

# **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*



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



*Use case =*

*Automated driving functions (AD)*

+ *Operational design domain (ODD)*

+ *Manœuvres = sequence of (automated) driving tasks*

- Need for a performance-based approach

- Technology agnostic
- Adaptable to various use-cases + functional and technical architectures

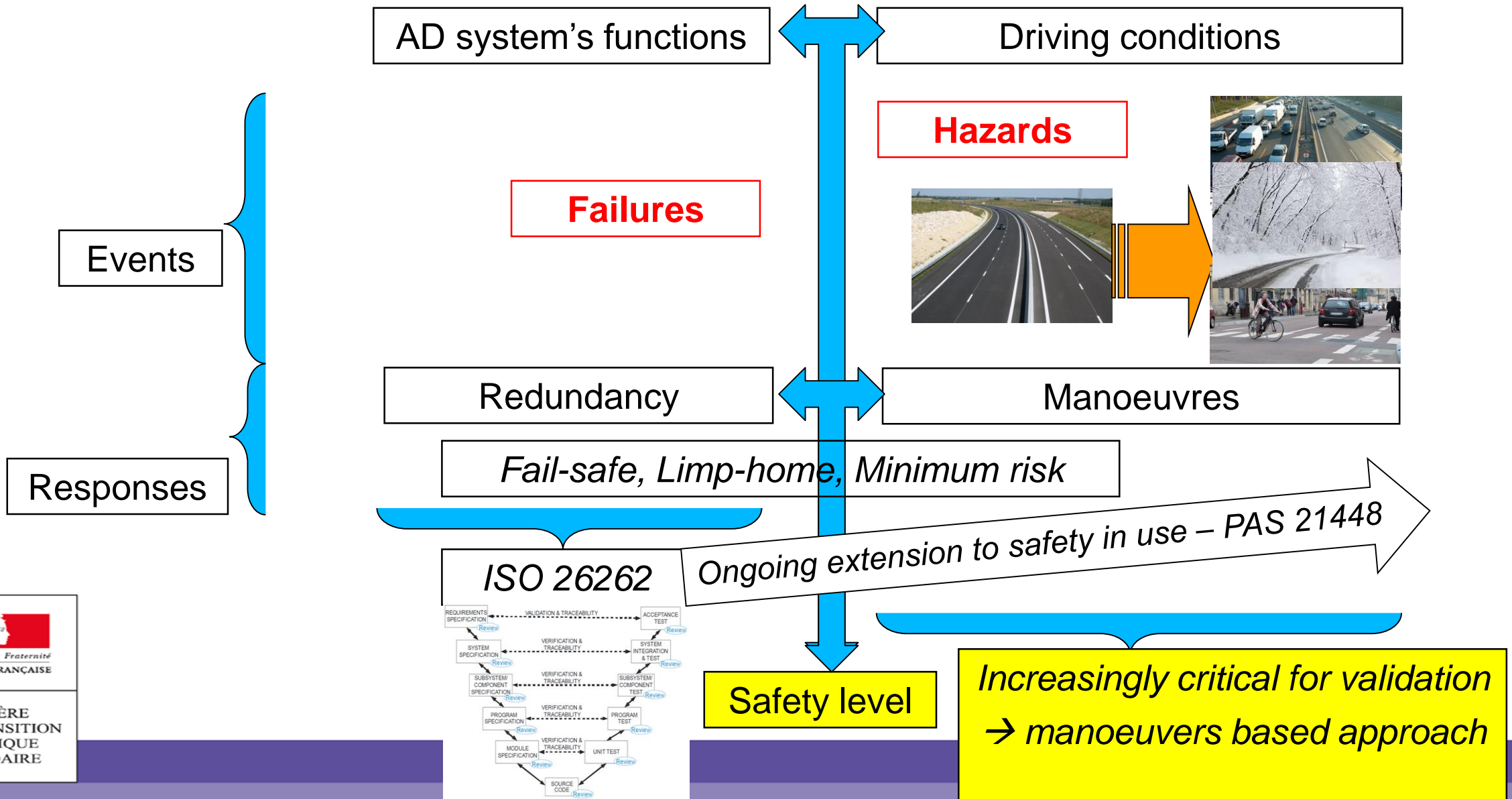
# Bird's-eye views (1)

