New validation approaches for automated driving safety

French views

UN-ECE / GRVA / VMAD

October 2019

Direction générale des infrastructures, des transports et de la mer
Direction générale de l’énergie et du climat
French approach: bird-eye view

- Conception
  - Functional descriptions
  - OEM’s risk analysis, incl. tests and simulations

- Audit
  - Closed site tests
  - Open road examination
  - Perception / interpretation studies

- Performance validation
French approach: main focuses (1/3)

- **Focus on functional descriptions**
  - ODD
  - Manœuvres: activation / de-activation, triggering conditions and logigrams
  - Safety rules: high level + (national) driving codes
- Risk analysis:
  - **Focus on scenarios management (cf. bellow)**
  - **Focus on simulation relevance** (including calibration)

**Transparent management of scenarios for validation**
- Combining systems’ failures and driving hazards
- Representing nominal and edge situations

Utilisation for tests

In-use reporting procedure to be addressed
French approach: main focuses (2/3): scenarios screening and scoring

1. Screening
   - Collection
     - Open road
     - Closed site
     - Experts' input
     - Accidents
     - In-use
   - Cleaning and labelling
   - Projection on parameters-space

2. Completing
   - Completeness analysis
     - Incl. external references (use cases, expertise)
   - Generation
     - Parameters variation
     - Additional inputs

3. Scoring
   - Quality, usability
   - Criticity
     - Exposure, Severity, Controlability (ISO26262)

4. Exploiting
   - Relevance analysis for:
     - Simulation
     - Closed site test
     - Open road test
     - Behavioral studies
     - Other?

Possible criteriae:
Best representative = exposure ≥ E4 and severity ≥ S1
Worst case – edge = severity ≥ S3 and exposure ≥ E2
French approach: main focuses (3/3)

- Closed sites tests
  - Unitary manoeuvres, including MRMs and limp-home
  - Edge-critical situations (pre-defined + randomly extracted from risk analysis / scenario screening)
- Open road evaluation / examination
  - Compliance with ODD
  - Compliance with (national) driving rules (e.g. signals)
  - Manoeuvres’ chains / logigrams
  - Interactions with other road users (etiquette, anticipation)
- Perception / interpretation studies
  - ODD definition
  - Manoeuvres’ triggering conditions / chains / logigrams
  - HMIs (internal and external)
  - Driver monitoring in real time to check well understanding of HMI

Audit

Performance validation

Link with 2b subgroup
# High level safety rules (extracts)

<table>
<thead>
<tr>
<th>Technical</th>
<th>A single perception malfunction without failure should not induce a hazardous event. Consequently, the set of sensors used for the perception of a safety relevant environmental feature shall not be based on a single physical principle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODD</td>
<td>The vehicle shall not be in AD mode out of its ODD.</td>
</tr>
<tr>
<td>Driven</td>
<td>The vehicle shall manage risks according to the following rules:</td>
</tr>
<tr>
<td></td>
<td>o Vehicle shall not create accident by its own</td>
</tr>
<tr>
<td></td>
<td>o Vehicle shall be robust, as far as reasonably possible, to risks caused by others</td>
</tr>
<tr>
<td></td>
<td>o Vehicle shall comply with applicable driving rules (including those applicable to human drivers) unless it is the only way to avoid an accident</td>
</tr>
<tr>
<td></td>
<td>This rule shall be fulfilled:</td>
</tr>
<tr>
<td></td>
<td>o wherever the vehicle is driving (e.g. country, road, ...)</td>
</tr>
<tr>
<td></td>
<td>o whenever the vehicle is driving (e.g. despite dynamic lane assignment; time dependent rule, introduction of a new type of traffic sign; rule change ...)</td>
</tr>
<tr>
<td>Transitions</td>
<td>A deliberate driver action is required to activate AD mode.</td>
</tr>
<tr>
<td>AD ↔ Manual</td>
<td></td>
</tr>
<tr>
<td>Scenarios</td>
<td>The OEMs shall set up a common process to create and maintain a common catalog of scenario, including misuses, to be used for safety argumentation during design and verification/validation phase.</td>
</tr>
</tbody>
</table>
Some open questions

- Learning systems and releases (in use performance monitoring and evaluation)
- AD systems where (dedicated) infrastructure provides a significant part of safety
- AD systems where connectivity (supervision) provides a significant part of safety
- Specific subsystems deserving specific validation focus (for learning systems ?)
  - Perception + recognition + positionning + mapping
  - Connectivity (cf. above)
  - HMIs
Thank you