system failures (triggering conditions + modes)
- Nominal positioning in nominal driving (cf. "etiquette behaviors" bellow)
    - Distance to lateral lanes (if customizable, ranges)
    - Time / distance to lead vehicle (if customizable, ranges)
    - Time for adaptation to nominal distance to lead vehicle
    - Modification of lateral positioning when passing or passed by a vehicle
        - Including for policy and emergency vehicles
    - Minimum buffer-time or inter-distance between vehicles for insertion in flow, at intersections, entries, turns or lane change (if customizable, ranges)
- Eligibility of specific sections or zones under autonomous mode :
    - lane merges
    - motorway exits
    - motorway entries
    - tolls
    - right turn
    - left turn
    - U turn
    - intersections crossing (with / without traffic signals)
    - roundabouts

    - pre-mapped work zones
    - incident management zones
    - pedestrian crossings
- Minimum risk and limp home manœuvres
    - Activation conditions (regarding end of ODD, system failures, driving hazards)
        - Including buffer-time after alerts and transition requests
    - Manoeuver's path
- Remote monitoring and actuation
    - Activation conditions (events, supervision capabilities, remote visibility)
        - Including on system's proposal versus on remote driver's initiative
    - Activable maneuvers

- ***User experience studies***

Autonomous systems' safety will highly depend on interactions with human beings, not only during activation / deactivation and transition phases, but also in traffic, while interacting with other (non autonomous) road users. Remote supervision will add-on specific issues.

Understandability of autonomous driving functionalities (ODDs, manoeuvers) is key to safety and acceptance. However, understandability is not an easy concept for validation, since unique measurements, standardized protocols and pass / fail criteriae are all but obvious.

Assessing how customers appropriate and use driving devices and functions is a long-time competence of the industry, in a highly innovative and competitive context.

Despite methodological difficulties and competition concerns, this domain deserves special attention by public validation authorities.

Main candidate topics for behavior and perception studies could be

- ODD understandability / interpretability
- Activation HMI functions
- Transition HMI functions
- AD external signaling interpretability (if available) by other drivers
- Nominal – current manoeuvers interpretability (etiquette) by other drivers

Additionally, some high-level safety rules might deserve to be challenged by potential users or citizens, being a structural acceptance factor.

Considering the variety of use-cases to which validation should apply, standardization of perception or behavior studies would be out of reach. This validation domain would rather be covered by description per use-case, that could covered:

- Function / manoeuver assessed
- Existing litterature / references
- Users' target
- Sampling
- Method (in particular : declared or naturalistic behaviors)
- Protocol
- Safety relevant results (and statistical confidence indicators if appropriate)

Among safety-critical perception issues, HMIs interpretability is central. Competitive and innovative differentiation observed so far might not cope long with safety concerns in situations where drivers (or remote supervisors) will have to react in a very short time to displayed complex information, and when HMI information will be the first step in the reconstitution of the driving environment to overtake control on the system. In this context, drivers, especially occasional drivers, cannot waste time to translate display modes to signs they immediately recognize and to which they can very quickly react. The shift from car ownership to car services will stress the importance of this issue.

Before some convergence on HMIs functions has been reached, each use-case HMI requires in-depth behavioral studies (in simulators or in open driving) which results can be audited. In the medium term, convergence on HMIs functions will partly shift this validation burden from use cases to HMIs component. This would allow some standardized tests on drivers' perception, applied to pre-defined situations and events in pre-defined driving scenarios and driver's pre-event attitude. Validation complements would be brought by other validation tools quoted above, namely entire sequence of manoeuvers in closed sites or open roads.

Expectations towards tests

Tests and simulations should assess the ability of autonomous driving systems or sub-systems to perform safely in representative driving conditions. Based on scenarios analysis, validation approaches should combine different tools:

- Simulation ↔ Closed sites tests ↔ Open road tests
    - which could be : use-case agnostic or use-case specific or endogenous
        - and : pre-defined or randomized

Usually, simulation is more relevant for assessing safety for separate sub-systems and addressing hypercritical situations or events (derived from edge scenario parameters). Simulation would be of particular interest in assessing sub-systems failures mitigation and/or fail-safe maneuvers.

Tests would probably be more appropriate for overall system performance, addressing most likely critical situations or events. Closed sites tests would probably be more appropriate for unitary maneuvers (such as automatic braking, lane keeping) in simple (though critical) driving situations (such as one object outside the ego-vehicle). Open road tests would, generally speaking, be more appropriate to assess a sequence of maneuvers, and their interactions with a diversity of other road users.

