Approval and Homologation of Autonomous Vehicles – With dSPACE Support

Jann-Eve Stavesand, Munich, November 20th, 2019
Contact

**Jann-Eve Stavesand**

Head of dSPACE Consulting

- Deep Knowledge of the development and verification processes in the automotive industry (OEMs and Suppliers)
- Functional Safety Expert – Contributes on ISO 26262 2nd Edition and ISO/PAS 21448 (SOTIF)
- Model-based Design & Virtual Testing
- Developing Test Strategies for Autonomous Driving Functions

**Address**
dSPACE GmbH
Rathenastraße 26 • 33102 Paderborn
Germany

**Phone**
+49 5251 1638 526
+49 160 8829466

**E-Mail**
JStavesand@dspace.de
Building Blocks of an Approval and Homologation Strategy

<table>
<thead>
<tr>
<th>Essential Blocks</th>
<th>Building an Approval Strategy from System Design to Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulations</td>
<td>Data Processing</td>
</tr>
<tr>
<td>Acceptance Criteria</td>
<td>Confidence &amp; Compliance</td>
</tr>
<tr>
<td>Safety &amp; Security</td>
<td>Training &amp; Prototyping</td>
</tr>
<tr>
<td>Assess &amp; Analyze Development Processes</td>
<td>Series Development &amp; System Integration</td>
</tr>
<tr>
<td>Confidence &amp; Compliance</td>
<td>Integration &amp; Testing</td>
</tr>
</tbody>
</table>

dSPACE Consulting - JStavesand@dspace.de
Evolution of Legislative Directives
**Future International Regulations for AD Type Approvals**

**General Concepts of Homologation**

- **USA**
  - Self Certification
  - Fast
- **China**
  - Integrated National Strategy
  - Medium
- **Europe**
  - External Compliance Demonstration
  - Slow

**GOAL:**
Increasing reliability and efficiency of development and testing

**Significant increase in development and testing efforts with different lead times**

**Levels of Type Approval – Decrease in Volume**

- UNECE 2007/46/EC
- Regulation No 130
- Regulation No 79
- Regulation No 13-H
- ...

**Vehicle**
- (WVTA)

**Vehicle Type Approval**

**Component Approval**
Concept for Certification – The Three Pillars – Phases of Type Approval

**Main Points for Certification**

➢ Overall impression of system behavior on public roads
➢ Assessment of system’s ability to cope with real world traffic
➢ Guidance through given set of situations which shall be passed

➢ Validation of audit/assessment results with real world behavior
➢ Assessment of system behavior in fixed set of challenging cases
➢ Reproducibility of situations is given

➢ Audit of development process and V&V Strategies
➢ Assessment of safety concept (functional safety, safety of use) and measures taken
➢ Use of simulation results
➢ Measuring process maturity
The Approval is Based on the Integrity of the Development Process
Evaluation of the Residual Risk – ISO/PAS 21448

- **Verification**: Evaluating system behaviour within known risks by requirements-based testing
- **Validation**: Evaluating the residual risk by identifying the Unknown Risks

Evaluation of the residual risk demands a suitable combination of testing approaches
- Requirements-based testing
- Scenario-based testing

Goal: Reduce the residual risk to a reasonable minimum and provide evidence of system behaviour within a known environment
- A combination of vehicle testing, simulation and virtual testing is necessary

- **Verification**: Evaluating known risks by requirements-based testing
  - Requirements-based testing based on known Triggering Events

- **Validation**: To evaluate the residual risk the Unknown Risks have to identified
  - Scenario-based testing to identify new Triggering Events and to reduce the Unknown Risks
Known Risks & Unknown Risks for Homologation

**Known Risks**
- ISO 26262 are established processes, but are not yet consistently implemented in many projects.
- Key aspect to qualify the projects for homologation

**Unknown Risks**
- The SOTIF process is a highly iterative process through the phases of system engineering and V&V
- Achieving the SOTIF is mainly based on identifying risks that are Triggering Conditions for system insufficiency
**SOTIF: Illustration of the Triggering Conditions Identification**

**SOURCE:** 431 ISO TC22-SC32 WG8 N701 ISO WD 21448 for commenting

dSPACE Consulting - JStavesand@dspace.de
V&V Techniques
Meaningfully Combined
## Test Methods and Test Environments

