Transmitted by France Document No. ITS/AD-12-07-2
(12th ITS/AD, 22 June 2017, agenda item 3-4)

Ministère de l’environnement, de l’énergie et de la mer may 26th, 2017
DGITM/SAGS/EP et DGEC/SD6 V11

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.

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.

4. Basic definitions

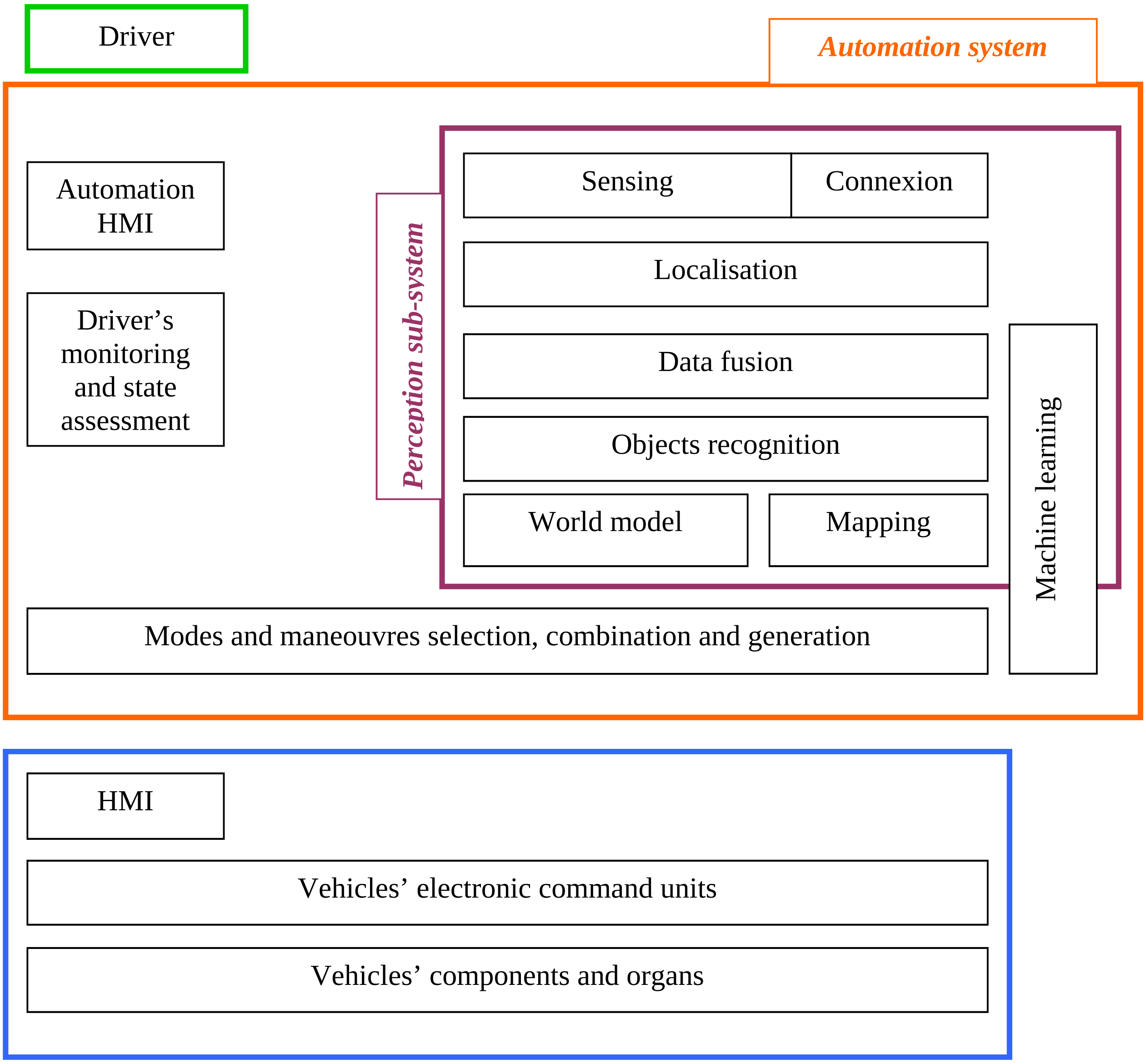
Clarity of concepts appears as a pre-requisite for a sound regulation architecture. This paragraph proposes definitions for three essential building concepts :

