Direction générale des infrastructures, des transports et de la mer

Direction générale de l'énergie et du climat

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

September 2019

DRAFT

Foreword :

Autonomous driving development requires an 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 draft 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 draft document is the second 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. It was already presented at UN level (ITS/AD 12th session, 22 June 2017).

---

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

This draft 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:

Validation domain / issue / approach	✓ *Covered (not : /)*
Operational design domain	✓
System architecture and redundancies	✓
Human machine interfaces	✓
Remote monitoring / actuation	✓
Manoeuvers specification and validation	✓
System activation / desactivation / transition	✓
Minimum risk manoeuvres	✓
High level safety rules	✓
Concept of safety envelop	✓
Risk analysis : object and events detect and response	✓
Management of validation scenarios'	✓
Role of process audit	✓
Relevance of simulations and tests	✓
Concept of "driving license"	✓
Education, awareness, training	/
Cybersecurity	/
Privacy	/
Aftermarket system update	/
Accident data recording	/
Crashworthiness	/

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

- It focuses on ***public expectations towards validation*** ;
- It intends to be ***use-case agnostic***, considering that the focus on motorway-individual-cars L2/L3/L4 use-cases might not be sufficiently forward looking ;
- It reflects common ***public-private thoughts and discussions*** from experts contributing to future regulations in the French autonomous driving eco-system.

---

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

1. *Context*

a. *Need to act*

Autonomous driving 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 autonomous driving development, 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 use cases 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.

---

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

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.

b. *French context*

- *National strategy*

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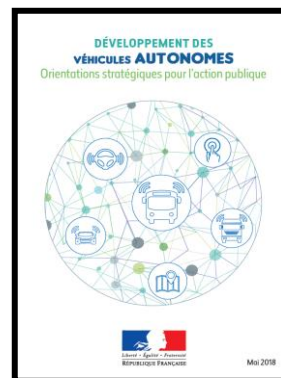
Under this strategy, the main actions undertaken cover the following axis:

- 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.

- *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).

---

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

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.

2. *Upstream considerations and general framework for future validation approaches*

The approach to safety validation should take into account four main considerations:

➢ Innovation and differentiation will come together with the ***diversification of use-cases***, namely their operation design domain and functionalities. In this respect, international reflections should seek convergence on validation approaches, not on use-case regulation. Said differently, a given use-case, 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 ***use-cases descriptions***. In line with this, validation approaches should cover use-cases in which the driver is to take control from outside the vehicle in certain circumstances, as well as use-cases in which safety is locally provided, to a large extent, by infrastructure, its equipment and connectivity ; validation approaches should cover these additional elements.

➢ Autonomous systems will be designed, manufactured and implemented under diverse conception approaches, some being traditionally applied in the automobile industry, such as the V-approach, some being more innovative.

➢ The concept of manoeuvre is key: driving, even automated, will remain a sequence of unitary manoeuvres that allow to go from point A to point B in sometimes hazardous driving conditions. Non-autonomous driving regulation (and namely, traffic rules and driving license examinations) are based on the concept of manoeuvers. Human drivers interact by observing and anticipating others' manoeuvres.

➢ The challenge of autonomous driving validation (compared to traditional automobile validation), is to manage the shift from system failures to driving hazards (previously handled by the driver) in risk analysis. Industry has undertaken this shift in standardization, under the Safety of intended functionalities (SOTIF) framework. Use-case specific risk analysis, dependent of the use-case, is at the core of validation ; it should handle all relevant foreseenable driving events (including "nominal" day-to-day and edge-critical) and failures.

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, and somehow independent angle for public validation, based on performances.

In a performance-based approach, ***manoeuvers, 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 the main window through which public authorities can scrutinize industry validation processes.

