Ministère de la transition écologique et solidaire, Ministère des transports
DGITM/SAGS/EP et DGEC/SD6

August 10, 2017

International horizontal regulation of automated vehicles

Preliminary framework considerations

Working document

Foreword

This working document aims to contribute to the reflexion opened in UN-ECE WP29 – ITS/AD on the development of technical regulations addressing the challenges of automated driving.

This working document proposes preliminary general considerations for a new framework for automated vehicle's regulation. It briefly presents the context, grounds and objectives for developping a new "horizontal" regulation framework, and some references. It then proposes basic concepts and definitions in order to clarify automation systems' functions, use-cases and regulation building blocks. This document finally proposes preliminary principles ("the philosophy") and a possible schematic framework for vehicle's regulation, including vehicle approval or validation.

These principles are illustrated on a use case, which allows to present how this horizontal regulation might articulate with "vertical" regulations, in particular R 79.

This working document intends to serve as an input and fuel to further discussions in UN-ECE WP 29. In this respect, it retains a rather general view, and presents a number of open questions.

This working document is not a consolidated nor formal proposal from the french authorities on vehicle regulation, neither on the ongoing discussions on regulation R 79 on ACSF, nor on the future of vehicle regulation at the UN-ECE and EU level.

1. Context and grounds to act

Vehicles' automation is developping rapidly, through increased levels of automation and diversified functionnalities and driving environments. This path will certainly continue in the future, although technologies' readiness and use-cases is still difficult to predict.

In this context, the main challenge for public policies is to set the right balance between innovation on one hand, and road safety and security concerns on the other. Vehicles' regulation, and its various possible levers, remain the key policy instrument to set this balance, at the national, regional or international level. The international dimension of this instrument is an opportunity to respond to the industry needs for a minimum set of commonalities among national or regional markets, taking into account national or regional social and economic specificities.

The existing vehicles' regulation system, including UN-ECE regulation and national / regional requirements, approval or certification processes, face significant challenges from the development of automation. These challenges may, in brief, be split into different categories :

a. automated vehicles are becoming increasingly ***complex systems***, in which all components interact, so that the "interactions management" of the system becomes more and more critical for road safety and security concerns ; in this context, the present philosophy of vehicles regulation to mainly address "elementary systems", might leave some critical road safety and security dimensions out of scope ; more precisely :
    - In the past, technical regulations scope would essentially cover aspects that are not linked to "sensing capacities" (perception of the environment) and "driving skills" (making the right decision at the right moment), because these aspects were considered as being under the driver's hands.
    - Sensing capacities (mainly eyes and ears of the driver) were considered as "sufficient" with the average driver.
    - Driving skills was then addressed by the process of "driving licence".
    - In the future, a new set of technical regulations must address aspects such as "sensing capacities" and "driving skills", as they will be partly or entirely in the hands of the "automated system".
    - Interactions between the system and the driver will have to be addressed too (communication from one to the other, i.e. HMI… take-over sequences…)
b. automated systems, namely in the progressive path to full automation, create a more complex and diverse set of ***interactions between the driver and the vehicle*** ; along this path, different automated systems are developped in coherence with a given "regime" of interactions between the driver and the systems (e.g. in terms of driver's delegation to the system, and vice-versa) ; the various possible "interactions regimes" are clustered in SAE levels ; although these levels are sometimes not sufficient to caracterize in details all automation use-cases, they provide useful general features of "task sharing" between the driver and the system ; vehicle's regulation needs to have this challenge on board, taking into account that vehicle's regulation adresses vehicles and not drivers ;
c. automated systems generally develop through a progressive extension or diversification of ***"design domains" or "driving conditions"*** ; vehicle's regulation needs to have this challenge on board, taking into account that vehicle's regulation adresses vehicles and not driving conditions ;
d. automated systems will increasingly be both ***learning and updated systems***, so that the "updated" performance of the systems will, more than today, be significanlty different from the initial performance.
e. automated systems, including their sensing capabilities and their automation functions, will increasingly be supplemented by ***connexion systems (V2V, V2I, V2X)***, making the vehicle's performance partly linked to external or remote systems' performance.

2. Scope and objectives

Among the challenges listed above, this document mainly aims at adressing challenges a), b), and c). The objective is hence to propose an architecture of regulation that considers :

- a systemic approach of the vehicle
- a diversity of "task sharing" between driver and system, from SAE level 2 to level 4
- the diversity of use-cases (e.g. beyond ACSF levels A to E that are under scrutiny in the revision of R 79)

It is important to note that the above challenges not only question UN-ECE vehicle's regulation, but also national or regional validation, type-approval or certification approaches, as well as periodic roadworthiness testing.

This working document proposes preliminary considerations on the relevance of different safety validation concepts or tools (eg. type-approval, performance based approach, auto-certification), considering, e.g. real versus virtual tools ; all-roads versus geo-fenced approaches ; admittance versus in-use approaches ; statistic versus one-vehicle-for-one-type approaches. Taking into account national or regional practices and differences on vehicle's safety validation, the considerations on approval, validation, certification processes are proposed as opened questions.

As far as validation approaches are concerned, this document doesn't address, at this stage, the issue of over-the-air software updates.

3. Main references

The main references used as inputs for this document are :

- Draft versions for the revised R 79 regulation on steering
- Proposed principles for UN regulation of automated driving, UNECE/WP29/ITS-AD, march 2017
- US-NHTSA guidance, september 2016
- EuroNCAP reflexions on assessment
- ISO 26262 standard on road vehicle system safety
- Various studies and research literature related to the evolution of automated vehicles' description, regulation, evaluation, testing.

Annex 4 to this document presents a synthetic overview of references related to :

- automation systems definitions
- use-cases definitions
- risk analysis and validation methods

4. Basic definitions

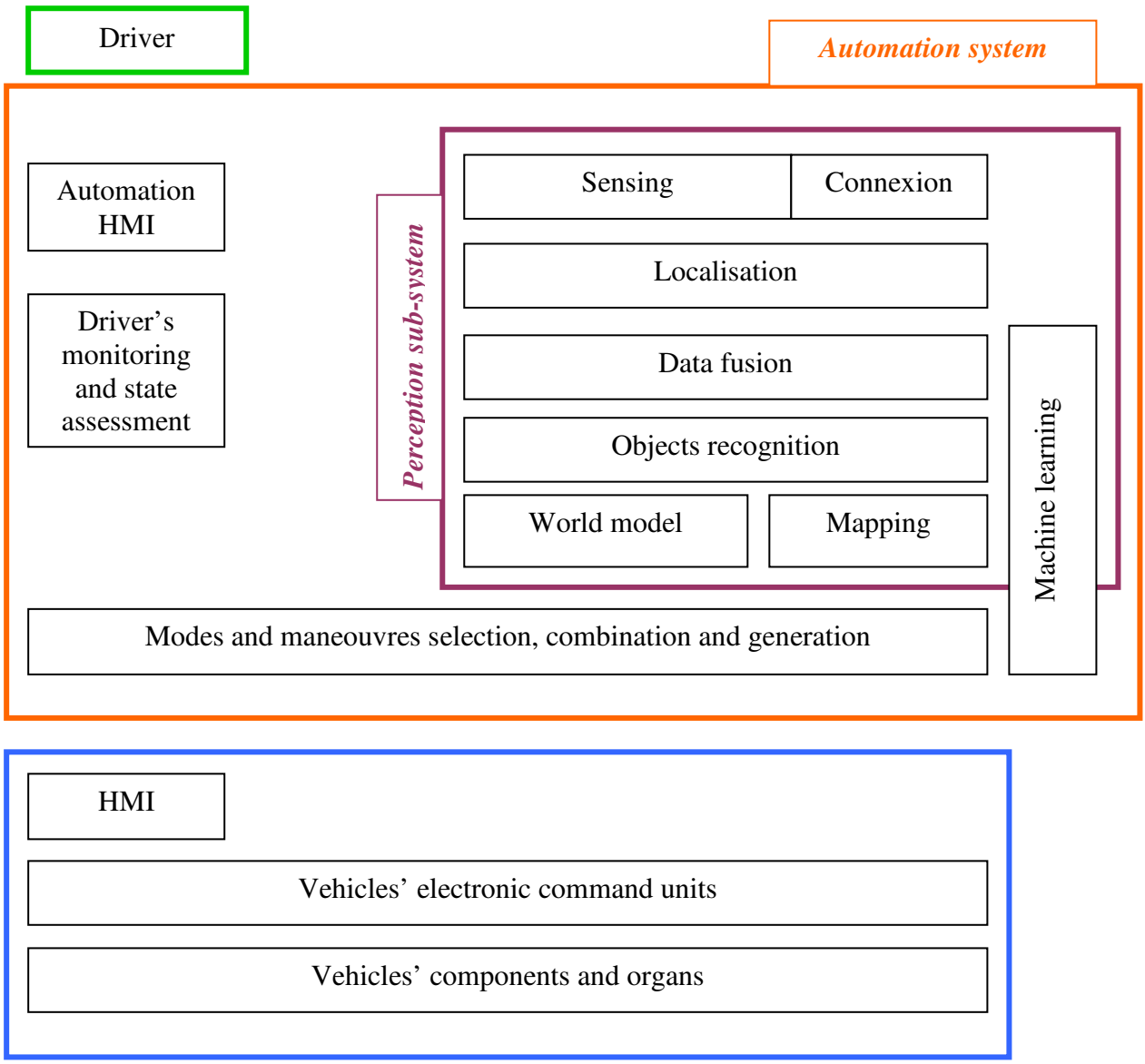
Clarity of concepts appears as a pre-requisite for a sound regulation architecture. This paragraph proposes definitions for three essential building concepts :

- vehicles' sub-systems
- automation use-cases
- regulation (or guidance) domains

Vehicles' sub-systems

The following scheme proposes to distinguish four main sub-systems of an automated vehicle :

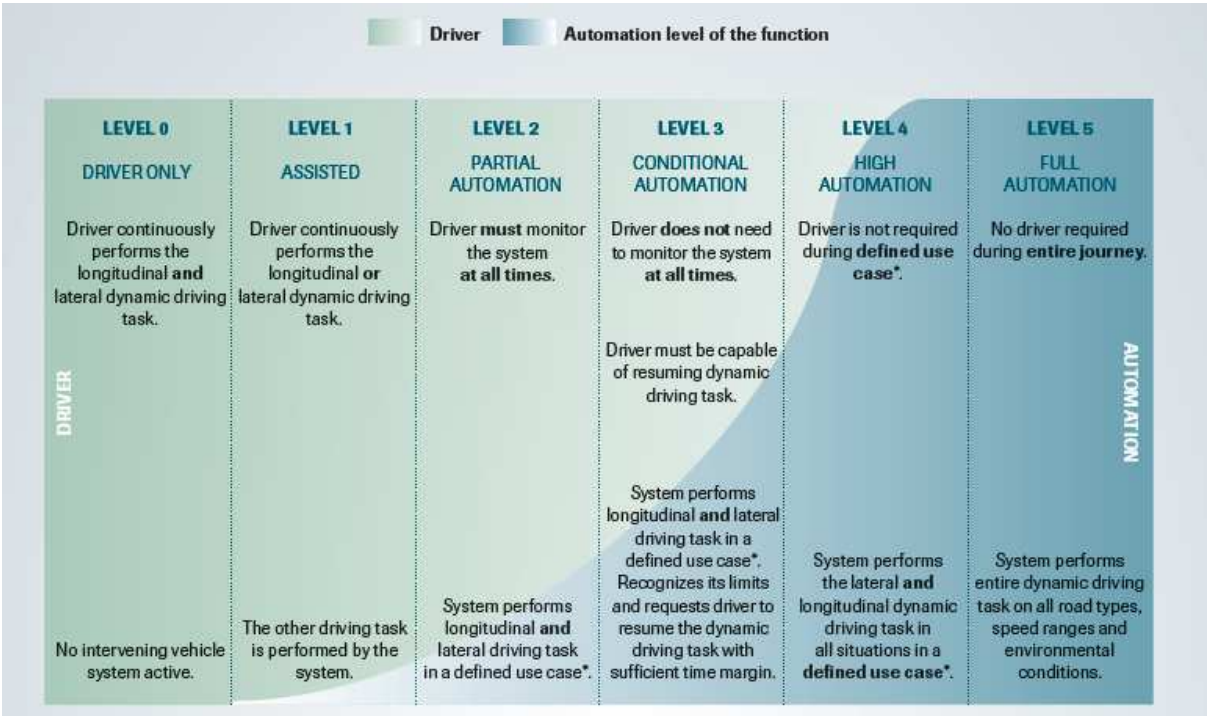
- Driver
- Human-machine interfaces
- Automation system
- Driving organs



4.2. Automation use-cases

Automation use-cases can basically be defined as a combination of four main parameters :

- specified driving environments or scenarios or "operational design domain" (e.g. type of infrastructure, type of signage, traffic and weather conditions, speed range, etc...).
- automation functionnalities or "elementary functions" (what manœuvre(s) does the system perform - e.g. lane change), under normal conditions
- activation / desactivation conditions and duration under normal conditions (~triggering conditions)
- expected « driving tasks sharing, e g driver's response to take over request » between the driver and the system, as set by SAE levels.



Other sets of parameters can usefully define a use-case more precisely, namely its functionnalities under transition conditions :

- transition procedures, and corresponding HMI functionnalities
- emergency or minimal risk maoeuvres functionnalities

It seems important to describe a use-case by the logic diagram by which are conditionnally articulated :

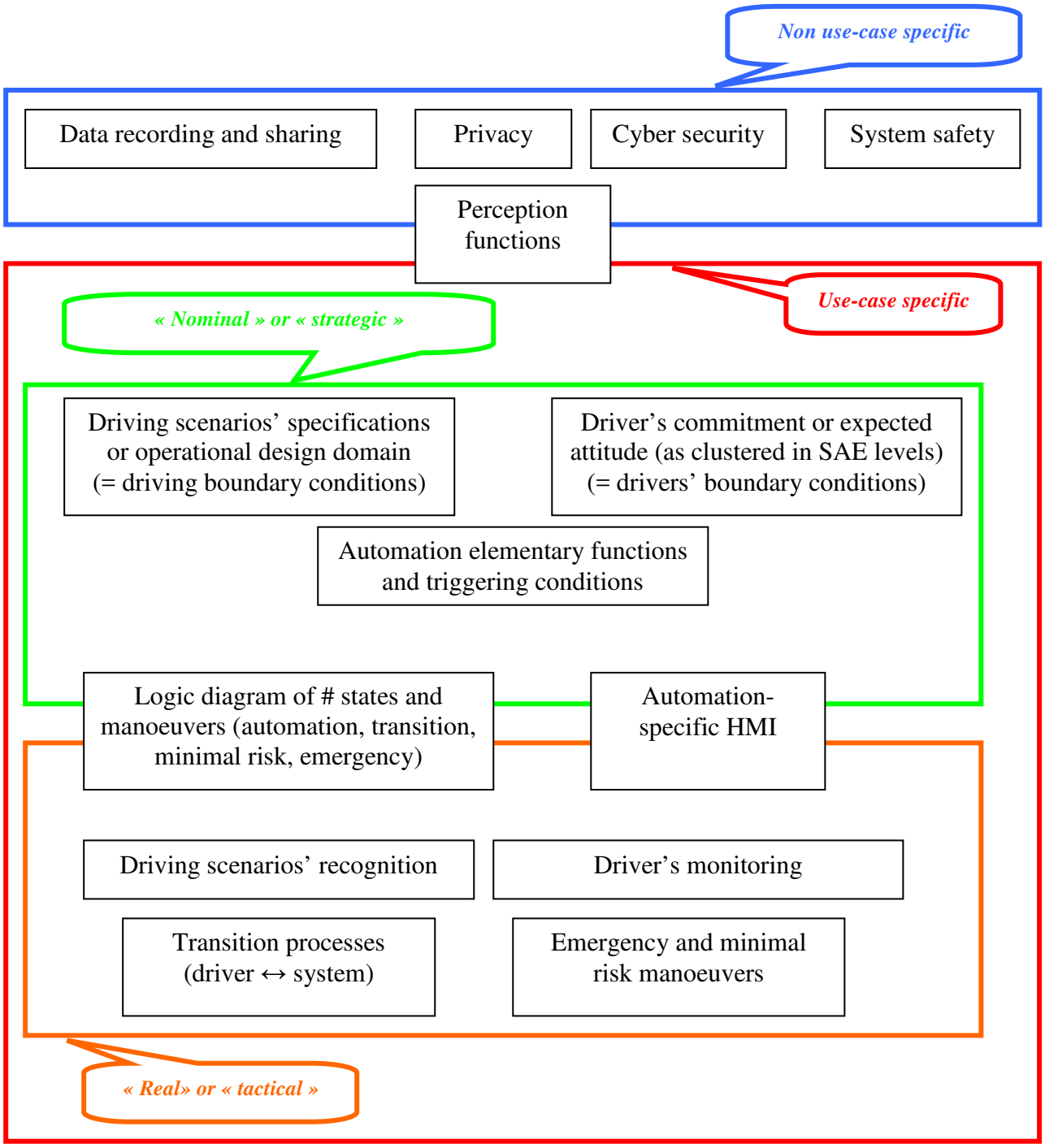
- different states of the automation system
- different states of the driver's
- vehicle's real environment (e.g. driving inside or approaching operational design domain limits ; unexpected situations, events or hasards)
- transition or emergency manoeuvres.

Finally, it seems important to include, in the system's description, the human machine interfaces (HMI) functionnalities, under three main sub-functions :

- drivers' information and warning on critical aspects of the vehicle's environment and safety ;
- transition requests to the driver ;
- driver's attitudes' and responses' monitoring functionnalities.

4.3. Regulation domains

The following graphs proposes a decomposition of regulation domains, based on above concepts and functions (This approach intends to be independant of technologies or systems).



5. Proposed regulation principles or « philosophy »

4.4. Use case description

The general principles or "philosophy" of a possible architecture for automated vehicle's regulation would be based on use-cases description, including their precise and applicable set of use-conditions (cf. above, and, most importantly by their driving scenarios, activation and desactivation modes) : different use-conditions should be considered as different use-cases.

In describing driving scenarios, it may be important to differentiate between :

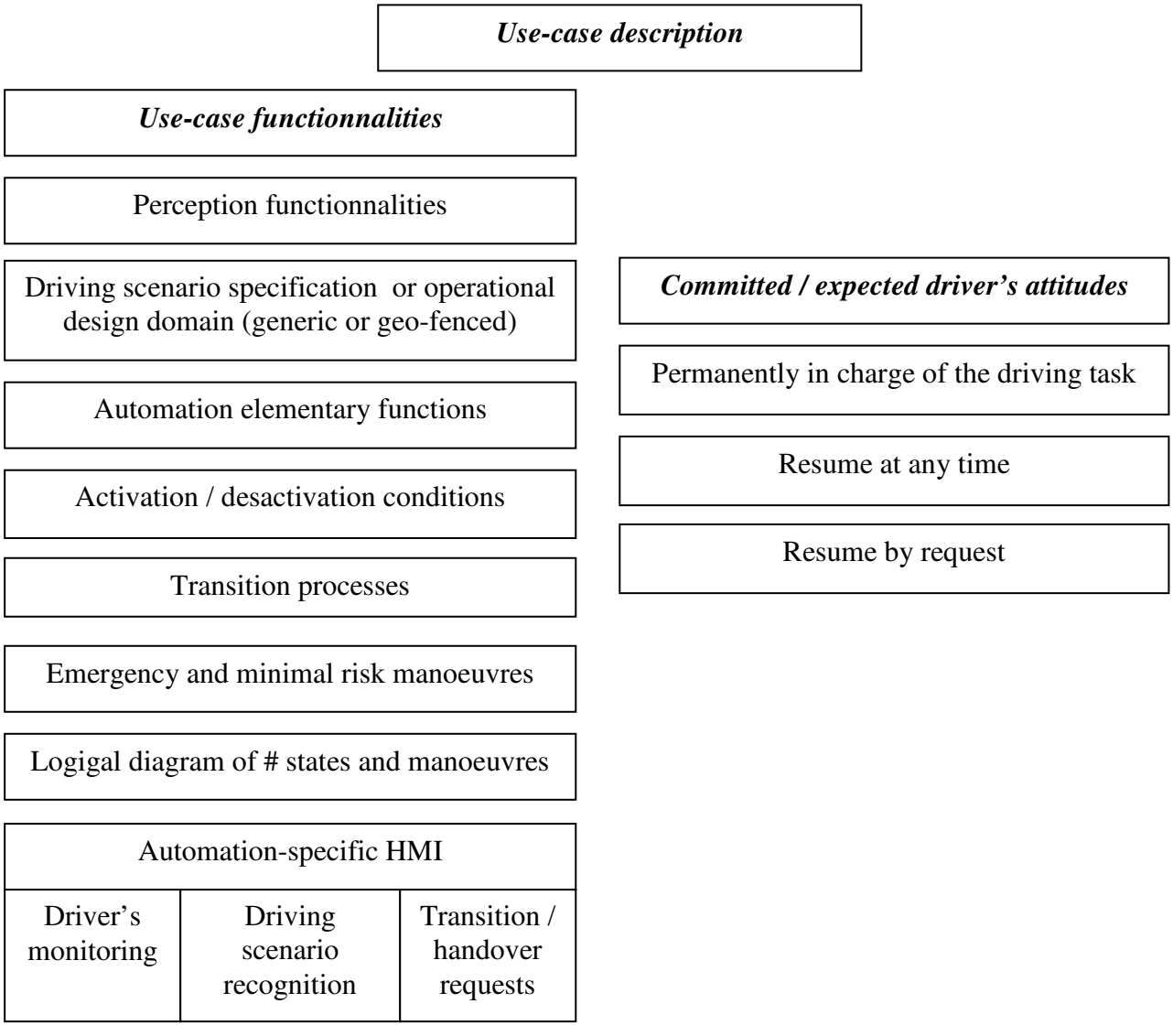
- generic driving scenarios (e.g. : highway, contextual speed : [90 – 130 km/h], daytime)
- pre-defined + localized driving scenarios, (thereafter called "geo-fenced"), e.g. for shuttles.

