SAFETY FIRST FOR AUTOMATED DRIVING

White paper globally published on 2nd of July 2019
ABSTRACT
Automated Driving Systems

› Publication merges input of OEMs, tiered suppliers and key technology providers

› Positive risk balance
  › Safety by design and verification & validation methods
  › Comprehensive approach to safety relevant topics

› Intends to collaborate to industrywide standardization
THE TWELVE PRINCIPLES OF AUTOMATED DRIVING

› **SAFE OPERATION**
  › Deal with degradation
  › Fail operational

› **SAFE LAYER**
  › Recognize system limits
  › React to minimize the risk

› **OPERATIONAL DESIGN DOMAIN**
  › ODD determination
  › Manage typical situations

› **BEHAVIOR IN TRAFFIC**
  › Manners on the road
  › Conforming to rules

› **USER RESPONSIBILITY**
  › Responsibilities
  › Mode awareness

› **VEHICLE-INITIATED HANDOVER**
  › Minimal risk condition
  › Takeover request

› **VEHICLE OPERATOR-INITIATED HANDOVER**
  › Engaging and disengaging of AD system
  › Ensure intent of handover with high confidence

› **INTERDEPENDENCY (OPERATOR ↔ AD SYSTEM)**
  › Take effects on the driver due to automation into account

› **DATA RECORDING**
  › Record relevant data when an event or incident is recognized
  › Complies with the applicable data privacy laws

› **SECURITY**
  › Protect the automated driving system from security threats

› **PASSIVE SAFETY**
  › Crash scenarios (vehicle layout modifications)
  › Alternative seating position (new uses for the interior)

› **SAFETY ASSESSMENT**
  › Verification and validation to ensure that safety goals are met
  › Reach a consistent improvement of the overall safety
This publication is structured as interconnected topics which build upon one another to achieve an overall safety vision.

The roof ridge in the figure represents the positive risk balance as an initial starting point and the overall goal.
HUMAN - MACHINE INTERACTION

- Introducing L3 automated driving system,
  - the vehicle operator is allowed to **cede full control to the vehicle** during the nominal driving task **within** ODD
  - user’s **correct interpretation** of the actual driving mode and related **responsibility** for dynamic driving tasks (DDT) is crucial to enable safe driving

![Roles of the User & Automated Driving System by Level of Driving Automation](image)

Levels of automation according to SAE J3016
REALIZING NOMINAL AND DEGRADED CAPABILITIES

› Capabilities based on Sense – Plan – Act to achieve nominal performance

› Ensure degradation in case of insufficient nominal performance or other failures

› Ensure safe mode transitions
### EXAMPLE TRAFFIC JAM PILOT (L3)

<table>
<thead>
<tr>
<th>Nominal Function Definition</th>
<th>Sensing Elements for Localization</th>
<th>Sensing Elements for Perceive Relevant Objects</th>
<th>ADS Mode Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>› <strong>Vigilant</strong> driver with driver’s license, › driving only on <strong>structurally separated roads</strong> › typically <strong>no</strong> pedestrians or cyclists › 60 km/h <strong>max</strong> › <strong>only</strong> with leading vehicles › <strong>no</strong> lane changing › <strong>no</strong> construction sites › <strong>only</strong> during daylight, without rain › <strong>only</strong> temperatures higher than freezing point</td>
<td>› Determine whether the vehicle is on the <strong>highway</strong></td>
<td>› Leading <strong>vehicles in front</strong> of the ego vehicle › Lane markings › <strong>(vulnerable) road users</strong> (even though they are excluded from the ODD) › <strong>Diversity object detection methods</strong> are preferred to cover the performance weakness of single sensors › <strong>High-level object fusion</strong> is considered a meaningful measure</td>
<td>› Check <strong>activation</strong> conditions › Check <strong>deactivation</strong> conditions › Ensure that the vehicle has either reached a <strong>fail-safe state</strong> › Or that the user has <strong>safely taken over</strong> control</td>
</tr>
</tbody>
</table>

| Minimal Risk Conditions | Driver has taken over control › Deactivate as soon driver has control or the vehicle is stopped › Vehicle is stopped **in-lane** › **Immediately** stop the vehicle with **fixed** deceleration › **lateral** vehicle movement based on **last valid** trajectory | | |

9 October 2019
Statistical demonstration of system safety and a **positive risk balance** without driver interaction

System safety with driver **interaction** (especially in takeover maneuvers)

Consideration of scenarios currently **not known** in traffic

Validation of various system **configurations** and **variants**

Validation of (sub) systems that are based on **machine learning**
A viable test strategy responds to the **key challenges** in the V&V of automated driving systems

- by carefully breaking down the overall **validation objective** into **specific test goals** for every object under test
- and by defining **appropriate** test platforms and test design techniques
SAFETY ASPECTS OF DEEP LEARNING IMPLEMENTATION

› **General considerations**
  › Be agnostic to means of implementation; documentation during full process chain, creation of safety artefacts.

› **Define**
  › ODD, Data set, probabilistic output, KPIs, target hardware

› **Specify**
  › Data set specs, labelling specs, labelling quality, DL model architectures, observers.
SAFETY ASPECTS OF DEEP LEARNING IMPLEMENTATION

› Develop & Evaluate
  › DL model architecture (layers, connectivity, activations, pooling/upsampling, stride, ...); composition of loss, regularization, optimization methods (solver, learning rate, ...).

› Deploy & Monitor
  › Challenges: unseen data, confidence interpretation, emerging features, distributional shift.