The following graphs translate these considerations in a general validation architecture, and its link with the objects and events detection and response (OEDR) approach.
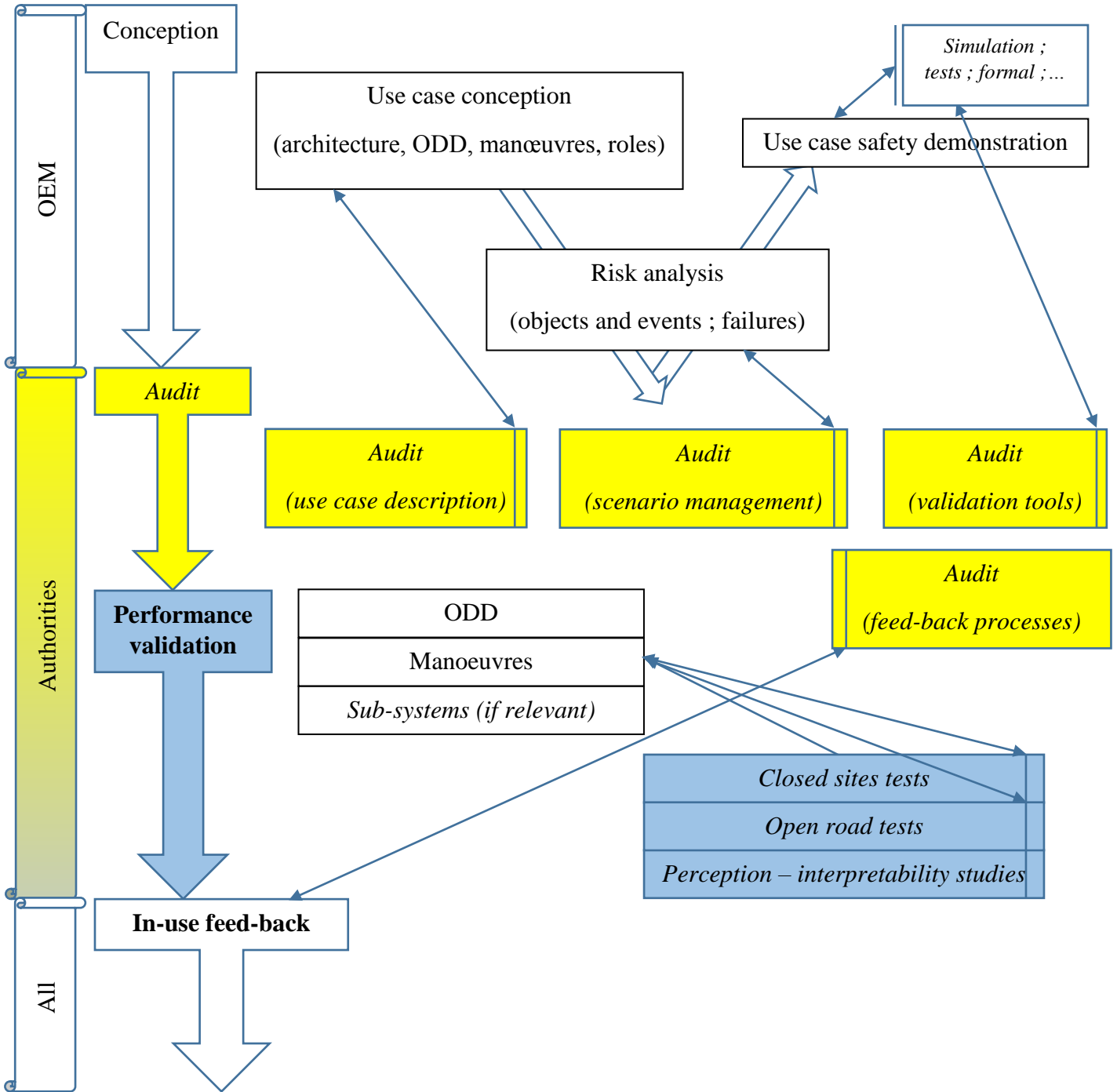
Graph 1 : overall approach : conception, audit and performance validation