Use-cases should also be characterized by the expected attitudes or commitment of the driver, as regard to the following tasks and their combination :

- perform a manoeuvre ; monitor a manœuvre ; supervise the driving environment ;
- permanently ; resume at any time ; resume by request.

Whenever possible, a correspondence between the use-case's expected driver's attitude and a SAE level ("target SAE level") should be used.

The following graph summarizes the main parameters defining a use case.



4.5. Requirements : HMIs, driving conditions and driver's monitoring

Monitoring functionnal requirements should be coherent with the target SAE level, and, more precisely, with the requirements on the driver's ability to dynamically resume control during use case.

Monitoring functionnal requirements should be independent of driving scenarios.

Driving scenarios recognition should ensure that the limits of the nominal scenario underlying a given use-case, are recognized and that, depending on the use-case, either the system or the driver is aware of limits beeing nearly crossed.

HMIs' sub-functions addressing drivers' information and warning on critical aspects of the vehicle's environment and safety, as well as transition or handover requests to the driver, will become an even more critical function of automation systems for higher level of automations. Apart from their ergonomy which will remain an industry know-how for which competitive differenciation will support innovation, their efficiency in addressing safety, will depend on their abaility in managing the driver's attention in various situations for various drivers. Some commonalities in HMIs' functionnalities might hence be useful, in order to minimize the risk of mis-understanding of a likely increasing number of warning signs.

Specific regulations adressing HMIs main functionnalities and message priority management, might hence be necessary.

4.6. Requirements : critical situations and event responses

Within use-cases and driving scenarios (e.g. lane change in a given set of infrastructures + traffic + speed + weather conditions), it appears necessary to identify "critical situations" or "events" for which the automated vehicle's behavior is expected to be specific.

These critical situations would be a combination of, e.g. :

- Real driving situations
    - Infrastructure
    - Current driving objectives (eg: lane changing manoeuvers - straight lane or curve)
    - Real level of Traffic
- Events to consider
    - Events related to road signageand infrastructure
    - Events related to other road users, unexpected events

Critical situations and events would include the breach of normal use conditions.

The recognition and response behavior of the vehicle operates mainly through continuous handling of the driving task, transition processes, emergency and risk minimal manoeuvres, alert and request HMIs, and the overall articulation of these functions. The "recognition and response" is fundamentally a know-how of OEMs. Furthermore, the combination of parameters is likely to lead to a large number of situations or events, making this concept difficult to grasp for technical regulation, even though this concept seems critical to ensure road safety concerns are taken into account.

To ensure that all critical situations and events would be taken into account by manufacturers, a way forward would be a multi-layer approach, depending on the criticality of situations and events, by, e.g., setting different requirement levels, proportionate to the level of criticity :

- ***Criticity level one : "situation and event aknowledgment"*** : for situation or event "X1", the regulation would require that the risk management approach has included this critical situation and event, whatever the response to this risk would be
- ***Criticity level two : "situation and event response availability"*** : for situation or event "X2", the regulation would require that there is a response by the system, whatever its functions and performance would be
- ***Criticity level three : "situation and event response functionnal description"*** : for situation or event "X3", the regulation would require that the way the system manages the event or situation is described (which would include, e.g. the logigram of manoeuvres and HMIs functionalities activated)
- ***Criticity level four : "situation and event response required functionnalities"*** : for situation or event "X4", a given set of response functions would be supposed to be available : the functions could for example be ADAS such as emergency braking, dead man manoeuvres, minimum risk manoeuvres
- ***Criticity level five : "situation and event response required performance"*** : for situation or event X5, the regulation would require a performance of response functions ; in this case, the performance level would be set specifically to the use case, whereas it would be set exogenously, by "vertical" regulations in level three above)

This proposal makes response functions requirements both :

- Based on risk analysis
- Propositionnate to criticity
- Dependent on the use-case, and the "target" SAE level.

This appears to meet three significative expectations of the future horizontal regulation.

4.7. Requirements : minimal risk manoeuvres

The approach presented above doesn't address in depth the issue of minimal risk manoeuvres regulation, though this part of automation functions is likely to be at the core of safety challenges. However, this approach suggests that different minimal risk manoeuvres (MRM) performance levels would need be set.

At this preliminary stage of thought, the following parameters for MRMs' functionnal performance might be useful to consider :

- speed range for activation
- traffic density conditions for activation
- deceleration capabilities (max, min)
- capacity to detect and manage vehicles ahead + approaching (including from the right)
- triggering caracteristics of the target lane or location for vehicle stop such as parking area (e.g. width ; required length free of obstacles, lane marking availability,...)
- number of possible lanes from the departure lane to the safety lane
- conditions to abort the MRM and replace it by, e.g., AEB

4.8. Link with connectivity

It seems important to consider that vehicle connectivity will soon be part of the vehicle's "world model". In the approach presented above, it seems that connectivity related issues can be brought in the analysis of critical situations and events rather easily, as soon as these connectivity issues are considered as an additionnal contribution to the vehicle's perception via sensing, in these critical situations and events. Making the activation of automation functions and the recognition of operational domain limits depending on connectivity, or providing sensing-base information to other vehicles, might require that the performance of connectivity is treated more specifically in the architecture.

4.9. Specificities of geo-fenced driving environments

Automated vehicules in geo-fenced driving environments (e.g. shuttles, pods), raise quite specific questions as regard to vehicle's regulation. These use cases are different from the developping automated passenger car's use case in various dimensions :

- critical situations' and events' identification requires in-site and case-by-case analysis ;
- responses can, parlty, be taylor-made to local critical situations and events, and not only involve the vehicle itself, but its driving environment (e.g. traffic flows separation or management on the shuttle's itinerary) ;
- connectivity and supervision plays a much more critical role in autoated functions, critical situations, and responses to them.

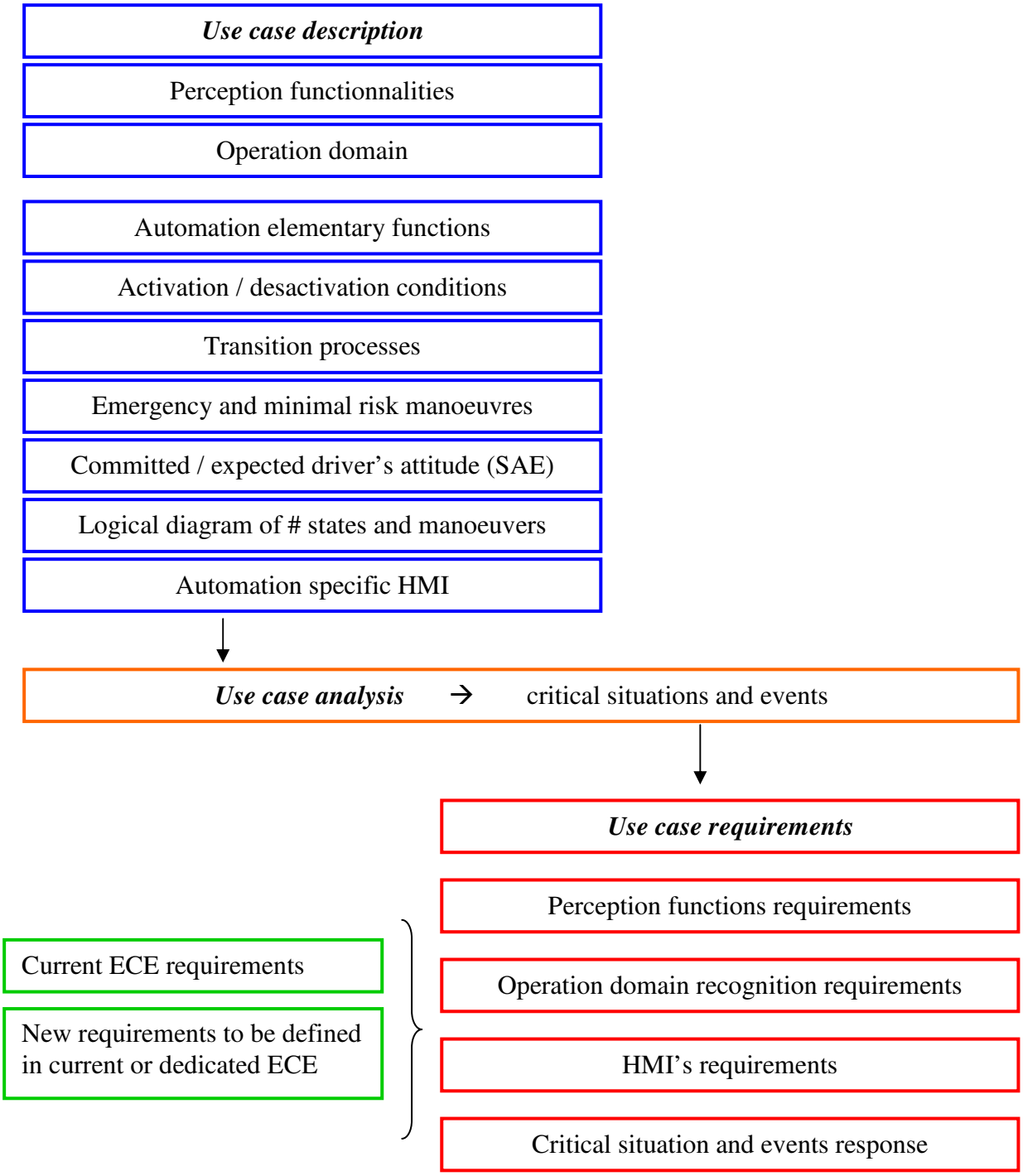
5. Proposed schematic architecture

The following graphs intend to present the logic of the proposed regulation's architecture.

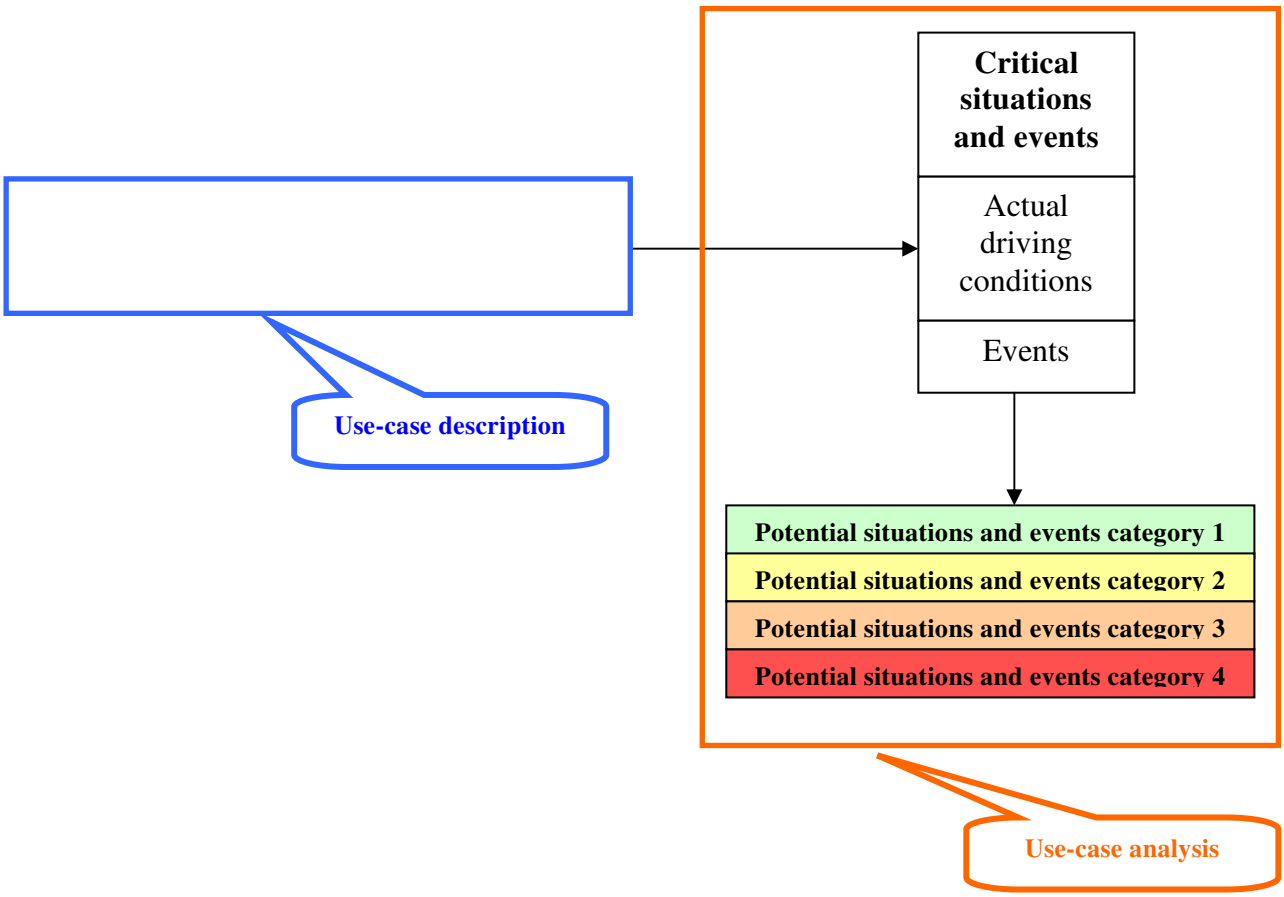
Regulation architecture = horizontal layer + vertical regulations

Horizontal layer = use-case description + use-case analysis + use-case requirements

The following graph summarizes the main building blocks of the regulation architecture.


Use case description
Perception functionnalities
Operation domain
Automation elementary functions
Activation / desactivation conditions
Transition processes
Emergency and minimal risk manoeuvres
Committed / expected driver's attitude (SAE)
Logical diagram of # states and manoeuvers
Automation specific HMI
Use case analysis → critical situations and events
Use case requirements
Perception functions requirements
Operation domain recognition requirements
HMI's requirements
Critical situation and events response
Current ECE requirements
New requirements to be defined in current or dedicated ECE

Focus on use case analysis and requirements



Use-case requirements

Use case # 1 (corresponding to committed drivers attitude level"x" SAE)				
Regulation domains	*Perception functions*	*Operation domain recognition functions*	*Automation HMI (driver's monitoring, environment info & warning, transition / handover requests)*	*Critical situations and events response functions (manoeuvers + specific HMIs) requirements*
Situations and events response category criticity # N1	Based on use-case's operation domain	Based on use-case's driving environment limits	Based on level "x" SAE of expected driver's attitude	Situations and events-specific
Situations and events response category criticity # N2				Situations and events-specific

Vertical regulation : current ECE reg (and new if necessary)

Non automatic functions
Steering (R79)
Braking (R13H)
Passive safety (R14, R16 etc...)
...
ADAS
AEB vehicle
AEB cycle
AEB pedestrian
ACC
...

Specific ECSR + MRM regulation

Critical situations and events response + minimum risk manoeuvres
Generic requirements
Use-case-specific requirements

6. Validation approaches and tools : preliminary refexions and open questions

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

6.1. Typology and temptative mapping of validation approaches

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

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

b. ***Risk assessement*** methods can, broadly speaking, either :
   - Follow ***no specific methodology***
   - Follow a ***declared methodology***
   - Follow a ***mandatory methodology***

c. ***Requirements*** towards the system could also, schematically, be defined gradually, from mere existence of a function, to a real performance level, as listed in chapter 5 above :
   - ***situation and event aknowledgment***:
   - situation and event ***response availability***
   - situation and event ***response functionnal description***
   - situation and event ***response required functionnalities***
   - situation and event ***response required performance***

d. It could also be useful to draw different levels of performance validation, depending on the ***involvment of "third parties***", especially public authorities, such as :
   - ***Declared*** performance (or existence or functionnalities)
   - ***Evidence-based*** performance (or existence or functionnalities)
   - ***Certified*** performance (or existence or functionnalities)
   - ***Tested*** performance (or existence or functionnalities)

e. The ***validation tools*** could also usefully distinguish :
   - ***Documentation screening or analysis***
   - ***Simulations***
   - ***Tests*** in real conditions ("one driver" or "drivers sample")

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

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

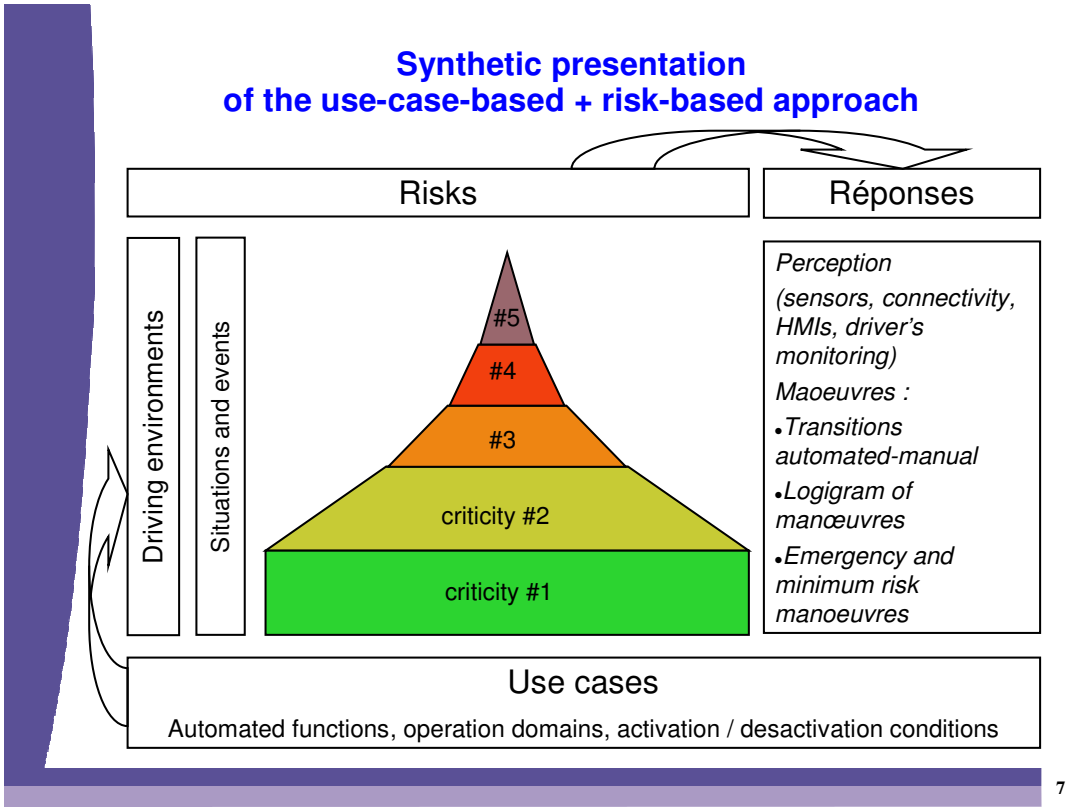
The following paragraphs propose to focus on three of the main typology parameters listed above, in order to elaborate first considerations of possible adequation between validation approaches and types of requirements.

