Informal document **GRVA-02-11**
2nd GRVA, 28 January - 1 February 2019
Agenda item 5(a)

New validation approaches for automated driving safety

Preliminary views and link with informal working group of GRVA

GRVA-02
29 January – 02 February 2019

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

Outline

- Bird's-eye views
- Need for new validation approaches
- Addressing systems failures and driving hazards
- Manœuvres-based approach and challenges
- Possible focuses for public validation / approval
- Open questions
- Synthesis

Bird's-eye views (1)

1. Validation should handle a ***wide variety of use-cases*** (functions, ODDs, manœuvres)
2. Validation should verify that ***reasonnably foreseable risks***, combining system failures and driving hazards, are identified and addressed, and their impacts are minimized
3. ***Transparency of managing risk scenarios*** for safety analysis, is key to build a proper balance between internal validation processes and public validation scruitiny
4. Validation by public authorities should :
   - focus on ***driving responses (manoeuvers)*** to systems failures and driving hazards
   - assess both :
     - critical manœuvres' safety, responding to edge scenarios
     - current manœuvres carefullness or roadmanship
   - combine ***physical tests, simulations and audits*** of internal safety demonstration processes

Bird's-eye views (2)

5. Physical tests should combine :
   - a ***standardized approach***, for a limited set of common functions or manœuvres
   - a ***use-cas-specific approach***, based on risk analysis, including randomly
6. Process audit should be based on ***manageable and interpretable descriptions*** of :
   - system architectures
   - manoeuvers overarching safety rules
   - risk screening and scoring methods and relevant results
     - including system failures and driving hazards scenarios
   - risk mitigation measures and their internal validation processes
     - including simulation methods

Need for new validation approaches

- Limits of « vertical » approaches
  - # vehicle components / functions
  - Interactions vehicle / driver / driving environment
  - Connectivity
  - Learning systems
- Need for a comprehensive approach
  - Increasing variety of use cases
    - # automated functions
    - # design domains
    - # triggering + transition conditions
  - Need for a performance-based approach
    - Technology agnostic
    - Adaptable to various use-cases + functional and technical architectures

Use case =

Automated driving functions (AD)

+ Operational design domain (ODD)

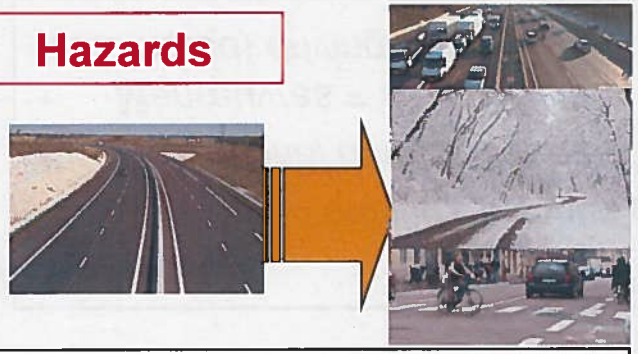
+ Manœuvres = sequence of (automated) driving tasks