6

Graph 2 : use case description, risk analysis and validation
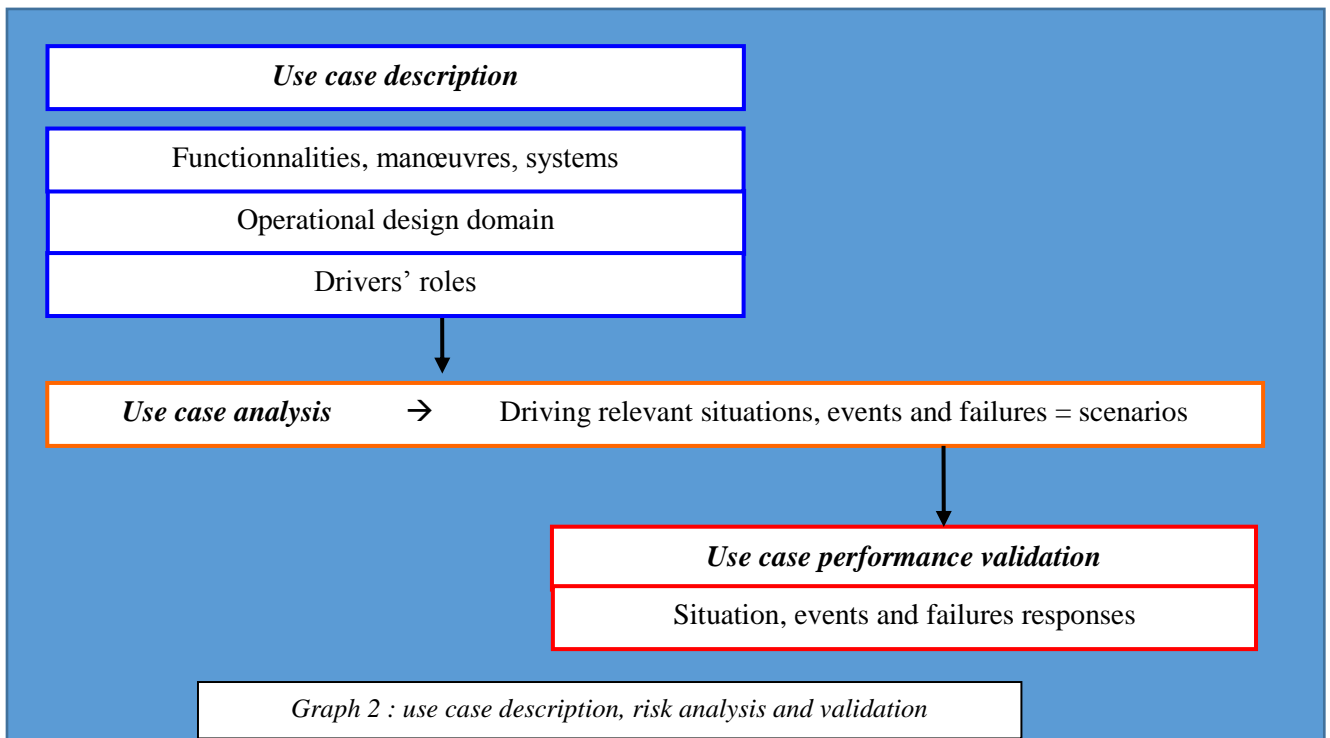
3. Validation principles

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, manoeuvres)

➢ *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*

  o *Principle # 3.1: Validation by public authorities should focus on driving responses (manoeuvers)* to systems failures and driving hazards and assess both :

    - critical manoeuvres' safety, responding to edge scenarios

    - current manoeuvres carefulness or roadmanship

  o *Principle # 3.2: Physical tests should combine* :

    - a standardized approach, for a limited set of common functions or manoeuvres

    - 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 statet of the art and public validation processes. Inter alia, public authorities should develop knowledge on critical driving situations, based on feedbacks by the industry.*

4. Validation building blocks

Validation building blocks should combine functions, conception processes and validation tools.

Functionnal items should mainly cover :
- ODDs
- Manoeuvres
- Relevant sub-functions (when appropriate)

Conception processes should mainly cover :
- High level safety rules
- System architecture
- Management of driving scenarios
- Management of validation tools

Validation tools could be divided in the following main categories :
- Descriptions
- Validations
  o Simulation
  o Tests (closed sites ; open driving)
- Behavioral and interpretability assessment

Based on this schematic taxonomy, the following schemes details articulation between validation items (functions and processes) and validation tools.

Automated driving systems functions		Description	Simulation	Tests (closed)	Driving (open)	Behavior / perception studies
Operational design domain	ODD definition	*				*
	ODD recognition / aknowledgment	*	*	*	*	
Manœuvres	Manoeuvres logigram	*			*	*
	Manoeuvers triggering conditions	*	*	*	*	*
	Unit manoeuvers (lane keeping, ACC)	*		*		
	Nominal manoeuvres (etiquette)	*			*	*
	Critical, Minimum risk, Fail Safe, Limp Home manoeuvers	*	*	*		
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	*	*	*	*	*
	System architecture	*	*	*		
	Management of driving scenarios	*				
	Management of validation tools	*				
	Test facilities and protocols	*				
	Simulation tools (accuracy)	*		*	*	

The previous table highlights the importance of functional descriptions as a basis for i) audit and ii) selection of relevant performance assessment validation tools (simulation, tests, behavioral studies).