The typology dimensions or parameters considered at this stage are :

- Requirements towards the system
  - Situation and event aknowledgment
  - Response availability
  - Response functionnal description
  - Response required functionnalities
  - Response required performance
- Level of verification :
  - (Self) declared
  - Evidence-based
  - Certified (by third party)
  - Tested (by public authority)
- Validation tools
  - Documentation screening or analysis
  - Simulations
  - Tests

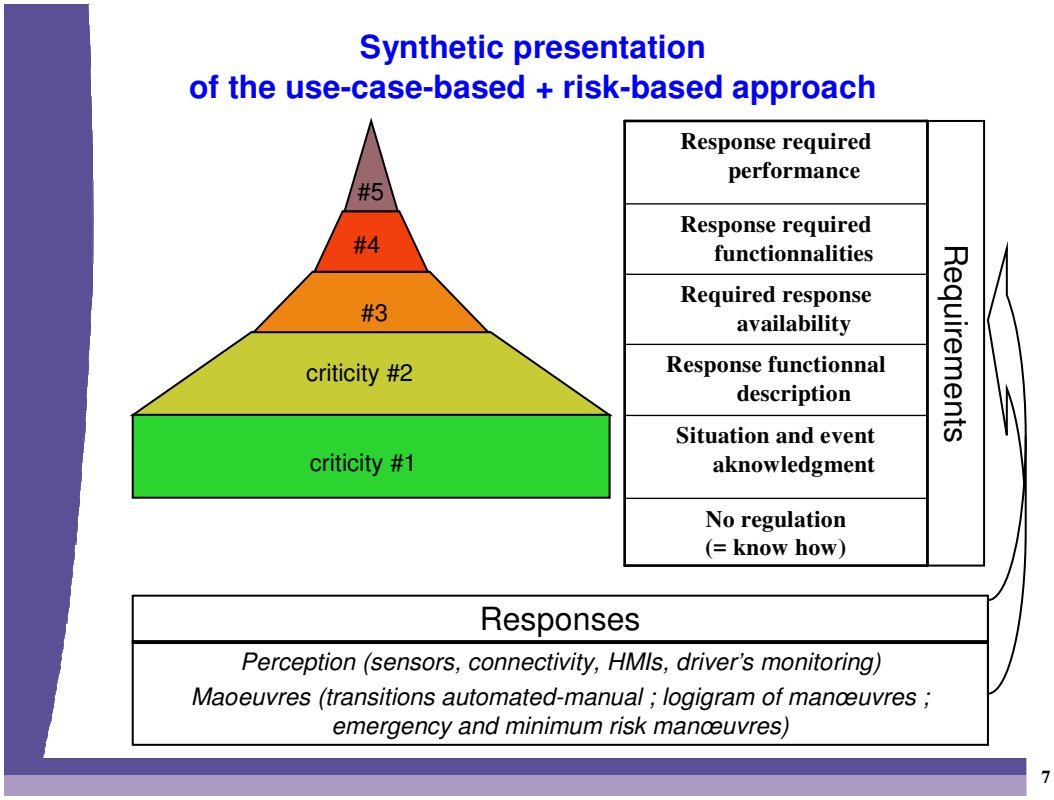
The following tables and graphs illustrate the proposed approach, pointing out the propotionnality between criticallity of identified situations and events on one hand, requirements and validation tools on the other hand.

Step 1 : use case description + risk analysis



Step 2 : proportionnate use-case requirements

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

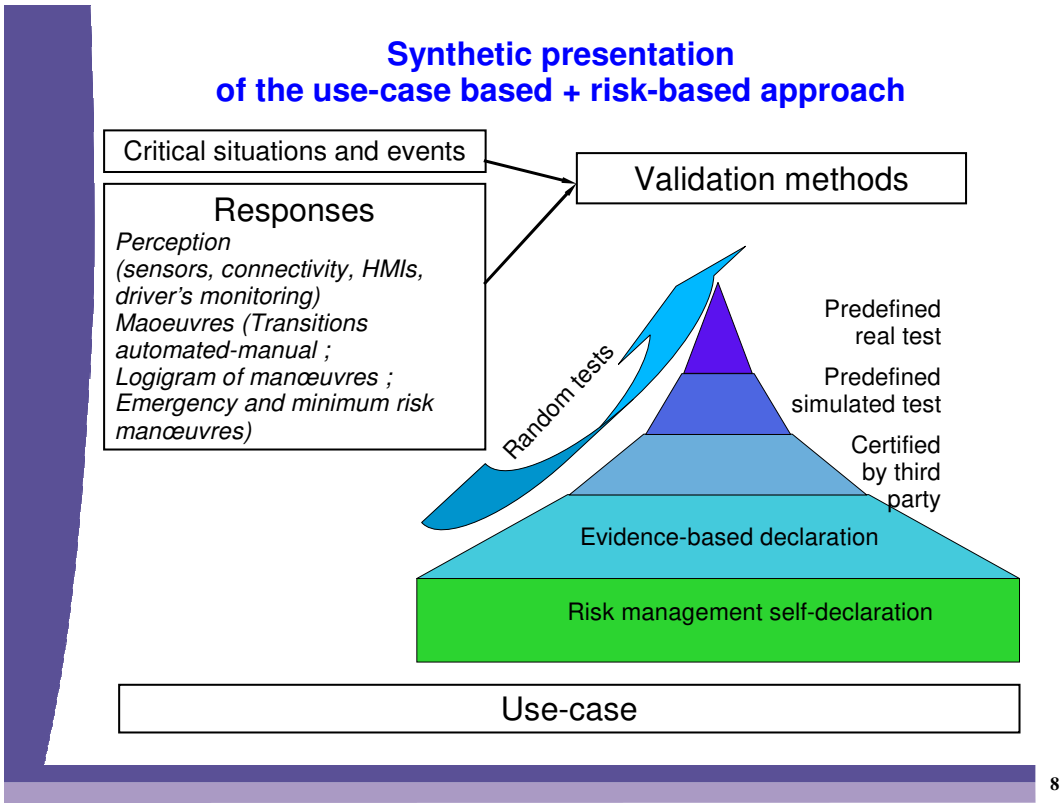


Step 3 : propotionnate validation methods

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

(see annex 4 for more detailled condiderations on the possible correspondance between requirements and verification / validation tools)

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



Example of a random draw for validation tools applied to, e.g. 10 sets of responses / requirements

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

Annexes

Annex 1 : regulation architecture's illustration on a use case

Annex 2 : correspondence with UNE-ECE on-going work : main sub-systems underlying on-going reflexions at WP29

Annex 3 : system tasks general requirements as recommended by UN-ECE WP29.

Annex 4 : correspondance between requirements and verification / validation tools)

Annex 5 : overview of litterature definition of systems, use cases, risk analysis and validation methods

Annex 1 : illustration on a use case

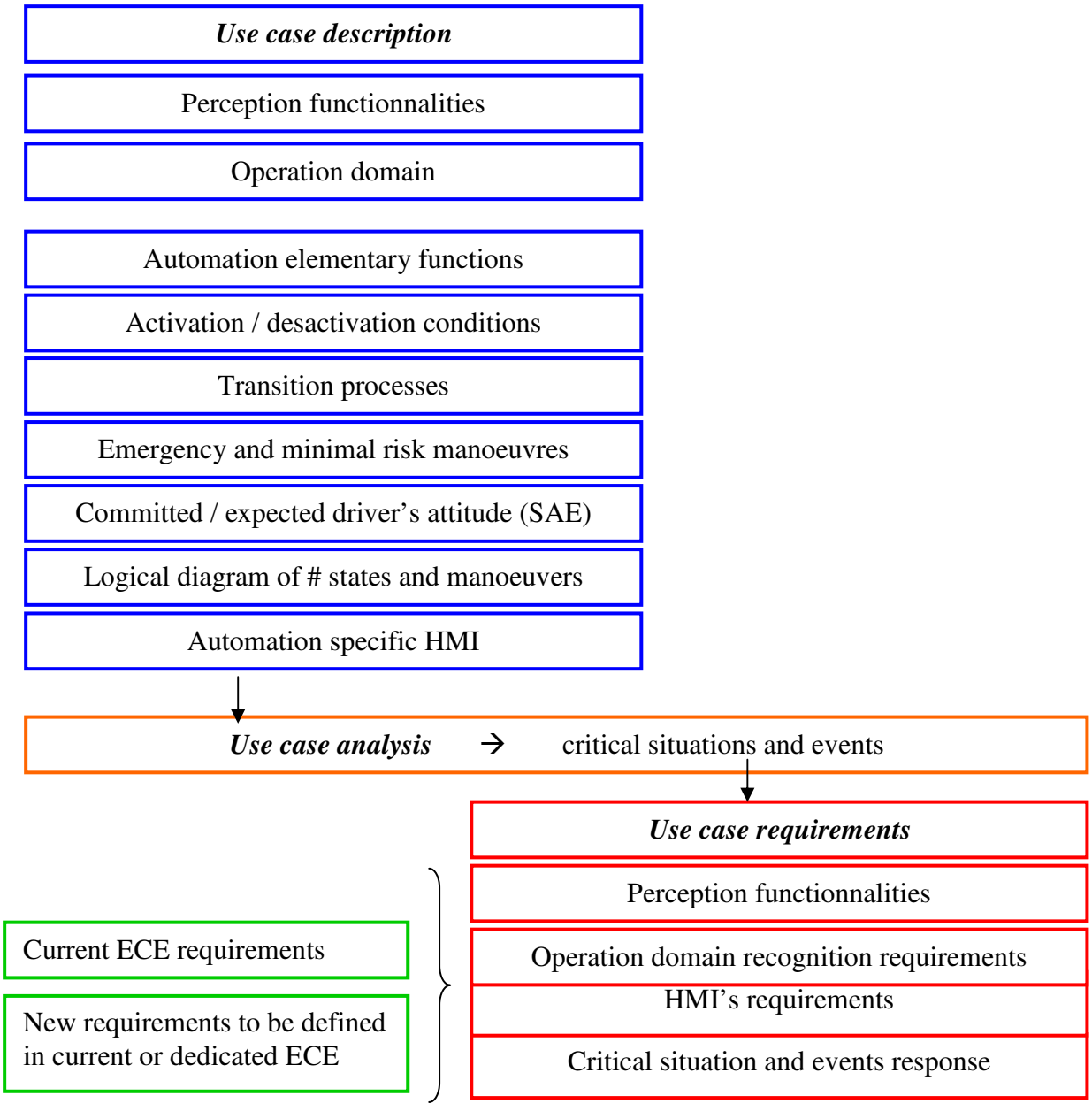
This annex illustrates the application of the regulation proposed "philosophy", architecture and systems tasks general requirements (as discussend in WP29 – ITS/AD – cf. Annex) to an illustrative use case, taking into account the above requirements on system's tasks.

The illustrative use case is defined as a combination of :

- specified driving environments or scenarios or "operational design domain"
- automation functionnalities or "elementary functions" (manœuvre(s) performed by the system under normal conditions)
- activation / desactivation conditions and duration under normal conditions
- expected systems / drivers' tasks sharing (cf. SAE level)

An illustrative logigram of manoeuvres is presented bellow.

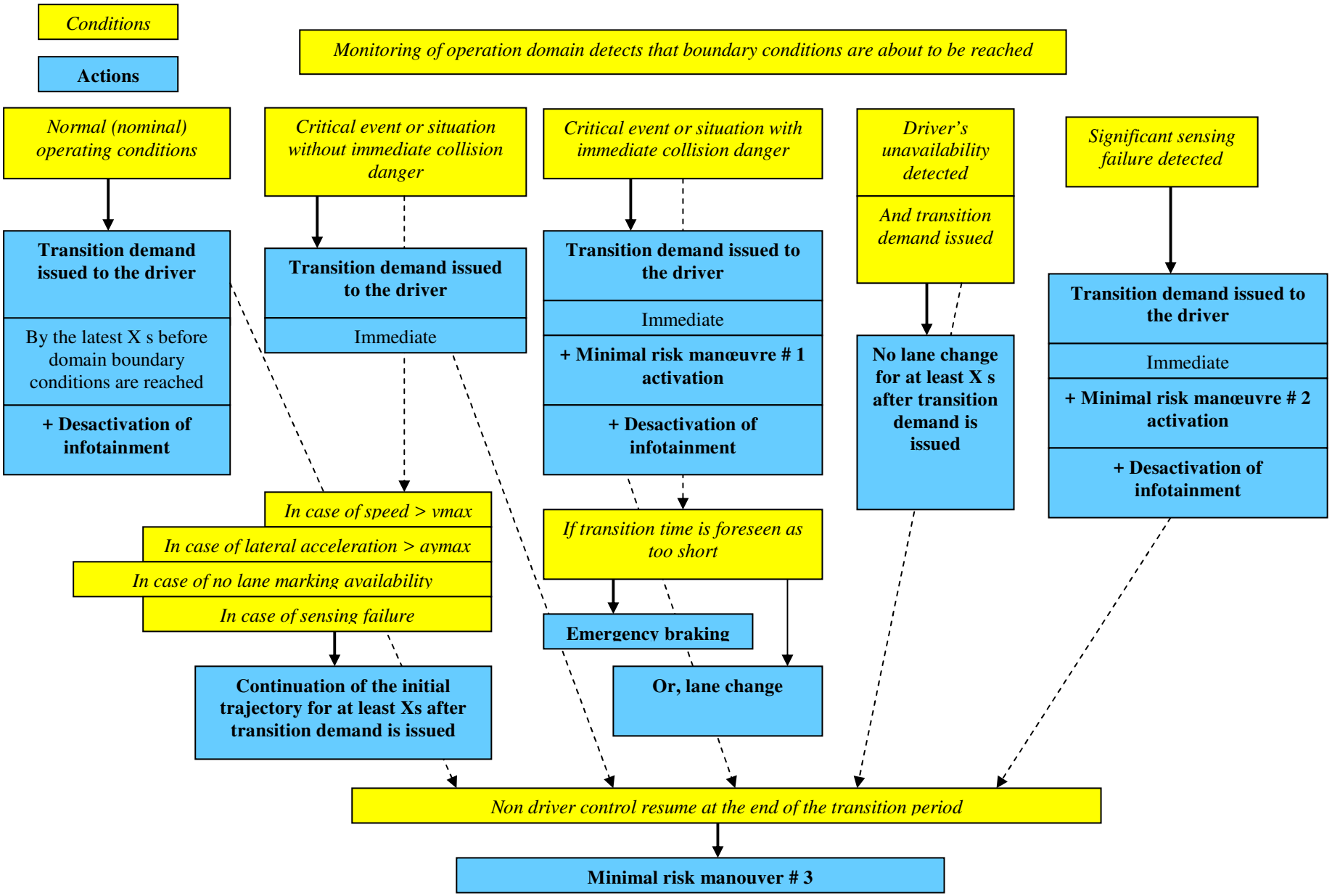
The regulation architecture is presented as suggested above, i.e. :



Use case description

Operation domain segmentation	**Operation domain # 1**	**Operation domain # 2**	**Operation domain # 3**	**Operation domain # 4**
Use-case type	***ACSF level E***	***Traffic jam assist without lane change***	***Urban chauffeur***	***Valet parking***
Operation type	Highway - fluid	Highway - congested	Congested dense city	Parking
Speed range	90 – 130 km/h	< 50 km/h	< 30 km/h	< 10 km/h
Day / Night	Day	Day and Night	Day	Day and Night
Weather / visibility	> 50 m	All	All	All
Automated elementary functions	Longitudinal + Lateral	Longitudinal + Lateral	Longitudinal + Lateral	Longitudinal + Lateral
Activation / desactivation conditions (permit activation)	• ***Function activation*** by the driver when the vehicle proposes • ***Function desactivation*** by the driver at anytime, including during a manoeuver • ***Function desactivation*** by the system outside operation domain • ***Manoeuver activation*** by the driver when triggering conditions are fullfilled • ***Manoeuver override*** by the driver at any time • ***Manoeuvre abortion*** by the system via a specific critical situation and event response ***(CSER # 1)***	• ***Function activation*** by the driver when the vehicle proposes • ***Function desactivation*** by the driver at anytime, including during a manoeuver • ***Function desactivation*** by the system outside operation domain • ***Manoeuver activation*** by the driver when triggering conditions are fullfilled • ***Manoeuver override*** by the driver at any time • ***Manoeuvre abortion*** by the system via a specific critical situation and event response ***(CSER # 2)***	• ***Function activation*** by the driver when the vehicle proposes • ***Function desactivation*** by the driver at anytime, including during a manoeuver • ***Function desactivation*** by the system outside operation domain • ***Manoeuver activation*** by the sdriver when triggering conditions are fullfilled • ***Manoeuver override*** by the driver at any time • ***Manoeuvre abortion*** by the system via a specific critical situation and event response ***(CSER # 3)***	• ***Function activation*** by the driver when the vehicle proposes • ***Manoeuver activation*** by the system when triggering conditions are fullfilled • ***Function desactivation*** by the system outside operation domain • ***Function desactivation*** by the driver at anytime, including during a manoeuver • ***Manoeuver override*** by the driver at any time • ***Manoeuvre abortion*** by the system via a specific event and critical situation and event response ***(CSER # 4)***
Driving tasks sharing level (SAE)	Level 3	Level 2	Level 3	Level 4
Logigram of manœuvres, including transition manoeuvres	Cf. bellow	Cf. bellow	Cf. bellow	Cf. bellow

Logigram of manoeuvres, including transition manoeuvres : illustrative example for operation domain # 1 (Highway – fluid, level 3)



Use case analysis

The following table illustrates a possible list of parameters and values that could be used, in order to identify potential critical situations and events. The priorisation of these situations and events could use a risk assessment method, such as ISO 26262. The example bellow is e.g. for a focus on operation domain # 1 “highway, fluid”.

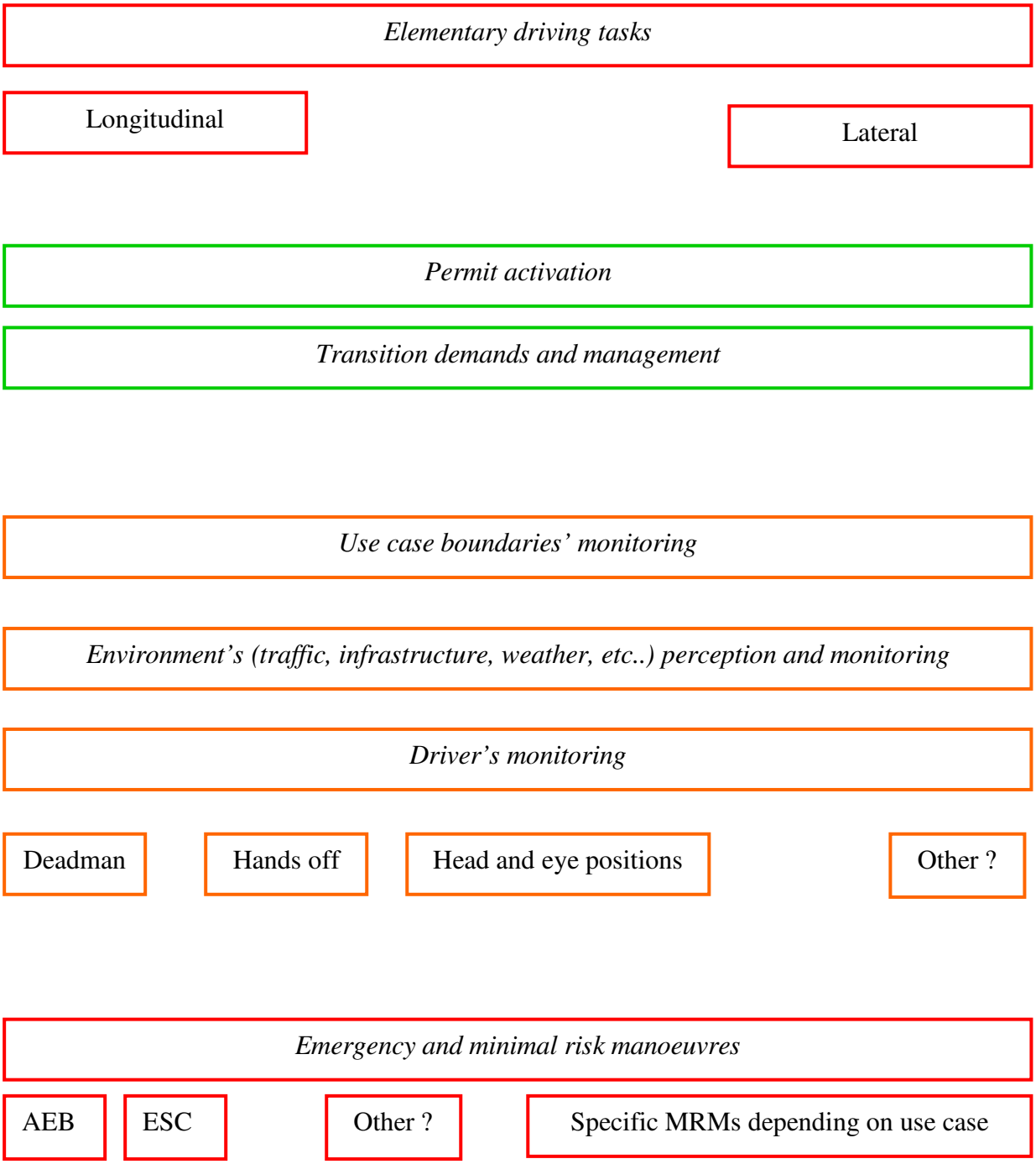
Situation and event attribute	***Possible values***
Driving objective	Lane keep Lane change
Driving infrastructure environment	2 * X lanes, separated driving ways, no entry / exit End of lane / lane merge Exit Merging ramp
Driving traffic environment	Fluid Dense
Driving weather / light conditions	Normal conditions Reduced visibility (< 100 m) Low angle light ....
Critical events and situations (types)	Lane marking unavailability for sensing Obstacle, debris Road works Idle animals Local slippery area Vehicle stopped People on road Emergency intervention ....