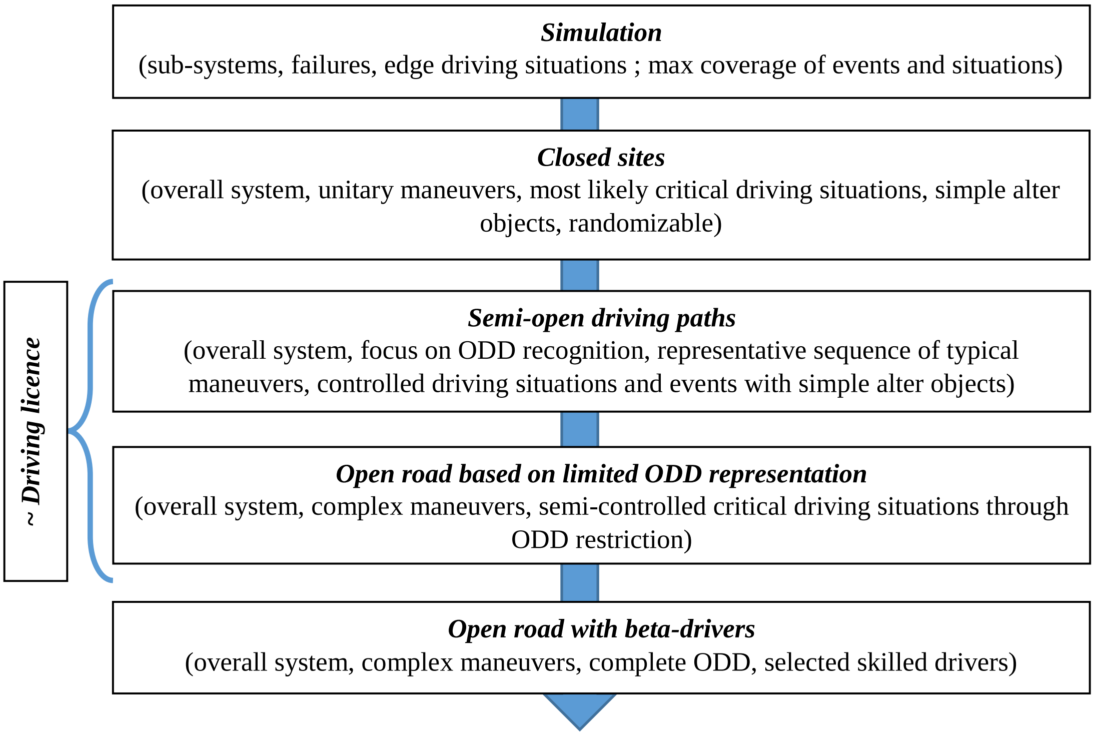
Some validation tools (either through simulation or tests) could address unitary maneuvers that prove to be common (such as automatic breaking, lane keeping) to all use-cases, which would naturally lead to standardized protocols. Some other maneuvers might deserve to have standardized protocols, if they prove to be common among use cases. Some minimum risk maneuvers might enter this category, though it is likely that minimum risk maneuvers will, in early development phases, differentiate manufacturers and, hence, require ad'hoc use-case-specific tests (namely, on closed sites).

Use-case-specific tests would probably play an increasing role to assess ODD recognition and acknowledgement (including corresponding transitions). Besides, use-case-specific tests could be necessary to assess a system's capabilities to perform common maneuvers within its ODD).

Standardizing these tests is an open question : it would require to set a common decomposition of maneuvers, which could be for example: change lane (left, right), overtake, pass a turnabout, pass different types of intersection (e.g. with or without traffic signals), pass a pedestrian crossing, make a right turn, make a left turn, make a U-turn, pass an object on lane (dimensions to be defined), pass a merging lane, enter or/and exit a lane from/to a different configuration (initial – target speeds * angle).

At this stage, it seems that standardizing such tests would be out of reach, due to numerous combination of maneuvers, driving situations and events. This might re-inforce the interest of open road testing, with semi-standardized manoeuvers (cf. list above) but no control on driving situations and events (as would a driver's license examination do). However, acceptance of this validation approach is questionable; especially in terms of situations coverage, so that a necessary step could be closed-sites tests, based on semi-standardized manoeuvers (cf. list above) and simple controllable driving situations and events (e.g. first with no surrounding / incoming / lateral traffic ; then with one max two objects outside the ego vehicle). Another option would be to locate tests on semi-open roads, i.e. where driving environment is real (infrastructure, signs, visibility) but moving and fix objects are artificial and controlled. Another possibility to explore would be, for a given use-case, to gradually expand the ODD in which it is tested, from the presumed safest parts of the ODD. Tests on open roads with skilled drivers would allow some feedback on non-safety-critical issues, e.g. on etiquette and reactions from other road users.

Randomization of tests could be an efficient tool to ensure a large coverage of situations in systems' performance. The need for randomization is particularly important for standardized use-case-agnostic closed-sites tests should concentrate on unitary maneuvers (e.g. emergency braking, under different visibility, position, angles and relative speeds; or lane keeping, under different visibility and bend situations).



Simulation
(sub-systems, failures, edge driving situations ; max coverage of events and situations)

Closed sites
(overall system, unitary maneuvers, most likely critical driving situations, simple alter objects, randomizable)

Semi-open driving paths
(overall system, focus on ODD recognition, representative sequence of typical maneuvers, controlled driving situations and events with simple alter objects)

Open road based on limited ODD representation
(overall system, complex maneuvers, semi-controlled critical driving situations through ODD restriction)

Open road with beta-drivers
(overall system, complex maneuvers, complete ODD, selected skilled drivers)

Challenges for specific subsystems

- ***Perception and recognition***

Objects and events perception and recognition functions are the basis of all automated vehicles. These systems should be able to detect and recognize objects (road equipment, road signs, marks but also other vehicles, pedestrians, animals, lost objects…) and events (e.g. lead vehicle braking, other vehicles changing lanes…) in different weather conditions.

The need, from public authorities, to validate perception and recognition sub-functions per se is not straight-forward : validating these sub-functions per se would go against the general performance-oriented approach. On the other hand, it is clear that this sub-function, along with localization, mapping and, for some use-cases, connectivity, is a core sub-functions. Besides, internal conception and assessment processes within manufacturers, and with their sub-contarctors, stress attention on this critical sub-function. There might hence be some rationale to open a dedicated validation focus on objects and events perception and recognition, as a pre-requisite to the validation of systems' responses (i.e. maneuvers). If relevant, the validation approach could, for instance, use a list of predefined objects and events and a list of events related to nominal maneuvers and critical maneuvers that the system has to be able to recognize.