1. Validation should handle a **wide variety of use-cases** (functions, ODDs, manoeuvres)
2. Validation should verify that **reasonably foreseeable 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 scrutiny
4. Validation by public authorities should :
  - focus on **driving responses (manoeuvres)** to systems failures and driving hazards
  - assess both :
    - critical manoeuvres' safety, responding to edge scenarios
    - current manoeuvres carefullness or roadmanship
  - combine **physical tests, simulations and audits** of internal safety demonstration processes

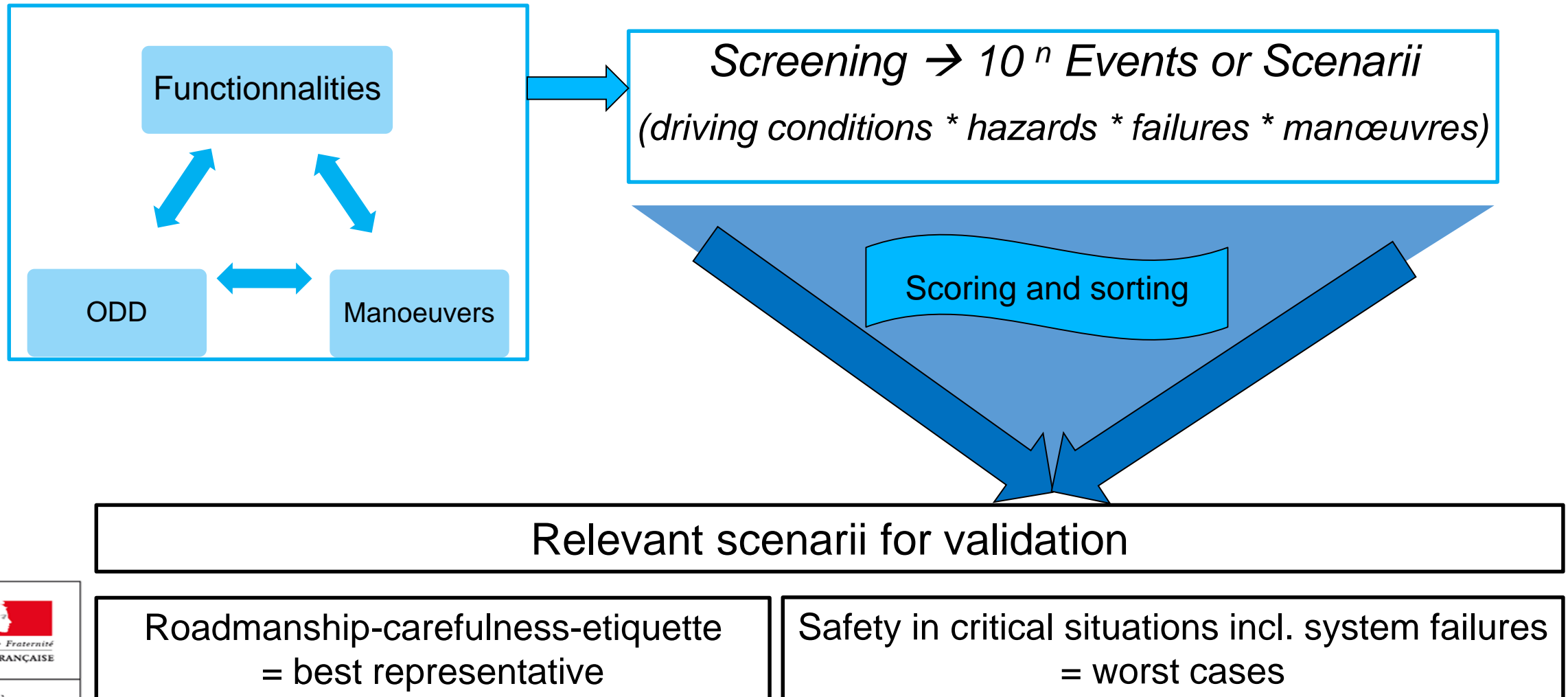
## Bird's-eye views (2)

5. Physical tests should combine :
  - a **standardized approach**, for a limited set of common functions or manoeuvres
  - 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
  - manoeuvres 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

