Proposal for the Future Certification of Automated/Autonomous Driving Systems

Submitted by the experts from International Organization of Motor Vehicle Manufacturers**

The text reproduced below was prepared by the experts from the International Organization of Motor Vehicle Manufacturers (OICA). The aim of this document is, following the intervention of the expert from Germany as reflected in ECE/TRANS/WP.29/GRVA/1, para. 22, to provide information on the proposed new innovative certification scheme "3-pillar approach" needed for demonstrating the level of safety and reliability which allows for safe market introduction of automated/autonomous vehicles.

* Formerly: Working Party on Brakes and Running Gear (GRRF).
** In accordance with the programme of work of the Inland Transport Committee for 2018–2019 (ECE/TRANS/274, para. 123 and ECE/TRANS/2018/21/Add.1, Cluster 3), the World Forum will develop, harmonize and update UN Regulations in order to enhance the performance of vehicles. The present document is submitted in conformity with that mandate.
I. Introduction

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

2. 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.

3. The aim of this document 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.

4. 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.

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

6. This document is based on several documents that International Organization of Motor Vehicle Manufacturers (OICA) submitted under the activities of Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG on ITS/AD) and the former Task Force (TF) on Automated Vehicles testing ("AutoVeh") including its subgroups.

II. General Challenges/Premises for a suitable Approach to Regulate Automated Driving

7. It is important to consider that the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) is aiming at regulating new technologies of which the majority is not available on the market to date.

⇒ Therefore, the 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.

8. It will be difficult to regulate each and every topic in detail from the early beginning

⇒ Therefore, there is the need to prioritize the different topics and start with a first set of requirements and develop further as the experience and data on new technologies grow.

9. Technology for Automated/Autonomous Driving Systems will continue to evolve rapidly over the next years.

⇒ Therefore, there is the need flexible structures that can be applied to the different kinds of Level 3 to Level 5 (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 or upgrades of regulations and would therefore not be practical. Furthermore, it could easily become highly design restrictive.

10. Therefore, it is necessary 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.

11. Besides, the structure should allow to add output of research initiatives and lessons learned at a later stage.
### III. Comparison of published Safety Principles

<table>
<thead>
<tr>
<th>Safety Principles</th>
<th>USA (NHTSA FAVP 3.0)</th>
<th>Japan (MLIT-Guideline)</th>
<th>Canada (Transport Canada)</th>
<th>Europe (EC Guidance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision: “0” accidents with injury or fatality by ADV</td>
<td>Ensure Safety: Within ODD ADV shall not cause rationally foreseeable &amp; preventable accidents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Safe Function (Redundancy)</td>
<td>1) System Safety ii) System safety by redundancy</td>
<td>6) Safety systems (and appropriate redundancies)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Safety Layer</td>
<td>3) (OEDR) ii) Automatic stop in situations outside ODD iii) Compliance with safety regulation iv) Compliance with standards recommended vii) for unmanned services: camera link &amp; notification to service center</td>
<td>4) International standards and best practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Operational Design Domain</td>
<td>2) Operational Design Domain i) Setting of ODD</td>
<td>2) Operational design domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Behavior in Traffic</td>
<td>3) OEDR 12) Federal, State and local Laws</td>
<td>3) OEDR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Driver’s Responsibilities</td>
<td>iv) HMI – driver monitoring for conditional automation</td>
<td>1) Level of automation and intended use 2) Driver/operator/ passenger interaction – information; driver monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Vehicle Initiated Take-Over</td>
<td>4) Fallback (MRC) 6) HMI ii) Automatic stop in situations outside ODD iv) HMI – inform about planned automatic stop</td>
<td>3) Transition of driving task – lead time; MRM; HMI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Driver Initiated Transfer</td>
<td>6) HMI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 Effects of Automation</td>
<td>7) HMI and Accessibility of Controls – unsafe misuse</td>
<td>1) System performance in automated mode - takeover</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Safety Certificate

- viii) Safety evaluation via simulation, track & real world testing
- ix) In-use safety - inspection

### Data Recording

- 10) Data Recording
- v) Installation of data recording devices

### Security

- 7) Vehicle Cybersecurity
- vi) Cybersecurity – safety by design
- ix) In-use safety – software update

### Passive Safety

- 8) Crashworthiness

### Driver's training

- 11) Consumer Education/Training
- x) Information provision to users

### Conclusions:

- General safety-frameworks are available. They are not design-restrictive and could be further explored for regulatory use at UNECE
- Internationally harmonized safety principles are endeavored by OICA

### IV. "Classical" Certification Approach

#### Example: UN Regulations Nos. 30, 54 and 117 dealing with tyres

12. The tire tests ("classical approach") are:

- 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

13. 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.

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

15. This approach is well suited for systems with limited complexity, limited interactions with other systems and clearly defined system boundaries (typical for mechanical systems/components).

