Prof. Dr. rer. nat. Hermann Winner
Dipl.-Ing. Walther Wachenfeld
Philipp Junietz, M.Sc.

Safety Assurance for Highly Automated Driving – The PEGASUS Approach
Considered Levels of Automated Driving

Highly Automated Driving:
- according to definition of BASt level 3 and
- VDA level 3: Conditional Automation
- NHTSA level 3: Limited Self-Driving Automation
- SAE level 3: Conditional Automation

Interpretation:
- No responsibility of human drivers (operators) during operation of automation, but the automation may shift back the driving task towards human in a reasonable transition time.

Sources: bast [1], VDA [2], SAE [3], NHTSA [4]
Meaning of Highly Automated Driving

Highly Automated Driving

- Expected as introduction path to fully or driverless driving
- Typical use case: Autobahn Chauffeur with $v_{\text{max}} = 130 \text{ km/h}$
- Function availability depends on preconditions => if preconditions are not given (foreseen or unforeseen) transition to driver

Pro (compared to level 4 systems):

- System can rely on capability of humans for handling of unknown or complex situations

Con:

- Transition might lead to new risks
Validation Challenge of Automated Driving

Challenge: Validation of promised safety level above the level of driving by humans

- Evidence is needed that risk does not exceed today reference.
- But what is the safety reference for validation?
Safety References

Reference variants:

- Possible safety references vary by several orders of magnitude, both far above and below today's reference safety values.

- Progress in safety validation for automated vehicles must be measured in comparison with today's risk values.

- At least two relevant metrics must to be measured:
  - accidents with personal injuries
  - accidents with fatalities

- Present day driving tests are far from collecting enough data to cover the reference risk figures

Numbers for Autobahn in Germany 2014

<table>
<thead>
<tr>
<th>Accident category</th>
<th>Distance between accidents [after 1]</th>
<th>Test-drive distance [2], [3]</th>
</tr>
</thead>
<tbody>
<tr>
<td>with injuries</td>
<td>12⋅10^6 km</td>
<td>240⋅10^6 km</td>
</tr>
<tr>
<td>with fatalities</td>
<td>660⋅10^6 km</td>
<td>13.2⋅10^9 km</td>
</tr>
</tbody>
</table>
STOP!!!!!!

For today’s vehicles (as in aviation) there is no need for such high testing distance, why here?

What is the fundamental difference?
Differences between conventional and automated vehicles

Current validation methods do not cover the yellow area according to Rasmussen [8] and Donges [9]
What do we know about driving safety performance?

**Statistics and Accident Research**

- Reports on accident frequencies and their causes
- Figures about time gaps and (exceeding) speeds on some roads

**Driver modeling**

- Qualitative models for information processing and driving tasks (Rasmussen, Donges, …) are able to explain the observed behavior.
- Quantitative models for simple scenarios (car following, lane change, intersection crossing) are able to explain and predict traffic flow figures, but not accident frequencies and severity.
- Human reliability models (Reichart, …) interpret the observed accident frequencies.
Swiss Cheese Model (adapted to human drivers)

Simple Probabilistic Accident Model

\[ n_{\text{accidents,hd}} = n_{\text{crit,hd}} \cdot \rho_{\text{transition,hd}} ; \quad n_{\text{crit,hd}} = f(\text{driver}_{\text{ego}}, E_{\text{traffic/road}}) \]

\[ \rho_{\text{transition,hd}} = f(\text{driver}_{\text{ego,hd}}, \text{driver}_{\text{traffic}}) \]

- \( n \) = frequency
- \( \rho \) = transition probability
- \( E \) = exposure of circumstances for potential hazards


Cheese model idea from [10]
Knowledge of the driving task and respective safety

Lacks:

- Serious figure of the accident avoidance capability of human drivers
  - Frequency and type of non-standard situations (both self-caused or innocently exposed)
  - Performance of human drivers in non-standard situations

Dark matter problem:

- We only know standard scenarios and reported failure scenarios (recorded accidents).
- Almost nothing is known about the transition probability from accident-free driving to accident occurrence and the frequency and type of critical scenarios.
- Avoiding the accidents that human drivers cause is not necessarily sufficient to reduce accident frequencies.
Dark Matter Problem (today)

