VALIDATION OF ASSISTED AND AUTOMATED DRIVING SYSTEMS

Udo Steininger · TÜV SÜD, Hans-Peter Schöner · Daimler, Mark Schiementz · BMW, Jens Mazzega · DLR

crash.tech, April 19 - 20 2016, Munich
In 1901 Daimler launched the first modern car with the *Mercedes 35 HP*.

At the same time Gottlieb Daimler said: „The worldwide demand for automobiles will not exceed one million if only due to the lack of chauffeurs.“

It is time now, to solve this obviously very old problem by rollout of systems for highly automated driving. But do we already know, how to validate those systems?
## Agenda

<table>
<thead>
<tr>
<th></th>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Initial situation</td>
</tr>
<tr>
<td>3</td>
<td>General approach</td>
</tr>
<tr>
<td>4</td>
<td>Final remarks</td>
</tr>
</tbody>
</table>
# VDA roadmap for introduction of assistance and automation

<table>
<thead>
<tr>
<th>Driver is always in the loop and monitors environment.</th>
<th>System monitors environment, driver is (temporarily) out of the loop.</th>
<th>Robot taxi</th>
</tr>
</thead>
<tbody>
<tr>
<td>n.a.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation 2(^{nd}) gen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation 1(^{st}) gen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New DAS</td>
<td>Eco ACC, Work site assistant, Congestion assistant, Park assist.</td>
<td></td>
</tr>
<tr>
<td>Established DAS</td>
<td>ACC, S&amp;G, PSA, LKA</td>
<td></td>
</tr>
<tr>
<td>Driver only (0)</td>
<td>Assisted (1)</td>
<td>Partially automated (2)</td>
</tr>
<tr>
<td>LCA, PDC, LDW, FCW</td>
<td></td>
<td>Highly automated (3)</td>
</tr>
<tr>
<td>LCA: Lane Change Assistant</td>
<td>LDW: Lane Departure Warning</td>
<td>Fully automated (4)</td>
</tr>
<tr>
<td>PDC: Park Distance Control</td>
<td>FCW: Forward Collision Warning</td>
<td>Driverless (5)</td>
</tr>
<tr>
<td>Assisted (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partially automated (2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Highly automated (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fully automated (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driverless (5)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LCA: Lane Change Assistant</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDW: Lane Departure Warning</td>
</tr>
<tr>
<td>FCW: Forward Collision Warning</td>
</tr>
<tr>
<td>ACC: Adaptive Cruise Control</td>
</tr>
<tr>
<td>S&amp;G: ACC incl. Stop &amp; Go</td>
</tr>
<tr>
<td>PSA: Park Steering Assistant</td>
</tr>
<tr>
<td>LKA: Lane Keeping Assistant</td>
</tr>
</tbody>
</table>
Time table

Fully automated

Highly automated (... within next decade)

Partially automated

>2025

VOLLAUTOMATISIERT
- Überwachung nicht erforderlich
- Fahrer muss die Fahraufgabe nicht übernehmen können
- Beispiel: Autobahnfahrt bis 130 km/h

2020

HOCHAUTOMATISIERT
- Überwachung nicht erforderlich
- Fahrer muss mit Vorteil die Fahraufgabe übernehmen können
- Beispiel: Stop & Go (Autobahn)

2016

TEILAUTOMATISIERT
- Systemüberwachung erforderlich
- Fahrer muss jederzeit die Fahraufgabe übernehmen können
- Beispiel: Stop & Go bis 30 km/h

© Continental
Core issues

- What criteria have systems for highly automated driving to fulfil?
- What is necessary in order to assure, that systems fulfil those criteria, actually?
What is PEGASUS?

- **Project for establishing generally accepted quality criteria, tools and methods as well as scenarios and (in German: und) situations for the release of highly automated driving functions**
- Founded by Federal Ministry for Economic Affairs and Energy (BMWi)
- PEGASUS will close gaps in the area of testing and approval of automated vehicles with the aim to transfer existing highly automated vehicle prototypes into products
- PEGASUS provides corresponding results and standards for product development and release
### General conditions

**Duration**  
January 2016 – June 2019

**Partners**  
*OEM:* Audi, BMW, Daimler, Opel, Volkswagen  
*Tier 1:* Automotive Distance Control, Bosch, Continental  
*Test Lab:* TÜV SÜD  
*SMB:* fka, iMAR, IPG, QTronic, TraceTronic, VIRES  
*Scientific institutes:* DLR, TU Darmstadt

**Subcontractors**  
IFR, ika, OFFIS, BFFT, Carmeq, EFS, Fortiss, MBTech, Nordsys, Philosys, VSI, WIVW

**Volume**  
total 34.5 Mio. EUR, supported volume 16.3 Mio. EUR

**Manpower**  
150 man years
Agenda

1. Introduction
2. Initial situation
3. General approach
4. Final remarks
Passive vs. active safety

- Assessment and validation of *passive safety* based on a practicable number of crash tests under well defined worst case conditions is well established and widely accepted.