<table>
<thead>
<tr>
<th>Test Method</th>
<th>...to check (examples) ...</th>
<th>MIL</th>
<th>SIL</th>
<th>PIL</th>
<th>HIL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements-based test</strong></td>
<td></td>
<td>Applicable for functional requirements on model level</td>
<td>Applicable for functional requirements on software level</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>• Software architectural design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Specified functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Interface test</strong></td>
<td></td>
<td>Partially applicable on model level</td>
<td>Applicable on code level without HW dependent software</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>• SW unit implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HW-SW interface specification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fault injection</strong></td>
<td></td>
<td>Partially applicable on model level</td>
<td>Applicable with instrumented software code</td>
<td>Applicable with prototyping hardware and/or instrumented software code</td>
<td>Applicable</td>
</tr>
<tr>
<td>• Testing of safety mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Robustness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resource usage / Performance test</strong></td>
<td></td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Partially applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>• Sufficiency of resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• HW architectural design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scenario-based test</strong></td>
<td></td>
<td>In most cases, there will be no model of the complete AD function</td>
<td>Applicable</td>
<td>Applicable</td>
<td>Applicable</td>
</tr>
<tr>
<td>• Validation of real life use cases</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SOTIF Validation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

dSPACE Consulting - JStavesand@dspace.de
Test Strategy for ADAS/AD

Sensing

Perception

Data processing

Fusion

Data fusion

Localization

Environment model

Application

Situation analysis

Trajectory planning

Decision making

Motion control

Actuation

OTA test bench

Data replay tests

Closed-loop SIL and HIL simulation

Real test drives
Homologation Starts From Day One
**Homologation Starts From Day One**

**Data Processing**
Know-how on data logging, ingesting, storing and handling of big data

**Training & Prototyping**
Know-how on AI and classical controller development and prototyping

**Integration & Testing**
Agile development, process automation and intensive use of simulation

**Confidence & Compliance**
Qualification of software tool chains and processes, reliability of test systems, enabling workflows for the highest level of safety criticality

**Series Development & System Integration**
Incremental integrations, seamless reuse of artefacts, release testing and series development, process reliability and collaboration of several parties

---

**dSPACE Consulting - JStavesand@dspace.de**
Homologation Starts From Day One

Data management

Raw data → enriched data → simulation scenarios → test data

Record data (test vehicle) → Ingest & store data → Select & enrich data → Train AI (F(x) 1...k) → Develop algo (1...j) → Integrate software

Replay data (SW reprocessing) → Simulate (closed-loop SIL) → Integrate software

Simulate (closed-loop SIL) → Integrate HW/SW sub system 1 → Integrate system

Integrate HW/SW sub system n → Simulate (closed-loop HIL) → Test drive (closed-loop HIL) → Field operation → Raw data

Continuous integration/ Continuous deployment

AD software stack

Data management

Raw data → enriched data → simulation scenarios → test data

Record data (test vehicle) → Ingest & store data → Select & enrich data → Train AI (F(x) 1...k) → Develop algo (1...j) → Integrate software

Replay data (SW reprocessing) → Simulate (closed-loop SIL) → Integrate software

Integrate system → Simulate (closed-loop HIL) → Test drive (closed-loop HIL) → Field operation → Raw data

Continuous integration/ Continuous deployment

AD software stack
Confidence & Compliance
Verification of Suitability

1. **Adequacy and Calibration**
   - Is the test environment (HIL system) technically capable to execute the planned tests as required in the verification planning of ISO 26262-8:2018 Section 9.4.1 (adequacy)?
   - How can we ensure that test equipment delivers valid and reproducible results as required by ISO 26262-2:2018 Section 5.4.5.1?

2. **Validation**
   - Does the model make the reality sufficiently accurate? [ISO 26262-6:2018 B.3.5 Verification (static and/or dynamic) (Clauses 9, 10 and 11)]
   - Does the bus or network simulation produces valid results?

3. **Software Tool Qualification**
   - What is the tool confidence level? [ISO 26262-8:2018 Section 11]
   - How can we qualify the software tool chain? [ISO 26262-8:2018 Section 11.4.6]
The entire development process is decisive for approval and homologation.

You need a partner with all the expertise directly from day one, with the necessary process and tool know-how and a partner network to support end-to-end.

Product Safety

<table>
<thead>
<tr>
<th>Standards for State-Of-The-Art Development and Testing</th>
<th>Regulations for Type Approval</th>
</tr>
</thead>
</table>

Data management

Raw data -> enriched data -> simulation scenarios -> test data

Continuous integration/Continuous deployment

AD software stack

Homologation

PTI

dSPACE Consulting - JStavesand@dspace.de
dSPACE will support you from day one to achieve the goal of approving systems for AD