Uncritical scenarios (very low potential for accidents)

Critical scenarios (potential for accident)

True accident scenarios
Swiss Cheese Model  
(adapted to automated driving)

**Accident Model for Automated Vehicles**

\[
n_{\text{accidents,ad}} = n_{\text{accidents,ad,old}} + n_{\text{accidents,ad,new}}
\]

\[
n_{\text{accidents,ad,old}} = n_{\text{crit,ad,old}} \cdot \rho_{\text{transition,ad,old}}
\]

**Automation Risks**

\[
n_{\text{accidents,new}} = n_{\text{crit,ad,new}} \cdot \rho_{\text{transition,ad,new}} ; n_{\text{crit,ad,old/new}} = f(\text{robot}_\text{ego}, E_{\text{traffic/road}})
\]

\[
\rho_{\text{transition,ad,old/new}} = f_{\text{old/new}}(\text{robot}_\text{ego}, \text{driver}_\text{partner})
\]
Dark Matter Problem

- Uncritical scenarios (very low potential for accidents)
- Critical scenarios (potential for accident, old type)
- True accident scenarios (old type)
- Critical scenarios under Automation, (new critical scenarios)
- Automation accidents (new type)
Missing Knowledge

In order to predict the safety of automated vehicles we need:

- Valid critical scenarios (remaining and new critical scenarios) and their specific characteristics, in sufficient quantity
- Valid models of the AV capability to control critical situations in a safe manner.
- All figures must be compared with the reference risks for each relevant class.

With respect to the Swiss Cheese Model:

- We must model each slice in order to predict the risk of AVs with high accuracy.

With respect to the Dark-Matter-Problem:

- The occurrence of critical scenarios and the capability to control them have made „bright“.
First conclusion

The obvious safety gain:

- The functional design of automated driving promises higher safety by reduction of frequency of known critical situations.

But we do not know:

- Capability of AD to avoid accidents in the remaining critical situations
- Frequency of new critical situations generated by automated driving and the capability to control them safely.

Validation of automated driving has to cover both and has to gain all necessary knowledge prerequisites.
Research project PEGASUS

EFFECTIVELY ENSURING AUTOMATED DRIVING.
Goals and Work Contents of PEGASUS

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 the Federal Ministry for Economic Affairs and Energy (BMWi)

- PEGASUS will close gaps in the area of testing and approving 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
## Key Figures

<table>
<thead>
<tr>
<th><strong>42 months term</strong></th>
<th><strong>January 1, 2016 – June 30, 2019</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>17 Partners</strong></td>
<td><strong>- OEM: Audi, BMW, Daimler, Opel, Volkswagen</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Tier 1: Automotive Distance Control, Bosch, Continental Teves</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Test Lab: TÜV SÜD</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- SMB: fka, iMAR, IPG, QTronic, TraceTronic, VIRES</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Scientific institutes: DLR, TU Darmstadt</strong></td>
</tr>
<tr>
<td><strong>12 Subcontracts</strong></td>
<td><strong>- i.a. IFR, ika, OFFIS</strong></td>
</tr>
<tr>
<td><strong>Project Volume</strong></td>
<td><strong>- approx. 34,5 Mio. EUR</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Subsidies: 16,3 Mio. EUR</strong></td>
</tr>
<tr>
<td><strong>Personnel deployment</strong></td>
<td><strong>- approx. 1.791 man-month or 149 man-years</strong></td>
</tr>
</tbody>
</table>
Goals and Work Contents of PEGASUS

Current State of Development of HAD

Prototypes

Lab / Testing Ground

Products

current status
## Current State of Development of HAD

### Prototypes
- Multitude of prototypes built by OEM with HAD-functionality
- Evidence, that HAD is technologically possible
- Partially tested in real traffic situations
- Test drives involve backup safety driver at all times

### Lab / Testing Ground
- Individual analyses to optimize prototypes
- Current test stands/testing grounds do not provide enough test coverage for all HAD features currently in focus
- There is no procedure for adequate testing (particularly performance) of HAD-systems

