Wie gut ist genug?

How good is good enough?
Goal: Safety argument

"How safe is safe enough?"

Start: Use-Case

PEGASUS Method for Assessment of Highly Automated Driving Function (HAD-F)
Exhibit Overview

PEGASUS Method for Assessment of Highly Automated Driving Function (HAD-F)

Assessment of Highly Automated Driving Function

- Requirements definition
- Database

Data processing

- Argumentation
- Evidence

Table of Contents

4 The Highway-Chauffeur
5 Scenario Description and knowledge-based scenario generation
6 L3-Transitions: Driver Takeover Capability in Real Traffic
7 Critical Scenarios for Human Drivers - Simulator Studies
8 Critical Scenarios for Human Drivers - Criticality
9 Critical Scenarios for Human Drivers - Impact Analysis
10 Potentially Critical Scenarios for and by the HAD-F (Automationrisks)
11 Social Acceptance for HAD
28 Safety Statement
29 Safety Argument

© PEGASUS
Part 1:
How Good is good enough?

Part 2:
Methods/Tools/Arguments
YOU ARE GOOD ENOUGH
there is no direct link between Safety of HAD and Social Acceptance
Individual risk acceptance

The individual accepted risk depends on the type of technology use!

Application of different risk acceptance principles

The individual accepted risk depends on the type of technology use!
Distance Based Approach

How long does an automated driving vehicle need to drive on highways without fatal accidents, in order to be confident (95% prob.) that it is better than a human equivalent?

<table>
<thead>
<tr>
<th>Thesis</th>
<th>A verification of this question needs to proof that the automated vehicle has less accidents with fatalities than the human peer group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently</td>
<td>614 million kilometers between two fatal accidents by humans</td>
</tr>
<tr>
<td>Target</td>
<td>Halve the risk of accidents with fatalities</td>
</tr>
<tr>
<td>Result</td>
<td>The required test distance is 6.14 billions kilometers</td>
</tr>
<tr>
<td>Challenge</td>
<td>Every system modification requires a repetition of all tests</td>
</tr>
</tbody>
</table>

Distance-based test approach is unfeasible for automated driving functions

A systematic scenario-based test approach is needed
Scenario Based Approach - PEGASUS

But how to map single test cases to global acceptance???
Safety Argument

What do people expect from highly automated mobility in the larger context? e.g. convenience, mobility benefits, data privacy

How to monitor a HAD-F over its entire life cycle? e.g. field monitoring

How to support a Safety Argumentation with evidence? e.g. safety case (Goal Structuring Notation, Assurance Case)

Which elements should a Safety Argumentation contain sufficiently? e.g. NHTSA design principles, German ethics commission

How to ensure necessarily compliance with all relevant standards and directives needed for homologation? e.g. ISO 26262, ISO/PAS 21448:2019(E)

AYER 0 - ACCEPTANCE MODEL
Embed a Safety Argumentation in a broader context of technology acceptance.

AYER 1 - TOP LEVEL SAFETY GOALS
Derive safety goals from agreed upon design principles in order to meet expectations such as positive risk balance.

AYER 2 - LOGICAL STRUCTURE
Build a logical link between safety goals to meet and evidence to support the Safety Argumentation.

AYER 3 - ACTIONS, METHODS AND TOOLS
Develop and implement actions, methods and tools to meet the top level safety goals.

AYER 4 - EVIDENCE
Consider results obtained by applying actions, methods and tools as evident because they are linked to top level goals.

INTEGRITY of elements

RELEVANCE of elements

FORMALIZATION of elements

NOT addressed in PEGASUS

EXEMPLARYLY addressed in PEGASUS

Focus of PEGASUS
So what’s the answer to the question?

How good is good enough?

To whom?

Customer / Society

What is good?

Safety / Risk

Risk is socially acceptable

positive risk balance

Verification & Validation of HAD behavioral performance

Security  HMI  ...