Use case requirements

Use case description					
Operation domain segmentation	***Operation domain # 1***	***Operation domain # 2***	***Operation domain # 3***	***Operation domain # 4***	***Overall requirement***
Operation type	*Highway - fluid*	*Highway - congested*	*Congested dense city*	*Parking surroundings*	
Speed range	*90 – 130 km/h*	*< 50 km/h*	*< 30 km/h*	*< 10 km/h*	
Automated elementary functions	*Longitudinal + Lateral*	*Longitudinal + lateral*	*Longitudinal + Lateral*	*Longitudinal + Lateral*	
Driving tasks sharing level (SAE)	*Level 3*	*Level 2*	*Level 3*	*Level 4*	
Use case requirements					
Drivers monitoring functions	To be defined in ACSF R79	Hands on defined in ACSF R79	To be defined in ACSF R79	None ? To be defined	Depending on the operation domain
Operation domain monitoring functions	As of the above operation domain limits	As of the above operation domain limits	As of the above operation domain limits	As of the above operation domain limits	
Specific functions like ADAS (examples)	• AEB static vehicle • AEB moving vehicle • ACC • LP	• AEB static vehicle • AEB moving vehicle • LPA	• AEB moving vehicle • AEB pedestrian • AEB cyclist • ACC • LP	• AEB pedestrian • ACC • LP	• Sum of the ADAS quoted
Critical situation and event responses	• *Depending on criticity level (1 to 5)*	• *Depending on criticity level (1 to 5)*	• *Depending on criticity level (1 to 5)*	• *Depending on criticity level (1 to 5)*	

Annex 2 : main sub-systems underlying on-going reflexions at WP29

The following graph simply presents the main subsystems underlying on-going reflexions on the future of automated driving regulation at WP29 (cf. ITS/AD meeting 9-10 march 2017).



Annex 3 : system tasks general requirements as recommended by UN-ECE WP29

This part summarizes general requirements towards the system, as issued by ITS/AD at its ad'hoc meeting 9-10 march 2017.

	Object and Event Detection and Response (OEDR) by the driver		Object and Event Detection and Response (OEDR) by the system		
	Monitor by Driver	Monitor by Driver	Monitor by System (Return to Driver Control on System Request)	Monitor by System Full Time under defined use case	Monitor by System only
Ref. SAE Level (J3016)	**1**	**2**	**3**	**4**	**5**
Outline of System Tasks	• Longitudinal or lateral control.	• Longitudinal and lateral control.	• All dynamic driving tasks within its designed use-case * or will otherwise transition to the driver offering sufficient lead time (driver is fallback). • Drives and monitors (specific to the use-case) the environment. • Detects system limits and issues a transition demand if these are reached	• Any situations in the concerned use case (fallback included). • May however request a takeover if the use case boundaries are reached (e.g. motorway exit).	• Any situations on all road types, speed ranges and environmental conditions.
Vehicle System Tasks	1. Execute either longitudinal (acceleration/braking) or lateral (steering) dynamic driving tasks when activated. The system is not able to detect all the situations in the use case. 2. System deactivated immediately at the request of the driver	1. Execute longitudinal (accelerating, braking) and lateral (steering) dynamic driving tasks when activated. The system is not able to detect all the situations in the use case. 2. System deactivated immediately upon request by the human driver. 3. No transition demand as such, only warnings. 4-A driver availability	1. Execute longitudinal (accelerating/braking) and lateral (steering) portions of the dynamic driving task when activated. Shall monitor the driving environment for operational decisions when activated. 2. Permit activation only under conditions for which it was designed. System deactivated immediately at the request of the driver. However the system may momentarily delay deactivation when immediate human takeover could compromise safety 3. System automatically deactivated only after requesting the driver to take-over with a sufficient lead time; may − under	1. Execute longitudinal (accelerating/braking) and lateral (steering) portions of the dynamic driving task when activated. Shall monitor the driving environment for any decisions happening in the use case (for example Emergency vehicles). 2 Permit activation only under conditions for which it was designed. System deactivated immediately at the request of the driver. However the system may momentarily delay deactivation when immediate human takeover could compromise safety	1. Monitor the driving environment 2. Execute longitudinal (accelerating/ braking) and lateral (steering) 3. Execute the OEDR subtasks of the dynamic driving task-human controls are not required in an extreme scenario 4. System will transfer the vehicle to a minimal risk condition

	Object and Event Detection and Response (OEDR) by the driver		Object and Event Detection and Response (OEDR) by the system		
	Monitor by Driver	Monitor by Driver	Monitor by System (Return to Driver Control on System Request)	Monitor by System Full Time under defined use case	Monitor by System only
		recognition function (could be realized, for example, as hands-on detection or monitoring cameras to detect the driver's head position and eyelid movement etc.) could evaluate the driver's involvement in the monitoring task and ability to intervene immediately.	certain, limited circumstances − transition (at least initiate) to minimal risk condition if the human driver does not take over. It would be beneficial if the vehicle displays used for the secondary activities were also used to improve the human takeover process. 4. Driver availability recognition shall be used to ensure the driver is in the position to take over when requested by the system. Potential technical solutions range from detecting the driver's manual operations to monitoring cameras to detect the driver's head position and eyelid movement. 5. Emergency braking measures must be accomplished by the system and not expected from the driver (due to secondary activities)	3. Shall deactivate automatically if design/boundary conditions are no longer met and must be able to transfer the vehicle to a minimal risk condition. May also ask for a transition demand before deactivating. 4. Driver availability recognition shall be used to ensure the driver is in the position to take over when requested by transition demand. This can however be lighter solutions than for level 3 because the system is able to transfer the vehicle to a minimal risk condition in the use case. 5. Emergency braking measures must be accomplished by the system and not expected from the driver (due to secondary activities)	

Annex 4 : some condiderations on the possible correspondance between requirements and verification / validation tools)

The following table presents preliminary considerations underlying the possible relevance of different validation principles or tools suggested above.

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

Level of criticity	*Type of requirement*	*Level of verification*	*Validation input / tools*
Criticity level 0	No regulation (= know how)		
Criticity level 1	Situation and event aknowledgment	Self-declaration or Evidence based	Documentation Simulations
Criticity level 2	Response functionnal description	Self-declaration or Evidence based	Documentation Simulation
Criticity level 3	Required response availability	Self-declaration or Certified or Certified	Documentation
Criticity level 4	Response required functionnalities	Self-declaration Evidence based or Certified	Documentation Simulations
Criticity level 5	Response required performance	Evidence based or Certified or Tested	Simulation Tests

Annex 5 : overview of litterature related to
definition of systems, use cases description, risk analysis and validation methods

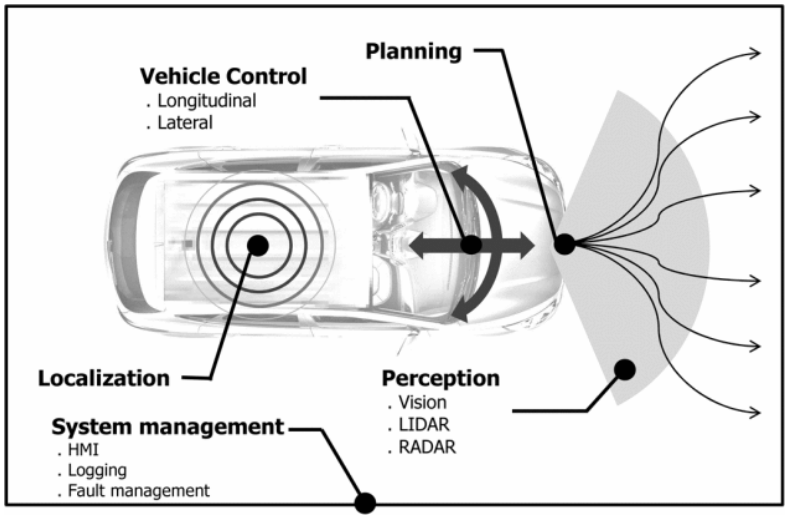
This annex provides a synoptic overview of references on which the approache proposed in this document have been build upon. These references are presented bellow in a schematic form, focusing on concepts, and, as much as possible, illustrated though graphs.

This annex is organised in 4 parts :

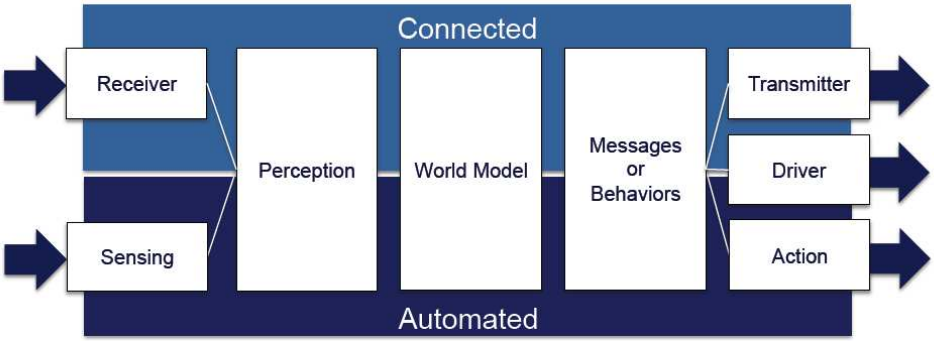
- A.5.1. Definitions of systems and functions
- A.5.2. Use case description
- A.5.3. Risk analysis methods
- A.5.4. Requirements and validation concepts

A.5.1. Definition of systems and functions

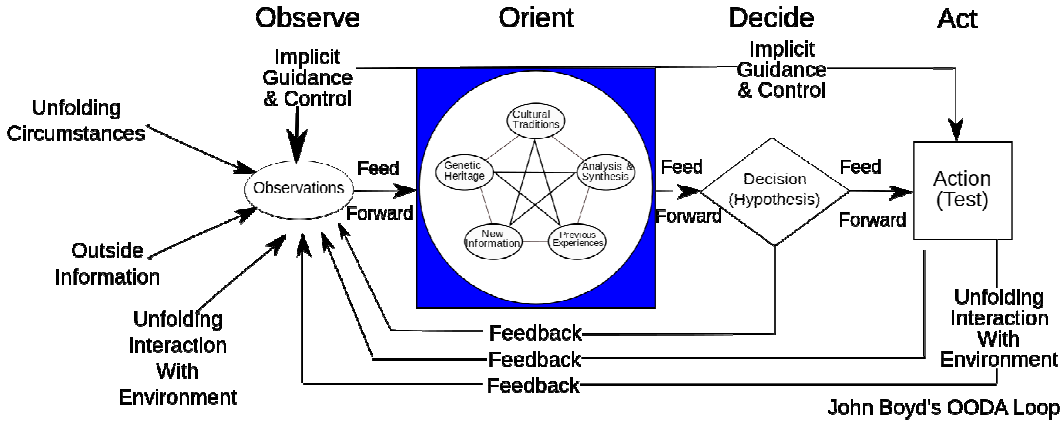
- ***IIEE, 2015***



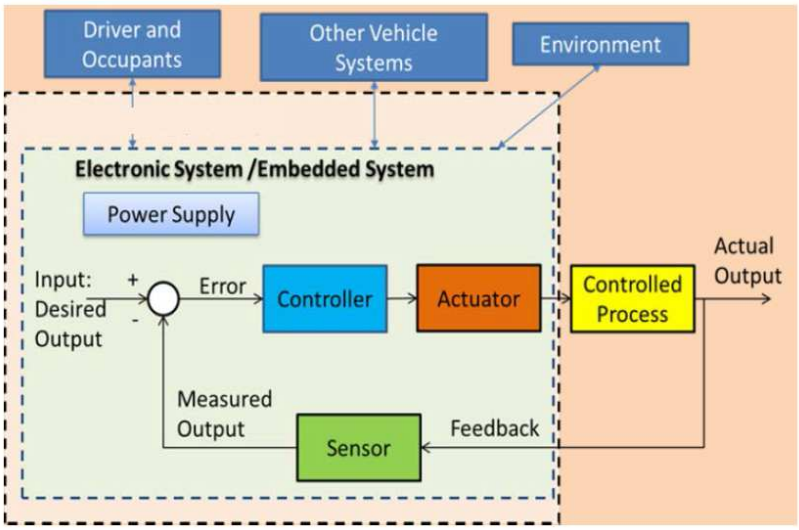
- ***Automated, Connected, and Electric Vehicle Systems. Expert Forecast and Roadmap for Sustainable Transportation, Steven Underwood, 2014***



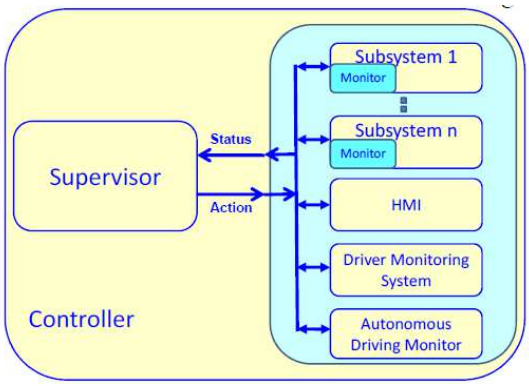
- ***The OODA loop, John Boyd, 1960***



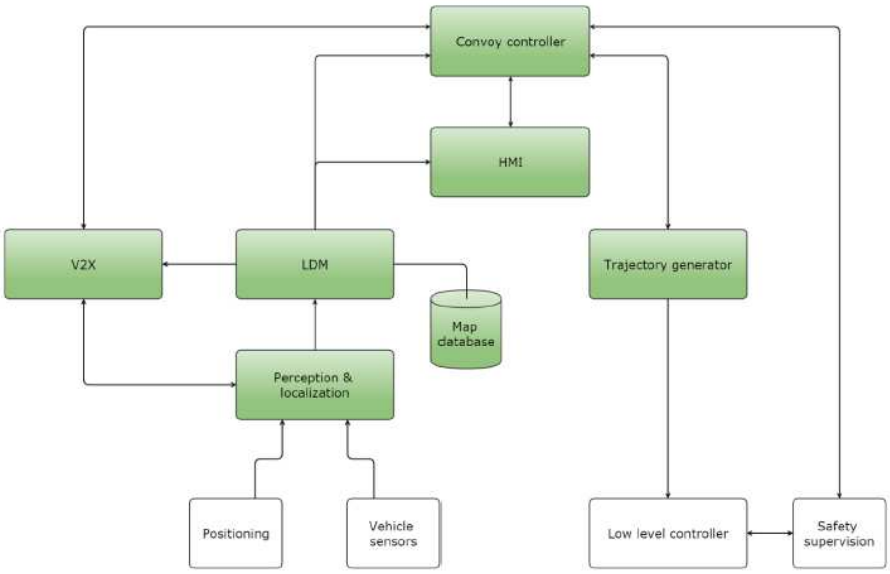
- ***Functional Safety Analysis of Automated Vehicle Lane Centering Control Systems, Brewer and Najm, Volpe National Transportation Systems Center, 2015***



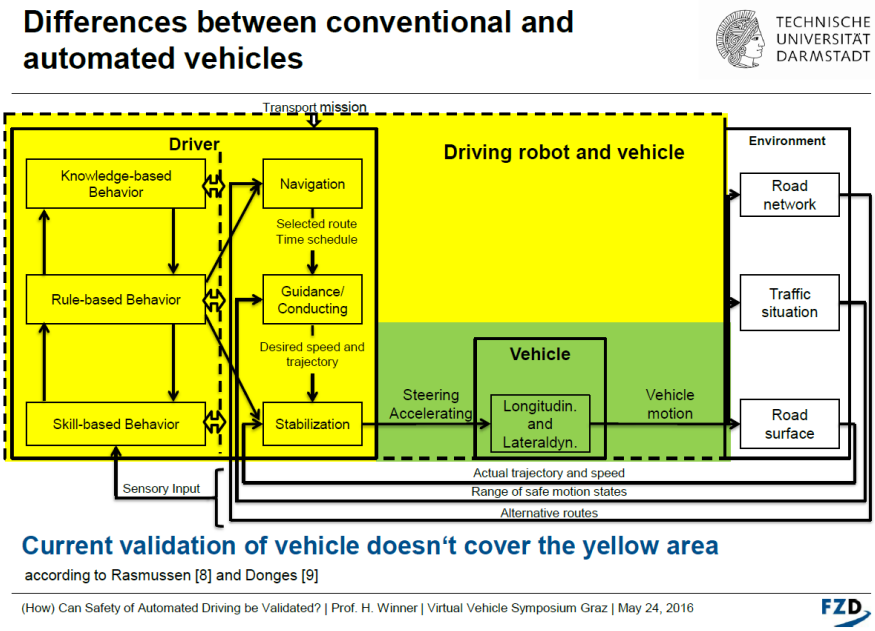
- ***Safety Strategy for Autonomous Systems, Debouk, Czerny, D'Ambrosio & Joyce, Critical Systems Labs***



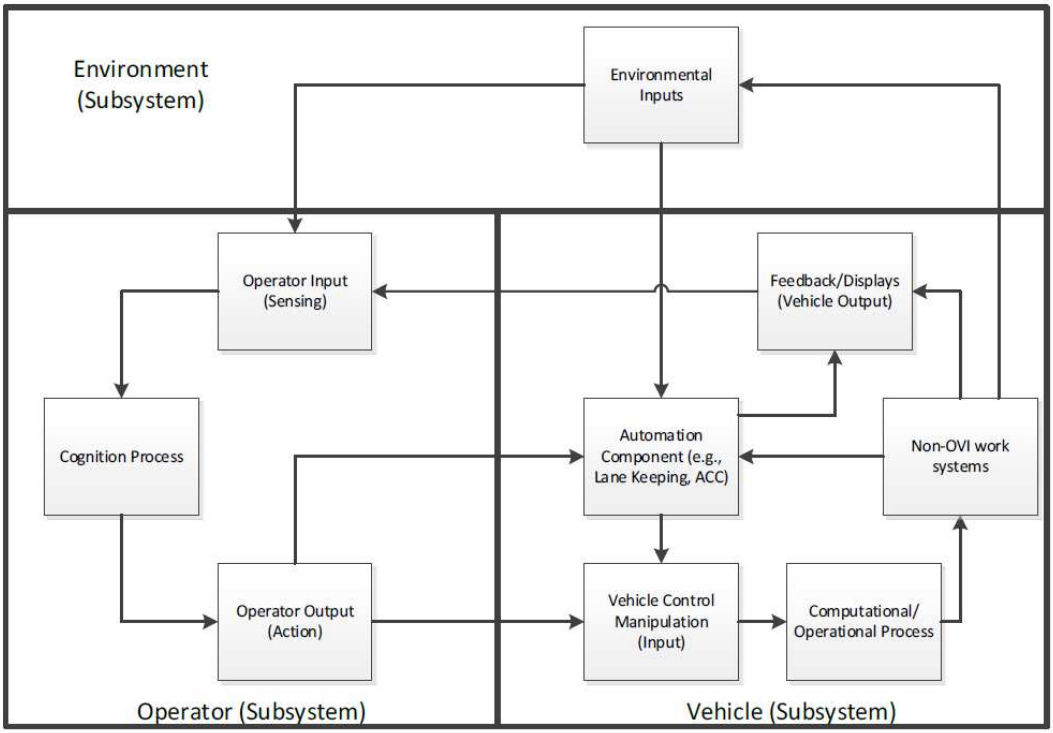
- ***Prototype validation report and performance analysis; Martionoli, Berg et al., 2016***