Safety validation : overall approach

AD system's functions

Driving conditions

Hazards



Failures

Events

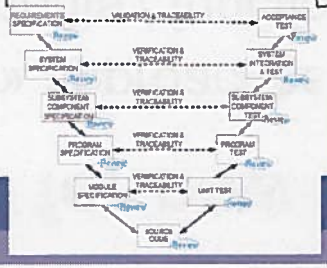
Redundancy

Manoeuvres

Responses

Fail-safe, Limp-home, Minimum risk

ISO 26262



Ongoing extension to safety in use – PAS 21448

Safety level

Increasingly critical for validation

→ manoeuvers based approach

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

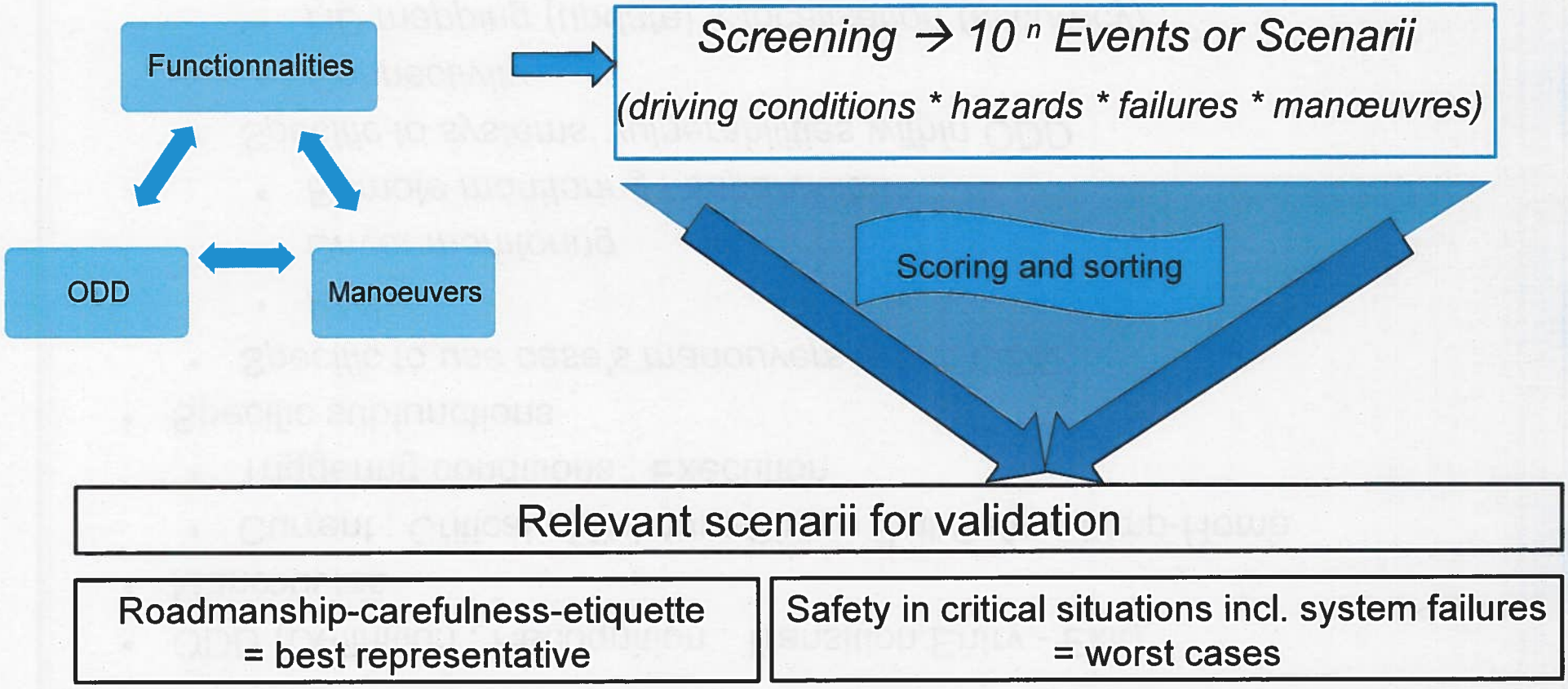
MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