Beyond description, validation should be based on a set of references, that will need to articulate standardized and use-case-specific approaches. Parts 5.a and 6 thereafter propose some preliminary considerations on the rationale for audit on one hand, the rationale for standardization of reference documents on the other hand.

Complementary considerations for selected building blocks

a. Rationale for audits : preliminary 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 manoeuvres) are assessed with a "completeness" criteria, i.e. ensuring that this type of event is identified properly and addressed by a response (manoeuvre). For the highest levels of criticity, the relevance and, furthermost, the safety of the response becomes the assessment criteria. For these responses (manoeuvres), 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 manoeuvres and ODD's design.
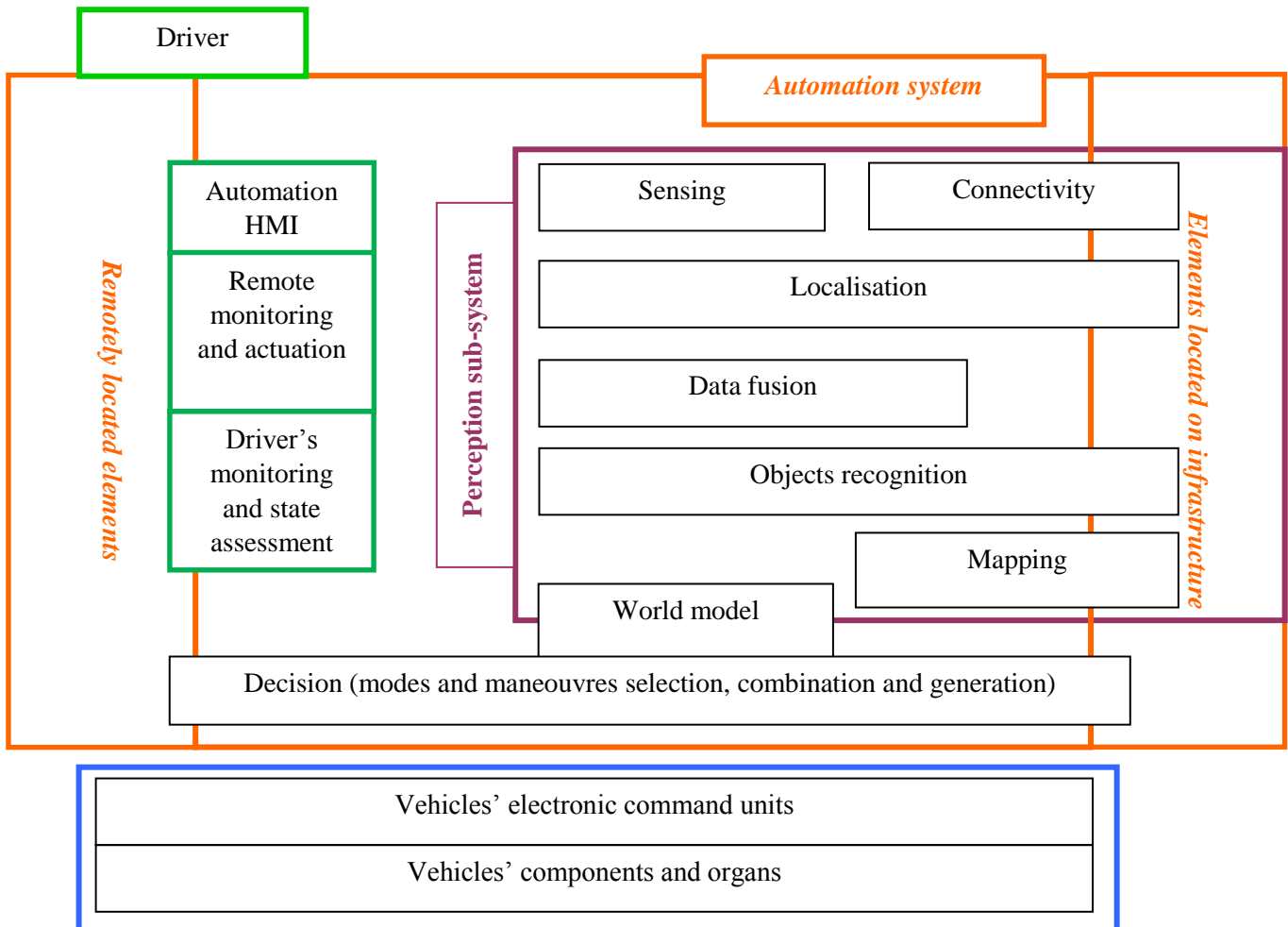
b. ODD description

