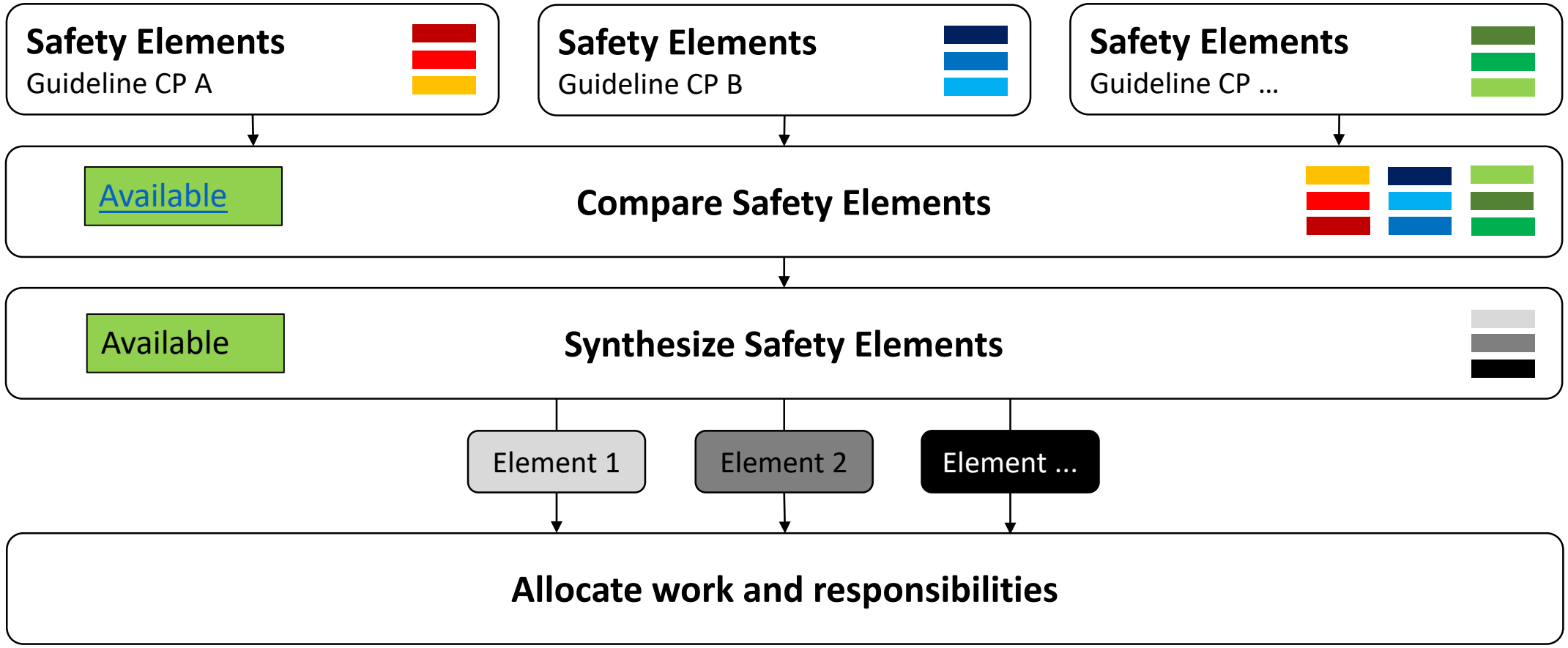
Submitted by OICA

Informal Document WP.29-177-20
177th session of WP.29, 12-15 March 2019,
agenda item 2.3.