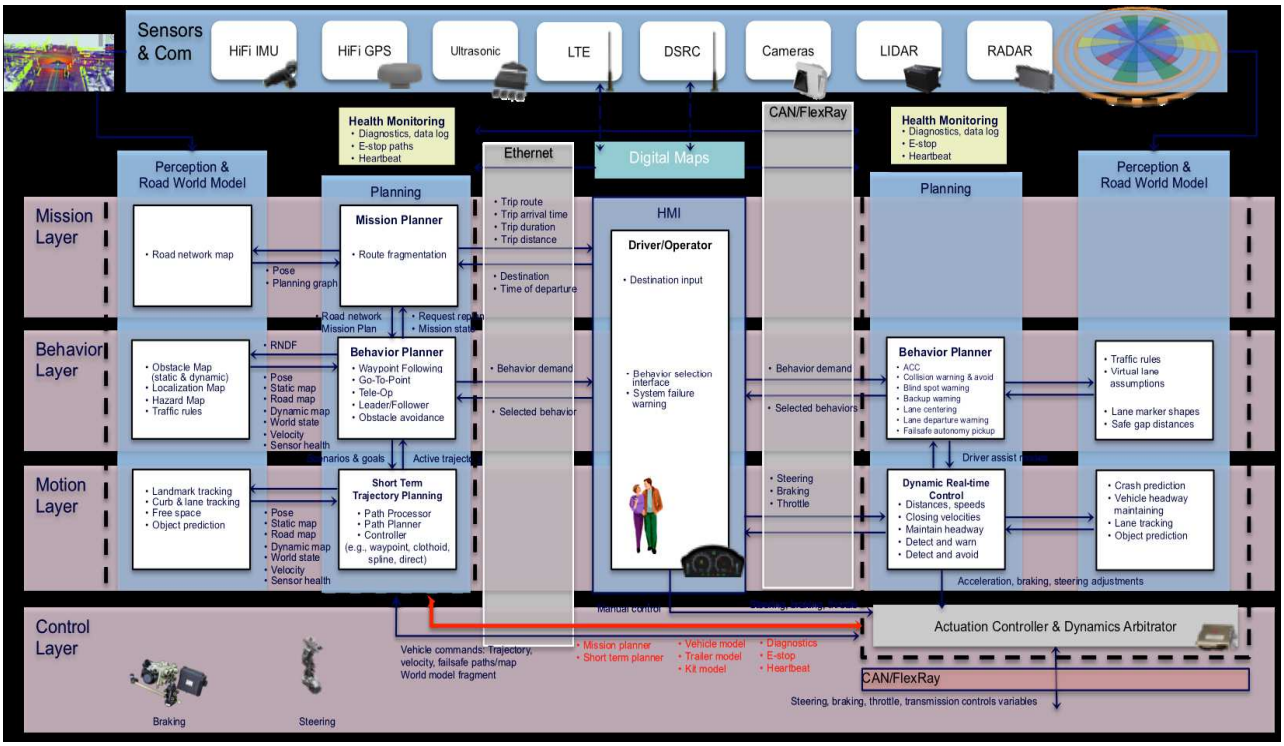
- ***(How) Can Safety of Automated Driving be Validated ? Winner, Wachefeld, Junnietz, Darmstadt University, 2016***



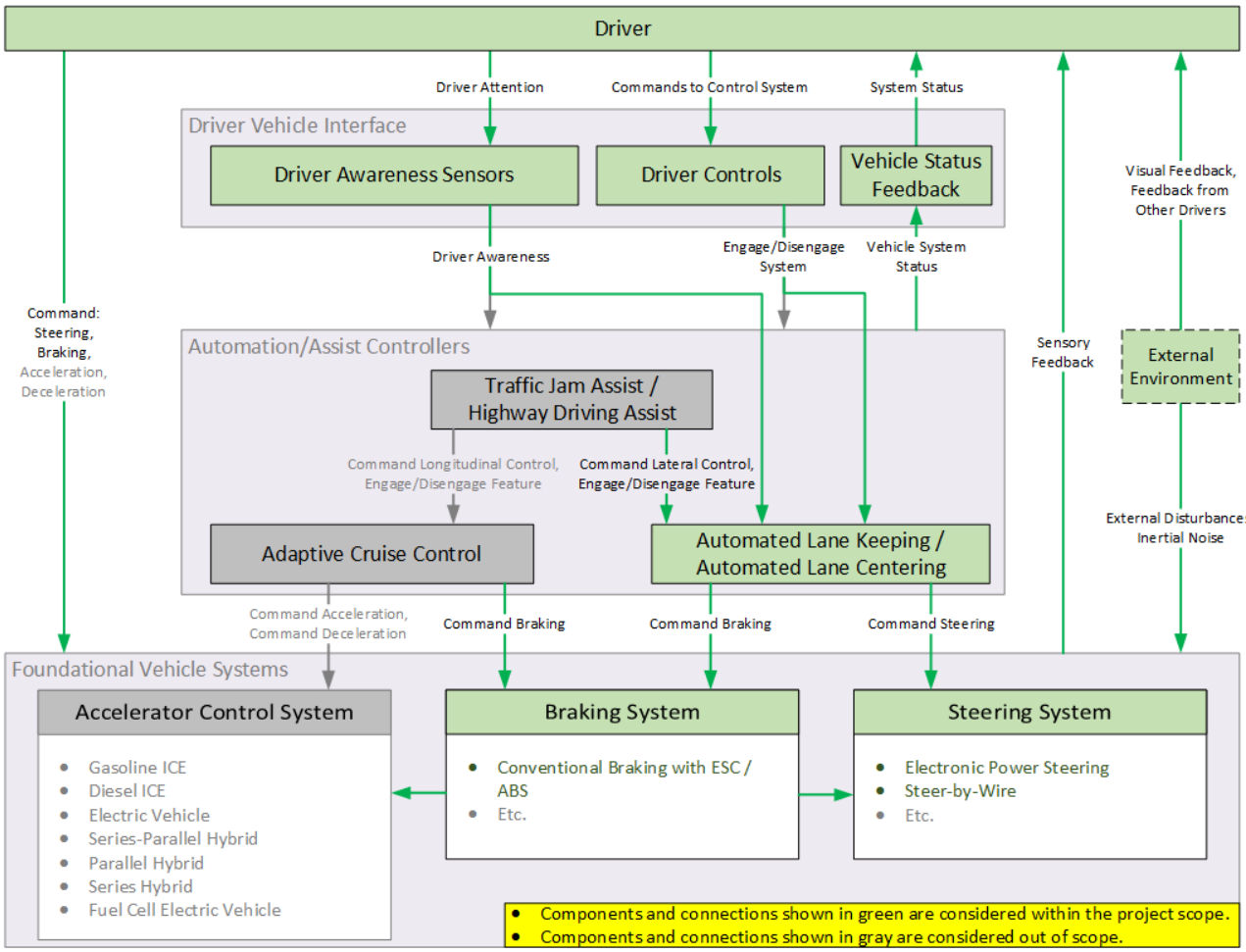
- ***Human Factors Evaluation of Level 2 And Level 3 Automated Driving Concepts, Concepts of Operation, NHTSA, 2014***



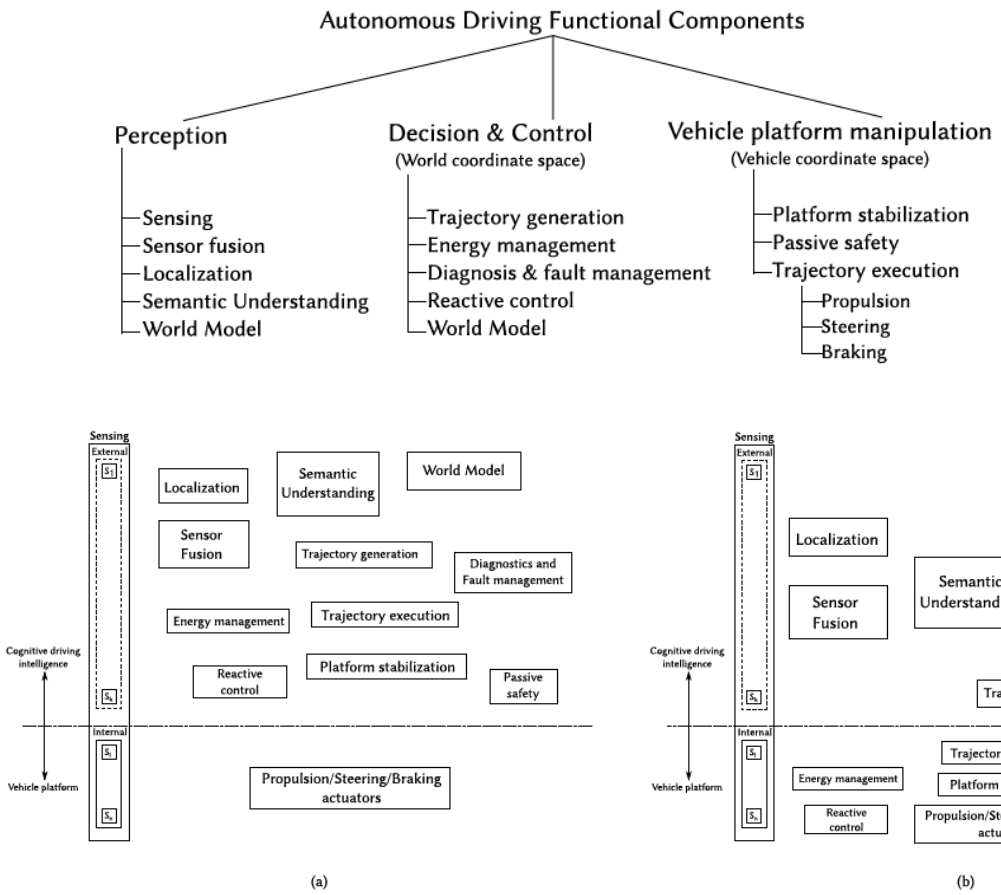
- ***Automated, Connected, and Electric Vehicle Systems. Expert Forecast and Roadmap for Sustainable Transportation, Steven Underwood, 2014***



- ***Functional Safety Analysis of Automated Vehicle Lane Centering Control Systems, SAE & Volpe centre, 2015***

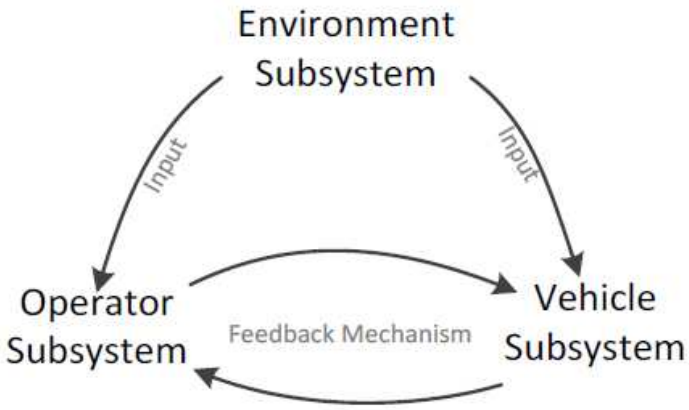


- ***A functional architecture for autonomous driving, Behere, Törngen, 2015***

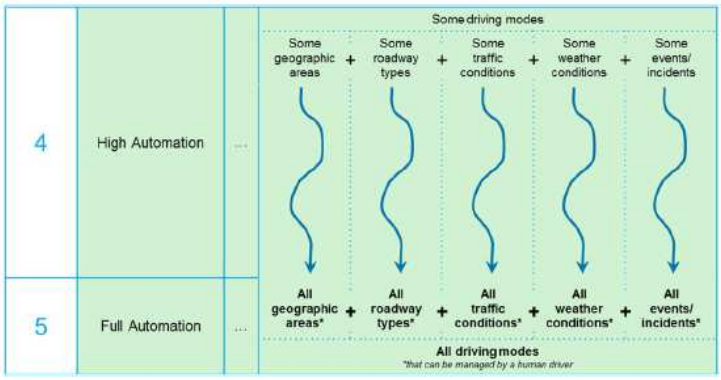


A.5.2. Use case description

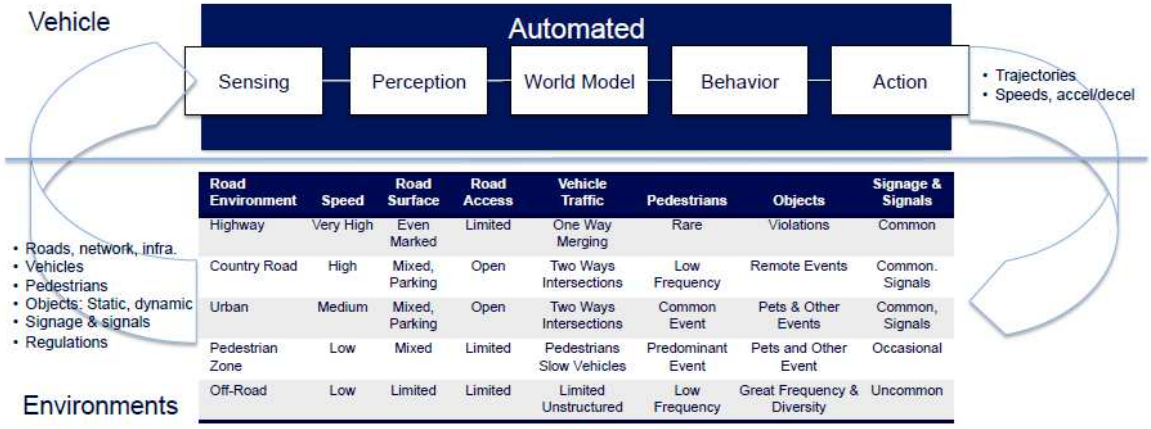
- ***Human Factors Evaluation of Level 2 And Level 3 Automated Driving Concepts Concepts of Operation ; NHTSA ; 2014***



- ***Automation driving modes and driving contexts, International Transport Forum, 2015***



- ***Automated, Connected, and Electric Vehicle Systems. Expert Forecast and Roadmap for Sustainable Transportation, Steven Underwood, 2014***

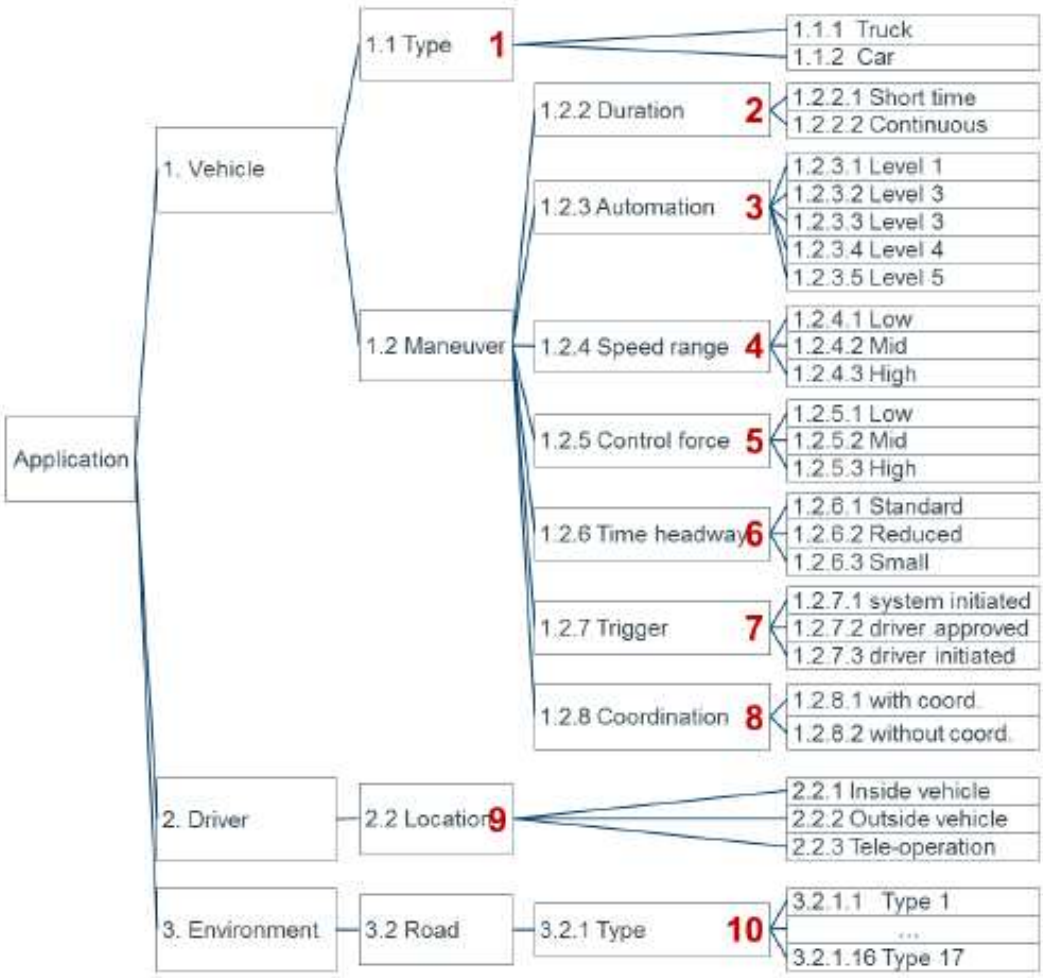


Road Environment	Speed	Road Surface	Road Access	Vehicle Traffic	Pedestrians	Objects	Signage & Signals
Highway	Very High	Even Marked	Limited	One Way Merging	Rare	Violations	Common
Country Road	High	Mixed, Parking	Open	Two Ways Intersections	Low Frequency	Remote Events	Common. Signals
Urban	Medium	Mixed, Parking	Open	Two Ways Intersections	Common Event	Pets & Other Events	Common, Signals
Pedestrian Zone	Low	Mixed	Limited	Pedestrians Slow Vehicles	Predominant Event	Pets and Other Event	Occasional
Off-Road	Low	Limited	Limited	Limited Unstructured	Low Frequency	Great Frequency & Diversity	Uncommon

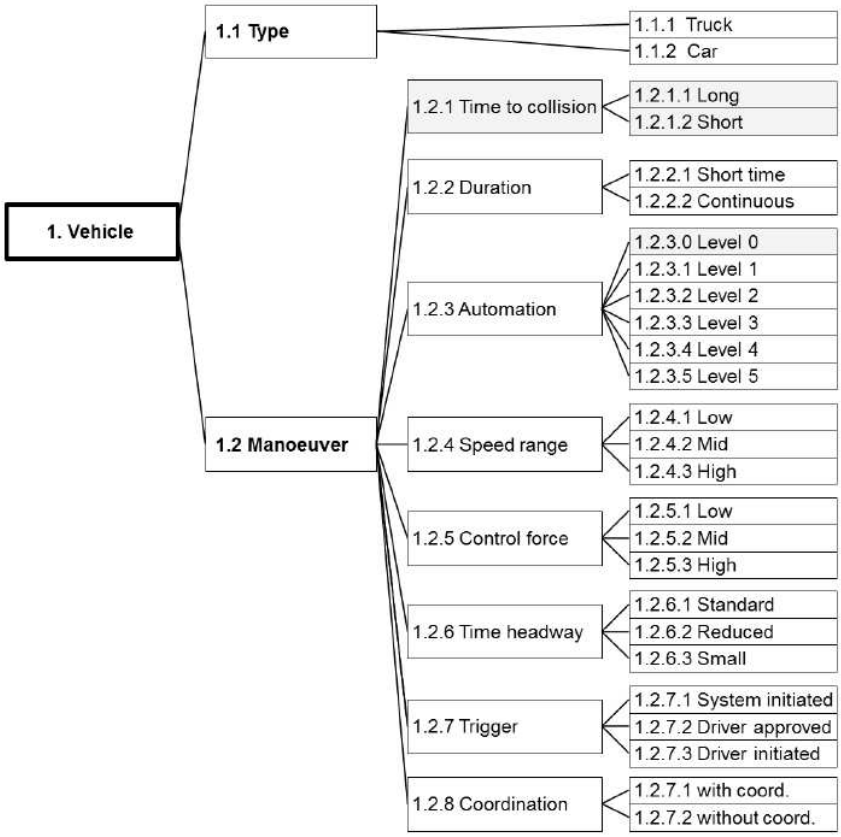
- ***Principles of Operation, Comprehensive definitions for automated driving and ADAS ; Gasser, Frey, Seeck & Auerswald***