Manoeuvers-based approach : candidate validation blocks

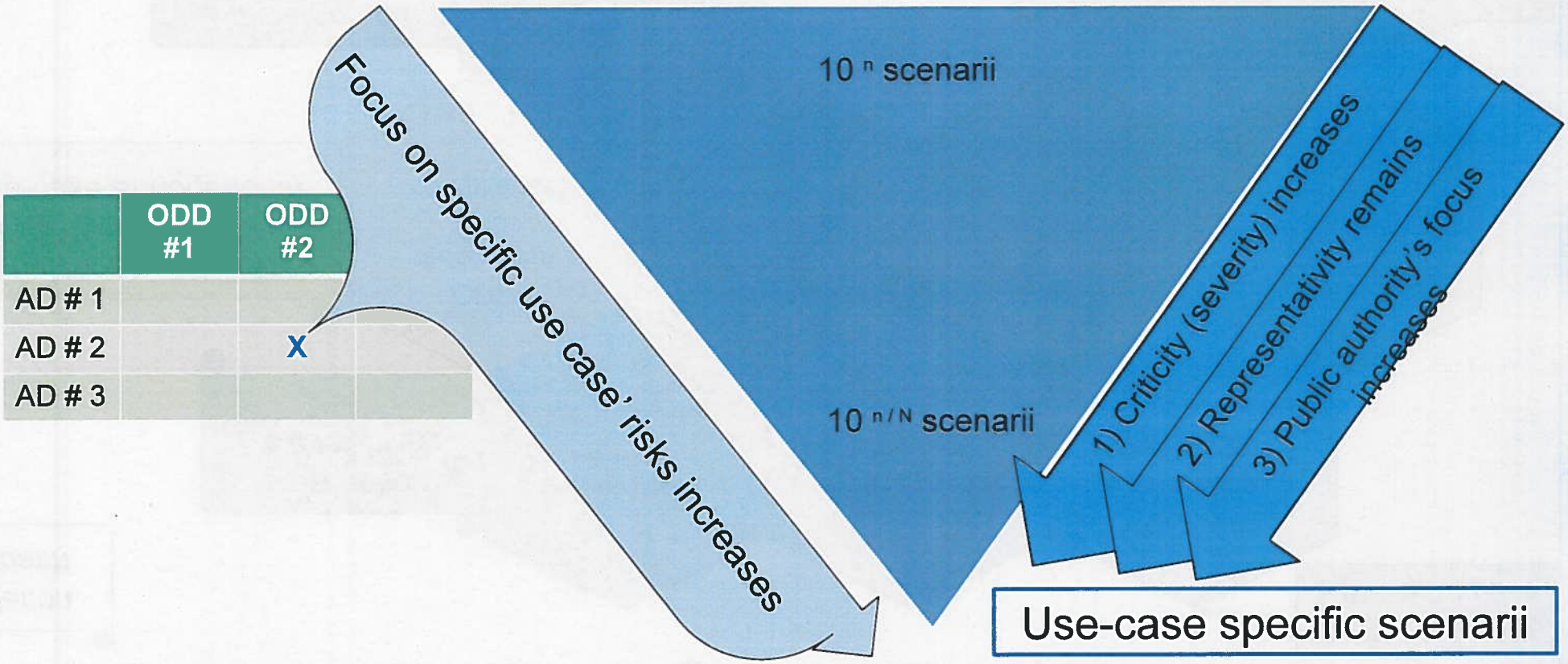
- ODD (Definition ; Recognition ; Transition Entry - Exit)
- Manœuvres
  - Current ; Critical ; Minimum-Risk – Fail-Safe – Limp-Home
  - Triggering conditions ; Execution
- Specific subfunctions
  - *Specific to use case's manouvers within ODD*
    - *HMI*
    - *Driver monitoring*
    - *Remote monitoring / supervision*
  - *Specific to systems' vulnerabilities within ODD*
    - *Connectivity*
    - *HD mapping (update) + localisation (accuracy)*
    - *Perception*