OICA views on the certification of automated / autonomous vehicle

How to derive the scope of work

Proposal: utilize what is readily available



→ **Some general safety-frameworks on national level are already available. They are not design-restrictive**
→ **Requirements and verification tests not to be split in two groups**

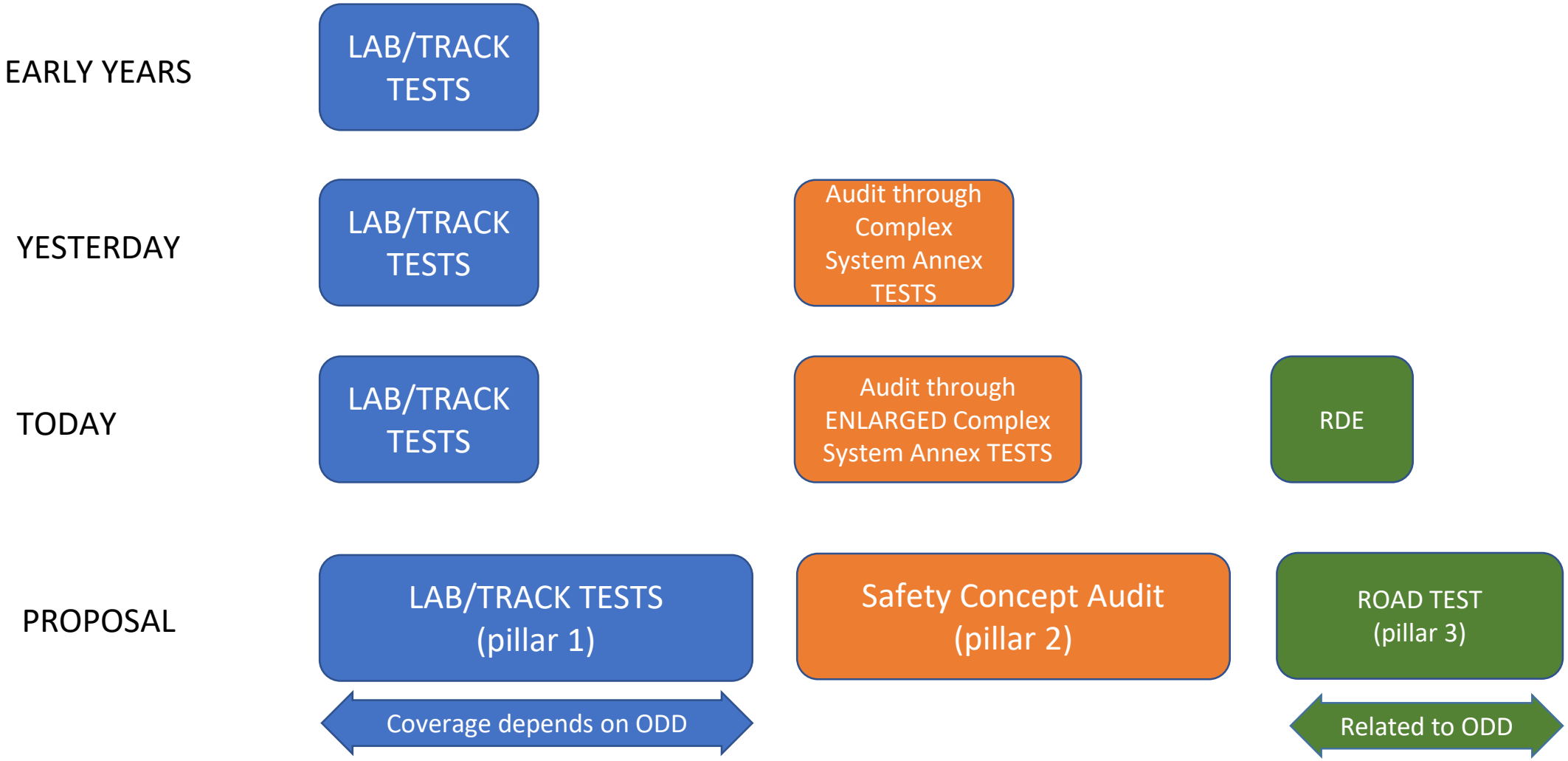
Introduction

Introduction

- 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 addition to the established certification schemes** (aka “Multi-Pillar Approach”) allowing to demonstrate the level of safety and reliability needed 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**
- 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)

