Requirements on tools for assessment and validation of assisted and automated driving systems

7. Tagung Fahrerassistenz

Udo Steininger, TÜV SÜD Auto Service
Dr. Hans-Peter Schöner, Daimler
Dr. Mark Schiementz, BMW

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction &amp; definitions</td>
</tr>
<tr>
<td>2</td>
<td>Problem</td>
</tr>
<tr>
<td>3</td>
<td>General approach</td>
</tr>
<tr>
<td>4</td>
<td>Tool chain</td>
</tr>
<tr>
<td>5</td>
<td>Application</td>
</tr>
</tbody>
</table>
### Levels of driving automation according to SAE / BASSt / NHTSA

(SAE report J3016)

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Narrative definition</th>
<th>Execution of steering and acceleration/deceleration</th>
<th>Monitoring of driving environment</th>
<th>Fallback performance of dynamic driving task</th>
<th>System capability (driving modes)</th>
<th>BASSt level</th>
<th>NHTSA level</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Automation</td>
<td>the full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Human driver</td>
<td>n/a</td>
<td>Driver only</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task</td>
<td>Human driver and system</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>Assisted</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Partial Automation</td>
<td>the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task</td>
<td>System</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>Partially automated</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Automation</td>
<td>the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene</td>
<td>System</td>
<td>System</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>Fully automated</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>High Automation</td>
<td>the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Some driving modes</td>
<td>Fully automated</td>
<td>3/4</td>
</tr>
<tr>
<td>5</td>
<td>Full Automation</td>
<td>the full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>All driving modes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### VDA roadmap for introduction of assistance and automation

<table>
<thead>
<tr>
<th></th>
<th>Driver is always in the loop and monitors environment.</th>
<th>System monitors environment, driver is (temporarily) out of the loop.</th>
</tr>
</thead>
<tbody>
<tr>
<td>n.a.</td>
<td></td>
<td>Robot taxi</td>
</tr>
<tr>
<td>Automation 2nd gen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automation 1st gen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New DAS</td>
<td>Eco ACC, Work site assistant</td>
<td>Congestion assistant, Park assist.</td>
</tr>
<tr>
<td>Established DAS</td>
<td>LCA, PDC, LDW, FCW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Driver only (0)</td>
<td>Assisted (1)</td>
</tr>
<tr>
<td></td>
<td>Partially automated (2)</td>
<td>Highly automated (3)</td>
</tr>
<tr>
<td></td>
<td>Fully automated (4)</td>
<td>Driverless (5)</td>
</tr>
</tbody>
</table>

- **Driver is always in the loop and monitors environment.**
  - Driver only (0)
  - Assisted (1)
  - Partially automated (2)
  - Highly automated (3)
  - Fully automated (4)

- **System monitors environment, driver is (temporarily) out of the loop.**

  - Highway pilot
  - Parking garage pilot

LCA: Lane Change Assistant  
LDW: Lane Departure Warning  
ACC: Adaptive Cruise Control  
S&G: ACC incl. Stop & Go  
PSA: Park Steering Assistant  
PDC: Park Distance Control  
FCW: Forward Collision Warning  
S&G: ACC incl. Stop & Go  
LKA: Lane Keeping Assistant
Time table

TÜV SÜD Auto Service GmbH

7. Tagung Fahrerassistenz - Steininger, Schöner, Schiementz

© Continental
## Agenda

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction &amp; definitions</td>
</tr>
<tr>
<td>2</td>
<td>Problem</td>
</tr>
<tr>
<td>3</td>
<td>General approach</td>
</tr>
<tr>
<td>4</td>
<td>Tool chain</td>
</tr>
<tr>
<td>5</td>
<td>Application</td>
</tr>
</tbody>
</table>

© Continental
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
Functional safety

• 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>C1</td>
<td>C2</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></td>
<td></td>
<td></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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>E1</td>
<td>QM</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• 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
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, for example 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 → also ISO 26262 is under revision
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction &amp; definitions</td>
</tr>
<tr>
<td>2</td>
<td>Problem</td>
</tr>
<tr>
<td>3</td>
<td>General approach</td>
</tr>
<tr>
<td>4</td>
<td>Tool chain</td>
</tr>
<tr>
<td>5</td>
<td>Application</td>
</tr>
</tbody>
</table>
Basis: General accepted safety requirements and risk criteria

General approach: Risk = Frequency x Damage

Accident statistics on German „Autobahn“

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

Sources: H.-P. Schöner, CESA 2014, and DESTATIS (German Federal Statistics Agency) 2013
• Systems have to be able to control scenarios → therefore an integral, scenario based approach is necessary

• taking into account different test levels like
  – virtual testing
  – proving ground tests
  – field tests
  in an adequate way

• sufficient for partial + high automation

• applicable
  – in the system development process as well as
  – for assessment and validation in frame of type approval and confirmation of product safety
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
Test process according to V model of HW & SW development

Step 1: Identification of scenarios and environments

Step 2: Specification and implementation of virtual tests

Step 3: Specification and implementation of proving ground tests

Step 4: Specification and implementation of field tests

Verification: Have I done things right?

…means to check whether proving ground tests confirm virtual tests

Validation: Have I done the right things?