➢ ***+ Scenarii for risk-assessment***

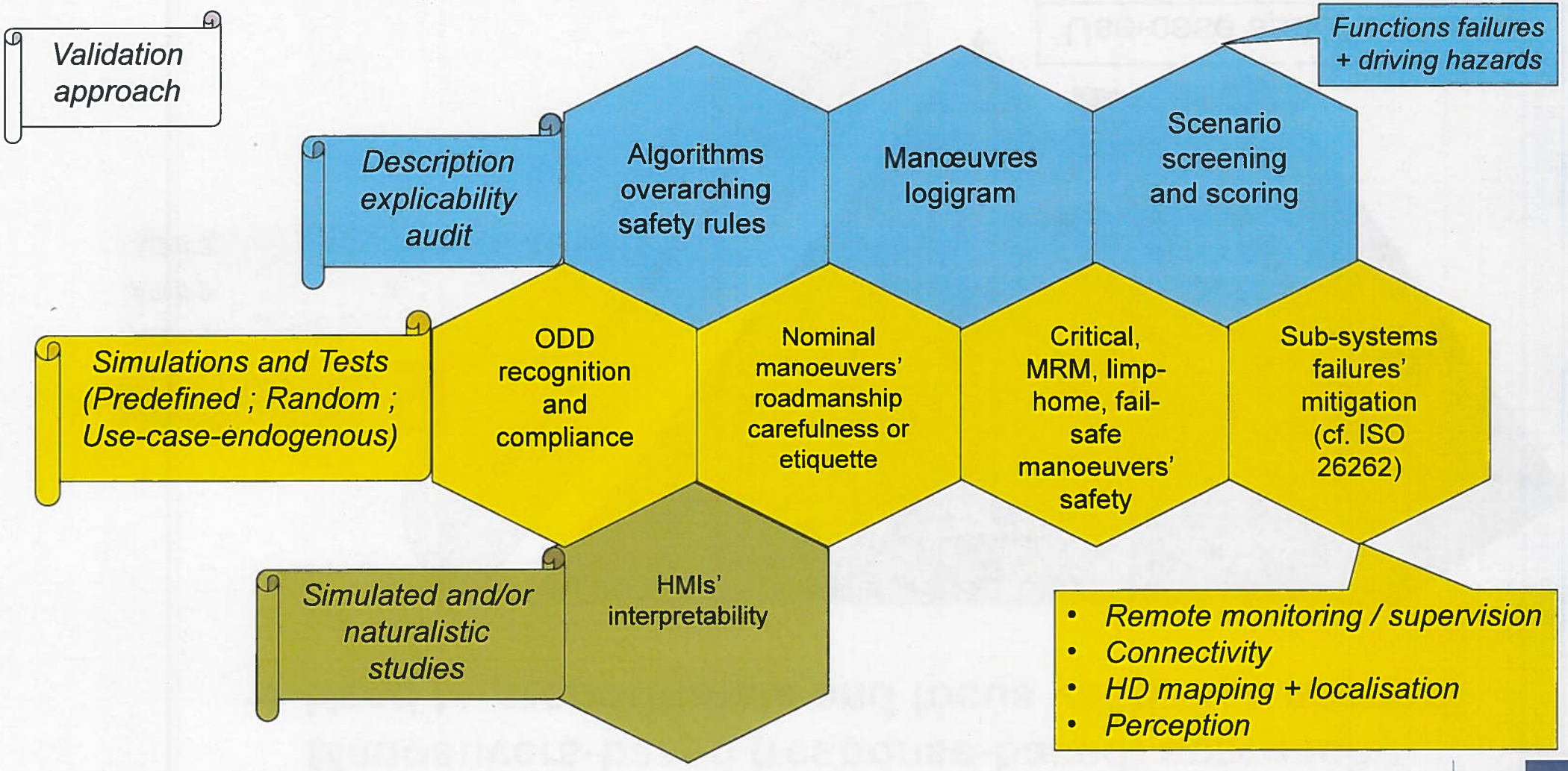
Manoeuvers-based (response-based) approach
→ managing scenarii becomes a major validation building block



Manoeuvers-based (response-based) approach :
→ Need to proportionate and focus validation scenarii