Principle of Operation A: Informing and warning	Principle of Operation B: Continuously automating	Principle of Operation C: temporarily intervening in accident-prone situations
Only indirect influence on vehicle guidance via the driver. 1. Status information 2. Warning (abstract hazard) 3. Warning (concrete hazard)	Take direct influence on vehicle guidance (conscious activation by the driver – divided responsibilities in execution of the dynamic driving task). Always overrideable.	Preventive machine intervention in case of negative situation prediction. Either: I. driver as controller does not react conform to expectation or is inaccessible II. in accident-prone situations drivers/ controllers cannot handle due to performance limitations

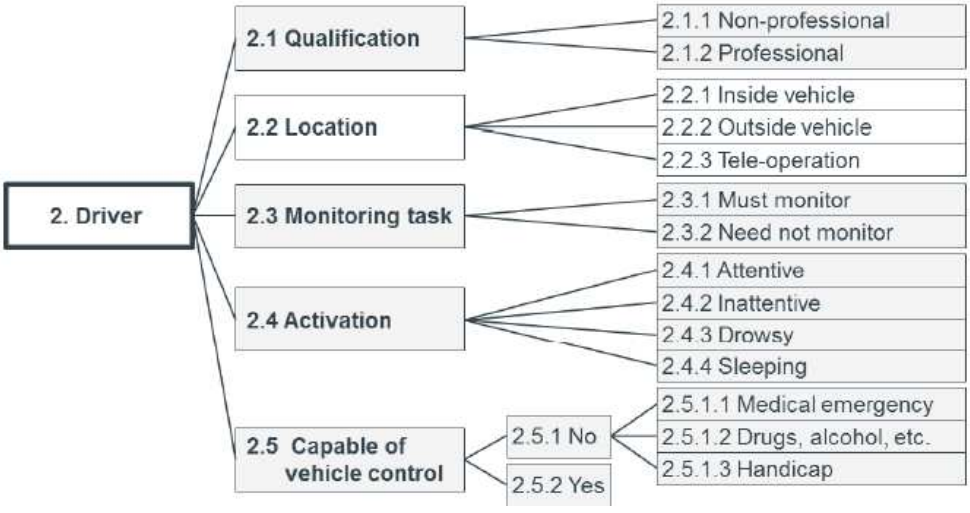
- ***Autonomous Driving - System Classification and Glossary ; Adaptive Project, 2015***
  - ***General architecture of use cases***



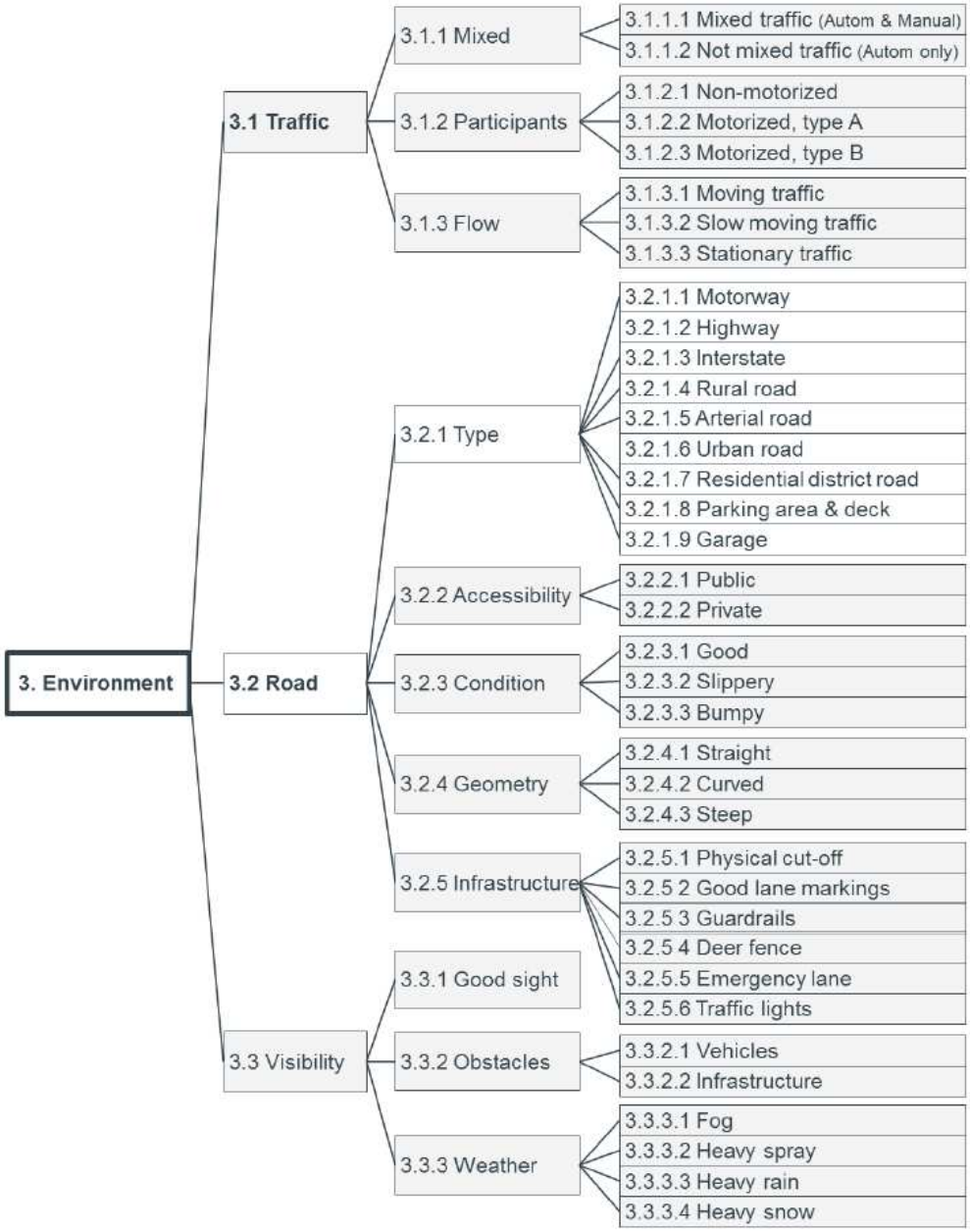
- ***Vehicle attributes***



- ***Driver tasks***



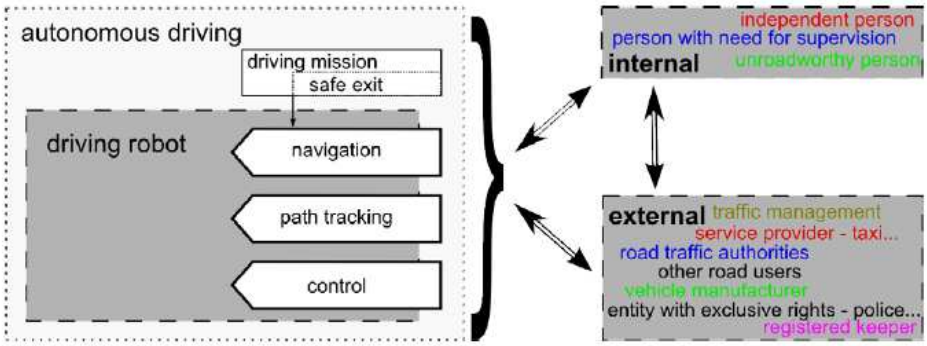
- ***Environment characteristics***



- ***Use case typology***

	Exemplary function	*Maneuver automation*	*Road type*	*Maneuver duration*	*Maneuver velocity*	*Maneuver control force*	*Maneuver Time headway*	*Maneuver trigger*	*Maneuver coordination*	*Driver location*	*Vehicle type*
1	Cruise Control	1	1, 5- 9	long	high	Low	n.a.	driver initiated	no	inside	car truck
2	Adaptive Cruise Control						standard				
3	Lane Keeping Assistance, Type II			long							
4	Active Lane Change Assistance			short							
5	Combined ACC and LKA, Type II			long			standard				
6	Active Traffic Light Assistance		10	short	mid						
7	Narrowing Assistance		8-11	long			n.a.				
8	Construction Site Assistance		4				standard				
9	Highway Assistance	2	1,5 - 7	long	high						
10	Overtaking Assistance			short							
11	Traffic Jam Assistance			long	mid						
12	Parking Assistance with steering	1	11-13	short	low	high	n.a.				car
13	Parking Assistance with steering and accelerating/braking	2								outside	
14	Key Parking										
15	Tele Operated Driving - Urban		8 - 12	long	mid		standard			tele	
16	Highway Chauffeur	3	1,5		high			driver approved		inside	car truck
17	Overtaking Chauffeur			short							
18	Traffic Jam Chauffeur			long	mid			driver initiated			
19	Platooning				high		small		yes		
20	Highway Pilot	4	1,5	long	high					inside	car truck
21	Overtaking Pilot			short				system initiated			
21	Traffic Jam Pilot			long	mid			driver initiated			
22	Driverless Valet Parking		14		low			System initiated		n.a.	car
23	Urban Robot Taxi		8-12		mid						car
24	Automated Mining Vehicles		16							n.a.	truck
25	Automated marshalling of trucks		17		low						
26	Universal Robot Taxi	5	1-14		high						car

- ***Use cases for Autonomous Driving; Wachenfeld & Winner, 2014***



Selected characteristics to describe the Use Cases

Characteristic A: Type of Occupant

1. *no cargo and no person*
2. *for transportation approved cargo*,
3. *person/s with agreed destinations*,
4. *persons with non-agreed destinations,*

Characteristic B: Maximum Permitted Gross Weight

1. *ultra-light vehicles* around 500 kg
2. *passenger vehicle* around 2 t,
3. *light commercial trucks and vans* around 8 t,
4. *trucks* around 32 t.

Characteristic C: Maximum Deployment Velocity

1. up to 5 km/h
2. up to 30 km/h
3. up to 60 km/h
4. up to 120 km/h
5. up to 240 km/h

Characteristic D: Scenery

1. Terrain (off-road)
2. Agricultural road
3. Parking lot or parking structure
4. Access road
5. Developed main traffic roads
6. Urban arterial road
7. Country road
8. Interstate
9. Special areas

Characteristic E: Dynamic Elements

1. *Without exclusion* : animals, pedestrians, cyclists, vehicles, law enforcement, etc. meet the autonomously driving vehicle in the scene.
2. *Only motor vehicles :* interaction of autonomous vehicles and human controlled motor vehicles ; animals, pedestrians, cyclist etc. are excluded
3. *Only autonomously driving* : a scenery exclusive for autonomously moving vehicles.
4. *No other dynamic elements* :exclusive for ONE autonomously driving vehicle.

Characteristic F: Information Flow between Driving Robot and Other Entities

1. *Navigation optimization*
2. *Path tracking optimization*
3. *Control optimization*
4. *Provision of environmental information*
5. *Updating the driving robot's capability*
6. *Monitoring the driving robot*
7. *Monitoring occupants*
8. *Occupant emergency call*

Characteristic G: Availability Concept

1. *No availability addition,* the driving robot waits until, through external influence, the scene becomes negotiable again and is covered by the specification of the driving robot.
2. *Availability through driver,* one occupant supports the driving robot negotiating the scene (left open, if by taking over the driving task or through maneuver commands).
3. *Tele-operated driving,* a service provider supports the driving robot negotiating the scene via a remote control.
4. *Pilot service,* an especially trained person proceeds to the vehicle and supports the driving robot negotiating the scene.
5. *Electric towing*. If the hardware necessary for the control task is operational, a tow vehicle with a direct connection can operate it, in order to support the driving robot in negotiating the scene.

Characteristic H: Extension Concept

1. *No substitute* beyond the operating area, i.e. the autonomous driving area covers the specified transportation tasks completely. The vehicle with this value is an exclusive-autonomous vehicle. If the deployment also covers the entire deployment of current vehicles, it is a fully autonomous vehicle.
2. *Driver,* a human takes over the driving task.
3. *Tele-operated driving,* the driving task is performed by an external operator.
4. *Pilot service,* an especially trained person takes over the driving task in a specific regime.
5. *Extra transportation device,* at the boundaries of deployment the driving robot coordinates the handover of the vehicle to an extra transportation device so that this transportation device can continue the transportation task.

Characteristic I: Options for Intervention

1. The vehicle concept offers the option for intervention on one of the three levels (navigation, path tracking and control) and the entity is authorized to intervene on the same level of the driving task. Therefore the entity can intervene.
2. The vehicle concept offers the option, but the entity is not authorized to intervene on one level. This situation correlates to a child that is in the driver's seat. For the use cases, it is assumed for this situation that law for this situation regulates the intervention by the entity.
3. The vehicle concept does not offer the option, but the entity is authorized to intervene on one level. This correlates to a driver in the back seat, who cannot intervene.
4. The use case offers the option on one level, however the entity is authorized to intervene on a different level of the driving task. Also with this combination, the intervention is not permitted to the entity.

- ***Human factors evaluation of level 2 & 3 automated driving ; concept of operation ; NHTSA, 2014***

Detailed operation domain caracteristics

Road Facility Type

- Limited-access Highway : Interstate highway, high speed, absence of traffic lights, pedestrians, bicycles, merge and exit at speed
- Rural Highway : High speeds, at-grade intersections, traffic lights, pedestrians, bicycles
- Suburban Arterial : Moderate speeds, at-grade intersections, traffic lights, pedestrians, bicycles
- City Streets : Moderate to slow speeds, frequent intersections, traffic lights, stop signs, pedestrians, bicycles
- Residential Streets : Slow speeds, greater prevalence of pedestrians/bikes, stop signs
- Off-street (parking facilities, etc.) : Typical parking lot or multi-level parking garage with pedestrians and other slow-speed vehicle traffic

Automated Vehicle Segregation

- Mixed Traffic : Automated vehicles operating in current traffic streams found on roads today
- Segregated Traffic : Automated vehicles operating only on facilities restricted to automated vehicles, with physical separation from human-driven vehicles.

Infrastructure Adaptation

- Adapted Infrastructure : Road facilities modified to optimally support automated vehicles by simplifying the road environment and/or enhancing the environment for sensors. This may be in the form of physically separated lanes and/or specialized road furniture/markings optimized for onboard sensors.
- Non-adapted infrastructure : The current road environment including human-driven traffic with lane markings of various types and quality.

Connected Automated Operation

- Information derived from the Internet via cellular data communications and Global Positioning System (GPS) technology is assumed to be generally available with signal dropout a possibility in all cases.
- V2V : Automation is implemented that uses IEEE 802.11p DSRC to exchange data between vehicles traveling in the vicinity of one another, including, but not limited to, the SAE J2735 Basic Safety Message.
- Vehicle-to-Infrastructure (V2I): Automation uses IEEE 802.11p DSRC to receive data from the infrastructure, including curve geometry, weather/road conditions, signage, traffic signal phase and timing, and intersection geometry. Additionally, the infrastructure uses vehicle data to adapt traffic control devices and collect probe data to support area-wide traffic management.
- Both : Use of both V2V and V2I.
- None : Automated vehicles rely on onboard sensors and information derived from the Internet and GPS.

Inter-Vehicle Coordination

- Platooning : Inter-vehicle communications are used to provide information about lead vehicle actuation to multiple automated vehicles following at close headways. The vehicular tasks are limited to following the vehicle ahead, maintaining the headway, and join/split maneuvers.
- Cooperative Headway Management : Inter-vehicle communications are used to implement C-ACC, thus shortening the distance between a lead vehicle and a single following vehicle. This function can be implemented as longitudinal control alone or in combination with lateral control. C-ACC offers significant improvement in fuel economy due to the aerodynamics of shorter headways.
- Individual Vehicle : "Free agent" operation; the automated vehicle coordination is typical of the operations regular drivers perform today; inter-vehicle communications do not play a role.

Speed of Travel

- Low speed (0–30 mph)
- Higher speeds only (30–75 mph)
- Full speed range : Encompasses full range of speeds (i.e., a system that is not limited to a specific speed range)

Traffic Density

- LOS A : Free flow
- LOS B : Flow with some restrictions
- LOS C : Stable flow; maneuverability and speed more restricted
- LOS D : Unstable flow, temporary restrictions momentarily slow vehicle
- LOS E : Unstable flow, vehicles unable to pass, temporary stoppages
- LOS F : Force traffic flow condition with low speed

Awareness of and Operation Relative to Traffic Control Devices

- Traffic signal (circular) : Detection of the state of traffic signals plus the lane assignment of traffic signals for more complex intersections
- Traffic signal (turn indication) : Detection/understanding of turn arrows and lane assignments to which the turn arrows are applicable
- Traffic circles : Detection of traffic circles, number of lanes in traffic circles, and observing proper behavior in traffic circles
- Pedestrian crossings : Detection of pedestrian crossing zones and observing local rules for allowing pedestrians to cross
- Lane restriction indications : Detecting and observing turn-only lanes and/or restrictions to certain vehicle types; this includes electronic message signs
- Work zones : Detecting work zones, special signed instructions, and lane designations via traffic cones or other markers.
- One-way street signs : Detecting and observing signage indicating one-way streets
- Yield signs : Detecting and observing yield signs

- Stop signs : Detecting and observing stop signs and behaving according to appropriate order of precedence
- Speed signs : Detecting speed signs and adjusting speed accordingly, including electronic speed signs

Awareness of Other Vehicle Indications

- Brake lights : Detection of brake lights on a lead vehicle as a redundant indication of deceleration (i.e., a backup to sensors and communication)
- Turn signals : Detection of turn signals on lead and/or adjacent vehicles as a means of assessing the intentions of other drivers

Situational Awareness

- Vehicles : Nearby vehicles
- Motorcycles : Nearby motorcycles
- Road condition : Detection of surface traction condition, potholes, etc.
- Road debris : Detection of debris on the road (e.g., tire/animal carcasses, items that may have fallen off other vehicles)
- Pedestrians : Pedestrians relevant to the planned travel path, particularly in right-turn movements made across crosswalks when the pedestrian is traveling in the same direction (the pedestrian may be in the driver's blind spot)
- Bicyclists : Nearby bicyclists, particularly in right-turn movements made across crosswalks when the bicyclist is traveling in the same direction (the bicyclist may be in the driver's blind spot) Animals : Awareness of animals on the road and those on the roadside who may bolt across the road

Vehicle Maneuvers under Automated Control

- Stay in Original Lane Only : Cruising at set speed; lane markings sufficient for lane detection may or may not be available
- Lane Change : Monitor adjacent lane for adequate gap; signal and execute lane change; lane markings sufficient for lane detection may or may not be available
- Freeway-to-Freeway Interchange : Maneuver to proper lane for merging onto the desired freeway and direction; merge into traffic on new freeway
- Diverge from Freeway to Surface Street: Signal for exit from freeway; detect and understand configuration at end of departure ramp; select proper lane and observe yield/stop/signal information
- Merge into Traffic : Merge into freeway traffic from surface street ramp with awareness of merging distance available
- Left Turn across Traffic: Make a left turn with awareness of any crossing pedestrians or bicyclists; awareness of any oncoming vehicles that may come into sensor view during the maneuver
- Right Turn : Make a right turn with awareness of any crossing pedestrians or bicyclists who have the right of way
- Stop/Start at Traffic Signal: Awareness of traffic signal state for travel lane; maintain proper gap behind lead vehicle while accelerating on green signal
- Stop-Controlled Intersections: Awareness of stop sign and configuration (two-way, four-

way); awareness of other vehicles at intersection and which vehicles have right of way; observance of order of precedence when multiple vehicles are at the intersection

- Traffic Circles : Awareness of traffic circle configuration, including number of lanes; observance of proper lane behavior; awareness of vehicles already in the traffic circle; awareness of right of way for each vehicle; enter and depart traffic circle following local rules
- Work Zones : Detection of lane boundaries (possibly unconventional) and/or stop indications; maneuver through work zone with awareness of other traffic and work zone speed limits; merge into adjacent lane in lane-drop situations
- Respond to Emergency Vehicles: Awareness of emergency vehicle and location relative to other vehicles; determine need to move out of the path of the emergency vehicle; determine safe and legal options to move out of the emergency vehicle path and execute the ideal maneuver
- Yield as Appropriate: Awareness of yield signs and road rules for yielding in the absence of signs; awareness of other vehicles and their right-of-way status; proceed in accordance with right of way

Weather Conditions

- No Adverse Conditions : Dry, clear
- Rain : Adapting speed as needed due to wet pavement and visibility
- Sleet : Adapting speed as needed due to pavement condition and visibility; alerting driver when automated control is no longer possible
- Snow : Adapting speed as needed due to pavement condition and visibility; alerting driver when automated control is no longer possible (e.g., due to obscured lane markings)
- Fog : Adapting speed as needed due to visibility; alerting driver when automated control is no longer possible
- Other (Smog, Smoke, Sand/Dust, Crosswind, Hail): Adapting speed as needed due to visibility; alerting driver when automated control is no longer possible; adapting steering as needed in crosswinds
- All Conditions : Automated vehicle can operate at minimum performance standards regardless of weather

Roadway Surface Conditions

- *(TBD in requirements)*

Driver Ability in Manual Driving

- Novice: A learning driver or one with less than one year of experience
- Experienced : A driver with one or more years of driving experience
- Impaired Due to Age or Disability: Drivers whose driving skills have started to degrade due to age; drivers whose cognitive and/or motor skills are degraded due to a medical condition

Driver Monitoring

- Yes : Systems are implemented that monitor some or all of lane-keeping stability, pedal application, steering inputs, manipulation of other controls, seating position, eye-blink rate, and gaze (on or off road)

- No: No monitoring at all

Driver Task Requirement to Maintain Engagement

  - Yes : Driver must take an action of some sort at defined intervals for the automated system to continue operation
  - No : The driver needs to take no action for the automated system to continue operation

ntended Duration of Automation

- Short : Less than 1 minute
- Medium : 1–10 minutes
- Extended : 10–30 minutes
- Long : Greater than 30 minutes

Engage/Disengage Method

- System Request: The system makes a request to the driver to engage or disengage
- Driver-Initiated: The driver requests the system to engage or disengage from driving
- Both: Both options are implemented
- Forced Disengage/Failure: The system requests the driver to resume control due to inadequate road conditions or a system failure; in the case of a non-responsive driver, the system brings the vehicle to a (relatively) safe state

Driver Engagement Timing

[Engagement timing refers to the amount of time the system allows the driver to re-engage operations after a period of automated driving).

