Highly automated driving in the predicament between technical possibilities, public expectations and safety & security requirements


Abstract

The lecture starts with the initial situation in assisted and automated driving including a short definition of several levels of automation, a description of technical features within this levels and time of introduction on the market.

Afterwards public expectations shall be discussed taking into account several stakeholders. Politics and society expect an increase of road traffic safety on the one hand. On the other hand, customers implicate benefit, e.g. increase of comfort, as well as harm, e.g. loss of control or vulnerability by cyber-attacks. In this context it is necessary to touch upon some legal issues, too.

Safety and security requirements for highly automated driving including system verification and validation are currently being developed. In a first step, they can be derived from existing regulations and standards, e.g. UNECE regulation or ISO 26262, and from approval procedures for existing vehicle systems, e.g. passive safety systems. But there are some important limitations in this way. On the one hand we have to deal with technical limitations of sensors and algorithms regarding environment recognition and situation awareness in system safety design (keyword: functional deficiencies). On the other hand, we have to approve a huge number of environmental conditions, traffic situations and driver behaviour. It is not possible to cover this variability only by real testing as it is recently done. So virtual testing will play an important role in frame of the approval of systems for highly automated driving.

The lecture gives an overview about recent activities in this field and closes with an outlook to further development of safety and security requirements as well as verification and validation procedures for highly and fully automated driving.
A VERY OLD PROBLEM – LACK OF CHAUFFEURS

In 1901 Daimler launched the first modern car - 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.“

Today we have the chance to solve the “problem” of the unavailability of human chauffeurs with the help of highly automated driving systems. But the challenge is, to make highly automated driving highly performant, safe and secure.

CONTENT

- Initial situation
- Public expectations
- Safety requirements
  - Current regulation & standardisation and challenges by introduction of level 3
  - Future requirements on system architecture for level 4 & 5
- Security requirements
- Resume
### SAE LEVEL OF AUTOMATION

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Narrative definition</th>
<th>Executive/steering and accelerator/brake classification</th>
<th>Monitoring of driving environment</th>
<th>Fulltime performance of dynamic driving task</th>
<th>System capability/drivers</th>
<th>Driving modes</th>
</tr>
</thead>
<tbody>
<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 performs all remaining aspects of the dynamic driving task.</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>System</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 performs 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>System</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 requests for intervention.</td>
<td>System</td>
<td>System</td>
<td>Human driver</td>
<td>Some driving modes</td>
<td>System</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 the human driver does not respond appropriately to a request for intervention.</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Some driving modes</td>
<td>System</td>
</tr>
<tr>
<td>5</td>
<td>Full Automation</td>
<td>the full-time performance by an automated driving system at all speeds 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>System</td>
</tr>
</tbody>
</table>

### VDA ROADMAP FOR INTRODUCTION OF AUTOMATED DRIVING (2015)

<table>
<thead>
<tr>
<th>Automation</th>
<th>2nd gen.</th>
<th>1st gen.</th>
<th>New DAS</th>
<th>Established DAS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Eco ACC, Work site assistant</td>
<td>LCA, PDC, LDW, FCW</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Congestion assistant, Park assist.</td>
<td>ACC, S&amp;G, PSA, LKA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Driver only</th>
<th>Assisted</th>
<th>Partially automated</th>
<th>Highly automated</th>
<th>Fully automated</th>
<th>Driverless</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0)</td>
<td>(1)</td>
<td>(2)</td>
<td>(3)</td>
<td>(4)</td>
<td>(5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LCA: Lane Change Assistant</th>
<th>LDA: Lane Departure Warning</th>
<th>ACC: Adaptive Cruise Control</th>
<th>PSA: Park Parking Assistant</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDW: Lane Departure Warning</td>
<td>ACC: Adaptive Cruise Control</td>
<td>PSA: Park Steering Assistant</td>
<td></td>
</tr>
<tr>
<td>LKA: Lane Keeping Assistant</td>
<td>LKA: Lane Keeping Assistant</td>
<td>LKA: Lane Keeping Assistant</td>
<td>LKA: Lane Keeping Assistant</td>
</tr>
</tbody>
</table>

https://doi.org/10.51202/9783181022962-283
Generiert durch IP '54.70.40.11', am 05.06.2021, 09:25:43.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.
VDA ROADMAP FOR INTRODUCTION OF AUTOMATED DRIVING (2015)

Market introduction of

- Level 2 systems, partially automated: 2016
- Level 3 systems, highly automated: 2020
- Level 4 systems, fully automated: > 2025

