# New validation approaches for automated driving safety

## G7 – Experts meeting on connected and automated driving

## 4-5 April 2019

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

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

# 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*

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

# 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

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

# 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

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

# Safety validation : overall approach

AD system's functions

Driving conditions

Events

Hazards

Failures

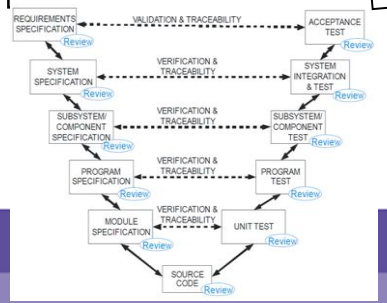
Responses

Redundancy

Manoeuvres

*Fail-safe, Limp-home, Minimum risk*

*ISO 26262*




*Ongoing extension to safety in use – PAS 21448*

Safety level

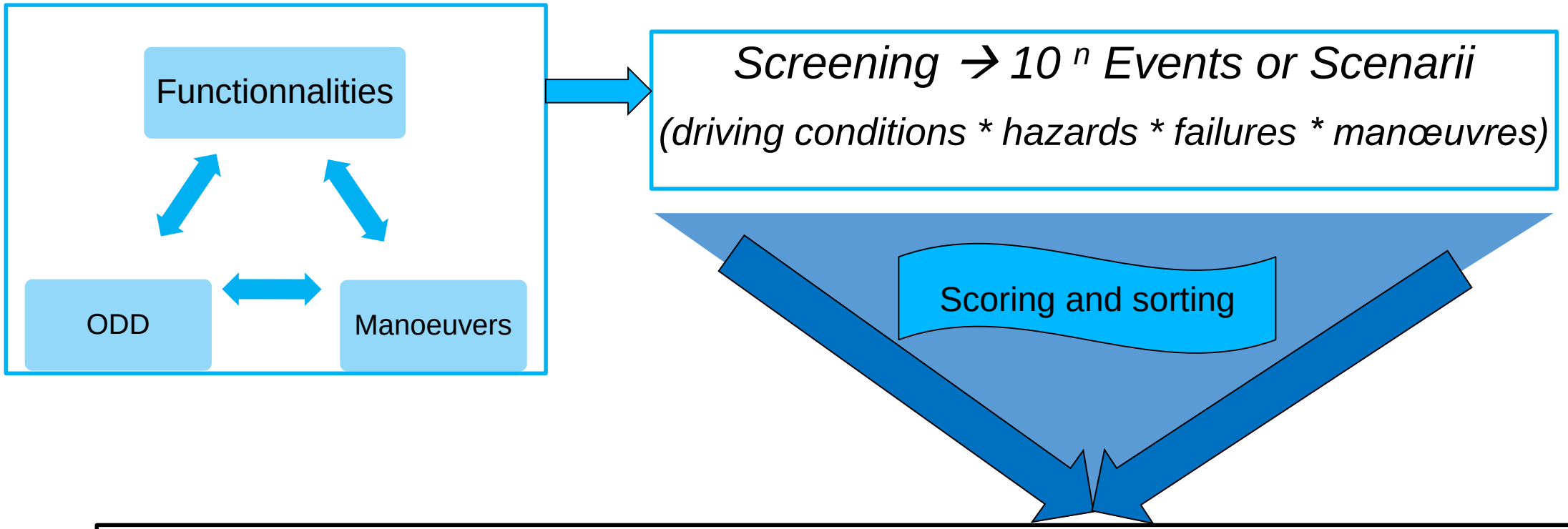
*Increasingly critical for validation*

*→ manoeuvers based approach*

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

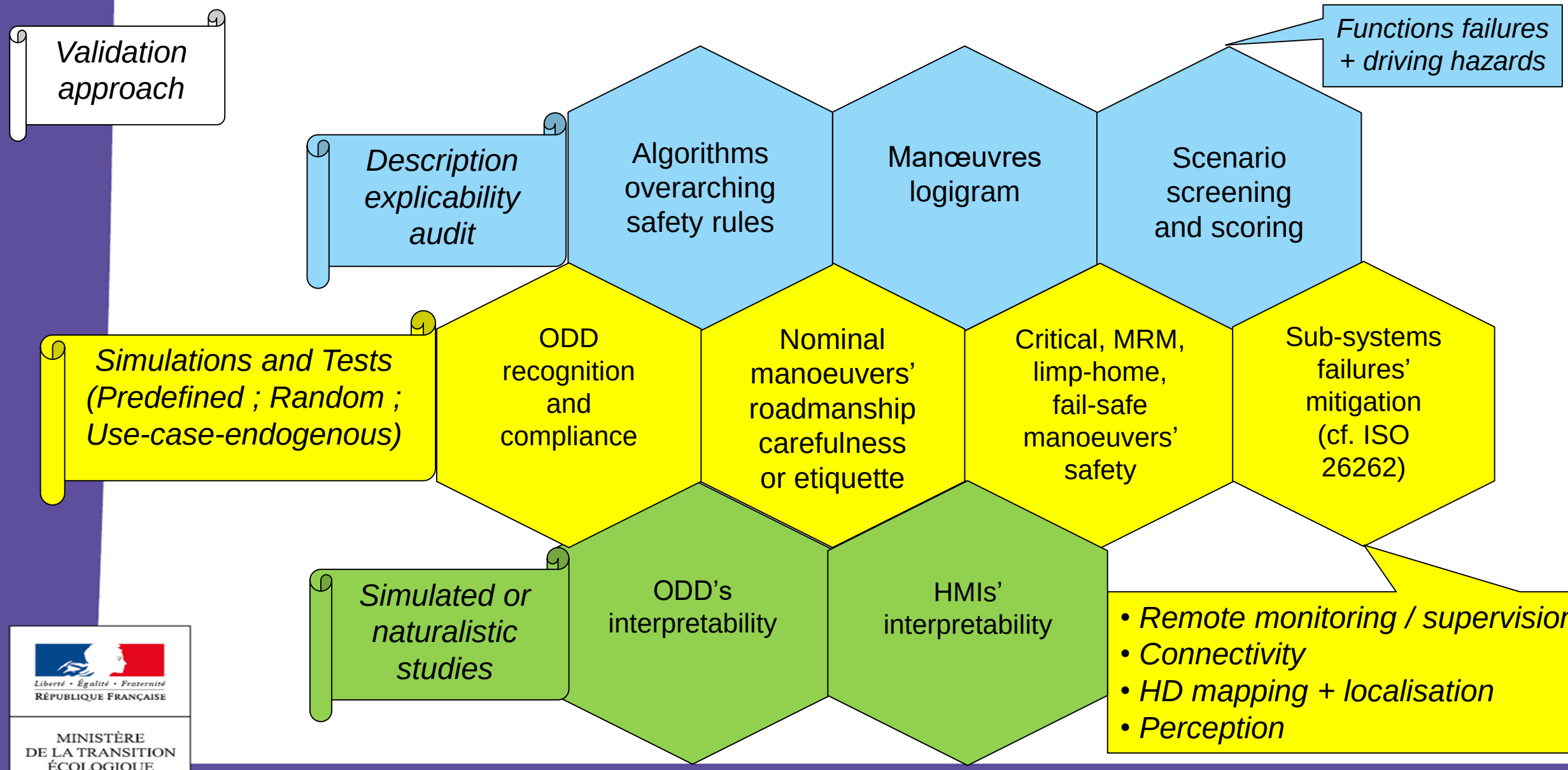
# Manoeuvers-based (response-based) approach
# → managing scenarii becomes a major validation building block




Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

# Main validation building blocks and approaches




Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE