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

4.1. Vehicles' sub-systems

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

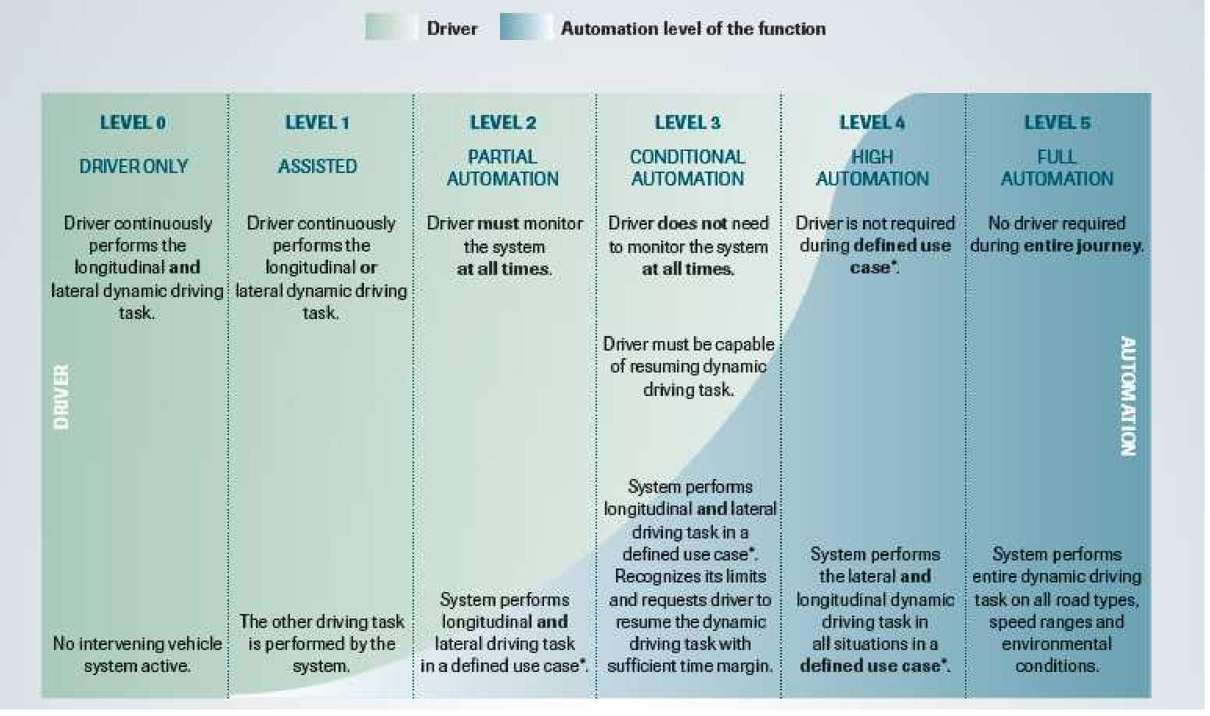
- Driver
- Human-machine interfaces
- Automation system
- Driving organs



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 :