CONTENT

- Initial situation
  - Public expectations
    - Safety requirements
      - Current regulation & standardisation and challenges by introduction of level 3
      - Future requirements on system architecture for level 4 & 5
    - Security requirements
    - Resume
STAKEHOLDER AND AREAS OF CONFLICTS

Politicians
- Pros:
  - Increase of road traffic safety
  - Increase of comfort and efficiency
  - Mobility for elder people

CONS:
- Traffic planners
  - Loss of control or driving pleasure
  - Responsibility in case of accidents
  - Cyber security and loss of privacy

Drivers & passengers
- Mobility service providers
  - Fleet operators

Car owners
- ICT service providers

Assurance companies

RISKS AND CHANCES

Unrealistic expectations, wrong promises e.g.
- „Vision Zero” by EC
- Tesla’s so called „Autopilot” which is in best case a level 2 DAS
- Time to market of fully automated and especially driverless vehicles

Uncertainty for automotive industry and mobility service provider because of regulations and standards have to be developed parallel to development of technical systems

Although it is a disruptive technology we will get an incremental market introduction (i.e. stakeholders have the chance to learn step by step how to deal with the technology)

Regulation and standardisation bodies take in to account technical feasibility and customer expectations in development of regulations and standards
SOME HIDDEN / UNDERESTIMATED ASPECTS

- Mixed traffic, i.e. different levels of automation (driver only to fully automated / driverless) have to be managed simultaneously for decades

- Influences on urban development, e.g. sclerosis of inner cities due to increasing commuting distances, elder people get able to live on countryside etc.

- Social and commercial aspects, e.g. huge number of people get online some additional hours per day during highly or fully automated driving

CONTENT

- Initial situation

- Public expectations

  - Safety requirements
    - Current regulation & standardisation and challenges by introduction of level 3
    - Future requirements on system architecture for level 4 & 5

- Security requirements

- Resume
REGULATION

- **European type approval** for passenger cars based on 2007/46/EC and ECE-Regulations 13 & 79 (brake & steering) with 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-R79 & 13 are under revision

STANDARDISATION

- **Product safety confirmation** for E/E systems of road vehicles based on ISO 26262 for Functional Safety

- Applicable for DAS in general and sufficient for established systems

- Limitation: ISO 26262 only deals with hazards resulting from malfunctions of technical systems, it doesn’t cover functional limitations (e.g. deficiencies in sensor setup and algorithms resulting in false positive system interventions)

- With ISO/AWI PAS 21448 a standard for “Safety of the Intended Functionality (SOTIF)” is under development
INTERNATIONAL CONTRACTS & NATIONAL LEGISLATION

- **VC 68** as well as German **StVG** has been adapted for further development of automated driving recently

- Changes do not allow full automation but
  - enable next steps, i.e. market introduction of level 3 systems / highly automated driving and
  - show political will to support automated driving at national and international level

CHALLENGES FOR LEVEL 3

- On the one hand systems have to fulfill very high functional safety requirements, e.g. for ASIL D random hardware failure rates $< 10^{-8}$ / h → It is not possible to prove those failure rates by conventional field tests with reasonable effort

- On the other hand we have to deal with a huge number of traffic situations, environmental conditions and driver behavior → It is not possible to cover this test space only by **real tests** at all

- Method of resolution: for verification & validation of level 3 systems **virtual testing** has to play an important role
CHARACTERISTICS OF SEVERAL TEST LEVELS

Virtual tests
- Analysis of 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

Uncertainties & simplifications

Effort for coverage of all relevant scenarios & environments

SCENARIO BASED APPROACH

- Identification of relevant scenarios and derivation of safety requirements

- Cover test space by virtual tests

- Verification of virtual test results by proving ground tests

- Validation of requirements by field tests
CONTENT

- Initial situation
- Public expectations
- Safety requirements
  - Current regulation & standardisation and challenges by introduction of level 3
  - Future requirements on system architecture for level 4 & 5
- Security requirements
- Resume

WHAT HAPPENS IN CASE OF FAILURES IN E/E SYSTEMS?