### Products
- No release or introduction of variety of HAD features without sufficient assurance
High standards regarding quality and performance of the automated vehicle → Measures that product needs to meet

Basic functionality is technologically given
Has been demonstrated in various projects

Existing measures for testing and release are insufficient, too cost-intensive and too complex

Consequently, the introduction of highly automated driving features today can only be achieved with great expenditure.
### Goals and Work Contents of PEGASUS

#### Central Issues of the Project

<table>
<thead>
<tr>
<th>Scenario Analysis &amp; Quality Measures</th>
<th>Implementation Process</th>
<th>Testing</th>
<th>Reflection of Results &amp; Embedding</th>
</tr>
</thead>
<tbody>
<tr>
<td>- What human capacity does the application require?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What about technical capacity?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Is it sufficiently accepted?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Which criteria and measures can be deducted from it?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Which tools, methods and processes are necessary?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- How can completeness of relevant test runs be ensured?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What do the criteria and measures for these test runs look like?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- What can be tested in labs or in simulation? What must be tested on test grounds, what must be tested on the road?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Is the concept sustainable?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- How does the process of embedding work?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Goals and Work Contents of PEGASUS

SP 1 Scenario Analysis and Quality Measures

- Determination of critical traffic situations
- Determination of safety level through assessment of probability of occurrence and mechanical manageability in critical situations
- Deduction of an accepted quality measure for automated driving features
- Determination of human and mechanical performance as well as effectiveness (accident avoidance potential)
- Description of application scenario (sample application: Autobahn-Chauffeur + enhanced application scenario)
- Deduction of requirements based on the accepted measure of quality
**Analysis**

of modification needs of existing metrics and automobile series development processes

**Transfer**

of systematic scenario guidelines into process steps in consideration of system classifications and levels of vehicle utilization

**Preparation**

of requirements definition for simulation, lab tests, testing ground and field coverage

**Guidelines and Protocols**

for the documentation of technological state-of-the-art compliance during the development process

---

1. **SP 2 Implementation Process**

   - Analysis
   - Transfer
   - Preparation
   - Guidelines and Protocols

   - Refinement of the guidelines for required documentation of process steps
Goals and Work Contents of PEGASUS

SP 3 Testing

- Detailing and completion of test scenarios of subproject 1, including technical quality measures as well as approval criteria
- Construction and filling of test specification database
- Establishment and verification of testing methods, interfaces, tools in the lab, on testing grounds and in real traffic
- Development and coordination of industrywide established models, tools and interfaces for the simulation

- Compilation of a test catalog and requirements for lab, testing ground and field coverage
- Construction of reference elements for practical testing and demonstration of functions
- Testing in the lab, on testing grounds and on the street
Goals and Work Contents of PEGASUS

SP 4 Reflection of Results & Embedding

**Statement**
about the distribution ratio between the applied test methods (from simulation to testing ground to field test)

**Assessment,**
whether the test goal can be achieved with the utilized processes and methods in PEGASUS

**Verification**
of methods to identify relevant situations, quality and criticality measures for the assurance of HAD features

**Proof of Concept**

**Assistance**
with embedding of acquired results with our project partners

**Lessons learned**
regarding the implementation of the results in existing corporate structures
Selected Goals of the Project

- Development of a procedure for the determination of design criteria and establishment of quality measures
- Considering the driver in regards to his abilities
- Design of the development process for the release of highly automated vehicle systems
- Conceptual design, assembly and demonstration of building blocks for an efficient toolchain for simulation, testing ground and field test
PEGASUS Goals beyond Research

- PEGASUS is a national project implementation for fast progress in automated driving
- Embedding of findings in the industry
- Distribution and pioneering of a standardization

⇒ All essential project results are freely accessible

- Collaboration with other consortia is highly appreciated
- We need a worldwide common understanding about how safety of automated driving has to be assured
- Exchange with safety assurance experts worldwide at PEGASUS interim presentation (Mid of October 2017)
Contact:
Technische Universität Darmstadt
Prof. Dr. rer. nat. Hermann Winner
winner@fzd.tu-darmstadt.de
+49 (0) 6151 / 16 24 200

More information:
www.pegasusprojekt.de