“Classical” Certification Approach Versus the “Multi Pillar Approach”

The „Multi-Pillar-Approach“ **Augments** the „Classical“ Certification Approach



Further Extension of the “Classical” Certification Approach

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

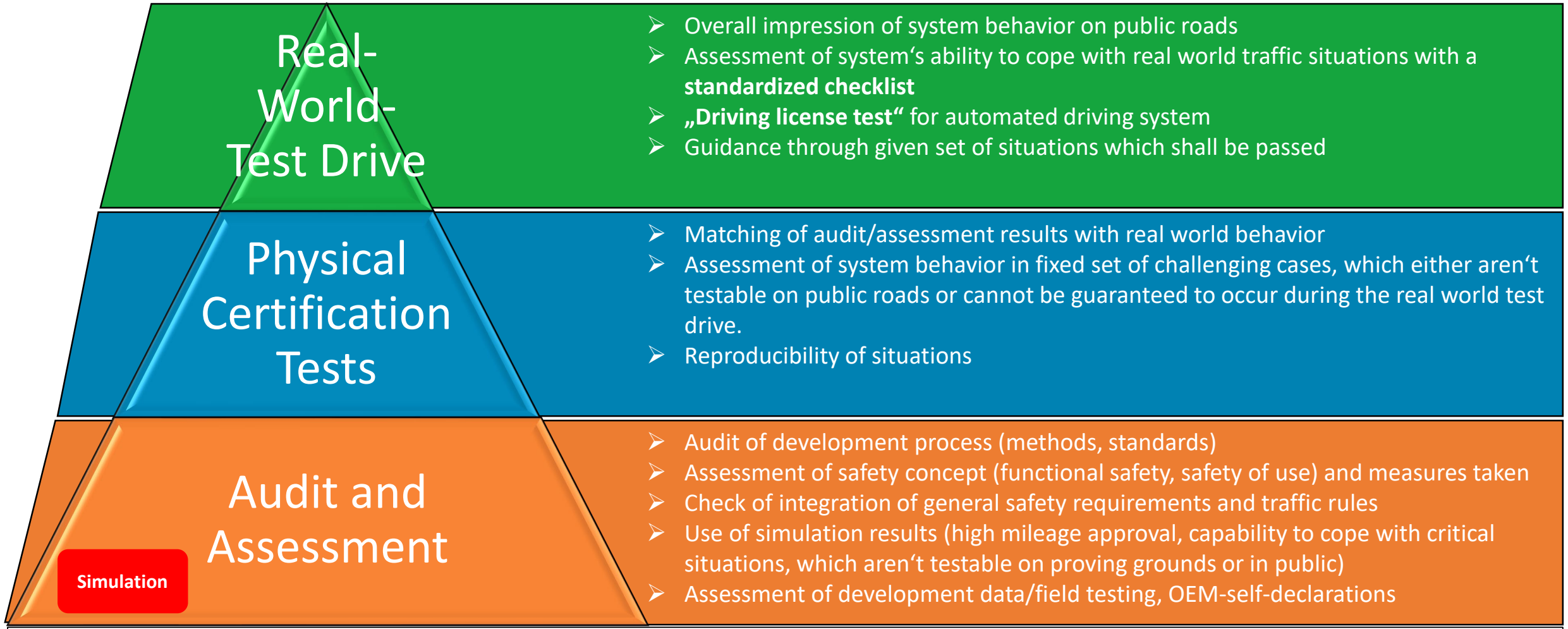
- The number of software-based functions and thereby the system complexity will continue to increase with automated driving systems. Compared to the complex electronic control systems, the potentially affected safety-areas and variances of scenarios will further increase and cannot fully be assessed 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. Additions are needed to appropriately cover the software related aspects – they will augment and not replace the classical certification approach.