### V. Existing Extension of the "Classical" Certification Approach

#### Example: the performance of a braking system as regulated in UN Regulation No. 13-H

16. The braking tests ("classical approach") are:
• The minimum deceleration is 6.43 m/s² and 2.44 m/s² for the fallback secondary braking system.
• The stopping distance in relation to initial speed is 60 m for 100 km/h.
• Parking brake has to hold the laden vehicle stationary on a 20% up or down gradient.

17. 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 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.

18. It should also be noted that when UN Regulation No. 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).

VI. Further Extension of the "Classical" Certification Approach

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

19. The system complexity and thereby the number of software-based functions will continue to increase with automated driving systems. Compared to the Complex Electronic (CEL) 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.

20. 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.

B. Why elements of the "classical" approach are still necessary?

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

22. Furthermore, classical certification elements (track testing) are an essential part of the three-pillar approach. Additions are needed to appropriately cover the software related aspects. They will augment and not replace the classical certification approach.
VII. Paradigm shift - new approach required

Manual and assisted Driving

- "Classical" approach (for a single system/component)
- Driving capabilities
- Driving Permit
  - Theoretical Test
  - Practical test
  - Excerpt of driver’s capabilities

E.g. vehicle with ADAS support (L1/L2)

Conditional Driving Automation

- "Classical" approach (for a single system/component)
- Driving capabilities
  - Driving capability (DDT, OEDR) with the system during operation, but handover to driver necessary
- Driving Permit
  - Theoretical Test
  - Practical test
  - Excerpt of driver’s capabilities

E.g. vehicle with ACSF B2 (L3)

High/Full Driving Automation

- "Classical" approach (for a single system/component)
- Driving capabilities + more...
- Driving Permit
  - Theoretical Test
  - Practical test
  - Excerpt of driver’s capabilities

E.g. vehicle with L4 system without conventional driver

VIII. Overview: Concept for ADS Certification

A. Concept for certification – the three pillars

Real-World Test Drive

- Overall impression of system behavior on public roads
- Assessment of system’s ability to cope with real world traffic situations with a standardized checklist
- "Driving license test" for automated driving system
- Guidance through given set of situations which shall be passed

Physical Certification Tests

- Matching of audit/assessment results with real world behavior
- 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.
- Reproducibility of situations is given

Audit and Assessment

- Audit of development process (methods, standards)
- Assessment of safety concept (functional safety, safety of use) and measures taken
- Check of integration of general safety requirements and traffic rules
- Use of simulation results (high mileage approval, capability to cope with critical situations, which aren’t testable on proving grounds or in public)

Simulation
• Certification depends on all three pillars – partial assessment doesn’t have significance
• The 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

B. Example of the different pillars’ functions

Scenario probability of occurrence in real world traffic

Complexity/risk of scenario

Typical traffic scenarios

Pedestrian crossing a crosswalk

Obstructed pedestrian crossing

Critical traffic scenarios

Obstructed pedestrian crossing + cyclist overtaking

Edge case scenarios

low probability, but high efforts to identify and confirm

Real World Test Drive

Physical Certification

Audit and Assessment (e.g. simulation)
C. Concept for certification – the three pillars and their individual purpose

<table>
<thead>
<tr>
<th>Audit/Assessment</th>
<th>Physical Certification Tests</th>
<th>Real World Test Drive</th>
</tr>
</thead>
</table>
| - 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 | - Assess critical scenarios that are technically difficult for the system, have a high injury severity and are representative for real traffic  
- Compare with critical test cases derived from simulation and validate simulation tools | - 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 |

D. Concept for certification of automated driving systems Level 3-5

(a) Why the new approach can generate an equivalent/higher safety-level compared to the "classical" approach?


24. Consequently, the 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.

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

26. To complement the assessment, the new approach includes a real-world-drive test in real world traffic (non-simulated).
IX.  Mapping of Safety Principles and the Pillars