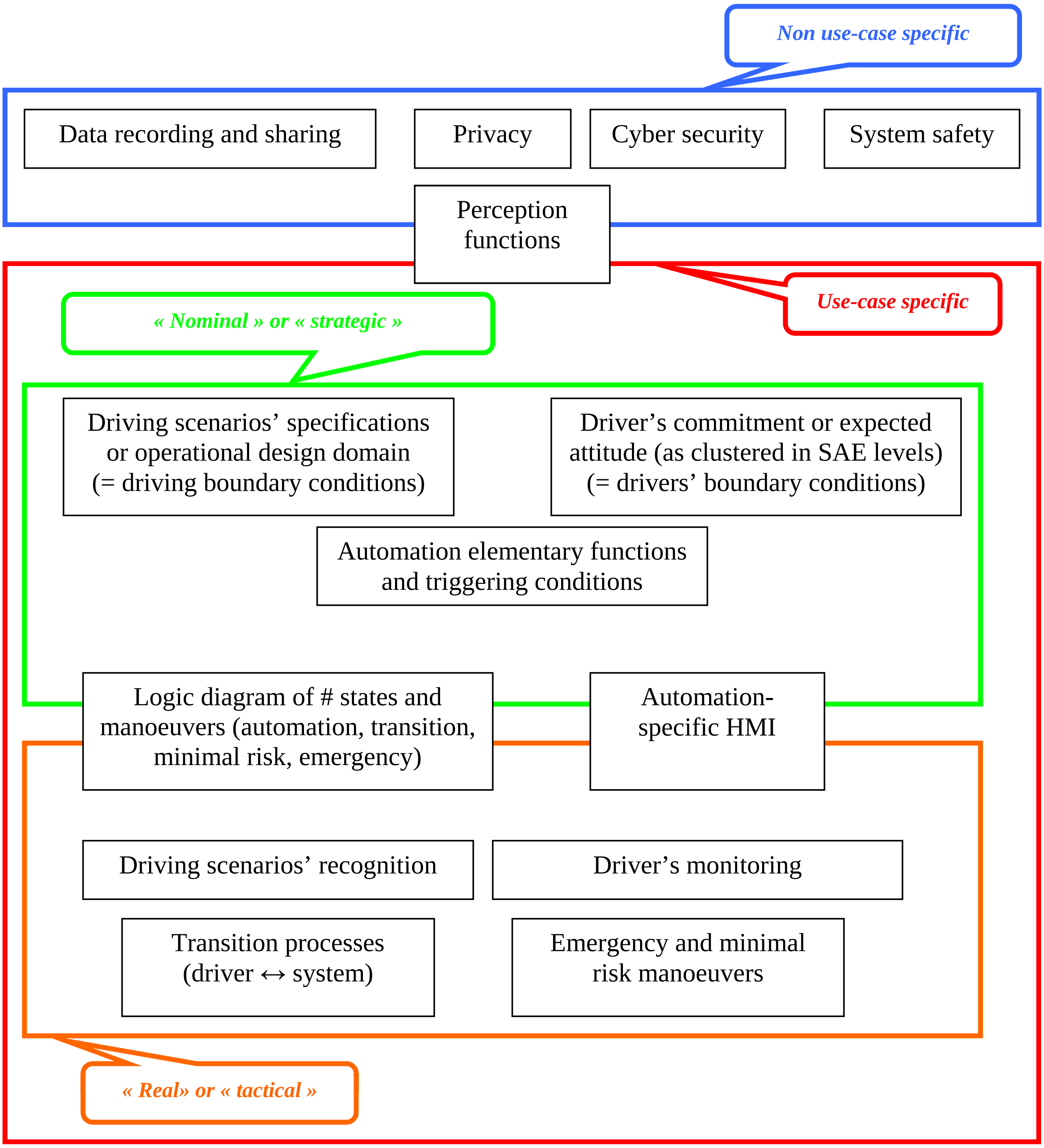
- different states of the automation system
- different states of the driver's
- vehicle's real environment (e.g. driving inside or approaching operational design domain limits ; unexpected situations, events or hasards)
- transition or emergency manoeuvres.

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.

Use-case description

Use-case functionnalities

- Perception functionnalities
- Driving scenario specification or operational design domain (generic or geo-fenced)
- Automation elementary functions
- Activation / desactivation conditions
- Transition processes
- Emergency and minimal risk manoeuvres
- Logigal diagram of # states and manoeuvres

Automation-specific HMI		
Driver's monitoring	Driving scenario recognition	Transition / handover requests

Committed / expected driver's attitudes

- Permanently in charge of the driving task
- Resume at any time
- Resume by request

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. 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.