One of the goal of the subsystem validation should be to check the ability of the system to recognize representative objects and events in representative weather conditions of the ODD, in order to ensure reliability of the perception/recognition functions.

Besides, these systems use often machine learning algorithms based on large datasets. Several concerns appear related to validation :

- Limited extent of datasets can introduce limitations for the use of algorithms, as systems won't be able to recognize an object/event whose structure is totally different from those contained in the dataset (the case of "black swans" is often given as an example);
- Machine learning needs labelled data : the process of data labelling can introduce wrong labels and, therefore, wrong algorithms outputs;
- As machine learning algorithms uses a large number of parameters, this can lead to fragility of the algorithm : for instance, two very similar images can be interpreted in two very different ways;
- Algorithms used are often probabilistics, raising questions for the safety validation.
- The fact that the learning process for the specific operation location of the vehicle may be continuous has to be taken into account in the validation method.

- ***Mapping and positioning.***

Whatever the use cases combined with their field of use, vehicle's localization shall be considered as a transverse methodical block in so far as its accuracy is a key indicator of the vehicle's behavior relatively to its environment. Depending on use cases, the vehicle's position, trajectory and description of its environment, are primarily linked with either an absolute or a relative location in a reference system. The definition of localization, if not necessarily associated with mapping, is commensurate with a three-dimensional modeling of a ground reality, which, according to use cases, may be used by automation system's algorithms as a decisive component of the methodological blocks pre-defined above:

Automated driving systems functions		Item concerned
Operational design domain	ODD recognition / acknowledgment	Matching between the location of the vehicle and ODD's digital modeling
Manoeuvers	Manoeuvers triggering conditions	Location of triggering events
	Unit manoeuvers (lane keeping, ACC)	Relocation on visual landmarks implemented in mapping
	Nominal manoeuvers (etiquette)	Validation of real trajectory
Sub-systems or functions	Mapping and positioning	Integrity of mapping, insurance quality for safety and regulation
	Perception and objects detection	Redundancy and relocation
	Road signs interpretation	Redundancy of regulatory information
Conception process	System architecture	Data governance and dissemination

For this purpose, the localization and HD mapping sub-system can be used to validate autonomous driving systems in accordance with the following complementary approaches (which will be tested within European and National experiments):

- Output approach by external and independent vehicle positioning control, based upon metrological and imaging technology, will allow the validation of i) the vehicle's positioning system ; ii) the behavior of the vehicle regarding a reference trajectory ; iii) the vehicle's geographic reference system
- Input approach by qualification of location mapping subsystems such as the integrity and accuracy of the cartography in specific localization use cases.

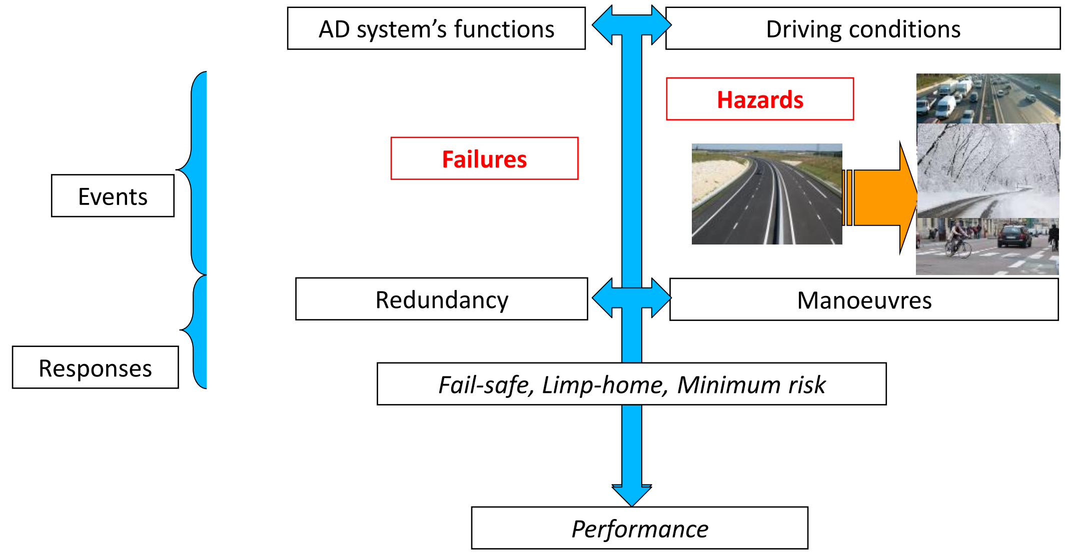
- ***HMI***

Automated systems, namely in the progressive path to full automation, create a more complex and diverse set of interactions between the vehicle, the driver and other road users. The use-case-centric approach underlying this document is intended to favor innovation in functionalities' design.

However, this approach might lead to an extremely complex set of requirements on drivers and other road users, in understandability of functions and interpretability of maneuvers. In this context, it is crucial that HMIs' understandability and interpretability by users would be a specific task of validation especially when ODDs will go outside motorways. Beyond this focus on validation, some standardization of functionalities might be necessary to balance the use-case-centric approach.

Expectations towards scenarios management

Driving scenarios are central in autonomous systems' validation approaches. They should enable an appropriate screening of events and failures, and their combination, that the vehicle might encounter in its driving environment during its driving policy in its ODD.