Product development

Other life cycle stages

Requirement definition

Data processing

Data Base

Assessment

The PEGASUS Method contributes to the Safety Argument

L0

Technology Acceptance

L1

Top Level Safety Goals

L2

- "The world in our heads is not a precise replica of reality; our expectations about the frequency of events are distorted by the prevalence and emotional intensity of the messages to which we are exposed." – Daniel Kahnemann (2011). Thinking, Fast and Slow (p.138)

- "... Homologation of automated Systems is acceptable, if they diminute damages in terms of a positive risk balance in comparison to human driving capabilities“ - German Ethics commisstion, June 2017

- 12 NHTSA design principles

- PEGASUS and other Methods

1. "The world in our heads is not a precise replica of reality; our expectations about the frequency of events are distorted by the prevalence and emotional intensity of the messages to which we are exposed." – Daniel Kahnemann (2011). Thinking, Fast and Slow (p.138)

2. "... Homologation of automated Systems is acceptable, if they diminute damages in terms of a positive risk balance in comparison to human driving capabilities“ - German Ethics commisstion, June 2017

3. 12 NHTSA design principles

4. PEGASUS and other Methods
Part 1: How Good is good enough?

Part 2: Methods/Tools/Arguments
The Highway Chauffeur

- Safeguarding of Level 3 (Highly Automated Driving) function
- Based on an application-oriented example, highway chauffeur
  - Basic function:
    - Highways or highway-like roads incl. road markings
    - Speed 0 - 130 km/h
    - Automated following in stop & go traffic jams
    - Automated lane changing
    - Automated emergency braking and collision avoidance
    - Construction sites
    - Automated exiting off the highway
    - Extreme weather conditions

source: VW
Scenarios and possibilities for description – Layer model

Layer 1: Road-Level
- Geometry, topology
- Quality, boundaries

Layer 2: Traffic Infrastructure
- Boundaries (structural)
- Traffic signs, elevated barriers

Layer 3: Temporary manipulation of Layer 1 and 2
- Geometry, topology (overlaid)
- Time frame > 1 day

Layer 4: Objects
- Static, dynamic, movable
- Interactions, maneuvers

Layer 5: Environment
- Weather, lighting and other surrounding conditions

Layer 6: Digital Information
- (e.g.) V2X information, digital map

© PEGASUS
### Functional scenarios

**Base road network:**
Three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs

**Stationary objects:**
- 

**Moveable objects:**
Ego vehicle, Traffic jam; Interaction: Ego in maneuver „approaching” on the middle lane, traffic jam moves slowly

**Environment:**
Summer, rain

### Logical scenarios

**Base road network:**
- Lane width: [2..4] m
- Curve radius: [0.6..0.9] km
- Position traffic sign: [0..200] m

**Stationary objects:**
- 

**Moveable objects:**
- End of traffic jam: [10..200] m
- Traffic jam speed: [0..30] km/h
- Ego distance: [50..300] m
- Ego speed: [80..130] km/h

**Environment:**
- Temperature: [10..40] °C
- Droplet size: [20..100] µm
- Rainfall: [0,1..10] mm/h

### Concrete scenarios

**Base road network:**
- Lane width: 3
- Curve radius: 0,7 km
- Position traffic sign: 150 m

**Stationary objects:**
- 

**Moveable objects:**
- End of traffic jam: 40 m
- Traffic jam speed: 30 km/h
- Ego distance: 200 m
- Ego speed: 100 km/h

**Environment:**
- Temperature: 20 °C
- Droplet size: 30 µm
- Rainfall: 2 mm/h

---

**Level of abstraction**

**Number of scenarios**
The human driver - driver takeover capability in real traffic

- holistic view on safeguarding of HAD requires consideration of the transition to manual
- testing of driver performance with a Level 3 driving function in real traffic on an approx. 120 km long motorway stretch near Cologne
- short takeover times, but partly insufficient or no safeguarding of the surrounding traffic during takeover