# Possible set of validation blocks / documents (1/2)

| ***System and manœuvre description*** |
|---|
| ODD |
| System functional architecture |
| Logigram of manoeuvres |
| Overarching safety principles or rules for manoeuvers |
| ***Risk assessement and scenario management*** |
| Risk screening and scoring method (failures * driving hazards) |
| Identified worst-hyper-critical or edge scenarios |
| Identified best representative current or nominal scenarios |
| Driver monitoring (simulation or testing) : method and results |

# Possible set of validation blocks / documents (2/2)

| |
|---|
| ***System reliability*** |
| Matrix : failures / effects / responses |
| Failures mitigation-by-design strategy |
| Internal testing and simulation strategy and results |
| ***Manœuvres safety, roadmanship, carefullness and etiquette*** |
| Internal testing and simulation strategy and results |
| ***HMIs*** |
| HMIs interpretability (simulation or naturalistic) : method and resuts |
| Driver monitoring (simulation or testing) : method and results |

# Need for common test references

| Type of manoeuvre | Needed references |
|---|---|
| Critical manoeuvers in edge scenarios | Minimum set of driving scenario to be tested (per agregate ODD ?)<br>Guidelines for setting random and / or use-case-engogenous tests<br>Pass-Fail principles or criteriae |
| Minimum risk, fail-safe, limp-home | |
| Nominal manoeuvers in current situation | |