Graph 3 : combining risks in scenarios for a maneuvers-based approach

Box: basic concepts and definitions for validation-relevant driving scenario

A driving scenario can be described with the following main concepts and parameters:

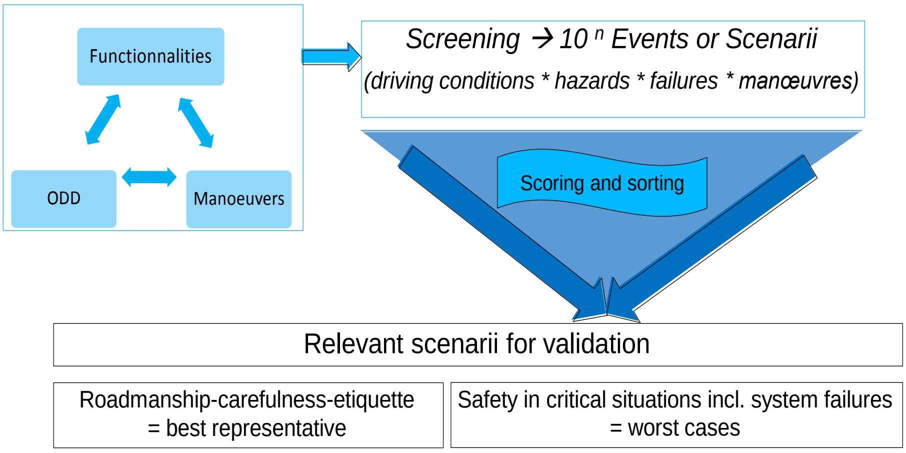
A scenario is an initial scene, to which adds a series of events and actions (responses) from the ego vehicle and alter users, leading to a final scene.

Scenes can mainly be described through the following typology of parameters:
- Static elements (lanes geometry, signs)
- Temporary elements (roadworks)
- Environment (light, visibility, rain/snow/wind/icy)
- Traffic elements
- Visibility masks

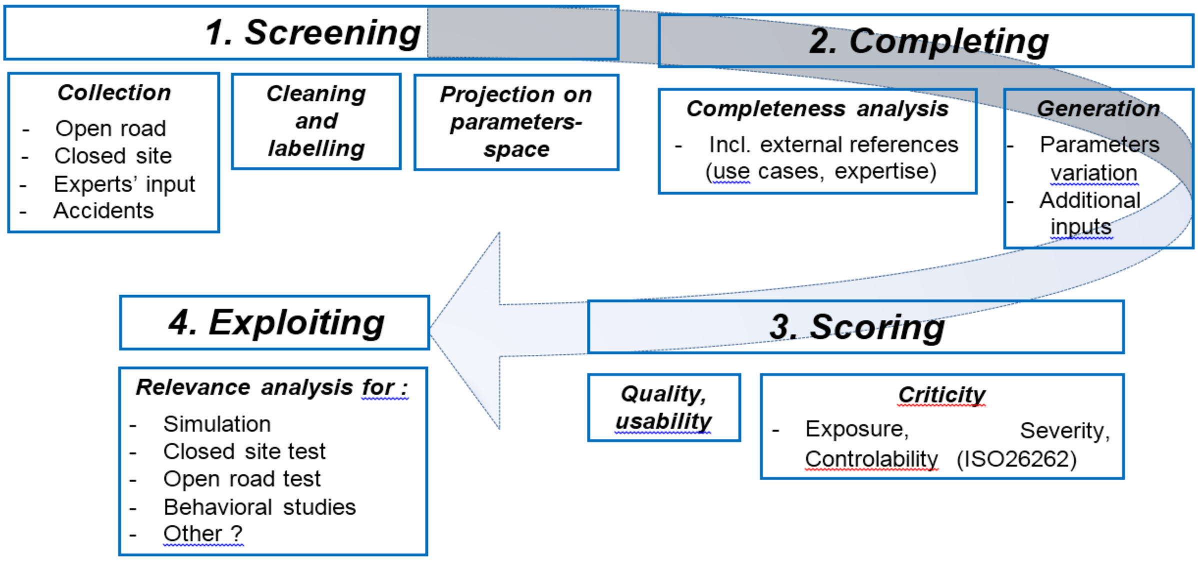
Events can be external of the ego vehicle or state modification of ego vehicle (e.g. failures