<table>
<thead>
<tr>
<th>takeover time (real traffic)</th>
<th>n</th>
<th>M (SD)</th>
<th>Min</th>
<th>Max</th>
<th>10th percentile</th>
<th>90th percentile</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal traffic</td>
<td>130</td>
<td>3.87 (1.35)</td>
<td>2.02</td>
<td>8.24</td>
<td>2.48</td>
<td>5.87</td>
</tr>
<tr>
<td>rush-hour traffic</td>
<td>107</td>
<td>3.21 (0.83)</td>
<td>2.05</td>
<td>6.69</td>
<td>2.46</td>
<td>4.11</td>
</tr>
</tbody>
</table>

- The question arises as to how a previous automated journey affects the handling of an unexpected event immediately after a completed takeover: Do the subjects really have control over the traffic situation after approx. four seconds?
  - A second study on a test track was conducted in order to investigate the subjects' handling of an unexpected event (suddenly braking vehicle in front).
  - A first evaluation of 20 participants shows that all were able to avoid a collision (16 participants by braking, 4 by braking and changing lanes). This could indicate that the human driver is able to handle an unexpected event after a completed takeover. It should be noted that there was no surrounding traffic.
  - The takeover times from the first study were confirmed in the second study.
Modeling Human Performance in Critical Scenarios

- **Human Performance in PEGASUS [3]**
  - ... a minimum requirement for the performance of highly automated vehicles
  - ... a benchmark against which highly automated driving functions can be compared [1]
  - ... a product of the driver’s capabilities and the task demands of the driving scenario [2].

- **Driving simulator studies are used to assess the thresholds of human performance in critical situations**
  - A stimulus (e.g. a cutting-in vehicle) is presented repeatedly with randomly varying intensity (e.g. criticality of the scenario).
  - Criticality was quantified by time to collision (TTC).
  - The threshold of human performance is represented by the probability to collide at a certain criticality.
Critical Scenarios for Human Drivers – Criticality Metric

- Goal: Definition of a metric to identify critical scenarios
  - Applied on human traffic, but eligible for automation
  - Identification for test case definition based on data recordings

- Two Approaches
  - Machine learned classification based on labelled scenarios
  - Optimization to find the trajectory with minimum criticality
The Human Driver – Impact Analysis

- Computation of the target population and the effectiveness of the highway chauffeur
  - ~27% of all fatalities on highways are addressed by the highway chauffeur
  - ~80% of all crashes of the target population of the highway chauffeur are caused by human factors

- Identification of extensions to the highway chauffeur or further actions, which have the highest benefit of increasing the target population
  - e.g. Extend the function that it could drive without lane markings or the lane markings have to be intact and visible

- Simulation of a generic highway chauffeur and comparison with the human driver from GIDAS
Potentially Challenging Scenarios for Highly Automated Driving

- Scenarios that are relatively easy to handle for humans may be challenging for HAD-F (e.g. missing lane markings)
- These scenarios need to be identified early to be tested exhaustively
- In order to do so and to ensure a view at this problem from different perspectives these scenarios were divided into three classes

### Challenges that arise from

- **Class (1):** Impacts of the environment on the automation (e.g. performance limitations of sensors, misguided interpretation of the environment)
- **Class (2):** Impacts of the automation on other traffic participants (e.g. reaction of automation cannot be anticipated by other road users)
- **Class (3):** Interaction with the human driver (e.g. mode confusion)

- For each of these classes a systematic method was developed to identify potentially challenging scenarios early with the help of expert knowledge
The overall rating of a test-case is derived by aggregating the time-discrete results of the multiple stages.

The contribution of the different stages to the overall test-case result differs depending on their character.
Safety Statement

Example for the multi-stage safety assessment

Video, re-simulation of a real world crash, where a merging car violates appropriate safety distances. The ego-vehicle (in this case a human driver) responds with a late braking intervention.

Video, same real world crash, where the ego-vehicle is now an automated car. In this simulation, the automated vehicle brakes earlier and thus avoids the crash.
Vielen Dank für Ihre Aufmerksamkeit!

Many thanks for your attention!