…means to check whether field tests confirm scenarios and environments
Validation plan

... should include amongst others:

• Requirements
  – derived from scenarios and requirements (step 1)
  – taking into account results from virtual tests (step 2) and proving ground tests (step 3)
  – include confirmation, how system fulfills these requirements

• Acceptance criteria to confirm that system meets defined requirements (confirmation of scenarios and environments ↔ driven km, time)
Comparison with other approaches

**Scenario based approach**

- Integral approach with focus on use cases / entire system (instead of km or time $\leftrightarrow$ rare events)

- Applicable in system development as well as in type approval and confirmation of product safety

- High effort for adaptation to different systems specifications / degrees of automation and resulting use cases / scenarios

**System based approaches**

- Decomposition: Confirmation of reliability / safety by system architecture (redundancy, diversity) $\rightarrow$ high potential because several sensors and sensor types are used in every application

- Probabilistic approaches: e.g. Fault Tree Analysis $\rightarrow$ very useful for system understanding / limitations

- Stochastic approaches: Road tests versus proven in use $\rightarrow$ some potential because of incremental increase of automation

**Conclusion:** Combination of different approaches can be helpful / necessary!
Agenda

1. Introduction & definitions
2. Problem
3. General approach
4. Tool chain
5. Application
Goals
• find all relevant (even rare) possibly critical incidents
• consider the identification of system limitations
• specify test cases

Tools
• Systematic procedure is necessary, e.g.
  – Hazard Analysis and Risk Assessment
  – Event Tree Analysis
  – Fault Tree Analysis

Challenges
• Generally accepted safety requirements and scenarios
• Reduction of test cases to a significant and sufficiently complete set
Virtual Tests

**Goals**
- Cover a large number of different test cases
- Combine base events to establish rare situations

**Tools**
- Test benches for MIL / SIL / VIL / HIL
- Simulation models for all relevant components

**Challenges**
- Importance of sensor and driver models (= interfaces to real world complexity)
- Perform a sufficiently dense coverage of the test state space
Proving ground tests

Goals
• Verify reference scenarios of the virtual tests
• Test of situations, which are unlikely to meet in field tests and which are hard to simulate
• Test of safety critical manoeuvres along the system limitation

Tools
• Reproducibility and accuracy by use of driving robots, self driving cars and targets for high statistical confidence level

Challenges
• Tool set to perform even critical tests
Field tests

Goals

• Validation of statistical probability of relevant situations or events
• Verification of automatic recognition of system limitations in field operation
• Safe handling of functional deficiencies of system components in random situations
• Interaction of drivers with the system

Tools

• Test vehicles with reference measurement equipment

Challenges

• Duration of field tests or indicators for sufficient test coverage
• …
Consolidation of results

Assessment Results

Virtual Assessment

Software in the Loop

Hardware 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

10^6 scenarios
10^3 scenarios
10^2 scenarios

Situation space mainly covered by virtual assessment
Agenda

1. Introduction & definitions
2. Problem
3. General approach
4. Tool chain
5. Application

© Continental
Verification and validation at the end of the process requires careful specification in the early system design phase.

**Investigation of properties of the system environment:**
Basis for system design
- Typical behaviour and parameters of:
  - Infrastructure, traffic, environment
  - Sensors, actuators
  - Drivers

**System design:**
Specification of system performance
- Risk assessment & management
- Functional limitations
- Functional requirements including fault management
- Define performance criteria and tests

**Illustration for example:**
- System

**Validation:**
Assessment of implementation with respect to desired functionality
- Confirmation of design assumptions
- Confirmation of risk assessment
- Examination of retroactive effects
- Safety in use, customers' benefits and acceptance

**Verification:**
Comparison of implementation with respect to design specification
- Perform system tests
- Evaluate test coverage

**Implementation**
System design – special aspects

Functional decomposition of complex systems

Design for high reliability:

- Redundant, self monitoring components
  ➢ fault tolerant system design
- Diverse components
  ➢ avoid common mode (correlated) faults
- Fault tree analysis
  ➢ avoid systematic errors
- Derive system failure rate by mathematical model

\[ \lambda_{\text{total}} = \lambda_1 + (\lambda_2)^3 + \lambda_3 + \lambda_4 \]
(only if all subsystems are uncorrelated !)
Type approval and product safety confirmation

• Range (i.e. number of relevant scenarios and environments) and level of detail (number of influence parameters, complexity of tests) of approvals and confirmations
  – depend on certain system specification and
  – increase with level of automation

• Next generation of partially automated systems (e.g. congestion and park assistants) are entering the market and will provide further field experience under drivers’ supervision

• BMVI has installed “FKT-Soneraausschuss Fahrerassistenzsysteme” to identify necessary changes within ECE-R13 and 79

• Because highly automated systems will be introduced within next decade, there is still some time for type approval and product safety confirmation, but
  – manufacturers and system developers need to know requirements in early development states and
  – public discourse about benefits and risks of highly automated driving is necessary
Next steps

• Achieve common understanding of authorities, test labs, notified bodies, manufacturers, system developers, scientific institutes ...

• Detailed development and test of general approach and all parts of tool chain

• Preparation of national / international legislation and standardisation

• For this purpose some national and international projects have been started or are in preparation, respectively
The authors thank Horst Mock and Axel Blumenstock, Daimler, and Thomas Ziegler, TÜV SÜD, for contributions to this lecture and helpful suggestions.

Picture credits (if not otherwise denoted): BMW, Daimler, TÜV SÜD