Source: SystemX

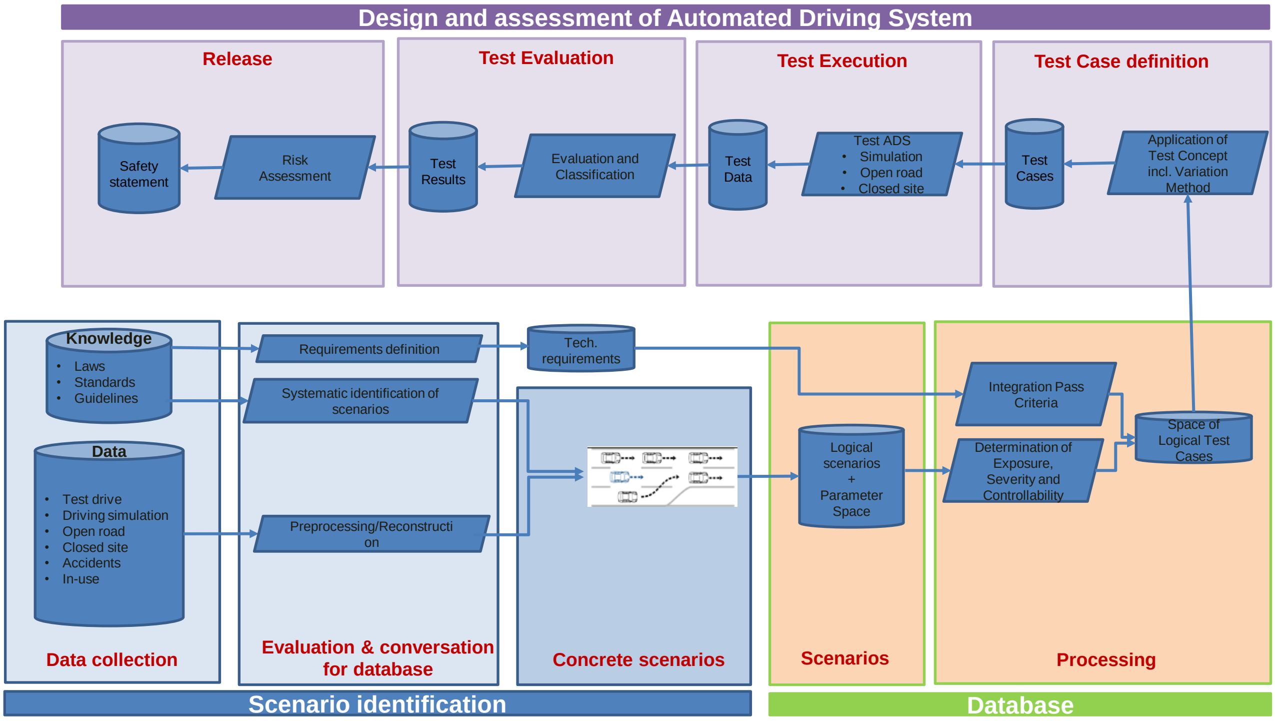
Scenario management has a key role to play in reducing the gap between the potentially infinite combination of driving conditions * events and responses (both from the ego vehicle and alter road users), and the capacity to address a limited number of scenario by the means of validation tools (either simulations or tests). Managing scenarios supports identification of both most likely and most critical scenarios. It helps reduce the probability of un-identified critical situations ("black-swans").


Functionnalities
ODD
Manoeuvers
Screening → 10 ⁿ Events or Scenarii
(driving conditions * hazards * failures * manœuvres)
Scoring and sorting
Relevant scenarii for validation
Roadmanship-carefulness-etiquette
= best representative
Safety in critical situations incl. system failures
= worst cases

Managing driving scenarios must be considered as a key process of autonomous driving systems' conception. This process' description and some of its outputs must be transparent to public output. Auditing this process should be part of public authority validation. This might require developing ad'hoc quality references or guidelines. The following graph proposes a schematic presentation of the main process steps for managing driving scenarios for validation.



The following graph presents a more detailed management cycle for driving scenarios, with a technical angle.



Regarding transparency to public authorities, important aspects of scenarios management are:

- Method applied for ***screening*** scenarios (e.g. sources used), in particular how driving hazards and sub-systems failures are combined
- Approaches applied for ***assessing completeness and, if necessary completing*** scenario database (e.g. driving scenarios in relevant ODDs for comparable systems ; external expertise ; scenario generation by parameters variation)
- Methods applied for scenario ***scoring*** (as regard to ISO26262 concept, the focus should be given to quotation of frequency and severity)
- Identified "***best representative***" and "***worst-case – edge***" scenarios[5]

[5] (as regard to ISO26262, best representative could cover scenarios which exposure ≥ E4 and severity ≥ S1 ; whereas worst case – edge could cover scenarios which severity ≥ S3 and exposure ≥ E2).

Relevance of validation building blocks and tools

The following table provides an overview of validation tools relevance for different building blocks listed in the previous chapters.

Automated driving systems functions		*Audit of description*	*Verification by simulation*	*Tests (closed sites)*	*Driving (open roads)*	*User experience studies*
Operational design domain	ODD definition	*				*
	ODD recognition / aknowledgment	*	*	*	*	
Manœuvres	Maneuvers / responses logigram	*			*	*
	Maneuvers / responses triggering conditions	*	*	*		
	Elementary maneuvers (lane keeping, ACC)	*	*	*		
	Nominal maneuvers (etiquette)	*			*	*
	Critical, Minimum risk, Fail Safe, Limp Home manoeuvers / responses	*	*	*		
Sub-systems or functions	Human machine interfaces	*		*	*	*
	Supervision, remote monitoring	*	*	*		*
	Mapping and positioning	*	*	*	*	
	Perception and objects detection	*	*	*		
	Road signs interpretation	*	*	*	*	
	Connectivity	*	*	*		
Conception and safety demonstration internal process	High level safety rules	*	*	*	*	*
	Redundancy through system architecture	*				
	Management of data (incl. driving scenarios) collected in-use	*				
	Management of validation tools	*				
	Test facilities and protocols	*				
	Simulation (tools accuracy + chain relevance)	*		*		

Overarching high-level safety rules

Overarching or high-level safety rules have a potential virtue of describing how an autonomous driving system is due to act, in simple, unambiguous and intelligible words. This is precious for validation. Those rules could cover the following domains:

- Autonomous driving activation conditions
    - including ODD acknowledgment (i.e. subsequent actions when out of ODD)
- Minimum risk maneuvers (MRM) activation conditions
- Safety envelope (longitudinal and lateral safe distances) (nominal maneuvers or MRM)
    - Including etiquette behaviors and possibilities for the driver to specify them
- Management of discrepancies in driving rules
    - e.g. international differences or handling of "fuzzy" driving rules
- Signaling to other road users
- Functional redundancies (e.g. for perception and positioning)
- Lessons learned and driving feedback management
- Drivers information on automated functions and ODD (pre-sale, pre-rent or pre-drive)

The following safety rules have been proposed by the French industry (within France Véhicules Autonomes) for the conception of their systems. They cover the highest levels of domains proposed above.

