Safety Assurance for Highly Automated Driving – The PEGASUS Approach

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

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 automated 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
Reference variants:

- Possible safety references are within a wide bandwidth (several orders of magnitude), much above today road safety as well as much below.

- A progress in safety by automation has to be measured in comparison with today risk as reference.

- At least two relevant categories have to be addressed as reference:
  - accidents with damage to persons and specifically
  - accidents with fatalities

- Reference risk figures are far from today testing horizons by real driving tests, e.g. for Autobahn in Germany 2014

<table>
<thead>
<tr>
<th>Accident category</th>
<th>Distance between accidents [after 5]</th>
<th>Test-drive distance [6], [7]</th>
</tr>
</thead>
<tbody>
<tr>
<td>with injuries</td>
<td>$12 \cdot 10^6 \text{ km}$</td>
<td>$240 \cdot 10^6 \text{ km}$</td>
</tr>
<tr>
<td>with fatalities</td>
<td>$660 \cdot 10^6 \text{ km}$</td>
<td>$13.2 \cdot 10^9 \text{ km}$</td>
</tr>
</tbody>
</table>
STOP!!!!

For today’s vehicles (and more extreme for aviation) there is no requirement for such high testing distance, why here?

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

Current validation of vehicle doesn’t 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 frequency of accidents and their causes
- Figures about time gaps and exceeding speeds of 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 accidents frequency and severity.
- Human reliability models (Reichart, ...) interpret the observed accidents frequency.
Swiss Cheese Model (adapted to human drivers)

Simple Probabilistic Accident Model

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

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

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

Knowledge about 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 the reported fail scenarios (accidents), but do not know the probability for transition from accident free driving to real accident occurrence.

- Avoiding the known human accident causes are not sufficient:
  1. The accidents avoidance capability of humans is not recorded.
  2. No quantitative figure about types of critical scenarios and their frequency where humans avoid accidents.
Dark Matter Problem

- 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

\[ n_{\text{accidents,new}} = n_{\text{crit,ad,new}} \cdot \rho_{\text{transition,ad,new}} \cdot n_{\text{crit,ad,old/new}} = f(\text{robot}_\text{ego}, E_{\text{traffic/road}}) \]
\[ \rho_{\text{transition,ad,old/new}} = f_{\text{old/new}}(\text{robot}_\text{ego}, \text{driver}_\text{partner}) \]
Dark Matter Problem

- Uncritical scenarios (very low potential for accidents)
- Critical scenarios (potential for accident, old type)
- True accident scenarios (old type)
- Automation risk exposure (new critical scenarios)
- Automation accidents (new type)
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.
OBJECTIVES AND WORK CONTENTS OF PEGASUS

Project for establishing generally accepted quality criteria, tools and methods, as well as scenarios and situations for the release of highly automated driving functions
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
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

*SME:* 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

Working capacity
150 person-years
Current stage of development for HAD

Prototypes

Test lab / test ground

Products

today
Current stage of development for HAD

**Prototypes**
- OEM built many prototypes with HAD functionality
- Proof that HAD is technologically feasible
- Partially tested in real traffic, but always with a safety driver

**Test lab / test ground**
- Single considerations for optimizing prototypes
- Current test benches / test sites do not provide adequate test coverage for HAD functionalities
- There is no procedure for sufficient safety assurance validation of HAD systems

**Products**
- Without adequate validation, the release or introduction of HAD vehicles is not possible

---

25.07.2016
Main research questions

- What performance and safety criteria do systems for highly automated driving have to fulfill?
  - How do we validate their performance?
  - Starting with Autobahn Chauffeur, later for HAD under more complex conditions.

- How good is the human performance within the use case?
- How good is the machine’s performance?
- Is it sufficiently socially accepted?
- Which quality criteria can be derived from that?

- Which tools, methods, and processes are required?

- How can the completeness of relevant test cases be guaranteed?
- Pass/fail criteria for these test cases (from quality factors)
- Which part of these test cases can be tested in simulations / labs, which on roads?

- Does the concept work in practise?
Subprojects

- **SP 1**
  - Scenario analysis & quality metrics
  - Application scenario
  - Quality metrics
  - Extended application scenario
  - Lead: Volkswagen

- **SP 2**
  - Implementation processes
  - Process methodology
  - Process specification
  - Lead: Adam Opel

- **SP 3**
  - Testing processes
  - Test specification database
  - Laboratory and simulation tests
  - Proving ground tests
  - Field tests
  - Lead: Daimler, BMW, TÜV SÜD

- **SP 4**
  - Proof reflection & embedding
  - Proof of concept
  - Embedding
  - Lead: Continental
Closing the gap by PEGASUS

Prototypes

Test lab / test ground

Products

today

advancements by PEGASUS
PEGASUS goals beyond research

- PEGASUS is a national project implementation for fast progress in automated driving.

- Embedding of knowledge into the industry, as well as dissemination of knowledge and experience across the appropriate committees for standardization.

- Open access to all essential project results.

- Collaboration with other consortia is highly appreciated.

- Exchange with safety assurance experts worldwide (starting with a symposium in spring 2017, presumably in Munich)

- We need a worldwide common understanding about how safety of automated driving has to be assured.