Validation of systems for (highly) automated driving

Matthias Stiller
Head of Testing Cross Divisional Systems
Integration and Validation of AD functions
4 Main Challenges

› The **driver** is (temporarily) **out of the Loop!**
  Validation of hand over scenarios.

› The **number of situations / scenarios** an automated driving vehicle will be able to handle correctly is **immense**!

› The resulting Integration & Testing effort **cannot be managed economically** by using traditional testing methods and processes!

› The assumption is that Automated Driving Functions will need to reduce the number of accidents by 50%
  ➔ The amount of testing kilometers to prove correct functionality is estimated with **several 100Mio Kilometers**
  (Prof. Winner)!
Function shall react to …

**TRUE** (Function reaction correct!)

- Event happened *as expected*
  - e.g. real obstacles are reported
  - Traffic Sign correctly reported
  - Lane tracked correctly

**FALSE** (Function reaction incorrect!)

- Event happened *unexpected*
  - e.g. non existing objects are reported
  - Traffic Signs are incorrectly reported
  - Lane tracking is incorrect

**NEGATIVE**

- No event, *as expected*
  - e.g. empty road

- Event not happened *unexpected*
  - e.g. a real obstacle is not reported
  - Traffic Signs are not detected
  - Lane tracking is not done

1 False Positive during a vehicle lifetime $\triangleq$ 1 incorrect event per 200,000km!

$\Rightarrow$ 1Mio test kilometers!
Integration & Validation Concept for Automated Driving

Approach

› Analyse Human behaviour / system in interaction with the environment. What is their interface?

› How does it come to critical / accident situations? What is the probability of an accident?

› How does a human driver react in critical / accident situations?

› All above mentioned questions can be summarized to:

   › What is the reference for automated driving functions?

› What is the consequence for system development and the resulting validation concept?
How does it come to accident situations in general?

Swiss Cheese Model (D. Orlandella, J. Reason)

Characteristics of environment
For instance: weather conditions, road conditions, unclear road intersections

Driver characteristics
For instance: age (young & old), high readiness to assume risk, overestimation of one’s own capabilities

Error of Driver
For instance: to low concentration, distraction by secondary tasks, conversation with fellow passengers

Vehicle characteristics
For instance: no ESP, worn tires, oversized engines

Violation of driver
For instance: drinking & driving, speeding, not enough safety distance, overtaking, tiredness

Conclusion: Accidents are a chain of unfortunate circumstances!
Swiss Cheese Model
Example

Ego Vehicle

Potential Conflict Object

- **driver error**
  - $p_1 = 1 \times 10^{-4}/h$

- **conflict object**
  - $p_2 = 1 \times 10^{-1}/h$

- **No avoidance Reaction driver**
  - $p_3 = 1 \times 10^{-2}/h$

- **no avoidance reaction by conflict object**
  - $p_4 = 1 \times 10^{-1}/h$

**ACCIDENT**

$pa = 1 \times 10^{-8}/h$
Failure tree model of an accident and its probabilities

The probability of an accident with a human driver on a freeway is about $1 \times 10^{-8}/h$.

**Idea**

- The overall accident probability ($p_a$) can only be decreased / improved by the system by improving / decreasing the probabilities $p_1$ and $p_3$.

- Acceptable failure probabilities: $p_1 \sim 1 \times 10^{-5}$, $p_3 \sim 1 \times 10^{-3} \Rightarrow 100!$
Two major issues
Ensure handling of loss of function and loss of integrity

Loss of function / fail operational: Redundancy necessary e.g. two EPS, two brake systems
Loss of integrity: Ensure that the performance of the function is correct.

Example: Loss of integrity

Validation Effort similar to current driver assistance systems!
Deduced Sensor Performance
Example: Radar
Sensor Performance of radar
and impact of influencing parameters

Variation of environmental Parameter

- Ideal Condition
- Reduced Performance
- Low Performance
- System Limit
Bottom Up approach after component validation focusing on System Integration and validation on vehicle level

Focus on vehicle level

- Intercomponent failure! Interface failure! Simulation environments and vehicle!
- Full chain of effects mainly with simulation methods but also vehicle tests! Focus critical scenarios!
PEGASUS
(Projekt zur Etablierung von generell akzeptierten Gütekriterien, Werkzeugen und Methoden sowie Szenarien und Situationen zur Freigabe hochautomatisierter Fahrfunktionen)

Objective:

› How good is good enough?
› How can we prove that the function works correctly?

TP 0 Projektmanagement

<table>
<thead>
<tr>
<th>TP 1</th>
<th>TP 2</th>
<th>TP 3</th>
<th>TP 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP 1.1</td>
<td>AP 2.1</td>
<td>AP 3.1</td>
<td>TP 4.1</td>
</tr>
<tr>
<td>Anwendungsszenario</td>
<td>Prozessanalyse</td>
<td>Testvorbereitung</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td>AP 1.2</td>
<td>AP 2.2</td>
<td>AP 3.2</td>
<td>TP 4.2</td>
</tr>
<tr>
<td>Qualitätsmaße</td>
<td>Prozessmethodik</td>
<td>Labortests/Simulation</td>
<td>Einbettung</td>
</tr>
<tr>
<td>AP 1.3</td>
<td>AP 2.3</td>
<td>AP 3.3</td>
<td></td>
</tr>
<tr>
<td>Erweitertes</td>
<td>Prozessspezifikation</td>
<td>Prüfgeländetest</td>
<td></td>
</tr>
<tr>
<td>Anwendungsszenario</td>
<td></td>
<td>AP 3.4</td>
<td>Feldabsicherung</td>
</tr>
<tr>
<td>AP 1.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Erweiterte Qualitätsmaße</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Objective of subprojects

TP 1: Szenarienanalyse und Qualitätsmaße
- Description of the Autobahn Chauffeur, determination of critical scenarios, analysis of human behavior in critical scenarios, definition of system limits, definition of quality and acceptance criteria

TP 2: Umsetzungsprozesse
- Identification and definition of general development and testing processes and methods for automated driving functions
Objective of subprojects

▶ TP 3: Testen

▶ Definition of tool chain simulation, vehicle test on test tracks as well as field operational tests/endurance runs, prove that critical scenarios can be handled correctly by the automation based on acceptance criteria defined in TP1

▶ TP 4: Ergebnisreflektion und Einbettung

▶ Proof of concept, critical reflection of the working packages of the other subprojects

PEGASUS
Thank you for your attention!