- ***Overarching rules***
    - ***Overall intention***: Automated Vehicle deployment shall improve the road safety
    - ***Safety qualitative objective***: The automated vehicle is free from unreasonable risk
    - ***High-level safety rules***: The vehicle shall comply with a set of high-level safety rules contributing to safety, whether or not their safety impact can be quantitatively assessed. A minimum set of high-level rules should be shared by all OEMs
    - ***Scenario-based approach***: design and verification/validation phases shall take into account relevant driving scenarios, including reasonably foreseeable misuses. A minimum set of these scenarios should be shared by all OEMs
    - ***Field experience*** shall be taken into account to continuously improve vehicle safety. Lessons learned from the field should be shared as far as possible
- ***High level rules***
    - ***Technical rules***

T-01	A single perception malfunction without failure should not induce a hazardous event. Consequently, the set of sensors used for the perception of a safety relevant environmental feature shall not be based on a single physical principle.
T-02	The vehicle design shall allow the driver to take over vehicle control at any time, according to the takeover procedure.
T-03	The driver shall be clearly informed that the vehicle is in AD mode or not.
T-04	In case of cohabitation on a single vehicle of several driving modes with different delegation levels, the necessary measures must be taken to control driver mode confusion risks (e.g. driver erroneously thinking he can stop to monitor vehicle and environment).
T-05	The driver shall be clearly informed of: o the vehicle behavior in AD mode and the limits of this behavior o his own responsibilities, the procedures to comply with (e.g. takeover procedure) and possible consequences if he does not comply.

T-06	In case of failure impacting safety in AD mode, an appropriate degradation concept shall be to inhibit AD mode until next vehicle switch off and vehicle proper operation has been verified either by self-diagnostic or by maintenance.

- **Operational Design Domain (ODD)**

ODD-01	The vehicle shall not be in AD mode out of its ODD

- **Autonomous driving (AD) mode**

DRV-01	The vehicle shall manage risks according to the following rules: o Vehicle shall not create accident by its own o Vehicle shall be robust, as far as reasonably possible, to risks caused by others o Vehicle shall comply with applicable driving rules (including those applicable to human drivers) unless it is the only way to avoid an accident This rule shall be fulfilled: o wherever the vehicle is driving (e.g. country, road, ...) o whenever the vehicle is driving (e.g. despite dynamic lane assignment; time dependent rule, introduction of a new type of traffic sign; rule change ...)
DRV-02	The vehicle behavior shall be, as far as possible, foreseeable by surrounding roads users (e.g. no lane change without prior turn indicator activation, no incautious lane change, foreseeable behavior while approaching a lane merge,...)
DRV-03	The vehicle shall maintain with the preceding vehicle a safety distance, according to the treatment of relevant scenarios.
DRV-04	After detection of a first significant shock while driving (e.g. frontal collision with airbags triggering or lateral collision during an insertion), the vehicle shall: o inhibit AD mode reactivation until proper operation has been verified, o perform predefined MRM in the best possible way, according to vehicle operational status and current situation Vehicle could also, simultaneously, request the driver to takeover vehicle control if vehicle and current situation are sufficiently controllable by the driver.

- **Transitions to/from autonomous driving mode**

TR-01	A deliberate driver action is required to activate AD mode.
TR-02	The driver actions to takeover shall be identical in both following cases: o the driver takes over from his/her own (without prior system request), o the system request the driver to takeover.
TR-03	When the driver takes over vehicle control on her/his own (without prior system request), the vehicle shall not disturb the driver takeover by an inappropriate action (e.g. by switching headlamps off, at night).
TR-04	When the driver takes over after a system request, the system shall give back the control to the driver with a vehicle configuration maximizing driver controllability (e.g. wipers ON in case of rain, headlamps ON by night).
TR-05	If the driver does not takeover vehicle control after a system request, the system shall start execution of a MRM. If the driver still does not takeover during the MRM, the vehicle will be stopped (refer to MRM requirements).
TR-06	The AD mode deactivation (end of vehicle longitudinal and lateral control) shall only be performed when system has verified that the driver has taken over vehicle control. This verification shall at least include a criterion on vehicle lateral control (except if the vehicle is already stopped).
TR-07	In AD mode, if situation would be difficult to control by the driver (taking into account vehicle technical status and urgency level) the vehicle: • shall manage the situation without requesting the driver to takeover, • shall inform the driver.

TR-08	“Non Driving activities” allowed in AD mode shall be consistent with the available delay for driver takeover after a system request. The driver has to be informed that he must be at any time in a situation, which enables him to answer to the requests of the system within the requested time period..
TR-09	“Non Driving activities” allowed in AD mode and available through vehicle systems shall be: o only available in AD mode, o interrupted, with a specific HMI, when the vehicle requests the driver to takeover or when the driver takes the control on her/his own.

- **Minimum risk manœuvres (MRM)**

MRM-01	For an automated function, which consists to operate at moderate speed, in dense traffic, on highway with a driver on-board, a possible MRM is to slow down the vehicle and stop it in its lane.
MRM-02	During whole MRM, driver can takeover in usual ways (refer to TR requirements).
MRM-03	In MRM phasis, when the vehicle is stopped, it shall signals itself to other drivers by flashing hazard (or stop) lights.
MRM-04	At the end of the MRM: o for a short period of time (typically 15 s), vehicle is maintained standing still without driver action (e.g. despite a slope) and driver can takeover in the usual way (refer to TR requirements) o after this period or if driver decide to immobilize the vehicle: • vehicle is definitively immobilized (Parking brake AND Gearbox N or P) OR (Gear on P) • AD mode is deactivated

