Future Certification of Automated Driving Systems

2019/01/28 - 2019/02/01, GRVA-02

Submitted by the experts of OICA
Introduction
Introduction

• With the introduction of automated driving systems the number of software-based functions and thereby complexity will continue to increase.

• Compared to conventional vehicles, the potentially affected safety-areas and variances of scenarios will increase and cannot fully be assessed with a limited number of tests that are performed on a test track or test bench.

• The aim of this presentation is to propose a new innovative certification scheme allowing to demonstrate the level of safety and reliability which allows for safe market introduction of automated/autonomous vehicles.

• The concept and building blocks for a future certification of automated/autonomous driving systems that are discussed in this presentation could be applied both under a type approval or self-certification regime.

• Application of a regulation under a self-certification regime requires precise descriptions of the procedures and tests to be applied by the manufacturer.

• This presentation is based on ECE/TRANS/WP.29/GRVA/2019/13 and several documents that OICA submitted under the activities of WP.29 IWG ITS/AD (see back-up).
General Challenges/Premises for a suitable Approach to Regulate Automated Driving

• It is important to consider that WP.29 GRVA is aiming at regulating new technologies of which the majority is not available on the market yet
  → lack of experience should not be neglected and tackled with reasonable strategies (e.g. generic safety-approaches/requirements) in order to guarantee the highest possible level of safety.

• It will be difficult to regulate each and every topic in detail from the early beginning
  → need to prioritize the different topics
  → start with a first set of requirements and develop further as the experience and data on new technologies grow

• Technology for Automated/Autonomous Driving Systems will continue to evolve rapidly over the next years
  → need flexible structures that can be applied to the different kinds of L3-L5 systems instead of limiting the variation/innovation of different kinds of systems by design restrictive requirements
  → Regulating “function by function” would require frequent updates/ upgrades of regulations and would therefore not be practical. Furthermore, it could easily become highly design restrictive

• Need to find a pragmatic way for industry and authorities that on the one hand leaves “controlled” flexibility and on the other hand defines reasonable requirements/principles to allow evolution of the new technology within the agreed safety principles over the next years
  → structure should allow to add output of research initiatives and lessons learned at a later stage
“Classical” Certification Approach
“Classical” Certification Approach

Example: Tires UN-R 30 and 54; UN-R 117

• Tire tests (“classical approach”):
  ➢ Mechanical strength: Load/speed performance tests
  ➢ Rolling sound emission values in relation to nominal section width and category of use
  ➢ Adhesion on wet surfaces (wet and snow grip index)
  ➢ Rolling resistance

→ The “classical certification approach” typically defines a limited number of performance criteria and physical certification tests to set-up the necessary safety-level as a prerequisite for market entrance

→ Such tests are performed on test tracks or on a test bench, requirements were refined over years

→ Approach is well suited for systems with limited complexity, limited interactions with other systems and clearly defined system boundaries (typical for mechanical systems/components)
Existing Extension of the “Classical” Certification Approach

Example: Performance of a braking system (UN-R 13-H)

• Braking Tests (“classical approach”):
  ➢ Min. deceleration: 6.43 m/s² and 2.44 m/s² for the fallback secondary braking system
  ➢ Stopping distance in relation to initial speed: 60 m for 100 km/h
  ➢ Parking brake to hold the laden vehicle stationary on a 20% up or down gradient

→ When ABS, ESP and Brake-Assist were regulated, it was realized that the “classical approach” was not able to address all safety-relevant areas of electric/electronic systems due to the high number of potential failures/scenarios:
  ➢ This led to the introduction of the process- and functional safety oriented audits: Annex 8 for safety of complex electronic vehicle control systems
  ➢ Introduction of simulation as acceptable simulation-approach for ESP

→ It should also be noted that at the time UN-R 13-H was updated regarding electronic control systems like ABS and ESP, such technologies were already deployed for some years and technically standardized (long-term-experience was available)
Further Extension of the “Classical” Certification Approach

Why the testing of the automated driving systems requires new elements:

- The number of software-based functions and thereby the system complexity will continue to increase with automated driving systems. Compared to the complex electronic control systems, the potentially affected safety-areas and variances of scenarios will further increase and cannot fully be assessed with a limited number of tests that are performed on a test track or test bench.

- The existing audit-approach used for electronic control systems both in safety systems (e.g. ABS, ESP) and driver assistance systems (L1, L2) should be further extended and upgraded to tackle L3-L5 systems.

Why elements of the “classical” approach are still necessary:

- Testing of existing conventional safety-regulations should continue with the “classical approach” also for vehicles that are equipped with automated driving systems.