A.  Comparison of published Safety Principles

<table>
<thead>
<tr>
<th>Safety Principles</th>
<th>USA (NHTSA FAVP 3.0)</th>
<th>Japan (MLIT-Guideline)</th>
<th>Canada (Transport Canada)</th>
<th>Europe (EC Guidance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision: &quot;0&quot; accidents with injury or fatality by ADV</td>
<td>Ensure Safety: Within ODD ADV shall not cause rationally foreseeable &amp; preventable accidents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Safe Function (Redundancy)</td>
<td>1) System Safety 9) Post Crash Behavior</td>
<td>ii) System safety by redundancy</td>
<td>6) Safety systems (and appropriate redundancies)</td>
<td>7) Safety assessment – redundancy; safety concept</td>
</tr>
<tr>
<td>2 Safety Layer</td>
<td>3) (OEDR)</td>
<td>ii) Automatic stop in situations outside ODD iii) Compliance with safety regulation iii) Compliance with standards recommended vii) for unmanned services: camera link &amp; notification to service center</td>
<td>4) International standards and best practices</td>
<td>2) Driver/operator/ passenger interaction - takeover delay; camera &amp; voice link for driverless systems</td>
</tr>
<tr>
<td>3 Operational Design Domain</td>
<td>2) Operational Design Domain</td>
<td>i) Setting of ODD</td>
<td>2) Operational design domain</td>
<td>1) System performance in automated mode – description 2) Driver/operator/ passenger interaction – boundary detection</td>
</tr>
<tr>
<td>4 Behavior in Traffic</td>
<td>3) OEDR 12) Federal, State and local Laws</td>
<td></td>
<td>3) OEDR</td>
<td>1) System performance in automated mode – behavior 4) MRM – traffic rules; information</td>
</tr>
<tr>
<td>5 Driver’s Responsibilities</td>
<td>4) Fallback (MRC) 6) HMI</td>
<td>iv) HMI – driver monitoring for conditional automation</td>
<td>1) Level of automation and intended use 7) HMI and access of controls – accidental misuse</td>
<td>2) Driver/operator/ passenger interaction – information; driver monitoring</td>
</tr>
<tr>
<td>6 Vehicle Initiated Take-Over</td>
<td>4) Fallback (MRC) 6) HMI</td>
<td>ii) Automatic stop in situations outside ODD iv) HMI – inform about planned automatic stop</td>
<td></td>
<td>3) Transition of driving task – lead time; MRM; HMI 4) MRM</td>
</tr>
<tr>
<td>7 Driver Initiated Transfer</td>
<td>6) HMI</td>
<td></td>
<td>7) HMI and Accessibility of Controls</td>
<td>1) System performance in automated mode - takeover</td>
</tr>
<tr>
<td>8 Effects of Automation</td>
<td></td>
<td></td>
<td>7) HMI and Accessibility of Controls – unsafe misuse</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Safety Certificate</td>
<td>viii) Safety evaluation via simulation, track &amp; real world testing ix) In-use safety - inspection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Data Recording</td>
<td>10) Data Recording v) Installation of data recording devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12) User privacy 13) Collaboration with government agencies &amp; law enforcement 5) Data storage system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Security</td>
<td>7) Vehicle Cybersecurity vi) Cybersecurity – safety by design ix) In-use safety – software update</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10) Cyber security 11) System update 6) Cyber security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Passive Safety</td>
<td>8) Crashworthiness</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9) User protection during collision &amp; system failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Driver’s training</td>
<td>11) Consumer Education/Training x) Information provision to users</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8) Public education and awareness 8) information provision to users</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conclusions:**

- General safety-frameworks are available. They are not design-restrictive and could be further explored for regulatory use at UNECE
- Internationally harmonized safety principles are endeavored by OICA
### B. Coverage of safety principles by the pillars

<table>
<thead>
<tr>
<th>Safety Principles</th>
<th>Audit/Assessment</th>
<th>Track Testing</th>
<th>Real-World-Test-Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> X = OICA views on how some requirements could be reasonably addressed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Safe Function (e.g. failure strategy, redundancy concepts, etc.)</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2 Safety Layer (OEDR, Emergency Maneuvers)</td>
<td>X X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Operational Design Domain (definition, recognition of the limits)</td>
<td>X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Behavior in Traffic (OEDR, compliance with traffic laws)</td>
<td>X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Driver’s Responsibilities (HMI, Driver Monitoring)</td>
<td>X X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Vehicle Initiated Take-Over (Minimum Risk Maneuver, transition scenario, HMI, etc.)</td>
<td>X X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Driver Initiated Transfer (e.g. activation, deactivation, override)</td>
<td>X X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 Effects of Automation (Driver Monitoring, System Design, driver’ support)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Safety Certificate (in-use-safety, testing and validation, etc.)</td>
<td>X X X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Data Recording</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Security</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 Passive Safety Testing of existing conventional safety-regulations continues with the &quot;classical approach&quot; (update of such regulations will be necessary)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Driver’s training</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

may be covered by conventional regulation
Annex

References

27. This document is based on several working papers that OICA submitted under the activities of the IWG on ITS/AD and under the former Task Force on Automated Vehicle testing "AutoVeh" including its two subgroups (available on the UNECE website https://wiki.unece.org/pages/viewpage.action?pageId=2523340):

(a) From the IWG on ITS/AD
   ITS_AD-12-11
   ITS_AD-13-05-Rev.1
   ITS_AD-14-07

(b) From the Task Force on Automated Vehicle testing "AutoVeh"
   TFAV-02-05

(c) From the Subgroup 1 of the TF AutoVeh
   TFAV-SG1-01-02
   TFAV-SG1-01-03
   TFAV-SG1-01-04
   TFAV-SG1-01-05
   TFAV-SG1-02-08
   TFAV-SG1-03-10

(d) From the Subgroup 2 of the TF AutoVeh
   TFAV-SG2-01-02
   TFAV-SG2-02-07