- ***Catalogue of scenarios***

SC-01	The OEMs shall set up a common process to create and maintain a common catalog of scenario, including misuses, to be used for safety argumentation during design and verification/validation phases the catalog will be enriched continuously. This set up shall be made in compliance with laws (e.g. competitive laws)

- ***Market feedback and after sales approach***

AS-01	The OEM shall set up internally, a process to collect, analyze and treat incidents/accidents faced by the customers, and if necessary, update the vehicles.
AS-02	The OEMs shall share the lessons learnt from field experience, including safety- related events occurring in real life vehicle use, in order to enrich a common scenario catalog (in compliance with laws - e.g. competitive laws)

Some implications for standardization priorities

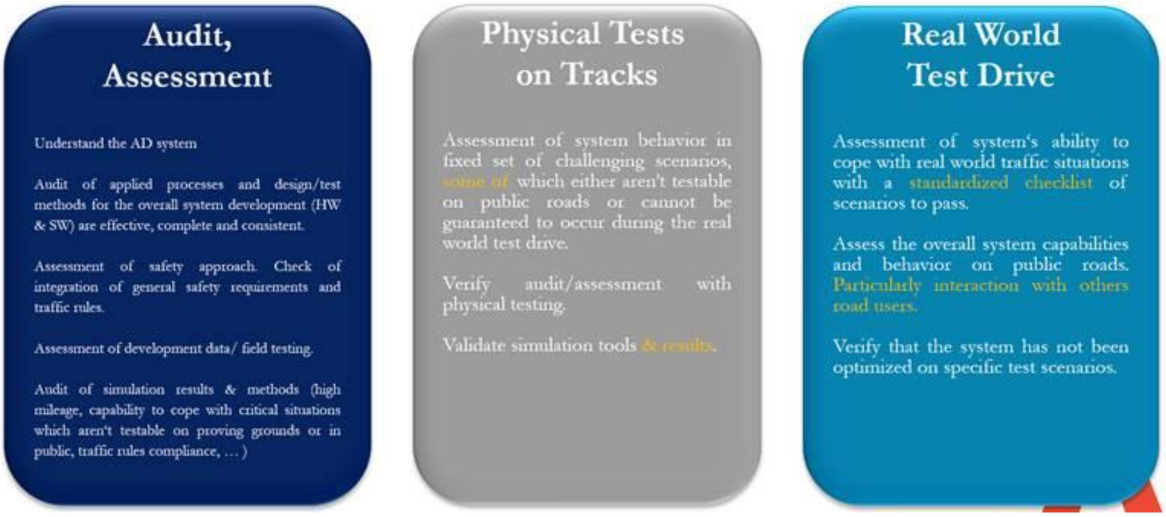
Standardization can efficiently support regulations on validation methods. Standardization has recently opened number of working items on automated and connected driving. Based on the approach proposed above, priority domains appear as follows:

Validation domain / issue / block	***Priority***
ODD definition (list of dimensions / parameters)	***
System reference architecture	*
Unitary manoeuvers taxonomy (e.g. brake, change lane)	**
Complex manoeuvers taxonomy	*
MRM taxonomy	**
Validation scenarios taxonomy	***
Scoring methods for scenario (e.g. severity, frequency)	**
Management of driving scenarios for validation (best practices)	**
Simulation accuracy validation methods	**
Unitary maneuvers test protocols	**
Complex manoeuvers test protocols	*
Combining simulation / tests (closed sites / open road) : best practices	*
Randomization methods for tests	*
HMIs safety critical functionalities	**
HMI testing and evaluation protocoles	***
HD mapping and positioning testing protocoles	**

Annex 1 : articulation with OICA « 3 pilars » approach : a bird-eye view

At this stage of reflections on future validation approaches, the OICA proposed approach is a key-reference, though not binding to public authorities, and though several other contributions have been put on the table.

This annex proposes a schematic view of the articulation between the proposed approach of this document, and the OICA "3 pilars" approach.



Audit, Assessment

Understand the AD system

Audit of applied processes and design/test methods for the overall system development (HW & SW) are effective, complete and consistent.

Assessment of safety approach. Check of integration of general safety requirements and traffic rules.

Assessment of development data/ field testing.

Audit of simulation results & methods (high mileage, capability to cope with critical situations which aren't testable on proving grounds or in public, traffic rules compliance, …)

Physical Tests on Tracks

Assessment of system behavior in fixed set of challenging scenarios, some of which either aren't testable on public roads or cannot be guaranteed to occur during the real world test drive.

Verify audit/assessment with physical testing.

Validate simulation tools & results.

Real World Test Drive

Assessment of system's ability to cope with real world traffic situations with a standardized checklist of scenarios to pass.

Assess the overall system capabilities and behavior on public roads. Particularly interaction with others road users.

Verify that the system has not been optimized on specific test scenarios.

Main additional focuses proposed in this document :

Pillar 1 : audit	*Pillar 2 : closed sites tests*	*Pillar 3 : open-road tests*
Understand the system : focus on ODD, manoeuvers, and system architecture descriptions	Assessment of system behavior (= safety performance) : endogenous – random tests could supplement fixed pre-defined tests according to use-case specific risk analysis	Assessment of system behavior (= integration in traffic) : focus on driving policies (i.e. complete maneuvers defined by strategic intention)
Assess the safety approach : focus on scenario management for validation	+ Assessment of critical sub-functions if relevant to use-case + risk analysis	Assessment of system behavior : focus on ODD management
Assess field testing / simulation strategy : focus on representativeness of scenarios		Assessment of system behavior : focus on other user's perception + understandability
Addendum : assessement tools involving drivers (ego, alter) : desk studies, simulations, tests		
Addendum : focuses on sub-functions when relevant to use-cases : HMI, perception-recognition, mapping and positioning, connectivity		

Annex 2 : glossary

Homologation: Homologation is the granting of approval by an official authority. To enter the automotive market you need to ensure your systems, components or vehicles satisfy the requirements set by national and international regulatory bodies.

