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
- Manoeuvres-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 **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 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
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
Safety validation: overall approach

- Events
  - AD system's functions
  - Hazards
  - Failures
  - Redundancy
    - Fail-safe, Limp-home, Minimum risk

- Responses
  - Drives conditions
  - Manoeuvres

ISO 26262

Increasingly critical for validation
→ manoeuvres based approach

Ongoing extension to safety in use – PAS 21448
Manoeuvres-based approach: candidate validation blocks

- ODD (Definition; Recognition; Transition Entry - Exit)
- Manoeuvres
  - Current; Critical; Minimum-Risk – Fail-Safe – Limp-Home
  - Triggering conditions; Execution
- Specific subfunctions
  - Specific to use case’s manoeuvres 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
Manoeuvres-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
Manoeuvres-based (response-based) approach:  
→ Need to proportionate and focus validation scenarii.
Main validation building blocks and approaches

- Verification approach

- Description explicability audit
- Algorithms overarching safety rules
- Manoeuvres logigram
- Scenario screening and scoring

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

- Simulated and/or naturalistic studies
- HMI’s interpretability

- Remote monitoring / supervision
- Connectivity
- HD mapping + localisation
- Perception
<table>
<thead>
<tr>
<th>Blocks</th>
<th>Authorities' possible focuses for validation</th>
<th>Response analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Maneuvres explicability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description audit</td>
</tr>
<tr>
<td>ODD</td>
<td>ODD definition</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>ODD recognition + Entry – Exit management</td>
<td>*</td>
</tr>
<tr>
<td>Manoeuvres</td>
<td>Manoeuvres logigram</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Manoeuvres triggering conditions</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Nominal manoeuvres carefulness</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Critical manoeuvres safety</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>MRM, Fail Safe, Limp Home safety</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>HMIs interpretability, Driver Monitoring safety</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Supervision, remote monitoring safety</td>
<td>*</td>
</tr>
<tr>
<td>Systems failures</td>
<td>Connectivity</td>
<td>*</td>
</tr>
<tr>
<td>mitigation</td>
<td>Positionning</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Perception</td>
<td>*</td>
</tr>
</tbody>
</table>
Organization of work in GRVA

Suggestion to have 2 informal groups on automated vehicles (as defined priorities):
• 1 for functional requirements (link to table TRANS/WP.29/1140)
• 1 for methods of demonstration of safety – compliance to functional 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:
  • Functional 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

<table>
<thead>
<tr>
<th>Validation block</th>
<th>Communication to validation authorities</th>
<th>Reference document to be developed (under VMAD ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System and manoeuvre description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODD</td>
<td>Description</td>
<td>Description rules for ODDs</td>
</tr>
<tr>
<td>System functional architecture</td>
<td>Description</td>
<td>Description rules for sub-functions</td>
</tr>
<tr>
<td>Logigram of manoeuvres</td>
<td>Description</td>
<td>Description rules for manoeuvers (nominal, critical, edge, minimum risk, fail-safe, limp-home)</td>
</tr>
<tr>
<td>Overarching safety principles or rules for manoeuvers</td>
<td>Description</td>
<td>Description rules for triggering conditions</td>
</tr>
</tbody>
</table>
Validation building blocks, communication to authorities and needs for reference documents

<table>
<thead>
<tr>
<th>Validation block</th>
<th>Communication to validation authorities</th>
<th>Reference document to be developed (under VMAD ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk assessment</strong></td>
<td>Description</td>
<td>(cf. ISO PAS 21448)</td>
</tr>
<tr>
<td>Risk screening and scoring method (failures * driving hazards)</td>
<td>Description</td>
<td>Criteria for « edge » or « worst »</td>
</tr>
<tr>
<td>Identified worst-hyper-critical or edge scenarios</td>
<td>Description</td>
<td>Indicative list per ODD</td>
</tr>
<tr>
<td>Identified best representative current or nominal scenarios</td>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Validation building blocks, communication to authorities and needs for reference documents

<table>
<thead>
<tr>
<th>Validation block</th>
<th>Communication to validation authorities</th>
<th>Reference document to be developed (under VMAD ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System reliability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Matrix : failures / effects / responses</td>
<td>Description</td>
<td>Description rules for critical vulnerabilities or failure scenarios by subfunctions</td>
</tr>
<tr>
<td>Failures mitigation-by-design strategy</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Internal testing and simulation strategy and results</td>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Validation building blocks, communication to authorities and needs for reference documents

<table>
<thead>
<tr>
<th>Validation block</th>
<th>Communication to validation authorities</th>
<th>Reference document to be developed (under VMAD ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manœuvres safety, roadmanship, carefullness and etiquette</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal testing and simulation strategy and results</td>
<td>Description</td>
<td>Pass / Fail principles or criteriae suitable for qualitative results (e.g. carefullness, etiquette)</td>
</tr>
<tr>
<td><strong>HMIs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMIs interpretability (simulation or naturalistic) : method and results</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Driver monitoring (simulation or testing) : method and results</td>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>
Validation building blocks: need for common test references

<table>
<thead>
<tr>
<th>Validation block</th>
<th>Reference testing document to be developed (under VMAD ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical manoeuvres in edge scenarios</td>
<td>Minimum set of driving scenario to be tested</td>
</tr>
<tr>
<td></td>
<td>(per aggregate ODD ?)</td>
</tr>
<tr>
<td>Minimum risk, fail-safe, limp-home</td>
<td>Guidelines for setting random and / or use-case-</td>
</tr>
<tr>
<td></td>
<td>engogenous tests</td>
</tr>
<tr>
<td>Nominal manoeuvres in current situation</td>
<td>Pass-Fail principles or criteriae</td>
</tr>
</tbody>
</table>
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.