SAFETY – CHALLENGES FOR E-MOBILITY AND AUTOMATED DRIVING
Safety – Challenges for E-Mobility and Automated Driving

Agenda

- Current challenge
  - FuSa vs. Safety
  - ISO 26262 and SOTIF
  - Fail-op. Systems
  - ...
- Aspects for solutions
- Conclusion
Safety – Challenges for E-Mobility and Automated Driving
Safety – Challenges for E-Mobility and Automated Driving

Safety

Control of Mission – Crash Avoidance / Crash Impact Mitigation
Control of Traffic
Control of Maintenance / Service
Control of Environmental Impact
Control Energy and other technology
Safety – Challenges for E-Mobility and Automated Driving

Safety Life-Cycle

<table>
<thead>
<tr>
<th>Role</th>
<th>Phase</th>
<th>Hazard (cause)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>(Design &amp; Production)</td>
<td>Incorrect product design (fire, thermal, high voltage, crash)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorrect assembly / production (failure in mechanical or electrical integration, installation of wrong software)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorrect instructions</td>
</tr>
<tr>
<td>Mission</td>
<td>(Driving)</td>
<td>Functional failure, Driver mistakes, Environmental impacts (noise, road traffic impacts, etc.)</td>
</tr>
<tr>
<td>Service</td>
<td>(Maintenance &amp; Repair)</td>
<td>Working protection, Incorrect instructions, Incorrect diagnostic (on-line, off-line, charging)</td>
</tr>
</tbody>
</table>

Figure 1: Safety Activities during vehicle Lifecycle
Safety – Challenges for E-Mobility and Automated Driving

View and Ergonomics

Figure 2: Steering Wheel Movement (Ergonomics)

Figure 3: Evaluation of 180° Field of Forward Vision of the Driver (View)
(Reference: GB/T 11562)

MOST REQUIREMENTS DERIVED FROM ARE RELEASE REGULATIONS SUCH AS ‘DIRECTIVE 2007/46/EC’ (equivalent to StVZO in Germany)

Ergonomics: Safety-in-use

- Information -> Driver
  - Correct interpretation of instruction by the driver
- Driver -> System
  - Incorrect realization of driver’s demand by the system

View: Forward Visibility

- The standard GB 11562 specifies the requirements and the measurement methods to achieve a successful 180° forward visibility for drivers.
- To restore visibility during the cold and wet weather conditions every vehicle should be equipped with a defrosting system and a demisting system specified by the standard GB 11555.
Safety – Challenges for E-Mobility and Automated Driving

Mission Phase:
The functional failure (malfunctions) derive from the possible degree of freedom of a generic 4 wheel car. It is the mayor source of hazards during the mission phase of a car.

Vehicle Level Degree of Freedom

a) Longitudinal: Acceleration / Deceleration

Malfunction
- Driving torque is too high / low / unintended
- Brake torque is too high / low / unintended

Hazard
- Side collision, Pedestrian / bicycle accident due to sudden acceleration
- Rear collision, Instable or not steerable vehicle due to locking wheels

b) Lateral: Left / Right; Steering / Destabilization; Yawing

Malfunction
- Yaw torque is too high / low / unintended
- Too less or too much steering angle / steering torque
- Oscillating Steering

Hazard
- Insufficient vehicle stability control, under / over-steering is possible
- Lane dereliction
- Accident with oncoming traffic
Elicitation of Sources of Technical Risk

- **Safety of intended functionality**
- **Nominal Performance**
- **Functional Inadequacy**

**Hazard**
- **Malfunction**
- **Situation**
- **Correct function**

**Malfunctions of E/E**

- **Expected / unexpected environmental impacts**
  - Misuse
  - Unusual situations
  - Not specified conditions
  - Regulations
  - Traffic

**Vehicle level boundary versus Item**

- Other non-functional impacts / effects
  - electrical, touch-protection
  - toxic
  - chemical
  - kinetic
  - radiation
  - thermic
  - nuclear
  - security

- **Safety of intended functionality**
- **Nominal Performance**
- **Functional Inadequacy**

**Scope of ISO26262**
Safety – Challenges for E-Mobility and Automated Driving

Standardization of Safety

The current standardization e.g. of ISO 26262, does not provide any best practices to be applied for those future challenges, such as:

- Fail operational systems
- Safety on performance requirements
- Safety of intended functionality
- Safety-in-use
- Control of unexpected events in the vehicle environment
- Both -> Security and Safety, etc.