Certification: Certification is a written certificate of compliance with a referential.

Automated Driving System (ADS): An automated driving system comprises a set of elements that offer a specific conditional or higher automated driving use case in or for a specific ODD.

Automated Vehicle (AV): Automated vehicles are vehicles equipped with at least one conditional (SAE L3) or higher (SAE L4/L5) automated driving system that enables them to provide an automated dynamic driving task.

Validation [ISO 15288]: "Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled" [ISO/IEC15288]. Takes place during validation testing to determine if an outcome is best for the end customer. Typically done at a later development stage with much slower feedback, as validation is normally performed via statistical methods with high number of tests.

Verification [ISO 15288]: "Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled" [ISO 15288]. Typically used to obtain fast feedback during development.

Safety [ISO26262]: This refers to the absence of unreasonable risk due to hazards.

Safety validation [ISO 26262]: It is an assurance, based on examination and tests, which the safety goals are sufficient and have been achieved.

Safety Of Intended Functionalities (SOTIF): "The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF)."

Operational Design Domain (ODD) [SAE J3016]: The ODD refers to the operating conditions under which a given automated driving system or feature thereof is specifically designed to function.

"These limitations reflect the technological capability of the automated driving system."

Object and Event Detection and Response (OEDR) [SaFAD]: The automated vehicles shall be able to detect and respond to object/events that may be reasonably expected in the ODD.

Human Machine Interaction (HMI) [SaFAD]: Human-machine interaction focuses on the interdisciplinary interaction between a human and computer and considers the human-machine interface (HMI). The aim is to develop an ideal user interface that satisfies the requirements regarding the mental, cognitive and manual abilities of the user.

Minimum Risk Manoeuvres (MRM) [SAE J3016]: Minimal risk maneuver refers to a procedure aimed at minimizing risks in traffic and which is automatically performed by the system, e.g. when the driver does not respond to a takeover request.

Capability based approach: Capabilities are driving competencies that an ADS proposes, that have to be verified or assessed towards expected performance levels. A capability-based homologation/certification approach relies on verifying that capabilities proposed by a given system perform as stated and that this performance is acceptable in terms of safety. Some capabilities can be functionnally pre-specified or their performance can be pre-specified. Some capabilities can be evaluated by comparison with the performance put forward by the manufacturer, without pre-specification of functions or level of performance.

In-use system monitoring and system update: It is a process of monitoring AD System Safety, automatic detection of discrepancies of unknown unsafe scenarios and AD System update when it is required.

Fail safe [SaFAD]: This means that the system still operates in a safe state in the event of a failure.

Fallback or Minimum Risk Condition (MRC) [SAE J3016]: It is a condition to which a user or an ADS may bring a vehicle after performing the Minimal Risk Maneuver in order to reduce the risk of a crash when a given trip cannot or should not be completed.

Takeover [SaFAD]: Transfer of responsibility for the driving task from the automated vehicle to the operator.

Assessment [ISO 26262]: an examination of a characteristic of an item or element.

Controllability [ISO 26262]: Controllability is an avoidance of the specified harm or damage through the timely reactions of the persons involved.

NOTE: The parameter C in hazard analysis and risk assessment represents the potential for controllability.

Hazard Analysis and Risk Assessment (HARA) [ISO 26262]: HARA is a method to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention or mitigation of these hazards in order to avoid unreasonable risk.

Functional Safety Concept (FSC) [ISO 262262]: Functional Safety Concept is a specification of the functional safety requirements, with associated information, their assignment to architectural elements, and their interaction necessary to achieve the safety goals.

Accident [SaFAD]: An accident is an undesirable, unplanned event that leads to an unrecoverable loss of service due to unfavorable external conditions, typically involving material damage, financial loss and (lethally) injured humans.

Event: modification in the external environment of the vehicle, e.g. target vehicle begins to decelerate, Pedestrian detection, end of lane, line marking change.

Failure [ISO 26262]: A failure is the termination of an intended behavior of an element or an item due to a fault manifestation.

Risk [ISO 26262]: a combination of the probability of occurrence of harm and the severity of that harm.

Residual risk [ISO 26262]: It is a risk remaining after the deployment of safety measures.

Hazard [ISO 26262]: Hazard is a potential source of harm.

Reasonably foreseeable risks [ISO 26262]: event that is technically possible and has a credible or measurable rate of occurrence.

NOTE: Credibility is normally determined by a group of knowledgeable people.

Audit [ISO 26262]: The audit is the examination of implemented process.

Simulation [SaFAD]: The approximated imitation of selected behavioral characteristics of one physical or abstract system by a static or dynamic model [according to ISO 2382/1]. The simulation represents the behavior over time in which the system or parts of it are replaced by the model. It includes SiL, SoL, HiL, HoL and DiL.

Scenario [SaFAD]: A scenario is a temporal sequence of scenes and covers a certain time span.

Abbreviated terms

ACC	Adaptive Cruise Control
AV	Automated Vehicle
ADS	Automated Driving System
HMI	Human Machine Interfaces
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OICA	Organisation Internationale des Constructeurs Automobiles
NHTSA	National Highway Traffic Safety Administration
MRC	Minimum Risk Condition
MRM	Minimum Risk Manoeuver
SAE	Society of Automotive Engineers
SOTIF	Safety Of Intended Functionalities