- Short : Less than 3 seconds
- Medium : 3–10 seconds
- Long : 10–30 seconds
- Extended : Greater than 30 seconds

Driver Training

- None : No driver training; the driver discovers system operation and forms his/her mental model of system operation
- Minimal : The driver is provided information (e.g., a video shown at the car dealership) before driving the vehicle for the first time
- Substantial : Before driving an automated vehicle, a special driving certification based on training must be obtained.

A.5.3. Risk analysis

Box : ISO 26262 and risk analysis for automated systems

Source : challenges in applying the ISO 26262 for driver assistance systems; Spanfelner, Richter, Ebel, Wilhelm, Branz and Patz ; 2012

The international Standard of ISO 26262 is the adaptation from IEC 61508 for the automative industry. IEC 61508 is titled 'Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems and is intended to be a basic functional safety standard applicable to all kind of industry. ISO 26262 is titled 'Road Vehicles – Functional Safety' and defines methods and measures to be taken to develop safety relevant systems comprised of electrical, electronic and software components'.

The main scope of ISO is to avoid E/E failures of theses systems. Therefore this standard includes a guidance to avoid or control theses systemaic and random hardware failures by appropriate requirements and processes and to reduce the expected risk to an acceptable level concerning injury or death of human beings.

ISO 26262 mainly aims to :

- Provide an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.
- Cover functional safety aspects of the entire development process (including such activities as requirements specification, design, implementation, integration, verification, validation, and configuration).
- Provide an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs).
- Use ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk.
- Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved.
- ISO 26262 provides requirements for relations with suppliers
- ISO 26262 is mainly the start point of safety-oriented analysis of the automated vehicle.

In common with IEC 61508, ISO 26262 uses also the concept of safety goals and a safety concept as follows :

- a *Hazard Analysis and Risk Assessment (H&R)* identifies hazards and hazardous events that need to be prevented, mitigated or controlled ;
- a *Safety Goal* is formulated for each hazardous event ;
- an *Automotive Safety Integrity Level (ASIL)* is associated with each safety goal ;
- the *Functional Safety Concept* is a statement of the functionality is implemented on the system level by hardware and software addressed by *Technocal Safety Requirements ;*
- *Software Safety Requirements* and *Hardware Safety Requirements* state the specific safety requirements which will be implemented as part of the software and hardware design.

In the ISO 26262, the V-Model is used as a reference for the development process.

The V-Model is organized into layers of abstraction of which each refines the specification of the previous layer and restricts the solution space by introducing design decisions. Each refinement may be (and usually is) guided by deductive models that correspond to the design decisions. Each layer serves as a specification for the next lower one and takes the role of a proof obligation for the subsequent development. Specific to the V-Model, and in this context especially important, is the tight integration of specification and verification on all layers.

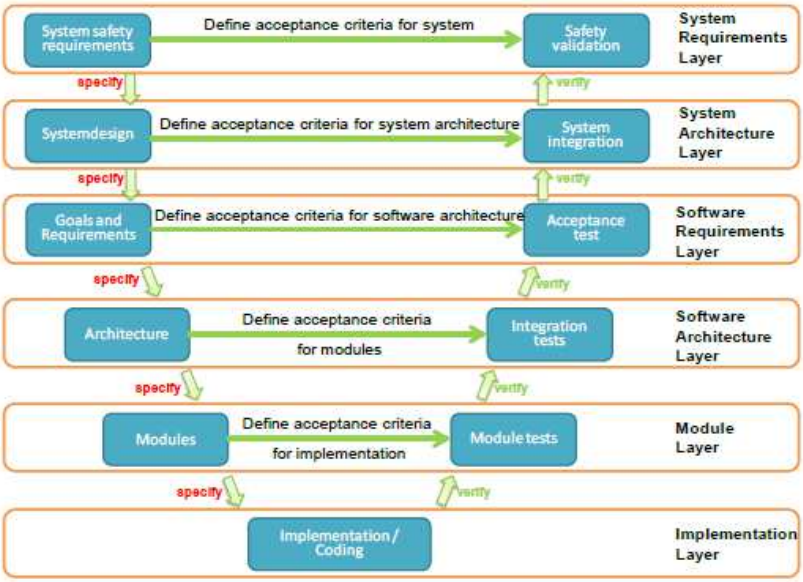
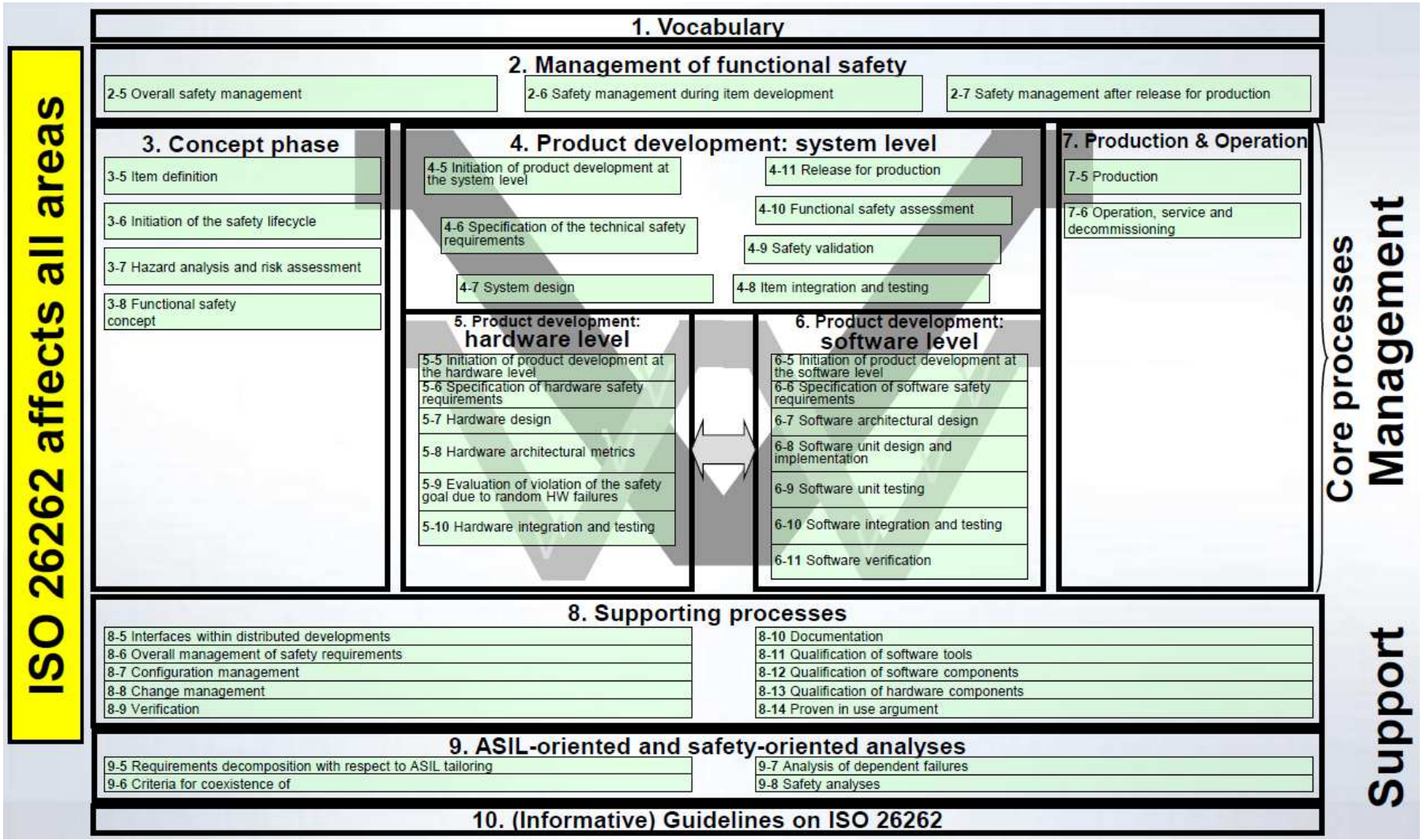


Figure 9: The V-Model and its layers of abstraction

- *Assessment of the ISO 26262 Standard, "Road Vehicles – Functional Safety"; Van Eikema Hommes; 2012*



Severity

Class	S0	S1	S2	S3
Description	No Injuries	Light and Moderate Injuries	Severe and Life-threatening Injuries(survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Exposure

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium Probability	High Probability

Controllability

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

ASIL

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

D: highest safety integrity level
A: lowest safety integrity level
QM: quality management

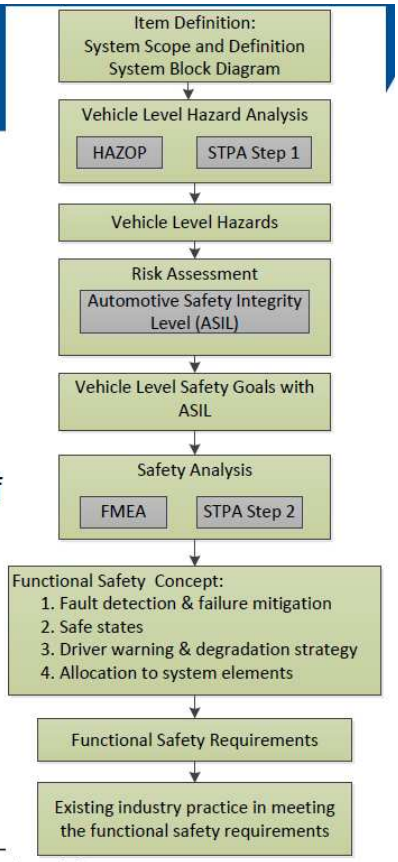
- ***Safety analysis approaches for automotive electronic control systems, SAE & Volpe centre, 2015***

Analysis Process and Approaches

- Follow the process in the ISO 26262 Concept Phase.
- Apply multiple approaches for hazard and safety analysis:
  - Hazard and Operability (HAZOP) Analysis
  - Failure Mode and Effects Analysis (FMEA)
  - System Theoretic Process Analysis (STPA)
- Aim to identify a comprehensive list of hazards and causal factors in order to support the development of safety requirements.
- Assess driver-vehicle interaction for vehicle automation levels 2-4.

Note: This presentation will focus on the STPA method, assuming the audience is familiar with HAZOP and FMEA.

**ISO 26262 does not recommend or endorse a particular method for hazard and safety analyses. Other comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.*



System Theoretic Process Analysis (STPA)

- A hazard analysis method aimed to identify causes leading to vehicle-level losses
- A top-down systems engineering approach
- Incorporates control system theory
- Considers both component failures and system interactions
- Integrates driver-vehicle interface in the overall modeling
- Assists the identification of software safety requirements
- Provides a well-guided and structured analysis process
- Produces documented and traceable rationales that link component failures and unsafe interactions to vehicle-level hazards and losses
- Generates hazards and causal factors that are inputs to safety requirements and constraints

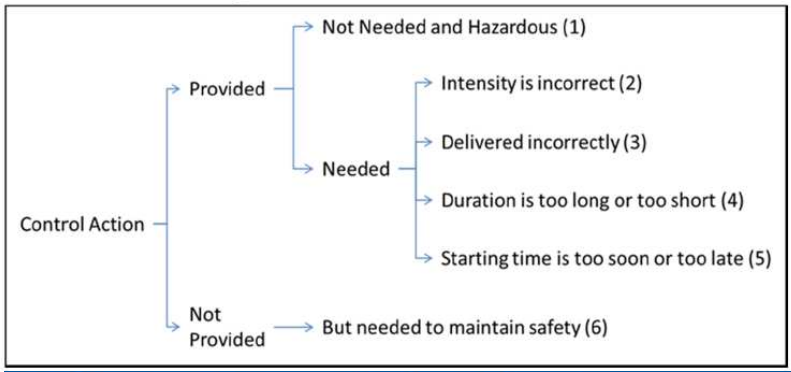
STPA Step 1: Unsafe Control Actions

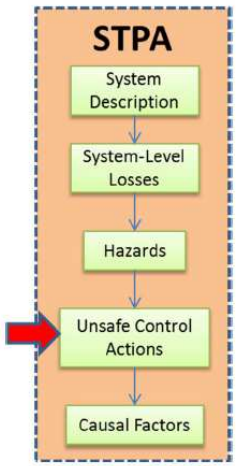
Unsafe Control Actions (UCAs) are commanded by controllers that can potentially cause the vehicle systems to transition from safe to hazardous states.

UCA Identification:

For each control action, consider:

1. Relevant system states
2. Six UCA guidewords

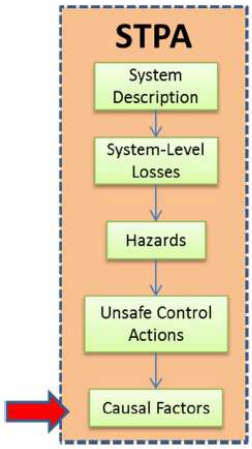




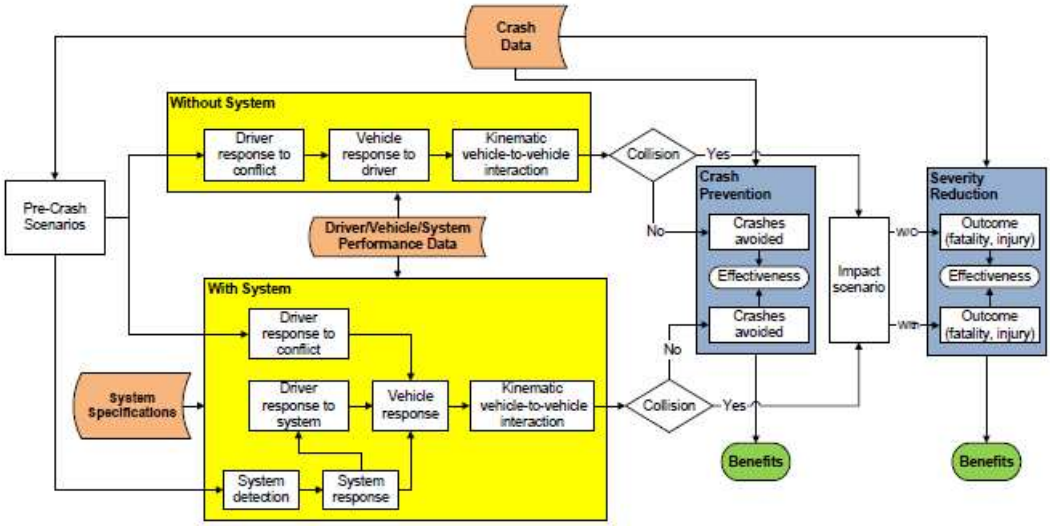
STPA Step 2: Causal Factor Categories

Causal factors (CFs) consider the following aspects of the control systems:

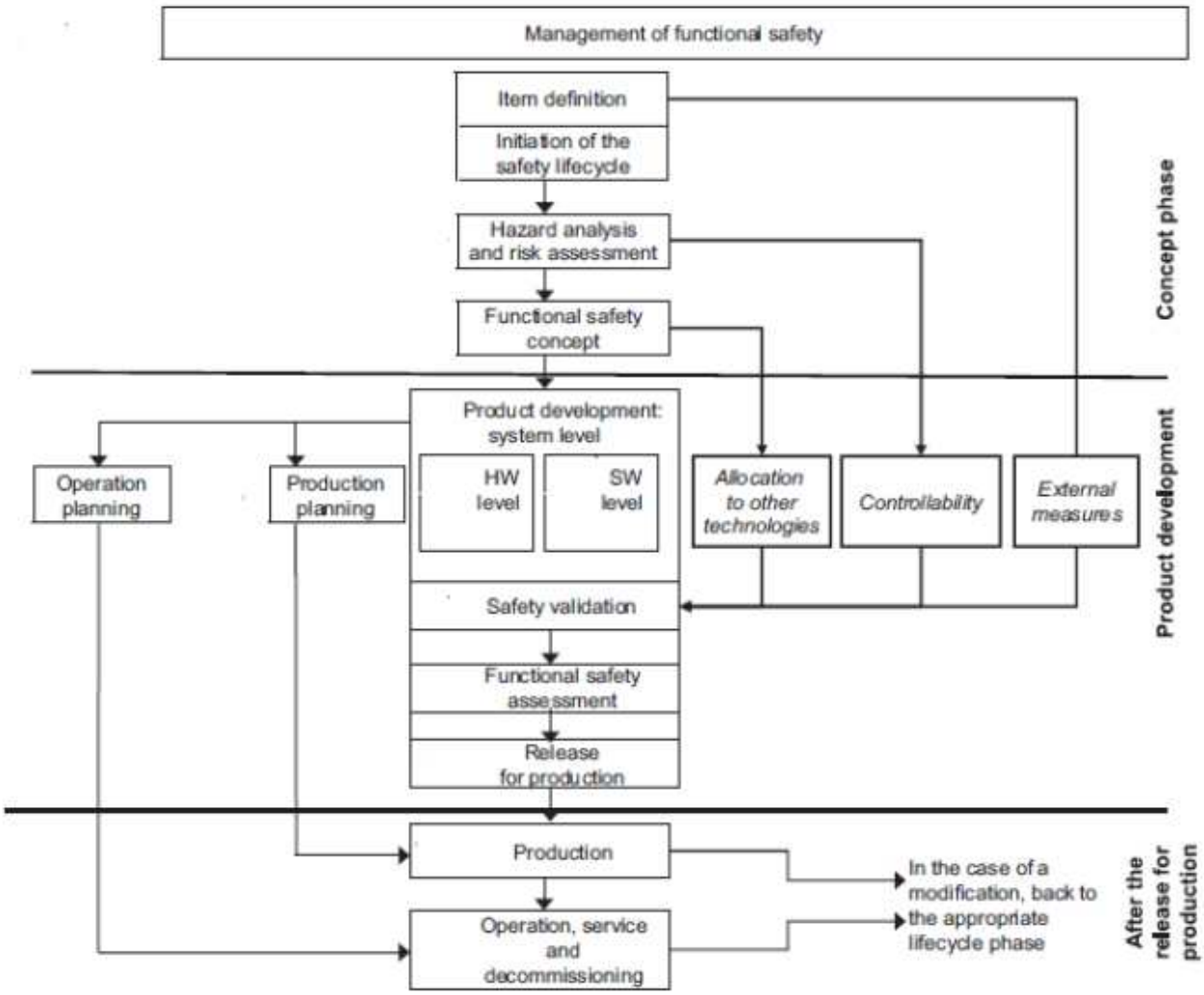
- Controller
- Sensor
- Actuator
- Controlled Process
- Communication links (wiring, connectors, or communication bus)
- Unsafe Interaction with Other Vehicle Systems
- Unsafe Interaction with External Environment