How would you handle those issues in the future?
## Safety – Challenges for E-Mobility and Automated Driving
### Risk and Avoidance of Incidents, Hazards

Risk identification, typical standards

<table>
<thead>
<tr>
<th>Industry</th>
<th>Automotive</th>
<th>Railway</th>
<th>Machinery</th>
<th>Aviation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk</strong></td>
<td>ISO 26262</td>
<td>EN 50126</td>
<td>ISO 12100</td>
<td>14 CFR 25.1309</td>
</tr>
<tr>
<td></td>
<td>(EE)</td>
<td>(RAMS)</td>
<td>(EUC)</td>
<td>(all risk)</td>
</tr>
<tr>
<td><strong>Control of Risk</strong></td>
<td>ISO 26262</td>
<td>EN 50126/28/29</td>
<td>ISO 13849</td>
<td>DO 178C, DO 254, etc.</td>
</tr>
<tr>
<td></td>
<td>(EE)</td>
<td>(SW, System)</td>
<td>(EE+)</td>
<td>(SW, HW, ...)</td>
</tr>
<tr>
<td><strong>Safety Integrity</strong></td>
<td>ISO 26262</td>
<td>derived from IEC 61508</td>
<td>ISO 13849</td>
<td>ARP 4754A / ARP 4761 (Assessments)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IEC 61508 (ff.)</td>
<td></td>
</tr>
<tr>
<td><strong>Safety Design</strong></td>
<td>ECE, EGAS,...</td>
<td>various</td>
<td>C-Norms</td>
<td>e.g. ATA (Air Transport Association), ...</td>
</tr>
<tr>
<td><strong>Principles</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Bosch Engineering GmbH 2017. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Safety – Challenges for E-Mobility and Automated Driving

Methodology of SAE ARP4761

Development of Safety Requirements

ARP4761, Guidelines and Methods for Conducting the Safety Assessment

Process on Civil Airborne Systems and Equipment is an Aerospace Recommended Practice from SAE International.

In conjunction with ARP4754, ARP4761 is used to demonstrate compliance with 14 CFR 25.1309 in the U.S. Federal Aviation Administration (FAA) airworthiness regulations for transport category aircraft, and also harmonized international airworthiness regulations such as European Aviation Safety Agency (EASA) CS–25.1309.
Safety – Challenges for E-Mobility and Automated Driving

Zonal Analysis

Functional Dependencies

\[ F_B = \text{longitudinal vector} \]
\[ F_s = \text{lateral vector} \]
\[ F_R = \text{resulting vector} \]
Safety – Challenges for E-Mobility and Automated Driving

Perspective

Figure: New Perspective for Risk Evaluation
Safety – Challenges for E-Mobility and Automated Driving

Different Level of Automation

- **By-Wire**
  - Driver in Vehicle
  - Actuator ↔ HMI via E/E
  - Driver controls vehicle
  - Degradation / Driver

- **Remote controlled by driver**
  - Driver outside of vehicle
  - E/E controls vehicle
  - E/E and traffic environment controlled by driver
  - Driver only active in limited conditions/ situations

- **System controlled**
  - Driver outside of vehicle
  - E/E controls vehicle
  - E/E and traffic environment controlled by E/E
Safety – Challenges for E-Mobility and Automated Driving

Analysis

Violations of Objectives

Quality  Performance  Safety  Reliability Maintainability  Availability  Security

failure effect:
Consequence of a product failure

failure mode:
Product failure

Failure cause:
Causes for product failure

Failure effect:
Consequence of a product failure

Failure mode:
Product failure

Failure cause:
Causes for product failure

function
malfunction / failure,
Error mode
failure cause / fault

failure effect (top-failure, consequence, risk, threat, harm etc.)

Measures
- prevention
- avoidance, control
- detection,
- mitigation (of causes for failure)
- reduction (of the probability of failure effects)

External failure/ error cause / intrusion

Figure: Analyzing of non-functional requirements
Safety – Challenges for E-Mobility and Automated Driving

Conclusion

- State-of-the-Art requires continuously updating of present knowledge

- Compliance to standards does not lead automatically to “State-of-the-Art” (products).

- In common projects and common usage of traffic environment need common understanding of the safety strategy!

- Common understanding of safety strategy does not mean working after a cocking recipe!

System Safety Engineering
Thank you very much

Hans-Leo Ross

Engineering Safety and Base System (BEG-PT/ESB5)
Bosch Engineering GmbH | Postfach 13 50 | 74003 Heilbronn | GERMANY |
www.bosch-engineering.com
Tel. +49(173) 314 1579 | Fax +49(7062)911-7544 |
Hans-Leo.Ross@de.bosch.com