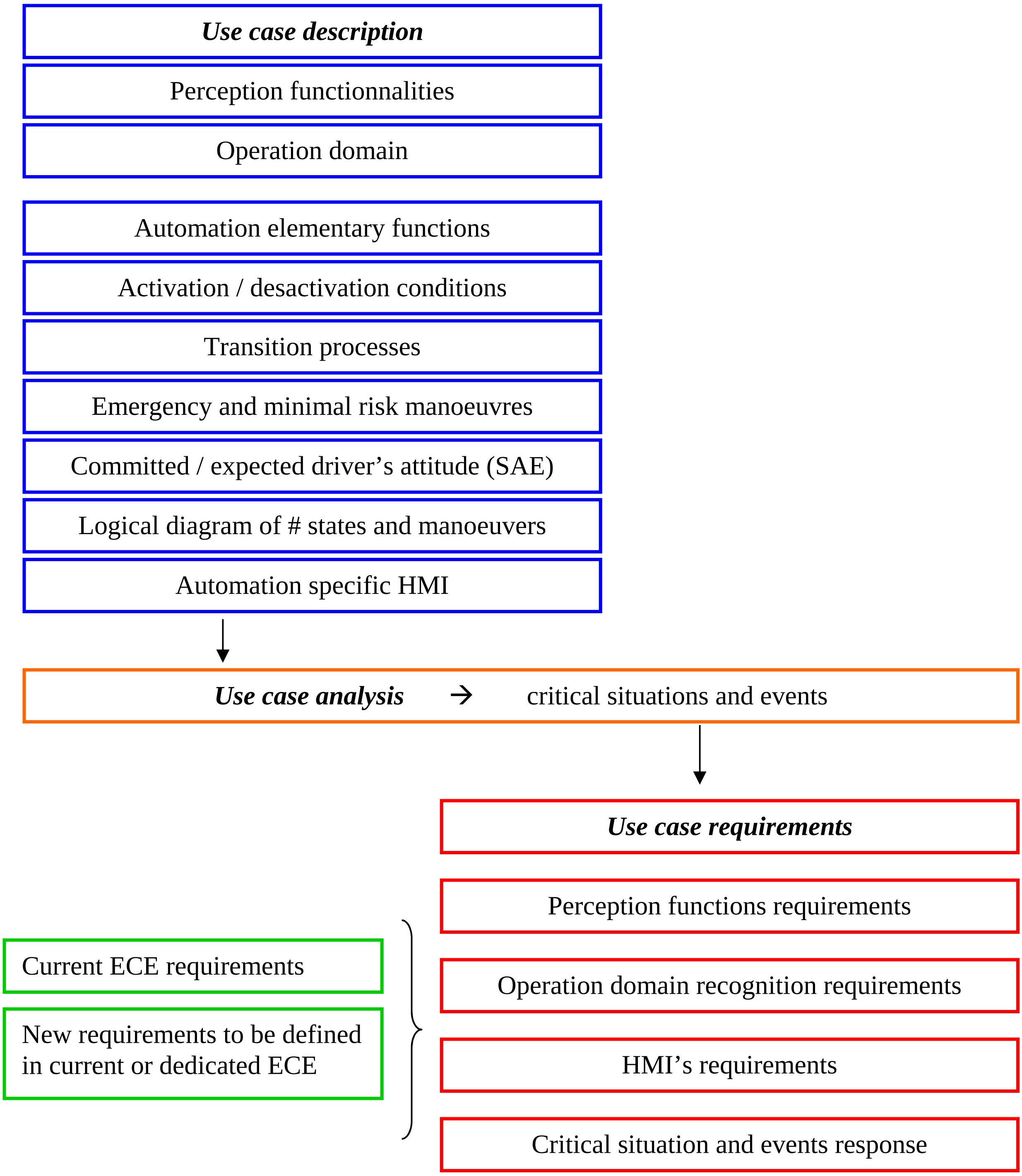
5. Proposed schematic architecture

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

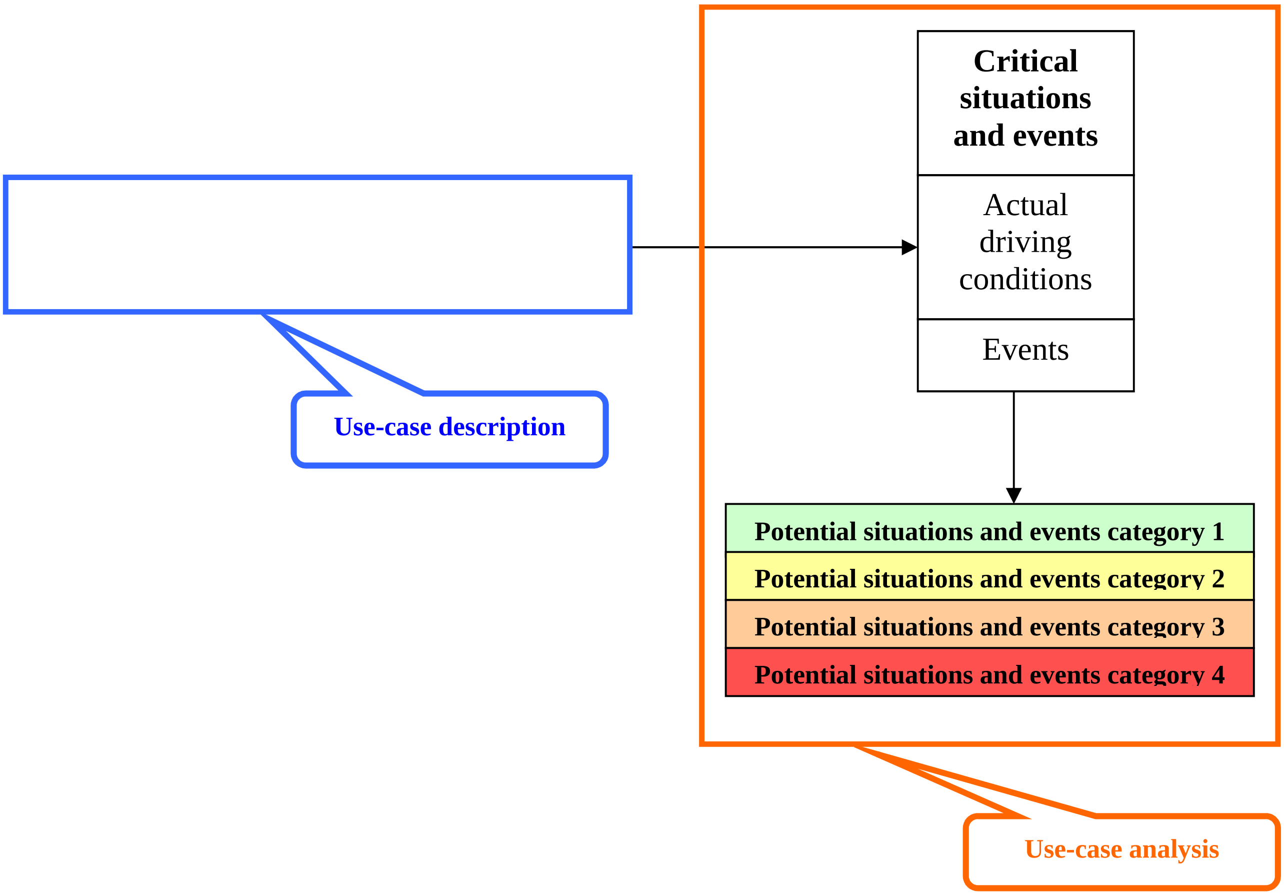
Regulation architecture = horizontal layer + vertical regulations

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 screenin or analysis
  - Simulations
  - Tests

The following graphs propose a simple presentation of a possible schematic correspondance between types of requirements and types of validation procedures and tools.

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 availability	Self-declaration or Evidence based or Certified	Documentation Simulation
Criticity level 3	Response functionnal description	Self-declaration 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

Level of verification ***Level of criticity***	Self-declaration	Evidence based	Certified	Tested
Criticity level 1	■	■		
Criticity level 2	■	■	■	
Criticity level 3	■		■	
Criticity level 4	■	■	■	
Criticity level 5		■	■	■

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).