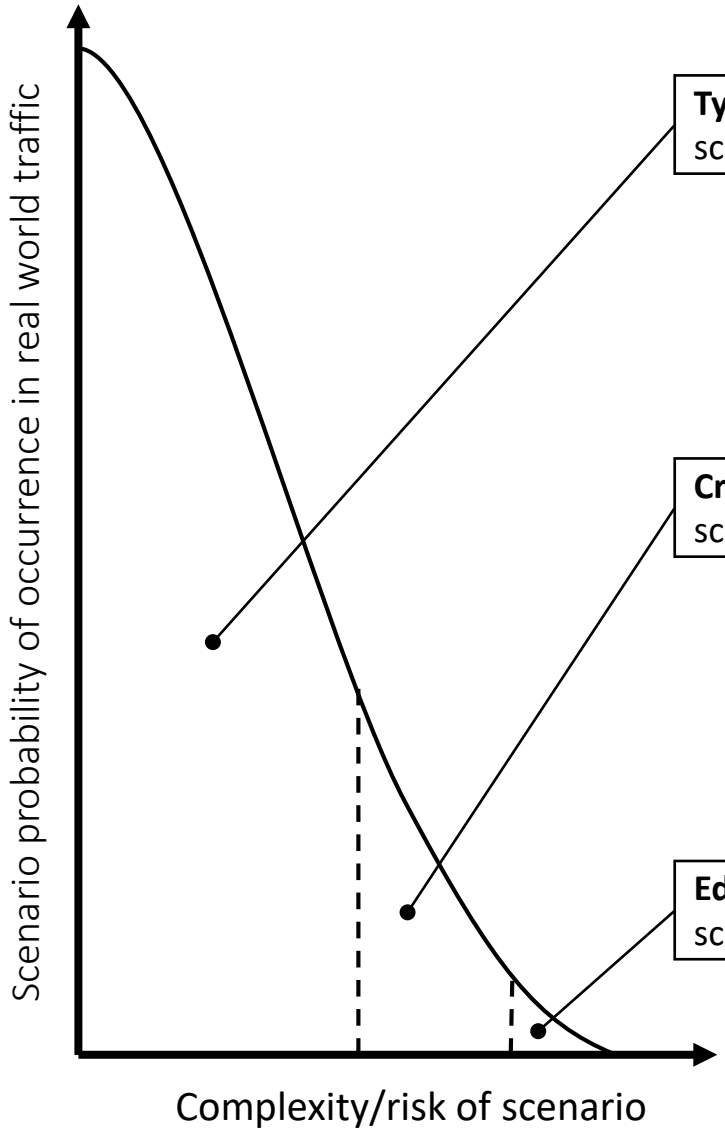
“Multi-Pillar” Certification Approach

Concept for certification

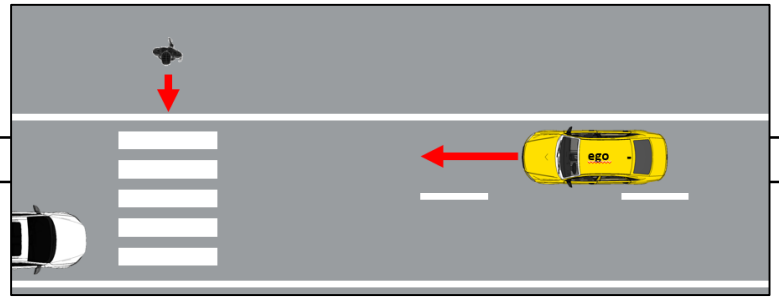


- Certification depends on all pillars – partial assessment doesn‘t have significance
- Scope of work should reduce with every step (audit/assessment: largest scope – real world test drive: final confirmation)
- Safety for test witnesses and other road users – no endangering tests on public roads
- Concept can be augmented by additional “pillars” in terms of requirements/methods/tools as needed (lessons learned)