<table>
<thead>
<tr>
<th>Level</th>
<th>Driver activities</th>
<th>E/E system design</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 2</td>
<td>intervention through mechanical connection between control element (steering column, brake pedal) and actuation</td>
<td>Fail safe</td>
</tr>
<tr>
<td>3</td>
<td>“respond appropriately to a request to intervene” (\rightarrow) affects system performance (request at right time) as well as allowed driver activities (appropriate reaction)</td>
<td>Fail safe + Minimum risk manoeuvre (MRM)</td>
</tr>
<tr>
<td>4 - 5</td>
<td>driver is not longer available for activities / there is no driver, i.e. mechanical connection between control element and actuation is not longer sufficient / will not exist</td>
<td>Fail operational</td>
</tr>
</tbody>
</table>
FAIL SAFE SYSTEM DESIGN

- Systems detect failures and shut down in case of failure (they deliver either intended function or no function at all)
- Typical architecture: intended function is controlled by several monitors (e.g. for power and time) and by a separate monitoring channel
- Typical application: Electrical Power Steering
  - Failure that leads to wrong steering torque at high speed is dangerous
  - Shut down in case of a failure provides a safe state because of mechanical fall back
  - If failure indication is no longer valid, function is available again after reset
- General prerequisite for fail safe design: Shut down is a safe state!

FAIL OPERATIONAL SYSTEM DESIGN

- Necessary, if shut down leads to an unsafe state
- Function has to be continued after a failure has detected
- Typical architecture: 2oo3 system, 3 redundant sub-systems with plausibility check of input and output data
- After detection of a single failure in a subsystem, function is fully available
- Typical application in aircrafts or Nuclear Power Plants
- Problem: very intensive regarding costs and installation space, high complexity
CONSEQUENCES FOR LEVEL 4 & 5 VEHICLES

- Vehicles will have redundant and / or diverse by-wire systems not only for automation but also for steering and braking with
  - consequent separation of subsystems from sensor to actuator level including power supply and
  - diversity in sensors and performance / safety processing to avoid common cause failures
- At the latest at level 5, also power train has to be redundant to reach safe state (i.e. a place where passengers can safely leave the vehicle) in case of failure
- After occurrence of a single failure, systems has to operate in a degraded mode (e.g. reduced velocity) \( \rightarrow \) consideration of independent 2\textsuperscript{nd} or subsequent failure in safety concept?!
CONTENT

- Initial situation
- Public expectations
- Safety requirements
  - Current regulation & standardisation and challenges by introduction of level 3
  - Future requirements on system architecture for level 4 & 5
- Security requirements
- Resume

AUTOMATED DRIVING AND SECURITY

- Historically, vehicles have been closed systems - first applications that connect vehicles with outside world where infotainment and navigation systems
- Automated driving is not the root cause and not the single mover for connectivity but it produces increasing number and amounts of data collected, processed and stored
- One reason is the limited range of on-board sensors, which yield to limitations in forecast of systems for automated driving
- For level 3+, vehicle to vehicle and vehicle to infrastructure communication (V2X) may be mandatory, therefore
V2X COMMUNICATION TECHNOLOGIES

CYBER SECURITY THREADS
SAFETY & SECURITY PROCESS FRAMEWORK

- Common understanding: Safety and security by design
- Common methods: for example HARA → TARA

CHALLENGES FROM CYBER SECURITY AND PRIVACY

Cyber security
- Same situation like in safety - driver is not longer available for prompt intervention
- Common understanding / guideline for security tests and verification & validation process still outstanding

Privacy
- For higher levels of automated driving, driver supervision and Event Data Recorder (EDR) will be mandatory but how to store and manage those data (black box, transfer to data trustees ...)?
CONTENT

- Initial situation
- Public expectations
- Safety requirements
  - Current regulation & standardisation and challenges by introduction of level 3
  - Future requirements on system architecture for level 4 & 5
- Security requirements
- Resume

RECENT SITUATION AND CHALLENGES

- Technology for level 3 is more or less ready to market and development of approaches and tools for assessment of systems is close to completion
- For higher levels of automation, completely new system architecture requirements will arise, not only automated driving systems will be affected but also braking, steering and power train
- Cyber security and privacy within the scope of automated driving are still in an early development stage
BACK TO OPENING QUESTION

Is the “problem” of missing human chauffeurs solved by automated driving?
- Technology at least for next level is generally available
- Political commitment exists widely
- Regulations and standards are under development

General questions
- What does the customer really wants / what is he willing to pay for?
- What happens, when accidents with automated vehicles occur?
- Who will rule the development – Old or New Economy?

HOW CAN WE HELP YOU?

Dipl.-Phys. Udo Steininger
Team Leader Automotive

Phone  +49 89 5791-3163
Mobile  +49 160 3601992
udo_steininger@tuev-sued.de

TÜV SÜD Rail GmbH
Barthstraße 16
80339 Munich