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 1 : illustration on a use case

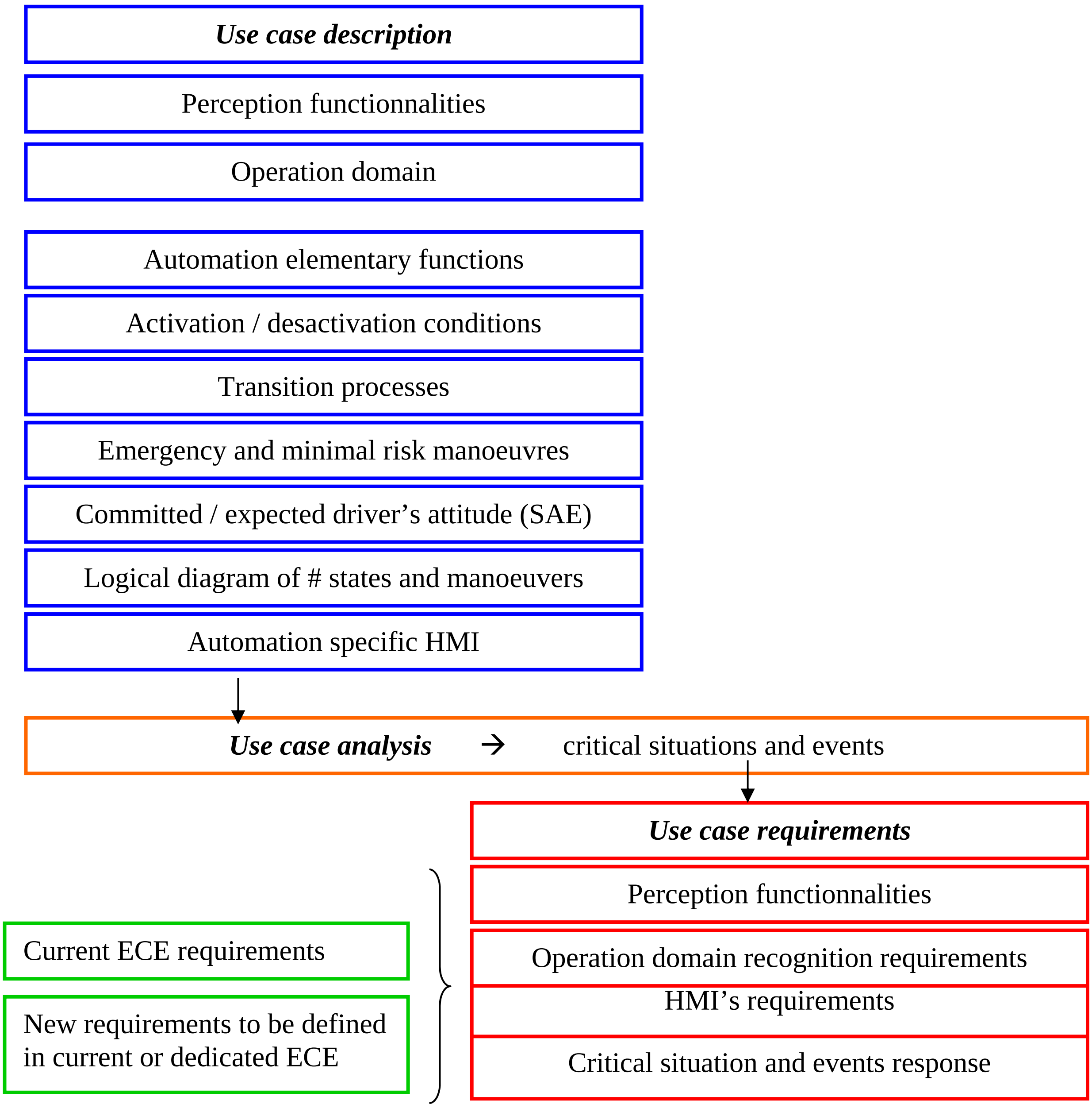
This annex illustrates the application of the regulation proposed "philosophy", architecture and systems tasks general requirements (as discussend in WP29 – ITS/AD – cf. Annex) to an illustrative use case, taking into account the above requirements on system's tasks.

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.