- Furthermore, classical certification elements (track testing) are an essential part of the multi-pillar approach (see from slide 14). Additions are needed to appropriately cover the software related aspects – they will augment and not replace the classical certification approach.
“Multi-Pillar” Certification Approach
## Concept for certification

<table>
<thead>
<tr>
<th>Real-World Test Drive</th>
<th>Physical Certification Tests</th>
<th>Audit and Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Overall impression of system behavior on public roads</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Assessment of system’s ability to cope with real world traffic situations with a standardized checklist</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ “Driving license test“ for automated driving system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Guidance through given set of situations which shall be passed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Matching of audit/assessment results with real world behavior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Assessment of system behavior in fixed set of challenging cases, which either aren’t testable on public roads or cannot be guaranteed to occur during the real world test drive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Reproducibility of situations is given</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Audit of development process (methods, standards)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Assessment of safety concept (functional safety, safety of use) and measures taken</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Check of integration of general safety requirements and traffic rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Use of simulation results (high mileage approval, capability to cope with critical situations, which aren’t testable on proving grounds or in public)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Assessment of development data/field testing, OEM-self-declarations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Certification depends on all pillars – partial assessment doesn’t have significance
- Scope of work should reduce with every step (audit/assessment: largest scope – real world test drive: final confirmation)
- Safety for test witnesses and other road users – no endangering tests on public roads
- Concept can be augmented by additional “pillars” in terms of requirements/methods/tools as needed (lessons learned)
Example of the different pillars’ functions

- **Typical traffic scenarios**
  - Pedestrian crossing a crosswalk

- **Critical traffic scenarios**
  - Obstructed pedestrian crossing

- **Edge case scenarios**
  - Obstructed pedestrian crossing + cyclist overtaking

- Real World Test Drive
- Physical Certification Tests
- Audit and Assessment (e.g. simulation)

Graph shows:
- Scenario probability of occurrence in real-world traffic vs. complexity/risk of scenario.
- Typical scenarios with low probability and high efforts required.
- Critical scenarios with high probability and high risk.
- Edge case with low probability and high risk, requiring high efforts to identify and confirm performance!
Concept for certification – the pillars and their individual purpose

**Audit/Assessment**
- Understand the system to be certified
- Assess that the applied processes and design/test methods for the overall system development (HW and SW) are effective, complete and consistent
- Assess system’s strategies/rest performance to address (multiple) fault-conditions and disturbances due to deteriorating external influences; vehicle behavior in variations of critical scenarios
- Simulation: Test parameter variations (e.g. distances, speeds) of scenarios and edge-cases that are difficult to test entirely on a test track

**Physical Certification Tests**
- Assess critical scenarios that are technically difficult for the system to cope with, have a high injury severity (in case the system would not cope with such a scenario) and are representative for real traffic
- Compare with critical test cases derived from simulation and validate simulation tools

**Real World Test Drive**
- Assess the overall system capabilities and behavior in non-simulated traffic on public roads and show that the system has not been optimized on specific test scenarios
- Assess system safety requirements like e.g. HMI and ODD
- Assess that the system achieves a performance comparable to an experienced driver
Concept for certification of automated driving systems Level 3-5

Why the new approach can generate an equivalent/higher safety-level compared to the “classical” approach:

• The multi-pillar approach recognizes established process and functional safety oriented audits for certification of complex electronic vehicle control systems as a foundation.

• Consequently, this new approach requires manufacturers to give evidence that their system has been designed and tested in a way that complies with established safety principles, different traffic rules, and ensures safe performance both under fault-conditions and arbitrary external influences.

• Furthermore, the new approach evaluates specific complex situations on a test track.

• To complement the assessment, the new approach includes a real-world-drive test in real world traffic (non-simulated).
Deriving the scope of work
Some general safety-frameworks on national level are already available. They are not design-restrictive and could be further explored for regulatory use at UNECE

Shared global understanding of safety elements endeavored by OICA/AAPC
Back-Up
References

This presentation is based on

- ECE/TRANS/WP.29/GRVA/2019/13
- GRVA-02-09
- and on several documents that OICA submitted under the activities of WP.29 IWG ITS/AD and under the former TF AutoVeh including its subgroups 1 and 2:

- ITS_AD-12-11
- ITS_AD-13-05-Rev1
- ITS_AD-14-07
- TFAV-02-05
- TFAV-SG1-01-02
- TFAV-SG1-01-03
- TFAV-SG1-01-04
- TFAV-SG1-01-05
- TFAV-SG2-01-02
- TFAV-SG1-02-08
- TFAV-SG2-02-07
- SG1-03-10