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)

c. *System architecture*

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

d. *Manoeuvres description*

Manoeuvres description is a key input to validation.

Autonomous driving systems will develop specific manoeuvres as responses to objects and events' detection. Manoeuvres' 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 manoeuvres should be preserved in the validation process. Hence, the only criteria for validating a manoeuvre should, in theory, be its safety. This principle may, however, raise issues on the compatibility of a given manoeuvre with national traffic rules. Besides, this general principe should be balanced considering that manoeuvres should be understandable by the "common alter driver", especially emergency manoeuvres, for which understandability challenges are even more important for safety.

Manoeuvres should be considered with two different and complementary angles : a large-angle view should consider a manoeuvre characterized by the overall driving intention (e.g. keep in line, overtake, turn left, exit a motorway, park) ; a focused-angle should consider sub-manoeuvres 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 manoeuvre. However, some sub-manoeuvres might have specific safety and interpretability challenges that should be identified as such and addressed by relevant validation or interpretability assessment tools.

Manoeuvres 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 manoeuvres

e. *Overarching or 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
   o including ODD acknowledgment (i.e. subsequent actions when out of ODD)
- Minimum risk manoeuvres (MRM) activation conditions
- Safety envelope (longitudinal and lateral safe distances) (nominal manoeuvres or MRM)
   o Including etiquette behaviors and possibilities for the driver to specify them
- Management of discrepancies in driving rules
   o 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*
   o *Overall intention*: Automated Vehicle deployment shall improve the road safety
   o *Safety qualitative objective*: The automated vehicle is free from unreasonable risk
   o *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
   o *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
   o *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*
   o *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.

o   Operational Design Domain (ODD)

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

o   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.

o   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.

o **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

o *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)

o *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)

f. 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 manoeuvres-based approach

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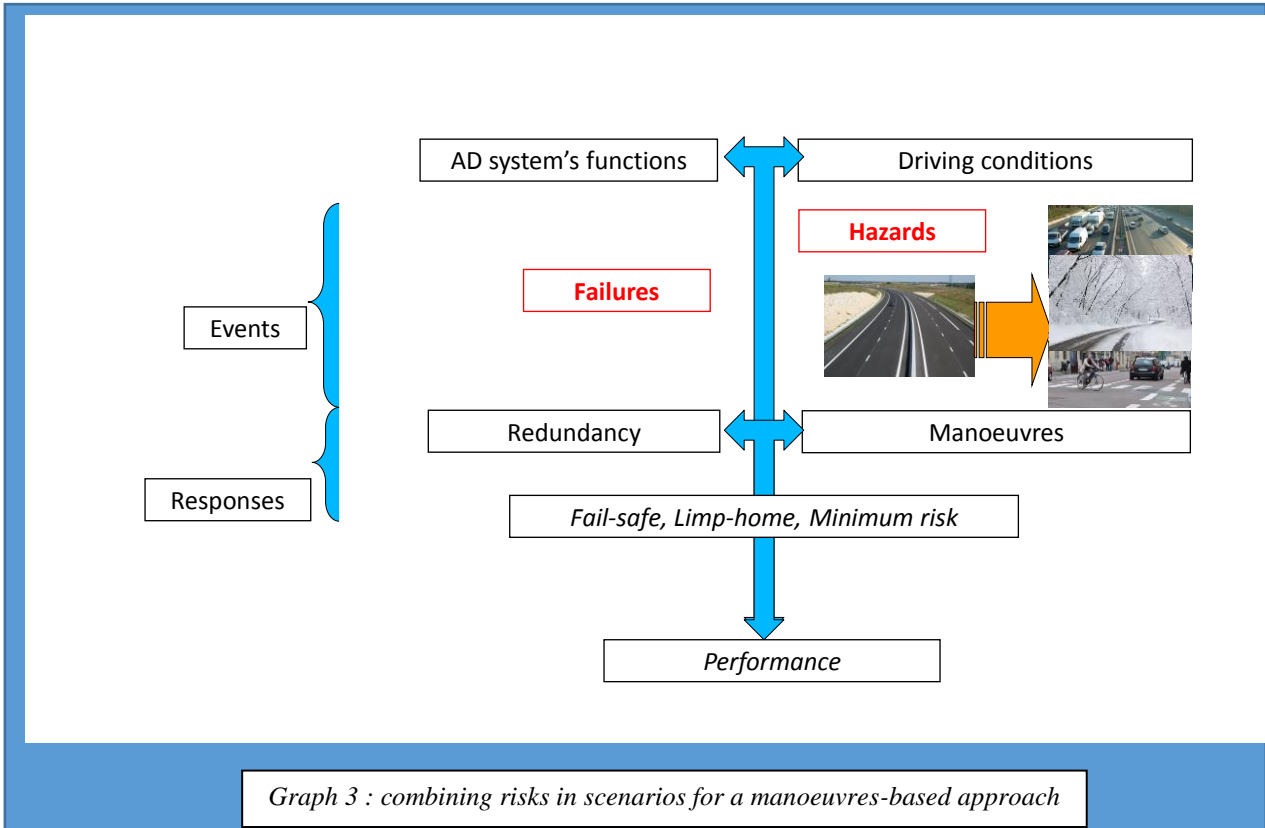
Box: basic concepts and definitions for validation-relevant driving scenario