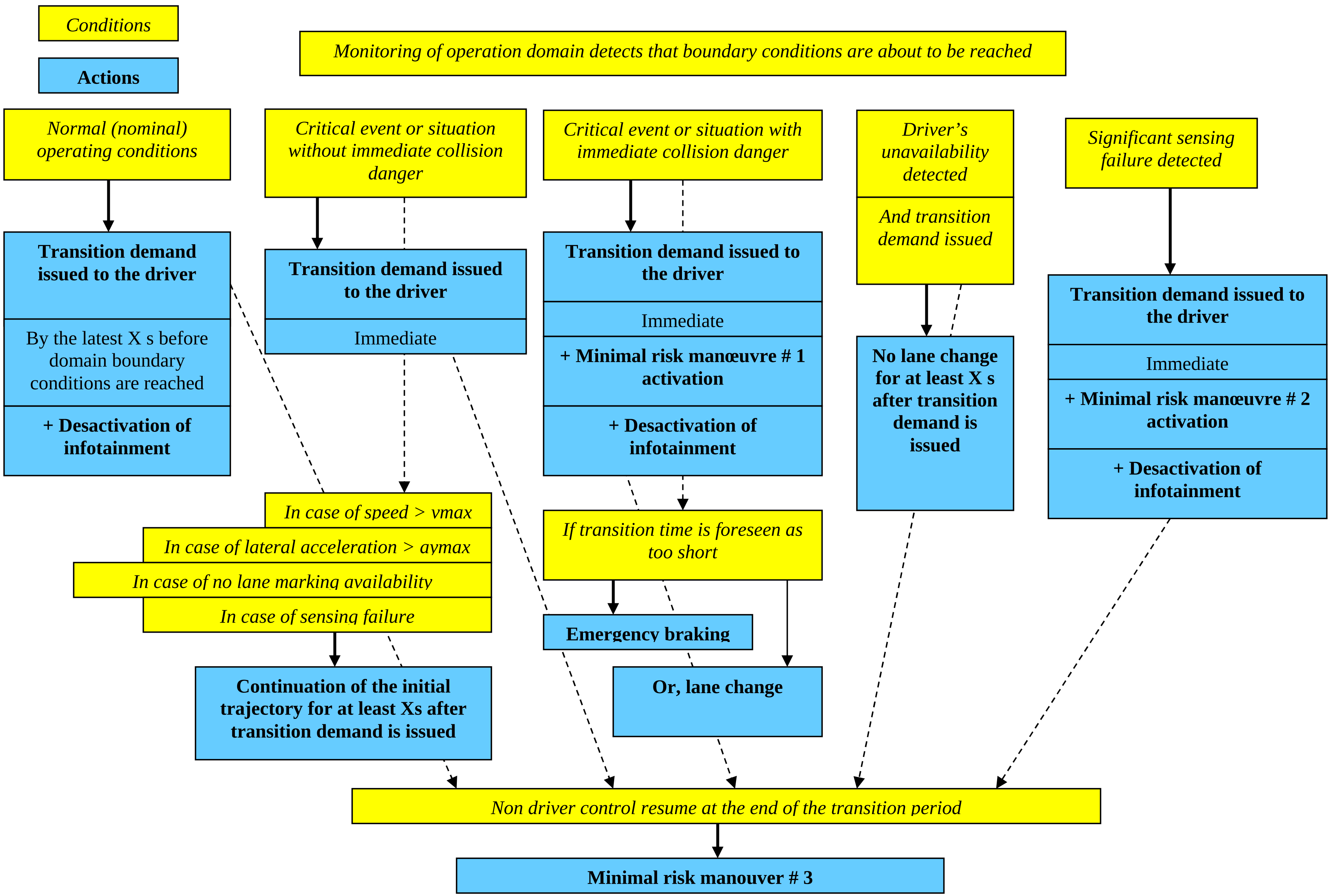
The regulation architecture is presented as suggested above, i.e. :



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”.