- In contrast testing of *active safety* systems is limited by:
  - huge number of relevant scenarios and environmental conditions
  - complexity of systems and variability of driver behaviour
  - methodological aspects (functional deficiencies)
Customer’s protection

- EuroNCAP, e.g., has a road map for assessment of active safety systems

- Tests are useful for comparison of systems from customer protection’s point of view (no driver intervention considered)

- They are only limited applicable for system development and validation because they do not represent real scenarios, environments and driver behaviour
Endurance tests

- Systems for highly automated driving have to fulfil very high functional safety requirements, e.g. random hardware failure rates < $10^{-8}$/h for ASIL D

- Besides before mentioned methodological limitations it is not possible
  - to prove those failure rates by conventional road tests with reasonable effort and
  - to prove completeness of tests considering very rare events in general

<table>
<thead>
<tr>
<th>ISO 26262 ASIL Determination</th>
<th>Exposure</th>
<th>Controllability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>C1</td>
</tr>
<tr>
<td>S1</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>QM</td>
</tr>
<tr>
<td>S2</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>A</td>
</tr>
<tr>
<td>S3</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>B</td>
</tr>
</tbody>
</table>
- Product safety confirmation based on ISO 26262 for functional safety of E/E systems in road vehicles

- Applicable for DAS in general and sufficient for established systems

- Limitations: ISO 26262 doesn’t cover functional disabilities, e.g. misinterpretation of objects / traffic situations and resulting false positive system interventions

With increasing level of automation, upgrade of functional safety standard seems to be necessary → ISO 26262 is under revision
Regulation

• European type approval for passenger cars, e.g., based on 2007/46/EC and ECE-Regulations 13 & 79 with so called electronic annexes

• Requirement: No influence of E/E systems on mechanical braking and steering functions

• Not focused on DAS, but sufficient as long as systems are fully controlled by driver in every situation according to 1968 Vienna Convention on Road Traffic (VC 68)

With increasing level of automation, we will reach a point, where those regulations are not longer sufficient → ECE-R13 & 79 are under revision
Agenda

1 Introduction
2 Initial situation
3 General approach
4 Final remarks
Key issues

• Safety requirements and socially accepted risk criteria (compared to human driver)

• Implementation in the development process

• System assessment
  – Verification
  – Validation

• Proof of concept and extension on other system specifications
... related to development process

Proof of concept and extension on other system specifications

System specification

System assessment

Validation

Verification

Integration test

HW test

SW test

System development process
Safety requirements

• Identification of relevant / critical scenarios
• Hazard analysis an risk assessment according to ISO 26262
• Resulting safety concept includes requirements to
  — components (e.g. failure rates)
  — systems (e.g. homogenous or diverse system redundancy)
  — item / unit (e.g. fail operational design)
Socially accepted risk criteria

**General approach: Risk = Frequency x Damage**

![Graph showing the relationship between log(Frequency) and log(Damage).]

**Accident statistics on German „Autobahn“**

With assumption, that there is 1 order of magnitude between severity levels according to ISO 26262:

![Graph showing accident rate per 1 bn. km against severity.]

Sources: H.-P. Schöner, CESA 2014, and DESTATIS (German Federal Statistics Agency) 2013
Approach for system assessment

• Testing against scenarios and events (also rare) instead of driving distance or time

• Considering virtual test (simulation) and real tests (proving ground and field tests)

• Necessary to cover complete test space (i.e. all relevant scenarios, environments and driver behavior)

... because all types of tests have advantages and disadvantages
Characteristics of test levels

- **Virtual tests**
  - Analysis of a huge number of scenarios, environments, system configurations and driver characteristics

- **Proving ground tests**
  - Reproducibility by use of driving robots, self driving cars and targets; critical manoeuvres are possible

- **Field tests**
  - Investigation of real driving situations and comparison with system specifications

Effort for coverage of all relevant scenarios & environments

Uncertainties & simplifications
Consolidation of results

Assessment Results

Virtual Assessment

SW in the Loop
HW in the Loop
Driving Simulator

Vehicle Testing
(NDS, fleet, proving ground, ...)

Model Database

Scenarios
(exposition, environment, ...)

Road Users
(driver, pedestrian, ...)

Vehicle
(driving dynamics, ...)

Sensors
(radar, lidar, camera, ...)

Legend:

- results
- relevant situations for further investigation
- validation, verification
- models

10^8 scenarios
10^3 scenarios
10^2 scenarios

Situation space mainly covered by virtual assessment
Agenda

1. Introduction
2. Initial situation
3. General approach
4. Final remarks
Results

• General concept & tools for assessment of a highway chauffeur

• Applicable for all interested parties (manufacturers, system developers, scientific institutes, test labs, notified bodies, authorities ...)

• Methodological expansion to other systems (e.g. inter urban or city chauffeurs)
Accompanying measures

- Achieving a common understanding of national and international players (manufacturers, system developers, scientific institutes, test labs, notified bodies, authorities ...) → e.g. by publications and lobbying

- Participation in national and international legislation and standardisation → e.g. WP.29 by UNECE or FKT Sonderaus- schuss FAS by BMVI
Final note

“People on horses look better than they are. People in cars look worse than they are.”
(Marya Manns)

Still right, because horses can already ride autonomously but cars can’t yet. It’s time to give cars wings with the help of automated driving systems - and to assess those systems with the help of PEGASUS!