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").
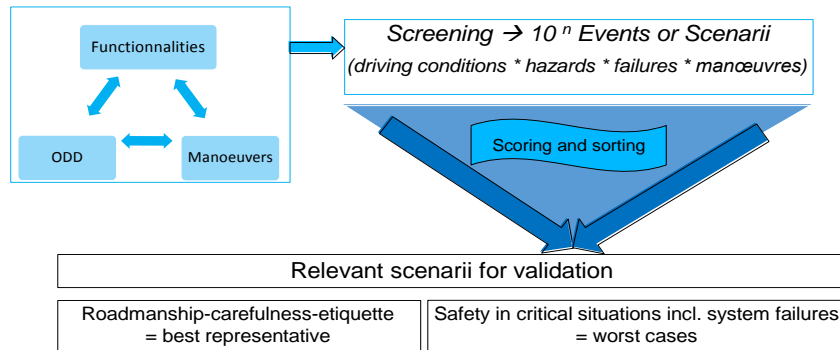
Managing driving scenarios must be considered as a key process of autonomous driving systems' conception. This process' description and some of its outputs must be transparent to public output. Auditing this process should be part of public authority validation. This might require developing ad'hoc quality references or guidelines. The following graph proposes a schematic presentation of the main process steps for managing driving scenarios for validation.
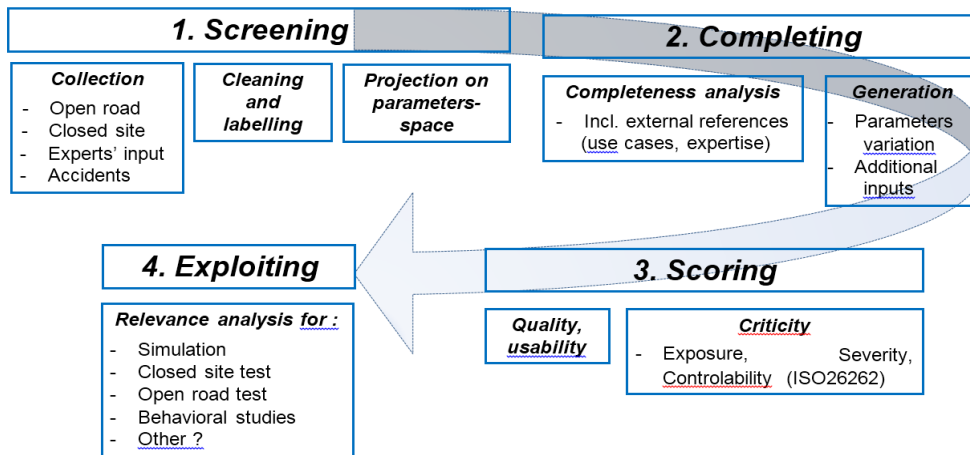
Regarding transparency to public authorities, important aspects of scenarios management are:
- Method applied for *screening* scenarios (e.g. sources used), in particular how driving hazards and sub-systems failures are combined
- Approaches applied for *assessing completeness and, if necessary completing* 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).