- ***Safety Impact Methodology Software Tool Logic (Source: Harding, Doyle, Sade, Lukuc, Simons, & Wang, 2014),***



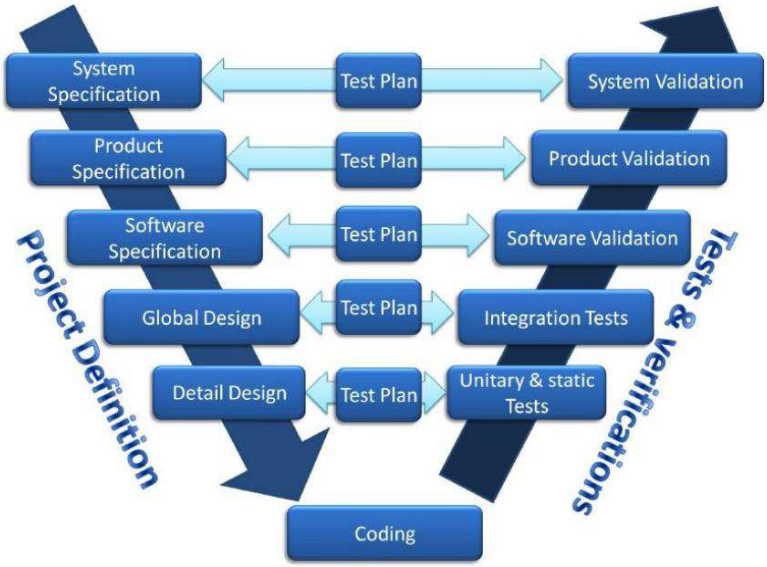
- ***Interactive Safety Analysis Framework of Autonomous Intelligent Vehicles; You Xiang Cui, Lei Sun, Li Hui Sui, Jun Kang, Yong Jiang; 2016***



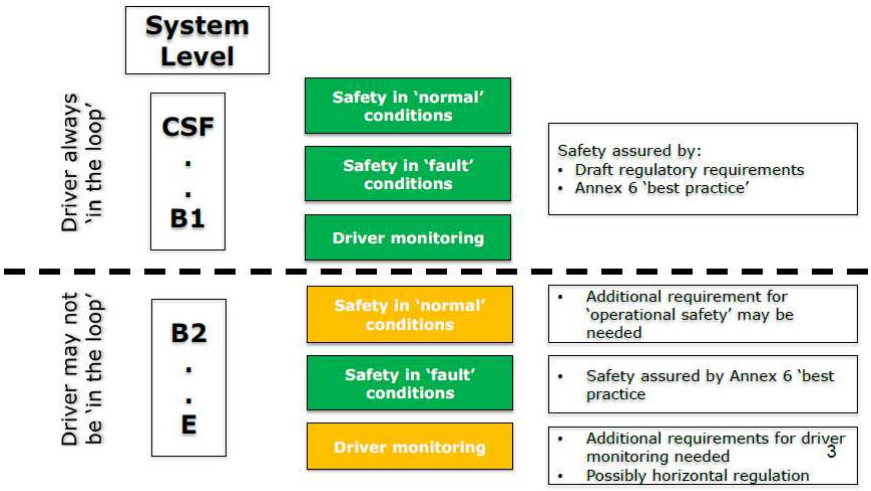
A.5.4. Validation methods

- ***European Commission Study on the assessment and certification of automated vehicles, 2016***

  - ***The "V approach" to validation under ISO 26262***



  - ***Rationale for requirements and best practices in ACSF categories***



Box : challenges in testing according to the ISO 26262 - V-Model

Source : Challenges in Autonomous Vehicle Testing and Validation; Koopman & Wagner; 2016

Driver out of the loop

- controllability challenges
- Autonomy Architecture Approaches

Complex requirements

- Requirements challenges (too numerous events to identify)
- Operational concept approaches
- Safety requirements and invariants

Non-deterministic algorithms

- Challenges of stochastic systems
- Non-determinism in testing

Machine learning systems

- Challenges of validating inductive learning
- Solutions to inductive learning

Mission critical operational requirements

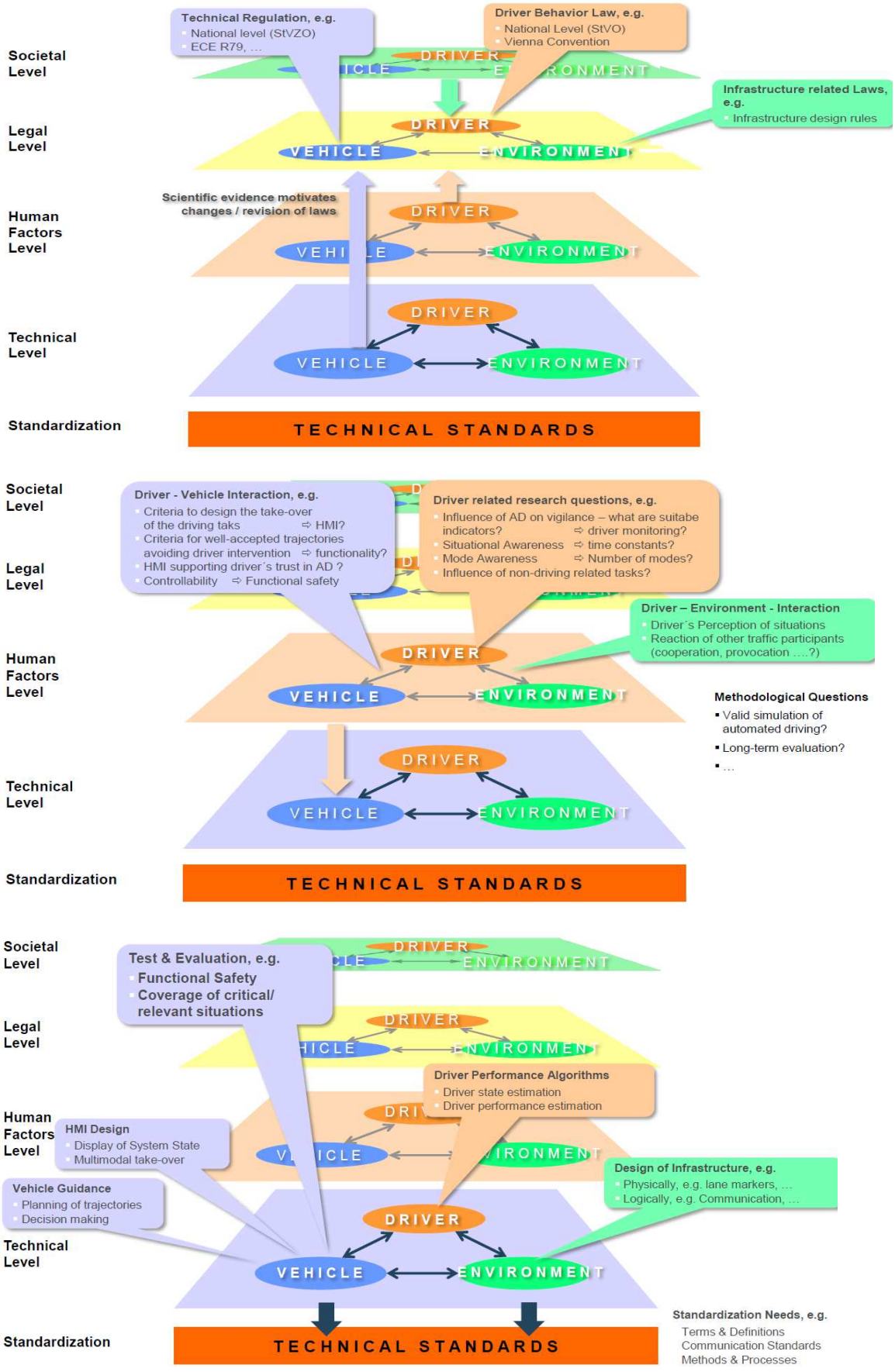
- Challenges of fail-operational system design
- Fail-over missions

Box : Necessity of validation through simulation

Source : Driving to Safety, How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability; Kalra & Paddock; 2016

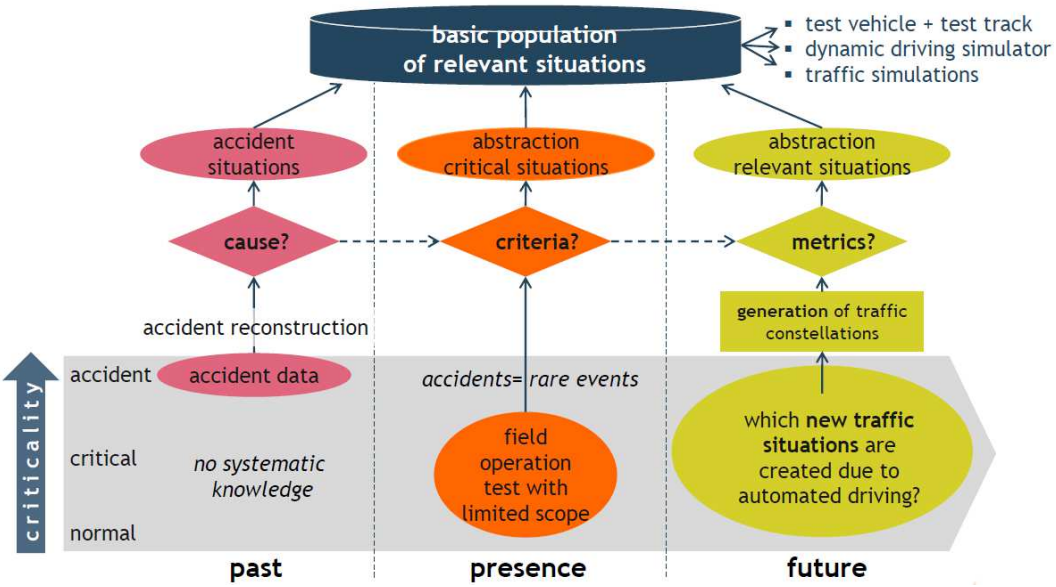
- Autonomous vehicles would have to be driven hundreds of millions of miles and sometimes hundreds of billions of miles to demonstrate their reliability in terms of fatalities and injuries.
- Under even aggressive testing assumptions, existing fleets would take tens and sometimes hundreds of years to drive these miles—an impossible proposition if the aim is to demonstrate their performance prior to releasing them on the roads for consumer use.
- Therefore, at least for fatalities and injuries, test-driving alone cannot provide sufficient evidence for demonstrating autonomous vehicle safety.
- Developers of this technology and third-party testers will need to develop innovative methods of demonstrating safety and reliability.
- Even with these methods, it may not be possible to establish with certainty the safety of autonomous vehicles. Uncertainty will persist.
- In parallel to creating new testing methods, it is imperative to develop adaptive regulations that are designed from the outset to evolve with the technology so that society can better harness the benefits and manage the risks of these rapidly evolving and potentially transformative technologies.

- ***Challenges and goals of evaluation, IKA, Aachen University, 2016***



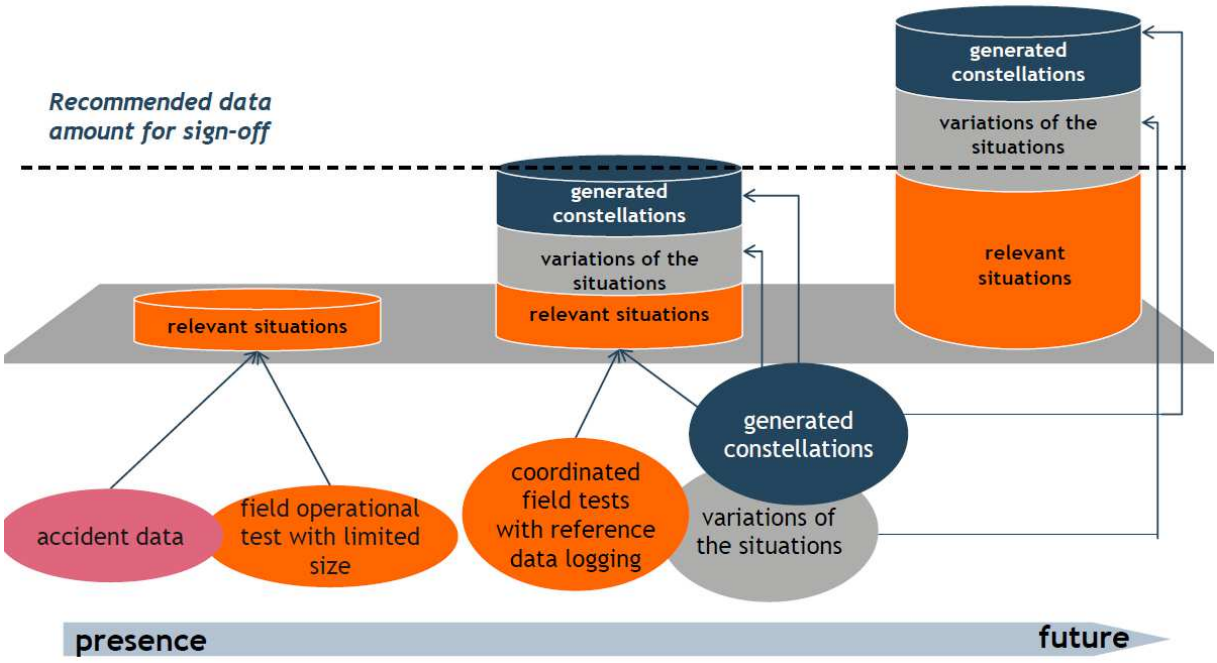
// Evaluation Methodology

Sources and Population of relevant Situations

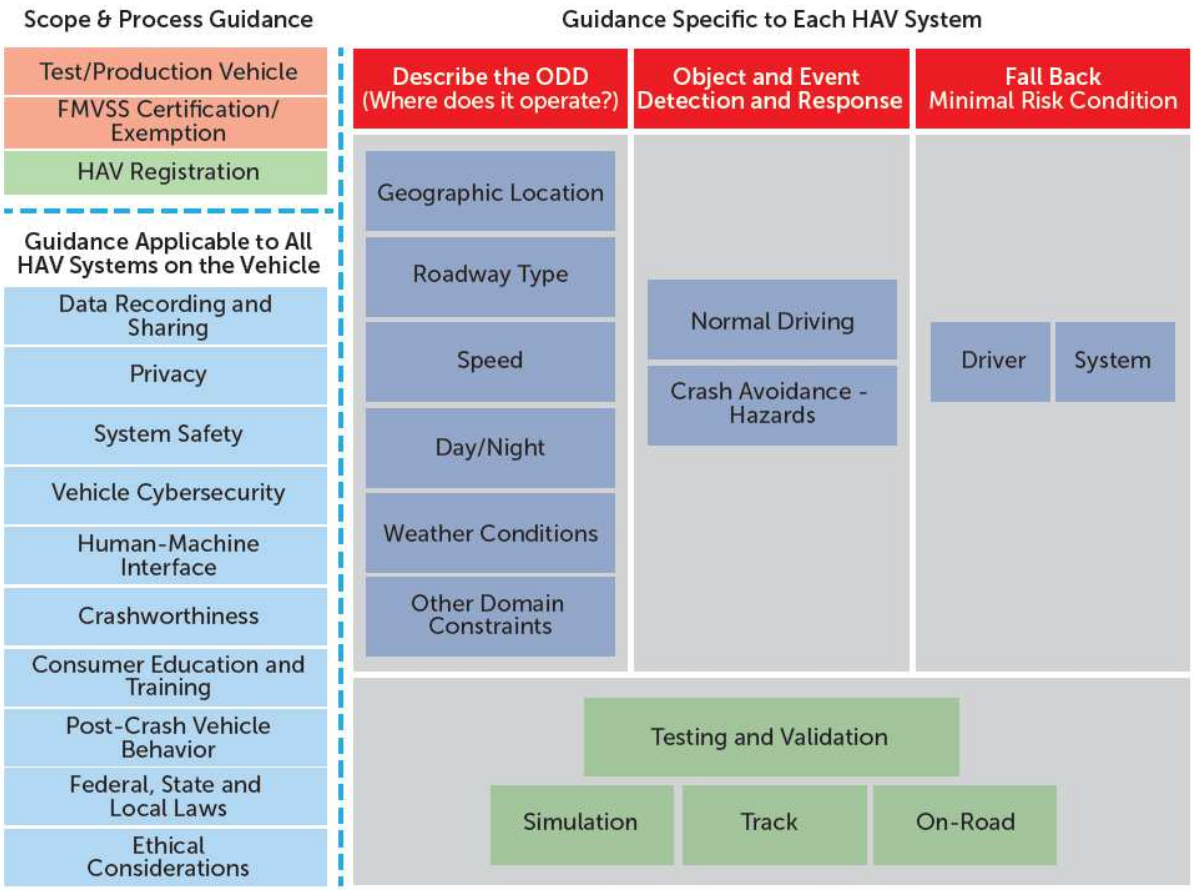


// Evaluation Methodology

Data Base Population over Time



- **NHTSA guidance, 2016**



Bibliography

1. Study on the assessment and certification of automated vehicles, Final Report; Mervyn Edwards, Matthias Seidl, Michelle Tress, Ashley Pressley and Saket Mohan; December – 2016
2. System Classification and Glossary; Arne Bartels, Ulrich Eberle, Andreas Knapp; February 2015
3. Use cases for Autonomous Driving; Walther Wachenfeld, Hermann Winner, June 2014
4. Validation of assisted and automated driving systems; Udo Steininger, Hans-Peter Schöner, Mark Schiementz, Jens Mazzega; April 2016
5. Safety assurance based on an objective identification of scenarios; Walther Wachenfeld, Philipp Themann; October 2016
6. From development to type approval; Felix Fahrenkrog, Adrian Zlocki; April 2016
7. Evaluation methodology for automated vehicles in AdaptIVe and beyond; Christian Rösener, Falix Fahrenkrog; April 2016
8. Requirements on tools for assessment and validation of assisted and automated driving systems; Udo Steininger, Hans-Peter Schöner, Mark Schiementz; November 2015
9. Safety Assurance for Highly Automated Driving – The PEGASUS Approach; Hermann Winner, Walther Wachenfeld, Philipp Junietz; July 2016
10. Prototype validation report and performance analysis; Martionoli, Berg et al.; November 2016
11. Assessment of the ISO 26262 Standard, “Road Vehicles – Functional Safety”; Qi Van Eikema Hommes; January 2012
12. Best Practices for Embedded Software Testing of Safety Compliant Systems; January 2016
13. Certification for Autonomous Vehicles; James Martin, Namhoon Kim, Dhruv Mittal, Micaiah Chisholm; 2015
14. Challenges in applying the ISO 26262 for driver assistance systems; Bernd Spanfelner, Detlev Richter, Susanne Ebel, Ulf Wilhelm, Wolfgang Branz, Carsten Patz; May 2012
15. ISO 26262 in Practice – Resolving Myths with Hazard & Risk Analyses; Pierre Metz, Stefan Kriso, Peter Grabs;
16. Challenges in Autonomous Vehicle Testing and Validation; Philipp Koopman, Michael Wagner; January 2016
17. Interactive Safety Analysis Framework of Autonomous Intelligent Vehicles; You Xiang Cui, Lei Sun, Li Hui Sui, Jun Kang, Yong Jiang; 2016
18. Driving to Safety, How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability; Nidhi Kalra, Susan M. Paddock; 2016
19. A Philosophy for Developing Trust in Self-Driving Cars; Michael Wagner and Philipp Koopman; 2015
20. Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts; Myra Blanco, Jon Atwood, Holland M. Vasquez et al.; August 2015
21. Comprehensive definitions for automated driving and ADAS; Tom Michael Gasser, Alexander Thomas Frey, Andre Seeck, Rico Auerswald.