Main validation building blocks and approaches



	Blocks	***Authorities' possible focuses for validation***				
		Response analysis				
		Manoeuvres explicability		*Manœuvres safety*		
		Description audit	*Behavior studies*	*Simulation (relevant)*	*Tests (closed)*	*Driving (open)*
ODD	ODD definition	*	*			
	ODD recognition + Entry – Exit management	*		*	*	*
Manœuvres	Manoeuvres logigram	*	*			
	Manoeuvers triggering conditions	*	*	*	*	
	Nominal manoeuvres carefulness	*			*	*
	Critical manoeuvres safety	*		*	*	
	MRM, Fail Safe, Limp Home safety	*		*	*	
	HMIs interpretability, Driver Monitoring safety	*	*	*	*	*
	Supervision, remote monitoring safety	*		*	*	
Systems failures mitigation	Connectivity	*		*	*	
	Positionning	*		*	*	
	Perception	*		*	*	

Organization of work in GRVA

Suggestion to have 2 informal groups on automated vehicles (as defined priorities) :

- 1 for functionnal requirements (link to table TRANS/WP.29/1140)
- 1 for methods of demonstration of safety – compliance to functionnal requirements

⇒ Working together ? In parallel ? With the same experts ? How to finish the work of ALKS (B2 low speed) ?

VMAD should define :

- proposal for an appropriate toolbox (validation tool / level of validation) per key blocks (see previous tentative proposal table) or per main use cases (urban - motorway)
- proposal of usage of current tool (ISO 26262 - ISO PAS 21448 – others ?)
- proposal of physical tests corresponding to :
  - Functionnal requirements already defined
  - Types of critical scenarios identified
- Opportunity of an overall safety target (ex : 10^{-9} fatalities / km)

Validation building blocks, communication to authorities and needs for reference documents

Validation block	Communication to validation authorities	Reference document to be developped (under VMAD ?)
System and manœuvre description		
ODD	Description	Description rules for ODDs
System functional architecture	Description	Description rules for sub-functions
Logigram of manoeuvres	Description	Description rules for manoeuvers (nominal, critical, edge, minimum risk, fail-safe, limp-home) Description rules for triggering conditions
Overarching safety principles or rules for manoeuvers	Description	

Validation building blocks, communication to authorities and needs for reference documents

Validation block	Communication to validation authorities	Reference document to be developped (under VMAD ?)
Risk assessement		
Risk screening and scoring method (failures * driving hazards)	Description	(cf. ISO PAS 21448)
Identified worst-hyper-critical or edge scenarios	Description	Criteria for « edge » or « worst »
Identified best representative current or nominal scenarios	Description	Indicative list per ODD

Validation building blocks, communication to authorities and needs for reference documents

Validation block	Communication to validation authorities	Reference document to be developped (under VMAD ?)
System reliability		
Matrix : failures / effects / responses	Description	Description rules for critical vulnerabilities or failure scenarios by subfunctions
Failures mitigation-by-design strategy	Description	
Internal testing and simulation strategy and results	Description	

Validation building blocks, communication to authorities and needs for reference documents

Validation block	Communication to validation authorities	Reference document to be developped (under VMAD ?)
Manœuvres safety, roadmanship, carefullness and etiquette		
Internal testing and simulation strategy and results	Description	Pass / Fail principles or criteriae suitable for qualitative results (e.g. carefullness, etiquette)
HMIs		
HMIs interpretability (simulation or naturalistic) : method and resuts	Description	
Driver monitoring (simulation or testing) : method and results	Description	

Validation building blocks : need for common test references

Validation block	Reference testing document to be developped (under VMAD ?)
Critical manoeuvers in edge scenarios	Minimum set of driving scenario to be tested (per agregate ODD ?) Guidelines for setting random and / or use-case-engogenous tests Pass-Fail principles or criteriae
Minimum risk, fail-safe, limp-home	
Nominal manoeuvers in current situation	

Thank you

Note : Views presented in this document are preliminary. They should be considered as experts' input to UNECE/WP29/GRVA inception tasks. These views shouldn't be considered as formal position from french authorities.