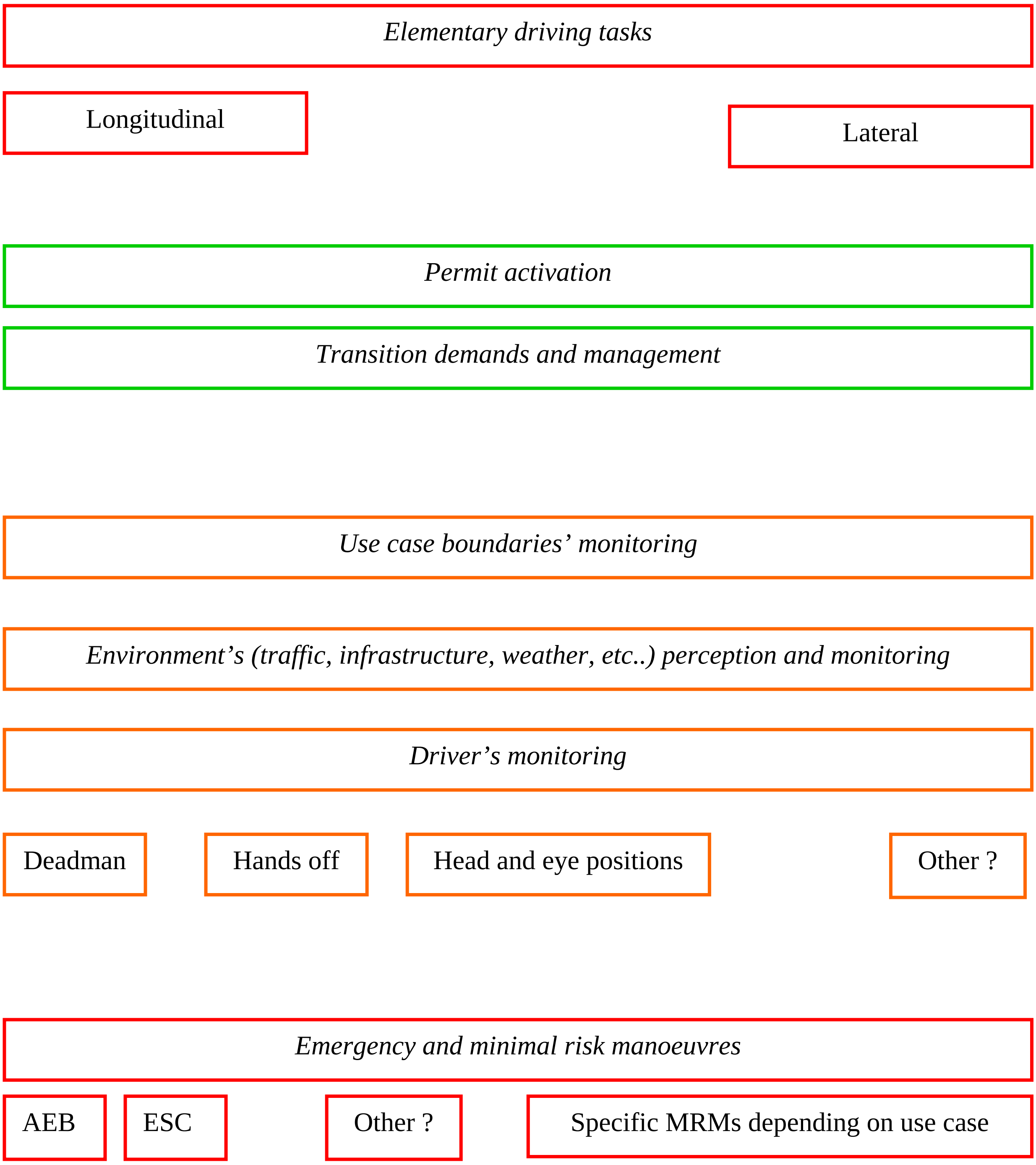
Situation and event attribute	***Possible values***
Driving objective	Lane keep Lane change
Driving infrastructure environment	2 * X lanes, separated driving ways, no entry / exit End of lane / lane merge Exit Merging ramp
Driving traffic environment	Fluid Dense
Driving weather / light conditions	Normal 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 <u>or</u> lateral control.	• Longitudinal <u>and</u> 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.	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
		4-A driver availability 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)	