Automated and connected driving—Chances/Challenges/Conditions

CITA International Conference & 19th General Assembly
April 2019 · Marko Gustke · Seoul
Outline

1. General overview & roadmap
2. Certification of automated driving systems
3. Security
4. Access to data generated in the vehicle
From assisted via automated through to autonomous driving

**Assisted Driving**
- Driver has to activate the function consciously and may exceed it at any time
- Driver monitors permanently and is a relapse level
- Immediate driver response is required in critical situations

**Automated Driving**
- The driver has to activate the function consciously and may exceed it at any time
- System monitors its function limits and, as soon as reached, hands over to the driver
- Vehicle driver is allowed to perform secondary activities, but is obliged to keep himself / herself ready for take-over whilst using the automated function and to recognize the requirements for the intended use of the automated system.

**Autonomous Driving**
- System controls the driving task in all situations
- Passenger might take over the driving task as far as the vehicle concept designates it

*In series today*

**2019**

**> 2020**

* First pilot and demonstration projects in selected areas of use
** In so far as the framework conditions for admission and use are available
In the future, autonomous vehicles will be able to take over the entire driving task.

Current demonstration- and flagship projects
Regulatory framework for automated vehicles in the worldwide comparison

**USA:**
- Self-certification based on safety guidelines possible (NHTSA)
- Heavily heterogeneous legal framework in the Federal States

**Germany**
- Road Traffic Act (StVG, 2017) defines:
  - Duties of the driver: readiness to take over
  - System requirements: Compliance with Road Traffic Regulations (StVO)
  - If a+b: Aversion from the driving task possible
- Technischen Vorschriften
  - UN-ECE ongoing
  - D-/EU-Exceptional procedure

**EU**
- Technical Regulation:
  - UN-ECE: not finished yet
  - EU-Exeptional procedure
- Code of Conduct: Vienna and Geneva Conventions
  - Automated and diverless driving (operator needed) allowed
  - National implementation necessary: various announcements

**China**
- Driverless driving not yet allowed
- Road tests under high test procedure standards and test drivers (mid-2018)
- Technical requirements are not yet clearly defined ➔ Standardization roadmap as a basis for legislation (90 projects) presented in early 2018

**Japan**
- Driverless driving not yet regulated
- Technical regulations based on UN regulation
- Testing in the public area: domain-specific exceptions / requirements
- Focus on intelligent infrastructure perceptible
Certification of automated driving systems with multi-pillar approach

Consolidated approach to satisfy technical, safety & regulatory requirements

Merge of the „classical“ and new certification approach
Future certification of automated driving systems is needed

Challenges

- Classical vertical regulation approach alone not sufficient
- Regulating new technologies of which the majority is not available on the market yet
- AD Systems will continue to evolve rapidly over the next years
- Number of software-based functions and thereby complexity will continue to increase
- Potentially affected safety-areas and variances of scenarios will increase
- Pragmatic way for industry and authorities for the evolution new technology within agreed safety principles ➔ "controlled" flexibility based on requirements/principles

Multi-pillar approach

- Combination of new elements with classical system regulation approach ➔ Focus: demonstrate the level of safety and reliability, which allows for safe market introduction
- Includes elements of self-certification regime ➔ requires precise descriptions of the procedures and tests to be applied by the manufacturer

Source: OICA
Concept for certification

- 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 behavior, 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)
  - Assessment of development data/field testing, OEM-self-declarations

- 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)

Source: OICA
Example of the different pillars’ functions

- **Typical traffic scenarios**
- **Critical traffic scenarios**
- **Edge case scenarios**

Complexity/risk of scenario vs. Scenario probability of occurrence in real world traffic

- **Pedestrian crossing a crosswalk**
- **Obstructed pedestrian crossing**
- **Obstructed pedestrian crossing + cyclist overtaking**

Source: OICA
Security
Holistic approach for networked and automated vehicles
Six logical interfaces that modern vehicles can use

- Vehicle-to-vehicle
- Vehicle-to-infrastructure
- Vehicle to charging point
- User interface
- OBD interface
- eCall interface
- Traffic and value-added services

"NEVADA - Share & Secure" is the name of the concept referred to in this document. It provides access to the vehicle and to the data generated in the vehicle. "NEVADA" (Neutral Extended Vehicle for Advanced Data Access) describes its technical implementation.
Hollistic security concept will be implemented

1. Define protection needs
2. Recognize Threats
3. Analyze and prioritize risks
4. Define & implement measures
5. Test protective effect

Vehicle to OEM-Server

Architecture & Development Phase
Production Phase
Operational Phase
Hollistic security concept will be implemented
Access to data generated in the vehicle
NEVADA-Share & Secure
Six logical interfaces that modern vehicles can use

- **Vehicle-to-vehicle**
- **Vehicle-to-infrastructure**
- **OBD interface**
- **eCall interface**
- **User interface**
- **Traffic and value-added services**

*NEVADA (Neutral Extended Vehicle for Advanced Data Access) describes its technical implementation.*

*“NEVADA – Share & Secure” is the name of the concept referred to in this document.*
Six logical interfaces that modern vehicles can use

Traffic and value-added services

*"NEVADA - Share & Secure" is the name of the concept referred to in this document. It provides access to the vehicle and to the data generated in the vehicle.

"NEVADA" (Neutral Extended Vehicle for Advanced Data Access) describes its technical implementation.
Access to vehicle-generated data

Vehicle safety
Vehicle- and IT security
Data security (Privacy)

Fair competition for digital innovations and business models
Interface between vehicle and OEM server for remote access to data

**Current state**

- Proprietary interface for encrypted data transfer between vehicle and vehicle manufacturer.
- Access to the vehicle via this interface exclusively via manufacturer.
- Vehicle security guaranteed.

Proprietary interface for encrypted data transfer between vehicle and vehicle manufacturer.

Access to the vehicle via this interface exclusively via manufacturer.

Vehicle security guaranteed.
The dongle for insecure data transfer

**Current state**

Security cannot be guaranteed

Service providers currently use dongle in conjunction with the OBD interface to retrieve data from the vehicle ➔ However, security of the connection is not guaranteed and ➔ only one dongle of a single service provider can be used.

Source: VDA

19
Standardized interface for remote access to vehicle data

Planned solution

ISO Standardised Interface

- OEM-Server
- Neutral server(s)
- Service provider

Road traffic safety
New business models
Innovations

Standardized, reliable, manufacturer-independent and sustainable interface between vehicle manufacturer's servers and business partners

Source: VDA
Access to maintenance and repair information via:

- OBD diagnostic interface (secured expert environment, eg workshop) or
- Remote access via neutral server
BMW & Daimler have already implemented NEVADA

Other vehicle manufacturers have announced the introduction for 2019!
Conclusion

- **Megatrend**: Automated and driverless driving
- **Technology paths**: Highway-applications and urban-shuttles
- **Framework**: Consistent requirements for technology & people needed
- **Type approval**: New approach/elements have to be implemented
- **Introduction**: National and international aspirations recognizable
- **Conditions**: Worldwide synchronization
- **NEVADA**: Competition and security/safety requirements in line
Thank you for your attention!
CITA International Conference & 19th General Assembly
April 2019 · Marko Gustke · Seoul