Perspectives on Automated Driving, Development Processes and Beyond
The Traditional Starting Point

Sensor Configuration

Different Sensor Views

Sensor Fusion

Planning and Decision Making in an Interpretation of the Physical World
A Look Beyond…
New challenges emerging due to high situational complexity

Traffic Environment
Missing information on Driver Intentions
Complex Road Structure
Signal Phases & Queues

Not even considering pedestrians, cyclists, kids etc.
Exemplary Test Approach for Automated Driving

Coupling of VEHICLE DYNAMICS and TRAFFIC FLOW simulations using DIGITAL TWIN
But there are simpler tasks than „just“ creating such a Digital Twin …
And Finally Facing Again the Old Enemy: Complexity

ACC: Long-Range-Radar and ECU:

36 Possible Combinations
And Finally Facing Again the Old Enemy: Complexity

ACC and LCA: Long-Range-Radar, Camera and ECU:

<table>
<thead>
<tr>
<th>Komponente</th>
<th>Motor/Getriebe</th>
<th>Bremse</th>
<th>Linkslenker/Rechtslenker</th>
<th>Werk</th>
</tr>
</thead>
<tbody>
<tr>
<td>LRR</td>
<td>LRR</td>
<td>LRR</td>
<td>LRR</td>
<td>A</td>
</tr>
<tr>
<td>ECU</td>
<td>ECU</td>
<td>ECU</td>
<td>ECU</td>
<td>A</td>
</tr>
<tr>
<td>Cam 1</td>
<td>Cam 2</td>
<td>Cam 2</td>
<td>Cam 2</td>
<td>A</td>
</tr>
</tbody>
</table>

Vehicle with ACC and LCA

⇒ 288 Possible Combinations
An Exemplary Development Process

Vehicle w/o Automation (early 2010s) and w/o considering Powertrain

Ca. 400 Manufacturing Options, 30 Electronic Control Units, Several Hundred Cal-Files, Thousands of Parameters

Duration: Several years, depending on specific OEM

T. Tiecke et al. (Opel)
The V-model is a process model originating from the software development that has established itself as well for the development of complex safe-critical systems in the avionics and automotive domain.

- **Requirements Vehicle Level**
- **Acceptance Tests Vehicle Level**

- **System Design**
  - The first step is to specify the requirements for the complete product (which is the vehicle here) from the perspective of the stakeholders.
  - For the final approval it is examined whether the complete product satisfies the requirements of the stakeholders.

- **System Tests**
  - The remaining part of the left branch of the V covers the design of the system on multiple levels of abstraction finally resulting in a technical implementation.

- **Subsystem Design**
- **Integration Tests**
  - The right branch of the V describes the verification and validation of the developed system. For this purpose for each abstraction level test obligations are defined that need to be satisfied for a successful product development.

- **Component Design**
- **Component Tests**

- **Technical Implementation**
V Model and ISO 26262

After defining the functional specification of the system under development, a hazard analysis and risk assessment is performed. Based on these results, the system is designed, and a safety concept is developed. The hardware and software development then takes place in further parallel runs of the V-model.

On the right branch of the V integration tests for the developed components are performed and a validation of the safety goals (safety validation) takes place as well as a functional safety assessment of the complete vehicle against the functional specification.
ISO and SOTIF

The Hazard and Risk Analysis (HARA, PHA) determines the Automotive Safety Integrity Level (ASIL) according to ISO-26262.

Severity: S1 ... S3:
Light injuries ... Life threatening injuries

Exposure: E1 ... E4:
Very low probability ... low ... medium ... high (>10%)

Controllability: C1 ... C3:
Simple (>99%) ... normal (>90%) ... difficult (<90%)

ISO26262 only as basis ... „Safety of the Intended Functionality“ needs to be covered as well.

NEW CHALLENGES: Mix Traffic and Issues at Other Cars

T. Weispfenning (Opel)
Process Extension

- „Silent Testing“ Approaches
- Staggered Deployment via Restricted Fleets

plus contingently

as well as the corresponding feedback cycles
Exemplary Impact on OEM Development

Scenario-State-Space

Scenario-based Toolchain

Not Captured Scenarios

Simulation-based Toolchain

Application in Vehicle Program A

Verification & Validation Vehicle Program A
By Team 1
For Market A

Application in Vehicle Program B

Verification & Validation Vehicle Program A
By Team 2
For Market B

Application in Vehicle Program C

Verification & Validation Vehicle Program B
By Team 3
For Market C

Global Feature with Regional Application Parameters
Exemplary Impact on OEM Development

- Investigate driving situations and influencing parameters
- Define real-world driving requirements
- Collect data in real-world scenarios
- HiL-resimulation of existing data
- Execute test cases (vehicle and HiL)
- Update SW / Update Calibrations
- Final SW
- SW development + calibration
- SW release

T. Weispfenning (Opel)
What is the impact on PEGASUS methodology?

- PEGASUS method needs to be coordinated with established OEM and industry processes
- Do we miss something when applying a scenario-based approach
- How may the testing effort be structured?
Approach to Assess and Structure Challenges

1. **Assumption coverage** - states the sufficiency of assumptions w.r.t. the design intent
2. **Unfounded evidence** - refers to arguments without supporting evidence
3. **Unused evidence** - refers to evidences not used for the safety case

II. Apply assessment criteria

<table>
<thead>
<tr>
<th>Considered Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Information base</td>
</tr>
<tr>
<td>2. Ontology</td>
</tr>
<tr>
<td>3. Criticality</td>
</tr>
<tr>
<td>4. Association</td>
</tr>
<tr>
<td>5. Relation</td>
</tr>
<tr>
<td>6. Variation</td>
</tr>
</tbody>
</table>

I. Identify elements with a potential for affecting the provided evidence
Specific Example: Information Basis

**Obtained scenes**
- NDS/FOT
- Accident Database
- etc.

**Information base**
- System knowledge
  - Automation risk I - III
  - Nomenclature

**Unknown unknowns**
- Unfounded

**Evidence**

Indicates the reachable evidence

- Solution: Ontology
- If not relevant

- If incomplete
- Solution: ?unknown?
Functional Decomposition

- A scenario-based approach is able to reduce the test effort
  - BUT the various scenarios still check all functional levels simultaneously.
  - High number of combinations of initial and boundary conditions lead a large number of test cases

- The functional decomposition and the structuring of relevant scenarios into „test case quants“, which test in structured way just one (or a few) functional levels:
  - Reduces the overall test effort
  - Enables the application of tools (XiL, proving ground etc.) according to their validity.
  - A reduction of the test risk.
Functional Decomposition

Relevant Scenarios (functional)

Matrix

Definition and Assignment of Failure Criteria via FTA

Elimination and Bundling of Failure Criteria

Which requirements result from certain scenarios for specific levels

Decision on Appropriate Test Cases and Test Tools for Remaining Failure Criteria

- Functional Levels
- Information access
- Information reception
- Information processing
- Behavioral decision
- Action
New development approaches should be as „downward-compatible“ to the existing automotive process world as possible (and as making sense)

AD vehicles initially could have a lower diversity than current cars to cope with complexity issues

Structured approaches needed to make clear what is known, what is not known and about what not even is known to be unknown.

Structured approaches like functional decomposition needed to reduce test efforts

To introduce AD cars, concepts like „silent testing“ in restricted fleets and a staggered deployment to real-world application including learning cycles are worth to be examined

PEGASUS is working on these challenges
Thank you … Merci beaucoup