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
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)
- Manoeuvres = sequence of (automated) driving tasks
1. Validation should handle a **wide variety of use-cases** (functions, ODDs, manœuvres)
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 manœuvres’ safety, responding to edge scenarios
     - current manœuvres carefulness or roadmanship
   - combine **physical tests, simulations and audits** of internal safety demonstration processes
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

- AD system’s functions
- Driving conditions
- Failures
- Hazards
- Redundancy
- Manoeuvres
- Fail-safe, Limp-home, Minimum risk
- ISO 26262
- Ongoing extension to safety in use – PAS 21448
- Increasingly critical for validation → manoeuvres based approach
Manoeuvers-based (response-based) approach → managing scenarii becomes a major validation building block

Screening → $10^n$ Events or Scenarii
(driving conditions * hazards * failures * manoeuvres)

Relevant scenarii for validation

- Roadmanship-carefulness-etiquette = best representative
- Safety in critical situations incl. system failures = worst cases
Main validation building blocks and approaches

Validation approach

Description explicability audit

Simulations and Tests (Predefined ; Random ; Use-case-endogenous)

- Remote monitoring / supervision
- Connectivity
- HD mapping + localisation
- Perception

Simulated or naturalistic studies

ODD recognition and compliance

Nominal manoeuvres’ roadmanship carefulness or etiquette

Critical, MRM, limp-home, fail-safe manoeuvres’ safety

Sub-systems failures’ mitigation (cf. ISO 26262)

 Algorithms overarching safety rules

Manoeuvres logigram

Scenario screening and scoring

Functions failures + driving hazards
Possible set of validation blocks / documents (1/2)

<table>
<thead>
<tr>
<th>System and manoeuvre description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODD</td>
</tr>
<tr>
<td>System functional architecture</td>
</tr>
<tr>
<td>Logigram of manoeuvres</td>
</tr>
<tr>
<td>Overarching safety principles or rules for manoeuvres</td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th><strong>System reliability</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Matrix: failures / effects / responses</td>
</tr>
<tr>
<td>Failures mitigation-by-design strategy</td>
</tr>
<tr>
<td>Internal testing and simulation strategy and results</td>
</tr>
</tbody>
</table>

**Manœuvres safety, roadmanship, carefulness 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

<table>
<thead>
<tr>
<th>Type of manoeuvre</th>
<th>Needed references</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical manoeuvres in edge scenarios</td>
<td>Minimum set of driving scenario to be tested (per aggregate ODD ?)</td>
</tr>
<tr>
<td>Minimum risk, fail-safe, limp-home</td>
<td>Guidelines for setting random and / or use-case-engenogenous tests</td>
</tr>
<tr>
<td>Nominal manoeuvres in current situation</td>
<td>Pass-Fail principles or criteriae</td>
</tr>
</tbody>
</table>