# Safety validation : overall approach

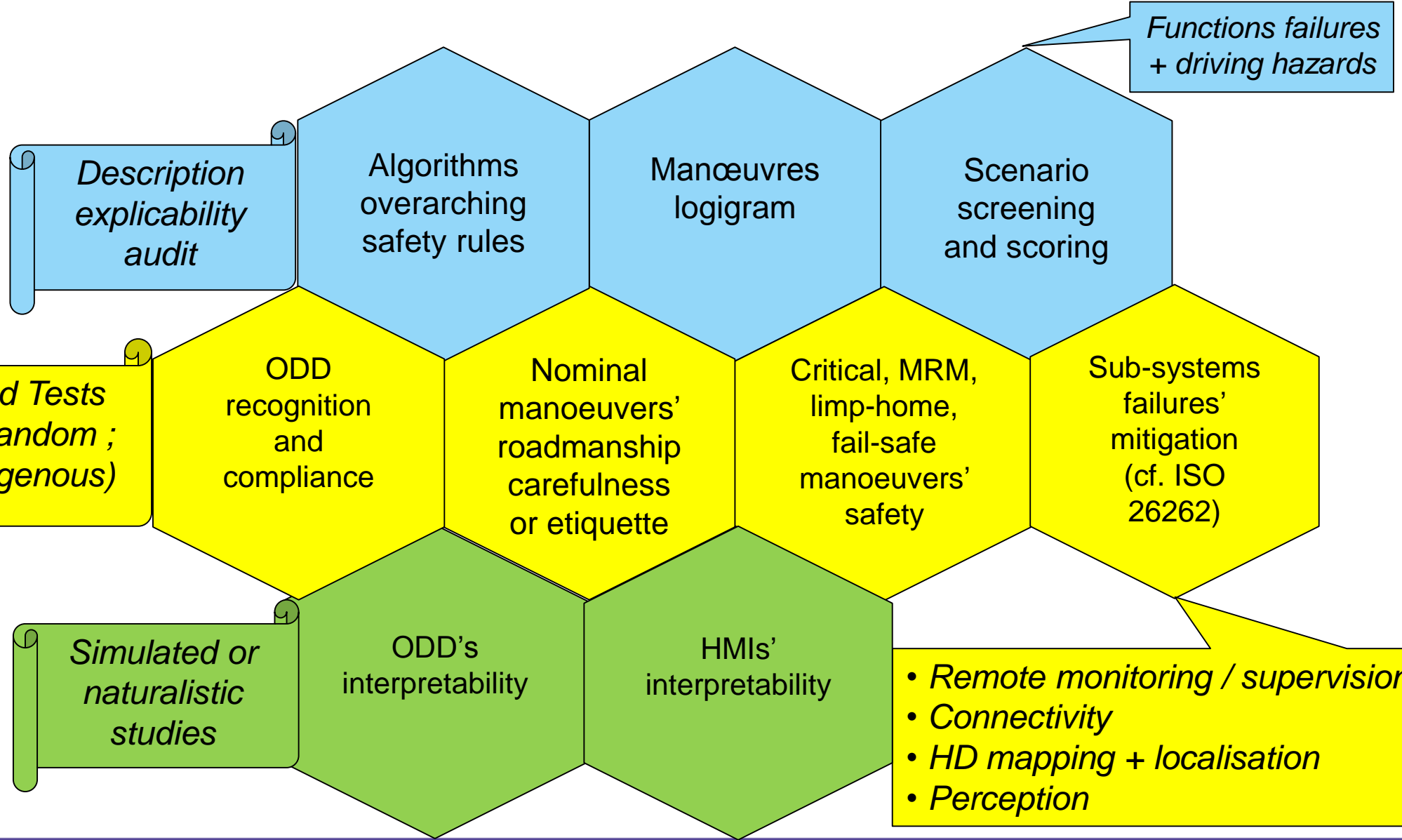


# Manoeuvres-based (response-based) approach → managing scenarii becomes a major validation building block



# Main validation building blocks and approaches

*Validation approach*



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

## ***System and manoeuvre description***

ODD

System functional architecture

Logigram of manoeuvres

Overarching safety principles or rules for manoeuvres

## ***Risk assessment 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

### ***Maœuvres safety, roadmanship, carefullness and etiquette***

Internal testing and simulation strategy and results

### ***HMIs***

HMIs interpretability (simulation or naturalistic) : method and results

Driver monitoring (simulation or testing) : method and results

## Need for common test references

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