Example of the different pillars' functions



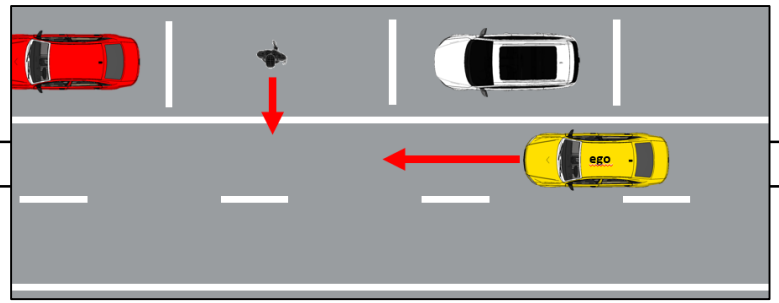
Typical traffic scenarios



Pedestrian crossing a crosswalk

Real World Test Drive

Critical traffic scenarios

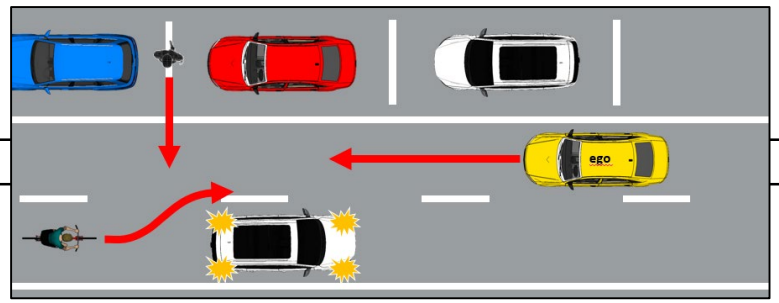


Obstructed pedestrian crossing

Physical Certification Tests

Edge case scenarios

low probability, but high efforts to identify and confirm performance!



Obstructed pedestrian crossing
+ cyclist overtaking

Audit and Assessment (e.g. simulation)

Concept for certification – the pillars and their individual purpose

Audit/Assessment

Simulation

- 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/test 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 processes and functional safety oriented audits for certification of complex electronic vehicle control systems as a foundation.
- Consequently, this 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, this 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).

Back-Up

1 **System Safety**
- Design & Validation Processes (best practices, design principles, standards)
- Testing methods
- Operational Design Domain setting and recognition
- Minimal Risk Manoeuvre
- Take over of DDT (if required, based on level of automation)
- Risk Analysis & Mitigation
  - Failures
  - Inadequate Control

a **Human Machine Interface**
- User (Driver / Passenger) information
  - Take-over request
  - System status
  - Malfunction
  - Communication of critical messages
  - Minimum risk manoeuvre in operation
  - Automated mode active
- Driver availability and override possibility (if required, based on level of automation)
- Signalling driving intentions to other road users

b **System Performance**
- Performance in critical / complex situations (includes response to priority vehicles)
- Response to scenarios and recognition of the OEDR
- Scenario recognition (object and event detection)
- Understanding the system limits and boundaries
- Dynamic behavior in road traffic
- Adherence to rules of the road (Federal and local laws)
- Vehicle behaviour predictability

c **Safety of in-use Vehicles**

 # existing regs have to be complied with
 # for ADS a review needs to be initiated
- Inspections / Repair / Modifications processes
- Software / system update process
- Maintenance of existing level of crashworthiness (for vehicles carrying occupants)
- Vehicle state monitoring
- Post-crash behaviours
  - collision notification to occupants and emergency services,
  - return to a safe-state,

d **Cybersecurity**
- Risk Analysis & Mitigation strategies
  - Cyberattack events
- Incident management
- Documentation strategies/changes/testing

2 **Consumer Awareness/Education**
- Training programmes
- System Operational domain/limits
- Systems prescribed use

3 **Data Recording & Storage System**
- Protocol, recording intervall, data elements
- Recording capacity / standardised access

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

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/s^2 and 2,44 m/s^2 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)

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