g. Challenges for specific subsystems (1) : 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. manoeuvres). If relevant, the validation approach could, for instance, use a list of predefined objects and events and a list of events related to nominal manoeuvres and critical manoeuvres 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.

h. Challenges for specific subsystems (2) : 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:

j.   *Tests and simulations*

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
  - o 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 manoeuvres.

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 manoeuvres (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 manoeuvres, and their interactions with a diversity of other road users.
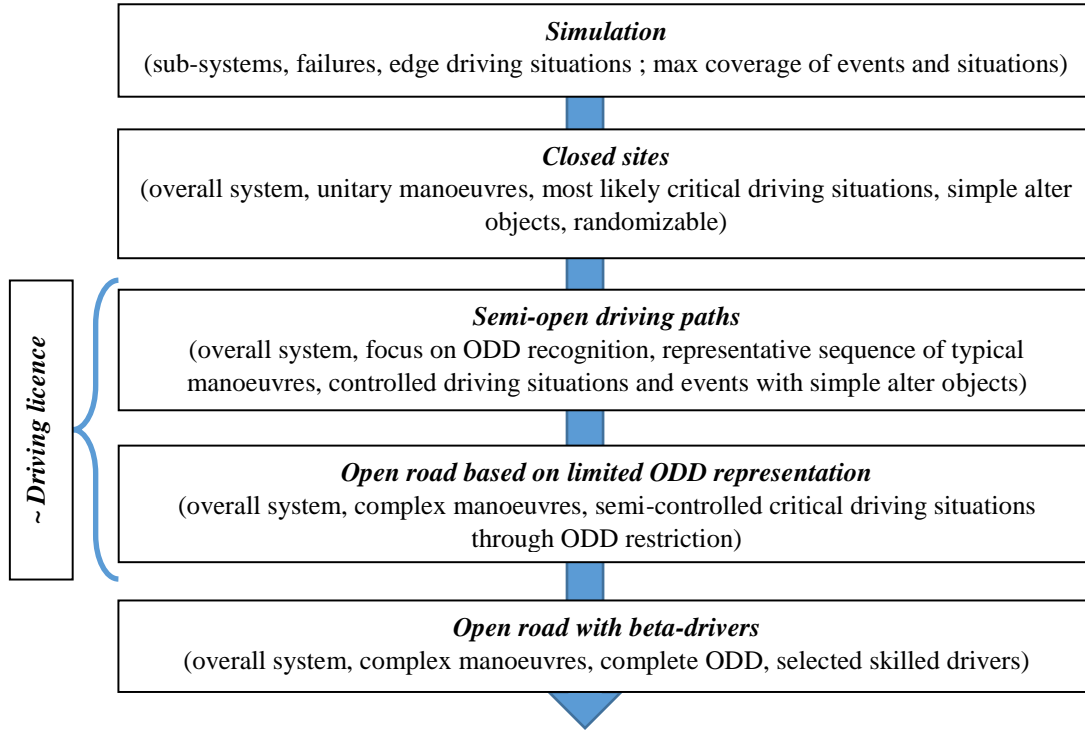
Some validation tools (either through simulation or tests) could address unitary manoeuvres that prove to be common (such as automatic breaking, lane keeping) to all use-cases, which would naturally lead to standardized protocols. Some other manoeuvres might deserve to have standardized protocols, if they prove to be common among use cases. Some minimum risk manoeuvres might enter this category, though it is likely that minimum risk manoeuvres 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 manoeuvres within its ODD).

Standardizing these tests is an open question : it would require to set a common decomposition of manoeuvres, 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 manoeuvres, 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.

20

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 manoeuvres (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 manoeuvres, most likely critical driving situations, simple alter objects, randomizable)

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

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

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

~ Driving licence

k. Behavior and perception 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.

6. *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 manoeuvres 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 : 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.

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 manoeuvres 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		